1 Introducció

Abans de començar hem de definir què entenem per *fonamentació de la Matemàtica*: és l'intent d'elucidar en què consisteix i què garanteix la veritat de les proposicions matemàtiques. Dit d'una altra manera, ¿en què ens podem basar per afirmar que un fonament matemàtic és cert?

Qualsevol teoria matemàtica està fonamentada sobre unes bases que es consideren evidents i són acceptades sense requerir una demostració: són els anomenats *axiomes*, els punts de partida per començar a construir. És semblant la noció de *postulat*, amb la diferència que un postulat no té per què ser evident però s'accepta perquè no existeix un altre principi a què poder-lo referir.

Al llarg de la història de la Matemàtica s'ha cercat aquesta solidesa en la fonamentació, en menor o major grau. Euclides (s. III a.C.), en el seu primer llibre dels *Elements*, ja va voler tractar la Geometria d'una manera formal i sistemàtica, per això comença amb 23 definicions, 5 postulats i 5 "nocions comunes", i en tot això basa les proposicions que en segueixen. El s. XIX va representar un intent de generar rigor i certesa en l'edifici de les Matemàtiques: Peano va definir els nombres naturals a partir d'uns axiomes i regles; Hilbert, després del daltabaix que suposà el descobriment de les geometries no euclidianes, va refonamentar la geometria a partir d'un nou sistema d'axiomes més genèric que no contenia el cinquè postulat d'Euclides (el de les paral·leles).

¿Però com podien estar segurs que els sistemes d'axiomes eren prou "bons"? Els matemàtics sempre s'han hagut d'enfrontar a situacions inesperades i sorprenents, paradoxes que han posat en dubte aquesta bondat de les bases de l'edifici matemàtic i que sovint han desembocat en una reformulació dels axiomes. Per exemple, el descobriment de la incommensurabilitat va tirar per terra la ferma creença de la secta pitagòrica que els nombres enters eren l'essència de l'univers i que, donats dos segments qualssevol, sempre es podia trobar un tercer que estigués contingut un nombre sencer de vegades en els dos primers; va ser la primera crisi de fonaments en la història de la Matemàtica. La paradoxa que afirma que "una part d'un conjunt infinit es pot posar en correspondència biunívoca amb el tot" va ser resolta per Cantor (s. XIX) després d'haver definit els conceptes adequats per comparar conjunts infinits, cosa que suposà una revolució de la qual nasqué la teoria de conjunts moderna. Però aquesta teoria tornà a trontollar quan Russell (s. XX) descobrí la paradoxa que duu el seu nom: considerem el conjunt X dels conjunts que no són elements d'ells mateixos, això és, $X = \{A \mid A \notin A\}$, i preguntem-nos si X pot ser un element d'ell mateix. Si fos $X \in X$ llavors, per definició, X verificarà $X \notin X$, contradicció. Però si suposem que $X \notin X$, de nou per definició de X tenim que $X \in X$, contradicció. Així, hem obtingut una proposició contradictòria: $X \in X \Leftrightarrow X \notin X$.

2 La crisi fundacional. Els teoremes de Gödel

La *crisi fundacional de les Matemàtiques* fou el terme emprat a principis del s. XX per referir-se a la recerca de fonaments sòlids de les Matemàtiques.

Després que diverses escoles de filosofia de les Matemàtiques comencessin a trobar-se amb dificultats al s. XX, es va començar a posar en dubte l'assumpció que les Matemàtiques tinguessin un fonament que es pogués establir dintre de les mateixes Matemàtiques.

Els intents de proporcionar uns fonaments inqüestionables per a les Matemàtiques xocaven amb les conegudes paradoxes lògiques (com la que hem vist de Russell) que provocaven situacions d'inconsistència. (Un sistema d'axiomes es diu *consistent* si no se'n pot derivar una proposició contradictòria.)

De les escoles filosòfiques de l'època, la líder era la formalista de David Hilbert, que culminà amb el programa que duia el seu nom i que pretenia fundar tota la matemàtica sobre un sistema d'axiomes complet i finit, tot proporcionant una prova que aquests axiomes fossin consistents. La consistència de sistemes més complicats, com ara l'anàlisi real, s'havien de poder provar en termes de sistemes més simples i, en últim terme, la consistència de tota la matemàtica s'havia de poder reduir a l'aritmètica bàsica.

Però els teoremes d'incompletesa de Gödel, provats el 1931, van tirar pel terra el programa de Hilbert. En el seu primer teorema, Gödel mostrà que tot sistema consistent amb un conjunt d'axiomes capaç d'expressar l'aritmètica bàsica (això és, els nombres naturals amb les seves operacions elementals) no pot ser mai complet, això és, pot construir-se una proposició certa però que no es pot provar ni refutar a partir de les regles formals del sistema (d'això se'n diu una proposició *indecidible*). En el seu segon teorema, demostrà que un sistema així no pot provar la seva pròpia consistència i, per tant, no pot emprar-se per provar la consistència de quelcom més complicat.

Veiem ara un esbós de demostració dels teoremes de Gödel, ometent els aspectes més tècnics. La gran idea de Gödel va consistir a convertir nocions tals com la de la demostrabilitat d'una proposició en proposicions de l'aritmètica. Aquest procés d'aritmetització del discurs el va dur a terme mitjançant una codificació, que avui coneixem com a *numeració de Gödel*, que consistia a assignar un nombre natural a cada símbol de l'alfabet finit que emprem per construir les proposicions (nombres, símbols lògics, etc.), de manera que a cada proposició li corresponia un nombre natural diferent. Concretament, si una proposició estava formada per n símbols $s_1, \ldots, s_n$, als quals els corresponen n nombres naturals $x_1, \ldots, x_n$, llavors la codificació de Gödel de la proposició és $2^{x_1} \cdot 3^{x_2} \cdot \ldots \cdot p_n^{x_n}$ on p_n és el n-èsim nombre primer. Així, per exemple, si el nombre de Gödel del símbol "0" és el 6 i el nombre de Gödel del símbol "=" és el 5, a la proposició "0 = 0" li correspon un nombre de

Gödel $2^6 \cdot 3^5 \cdot 5^6$. Gràcies al teorema fonamental de l'aritmètica, qualsevol nombre obtingut d'aquesta manera factoritza de forma única com a producte de primers, per tant és possible recuperar la proposició original a partir del seu nombre de Gödel.

En particular, el conjunt de propietats del nostre *sistema formal* (el nostre conjunt de símbols i regles per operar-hi formant proposicions) es numerable i podem formar una successió $\{W_i\}_{i\in\mathbb{N}}$ amb totes les propietats dels nombres naturals. Llavors podem notar $W_p(n)$ la proposició "el nombre n té la propietat W_p" i sigui $\phi(n,p)$ el nombre de Gödel d'aquesta proposició.

Sigui D el conjunt de nombres de Gödel de les proposicions demostrables del sistema, això és, $\phi(n,p) \in D$ si i només si $W_p(n)$ és demostrable. Donat un nombre natural n, considerem la següent propietat: $\phi(n,n) \notin D$ (que equival a dir $W_n(n)$ no és demostrable, o bé, no és demostrable que n tingui la propietat W_n). Com aquesta és una propietat possible dels nombres naturals, li correspondrà un índex q dins de la successió $\{W_i\}_{i\in\mathbb{N}}$ de totes les propietats, de manera que $W_q(n)$ és la proposició "$W_n(n)$ no és demostrable", o equivalentment, "$\phi(n,n) \notin D$". Amb tot això, es defineix la *proposició de Gödel*:

$$\mathcal{G} = \text{“}\phi(q,q) \notin D\text{”},$$

que, pel que acabem de dir, equival a "$W_q(q)$ no és demostrable", que és precisament la proposició $W_q(q)$. Observem que, procedint d'aquesta forma, Gödel aconsegueix construir formalment una paradoxa semblant a la de la proposició "aquesta frase no és certa".

Ara ja és fàcil acabar. Com $\mathcal{G} = W_q(q)$, el seu nombre de Gödel és $\phi(q,q)$. Llavors, si suposem que $\mathcal{G}$ és demostrable estem dient que $\phi(q,q) \in D$, però això entra en contradicció amb allò que afirma $\mathcal{G}$, que és precisament el contrari: $\phi(q,q) \notin D$. Si, pel contrari, suposem que $\mathcal{G}$ no és demostrable estem dient $\phi(q,q) \notin D$, que és precisament l'enunciat de $\mathcal{G}$ i, per tant, $\mathcal{G}$ seria demostrable, contràriament a allò que hem suposat. En conclusió, $\mathcal{G}$ és una proposició *indecidible*. A més a més, en un cert sentit $\mathcal{G}$ també és certa, perquè està afirmant quelcom que té lloc: $\phi(q,q) \notin D$. Això acaba la prova del primer teorema d'incompletesa de Gödel.

El segon teorema, que afirma que un sistema formal prou complex com per contenir l'aritmètica dels nombres naturals no pot provar la seva pròpia consistència, es pot deduir del primer de la següent manera: considerem la proposició que afirma la consistència del sistema, això és, "D'aquest sistema no se'n pot derivar una proposició i la seva negació". Anomenem-la, de manera abreujada, AC (Absència de Contradicció) i tornem a considerar la proposició de Gödel $\mathcal{G}$ del primer teorema. Ja hem vist que si el sistema és consistent (això és, si podem provar AC) llavors $\mathcal{G}$ no és demostrable; llavors, si formalitzem aquesta prova en el sistema obtenim que la proposició "$\mathcal{G}$ no és demostrable" es pot provar dins el sistema. Però aquesta proposició equival a la mateixa $\mathcal{G}$, per tant $\mathcal{G}$ es pot provar en el

sistema. Aquesta contradicció prové d'haver suposat que podem demostrar AC.

3 Conseqüències dels teoremes de Gödel

Els teoremes de Gödel no empobreixen la Matemàtica, sinó que ens ajuden a desfer-nos d'un prejudici que ha imperat per molt de temps sobre allò que la Matemàtica en realitat és. En particular, van acabar amb el desig de l'escola formalista de Hilbert de tenir una completa seguretat a través d'una demostració que els principis sobre els quals es treballa són sòlids i que en el seu edifici no apareixeran mai esquerdes que obliguin a remodelacions més o menys substancials, com ha passat al llarg de la història de les Matemàtiques. Per contra, això ha fet que els matemàtics s'acostumin a conviure amb proposicions indecidibles dintre dels sistemes formals, cosa que brinda una fantàstica oportunitat per descobrir i explorar nous universos: només cal recordar que les geometries no euclidianes van néixer en el moment que Lobatxevski i Bolyai van adonar-se que el postulat de les paral·leles era indecidible dins de la geometria absoluta i van construir un sistema d'axiomes consistent format pels de la geometria absoluta juntament amb la negació del de les paral·leles.

Tanmateix, una bona part del programa del Hilbert sí que es va poder salvar després de modificar-ne lleugerament els objectius: moltes línies de recerca actuals en lògica matemàtica i teoria de la demostració es poden veure com a continuacions naturals del programa. Una sèrie de resultats que s'han pogut obtenir són:

- Tot i que no és possible formalitzar totes les Matemàtiques, sí que es pot formalitzar essencialment tota la Matemàtica que "tothom fa servir" en l'actualitat. A la pràctica, la immensa majoria dels matemàtics accepten de forma general com a sistema formal satisfactori el sistema d'axiomes de Zermelo-Fraenkel amb l'axioma de l'elecció (abreujadament, ZFC) combinat amb la lògica de primer ordre, amb el qual s'eviten les paradoxes lògiques com la de Russell. Cal notar que, a conseqüència dels teoremes de Gödel, ZFC no pot provar la seva pròpia consistència a menys que sigui inconsistent, però avui dia es creu molt improbable que ZFC contingui alguna contradicció.

- Tot i que no és possible provar la completesa per sistemes almenys tan potents com l'aritmètica de Peano, sí que és possible provar formes de completesa per a molts sistemes interessants. El primer gran èxit fou degut al mateix Gödel, que demostrà el teorema de completesa per a la lògica de primer ordre, mostrant que qualsevol conseqüència lògica d'una sèrie d'axiomes és demostrable.

- Tot i que no existeix cap algorisme per decidir la veracitat o falsedat de proposicions

dins de l'aritmètica de Peano, hi ha multitud de teories interessants per a les quals sí existeixen algorismes així. Per exemple, existeix un algorisme per determinar la veracitat de qualsevol proposició de la geometria euclidiana.

D'altra banda, podem enumerar algunes de les proposicions més famoses que s'ha demostrat que són indecidibles:

- **El problema de la parada** (*halting problem* en anglès). En teoria de la computabilitat, és un problema de decisió que pot enunciar-se així: "Donat un programa i una entrada, decidir si el programa s'atura en un nombre finit de passos o, pel contrari, continua executant-se indefinidament". Alan Turing demostrà el 1936 que no pot existir un algorisme que resolgui el problema per a totes les parelles possibles programa-entrada. Diem que aquest problema és indecidible sobre màquines de Turing.
- **La hipòtesi del continu** (abreujadament, HC). Fou una conjectura formulada per Cantor el 1877, que establia: "No existeix cap conjunt la cardinalitat del qual estigui estrictament compresa entre la dels nombres naturals ($\aleph_0$) i la dels nombres reals ($2^{\aleph_0}$)". Aquesta conjectura es convertí en el primer dels 23 problemes de Hilbert de l'any 1 900. El 1 940 Gödel mostrà que HC no es pot refutar basant-se en ZFC i el 1 963 Paul Cohen mostrà que tampoc no es pot provar dins de ZFC. Tots dos resultats es basen en la hipòtesi que ZFC és consistent, cosa que, com hem comentat abans, és avui dia àmpliament acceptada. Així, la independència de HC respecte de ZFC fa que ZFC+HC i ZFC+$\neg$HC siguin dues teories de conjunts essencialment diferents.
- **L'axioma de l'elecció** (abreujadament, AC). Formulat per Zermelo el 1 904: "Donada una col·lecció $(S_i)_{i\in I}$ de conjunts no buits, existeix una col·lecció $(x_i)_{i\in I}$ d'elements tals que $x_i \in S_i$ per a tot $i \in I$". Dit de manera informal, AC afirma que, donada una col·lecció de conjunts no buits, sempre es pot triar un element de cada conjunt. En molts casos no cal recórrer a aquest axioma per fer una tria així, per exemple, quan la col·lecció de conjunts és finita o bé la regla de selecció està ben definida. Es demostrà que AC és indecidible en ZF, per tant independent de ZF, i s'acostuma a afegir a ZF per formar ZFC, el sistema d'axiomes estàndard.

Els teoremes d'incompletesa de Gödel també han servit per provar altres resultats, com per exemple el desè problema de Hilbert, enunciat l'any 1 900, que dia: "Donada una equació diofàntica amb qualsevol nombre d'incògnites amb coeficients enters, donar un algorisme amb què, en un nombre finit de passos, pugui determinar-se'n la resolubilitat sobre els enters". L'any 1 970 el matemàtic soviètic Yuri Matiyasévich demostrà, tot emprant els teoremes de Gödel, que no podia existir un algorisme així.