



FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Os Teoremas da incompletude de Gödel

Álvaro Carro Viqueira

2023/2024

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Os Teoremas da incompletude de Gödel

Álvaro Carro Viqueira

xullo, 2024

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo Proposto

Área de Coñecemento: Análise Matemática
Título: Os Teoremas da incompletude de Gödel
Breve descrición do contido
Neste traballo proponse facer unha breve introdución á lóxica formal moderna, cun énfase na completude ou falta dela nas teorías lóxicas. En particular, preténdese demostrar os teoremas da incompletude de Gödel, aportando ademais unha perspectiva histórica destes descubrimentos.

Agradecementos

Quero dar as grazas ó meu titor, Adrián, por apoiarme na idea inicial do tema e axudarme no desenvolvemento da mesma. Foi un luxo pescudar sobre lóxica baixo a súa supervisión, e sen el este traballo non tería xeito ningún.

Tamén ós meus amigos da facultade, cos que compartín esta experiencia (non atopo un adxectivo coa que describila) de elaborar o TFG.

E non podo esquecer ós meus pais. Se estades a ler isto, lembrade: podésvos saltar as demostracións, non fai falla lelas. Faríase imposible enumerar todas as cousas que fixestes por min, así que simplemente grazas, supoño.

Índice

Resumo	x
Introdución	i
1. Sistemas lóxicos	1
1.1. Cálculo proposicional	2
1.2. Cálculo predicativo	5
1.2.1. Linguaxe do cálculo predicativo	6
1.2.2. Semántica	9
1.2.3. Teoría formal para o cálculo predicativo	13
2. A completude de Gödel	17
2.1. Consistencia	18
2.2. Completude sintáctica	18
2.3. Completude semántica	21
3. Aritmetización	25
3.1. Teorías de primeira orde con igualdade	25
3.2. Aritmética de Peano	27
4. Os teoremas da incompletude	31
4.1. Recursividade	32

4.1.1. Funcións recursivas	32
4.1.2. Relacións recursivas	35
4.1.3. A función beta de Gödel	37
4.2. Numeración de Gödel	38
4.3. Primeiro teorema da incompletude	42
4.3.1. Diagonalización	43
4.3.2. Demostración	45
4.3.3. Alternativas	47
4.4. Segundo teorema da incompletude	48
5. Consecuencias	51
5.1. O programa de Hilbert despois de Gödel	51
5.2. Computabilidade	52
5.3. Legado	53
Índice alfabético	57
Bibliografía	60

Resumo

Os teoremas da incompletude de Gödel, formulados polo lóxico austríaco Kurt Gödel en 1931, tiveron un impacto revolucionario na matemática e na filosofía. O primeiro establece que en calquera sistema lóxico suficientemente potente como para incluír á aritmética dos números naturais, haberá sempre enunciados verdadeiros mais non demostrables dentro dese sistema. O segundo nega a posibilidade de probar a súa propia consistencia.

Neste traballo abordarase o estudo dos sistemas lóxicos, que son marcos formais nos que se poden expresar axiomas e demostrar teoremas. Probarase a completude de certos destes sistemas para posteriormente estudar a aritmética común, co obxectivo último de demostrar ambos teoremas da incompletude.

Abstract

Gödel's incompleteness theorems, formulated by the Austrian logician Kurt Gödel in 1931, had a revolutionary impact on mathematics and philosophy. The first establishes that in any sufficiently powerful logical system to include the arithmetic of natural numbers, there will always be true statements that cannot be proven within that system. The second denies the possibility of proving its own consistency.

In this work, we will address the study of logical systems, which are formal frameworks in which axioms can be expressed and theorems be proven. We will show completeness in certain of these systems in order to study ordinary arithmetic, with the ultimate goal of proving both incompleteness theorems.

Introdución

No ano 1931, o afamado Kurt Gödel publicou os seus teoremas da incompletude que, sen ningunha dúbida, son dos resultados con máis relevancia nas matemáticas do último século. Enuncian que a matemática máis elemental, a aritmética (a partir da cal constrúese o resto), é esencialmente incompleta. Isto quere dicir que existen afirmacións que non se poden demostrar, unha delas sendo a de “A aritmética non posúe contradicións”. Para chegar a probar este resultado cómpre saber que é exactamente a aritmética. Así pois, desenvolverase unha *formalización* da mesma, penetrando nos fundamentos da matemática, e en como interactúan símbolos, axiomas e regras da dedución entre eles. Por este motivo, moitos dos razoamentos desta disertación serán puramente *metamatemáticos*.

Definir a metamatemática é unha tarefa algo complexa, mais proporcionando unha distinción coa propia matemática, é posible entender a que nos estamos a referir. Certamente, facer matemáticas consiste en demostrar afirmacións, a partir de teoremas ou axiomas previos. Agora ben, que é exactamente unha demostración? E unha afirmación? Os razoamentos que levan a definir e traballar con estes conceptos son os que ocupan á metamatemática. Por exemplo, “ \mathbb{C} é un corpo alxebricamente pechado” é unha afirmación puramente matemática: un resultado demostrable en base a unhas definicións e teoremas coñecidos. Por outro lado “Os postulados de Peano son cinco” é unha afirmación expresada en metamatemáticas: non é máis que unha frase



Figura 1: Kurt Gödel, Princeton 1970 [6].

indicando que, ó escribir os postulados de Peano nun papel, cóntanse cinco oracións.

O libro de Elliot Mendelson *Introduction to mathematical logic* [8], foi clave para o desenvolvemento do traballo. A maioría das publicacións introdutorias á lóxica consultadas teñen unha achega similar ós teoremas da incompletude; porén, a notación de Mendelson resultoume quizais a máis accesible de todas. Así pois, gran parte dos resultados teóricos están adaptados das definicións, teoremas e demostracións do mesmo. Por outro lado, o libro dixital de Carlos Ivorra, *Lógica y Teoría de Conjuntos* [5], prestouse moi útil para a comprensión dos conceptos, debido ó alto carácter abstracto do tema.

O obxectivo do primeiro capítulo, *Sistemas lóxicos*, non é outro que o de establecer a linguaxe empregada ó longo do traballo. Facendo unha pequena introdución á lóxica siloxística e estoica, grazas a *Ancient Logic*. [2] de Suzanne Bozbien, e pasando polo cálculo proposicional, construírase una teoría matemática, chamada *cálculo predicativo*. A súa vez, darase unha visión interpretativa desta teoría, achegándose á linguaxe humana e o concepto da “verdade”. Aquí, *Historia de la lógica* [7] de Julián Lombraña foi fundamental, pois ofreceume unha visión moito máis ampla das linguaxes formais. Especialmente os capítulos 12 e 13, onde Lombraña explica os antecedentes ó cálculo predicativo de Gottlob Frege: De Morgan, Boole e mesmo Leibniz, cada un deles construíndo un cálculo de proposicións propio. En canto á información específica sobre o sistema de Frege, a publicación de Zalta [13] resultou de grande axuda.

Seguidamente pásase a introducir a figura de Kurt Gödel. No capítulo *A completeness de Gödel*, co interese último de probar dita característica do cálculo predicativo, danse unha serie de propiedades dos sistemas lóxicos: a consistencia, a decidibilidade, a completude sintáctica e mais a completude semántica. Non só neste, senón tamén nos seguintes capítulos, o principal apoio para a comprensión da obra do matemático foi *Kurt Gödel. The genius of metamathematics* [4], de William D. Brewer. O libro detalla moi extensamente a súa vida e todas as contribucións que fixo á ciencia. En particular, os capítulos 7, 8 e 9 (sobre os teoremas da completude, incompletude e computabilidade), ademais de notas esparexidas sobre a súa vida privada, axudáronme a comprender o persoeiro e afondar nel.

En terceiro lugar, precísase facer un pequeno inciso sobre teoría de números. Nomeadamente, a intención do capítulo *Aritmetización* é a de presentar, de maneira formal, a coñecida *aritmética de Peano*, coa súa linguaxe e axiomas propios. A notación seguida foi adaptada de Mendelson [8, seccións 2.8 e 3.1], mais para interpretar este “novo” sistema lóxico, resultou conveniente acudir a Lombraña [7, sección 13.5].

Chégase así ó capítulo con máis relevancia do traballo, *Os teoremas da incompletude*. O alemán David Hilbert era un *formalista*, e estaba convencido da capacidade da matemática (empregando os axiomas axeitados) para demostrar calquera resultado certo, e refutar calquera falso.

Practicamente toda a bibliografía empregada aborda este tema, mais [12] incide particularmente no impacto de Gödel nesta escola de pensamento. Seguindo de novo a notación de Mendelson [8], defínense as funcións recursivas e o sistema de numeración inventado polo austríaco. En último lugar demóstranse ambos os dous teoremas da incompletude, explicando paralelamente os paradoxos cos que se poden comparar.

Finalmente, remata a disertación co capítulo curto *Consecuencias*, onde analizo os obxectivos do programa de Hilbert despois da publicación dos teoremas da incompletude apoiándome en [12], así como as achegas (en certa maneira equivalentes) de Church e Turing á teoría da computabilidade, e a relación destas coa recursividade de Gödel. Termínase incidindo nalgunha curiosidade da particular vida de Kurt Gödel e o seu legado como matemático.

O lector poderá atopar un índice alfabético con todas os conceptos empregados ó longo do traballo na páxina 55.

Agardo que esta non sexa unha lectura demasiado pesada e, por encima de todo, que vos convide a reflexionar.

Deus existe, pois a matemática é consistente; e o demo existe, pois non podemos demostralo.

André Weil

Capítulo 1

Sistemas lóxicos

O filósofo grego antigo Aristóteles, que viviu uns 50 anos antes de Euclides, é xeralmente considerado o primeiro pai da lóxica formal, tendo desenvolvido un sistema de lóxica baseado no *siloxismo*. Esta palabra deriva das raíces grecas *syn* (“xuntos”, “combinar”) e *logos* (“razonar”), é dicir, a combinación de expresións razonadas. Segundo Aristóteles, consiste nun par de suposicións (chamadas *premis maior* e *premis menor*) que conducen a unha conclusión lóxicamente convincente. Tamén considerou a posibilidade de chegar a conclusións por *indución*, un proceso de extrapolación de fenómenos da realidade xa coñecidos ou observados a un caso concreto. Dúas premisas e a súa conclusión forman un siloxismo; varios ou moitos siloxismos poden combinarse como unha cadea racional para formar un argumento complexo de lóxica formal.

Dentro da sintáctica da conclusión coexisten o *suxeito* S mais o *predicado* P, que son partillados entre cada unha das premisas iniciais. Así, a premisa maior terá o chamado *termo medio* M como suxeito e compartirá o predicado P coa conclusión. Reciprocamente, a premisa menor conterà o suxeito S mais o predicado M. A inferencia dada por este sistema lóxico elimina o termo medio grazas á conexión lóxica de M e P para implicar a conclusión sobre S.

Exemplo 1.1. Un exemplo de siloxismo é o seguinte:

- Premisa maior: “Todos os homes son mortais”.
- Premisa menor: “Jordi Hurtado é un home”.
- Conclusión: “Jordi Hurtado é mortal”.

Aquí, “home” é o termo medio, é dicir, o suxeito/predicado M; “mortais” é o predicado P; e “Jordi Hurtado” é o suxeito S. É posible facer varias combinacións cos termos nas premisas e na conclusión, e foron catalogadas por Aristóteles, que as chamou *figuras*.

Ó longo deste traballo falarase de *teorías* e de *lóxicas* (ou *linguaxes*). Cabe resaltar entón a diferenza entre ambas as dúas. Unha lóxica é basicamente unha colección de símbolos que, concatenados entre eles, forman expresións. Ó engadir unhas regras de manipulación sobre eses símbolos, acompañadas de certos axiomas, créase unha teoría formal.

Definición 1.2. Unha *teoría formal* \mathcal{K} é un obxecto que satisfai as seguintes condicións:

1. Contén un conxunto (numerable) de símbolos, que, cando se combinan nunha sucesión, constrúen unha *expresión* de \mathcal{K} .
2. Hai un subconxunto do conxunto de expresións de \mathcal{K} chamado o conxunto das *frases ben formuladas* (denotadas por *fbf/fbfs*).
3. Contén un conxunto de *axiomas* de \mathcal{K} , que forman parte das *fbfs*.
4. Inclúe un conxunto finito de relacións R_1, \dots, R_n entre *fbfs*, chamadas *regras de inferencia*.

Definición 1.3. Unha *demostración* en \mathcal{K} é unha sucesión B_1, \dots, B_n de *fbf* tal que, para cada i , tense que B_i é un axioma ou un resultado directo (mediante regras de inferencia) de certas *fbfs* precedentes na sucesión.

Denótase *teorema* de \mathcal{K} á derradeira *fbf* dunha demostración en \mathcal{K} . Se B_1, \dots, B_n é unha demostración en \mathcal{K} , escríbese $B_1, \dots, B_{n-1} \vdash_{\mathcal{K}} B_n$ ou directamente $\vdash_{\mathcal{K}} B_n$ para sinalar que B_n é un teorema. No caso contrario, denotarase $\not\vdash_{\mathcal{K}} B_n$. Por acurtar, escríbese en moitas ocasións directamente $\vdash B_n$, sempre e cando isto non cause confusión.

Ó mesmo tempo, se B_1, \dots, B_n son *fbfs* calquera, escríbese $B_1, \dots, B_{n-1} \vdash_{\mathcal{K}} B_n$ para indicar que das *fbfs* B_1, \dots, B_{n-1} , tomadas como axiomas a maiores dos de \mathcal{K} , dedúcese B_n .

1.1. Cálculo proposicional

A lóxica de Aristóteles pode ser vista como unha lóxica de clasificación. Fai uso de catro termos lóxicos “todos”, “algúns”, “ser” e “non ser” (Exemplo 1.1) e, nese sentido, é bastante estática. Unha xeración máis tarde, e da man do filósofo grego Crisipo de Solos, naceu a lóxica *estoica* (do estoicismo, fundado por Zenón de Citio), considerada a miúdo a escola sucesora do siloxismo. Os estoicos precisaban dunha lóxica que examinara a causa mais o efecto. Por iso, desenvolveron unha lóxica de proposicións que usaba conectores máis complexos, como “se... entón...”, “... e...”, “ou... ou...” e “nin... nin...”. As proposicións estoicas defínense como un sistema de polo menos dúas premisas mais unha conclusión. Todas as intermedias comezan cun “Mais” ou un “Agora ben”, e a conclusión por un “Polo tanto”.

Exemplo 1.4. O seguinte é un argumento estoicista con dúas premisas:

- Se é de día, entón hai luz.
- Mais non hai luz.
- Polo tanto, non é de día.

Aínda que gran parte da súa obra foi perdida, o sistema sobreviviu reinventado polo monxe francés Pedro Abelardo (s. XII).

Coa chegada do século XX, volveu o interese pola lóxica no mundo das matemáticas. Grazas á labor divulgativa de Giuseppe Peano (1858-1932) e de Bertrand Russell (1872-1970), reviviron os resultados acadados polo matemático alemán Gottlob Frege (1848-1925), considerado agora coma o lóxico máis importante da historia xunto con Aristóteles. Segundo Susanne Bozbien [2, sección 5], a súa filosofía da lóxica compartía una cantidade sorprendente de similitudes con aquela de Crisipo. A súa contribución máis destacada consistiu en matematizar a linguaxe da lóxica e dar unha nova vida a unha disciplina que xa parecía ter chegado ó seu límite.

O problema que rondaba a cabeza de Frege era a existencia de verdades obxectivas. Isto relaciónase co problema de *dedución* fronte á *indución*, o problema de xuízos analíticos fronte a xuízos sintéticos, ou o problema da seguridade no coñecemento fronte á probabilidade no coñecemento. Todo isto viña arrastrado en filosofía dende hai séculos, pero o alemán enfrontouno dunha forma particular. El cría que si existen *verdades obxectivas*, independentes das observacións experimentais e por ende independentes da subxectividade. Na liña de Descartes [11], pensa que a solución está nas matemáticas e no método dedutivo; é dicir, partir dun axioma (unha verdade que non necesita demostración) para chegar a un resultado cen por cen “verdadeiro” mediante cadeas de razoamento. Pero Frege vai máis aló e cuestiónase: como se fundamentan as matemáticas? como se da este encadeamento? Para fundamentar as matemáticas na lóxica, con toda unha serie de normas correctas que nos permitan deducir sempre os teoremas das matemáticas, terá que facer algo inmenso: construír unha linguaxe acompañada de todas as súas regras. É a isto o que adicaría gran parte do seu traballo e polo que é coñecido como o segundo pai da lóxica matemática formal.

En primeiro lugar, Frege comeza estudando a lóxica proposicional sinxela, dende a base aristotélica, coa intención de crear algo máis perfecto e completo. Na súa obra *Begriffsschrift* [13, sección 2.1], que quere dicir “a escritura dos conceptos” constrúe unha teoría formal para a lóxica proposicional, cunha linguaxe propia arroupada dunha serie de leis e regras para o cálculo e demostración dos teoremas.

Definición 1.5. Unha *teoría de orde cero* \mathcal{K}_0 é unha teoría formal contendo:

- Símbolos:

1. *Conectores primitivos*: \neg (negación) e \rightarrow (condicional).
2. Os signos de puntuación: paréntesis esquerdos “(”, dereitos “)”, e vírgulas “,”.
3. Un conxunto de *letras de afirmación* A_1, A_2, \dots

- Frases ben formuladas (*fbf*/*fbfs*):

1. Todas as letras de afirmación.
2. $(\neg B)$ e $(B \rightarrow C)$, sendo B e C frases ben formuladas.

- Axiomas lógicos (sendo B, C , e D *fbfs* de \mathcal{K}_0):

$$\Delta_1: B \rightarrow (C \rightarrow B).$$

$$\Delta_2: (B \rightarrow (C \rightarrow D)) \rightarrow ((B \rightarrow C) \rightarrow (B \rightarrow D)).$$

$$\Delta_3: (\neg B \rightarrow \neg C) \rightarrow ((\neg C \rightarrow B) \rightarrow C).$$

- Unha única regra de inferencia, o *modus ponens*: C dedúcese de B e $(B \rightarrow C)$, é dicir, $B, (B \rightarrow C) \vdash C$.

Os símbolos e as *fbfs* son a linguaxe da teoría, é dicir, conforman a *lógica de orde cero*. Ó engadir os axiomas mais a regra de inferencia *modus ponens* obtense \mathcal{K}_0 .

O teorema a continuación pertence a calquera teoría de orde cero. Deste xeito, pódese demostrar a partir dos axiomas e a regra de inferencia. A proba atópase en [8, sección 1.4], mais non será desenvolvida aquí. Existe un resultado análogo para o tipo de sistema formal estudado na seguinte sección (Teorema 1.33).

Teorema 1.6 (da dedución). *Sexan dúas fbfs B, C e un conxunto de fbfs Γ .*

$$\text{Se } \Gamma, B \vdash C, \text{ entón } \Gamma \vdash (B \rightarrow C).$$

As expresións das teorías formais adoitan recibir un “significado”, coñecido comunmente como *interpretación* dunha teoría (ou dunha linguaxe). Neste senso, o cálculo proposicional clásico non é máis que unha interpretación de \mathcal{K}_0 onde as *fbfs* son precisamente as “proposicións”. Máis adiante (Definición 1.21) verase a definición rigorosa de interpretación para as lógicas de primeira orde.

Observación 1.7. Ademais dos conectores primitivos, pódense establecer os seguintes por definición:

1. $B \wedge C$ significa $\neg(B \rightarrow \neg C)$,

2. $B \vee C$ significa $\neg B \rightarrow C$,
3. $B \leftrightarrow C$ significa $(B \rightarrow C) \wedge (C \rightarrow B)$,

que son tres dos conectores clásicos do cálculo proposicional: “ \wedge ” (e), “ \vee ” (ou) e “ \leftrightarrow ” (se e só se).

Exemplo 1.8. No Cadro 1.1 amósase unha unha táboa de verdade, empregada para mostrar as relacións entre proposicións. Para cada combinación posible de valores de verdade (verdadero ou falso) dunhas *fbfs* iniciais, mostra o valor de verdade doutras compostas a partir delas. Nesta táboa aparecen ó comezo dúas *fbfs* A e B , polo que as posibles combinacións de valores de verdade son VV, VF, FV e FF. Ademais, $\neg A$ é verdadeira cando A é falsa, e viceversa. Por outro lado, $A \rightarrow B$ é sempre verdadeira agás no caso no que A é verdadeira e B é falsa.

A	B	$\neg A$	$A \rightarrow B$	$\neg A \rightarrow (A \rightarrow B)$
V	V	F	V	V
V	F	F	F	V
F	V	V	V	V
F	F	V	V	V

Cadro 1.1: Tautoloxía $\neg A \rightarrow (A \rightarrow B)$.

En conclusión, obtense a *fbf* $\neg A \rightarrow (A \rightarrow B)$, que resulta verdadeira en todos os escenarios posibles. As *fbfs* nesta situación coñécense como *tautoloxías*, e no caso contrario (se sempre resultan falsas) *contradiccións*.

Observación 1.9. En calquera teoría de orde cero \mathcal{K}_0 , os teoremas coinciden coas tautoloxías. Por exemplo, tense $\vdash \neg A \rightarrow (A \rightarrow B)$. Este feito coñécese como a *completude semántica* do cálculo proposicional [8, sección 1.4].

1.2. Cálculo predicativo

A *Begriffsschrift* marcou unha nova etapa, incluíndo un tratamento rigoroso das ideas de funcións e variables. De feito, Frege inventou a lóxica de predicados, en gran parte grazas á introdución de variables cuantificadas (mediante o *cuantificador universal* “ \forall ”) que eventualmente se tornaron ubicuas en matemáticas e lóxica, e que resolveron o problema da xeneralidade múltiple. As interaccións dalgúns conectores da lóxica anterior, especialmente “algún” e “todo”, non se comprendían moi ben: mesmo a distinción entre unha frase como “todo rapaz ama a algunha rapaza” e “algunha rapaza é amada por todo rapaz” só se podía representar de maneira moi artificial. Pola contra, o formalismo de Frege non tiña sequera dificultade en expresar as diferentes

interpretacións de frases como “todo rapaz ama a algunha rapaza que ama a algún rapaz que ama a algunha rapaza” e outras do estilo.

Con todo, a lóxica que vai ser seguida neste traballo será a desenvolta por Bertrand Rusell (1872-1970) e Alfred Whitehead (1861-1947) na súa obra *Principia Mathematica*¹ (1910-1912), pois foi a que Gödel empregou como base para os seus teoremas (xunto cos axiomas aritméticos de Peano), ó ser a máis completa [7, p. 386]. De acordo á súa introdución, *Principia Mathematica* tiña tres obxectivos:

1. Analizar da forma máis extensa posible as ideas da lóxica matemática minimizando a cantidade de nocións primitivas, axiomas e regras de inferencia.
2. Proporcionar unha linguaxe cunha capacidade de expresión suficiente para formalizar os enunciados matemáticos.
3. Solucionar o problema da existencia de paradoxos.

1.2.1. Linguaxe do cálculo predicativo

A principal novidade con respecto as lóxicas de orde cero, ademais da cuantificación, foi a inclusión de *variables*, símbolos de *función* e símbolos de *relación* ou predicado.

Definición 1.10. Unha *lóxica de primeira orde* \mathcal{L} é unha colección de signos divididos nas seguintes categorías:

- Símbolos:
 1. Os conectores proposicionais \neg (negación) e \rightarrow (implicación), mais o cuantificador universal \forall .
 2. Os signos de puntuación: parénteses esquerdos “(”, dereitos “)”, e vírgulas “,”.
 3. Un conxunto baleiro, finito ou numerable de *constantes* c_1, c_2, \dots
 4. Unha cantidade numerable de *variables* x_1, x_2, \dots
 5. Un conxunto non baleiro de *letras de predicado* (ou *relatores*) A_1, A_2, \dots
 6. Un conxunto baleiro, finito ou numerable de *letras de función* (ou *funtores*) f_1, f_2, \dots

Facendo unha equivalencia coa linguaxe común, empregaranse as constantes como “nomes” de obxectos (por exemplo, b pode significar Brais). Ademais, os relatores funcionarán de xeito similar ós “verbos”, divididos por *rango* segundo o número de compoñentes que precisen para ter senso. Así, “ H : ser un home” é un relator *monádico* ou de rango 1 ($H(b)$)

¹Non confundir con *Philosophiæ naturalis principia mathematica*, de Sir Isaac Newton.

significa que Brais é un home), mentres que “ A : ser amigos” é un relator *diádico* ou de rango 2 ($A(b, c)$ pode significar que Brais e Claudia son amigos). Exemplos de relatores moi empregados en matemáticas son “ \in ”, “ \subset ”, “ $=$ ” ou “ \leq ”.

Por claridade, e sempre que non haia perigo de confusión, empregaranse as letras x, y, \dots para denotar as variables nas lóxicas formais. As variables usaranse sempre xunto ós cuantificadores. Por exemplo, $(\forall x)H(x)$ significa que para todo x , x é un home ou, o que é o mesmo, que soamente hai homes. En xeral, $(\forall x)P(x)$ significa que a propiedade P acontece para todo x , ou que é o mesmo, que todo ten a propiedade P .

Por outro lado, os funtores complétanse con obxectos e dan outro como froito. Seguindo os exemplos anteriores, poderíamos ter un functor diádico (V : o máis vello) polo cal a sentencia (Vbc) devolvería como obxecto ó máis vello de entre Brais e Claudia.

- Termos:

1. As variables e constantes individuais.
2. As expresións da forma $f_k(t_1, t_2, \dots, t_n)$, onde f_k é un functor n -ádico e cada t_i é un termo.

Entón, os termos equivalerán ós substantivos ou ás frases feitas a partir deles. Por exemplo: “un”, “catro” ou “catro máis x ”.

- Frases ben formuladas (*fbf*/*fbfs*):

1. As fórmulas da forma $A_k(t_1, t_2, \dots, t_n)$ (chamadas *fbfs atómicas*), onde A_k é unha letra de predicado e cada t_i é un termo.
2. $(\neg B)$, $(B \rightarrow C)$ e $((\forall y)B)$, onde B e C son *fbfs* e y é unha variable.

A lóxica de primeira orde aplícase sobre “individuos” membros dun “dominio de individuos”. O significado destes individuos depende do sistema ao que se aplique a lóxica; poden ser nomes de persoas, números ou frases. Por exemplo, no caso da aritmética ordinaria, son os números naturais, membros do dominio \mathbb{N} . Os individuos poden aparecer como variables (con valores determinados polas frases nas que aparecen) ou constantes, se os seus valores están fixados de antemán.

Unha teoría formal sobre esta clase de lóxica emprega unha linguaxe \mathcal{L} , con símbolos que dependen moito de cada autor. Algunhas propiedades de interese neste estudo son a *consistencia* e a *completude*. A primeira evita absurdos, pois require que non se poidan demostrar unha afirmación máis a contraria á vez. Por outra banda, a completude (sintáctica) garante que toda afirmación ben construída ten unha demostración no sistema (ou, no seu lugar, a súa negación).

Observación 1.11. Non é preciso introducir o cuantificador existencial \exists (nin o seu oposto, \nexists) como símbolo da lóxica, pódese ver que $(\exists x)B$ equivale intuitivamente a $\neg((\forall x)(\neg B))$. Empregárase o símbolo \exists como método de simplificar a notación. Ademais, usaranse tamén os conectores clásicos do cálculo proposicional introducidos na Observación 1.7: “ \wedge ”, “ \vee ” e “ \leftrightarrow ”.

Observación 1.12. Poderíase considerar como parte da linguaxe ó *descriptor* “tal que”, a miúdo representado co símbolo “|”. Por exemplo, a expresión $x|A(x, c)$ significaría “o x tal que x é amigo de Claudia. Porén, polos problemas que poida causar non se empregará este conector lóxico. Bertrand Russell dixo nunha ocasión: “O actual rei da Francia é calvo”, afirmación que se podería traducir a linguaxe formal na forma $C(x|ARF(x))$. Acontece que na actualidade Francia non ten rei, $(\forall x)\neg ARF(x)$, e xorde un problema de interpretación. Para máis información con respecto ó descriptor, consultar [5].

O feito de falar de lóxicas de orde cero, un, etc, induce a preguntarse se poden existir outras de orde maior. Así pois, a lóxica de segunda orde traballa con entidades máis complexas ca individuos (conxuntos, propiedades de individuos, clases...), o que a fai máis poderosa para achar conclusións, ó mesmo tempo que se torna máis complicada nun senso metamatemático (Gödel demostraría a súa incompletude semántica, é dicir, a existencia de afirmacións verdadeiras que non se poden demostrar).

Coa fin de empregar os parénteses dunha maneira máis eficiente, así como para facilitar a lectura e manexo das expresións, establécese a seguinte orde de prioridade con respecto ós símbolos:

$$\neg, \wedge, \vee, (\forall x), (\exists x), \rightarrow, \leftrightarrow.$$

Definición 1.13. Enténdese unha *instancia* dunha variable nunha *fbf* como unha aparición da variable en cuestión. Por exemplo, en $B(x, y) \rightarrow C(x)$, a variable x ten dúas instancias.

Definición 1.14. Dise que unha instancia de x está *anoada* nunha *fbf* B se forma parte da expresión dun cuantificador $(\forall x)$ de B ou está afectada polo mesmo. No caso contrario diremos que a instancia de x é *libre* en B .

Unha variable x está anoada (é libre) en B se ten unha instancia anoada (libre) en B . Nótese que unha variable pode ser libre e estar anoada ó mesmo tempo. Por exemplo, a variable x na *fbf* $(\forall x)A(x) \rightarrow B(x)$.

De xeito semellante, un termo t é *libre para x en B* se non hai instancias de x en B afectadas por cuantificadores da forma $(\forall y)$, sendo y outra variable distinta en t . Esta definición é vantaxosa, pois o feito de que un termo sexa libre para unha variable x garante que, ao substituír toda instancia libre de x polo termo, ningunha das variables do termo ficará anoada.

Exemplo 1.15. Na *fbf* $(\forall x)A_1(x, y)$, as dúas instancias de x están anoadas, mentres que a

única instancia de y é libre (non está afectada por un $(\forall y)$). O termo $f(x, y)$ é libre para x na fbf $(\forall z)A_1(x, y, z)$, mais non o é na fbf $(\exists y)A_1(x, y, z)$.

Definición 1.16. Unha fbf na que todas as variables están anoadas dirase *pechada*.

A *clausura* dunha fbf B obtense engadindo cuantificadores universais correspondentes a cada unha das variables libres.

Exemplo 1.17. A clausura da seguinte fbf :

$$A_1(x_1) \rightarrow (\forall x_2)A_2(x_2, x_5),$$

é a nova fbf pechada:

$$(\forall x_1)(\forall x_5)(A_1(x_1) \rightarrow (\forall x_2)A_2(x_2, x_5)).$$

Observación 1.18. Téñense os seguintes resultados:

1. O termo x é libre para x en calquera fbf .
2. Un termo que non contén variables é libre para calquera variable en calquera fbf .
3. Un termo é libre para calquera variable en B se ningunha das súas variables está anoada en B .
4. Calquera termo é libre para x en B se B non contén instancias libres de x .

Observación 1.19. Ó considerar unha fbf B , a miúdo escribírase $B(x_1, \dots, x_n)$ para indicar que as variables x_1, \dots, x_n son libres en B . Esta notación non exclúe outras variables de aparecer en B , soamente indica cales non están anoadas.

1.2.2. Semántica

Os estoicos de Crisipo foron dos primeiros en introducir o concepto de *interpretación* dunha linguaxe, definindo unha especie de “esquemas” nos que poder xulgar a forma lóxica do argumento en cuestión, sen atender a posible veracidade ou falsidade del. Estes esquemas difiren do argumento en si por ter números ordinais no lugar dos asertivos.

Exemplo 1.20. A forma esquemática do argumento estoicista do Exemplo 1.4 é:

- Se o 1º, o 2º.
- Mais non: o 2º.
- Polo tanto, non: o 1º.

Así pois, o argumento do Exemplo 1.4 é unha interpretación deste esquema.

Definición 1.21. Unha *interpretación* \mathcal{M} dunha lóxica de primeira orde \mathcal{L} consiste dos seguintes elementos:

1. Unha colección U de obxectos chamada o *universo* de \mathcal{M} .
2. Un criterio que asocia un *elemento* $M(c_i) \in U$ a cada constante $c_i \in \mathcal{L}$.
3. Un criterio que asocia unha *relación* n -ádica $M(A_i) \subset U^n$ a cada relator n -ádico $A_i \in \mathcal{L}$.
4. Un criterio que asocia unha *función* (en ocasións chamada *operación*) n -ádica $M(f_i) : D^n \rightarrow D$ a cada funtor n -ádico $f_i \in \mathcal{L}$.

linguaxe \longrightarrow interpretación

Exemplo 1.22. Considérese a linguaxe \mathcal{L} (Definición 1.10) e a seguinte interpretación \mathcal{M} :

1. O universo U dos números naturais positivos.
2. $M(c_1)$ é o número 0.
3. $M(A_1)$ é a relación diádica “=”, e $M(A_2)$ é a relación diádica “ \leq ”.
4. $M(f_1)$ e $M(f_2)$ son as funcións suma e produto usuais (diádicas).

Entón, a *fbf* $(\forall y)A_2(x, y)$ correspóndese coa frase interpretada en metalinguaxe “para cada natural y , x é máis pequeno”. Por outra banda, a *fbf* $(\nexists x)A_1(f_1(x, 0), 0)$ afirma que non existe ningún natural positivo x tal que $x + 0 = 0$. Esta derradeira afirmación é intuitivamente verdadeira, o que convida a pensar se pode haber unha definición formal do concepto da “verdade”.

Os conceptos de “verdade” e “falsidade” (primeiramente intuitivos) pertencen exclusivamente ás interpretacións: soamente unha expresión “do mundo real” pode ser verdadeira ou falsa. O obxectivo último da sección é determinar un concepto de “verdade” máis amplo, non anoado a ningunha interpretación. Quérese definir a *validez lóxica*, unha propiedade que poden cumprir as expresións lógicas nas teorías formais.

Por este motivo, cómpre definir formalmente o concepto da *verdade*, comezando primeiro polo de *satisfactoriedade*. Como paso preliminar, constrúese unha función γ “de significado”, que asigne a cada termo t da linguaxe un elemento $\gamma(t)$ no universo da interpretación. Sexa \mathcal{M} unha

interpretación dunha linguaxe \mathcal{L} , sexa U o seu universo e sexa (s_1, s_2, \dots) unha sucesión finita de elementos de U . Esta conterà tantos elementos como se precisen, concretamente tantos como número de variables da linguaxe haia na expresión en estudo. Entón defínese γ do seguinte xeito:

1. Se t é unha variable x_i , sexa $\gamma(x_i) = s_i$.
2. Se t é unha constante c_i , sexa $\gamma(c_i) = M(c_i)$.
3. Se t_1, \dots, t_n son termos, f_i un funtor e $M(f_i)$ a súa función correspondente en U , tense $\gamma(f_i(t_1, \dots, t_n)) = M(f_i)(\gamma(t_1), \dots, \gamma(t_n))$.

Exemplo 1.23. No caso da interpretación \mathcal{M} do Exemplo 1.22, a *fbf*

$$f_1(x_1, f_2(x_2, c_1)),$$

transformada pola función de significado γ , torna en:

$$s_1 + (s_2 \cdot 0).$$

Definición 1.24. Sexan $A_i(t_1, \dots, t_n)$, B e C tres *fbfs*, e (s_1, s_2, \dots) unha sucesión de elementos do universo U dunha interpretación \mathcal{M} . Defínese a *satisfatoriedade* de forma inductiva:

1. (s_1, s_2, \dots) *satisfai* $A_i(t_1, \dots, t_n)$ se e só se $M(A_i)(\gamma(t_1), \dots, \gamma(t_n))$. Nótese que a función γ depende da sucesión sempre e cando algún dos termos conteña variables. Nese caso, algún $\gamma(t_j)$ conterà algún s_k .
2. (s_1, s_2, \dots) *satisfai* $\neg B$ se e só se (s_1, s_2, \dots) non *satisfai* B .
3. (s_1, s_2, \dots) *satisfai* $B \rightarrow C$ se e só se (s_1, s_2, \dots) *satisfai* C ou non *satisfai* B .
4. (s_1, \dots, s_i, \dots) *satisfai* $(\forall x_i)B$ se e só se (s_1, \dots, u, \dots) *satisfai* B para todo elemento u do universo, onde (s_1, \dots, u, \dots) denota a sucesión obtida de substituír na orixinal o elemento x_i polo elemento u . Nótese que en consecuencia, (s_1, s_2, \dots) tamén *satisfai* B .

Intuitivamente, unha sucesión (s_1, s_2, \dots) de elementos dunha interpretación *satisfai* unha *fbf* se, ó substituír as instancias libres de x_i (para cada x_i) na *fbf* por cada s_i correspondente, o enunciado resultante cúmprese.

Exemplo 1.25. Sexa U o conxunto dos números reais, $M(A_1)$ a relación diádica “ \leq ” e $M(f_1(x))$ a función e^x . Entón unha sucesión (s_1, s_2, \dots) de números reais *satisfai* $A_1(f_1(x_1), x_3)$ se e só se $e^{s_1} \leq s_3$. Tomando a sucesión (lémbrese, finita) $(1, 3)$ tense que $e^1 \leq 3$, co cal pódese dicir que a sucesión $(1, 3)$ *satisfai* a *fbf* $A_1(f_1(x_1), x_3)$. Por outra banda, $(2, 3)$ non o fai.

Definición 1.26. Unha *fbf* B é *verdadeira* baixo a interpretación \mathcal{M} (denótase $\models_{\mathcal{M}} B$) se e só se calquera sucesión (s_1, s_2, \dots) de elementos de U satisfai B . Se ningunha o fai, B dirase *falsa*.

Exemplo 1.27. A *fbf* $B : (\forall x)A_1(f_2(x, 0), 0)$ é verdadeira baixo a interpretación \mathcal{M} do Exemplo 1.22. Certamente, unha sucesión (s_1, s_2, \dots) satisfai B se e só se $s_1 \cdot 0 = 0 \forall s_1$. Ó estar a considerar o universo dos números naturais, esta afirmación cúmprese para calquera sucesión.

Observación 1.28. Nótese que existen *fbfs* que non son nin verdadeiras nin falsas. Considérese por exemplo a *fbf* $B : A_1(f_1(2, x), 4)$ baixo a interpretación \mathcal{M} do Exemplo 1.22. Unha sucesión (s_1, s_2, \dots) satisfai B se e só se $2 + s_1 = 4$. O único número real que cumpre esta igualdade é $s_1 = 2$. Así pois, B non é verdadeira ($2 + 3 \neq 4$) nin falsa ($2 + 2 = 4$).

Para B, C e D *fbf*, e unha interpretación \mathcal{M} , téñense os seguintes resultados:

- I** B é falsa (verdadeira) baixo \mathcal{M} se e só se $\neg B$ é verdadeira (falsa) baixo \mathcal{M} .
- II** Non se poden dar $\models_{\mathcal{M}} B$ e $\models_{\mathcal{M}} \neg B$ á vez.
- III** $\models_{\mathcal{M}} B$ e $\models_{\mathcal{M}} B \rightarrow C$ deducen $\models_{\mathcal{M}} C$.
- IV** $\models_{\mathcal{M}} B$ se e só se $\models_{\mathcal{M}} (\forall x)B$.
- V** Toda instancia² dunha tautoloxía é verdadeira (baixo calquera interpretación).
- VI** Se o termo t é libre para a variable x en $B(x)$, entón $(\forall x)B(x) \rightarrow B(t)$ é verdadeira (baixo calquera interpretación).
- VII** Se x está anoada en B , entón $(\forall x)(B \rightarrow C) \rightarrow (B \rightarrow (\forall x)C)$ é verdadeira (baixo calquera interpretación).

O concepto verdadeiramente importante, que xa viña sendo investigado dende a antiga Grecia, era o de unha forma de “verdade” que transcendera unha interpretación en particular. Interesa entón definir unha *validez lóxica*, unha verdade absoluta que non dependese do significado que alguén lle poida dar.

Definición 1.29. Unha *fbf* B de \mathcal{L} é *loxicamente válida* se e só se é verdadeira baixo calquera interpretación. Denótase $\models_{\mathcal{L}} B$ ou, se non causa confusión, simplemente $\models B$.

Definición 1.30. Un *modelo* M dunha teoría \mathcal{K} é unha interpretación na cal todo teorema en \mathcal{K} é verdadeiro en M . Dise *numerable* se o seu universo é numerable.

²Unha instancia dunha tautoloxía obtense substituíndo proposicións por relatores. Por exemplo, de $P \rightarrow Q$ sae $A_1(x) \rightarrow A_2(y)$.

1.2.3. Teoría formal para o cálculo predicativo

Dispoñendo xa dunha linguaxe de primeira orde, cómpre desenvolver un sistema de inferencia: unhas regras que permitan, partindo dunha cantidade finita de teoremas dados por certos (axiomas), demostrar outros como conclusión.

Definición 1.31. Unha *teoría de primeira orde* \mathcal{K}_1 nunha linguaxe \mathcal{L} é unha teoría formal cuxos símbolos e *fbfs* son os mesmos que en \mathcal{L} e ademais posúe:

1. Axiomas lóxicos (sendo B, C , e D *fbfs* de \mathcal{L}):

$$\Delta_1: \quad B \rightarrow (C \rightarrow B).$$

$$\Delta_2: \quad (B \rightarrow (C \rightarrow D)) \rightarrow ((B \rightarrow C) \rightarrow (B \rightarrow D)).$$

$$\Delta_3: \quad (\neg B \rightarrow \neg B) \rightarrow ((\neg C \rightarrow B) \rightarrow C).$$

$$\Delta_4: \quad (\forall x)B(x) \rightarrow B(t), \text{ se } B(x) \text{ é unha } \textit{fbf} \text{ de } \mathcal{L} \text{ e } t \text{ é un termo libre para } x \text{ en } B(x).$$

$$\Delta_5: \quad (\forall x)(B \rightarrow C) \rightarrow (B \rightarrow (\forall x)C), \text{ se } B \text{ non contén instancias libres de } x.$$

2. Axiomas propios, particulares a cada teoría.

3. Regras de inferencia:

$$a) \textit{ Modus ponens: } B, (B \rightarrow C) \vdash C.$$

$$b) \textit{ Xeneralización: } B \vdash (\forall x)B.$$

Exemplo 1.32. Un exemplo de teoría de primeira orde é a *teoría de grupos*. Esta considera unha linguaxe \mathcal{L} cunha única constante c_1 , un funtor diádico f_1 (escribírase $+$) e un relator diádico A_1 (escribírase $=$). Ademais dos lóxicos, posúe os seguintes axiomas propios:

$$\textit{Elemento neutro:} \quad (\forall x)(x + 0 = 0).$$

$$\textit{Elemento inverso:} \quad (\forall x)(\exists y)(x + y = 0).$$

$$\textit{Asociatividade:} \quad (\forall x)(\forall y)(\forall z)(x + (y + z) = (x + y) + z).$$

Mais os catro axiomas correspondentes á *reflexividade*, *simetría*, *transitividade* e *substitución* da igualdade.

Ó igual que co cálculo proposicional, a continuación preséntase un resultado en certa maneira complementario á regra de inferencia *modus ponens*.

Teorema 1.33 (da dedución). *Sexan dúas fbfs* B, C *e un conxunto de fbfs* Γ . *Se:*

1. $\Gamma, B \vdash C$,

2. Para cada fbf D de Γ na demostración de C , e cada xeneralización $(\forall x_k)D$, x_k está anoada en B .

Entón $\Gamma \vdash B \rightarrow C$.

Demostración. Supóñase a demostración da forma $D_1, \dots, D_{n-1}, D_n = C$. A intención é demostrar $\Gamma \vdash B \rightarrow D_k$, con $k = 1, \dots, n$ empregando o principio de indución.

Para $k = 1$, tense que D_1 ou ben é un axioma, ou ben pertence a Γ , ou ben é o propio C . En todo caso, fica nas hipóteses do Teorema da dedución para o cálculo proposicional 1.6 e, en consecuencia, $\Gamma \vdash B \rightarrow D_1$.

Para $k = j$, supóñase certo para $k = 1, \dots, j - 1$. Se D_j ou ben é un axioma, ou ben pertence a Γ , ou ben é o propio C , a demostración séguese tamén do Teorema da dedución para o cálculo proposicional. Da mesma maneira, no caso no que D_j se obteña por *modus ponens* a partires dos anteriores. Resta entón o caso no que se obtivo por *xeneralización*. Supoñendo que D_j é a fbf $(\forall x_l)B_m$, con $m < j$, existen dous casos diferenciados:

- B non pertence á demostración de D_m . Por hipótese, $\Gamma \vdash D_m$, e xeneralizando:

$$\Gamma \vdash D_j.$$

Grazas ó axioma Δ_1 ,

$$\vdash D_j \rightarrow (B \rightarrow D_j),$$

e por *modus ponens* obtense o resultado desexado, $\Gamma \vdash B \rightarrow D_j$.

- B si pertence á demostración de D_m e, por hipótese, x_l está anoado en B . Por hipótese mais o axioma Δ_5 :

$$\Gamma \vdash (\forall x_l)(B \rightarrow D_m) \rightarrow (B \rightarrow (\forall x_l)D_m).$$

Xeneralizando na hipótese de indución:

$$\Gamma \vdash (\forall x_l)(B \rightarrow D_m),$$

e finalmente, por *modus ponens*, $\Gamma \vdash B \rightarrow (\forall x_l)D_m$, é dicir, $\Gamma \vdash B \rightarrow D_j$.

Grazas ó principio de indución, tense $\Gamma \vdash B \rightarrow D$. □

O Teorema da dedución afirma esencialmente que, para demostrar unha implicación $B \rightarrow C$, podemos supoñer B e intentar chegar a C . Unha hipótese máis forte induce o seguinte corolario.

Corolario 1.34. *Se $\Gamma, B \vdash C$ e a fbf B é pechada, entón $\Gamma \vdash B \rightarrow C$.*

Demostración. É directo, cúmprense as dúas condicións do Teorema da dedución 1.33. Se B é pechada, toda variable x_k está anoada en B . \square

Definición 1.35. Toda teoría de primeira orde na linguaxe \mathcal{L} que non posúa axiomas propios coñecerase como *cálculo predicativo* \mathcal{P} .

Unha propiedade moi interesante e útil do cálculo predicativo é a seguinte:

Proposición 1.36. *Toda instancia dunha tautoloxía é un teorema en \mathcal{P} .*

Demostración. Grazas á completude semántica do cálculo proposicional (Observación 1.9), tense que cada tautoloxía é un teorema en \mathcal{K}_0 . Como \mathcal{K}_0 contén tamén os axiomas Δ_1 , Δ_2 , Δ_3 mais *modus ponens*, todo teorema de \mathcal{K}_0 é un teorema de \mathcal{P} . Polo tanto, toda instancia dunha tautoloxía é un teorema do cálculo predicativo. \square

Proposición 1.37. *No cálculo predicativo, todo teorema é loricamente válido, ou o que é o mesmo,*

$$se \vdash B, \text{ entón } \models B.$$

Demostración. Primeiramente móstrase a validez lóxica dos axiomas:

Grazas ó resultado **V** sobre verdades lóxicas, sábese que toda instancia nunha tautoloxía sempre é verdadeira (baixo calquera interpretación). Deste xeito, os axiomas Δ_1 , Δ_2 e Δ_3 , por ser tautoloxías, son loricamente válidos. Ademais, os resultados **VI** e **VII** demostran directamente a validez lóxica dos axiomas Δ_4 e Δ_5 .

Por mor dos resultados **III** e **IV**, as dúas regras de inferencia do *modus ponens* e da *xeneralización* preservan a validez lóxica. Ó derivaren dos axiomas mediante estas regras, todos os teoremas son tamén loricamente válidos. \square

Observación 1.38. En consecuencia, toda interpretación do cálculo predicativo é un modelo.

Exemplo 1.39. Un exemplo de *fbf* que non é un teorema do cálculo predicativo pode ser o seguinte:

$$(\forall x)(\exists y)A_1(x, y) \rightarrow (\exists y)(\forall x)A_1(x, y).$$

Considerando unha interpretación na que o universo é o conxunto dos números enteiros e o relator $A(x, y)$ é a relación “ $x < y$ ”, tense que a *fbf* $(\forall x)(\exists y)A_1(x, y)$ é verdadeira (para cada enteiro existe outro máis pequeno ca el) pero $(\exists y)(\forall x)A_1(x, y)$ é falsa (o conxunto dos enteiros non ten supremo). Porén, o exemplo proposto non é unha *fbf* loricamente válida e en conclusión non é un teorema do cálculo predicativo.

A propiedade descrita na Proposición 1.37 chámase *solidez* (en inglés, *soundness*) e as teorías que a cumpren, teorías *sólidas*. Precisamente o obxectivo do seguinte capítulo será demostrar a propiedade recíproca, a chamada *completude semántica*.

Capítulo 2

A completude de Gödel

Kurt Friedrich Gödel naceu un 28 de abril de 1906 en Brno, na Chequia do Imperio Austrohúngaro, no seno dunha familia acomodada. Cando era pequeno, adoitaba recibir o sobrenome “Señor Por Que” (*Herr Warum*), pola súa insaciable curiosidade. Aos 18 anos ingresou na Universidade de Viena, co obxectivo inicial de estudar física teórica, aínda que máis tarde decantárase pola teoría de números e a lóxica. O interese por esta última ten moito que ver coas súas asistencias ás reunións do famoso *Círculo de Viena*, organismo científico-filosófico fundado polo austríaco Moritz Schlick (1882-1936). Foi precisamente un seminario impartido por Schlick [4, capítulo 8] sobre o libro de Bertrand Russell *Introducción á filosofía matemática* o que o fixo interesarse pola rama matemática da lóxica.

Coma tantos outros científicos excepcionais, un dos talentos especiais de Gödel era facer as preguntas axeitadas, en particular aquelas que outras persoas ou ben non pensarán, ou ben non se atreverán a preguntar. Esta habilidade de Gödel faise evidente na súa elección de tema de tese de doutoramento, á que chegou por si mesmo. O tema que elixiu derivou do programa de crear unha base axiomática-lóxica para a teoría de números, comezado por Frege e Peano e continuado por Russell e Whitehead, e por Hilbert e a súa escola. Peano definiu un conxunto de axiomas para a aritmética, mentres que Frege desenvolveu unha linguaxe, a lóxica de primeira orde, conformando así un primeiro cálculo predicativo.

O que Gödel fixo na súa tese, *The Completeness of the Axioms of logical Functional Calculus*, foi considerar e demostrar a consistencia e a completude (semántica) do cálculo predicativo, dúas propiedades consideradas importantes para establecer a validez dun sistema lóxico. No camiño introduciu o teorema de compacidade, considerado por algúns como o resultado máis importante da súa tese. Non se mencionou especificamente na propia tese, pero foi declarado na publicación resultante no 1930.

2.1. Consistencia

Definición 2.1. Unha teoría de primeira orde dise *consistente* se, para todo teorema, a súa negación non o é; é dicir, non se pode demostrar un teorema e o seu contrario (se $\vdash B$ entón $\not\vdash \neg B$). Noutro caso, dirase *inconsistente*.

Observación 2.2 (Principio de Explosión). Nunha teoría inconsistente existe unha *fbf* B tal que $\vdash B$ e $\vdash \neg B$. En consecuencia toda *fbf* é un teorema, por mor da tautoloxía $\neg P \rightarrow (P \rightarrow Q)$. Certamente, téñense os seguintes tres teoremas:

1. $\vdash B$,
2. $\vdash \neg B$,
3. $\vdash \neg B \rightarrow (B \rightarrow C)$.

O segundo máis o terceiro deducen $\vdash B \rightarrow C$. Aplicando neste último teorema *modus ponens* co primeiro, tense $\vdash C$, para unha *fbf* C arbitraria.

Este resultado provén do famoso principio lóxico *ex falso quodlibet* (en galego, “dunha contradición, todo segue”), probado por primeira vez polo filósofo francés Guillaume de Soissons no século XII.

Proposición 2.3. *O cálculo predicativo é consistente.*

Demostración. Se B e $\neg B$ fosen teoremas, serían tamén lóxicamente válidos (Proposición 1.37), o cal é imposible. \square

2.2. Completude sintáctica

Gödel era ben consciente da necesidade de diferenciar entre as propiedades sintácticas e semánticas dun sistema lóxico, xa dende o seu traballo de tese. En particular, a noción da completude é diferente no senso sintáctico (teórico da proba) e no senso semántico (teórico do modelo). De feito, Gödel empregou distinta terminoloxía para eses dous conceptos: chamou á completude no sentido semántico *vollständigkeit*, que se traduce directamente por “completude”; pero a completude no sentido sintáctico denominouna *entscheidungsdefinit*, que Dawson [4, p. 137] traduce como “decidibilidade”.

A intención desta sección non é demostrar a completude sintáctica do cálculo predicativo, senón introducir o concepto de forma rigorosa. Nos seus *Teoremas da incompletude*, Gödel probaría que certos sistemas formais máis poderosos ca este son esencialmente incompletos.

Lema 2.4. *Sexa unha fbf pechada B , e \mathcal{P}' a teoría resultante de engadir B como axioma ó cálculo predicativo \mathcal{P} . Se $\neg B$ non é demostrable en \mathcal{P} , entón \mathcal{P}' é consistente.*

Demostración. Por contradición, asúmase \mathcal{P}' inconsistente. Entón existe unha fbf C en \mathcal{P}' tal que

$$\vdash_{\mathcal{P}'} C \text{ e } \vdash_{\mathcal{P}'} \neg C.$$

A expresión $P \rightarrow (\neg P \rightarrow \neg Q)$ é unha tautoloxía, polo tanto $\vdash_{\mathcal{P}'} C \rightarrow (\neg C \rightarrow \neg B)$. Aplicando dúas veces *modus ponens*, $\vdash_{\mathcal{P}'} \neg B$. O emprego de B como axioma nunha demostración en \mathcal{P}' pódese ver como hipótese dunha demostración en \mathcal{P} , polo que $B \vdash_{\mathcal{P}} \neg B$.

Como B é pechada, do Corolario 1.34 dedúcese

$$\vdash_{\mathcal{P}} B \rightarrow \neg B.$$

Ó ser instancia dunha tautoloxía, tense

$$\vdash_{\mathcal{P}} (B \rightarrow \neg B) \rightarrow \neg B.$$

Aplicando *modus ponens*, $\vdash_{\mathcal{P}} \neg B$, o cal contradí a hipótese inicial. □

Unha diferenza entre a sintaxe (cálculo predicativo) e a semántica (modelos) é a necesidade que ten unha expresión de ser verdadeira ou falsa nun modelo dado, mentres que non existe requirimento ningún de que teña que ser demostrable ou refutable na teoría de referencia. Garantido xa que o cálculo predicativo ten un modelo, xorde entón a noción da completude sintáctica:

Definición 2.5. Unha teoría dise *completa* se, para calquera fbf pechada B , tense ou ben $\vdash B$ ou ben $\vdash \neg B$. Noutro caso, dirase *incompleta*.

Empregaranse as expresións *completude* e *completude sintáctica* co mesmo significado. Con todo, na seguinte sección verase outro concepto completamente distinto, a *completude semántica*.

Facendo un pequeno inciso, na actualidade unha teoría dise *decidible* (noción da completude sintáctica para Gödel) se existe un método algorítmico para determinar se unha fórmula arbitraria é un teorema ou non. Por exemplo, o cálculo proposicional é unha teoría incompleta pero decidible pois existen as táboas de verdade, que se poden empregar para determinar se unha fbf é lxicamente válida ou non. Así pois, a *decidibilidade* é unha versión (en certo sentido) máis forte da completude sintáctica. A seguinte definición será útil:

Definición 2.6. Unha *sentencia indecible* é unha fbf pechada B de unha teoría \mathcal{K} tal que nin ela nin a súa negación son demostrables.

Observación 2.7. É trivial que se unha teoría \mathcal{K} contén unha sentencia indecidible, entón é unha teoría incompleta.

No ano 1936, foi mostrado (de maneira independente) por Alonzo Church (1903-1955) e Alan Turing (1912-1954) que, en xeral, o cálculo predicativo non é unha teoría decidible. Aínda así, é complicado demostrar un resultado do estilo, ó non estaren exactamente determinados cales son os elementos que o conforman (constantes, funtores, relatores...). Porén, concretando o tipo de cálculo que se está a empregar pode demostrarse a súa decidibilidade. Por exemplo, o *cálculo predicativo monádico*, unha versión sen funtores e sendo todos os seus relatores de rango un, foi probado decidible polo loxicista alemán Leopold Löwenheim no 1915 [4].

O teorema a continuación mostrará que existen sistemas máis amplos que o cálculo predicativo nos que a súa completude si está garantida.

Definición 2.8. Unha teoría \mathcal{K}' é unha *extensión* doutra teoría \mathcal{K} se todo teorema da segunda tamén o é da primeira. Secasí, a teoría \mathcal{K}' conterá, alo menos, todas as constantes, relatores, funtores, variables e signos de puntuación da teoría orixinal.

Lema 2.9 (de Lindenbaum). *Se \mathcal{K} é unha teoría consistente, entón existe unha extensión completa e consistente de \mathcal{K} .*

Demostración. Sexa $(B_n)_{n \in \mathbb{N}}$ o conxunto de *fbfs* pechadas de \mathcal{K} . Defínese o seguinte conxunto de teorías $(T_n)_{n \in \mathbb{N}}$:

$$\begin{aligned} T_0 &= \mathcal{K} \\ T_n &= \begin{cases} T_{n-1}, & \text{se } \vdash_{T_{n-1}} \neg B_n, \\ T_{n-1} \text{ máis } B_n \text{ como axioma,} & \text{se } \not\vdash_{T_{n-1}} \neg B_n, \end{cases} \end{aligned}$$

A intención é demostrar que T , a teoría obtida tomando todos os axiomas das $(T_n)_{n \in \mathbb{N}}$, é unha extensión completa e consistente. T conterá como axiomas a todas aquelas *fbfs* pechadas de \mathcal{K} que non sexan demostrables. Claramente, T é unha extensión de T_i , para cada $i \in \mathbb{N}$, que son á súa vez extensións de \mathcal{K} .

- **Consistencia:** como \mathcal{K} é consistente, grazas ó Lema 2.4, cada T_i tamén o é, para todo $i \in \mathbb{N}$. Se T non fose consistente, existiría unha *fbf* tal que $\vdash_T C$ e $\not\vdash_T C$. Existe unha T_j contendo todas as demostracións destes dous teoremas, ou sexa que $\vdash_{T_j} C$ e $\not\vdash_{T_j} C$, o que é unha contradición.
- **completude:** as *fbfs* de T coinciden coas de \mathcal{K} . Sexa pois unha *fbf* $C = B_j$ de T . Tense que ou ben $\vdash_{T_{j-1}} \neg B_j$ ou ben $\not\vdash_{T_{j-1}} \neg B_j$, polo que $\vdash_{T_j} B_j$ ou $\vdash_{T_j} \neg B_j$. Porén, $\vdash_T B_j$ ou $\vdash_T \neg B_j$. □

Corolario 2.10. *Existe unha extensión completa do cálculo predicativo.*

Demostración. Resultado directo da consistencia do cálculo predicativo. □

Exemplo 2.11. A *aritmética de Presburger* é unha extensión do cálculo predicativo contendo dúas constantes ($\{0, 1\}$), un funtor ($+$), un relator ($=$) e os seguintes axiomas:

1. $\neg(0 = x+1)$, (0 non é o seguinte de ningún número)
2. $x+1 = y+1 \rightarrow x = y$, (inxectividade da función seguinte)
3. $x+0 = x$, (elemento neutro para a suma)
4. $x+(y+1) = (x+y)+1$, (propiedade asociativa)
5. $(P(0) \wedge \forall x(P(x) \rightarrow P(x+1))) \rightarrow \forall yP(y)$, sendo x libre en $P(x)$. (principio de indución)

A proba da súa completude foi dada polo matemático polaco Mojżesz Presburger no 1929 e radicaba en ir eliminando cuantificadores das expresións (ver [10]). No capítulo seguinte introdúcese a *aritmética de Peano*, unha extensión da aritmética de Presburger. Darase unha noción intuitiva dos seus axiomas (os de Presburger están contidos neles) e que, ó contrario que esta, a de Peano non é unha teoría completa

2.3. Completude semántica

No capítulo anterior xa se demostrou que os teoremas do cálculo predicativo son lxicamente válidos (Proposición 1.37). Ben, nesta sección verase que esta relación é en ambos sentidos, é dicir, toda *fbf* lxicamente válida é un teorema.

Proposición 2.12. *Toda teoría consistente \mathcal{K} admite un modelo numerable.*

A demostración da Proposición 2.12 é algo complicada. Baséase en estender a linguaxe de \mathcal{K} cunha cantidade numerable de novas constantes individuais c_1, c_2, \dots . Considéranse todas as *fbfs* cunha única variable libre B_1, B_2, \dots , e constrúese unha sucesión de sistemas formais $\mathcal{K}, \mathcal{K}_1, \mathcal{K}_2, \dots$, onde cada \mathcal{K}_i constrúese a partir de B_i e c_i . Aplicando o Lema de Lindenbaum 2.9, existe unha extensión \mathcal{T} consistente e completa. Finalmente constrúese unha interpretación cuxo universo é o conxunto de termos sen variables de \mathcal{T} . A proba completa pódese atopar en [8, capítulo 2.7].

Proposición 2.13. *Unha *fbf* é lxicamente válida se e só se tamén o é a súa clausura.*

Demostración. Convén probar primeiramente a propiedade **IV** da Definición 1.26 en xeral:

$$\models B \text{ se e só se } \models (\forall x_i)B.$$

\Rightarrow / Se $\models B$, entón baixo calquera interpretación, toda sucesión de elementos do seu universo (s_1, s_2, \dots) satisfai B . En particular, toda sucesión que difira doutra en como moito unha posición, i . Así, calquera sucesión satisfai $(\forall x_i)B$.

\Leftarrow / Asíumase $(\forall x_i)B$. Se (s_1, s_2, \dots) é unha sucesión de elementos do universo dunha interpretación, tense que calquera outra sucesión que difira da primeira en como moito unha posición i satisfai B . En consecuencia, toda sucesión satisfai B e $\models B$.

Razoando de forma indutiva sobre $(\forall x_{r_n}) \dots (\forall x_{r_1})B$, onde r_1, \dots, r_n proporcionan as variables que clausuran B , tense o resultado. \square

Proposición 2.14. *Unha fbf é un teorema en \mathcal{K} se e só se tamén o é a súa clausura.*

Demostración.

\Rightarrow / Se $\vdash B$, aplicando sucesivamente a regra de *xeneralización* obtense $\vdash (\forall x_{r_n}) \dots (\forall x_{r_1})B$, onde r_1, \dots, r_n proporcionan as variables libres que clausuran B .

\Leftarrow / Tendo $\vdash (\forall x_{r_n}) \dots (\forall x_{r_1})B$ e aplicando o axioma Δ_4 para x_1 , obtense $\vdash (\forall x_{r_n}) \dots (\forall x_{r_2})B$. Entón, empregándoo en n ocasións, para $i \in 1, \dots, n$ resulta $\vdash B$. \square

Finalmente, velaquí a proba do teorema da completude:

Teorema 2.15 (completude de Gödel, 1930). *No cálculo predicativo, toda fbf loxicamente válida é un teorema, ou o que é o mesmo,*

$$\text{se } \models B, \text{ entón } \vdash B.$$

Demostración. Basta con considerar unha fbf loxicamente válida pechada. Por contradición, asíumase $\not\models B$. Engadindo $\neg B$ como axioma a \mathcal{K} , a nova teoría \mathcal{K}' é consistente, logo ten un modelo numerable M . Como $\neg B$ é un axioma de \mathcal{K}' , $\neg B$ é verdadeira en M . Mais B tamén é verdadeira en M , ó ser loxicamente válida. Temos pois unha contradición. \square

A completude á que se refire o teorema de Gödel é a semántica. Dirase pois que o cálculo predicativo é *semanticamente completo*, así como calquera teoría que cumpra a propiedade do Teorema 2.15.

Corolario 2.16. *No cálculo predicativo \mathcal{P} , os teoremas coinciden coas fbfs loricamente válidas, é dicir:*

$$\models B \text{ equivale a } \vdash B.$$

Demostración. Isto é consecuencia directa da Proposición 1.37 e o Teorema da completude 2.15. □

En resumo, o cálculo predicativo é sólido e semánticamente completo.

Capítulo 3

Aritmetización

A teoría de números, ou aritmética, do grego *arithmos* (“número”) é a rama das matemáticas que estuda os números e as operacións elementais (suma, resta, produto e división) entre eles. Dos seus intentos de formalización axiomatica, quizais os máis coñecidos son os axiomas de Peano-Dedekind e as construcións a partir de teoría de conxuntos.

Richard Dedekind (1831-1916) propuxo uns principios básicos posteriormente refinados polo matemático e glotólogo¹ italiano Guiseppe Peano (1858-1932), que publicou no ano 1889 unha serie de postulados suficientes para definir os números naturais:

1. Existe un elemento, 1, que é un número natural.
2. Dado un número natural n , existe outro n' univocamente determinado chamado *sucesor de n* .
3. O 1 non é sucesor de ningún outro natural.
4. Dados dous naturais co mesmo sucesor, entón son o mesmo número.
5. Se o 1 pertence a un conxunto calquera e, dado outro natural n pertencente, o seu sucesor tamén está contido no conxunto, tense que todo número natural está dentro del.

3.1. Teorías de primeira orde con igualdade

Definición 3.1. Unha *teoría con igualdade* é unha teoría de primeira orde nunha linguaxe \mathcal{L} cun relator diádico propio $A_1(x, y)$, que se escribe do xeito “ $x = y$ ” (\neq será $\neg A_1(x, y)$), e cos seguintes dous axiomas propios:

¹A glotoloxía é a rama da lingüística que estuda a evolución das diferentes linguas ó longo do tempo.

$$\Delta_6: \quad (\forall x)(x = x),$$

$$\Delta_7: \quad x = y \rightarrow (B(x, x) \rightarrow B(x, y)),$$

onde x e y son variables, $B(x, x)$ é unha *fbf* calquera e $B(x, y)$ resulta de substituír algunhas das instancias libres de x pola variable y (sendo y libre para x na *fbf*).

Proposición 3.2. *Nunha teoría con igualdade, e para calquera termo t , s e r , as seguintes fbfs son teoremas:*

$$1. \vdash t = t.$$

$$2. \vdash t = s \rightarrow s = t.$$

$$3. \vdash t = s \rightarrow (s = r \rightarrow t = r).$$

Demostración. 1. Polo axioma Δ_6 ,

$$\vdash (\forall x)(x = x),$$

agora ben, o axioma Δ_4 das teorías de primeira orde $((\forall x)B(x) \rightarrow B(t))$ permite concluír que $\vdash t = t$.

2. Considerando x e y dúas variables sen instancias en t nin en s mais o axioma Δ_7 :

$$\vdash x = y \rightarrow (x = x \rightarrow y = x).$$

Pódese comprobar que a seguinte é unha tautoloxía:

$$(A \rightarrow (B \rightarrow C)) \rightarrow (B \rightarrow (A \rightarrow C)),$$

polo tanto:

$$\vdash x = x \rightarrow (x = y \rightarrow y = x),$$

e do apartado anterior tense $\vdash x = x$, de esta forma, aplicando *modus ponens*:

$$\vdash x = y \rightarrow y = x.$$

Finalmente, empregando dúas voltas a regra da *xeneralización* e o axioma Δ_4 :

$$\vdash (\forall x)(\forall y)(x = y \rightarrow y = x),$$

$$\vdash t = s \rightarrow s = t.$$

3. Considéranse x, y e z tres variables sen instancias en t, s ou r mais o axioma Δ_7 :

$$\vdash y = x \rightarrow (y = z \rightarrow x = z).$$

Pódese comprobar que a seguinte é unha tautoloxía:

$$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C)),$$

e do apartado anterior tense $\vdash x = y \rightarrow y = x$, con *modus ponens*:

$$\vdash x = y \rightarrow (y = z \rightarrow x = z).$$

Do mesmo xeito que antes, xeneralizando e co axioma Δ_4 :

$$\vdash (\forall x)(\forall y)(\forall z)(x = y \rightarrow (y = z \rightarrow x = z)),$$

$$\vdash t = s \rightarrow (s = r \rightarrow t = r).$$

□

Observación 3.3. Nunha teoría con igualdade, pódese definir o cuantificador existencial de unicidade do xeito seguinte:

$$(\exists!x)B(x) \quad \text{equivale a} \quad (\exists x)B(x) \wedge (\forall x)(\forall y)(B(x) \wedge B(y) \rightarrow x = y),$$

así como as seguintes relacións de orde, para dous termos t e s arbitrarios:

$$t < s \quad \text{equivale a} \quad (\exists x)(x \neq 0 \wedge x + t = s),$$

$$t \leq s \quad \text{equivale a} \quad t < s \vee t = s.$$

3.2. Aritmética de Peano

Peano non estaba ó tanto das contribucións da *Begriffsschrift* de Frege, e construíu os seus axiomas en base á lóxica de Boole e Schröder. Apoiándose nunha cantidade moi pequena de obxectos primitivos, relacionados entre eles polas regras do seu sistema de axiomas, conseguiu construír unha teoría formal da que foi posible interpretar a totalidade da aritmética.

En primeiro lugar, precísase construír unha linguaxe de primeira orde \mathcal{L}_A , posuíndo:

- Un único relator $A_1(x, y)$, diádico, que se escribe da forma $x = y$ (igual).
- Unha única constante c_1 , que se denotará 0 (cero).
- Un funtor monádico $f_1(x)$, escribirase x' (seguinte).

- Dous funtores diádicos, $f_2(x, y)$ e $f_3(x, y)$, que se usarán na forma $x + y$ (suma) e $x \cdot y$ (produto), respectivamente.

Na súa formulación inicial, Peano estableceu o 1 como constante da teoría (e primeiro número natural). Porén, por simplificar a notación nos próximos capítulos, empregárase o 0 nesta linguaxe.

Denominárase *numeral*, e escribírase como \bar{n} , ó termo resultante de aplicar n veces o funtor “seguinte” sobre o 0. Por exemplo, o numeral $\bar{3}$ correspóndese co termo $0'''$. Esta será a forma de denotar ós números naturais nesta linguaxe. Nótese que non son constantes, senón elementos da lóxica resultantes de aplicar o funtor “seguinte” un número determinado de voltas na única constante, o cero. Os números naturais en si pertencen ás interpretacións de \mathcal{L}_A .

Observación 3.4. Chamárase *interpretación natural* de \mathcal{L}_A á estrutura \mathcal{M} que consiste de:

1. O universo dos números naturais $U = \mathbb{N}$.
2. Asignar o natural $0 \in U$ á constante $c_1 \in \mathcal{L}$.
3. Asociar a función $S(n) = n + 1$ ó funtor monádico $f_0 \in \mathcal{L}$; e a suma (+) e produto (\cdot) usuais ós funtores $f_1, f_2 \in \mathcal{L}$.

Poderíase considerar un universo que soamente conteña o número natural 0, coas mesmas interpretacións xa escritas, o que resultaría nunha estrutura distinta (a función seguinte interpretaríase como a función constante). A diferenza entre esta interpretación e a natural será que todos os axiomas de Peano serán verdadeiros respecto á segunda mentres que na primeira un deles será falso. Por exemplo, a *fbf* $(\forall x)x' \cdot x'' \neq 0$ é verdadeira na interpretación natural, e falsa na nova ($0 \cdot 0 = 0$).

Definición 3.5. A *aritmética de Peano* é unha teoría con igualdade \mathcal{AP} na linguaxe \mathcal{L}_A cos seguintes oito axiomas propios:

$$\Lambda_1: \quad x = y \rightarrow (x = z \rightarrow y = z), \quad (\text{transitividade da igualdade})$$

$$\Lambda_2: \quad x = y \rightarrow x' = y', \quad (x' \text{ é unha función})$$

$$\Lambda_3: \quad 0 \neq x', \quad (0 \text{ non ten seguinte})$$

$$\Lambda_4: \quad x' = y' \rightarrow x = y, \quad (\text{inxectividade de } x')$$

$$\Lambda_5: \quad x+0 = x, \quad (\text{elemento neutro para a suma})$$

$$\Lambda_6: \quad x+y' = (x+y)', \quad (\text{seguinte dunha suma})$$

$$\Lambda_7: \quad x \cdot 0 = 0, \quad (0 \text{ anula o produto})$$

$$\Lambda_8: \quad x \cdot y' = x \cdot y + x, \quad (\text{produto do seguinte})$$

mais o axioma coñecido por *principio de indución matemática*:

$$\Lambda_9: \quad B(0) \rightarrow ((\forall x)(B(x) \rightarrow B(y)) \rightarrow (\forall x)B(x)) \text{ para calquera } fbf \ B.$$

Observación 3.6. Nótese que, en realidade, o principio de indución matemática Λ_9 é un esquema axiomático, contendo unha cantidade infinita de axiomas.

Observación 3.7. Certamente, os axiomas teñen sentido. Λ_1 e Λ_2 non son máis que propiedades básicas da igualdade, probablemente consideradas intuitivas por Dedekind e Peano. Λ_3 corresponde ó terceiro postulado de Peano: o 1 non é sucesor de ningún outro natural; por outro lado Λ_4 garante a inxectividade do funtor seguinte (cuarto postulado). Finalmente, os axiomas Λ_5 , Λ_6 , Λ_7 e Λ_8 son os necesarios para definir a suma e produto usuais. Estes non foron considerados como postulados pois tomábase como base certa teoría intuitiva de conxuntos (consultar [8, capítulo 3]).

A aritmética de Peano permite tratar rigorosamente os números naturais sen especificar en ningún momento que o son. Poderíase considerar unha *fbf* B da forma:

$$(\forall x)(\forall y)(\forall z)(x + y) + z = x + (y + z),$$

que é un teorema en \mathcal{AP} . Mais con B non se estaría a firmar que a suma de naturais sexa asociativa, senón unicamente que é posible atopar unha demostración (sucesión de teoremas) coa que chegar a ela como conclusión mediante os axiomas $\Delta_1 - \Delta_7$, $\Lambda_1 - \Lambda_9$.

Cabe resaltar que a maioría dos conceptos empregados nas teorías formais hoxe en día (cuantificadores, variables, relatores, etc) foron introducidos por Frege, aínda que a súa notación difería moito da moderna, debida principalmente á labor de Peano. Unha diferenza esencial entre os dous formalismos, ademais dos símbolos, foi a linearidade da aritmética de Peano: mentres que esta lese de esquerda a dereita, a lóxica de Frege era bidimensional [7, capítulo 13].

Proposición 3.8. *Para calquera tripla de termos t , r e s , os seguintes son teoremas de \mathcal{AP} :*

$$1. \quad t \cdot (r + s) = (t \cdot r) + (t \cdot s),$$

$$2. \quad (r + s) \cdot t = (r \cdot t) + (s \cdot t),$$

$$3. \quad (t \cdot r) \cdot s = t \cdot (r \cdot s),$$

$$4. \quad t + s = r + s \rightarrow t = r.$$

As dúas primeiras coñécense como propiedade distributiva, a terceira como asociatividade para o produto e a derradeira é a lei de cancelación para a suma.

Capítulo 4

Os teoremas da incompletude

A comezos do século XX, e co descubrimento de diversos paradoxos e resultados contraintuitivos, xurdiu a coñecida como *crise fundacional das matemáticas*. Como resultado, naceron tres escolas (directamente opostas) dentro da filosofía das matemáticas: o intuicionismo, o loxicismo e o formalismo. O famoso matemático alemán David Hilbert (1862-1943) pertenceu a esta última, que sostén que a matemática non é máis que o resultado de “xogar” cunha linguaxe de símbolos e certas regras de manipulación (de inferencia) coas que xerar novos resultados dentro da mesma linguaxe. O 8 de agosto de 1900, no Segundo Congreso Internacional de Matemáticas en París, Hilbert publicaría unha lista de 23 problemas sen resolver. O segundo deles rezaba: “*Pódese demostrar, dunha maneira finitaria, que os axiomas da aritmética son consistentes?*”.

Na década dos 1920, e como resposta á crise, Hilbert propuxo de forma explícita un proxecto de investigación (en metamatemática, como se chamou entón) que acabou sendo coñecido como *programa de Hilbert*. Quería que a matemática fose formulada sobre unhas bases sólidas e completamente lóxicas. Cría que, en principio, isto podía lograrse, mostrando:

1. Unha formalización xeral, é dicir, unha linguaxe formal na que todo enunciado matemático se poida escribir de forma precisa a ser manipulado segundo unha serie de regras ben definidas.
2. Consistencia: coa fin de evitar contradicións dentro do sistema formal.
3. Completude: unha garantía de que todo enunciado matemático verdadeiro puidese ser demostrado.
4. Conservación: unha proba de que calquera resultado sobre un “obxecto real” obtido usando razoamentos da linguaxe se poida probar empregando exclusivamente “obxectos reais”.
5. Decidibilidade: debería de haber un algoritmo para determinar a veracidade ou falsidade

de calquera enunciado matemático.

Con todo, o seu intento de dar soporte á matemática axiomatizada con principios definidos, que eliminase as incertezas teóricas, sucumbiu nun fracaso inesperado. Nese contexto, Gödel comezara a traballar nun dos seus teoremas máis famosos: o *teorema da incompletude*, publicándoo tan só un ano despois da súa tese, sacudindo os cimentos da investigación matemática e filosófica. Mostrou que o ambicioso plan de Hilbert era imposible tal como se estaba a expoñer: o segundo requisito non podía combinarse co primeiro de forma razoable.

O traballo de Hilbert levou á necesidade de comprender a obra de Gödel e, anos máis tarde, ó desenvolvemento da teoría da computabilidade, así como da lóxica matemática como disciplina autónoma. Deste “debate” naceu directamente a base para a informática teórica de Alonzo Church e Alan Turing.

4.1. Recursividade

Introducidas primeiramente por Gödel como preliminares para a demostración dos seus teoremas, as funcións recursivas teñen un gran interese por si mesmas. Turing expresou a súa equivalencia coa clase de funcións calculables mediante un algoritmo, na súa famosa *Tese de Church-Turing*.

A definición de *función aritmética* é puramente metamatemática, polo que non están anoadas a ningunha teoría formal en concreto (non son funtores). Trátase de funcións cuxas entradas e saídas son números naturais, como por exemplo o son a suma e o produto. Do mesmo xeito, unha *relación aritmética* non é máis que aquela que ten os números naturais como argumentos. Daquela, cando se estea a tratar con este tipo de funcións ou relacións, empregaranse os símbolos da linguaxe matemática común. Por exemplo, considérese unha función aritmética $f(x, y) = \min(x, y!)$. Ningún dos elementos que a conforman pertencen a unha lóxica en particular (nin as variables, nin os parénteses, nin o factorial, etc).

Nesta sección considerarase unha teoría arbitraria \mathcal{K}_1 con igualdade na linguaxe da aritmética \mathcal{L}_A , polo que os resultados sucesivos serán aplicables a \mathcal{AP} .

4.1.1. Funcións recursivas

Antes de introducir as funcións recursivas, precísanse unha serie de funcións de partida mais unha serie de regras para obter outras novas.

Definición 4.1. As seguintes funcións aritméticas chámanse *funcións iniciais*:

1. A *función cero*: $Z(x) = 0$ para todo x .
2. A *función seguinte*: $S(x) = x + 1$ para todo x .
3. As *proxeccións*: $P_i(x_1, \dots, x_n) = x_i$ para todo x_1, \dots, x_n .

A continuación danse tres regras da dedución, a *substitución*, a *recursividade* mais a *minimización*, que se empregarán un número finito de veces para obter o tipo de funcións que interesan.

Substitución: dirase que f foi obtida por *substitución* a partir das funcións h_1, \dots, h_m e g se é da forma:

$$f(x_1, \dots, x_n) = g(h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n)).$$

Recursividade: dirase que f foi obtida por *recursividade* a partir das funcións g e h se é da forma:

$$\begin{aligned} f(x_1, \dots, x_n, 0) &= g(x_1, \dots, x_n), \\ f(x_1, \dots, x_n, y + 1) &= h(x_1, \dots, x_n, y, f(x_1, \dots, x_n, y)). \end{aligned}$$

Minimización: dirase que f foi obtida por *minimización* a partir de g se é da forma:

$$f(x_1, \dots, x_n) = \mu y (g(x_1, \dots, x_n, y) = 0),$$

onde $\mu y (R)$ denota o mínimo valor de y que torne R verdadeira, para calquera relación R .

Definición 4.2. Unha función f dise *recursiva primitiva* se é posible obtela mediante unha cantidade finita de substitucións e recursividade a partir dunha función inicial. Se ademais tamén se aplica minimización (nunha cantidade finita de ocasións), f dirase simplemente *recursiva*.

As funcións empregadas por Gödel na súa demostración dos teoremas da incompletude foron as recursivas primitivas. Con todo, el chamoulles simplemente *recursivas*. A necesidade do cambio de notación xordeu coas funcións *recursivas xerais* que introduciu Herbrand, posteriormente demostrado por Kleene [4, capítulo 8] o feito de coincidir exactamente coas de Gödel engadindo procedementos de minimización (é dicir, as simplemente recursivas da Definición 4.2).

Exemplo 4.3. As seguintes son funcións recursivas primitivas:

- A suma $x + y$, aplicando a regra de recursividade con $g = P_1(x)$ (proxección) e $h = S(x + y)$ (función seguinte):

$$\begin{aligned} f(x, 0) = P_1(x) &\quad \rightsquigarrow \quad x + 0 = x, \\ f(x, y + 1) = S(f(x, y)) &\quad \rightsquigarrow \quad x + (y + 1) = S(x + y). \end{aligned}$$

- O produto $x \cdot y$, aplicando a regra de recursividade con $g = Z(x)$ (función cero) e h a función suma:

$$\begin{aligned} f(x, 0) = Z(x) &\quad \rightsquigarrow \quad x \cdot 0 = 0, \\ f(x, y + 1) = h(f(x, y), x) &\quad \rightsquigarrow \quad x \cdot (y + 1) = (x \cdot y) + x. \end{aligned}$$

- A función delta,

$$\delta(x) = \begin{cases} 0 & \text{se } x = 0, \\ x - 1 & \text{se } x > 0, \end{cases}$$

que devolve o elemento anterior, aplicando a regra de recursividade sobre a función cero e unha proxección:

$$\begin{aligned} \delta(y, 0) = Z(y) &\quad \rightsquigarrow \quad \delta(0) = 0, \\ \delta(y + 1) = P_1(y, \delta(y)) &\quad \rightsquigarrow \quad \delta(y + 1) = y. \end{aligned}$$

- A resta natural,

$$x \leftarrow y = \begin{cases} x - y & \text{se } y \leq x, \\ 0 & \text{se } y > x, \end{cases}$$

por recursividade e substitución con dúas proxeccións mais a función $\delta(x)$:

$$\begin{aligned} f(x, 0) = Z(y) &\quad \rightsquigarrow \quad x \leftarrow 0 = 0, \\ f(x, y + 1) = \delta(P_3(x, y, f(x, y + 1))) &\quad \rightsquigarrow \quad x \leftarrow (y + 1) = \delta(x \leftarrow y). \end{aligned}$$

- A función signo,

$$sgn(x) = \begin{cases} 0 & \text{se } x = 0, \\ 1 & \text{se } x \neq 0, \end{cases}$$

que non é máis que a substitución de $\delta(x)$ por y na resta natural:

$$sgn(x) = x \leftarrow \delta(x).$$

- A diferenza,

$$|x - y| = \begin{cases} x - y & \text{se } y \leq x, \\ y - x & \text{se } y > x, \end{cases}$$

obtida tamén por substitución:

$$|x - y| = (x \leftarrow y) + (y \leftarrow x).$$

- As funcións x^y , $x!$, $\min(x_1, \dots, x_n)$, $\max(x_1, \dots, x_n)$, mais as sumas e produtos limitados $\sum_{y < z} f(x_1, \dots, x_n, y)$ e $\prod_{y < z} f(x_1, \dots, x_n, y)$, sempre e cando a función f sexa tamén recursiva primitiva.

Xorde agora a necesidade de describir, de algunha maneira, estas funcións aritméticas dentro da teoría formal. Coa definición a continuación, vese que é tan sinxelo como atopar unha *fbf* que equivalla á función para cada un dos valores do seu dominio e percorrido¹

Definición 4.4. Unha función f dise *representable* en \mathcal{K}_1 se existe unha *fbf* $B(x_1, \dots, x_n, y)$, con x_1, \dots, x_n variables libres, tal que para todo k_1, \dots, k_n, m números naturais, cúmprense as seguintes dúas condicións:

1. Se $f(k_1, \dots, k_n) = m$, entón $\vdash B(\overline{k_1}, \dots, \overline{k_n}, \overline{m})$,
2. $\vdash (\exists!y)B(\overline{k_1}, \dots, \overline{k_n}, y)$.

A segunda condición é equivalente a $\vdash (\exists!y)B(x_1, \dots, x_n, y)$ [8, sección 3.2].

Exemplo 4.5. A función seguinte, $S(x) = x + 1$, é representable en \mathcal{K}_1 . Existe unha *fbf*, $y = x'_1$, con x_1 libre, tal que para todo k e m naturais:

1. $S(k) = m$ equivale a $m = k + 1$, logo $\vdash \overline{m} = \overline{k}'$,
2. $\vdash (\exists!y)(y = x'_1)$.

A función cero e as proxeccións son tamén representables en \mathcal{K}_1 .

4.1.2. Relacións recursivas

Definición 4.6. Unha relación aritmética $R(x_1, \dots, x_n)$ dise *recursiva (primitiva)* se a seguinte función, chamada *función característica de R*, é recursiva (primitiva):

$$\chi_R = \begin{cases} 0 & \text{se } R(x_1, \dots, x_n) \text{ é verdadeira,} \\ 1 & \text{se } R(x_1, \dots, x_n) \text{ é falsa.} \end{cases}$$

Exemplo 4.7. A relación de igualdade $x_1 = x_2$ é recursiva primitiva, a súa función característica:

$$\chi_{x_1=x_2} = \begin{cases} 0 & \text{se } x_1 = x_2, \\ 1 & \text{se } x_1 \neq x_2, \end{cases}$$

é recursiva primitiva, pois é posible obtela por substitución (tomando x como $|x_1 - x_2|$) a partir da función signo:

$$\chi_{x_1=x_2} = \text{sgn}(|x_1 - x_2|) = \begin{cases} 0 & \text{se } |x_1 - x_2| = 0, \\ 1 & \text{se } |x_1 - x_2| \neq 0. \end{cases}$$

¹Aquí *dominio* quere dicir os valores de entrada que acepta, e o *percorrido* son todas as súas posibles avaliacións.

O seguinte resultado pode ser de moita axuda para demostrar a recursividade de certas relacións:

Proposición 4.8. *Sexan g_1, \dots, g_n funcións e R_1, \dots, R_n relacións, todas recursivas (primitivas). Se soamente unha das relacións $R_1(x_1, \dots, x_n), \dots, R_n(x_1, \dots, x_n)$ é verdadeira, para calquera x_1, \dots, x_n , entón a seguinte función é recursiva (primitiva):*

$$f(x_1, \dots, x_n) = \begin{cases} g_1(x_1, \dots, x_n) & \text{se } R_1(g_1(x_1, \dots, x_n)) \text{ é verdadeira,} \\ g_2(x_1, \dots, x_n) & \text{se } R_2(g_1(x_1, \dots, x_n)) \text{ é verdadeira,} \\ \dots & \dots \\ g_n(x_1, \dots, x_n) & \text{se } R_n(g_1(x_1, \dots, x_n)) \text{ é verdadeira.} \end{cases}$$

Por último, e da mesma forma que cas funcións representables, pódese definir un concepto análogo nas relacións aritméticas, coas consecuencias que supón.

Definición 4.9. Unha relación aritmética R dise *expresable* en \mathcal{K}_1 se existe unha *fbf* $B(x_1, \dots, x_n)$ con x_1, \dots, x_n libres tal que para todo k_1, \dots, k_n naturais, cúmprense as seguintes dúas condicións:

1. Se $R(k_1, \dots, k_n)$ é verdadeira, entón $\vdash B(\bar{k}_1, \dots, \bar{k}_n)$.
2. Se $R(k_1, \dots, k_n)$ é falsa, entón $\vdash \neg B(\bar{k}_1, \dots, \bar{k}_n)$.

Proposición 4.10. *Sexa unha teoría \mathcal{K}_1 con igualdade en \mathcal{L}_A tal que $\vdash 0 \neq \bar{1}$. Entón unha relación aritmética R é expresable se e só se χ_R é representable.*

Demostración.

\Rightarrow / Supóñase que R é expresable por unha *fbf* $B(x_1, \dots, x_n)$. Entón χ_R é representable pola *fbf*:

$$(B(x_1, \dots, x_n) \wedge y = 0) \vee (\neg(B(x_1, \dots, x_n) \wedge y = \bar{1})).$$

\Leftarrow / Se a función característica χ_R é representable por unha *fbf* $B(x_1, \dots, x_n)$, empregando a asunción $\vdash 0 \neq \bar{1}$, a relación R é expresable pola *fbf* $B(x_1, \dots, x_n, 0)$. \square

Proposición 4.11. *As relacións obtidas a partir de outras recursivas (primitivas) mediante conectores proposicionais son tamén recursivas (primitivas).*

Demostración. Considérense dúas relacións arbitrarias $R_1(x_1, \dots, x_n), R_2(x_1, \dots, x_n)$ recursivas (primitivas). Por definición, as súas funcións características χ_{R_1} e χ_{R_2} son tamén recursivas (primitivas). Nótese que, aplicando a resta natural, $1 \leftarrow \chi_{R_1}(x_1, \dots, x_n) = \chi_{\neg R_1}$, polo que $\neg R_1$ é tamén recursiva (primitiva). Por outro lado, $\chi_{R_1 \wedge R_2}(x_1, \dots, x_2) = \chi_{R_1}(x_1, \dots, x_2) \cdot \chi_{R_2}(x_1, \dots, x_2)$, e grazas á recursividade primitiva do produto, $R_1 \wedge R_2$ é tamén recursiva primitiva. Agora,

recórdese que $B \vee C$ equivale a $\neg B \rightarrow C$ para dúas *fbfs* B e C calesquera. Pódese expresar entón a implicación mediante a negación e a disxunción: $B \rightarrow C$ equivale a $\neg B \vee C$. Tense o resultado, pois todo conector pode ser expresado por medio de \rightarrow e \neg . \square

4.1.3. A función beta de Gödel

Agora xorde unha cuestión: son todas as funcións recursivas representables na linguaxe da aritmética? Na súa proba do primeiro teorema da incompletude, Gödel introduciu unha función que lle permitía cuantificar sucesións finitas de números naturais. A maior utilidade que tiña era mostrar que a clase de funcións aritméticas é pechada baixo a recursividade primitiva e, polo tanto, inclúe todas as funcións recursivas primitivas.

Definición 4.12. A seguinte función aritmética chámase *beta de Gödel*:

$$\beta(x_1, x_2, x_3) = \text{resto}(1 + (x_3 + 1) \cdot x_2, x_1),$$

onde $\text{resto}(x, y)$ é a función que devolve o resto da división de y entre x . Unha formulación equivalente da función é:

$$\beta(x_1, x_2, x_3) \equiv x_1 \pmod{1 + (x_3 + 1) \cdot x_2}.$$

Proposición 4.13. *Téñense os seguintes resultados:*

1. *A beta de Gödel é recursiva primitiva.*
2. *A beta de Gödel é representable en \mathcal{AP} .*

Demostración.

1. Basta con demostrar que a función resto é recursiva primitiva. Certamente, pódese obter mediante recursividade:

$$\begin{aligned} \text{resto}(x, 0) &= 0, \\ \text{resto}(x, y + 1) &= S(\text{resto}(x, y)) \cdot \text{sgn}(|x - S(\text{resto}(x, y))|). \end{aligned}$$

2. Pódese comprobar que a seguinte *fbf* $Bt(x_1, x_2, x_3, y)$ representa a β :

$$(\exists w)(x_1 = (1 + (x_3 + 1) \cdot x_2) \cdot w + y \wedge y < 1 + (x_3 + 1 \cdot x_2)). \quad \square$$

Lema 4.14. *Para calquera sucesión de números naturais k_0, k_1, \dots, k_n , existen dous naturais b e c tales que:*

$$\beta(b, c, i) = k_i \quad \text{para cada } i \in \{0, 1, \dots, n\}.$$

Demostración. Sexan $m = \max(n, k_0, \dots, k_n)$ e $c = m!$. Considérense os naturais:

$$u_i = 1 + (i + 1)c \quad \text{para cada } i \in \{0, 1, \dots, n\}.$$

En primeiro lugar, tense que $\text{mcd}(u_i, u_j) = 1$ para cada $i, j \in \{0, 1, \dots, n\}$, onde $\text{mcd}(x, y)$ denota o máximo común divisor entre dous números. Certamente, se un primo p dividise a $1 + (i + 1)c$ e $1 + (j + 1)c$ para cada $i, j \in \{0, 1, \dots, n\}$, $i < j$, p dividiría tamén á súa diferenza $(j - i)c$. Porén, p non divide a c (nese caso tamén dividiría a $(i + 1)c$ e $1 + (i + 1)c$, o cal é imposible) nin a $(j - i)$ ($j - i$ divide a $m! = c$ para $j - i \leq n \leq m$, polo que p tamén dividiría a c). Deste xeito, os u_i son coprimos entre eles. Nótese ademais que para $i \in \{0, \dots, n\}$, tense que $k_i \leq m \leq m! = c < 1 + (i + 1)c = u_i$.

Finalmente, grazas ó Teorema chinés dos restos, existe un natural $b < u_0 \cdot u_1 \cdots u_n$ tal que $\text{resto}(u_i, b) = k_i$ para cada $i \in \{0, \dots, n\}$. En consecuencia, $\beta(b, c, i) = \text{resto}(1 + (i + 1)c, b) = \text{resto}(u_i, b) = k_i$. \square

En consecuencia, fixando b e c adecuadamente, a beta de Gödel convértese nunha función monádica coincidente cunha sucesión finita prefixada, o cal é moi útil, pois permite codificar sucesións finitas de números naturais mediante só dous números.

Exemplo 4.15. A sucesión de números naturais $(2, 0, 2, 4)$ pódese codificar mediante a beta de Gödel empregando $b = 602$ e $c = 3$:

$$\begin{aligned} \text{resto}(1 + (0 + 1) \cdot 3, 602) &= 2, \\ \text{resto}(1 + (1 + 1) \cdot 3, 602) &= 0, \\ \text{resto}(1 + (2 + 1) \cdot 3, 602) &= 2, \\ \text{resto}(1 + (3 + 1) \cdot 3, 602) &= 4, \end{aligned}$$

A propiedade do Lema 4.14 preséntase fundamental na proba do teorema a continuación: mediante a beta de Gödel calquera función aritmética pódese representar en \mathcal{AP} , o cal mostra que toda función recursiva é tamén representable. A demostración é longa pero pode atoparse en [8, capítulo 3.3]. Este resultado non é preciso para probar os teoremas da incompletude, mais convén telo en conta para poder interpretalos adecuadamente.

Teorema 4.16. *Toda función recursiva é representable na aritmética de Peano \mathcal{AP} .*

Corolario 4.17. *Toda relación recursiva é expresable na aritmética de Peano \mathcal{AP} .*

4.2. Numeración de Gödel

Gödel observou que cada expresión dunha teoría formal podía ser representada por un número natural (chamado *número de Gödel*). Isto é significativo, xa que o estudo das propiedades

dunha expresión en concreto equivalería ó estudo das propiedades do seu número de Gödel correspondente. Aínda que estes poidan chegar a ser moi grandes, isto non é un impedimento, o verdadeiramente importante é a constructibilidade dos mesmos.

O austríaco deseñou un método polo cal a cada expresión élle asignado un único número, permitindo bailar adiante e atrás entre fórmulas e números de Gödel. En realidade, existen moitas formas de facer isto. Un exemplo sinxelo é o código *ASCII*, que emprega 7 bits para representar todos os caracteres do alfabeto latino na computadora: a palabra “estoxo” equivale á cadea de naturais 101 115 116 111 120 111.

Para unha teoría de primeira orde \mathcal{K}_1 , constrúese a numeración de Gödel coma unha aplicación g que vai do conxunto de símbolos de \mathcal{K}_1 ós números naturais.

$$\begin{aligned}
 g : \mathcal{K}_1 &\longrightarrow \mathbb{N} \\
 (&\mapsto 3 \\
) &\mapsto 5 \\
 , &\mapsto 7 \\
 \neg &\mapsto 9 \\
 \rightarrow &\mapsto 11 \\
 \forall &\mapsto 13 \\
 x_k &\mapsto 13 + 8k, \quad k \geq 1 \\
 a_k &\mapsto 7 + 8k, \quad k \geq 1 \\
 f_k^n &\mapsto 1 + 8(2^n 3^k), \quad k, n \geq 1 \\
 A_k^n &\mapsto 3 + 8(2^n 3^k), \quad k, n \geq 1
 \end{aligned}$$

O superíndice n indica o rango dun relator ou funtor (por exemplo, $n = 2$ para un relator diádico). Nótese que todo número de Gödel é impar, e que ao dividilos entre 8, terán distinto resto dependendo de se veñen dunha variable (5), dunha constante (7), dun funtor (1), ou dun relator (3).

Dada unha expresión u_1, \dots, u_n de \mathcal{K}_1 , onde cada u_i é un símbolo, o seu número de Gödel correspondente é o seguinte:

$$g(u_1, \dots, u_n) = 2^{g(u_1)} \cdot 3^{g(u_2)} \cdot \dots \cdot p_n^{g(u_n)},$$

sendo p_n o n -ésimo número primo (comenzando por $p_0 = 2$). Ademais, tamén se lle pode asignar un número a cada sucesión de expresións e_1, \dots, e_n do mesmo xeito:

$$g(e_1, \dots, e_n) = 2^{g(e_1)} \cdot 3^{g(e_2)} \cdot \dots \cdot p_n^{g(e_n)}.$$

Grazas á unicidade da factorización de enteiros en números primos, cada expresión ou sucesión delas ten un número de Gödel exclusivo. De feito, ata un símbolo u pode ter dous números

distintos segundo se considere soamente como símbolo, u , ou como expresión, $e : u$. É obvio que, ó seren un subconxunto do conxunto das expresións, as *fbfs* terán tamén o seu propio número asignado, así como os teoremas e as demostracións.

Exemplo 4.18. O número de Gödel da expresión $A_1^1(x_1, f_3^1(x_1))$ é o seguinte:

$$\begin{aligned} g(A_1^1(x_1, f_3^1(x_1))) &= 2^{g(A_1^1)} \cdot 3^{g(()} \cdot 5^{g(x_1)} \cdot 7^{g(,)} \cdot 11^{g(x_2)} \cdot 13^{g(f_3^1)} \cdot 17^{g(()} \cdot 19^{g(x_1)} \cdot 23^{g(()} \cdot 27^{g(()} \\ &= 2^{51} \cdot 3^3 \cdot 5^{21} \cdot 7^7 \cdot 11^{29} \cdot 13^{433} \cdot 17^3 \cdot 19^{21} \cdot 23^5 \cdot 27^5. \end{aligned}$$

Exemplo 4.19. Dado o número de Gödel $214366293288 \cdot 5^{25}$, é posible obter a expresión da que provén. Efectivamente, factorizando en primos obtense:

$$214366293288 \cdot 5^{25} = 2^3 \cdot 3^{13} \cdot 5^{25} \cdot 7^5,$$

polo que a expresión agochada era $(\forall x_1)$.

Exemplo 4.20. Aplicando esta numeración á aritmética de Peano \mathcal{AP} , obtense:

$$\begin{aligned} g : \mathcal{AP} &\longrightarrow \mathbb{N} \\ (&\mapsto 3 \\) &\mapsto 5 \\ , &\mapsto 7 \\ \neg &\mapsto 9 \\ \rightarrow &\mapsto 11 \\ \forall &\mapsto 13 \\ 0 &\mapsto 15 \\ ' &\mapsto 49 \\ + &\mapsto 289 \\ \cdot &\mapsto 865 \\ = &\mapsto 99 \\ x_k &\mapsto 13 + 8k, \quad k \geq 1 \end{aligned}$$

Definición 4.21. Unha teoría de primeira orde \mathcal{K}_1 ten un *vocabulario recursivo (primitivo)* se as seguintes tres relacións son recursivas (primitivas):

1. $Cte(x) : x$ é o número de Gödel dunha constante individual c_k ,

$$g(c_k) = 7 + 8k = x.$$

2. $Fun(x) : x$ é o número de Gödel dun functor f_k^n ,

$$g(f_k^n) = 1 + 8(2^n 3^k) = x.$$

3. $Rel(x) : x$ é o número de Gödel dun relator A_k^n ,

$$g(A_k^n) = 3 + 8(2^n 3^k) = x.$$

Á súa vez, unha teoría de primeira orde \mathcal{K}_1 dise de ter un *sistema de axiomas recursivo* (primitivo) se a seguinte relación é recursiva (primitiva):

4. $Axm(x) : x$ é o número de Gödel dun axioma propio.

Observación 4.22. Toda teoría cun número finito de constantes, funtores e relatores terá un vocabulario recursivo primitivo. Certamente, supóñase unha teoría \mathcal{K} con constantes c_1, \dots, c_n . Entón $Cte(x)$ se e só se $x = g(c_1) = 7 + 8 \cdot 1 \vee x = g(c_2) = 7 + 8 \cdot 2 \vee \dots \vee x = g(c_n) = 7 + 8 \cdot n$. Aplicando a recursividade primitiva da suma, do produto e a conservación por conxunción (Proposición 4.11), tense que $Cte(x)$ é recursiva primitiva. Os casos de $Fun(x)$ e $Rel(x)$ son análogos. Polo tanto, a aritmética de Peano ten un vocabulario recursivo. Ademais, é sinxelo observar que tamén posúe un sistema de axiomas recursivo.

Exemplo 4.23. Nunha teoría con igualdade en \mathcal{L}_A cun sistema de axiomas recursivo (primitivo), en particular, na aritmética de Peano \mathcal{AP} , as seguintes relacións son recursivas (primitivas):

1. $Cte(x) : x$ é o número de Gödel dunha constante,
2. $Fun(x) : x$ é o número de Gödel dun funtor,
3. $Rel(x) : x$ é o número de Gödel dun relator,
4. $Axm(x) : x$ é o número de Gödel dun axioma,
5. $Xpr(x) : x$ é o número de Gödel dunha expresión,
6. $Trm(x) : x$ é o número de Gödel dun termo,
7. $Fbf(x) : x$ é o número de Gödel dunha *fbf*,
8. $Dem(x) : x$ é o número de Gödel dunha demostración,
9. $Dem(y, x) : y$ é o número de Gödel dunha demostración con número de Gödel x .

así como as seguintes funcións:

10. $Num(x) : x$ é o número de Gödel do numeral \bar{x} ,
11. $Sub(x, u, v) : x$ é o número de Gödel resultante de substituír o termo con número de Gödel u nas instancias libres da variable con número de Gödel v na expresión con número de Gödel x .

12. $Neg(x)$: o número de Gödel de $(\neg B)$, sendo x o número de Gödel de B .

A proba de recursividade pode atoparse en [8, capítulo 3.4].

4.3. Primeiro teorema da incompletude

Despois da publicación da súa tese sobre a completude do cálculo predicativo, e co obxectivo de conseguir a habilitación para profesorado na universidade de Viena, Gödel tivo que desenvolver unha nova investigación. Naquel momento, unha das cuestións “de moda” no círculo de Viena era a capacidade (ou non) dunha linguaxe formal para probar toda afirmación expresada coa mesma linguaxe. O primeiro teorema, publicado en *On Formally Undecidable Propositions of Principia Mathematica and Related Systems* no ano 1931, rezaba:

En calquera teoría consistente contendo a aritmética básica, é posible construír unha expresión non demostrable coas ferramentas da propia teoría.

Para demostrar este resultado, Gödel considera unha *fbf* A cunha única variable libre x_1 , $A(x_1)$. O seu número de Gödel é $g(A(x_1))$, que se pode substituír por x_1 dentro de $A(x_1)$, obtendo $A(g(A(x_1)))$. Este proceso, chamado *diagonalización*, provoca que a expresión sexa autoreferencial. Seguidamente, expresa unha afirmación no sistema, $\neg dem$ e, diagonalizándoa, obtén unha *fbf* que afirma que ela mesma non é demostrable. Se esta nova *fbf* fose un teorema, caeríase nunha contradición e o sistema sería inconsistente. Así pois, non se pode nin demostrar nin refutar e a teoría formal resulta incompleta.

Exemplo 4.24 (O paradoxo do mentireiro). Sendo un dos máis antigos que se coñecen, o *paradoxo do mentireiro* tivo moitas reformulacións ó longo da historia. Ebulides de Mileto (s. IV a.C.) fixo a pregunta “Un home di que está a mentir. O que di é verdadeiro ou é falso?”. A versión máis básica desta fórmula é a seguinte frase:

Esta afirmación é falsa.

Para probar o teorema da incompletude, Gödel empregou unha versión lixeiramente modificada deste paradoxo, para ter unha *fbf* verdadeira pero indecible:

Esta afirmación non é demostrable.

4.3.1. Diagonalización

Definición 4.25. Defínese a seguinte función recursiva chamada *función diagonal*:

$$\begin{aligned} \text{diag}(u) &= \text{Sub}(u, \text{Num}(u), 21) \\ &= \text{Sub}(g(B(x_1)), g(\bar{u}), g(x_1)) \\ &= g(B(\bar{u})) \end{aligned}$$

que proporciona o número de Gödel de $B(\bar{u})$, sendo u o número de Gödel dunha *fbf* $B(x_1^2)$.

Intuitivamente, se B afirma unha propiedade de x , a función diagonal $\text{diag}(u) = \text{diag}(g(B(x_1))) = g(B(g(B(x_1))))$ mostra unha fórmula que afirma que o seu propio número de Gödel ten esa propiedade.

$$B(x_1) \xrightarrow{g} u \xrightarrow{-} \bar{u} \xrightarrow{B} B(\bar{u}) \xrightarrow{g} \text{diag}(u)$$

Lema 4.26 (de diagonalización). *Sexa unha teoría con igualdade \mathcal{K}_1 en \mathcal{L}_A na que a función diagonal é representable. Entón, para cada *fbf* cunha única variable libre $B(x_1)$, existe unha *fbf* pechada C tal que:*

$$\vdash C \leftrightarrow B(\overline{g(C)}).$$

Demostración. Considérese $D(x_1, x_2)$ unha *fbf* en \mathcal{K}_1 que representa a función *diag*. Sexan a *fbf* $A(x_1)$ mais o seu respectivo número de Gödel:

$$A(x_1) : (\forall x_2)(D(x_1, x_2) \leftrightarrow B(x_2)),$$

$$m = g(A(x_1)),$$

e denótese por C á *fbf* $A(\bar{m})$, con q o seu número de Gödel:

$$C : (\forall x_2)(D(\bar{m}, x_2) \leftrightarrow B(x_2)),$$

$$q = g(C).$$

Por construción, é obvio que $\text{diag}(m) = g(A(\bar{m})) = q$, polo que $\vdash D(\bar{m}, q)$ e, como *diag* representa a D , $\vdash (\exists! x_2)D(\bar{m}, x_2)$.

²Nótese que 21 é o número de Gödel de x_1 .

A intención é agora probar $\vdash C \rightarrow B(\bar{q})$:

$(\forall x_2)(D(\bar{m}, x_2) \rightarrow B(x_2))$	hipótese
$(\forall x_2)(D(\bar{m}, x_2) \rightarrow B(x_2)) \rightarrow (D(\bar{m}, \bar{q}) \rightarrow B(\bar{q}))$	Δ_4
$D(\bar{m}, \bar{q}) \rightarrow B(\bar{q})$	<i>modus ponens</i>
$D(\bar{m}, \bar{q})$	$\vdash D(\bar{m}, \bar{q})$
$B(\bar{q})$	<i>modus ponens</i>

Polo que $C \vdash B(\bar{q})$ e, grazas ó Teorema da dedución (1.33), $\vdash C \rightarrow B(\bar{q})$.

Por último, próbese o recíproco $\vdash B(\bar{q}) \rightarrow C$:

$B(\bar{q})$	hipótese
$D(\bar{m}, x_2)$	hipótese
$\vdash D(\bar{m}, \bar{q})$	
$\vdash (\exists! x_2)D(\bar{m}, x_2)$	
$\bar{q} = x_2$	definición de $\exists!$
$(\bar{q} = x_2) \rightarrow (B(\bar{q}) \rightarrow B(x_2))$	Δ_7
$B(\bar{q}) \rightarrow B(x_2)$	<i>modus ponens</i>
$B(x_2)$	<i>modus ponens</i>

Dedúcese que $B(\bar{q}), D(\bar{m}, x_2) \vdash B(x_2)$ e, repetindo o razoamento anterior, $B(\bar{q}) \vdash D(\bar{m}, x_2) \rightarrow B(x_2)$. Xeneralizando e polo teorema da dedución, $\vdash B(\bar{q}) \rightarrow C$, o cal finaliza a demostración. \square

Corolario 4.27. *Sexa unha teoría con igualdade \mathcal{K}_1 en \mathcal{L}_A na que toda función recursiva é representable. Entón, para cada fbf cunha única variable libre $B(x_1)$, existe unha fbf pechada C tal que:*

$$\vdash C \leftrightarrow B(\overline{g(C)}).$$

Introducírase agora unha definición auxiliar dada por Kurt Gödel na súa proba orixinal do teorema da incompletude, unha forma máis forte de consistencia.

Definición 4.28. Unha teoría arbitraria \mathcal{K} dise ω -consistente se, para cada fbf $B(x)$ con x única variable libre, tense o seguinte:

$$\text{se } \vdash \neg B(\bar{n}) \text{ para todo } n \text{ natural, entón } \not\vdash (\exists x)B(x).$$

Dentro dunha teoría non ω -consistente é posible probar que cada número natural cumpre unha propiedade determinada e, ó mesmo tempo, probar que non todo número natural a cumpre. Nótese que a noción de ω -consistencia dunha teoría \mathcal{K} presupón que os números naturais son algo que existe previamente a \mathcal{K} . Alguén que quixera identificar os naturais con obxectos formais definidos dentro da propia teoría, non podería darlle un sentido real á afirmación “ \mathcal{K} é ω -consistente”.

Proposición 4.29. *Se \mathcal{K} é ω -consistente, entón é consistente.*

Demostración. Sexa $C(x)$ unha *fbf* con x única variable libre, e sexa $B(x)$ a *fbf* $C(x) \wedge \neg C(x)$. Tense entón $\vdash \neg B(\bar{n})$ para cada n natural, ó seren unha instancia da tautoloxía $\neg(Q \wedge \neg Q)$. Por hipótese, tense $\not\vdash (\exists x)B(x)$. Atopamos unha *fbf* non demostrable en \mathcal{K} , polo que a teoría é consistente (ver Observación 2.2). \square

4.3.2. Demostración

Antes de proceder coa proba do primeiro teorema da incompletude de Gödel, é conveniente atender ás condicións esenciais que require, que permitirán facer uso dalgúns dos resultados vistos anteriormente, co obxectivo en mente de construír a sentencia contraditoria. Estes “mínimos” son tres propiedades dunha teoría con igualdade \mathcal{K}_1 na linguaxe da aritmética:

1. \mathcal{K}_1 ten un sistema de axiomas recursivo.
2. $\vdash 0 \neq \bar{1}$.
3. Toda función recursiva é representable en \mathcal{K}_1 .

A primeira hipótese permitirá empregar as relacións e funcións recursivas do Exemplo 4.23. A segunda e a terceira, acompañadas da Proposición 4.10, deducen que toda relación recursiva é tamén expresable. Por último, a terceira dá pé a usar o Corolario do Lema de diagonalización 4.27. Tense entón que a seguinte relación é recursiva e expresable:

$Dem(y, x) : y$ é o número de Gödel dunha demostración dunha *fbf* con número de Gödel x .

Sexa $dem(x_2, x_1)$ a *fbf* que expresa a $Dem(y, x)$, e sexa $C(x_1)$ a *fbf* $(\forall x_2)\neg dem(x_2, x_1)$. Grazas ó Corolario do Lema de diagonalización 4.27, existe unha *fbf* pechada \mathcal{G} (chamada *sentencia de Gödel*) tal que:

$$\vdash \mathcal{G} \leftrightarrow (\forall x_2)\neg dem(x_2, \overline{g(\mathcal{G})}) \quad (4.1)$$

O lado dereito da equivalencia afirma que non existe demostración de \mathcal{G} en \mathcal{K}_1 . É dicir, \mathcal{G} é equivalente a unha sentencia que afirma que non é demostrable.

Pódese agora comezar a demostración do teorema da incompletude.

Teorema 4.30 (Primeiro teorema da incompletude de Gödel). *Sexa unha teoría con igualdade \mathcal{K}_1 en \mathcal{L}_A tal que:*

1. \mathcal{K}_1 ten un sistema de axiomas recursivo.

2. $\vdash 0 \neq \bar{1}$.

3. Toda función recursiva é representable en \mathcal{K}_1 .

Téñense logo os dous seguintes resultados:

A. Se \mathcal{K}_1 é consistente, entón $\not\vdash \mathcal{G}$.

B. Se \mathcal{K}_1 é ω -consistente, entón $\not\vdash \neg\mathcal{G}$.

Demostración. Sexa q o número de Gödel de \mathcal{G} , $q = g(\mathcal{G})$.

A. Por contradición, supóñase $\vdash \mathcal{G}$. Sexa r o número de Gödel dunha demostración de \mathcal{G} . Tense entón $\vdash dem(\bar{r}, \bar{q})$, ou o que é o mesmo, $\vdash dem(\bar{r}, \overline{g(\mathcal{G})})$. Por outro lado, aplicando *modus ponens* con (4.1) mais a hipótese inicial:

$$\vdash (\forall x_2)\neg dem(x_2, \overline{g(\mathcal{G})}),$$

e grazas ó axioma Δ_4 ,

$$\vdash \neg dem(\bar{r}, \overline{g(\mathcal{G})}),$$

o cal é unha contradición, así que a teoría \mathcal{K} é inconsistente.

B. Asíumase $\vdash \neg\mathcal{G}$. De (4.1) por *modus ponens* obtense:

$$\vdash \neg(\forall x_2)\neg dem(x_2, \overline{g(\mathcal{G})}),$$

ou o que é o mesmo,

$$\vdash (\exists x_2) dem(x_2, \overline{g(\mathcal{G})}).$$

Por outro lado, ó ser \mathcal{K} unha teoría ω -consistente, tamén é consistente. Logo $\not\vdash \mathcal{G}$ e $\vdash \neg\mathcal{G}$, así que $\vdash \neg dem(\bar{n}, \overline{g(\mathcal{G})})$ para cada n natural e, pola definición de ω -consistencia,

$$\not\vdash (\exists x_2) dem(x_2, \overline{g(\mathcal{G})}),$$

tendo unha contradición e rematando a demostración. □

Observación 4.31. Unha teoría ω -consistente é tamén consistente (4.29). Consecuentemente, tense que nin \mathcal{G} nin a súa negación son teoremas, é dicir, \mathcal{G} é unha sentencia indecible. En consecuencia, a teoría é incompleta.

Observación 4.32. A aritmética de Peano \mathcal{AP} fica nas hipóteses do teorema da incompletude. Deste feito, e supoñéndoa ω -consistente, \mathcal{AP} é unha teoría incompleta.

Supoñendo unha cuarta condición semántica no teorema da incompletude obtense unha proba máis sinxela:

Proposición 4.33. *Engadindo a seguinte hipótese ó Teorema da incompletude 4.30, téñense os mesmos resultados:*

4. *Os axiomas propios de \mathcal{K}_1 son verdadeiros baixo a súa interpretación natural³.*

Demostración. Certamente, a sentencia de Gödel \mathcal{G} afirma a súa propia indecidibilidade na interpretación natural de \mathcal{L}_A .

A. Por contradición, supóñase $\vdash \mathcal{G}$. Xa que $\vdash \mathcal{G} \leftrightarrow (\forall x_2)\neg dem(x_2, \overline{g(\mathcal{G})})$, séguese

$$\vdash (\forall x_2)\neg dem(x_2, \overline{g(\mathcal{G})}),$$

que é verdadeira baixo a interpretación natural (por hipótese). É dicir, que \mathcal{G} non é un teorema, contradicindo a suposición inicial.

B. Asíumase $\vdash \neg\mathcal{G}$. Do mesmo xeito, séguese $\vdash \neg(\forall x_2)\neg dem(x_2, \overline{g(\mathcal{G})})$, que equivale a

$$\vdash (\exists x_2)dem(x_2, \overline{g(\mathcal{G})}),$$

que é verdadeira baixo a interpretación natural. É dicir, que \mathcal{G} é un teorema, contradicindo o resultado de A. \square

4.3.3. Alternativas

A indecidibilidade de sentencia de Gödel \mathcal{G} ven da asunción de ω -consistencia. Porén, no ano 1936 o loxicista John Barkley Rosser (1907-1989), estudante de Alonzo Church, demostrou unha versión máis forte do teorema de Gödel na que precisaba soamente da consistencia para probar a incompletude. No canto de empregar \mathcal{G} , construíu outra sentencia \mathcal{R} que afirmaba “Para cada demostración miña, existe unha demostración máis curta da miña negación”. En linguaxe formal, a *sentencia de Rosser* é tal que:

$$\vdash \mathcal{R} \leftrightarrow E(\overline{g(\mathcal{R})}),$$

sendo $E(x_1)$ a seguinte *fbf*:

$$(\forall x_2)(dem(x_2, x_1) \rightarrow (\forall x_3)(neg(x_1, x_3) \rightarrow (\exists x_4)(x_4 \leq x_2 \wedge dem(x_4, x_3))))),$$

e $neg(x_1, x_2)$ unha *fbf* que expresa a función *Neg* na teoría.

Corolario 4.34 (Rosser). *Se a aritmética de Peano \mathcal{AP} é consistente, entón é incompleta.*

³As teorías que cumpren esta condición chámanse *verdadeiras*.

Ningunha teoría formal capaz de describir a aritmética mais os números naturais con certa capacidade de expresión pode ser consistente e completa á vez. Mais unha teoría inconsistente non ten valor (Observación 2.2), polo que calquera teoría cos mínimos descritos vai fallar na súa capacidade de abranguer: haberá afirmacións matemáticas que non poderá demostrar.

Exemplo 4.35 (O paradoxo de Berry). Proposta por Rusell, mais atribuída por el mesmo ao bibliotecario de Oxford G. G. Berry (1867–1928), o *paradoxo de Berry* consiste dunha afirmación autoreferencial do estilo:

O número natural máis pequeno que non se pode definir con menos de dezaseis palabras.

Esta sentenza pretende describir un número natural n que precisa como mínimo de 16 palabras para ser definido. Con todo, o paradoxo soamente consta de 15 palabras, o cal podería inducir a pensar que se trata dunha frase *mal* formulada. Non é o caso, pois a súa tradución a linguaxe formal foi dada polo matemático arxentino Gregory Chaitin.

Na súa tese *A simple proof of Gödel's first incompleteness theorem*, o loxicista americano George Boolos (1940-1996) deu unha demostración equivalente do primeiro teorema da incompletude baseándose neste paradoxo, no lugar do paradoxo do mentireiro. Para Boolos, unha *definición de n* era unha proposición que se satisfai para x se e só se $x = n$ para algún natural n . A idea da proba foi formalizar a proposición “ m é o primeiro natural non definible en menos de k símbolos” e probar que era unha definición no senso establecido (consultable en [3]).

4.4. Segundo teorema da incompletude

Publicado no mesmo artigo que o primeiro (aínda que sen ofrecer proba ningunha), o segundo teorema da incompletude da resposta ó famoso segundo problema de Hilbert: “Existe unha demostración finitaria da consistencia da aritmética?”. A formulación do teorema é a seguinte:

Ningunha teoría consistente contendo a aritmética básica é capaz de probar a súa propia consistencia.

En primeiro lugar, considérese unha *fbf* pechada que expresa a non existencia de demostracións dunha *fbf* e a súa negación á vez (é dicir, expresa a consistencia da teoría):

$$\text{Consist} : (\forall x_1)(\forall x_2)(\forall x_3)(\forall x_4)\neg(\text{dem}(x_1, x_3) \wedge \text{dem}(x_2, x_4) \wedge \text{neg}(x_3, x_4)).$$

Entón, o primeiro teorema da incompletude (4.30, A) pode reescribirse da seguinte forma:

$$\text{Consist} \rightarrow \mathcal{G}.$$

Teorema 4.36 (Segundo teorema da incompletude de Gödel). *Se a aritmética de Peano \mathcal{AP} é unha teoría consistente, entón $\not\vdash \text{Consist}$.*

Demostración. Nótese primeiramente que \mathcal{AP} cumpre as hipóteses do primeiro Teorema da incompletude 4.30. Todo o razoamento metamatemático empregado na demostración do apartado A de 4.30 pode ser expresado mediante *fbfs* de \mathcal{AP} , polo que $\vdash \text{Consist} \rightarrow \mathcal{G}$. Con todo, se \mathcal{AP} é consistente, tense entón que $\not\vdash \mathcal{G}$. Se Consist fose un teorema, por *modus ponens* teríase que \mathcal{G} tamén o é, o cal é unha contradición. \square

Observación 4.37. O teorema 4.36 foi probado para a aritmética de Peano, mais a demostración é exactamente a mesma para calquera extensión dela, sempre e cando conserve un sistema de axiomas recursivo.

Observación 4.38. Como resultado de ambos teoremas da incompletude, as teorías cumprindo as hipóteses requiridas non poden ser consistentes e completas ó mesmo tempo.

En consecuencia, ningunha teoría formal (axiomáticamente recursiva) contendo a aritmética de Peano sería capaz de probar a súa consistencia, de ser esta consistente. É dicir, a demostración da consistencia ten que vir de fóra. No capítulo a continuación menciónase unha proba dada no 1936 por un dos asistentes de Hilbert, Gerhard Gentzen.

Entre os matemáticos, o seu traballo sobre a incompletude foi xeralmente recoñecido como importante e incluso épico. O mesmo John von Neumann, cando Gödel recibiu o Premio Einstein en 1951 (xunto con Julian Schwinger) dixo del: “O logro de Kurt Gödel na lóxica moderna é singular e monumental - de feito, é máis que un monumento, é un fito que permanecerá visible lonxe no espazo e no tempo” [4, p. 157]. Aínda así, non todo foron sorrisos. En setembro de 1931 (despois de encontrarse con el nunha conferencia), Ernst Zermelo (1871-1953) escribiu a Gödel, dicindo que atopara un erro no seu teorema da incompletude. Iniciaron pois unha longa correspondencia, na que Gödel fixo un considerable esforzo por explicar e aclarar a súa demostración a Zermelo. O carteo permaneceu cordial, mais Zermelo non ficou convencido. Foi entón cando Gödel recorreu ó seu compañeiro do círculo de Viena Rudolf Carnap (1891-1970), e ámbolos dous estiveron de acordo en que Zermelo simplemente non acabara de entender a demostración.

Capítulo 5

Consecuencias

5.1. O programa de Hilbert despois de Gödel

Nun principio, a Hilbert non lle agradaron moito os resultados de Gödel, mais tempo despois acabaría por aceptalos como correctos e tentaría adaptar o seu propio programa en consecuencia. No entanto, Gödel descubriu que, na súa opinión, algúns deses intentos non tiñan en conta correctamente os seus resultados e tampouco eran consistentes cos propios principios de Hilbert.

Gödel declarou que era imposible alcanzar a gran maioría dos obxectivos do programa de Hilbert, polo menos na súa interpretación máis natural. O seu segundo teorema da incompletude mostrou que calquera teoría abondo consistente para codificar a suma e o produto de enteiros non é capaz de demostrar a súa propia consistencia. O programa veuse abaixo:

1. É imposible formalizar toda a matemática, sempre existirán afirmacións verdadeiras que non poidan ser demostradas¹. Non existen extensións completas e consistentes mesmo da aritmética de Peano (axiomáticamente recursivas), polo que a meirande parte das teorías relevantes fican incompletas.
2. Se a aritmética de Peano, \mathcal{AP} , non pode sequera probar a súa propia consistencia, resulta aínda máis complicado demostrar a consistencia de teorías máis poderosas (véxase a teoría de conxuntos).
3. Non existe un algoritmo que poida determinar a veracidade ou falsidade de afirmacións dentro da aritmética de Peano, nin en extensións consistentes dela. Esta conclusión apareceu anos máis tarde da publicación dos teoremas da incompletude, cando xa se definira exactamente o que era un algoritmo.

¹Un exemplo é a hipótese do continuo.

Con todo, o programa de Hilbert continuou a ser de gran importancia para moitas liñas de investigación na lóxica, en concreto na *teoría da demostración* e na *matemática inversa*. Facendo lixeiras modificacións nos seus obxectivos orixinais, gran parte deles puido ser salvado.

En primeiro lugar, aínda que non é posible probar a completude para sistemas que poden expresar polo menos a aritmética de Peano, si é posible probar formas da completude para moitos outros sistemas que poden ser de interese. Un exemplo é teoría dos corpos alxeбраicamente pechados con característica fixa, cuxa completude foi probada. O mesmo acontece coa imposible decidibilidade da aritmética, o polaco Alfred Tarski (1901-1983) acadou un algoritmo para decidir a veracidade ou falsidade de calquera enunciado en xeometría analítica [4]. En consecuencia, e dado o axioma de *Cantor-Dedekind*, a xeometría euclidiana é unha teoría decidable.

A cuestión da existencia de demostracións finitarias da consistencia é difícil de responder, principalmente porque non hai unha definición xeralmente aceptada dunha “demostración finitaria”. A maioría dos matemáticos na teoría da demostración semella considerar a matemática finitaria como contida na aritmética de Peano, e neste caso non é posible dar probas finitarias de teorías razoablemente fortes. A primeira demostración externa de consistencia para a aritmética veu no ano 1936 da man do alemán Gerhard Gentzen (1909-1945), a chamada *proba do paquete*. Permitted unha demostración correcta empregando métodos alleos á teoría formal, como o principio de indución transfinita [12, sección 2.3]. O seu traballo marcou o comezo da teoría da demostración post-Gödeliana: de Gentzen en adiante, as teorías axiomáticas analízanse segundo os principios de indución transfinita, necesarios para probar a consistencia da teoría. Con todo, a contribución e a influencia de Gentzen van máis aló: el enfatizou que os métodos da teoría da demostración non só permiten probar a consistencia dunha teoría, senón que tamén permiten extraer información das probas máis alá do feito de que o teorema dedúcese a partir dos axiomas.

Por último, cabe destacar que, aínda que non sexa posible formalizar toda a matemática, si que é posible facelo para practicamente toda a que se usa no día a día. En particular, a teoría de conxuntos de Zermelo-Fraenkel, combinada coa lóxica de primeira orde, proporciona un formalismo satisfactorio e xeralmente aceptado para case toda a matemática actual.

5.2. Computabilidade

No ano 1936, á sorprendente idade de 23 anos, Alan Turing publicou un artigo en resposta ó problema “de decisión” de Hilbert (*Entscheidungsproblem*). A intención era demostrar que non existe un algoritmo capaz de dicir se unha *fbf* dada nunha teoría formal \mathcal{K}_1 é lóxicamente válida ou non. É dicir, probar que o cálculo predicativo é indecible.

Lémbrese que o teorema da completude de Gödel establecía unha equivalencia entre as *fbfs*

lógicamente validas e as *fbfs* demostrables. De esta maneira, o *Entscheidungsproblem* equivalería a encontrar un método mecánico que decidira se unha *fbf* é un teorema ou non, empregando as regras da lóxica (axiomas e inferencia). Esta idea corresponde a noción de *función computable*, coa que Turing mostrou que o problema non tiña solución: non existe tal algoritmo. O resultado coñécese hoxe en día como *Tese de Church-Turing*, pois foi deducida polos dous matemáticos ó mesmo tempo e de forma independente: Church mediante o seu *cálculo- λ* e Turing grazas ás famosas *máquinas de Turing*. Posteriormente, o matemático americano Stephen Kleene (1909-1994), estudante de Church, demostrou que estas dúas nocións, así como a de *función recursiva*, eran equivalentes [4, capítulo 12]. Así pois, os teoremas da incompletude poden ser demostrados empregando as máquinas de Turing ou ben o cálculo- λ .

Como resposta ós teoremas da incompletude, algúns lóxicos e filósofos negan a posible existencia dunha máquina que poida chegar a pensar e comprender igual ca o ser humano. Especificamente, pensan que non podería levar a cabo probas matemáticas sen intervención dunha persoa. O propio Gödel inclinábase a favor desta postura, aínda que se abstivo de concretar a súa opinión de maneira formal, pois consideraba que faltaban moitos conceptos por definir: a intuición, a consciencia, o entendemento... Por outro lado, a cuestión de se a mente humana pode ser considerada como unha computadora baseada en nervios e neurotransmisores (no canto de electricidade e cables), está á orde do día.

Un dos argumentos contrarios á intelixencia artificial (xeral) máis famosos é o do filósofo John Lucas. Empregando o primeiro teorema da incompletude, mostrou as limitacións do sistema formal (ou máquina). Se hai sentencias indecibíbles (\mathcal{G}) que este non pode probar pero unha persoa si, iso significa que a mente humana posúe una intuición ou capacidade mental superior á da máquina. En consecuencia, o humano pode escapar o determinismo do sistema, e ten libre albedrío. Hai dúas formas de refutar este argumento, segundo o Dr. Mark Colyvan [9]: quen di que na mente humana non existe outra sentencia indecible propia, dígase \mathcal{G}_H , indetectable por definición? ou quen di que a mente humana é consistente?

5.3. Legado

No ano 1938, debido á anexión de Austria pola Alemaña nazi, Gödel tívose que trasladar de Viena a Nova Jersey, nos Estados Unidos. Alí comezou a traballar no acabado de inaugurar *Institute for Advanced Study* da universidade de Princeton, colaborando con académicos destacados como Albert Einstein, con quen mantiña unha bela amizade. Einstein [4, capítulo 14] dixo unha vez “O meu traballo xa non importa demasiado, a miña única motivación para achegarme á universidade e pra ter o privilexio de regresar a casa camiñando xunto a Kurt”. De feito foi o alemán o que axudou a Gödel a recibir a cidadanía estadounidense, que requiría coñecer a cons-

titución do país. No exame, Kurt informou ó xuíz que descubrira unha forma totalmente legal pola que alguén se podería converter en dictador dos Estados Unidos, achando unha contradición lóxica na propia constitución. Einstein mais o xuíz impidíronlle continuar a súa explicación, e a cidadanía fóiselle entregada no momento.



Figura 5.1: Kurt Gödel e Albert Einstein, 1950. Fotografía de Richard Arens, cortesía de *AIP Emilio Segrè Visual Archives* [1].

Ó longo da súa vida, Gödel enfrontouse a serios problemas de saúde mental, que se viron agravados coa súa marcha de Europa. Desenvolveu paranoias, o que o levou a illarse cada vez máis, temendo ser perseguido polos nazis. Esta condición afectoulle non soamente á súa saúde mental, senón á física: tiña un medo terrible a ser envelenado, e non comía agás que lle dera a comida a súa esposa Adele. Cando esta tivo que ser hospitalizada, Gödel deixou de alimentarse, conducíndoo á morte en 1978, pesando soamente 30 quilogramos. Segundo os médicos de Princeton, morreu “de desnutrición e inanición, por perturbacións na personalidade”.

A obra de Kurt Gödel sigue viva na actualidade. Os teoremas da incompletude marcaron profundamente campos como a lóxica, a filosofía e mesmo a informática. De feito, existe un *premio Gödel*, outorgado anualmente a publicacións sobresaíntes relacionadas coa teoría da computación. O seu traballo desafiou as ideas tradicionais da “invencibilidade do formalismo”, promulgando novas liñas de investigación e debate na filosofía das matemáticas e inspirando a aqueles que exploran os enigmas da lóxica e a verdade matemática.

Índice alfabético

	<i>existencial de unicidade</i>	27
	<i>universal</i>	6
	D	
	decidibilidad	19
	demostración	2
	E	
	elemento	10
	estoicismo	2
	expresión	2
	extensión	20
	F	
	<i>fbf</i> /frase ben formulada.....	2, 4, 7
	<i>falsa</i>	12
	<i>lógicamente válida</i>	12
	<i>pechada</i>	9
	<i>verdadeira</i>	12
	función.....	10
	<i>aritmética</i>	32
	<i>beta de Gödel</i>	37
	<i>característica</i>	35
	<i>cero</i>	33
	<i>diagonal</i>	43
	<i>inicial</i>	32
	<i>proyección</i>	33
	<i>recursiva</i>	33
A		
aritmética.....		25
<i>de Peano</i>		28
axioma.....		2
<i>de Peano-Dedekind</i>		25
<i>do principio de indución</i>		29
<i>lógico</i>		4, 13
<i>propio</i>		13
C		
cálculo		
<i>predicativo</i>		15
<i>proposicional</i>		4
clausura.....		9
completude.....		19
<i>semántica</i>		22
<i>sintáctica</i>		19
conector		
<i>clásico</i>		5
<i>primitivo</i>		4
consistencia.....		18
constante.....		6
<i>cero</i>		27
contradición.....		5
cuantificador		
<i>existencial</i>		8

<i>recursiva primitiva</i>	33		
<i>representable</i>	35		
<i>seguinte</i>	33		
funtor.....	6		
<i>n-ádico</i>	6		
<i>produto</i>	28		
<i>seguinte</i>	27		
<i>suma</i>	28		
			I
instancia.....	8		
<i>anoada</i>	8		
<i>libre</i>	8		
interpretación.....	4		
<i>dunha lóxica de primeira orde</i>	10		
<i>natural</i>	28		
			L
letra			
<i>de afirmación</i>	4		
<i>de función</i>	6		
<i>véxase funtor</i>	6		
<i>de predicado</i>	6		
<i>véxase relator</i>	6		
linguaxe			
<i>véxase lóxica</i>	2		
lóxica.....	2		
<i>aritmética</i>	27		
<i>de orde cero</i>	4		
<i>de predicados</i>	5		
<i>de primeira orde</i>	6		
<i>de segunda orde</i>	8		
<i>proposicional</i>	3		
			M
modelo.....	12		
<i>modus ponens</i>	4, 13		
			N
numeral.....	28		
número de Gödel.....	39		
			P
paradoxo			
<i>de Berry</i>	48		
<i>do mentireiro</i>	42		
premise.....	1		
problemas de Hilbert.....	31		
programa de Hilbert.....	31		
proposición.....	2		
			R
rango.....	6		
regra			
<i>de inferencia</i>	2		
<i>de minimización</i>	33		
<i>de recursividade</i>	33		
<i>de substitución</i>	33		
relación.....	10		
<i>aritmética</i>	32		
<i>expresable</i>	36		
<i>recursiva</i>	35		
<i>recursiva primitiva</i>	35		
relator.....	6		
<i>de igualdade</i>	27		
<i>n-ádico</i>	6		
			S
satisfatoriedade.....	11		
sentencia			
<i>de Gödel</i>	45		
sentencia indecidible.....	19		
signo de puntuación.....	4		
siloxismo.....	1		

Bibliografía

- [1] Arens, R.: *Kurt Gödel and Albert Einstein standing outdoors, courtesy AIP Emilio Segrè Visual Archives*. (1954). URL <https://repository.aip.org/islandora/object/nbla%3A290524>
- [2] Bobzien, S.: *Ancient Logic*. In: E.N. Zalta (ed.) *The Stanford Encyclopedia of Philosophy*, Summer 2020 edn. Metaphysics Research Lab, Stanford University (2020)
- [3] Boolos, G.: *Una demostración del Teorema de Incompletitud de Gödel*. *Gaceta de la Real Sociedad Matemática Española* 4(3), 521–526 (2001)
- [4] Brewer, W.D.: *Kurt Gödel. The genius of metamathematics*. Springer (2022)
- [5] Castillo, C.I.: *Lógica y Teoría de Conjuntos*. URL <https://www.uv.es/ivorra/Libros/Logica.pdf>
- [6] Gödel, K.: *Kurt Gödel's portrait*. (1970). URL <https://commons.wikimedia.org/w/index.php?curid=144622468>
- [7] Lombrana, J.V.: *Historia de la lógica*, 1ª edn. Servicio de Publicaciones de la Universidad de Oviedo. (1989)
- [8] Mendelson, E.: *Introduction to mathematical logic*, 6th edn. Textb. Math. Boca Raton, FL: CRC Press (2015)
- [9] Pensées, P.: *Gödel's Incompleteness Theorems vs. AI Minds* (2023). URL <https://www.youtube.com/watch?v=hHtXbIFn1Ng&t=440s>
- [10] Stansifer, R.: *Presburger's Article on Integer Arithmetic: Remarks and Translation*. Tech. Rep. TR84-639, Cornell University, Computer Science Department (1984)
- [11] Travesía, L.: *Gottlob Frege y el Nacimiento de la Lógica Matemática - Filosofía del siglo XX (y XIX)* (2024). URL <https://www.youtube.com/watch?v=4IUDk1xW-Bc>

- [12] Zach, R.: - *Hilbert's Program Then and Now*. In: D. Jacquette (ed.) *Philosophy of Logic, Handbook of the Philosophy of Science*, pp. 411–447. North-Holland, Amsterdam (2007)
- [13] Zalta, E.N.: *Gottlob Frege*. In: E.N. Zalta (ed.) *The Stanford Encyclopedia of Philosophy*, Summer 2009 edn. Metaphysics Research Lab, Stanford University (2009)

