El Teorema de Gödel
Indecidibilitat i Recursivitat

Josep Pla i Carrera
Professor emèrit de la UB

Acte
La lògica matemàtica i la història de la ciència

Càtedra Lluís Santaló d'Aplicacions de la Matemàtica
Casa de Cultura de la Diputació de Girona

Aula Magna (Casa de Culura)
Girona, 11 de desembre de 2014

Índex

1. INTRODUCCIÓ

Georg [Ferdinand Ludwig Philipp] Cantor

St. Petersburg (Rússia), 3 de març de 1845.
Halle (Alemanya), 6 de gener de 1918.

Una primera qüestió deguda a Georg Cantor

Amb els conceptes:

Equipotència [$X \sim Y$] de dos conjunts X i Y,

Dominància estricta [$X \prec Y$] d'un conjunt Y sobre un altre X,

Cantor estableix el teorema següent:

Teorema de Cantor

Per a cada conjunt X, el conjunt $\mathcal{P}(X)$ de «tots els subconjunts» de X ***domina estrictament*** *el conjunt X. O sigui $X \prec \mathcal{P}(X)$.*

Una primera qüestió deguda a Georg Cantor

Del teorema de Cantor en resulta un corol·lari trivial:

Si el «grau d'infinitud» del conjunt $\mathbb{N}$ dels nombres naturals és $\aleph_0$, aleshores «grau d'infinitud» del conjunt $\mathcal{P}(\mathbb{N})$, $2^{\aleph_0} := \aleph_1$ (?) —que és el mateix que el del conjunt $\mathbb{R}$ dels nombres reals— és estrictament més gran. És a dir, $\aleph_0 < \aleph_1$.

Cantor demostra també el resultat següent:

*Les paraules i frases **finites** que podem fer amb qualsevol llenguatge **finit** tenen el grau d'infinitud de $\mathbb{N}$; és a dir, $\aleph_0$.*

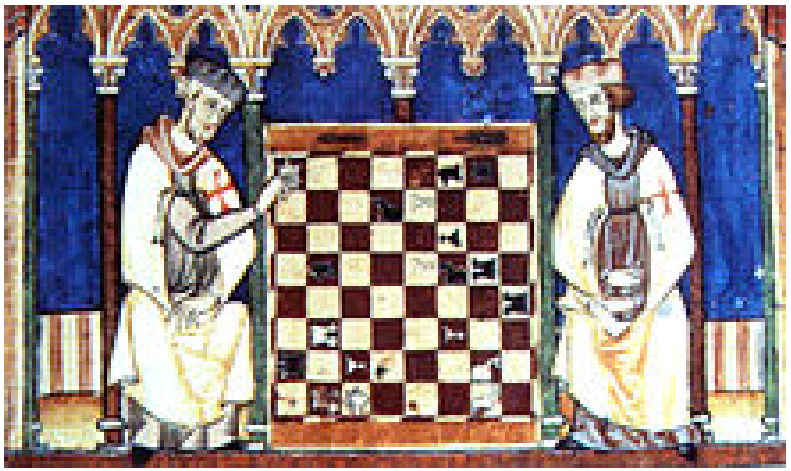
Una conseqüència que m'interessa posar de manifest:

Un llenguatge finit no permet descriure tots els subconjunts de $\mathbb{N}$, ni tampoc tots els nombres reals. No hi ha prou paraules.

No és possible «donar nom a totes les coses».

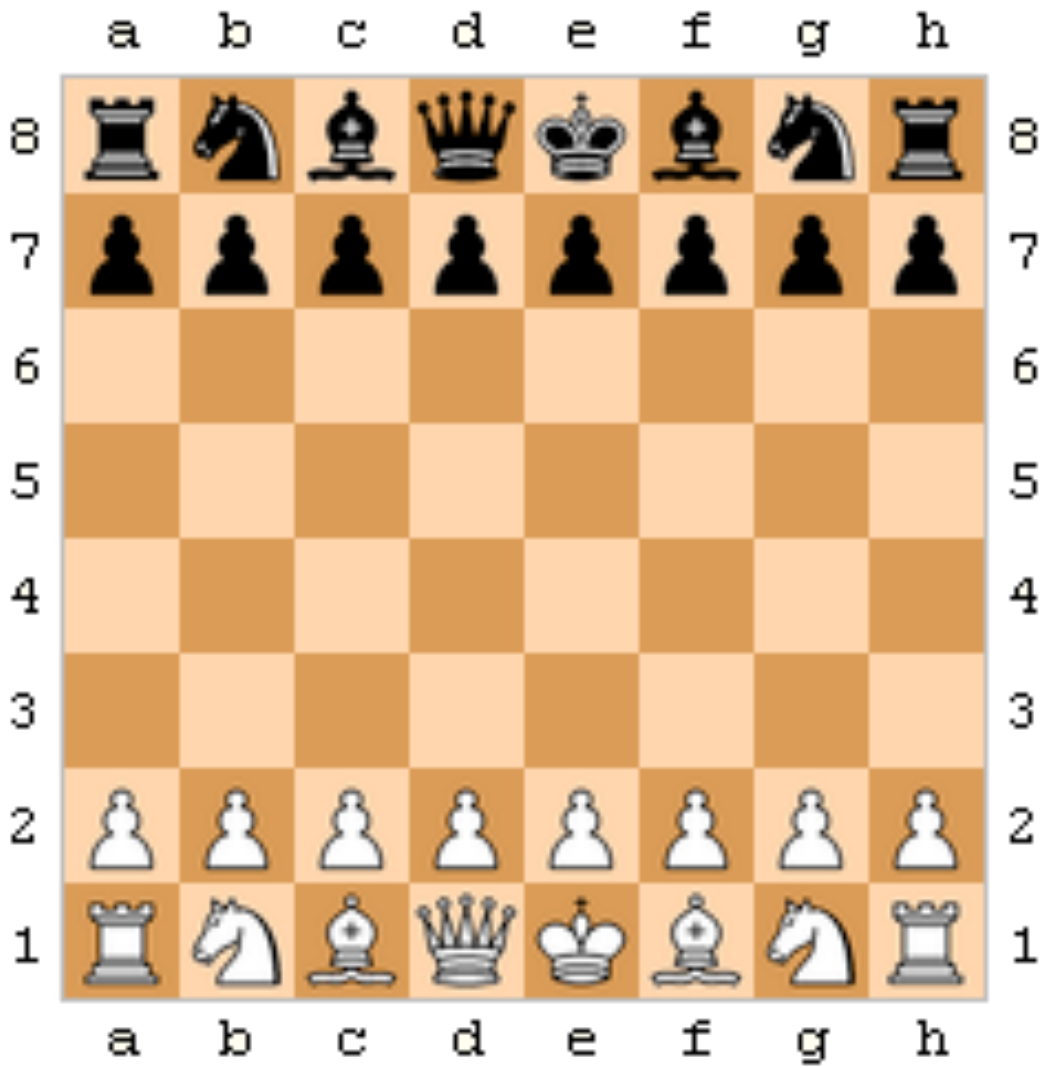
Hi ha, doncs, certes possibilitats que, no només no podem demostrar, sinó que ni tan solament podem enunciar.

El braman indi Lahur Sessa creant el xaturanga, predecessor del Joc d'Escacs (de l'artista brasiler Thiago Cruz, 2007).



Templers disputant una partida d'escacs en una miniatura del *Libro de los juegos* (Alfons X el Savi, 1283).

El joc d'escacs



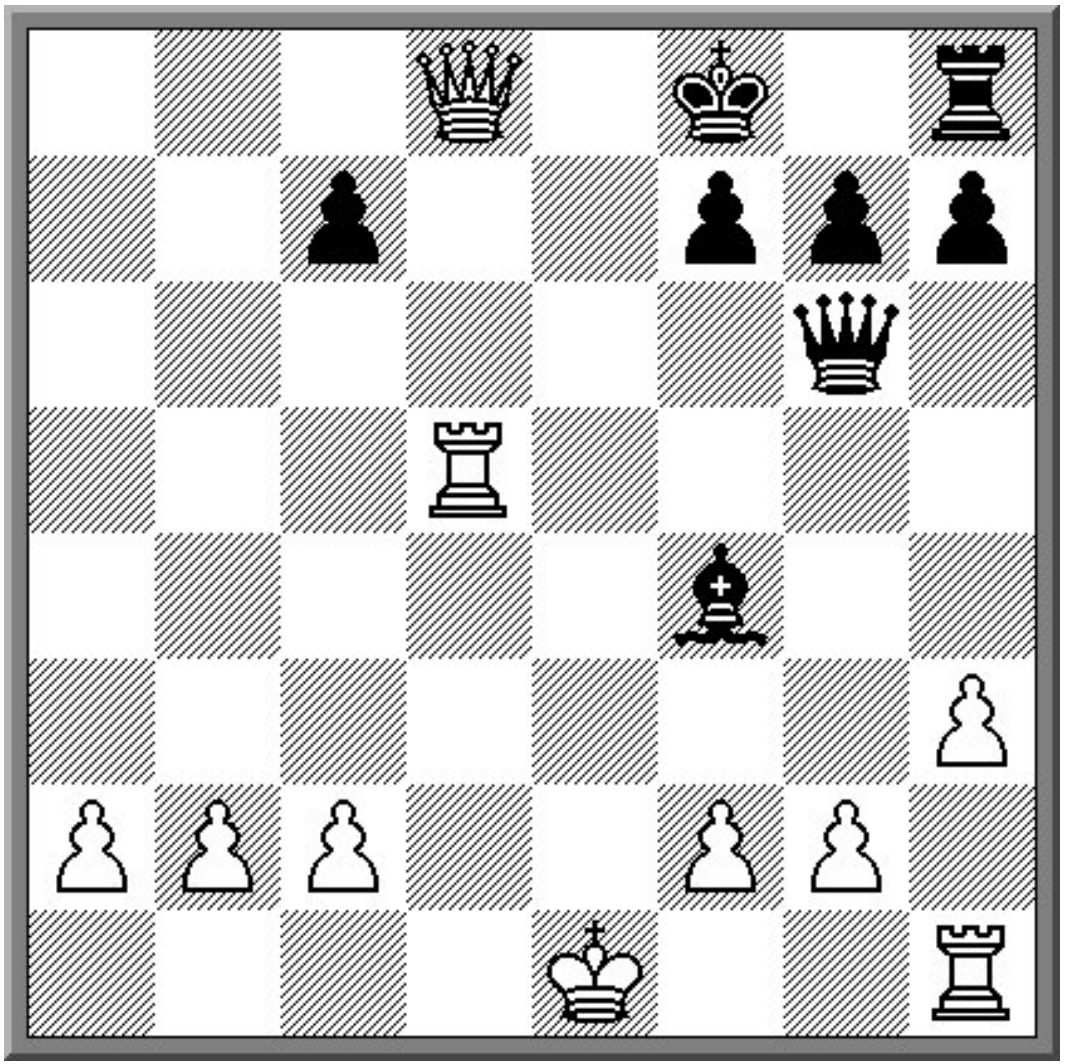
Fitxes (els objectes)

Moviments (les regles).

Inici (l'axioma).

El joc d'escacs

Castellví (blanques)-Vinyoles (negres), València, c. 1475



1. **e4 d5**; 2. **ed5 Dd5**;
3. **Cc3 Dd8**; 4. **Ac4 Cf6**;
5. **Cf3 Ag4**; 6. **h3 Af3**;
7. **Df3 e6**; 8. **Db7 Cbd7**;
9. **Cb5 Tc8**; 10. **Ca7 Cb6**;
11. **Cc8 Cc8**; 12. **d4 Cd6**;
13. **Ab5 Cb5**; 14. **Db5 Cd7**;
15. **d5 ed5**; 16. **Ae3 Ad6**;
17. **Td1 Df6**; 18. **Td5 Dg6**;
19. **Af4 Af4**; 20. **Dd7 Rf8**;
21. **Dd8 mat**.

El tauler mostra la disposició final: d'escac i mat.

Jules Richard

Blet (Cherm, França), 12 d'agost de 1862.

Châtoroux (Indre, França), 14 d'octubre de 1956.

La paradoxa de Richard

La **paradoxa de Richard** tracta dels signes associats a les frases.

Fem totes les **frases aritmètiques** catalanes possibles [en total $\aleph_0$].

«és l'u».	(**1**)
⋮	⋮
«és primer».	(**5**)
⋮	⋮
«és més gran que vint-i-tres».	(**23**)
⋮	⋮
«és el nombre primer més gran de tots els nombres primers».	(**1001**)
⋮	⋮
«és aquell que, escrit en base dos, té, en total, menys de dos milions de símbols zero i u».	(**7033**)
⋮	

La paradoxa de Richard

Ara podem establir la definició següent:

Definició de Richard

Un nombre natural **n** és **richardià** si **no satisfà** la propietat que enumera. Altrament, és **no-richardià**

Aleshores, segons el llistat anterior,

1 **és** **no-richardià**.
5 **és** **no-richardià**.
23 **és** **richardià**.
1001 **és** **richardià**.
7033 **és** **richardià**.

Pregunta natural:

El nombre natural **r** que correspon a la frase aritmètica «**és richardià**», **com és**? **És richardià** o **no-richradià**?

Resposta:

r és **richardià** si, i només si, és **no-richardià**.

Heus ací la paradoxa de Richard.

La paradoxa de Richard

La **paradoxa de Richard** tracta dels signes associats a les frases.

Fem totes les **frases aritmètiques** catalanes possibles [en total $\aleph_0$].

«és l'u».	$(\frac{1}{1})$	**(1000)**
⋮	⋮	⋮
«és primer».	$(\frac{1}{5})$	**(3)**
⋮	⋮	⋮
«és més gran que vint-i-tres».	$(\frac{1}{23})$	**(70 212)**
⋮	⋮	⋮
«és el nombre primer més gran de tots els nombres primers».	$(\frac{1}{1001})$	**(33)**
⋮	⋮	⋮
«és aquell que, escrit en base dos, té, en total, menys de dos milions de símbols zero i u».	$(\frac{1}{7033})$	$(\mathbf{2^{1001}-1})$
⋮		

Giuseppe Peano

Spinetta (Piemont, Itàlia), 27 d'agost de 1858.

Torí (Itàlia), 20 d'abril de 1932.

Què són els nombres naturals?

Els nombres naturals són els objectes que satisfan els postulats:

P1. *Hi ha un primer element, el* 0. És a dir, el nombre natural 0 no és el següent de cap altre.

P1, formalment: $\forall v(\mathbf{s}(v) \not\equiv \mathbf{0})$.

P2. *Tot nombre natural té un següent.*

P2, formalment: $\forall v \exists w(v \equiv \mathbf{s}(w))$.

P3. *Si dos nombres naturals tenen següents iguals són iguals.*

P3, formalment: $\forall v \forall w(\mathbf{s}(v) \equiv \mathbf{s}(w) \rightarrow v \equiv w)$.

P4. *Tot conjunt* A *de nombres naturals* $[\subseteq \mathbb{N}]$ *que compleixi:*

$$\left\{ \begin{array}{l} (a)\ 0 \in A \\ (b)\ \text{si } n \in A,\ \text{aleshores } (n+1) \in A \end{array} \right\},$$

és el conjunt $\mathbb{N}$ *de* ***tots*** *els nombres naturals* $[A = \mathbb{N}]$.

Què són els nombres naturals?

Segons el resultat de Cantor, a l'hora de formalitzar **P4** tenim un problema

Les variables u, v, w,..., solament es refereixen a **una** mena d'objectes —en el nostre cas als «nombres naturals».

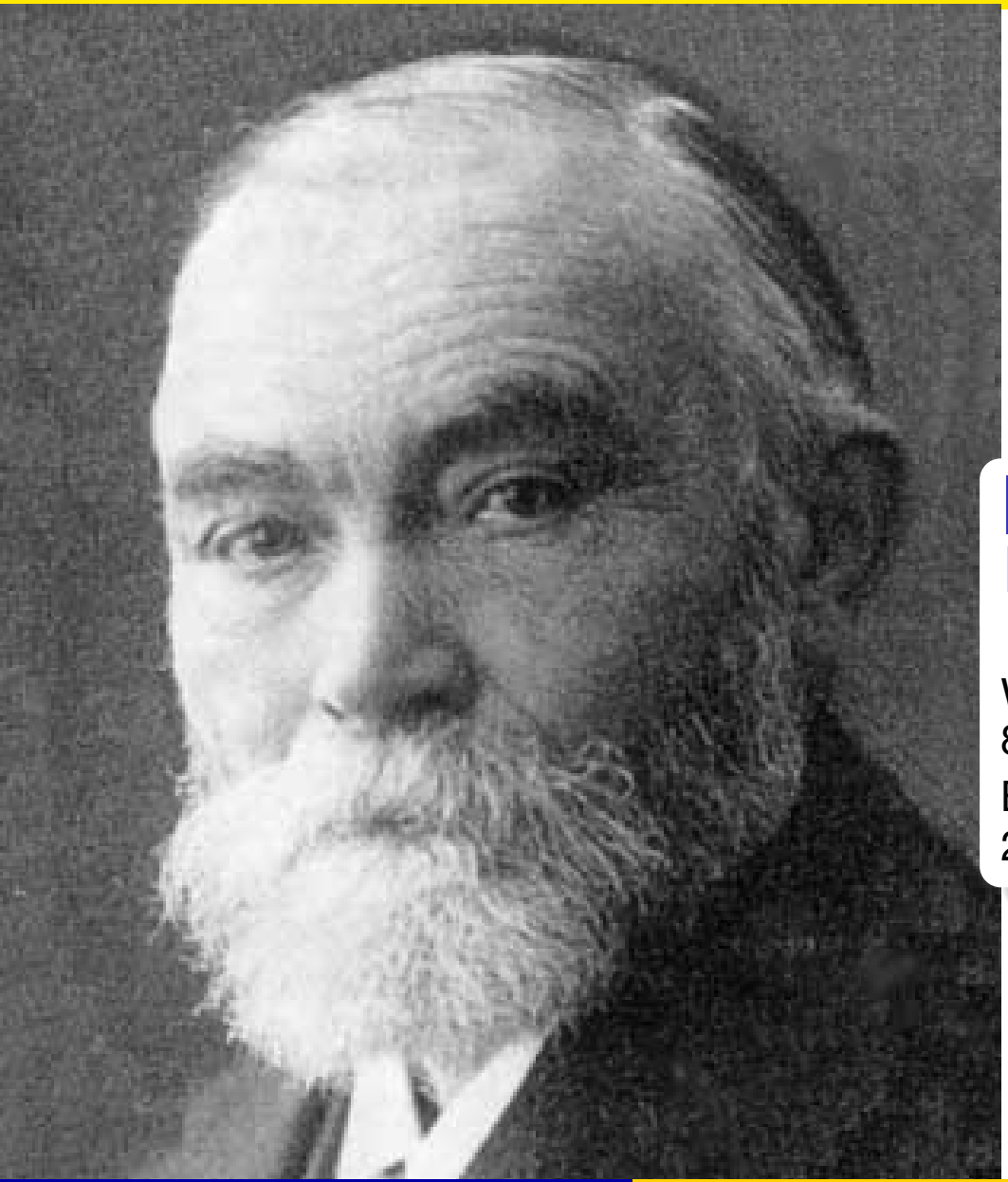
No poden designar alhora «nombres naturals» i «conjunts de nombres naturals».

Com ho podem resoldre?

Hem de recórrer a una idea de Gottlob Frege:

Identificar els conjunts de nombres naturals amb les fórmules del llenguatge formal amb una variable lliure.

Metalingüísticament les representarem $\varphi(u)$.



[Friedrich Ludwig] Gottlob Frege

Wismar (Mecklenburg-Schwerin, Alemanya),
8 de novembre de 1848.

Bad Kleinen (Mecklenburg-Schwerin, Alemanya)
26 de juliol de 1925.

Què són els nombres naturals?

Exemples. $\sigma_1 := \forall v \exists w (v \equiv \mathbf{s}(w))$ i $\sigma_2 := \forall v (\mathbf{s}(v) \not\equiv \mathbf{0})$ són sentències.

$\varphi_1(v) := \exists w (v \equiv \mathbf{s}(w))$ i $\varphi_2(w) := \forall v (\mathbf{s}(v) \equiv \mathbf{s}(w) \to v \equiv w)$ tenen, respectivament, lliure la variable v, w i, en cada cas, solament aquesta és lliure.

Necessitem la **idea de Frege**.

Els objectes que satisfan $\varphi(v)$ formen un conjunt (ideal, formal (?))
$A_\varphi := \{\mathbf{v} : \varphi(\mathbf{v})\}$.

Què són els nombres naturals?

Ja podem formalitzar **P4** al si del llenguatge $\mathcal{L}_{\text{ar}} := \langle \mathbf{0}, \mathbf{s}, (+, \cdot), = \rangle$.

Sigui $\varphi(v)$ una fórmula amb una variable lliure, la variable v, aleshores considerem

$$\mathbf{P4}'_{\varphi(v)}\text{: } \textit{Si} \left\{ \begin{array}{l} a)\ \varphi(\mathbf{0}), \\ b)\ \varphi(v) \to \varphi(\mathbf{s}(v)), \end{array} \right\}, \textit{ aleshores } \forall v \varphi(v).$$

No hem formalitzat **P4**!!! Hem formalitzat $\mathbf{P4}'_{\varphi(v)}$.

Ara canviem l'axioma **únic P4** per la **infinitat** d'axiomes $\mathbf{P4}'_{\varphi(v)}$ —una per cada fórmula $\varphi(v)$ i obtenim la teoria aritmètica de primer ordre $\mathbf{T}_{\text{ar}}$.

A causa del teorema de Cantor —malgrat recórrer a la infinitat d'expressions $\mathbf{P4}'_{\varphi(v)}$— l'axiomàtica aritmètica de primer ordre que en resulta és molt més pobre que la de Peano, amb l'únic axioma **P4**.

La veritat i la certesa

Quan es treballa amb expressions formals, com sabem si són **certes** o **vertaderes**?

Hi ha dos camins.

El **camí sintàtic** —el de la certesa— i el **camí semàntic** —el de la veritat.

Atenció!. Ambdós camins són relatius.

Un exemple molt senzill: la teoria de grups.
El llenguatge formal és: $\mathcal{L}_g := <*, \mathbf{e}, =>$.

Definició formal de [la **teoria $\mathbf{T}_g$** dels] grups

$$\left\{ \begin{array}{ll} \mathrm{G}_1.\ \forall \mathbf{u}\forall \mathbf{v}\forall \mathbf{w}\Big(((\mathbf{u}*\mathbf{v})*\mathbf{w}) = (\mathbf{u}*(\mathbf{v}*\mathbf{w}))\Big). & \text{Associativa} \\ \mathrm{G}_2.\ \forall \mathbf{u}((\mathbf{u}*\mathbf{e}) = (\mathbf{e}*\mathbf{u}) = \mathbf{u}). & \text{Element neutre (per a tots)} \\ \mathrm{G}_3.\ \forall \mathbf{u}\exists \mathbf{v}((\mathbf{u}*\mathbf{v}) = (\mathbf{v}*\mathbf{u}) = \mathbf{e}). & \text{Element invers (de cada element)} \end{array} \right.$$

La veritat i la certesa

La **certesa d'una teoria**. Allò que podem deduir correctament:

1. $\forall \mathbf{u}((\mathbf{u} * \mathbf{e}) = \mathbf{u})$ (G_2)
2. $\forall \mathbf{u}((\mathbf{u} * \mathbf{e}') = \mathbf{u})$ (Hipòtesi)
3. $(\mathbf{u} * \mathbf{e}) = (\mathbf{u} * \mathbf{e}')$ (Llei d'igualtat i particularització)
4. $\mathbf{u}^{-1} * (\mathbf{u} * \mathbf{e}) = \mathbf{u}^{-1} * (\mathbf{u} * \mathbf{e}')$ (Invers)
5. $(\mathbf{u}^{-1} * \mathbf{u}) * \mathbf{e} = (\mathbf{u}^{-1} * \mathbf{u}) * \mathbf{e}'$ (Associativa)
6. $\mathbf{e} = \mathbf{e} * \mathbf{e} = \mathbf{e} * \mathbf{e}' = \mathbf{e}$ (Neutre)

La sentència de (3) és un **teorema** de la teoria de grups; i també ho és la (2).

Per tant, és **tan** certa com certs siguin els axiomes que hem triat.

La **veritat en un model de la teoria**. Allò que és vertader en una es- tructura en la qual són vàlids els axiomes.

Considerem les estructures:

$$\mathcal{Z} = \{\mathbb{Z}, 0, +, =\},$$
$$\mathcal{Z}' = \{\mathbb{Z}, 0, -, =\},$$
$$\mathcal{N} = \{\mathbb{N}, 0, +, =\}.$$

Així, G_1, G_2 i G_3, llegides a $\mathcal{Z}$ són **vertaderes** o $\mathcal{Z}$-**vertaderes**.

En canvi, llegides a $\mathcal{Z}'$ falla (G_1) i llegides a $\mathcal{N}$ falla (G_3)

Diem aleshores que $\mathcal{Z}$ és un model de la teoria de grups —o simplement que $\mathcal{Z}$ **és un grup**.

La veritat i la certesa

De forma natural es planteja una pregunta:

La validesa i la certesa són el mateix?
Tenen alguna mena de lligam?

És fàcil demostrar que les regles lògiques —les regles que permeten fabricar els teoremes— conserven la validesa.

Tots els teoremes són vertaders en **tots** els models dels axiomes.

Queda, doncs una pregunta:

Podem afirmar que totes les sentències vàlides en un model d'una teoria són demostrables en la teoria? És a dir, són teoremes?

La resposta, **afirmativa**, la dónà Kurt Gödel en la tesi doctoral (1930).

Es coneix amb el nom de **teorema de completesa de Gödel** (1930).

$$\text{Vertader}(\mathcal{M}_{\mathbf{T}}) = \text{Teorema}(\mathbf{T})$$

2. ANÀLISI DEL TEOREMA

KURT [FRIEDRICH] GÖDEL

Brno, Moravia (Imperi austrohongar),
28 d'abril de 1906.

Princeton, New Jersey, (EEUU),
14 de gener de 1978.

L'enunciat del teorema d'incompletesa de Gödel

Teorema. ***Hi ha*** *una sentència* σ_G *que es pot escriure en el llenguatge aritmètic* $\mathcal{L}_{ar} := \langle \mathbf{0}, \mathbf{s}, (+, \cdot), = \rangle$ *que ni* σ_G*, ni* $\neg\sigma_G$ ***no és*** *demostrable en la teoria de primer ordre* $\mathbf{T}_{\text{ar}}$ *en el benentès que* $\mathbf{T}_{\text{ar}}$ és **consistent**.

És el **teorema d'incompletesa de Gödel** (1931).

Observació 1. Una de les dues sentències σ_G, $\neg\sigma_g$ és sempre verta-dera en tot model de la teoria de Peano.

En particular, una d'elles —σ_G o $\neg\sigma_G$— és vertadera en el model estàndard $\mathcal{N} = \{\mathbb{N}, 0, s, (+, \cdot), =\}$.

Observació 2. Una de les dues: en alguns models ho és una i en d'altres, l'altra.

Els tres llenguatges

En parlar de l'aritmètica parlem de **nombre naturals** i les seves propietats. És a dir, treballem al si del conjunt $\mathfrak{N}_{\text{ar}} := \langle \mathbb{N}, s, +, \cdot, =, < \rangle$.

Així, en català, podem dir: El número tres és un número primer.

Per traslladar-ho al llenguatge conjuntista, cal el conjunt:

$$\Pi := \{n \in \mathbb{N} : \ \textbf{per a tot } p, q \in \mathbb{N}\,(n = p \cdot q \to p = 1 \vee q = 1)\}.$$

Aleshores l'expressió anterior es pot reescriure: $3 \in \Pi$.

També podem dir, El conjunt dels nombres primers és **infinit**, que es reescriu, **Per a tot** $p \in \Pi$, **existeix un** $q \in \Pi, q > p$.

Heus ací dos llenguatges:
el llenguatge **natural** i el llenguatge **conjuntista**.

Els tres llenguatges

Per parlar d'aritmètica però al si d'una teoria formal, cal un llenguatge formal de primer ordre $\mathcal{L}_{\text{ar}} := \langle \mathbf{0}, \mathbf{s}, (+, \cdot), = \rangle$, i els **axiomes de Peano** per poder establir els **teoremes formals** de la teoria de Peano: $\mathcal{T}_{\text{ar}}$.

Si ara volem provar que

Hi ha una **infinitat** de nombres primers,

és un teorema d'aquesta teoria formal, d'entrada, cal **formalitzar** la propietat «u és primer».

$$\Pi(u) := \forall v \forall w \left(u = v \cdot w\right) \to \Big(\left(v \equiv \mathbf{s}\left(\mathbf{0}\right)\right) \vee \left(w \equiv \mathbf{s}\left(\mathbf{0}\right)\right)\Big).$$

Després hem de veure que **hi ha infinits primers**.
És a dir, la sentència

$$\sigma_{\text{primer}} := \forall u \Big(\Pi(u) \to \exists v \left(\Pi(v) \wedge v > u\right)\Big) \in \mathcal{T}_{\text{ar}}.$$

és un $\mathcal{T}_{\text{ar}}$-teorema. Breument, $\sigma_{\text{primer}} \in \mathcal{T}_{\text{ar}}$ o $\vdash_{\text{ar}} \sigma_{\text{primer}}$.

Heus ací el llenguatge **formal**.

Els tres llenguatges

Seguint Gödel, podem dir

> ***Teorema d'incompletesa de Gödel***. *Si la teoria de Peano de primer ordre $\mathcal{T}_{ar}$ és* ***consistent***, ***hi ha*** *una sentència σ_G del llenguatge aritmètic $\mathcal{L}_{ar}{:=}\langle \mathbf{0}, \mathbf{s}, (+, \cdot), = \rangle$* ***indecidible***. *És a dir, ni σ_G, ni $\neg\sigma_G$* ***no són*** *demostrables en la teoria $\mathcal{T}_{ar}$.*

Heus ací un enunciat en català ampliat amb certs signes per poder-nos referir de forma abreujada i clara tant a la teoria formal de Peano de primer ordre com a la sentència gödeliana indecidible.

Heus ací el llenguatge **natural**.

Els tres diccionaris

llenguatge **formal**

$\sigma := \forall v_1 \left(v_1 + \mathbf{s}(\mathbf{0}) \equiv \mathbf{s}(v_1) \right)$

$\overset{G}{\swarrow}$ $\overset{C}{\swarrow}$ $\overset{\mathbf{B}}{\nearrow}$

llenguatge **conjuntista**

$\forall x \in \mathbb{N} \left(x + s(0) = x + 1 \right)$

$\overset{A}{\leftrightarrows}$

$\overset{D}{\rightarrow}$

$\overset{D}{\searrow}$ $\overset{G}{\searrow}$

llenguatge **natural**

σ és un axioma de T_{ar}

$\overset{A}{\longleftarrow}$: Traslladant

$\overset{\mathbf{B}}{\nearrow}$: **La representabilitat**

$\overset{C}{\swarrow}$: Interpretació

$\overset{D}{\searrow}$ i $\overset{D}{\longrightarrow}$: Llegint

$\overset{G}{\swarrow}$ i $\overset{G}{\searrow}$: Gödelització

$$\mathbf{1} := \mathbf{s}(\mathbf{0}),\ \mathbf{2} := \mathbf{s}(\mathbf{s}(\mathbf{0})),\ \ldots,\ \mathbf{n} := \mathbf{s}\left(\overset{n)}{\cdots}\mathbf{s}\left(\left(\mathbf{s}(\mathbf{s}(\mathbf{0}))\right)\cdots\right)\right)$$

Els tres diccionaris

llenguatge formal

$\tau := \forall v_1 \forall v_2 \left(v_1 + v_2 \equiv v_2 + v_1 \right)$

$\sigma_1, \sigma_2, \ldots, \sigma_n, \varphi(\mathbf{f})$
$\sigma_1 2, \sigma_2, \ldots, \sigma_n \vdash_{\text{ar}} \varphi(\mathbf{f})$

$\vdash_{\text{ar}} \mathfrak{Dem}\left(\mathbf{m}, \mathbf{n} \right)$

llenguatge conjuntista

$\forall x \forall y \in \mathbb{N} \left(x + y = y + x \right)$

$q \in \mathbb{S}\text{ent} =$
$= \left\{ q = g\left(\mathfrak{Sent}(v) \right) \in \mathbb{N} \right\}$

$\models_{\mathbb{N}} \mathfrak{Sent}\left(v \right) [\![\mathbf{q}]\!],$

$< m, n > \in \mathbb{D}\text{em}$

$\models_{\mathbb{N}} \mathfrak{Dem}\left(u, v \right) [\![\mathbf{m}, \mathbf{n}]\!],$

$\mathfrak{G}(u) := \forall v \neg \mathfrak{Dem}(v, u)$
$\sigma_{\text{G}} := \forall v \neg \mathfrak{Dem}(v, \mathbf{g})$
$\mathfrak{Teor}(u) := \exists v \mathfrak{Dem}(v, u)$
$\mathfrak{Consist}(\mathcal{T}_{\text{ar}}) := \neg \mathfrak{Teor}(\mathbf{0} \neq \mathbf{0})$

$\nvdash_{\text{ar}} \sigma_{\text{G}}$ i $\nvdash_{\text{ar}} \neg \sigma_{\text{G}}$
$\vdash_{\text{ar}} \mathfrak{Consist}(\mathcal{T}_{\text{ar}}) \rightarrow \sigma_{\text{G}}$

llenguatge natural

τ és un $\mathcal{L}_{\text{ar}}$-sentència
$q = g\left(\mathfrak{Sent}(v) \right)$
τ és un $\mathcal{T}_{\text{ar}}$-teorema
$\sigma_1, \ldots, \sigma_n$ és una
$\mathcal{T}_{\text{ar}}$-demostració de $\varphi(\mathbf{f})$
$f = g\left(\varphi(v) \right)$
$m = g(\sigma_1, \ldots, \sigma_n)$
i $n = g\left(\varphi(\mathbf{f}) \right)$
$g = g\left(\mathfrak{G}(u) \right)$

2. LA RECURSIVITAT

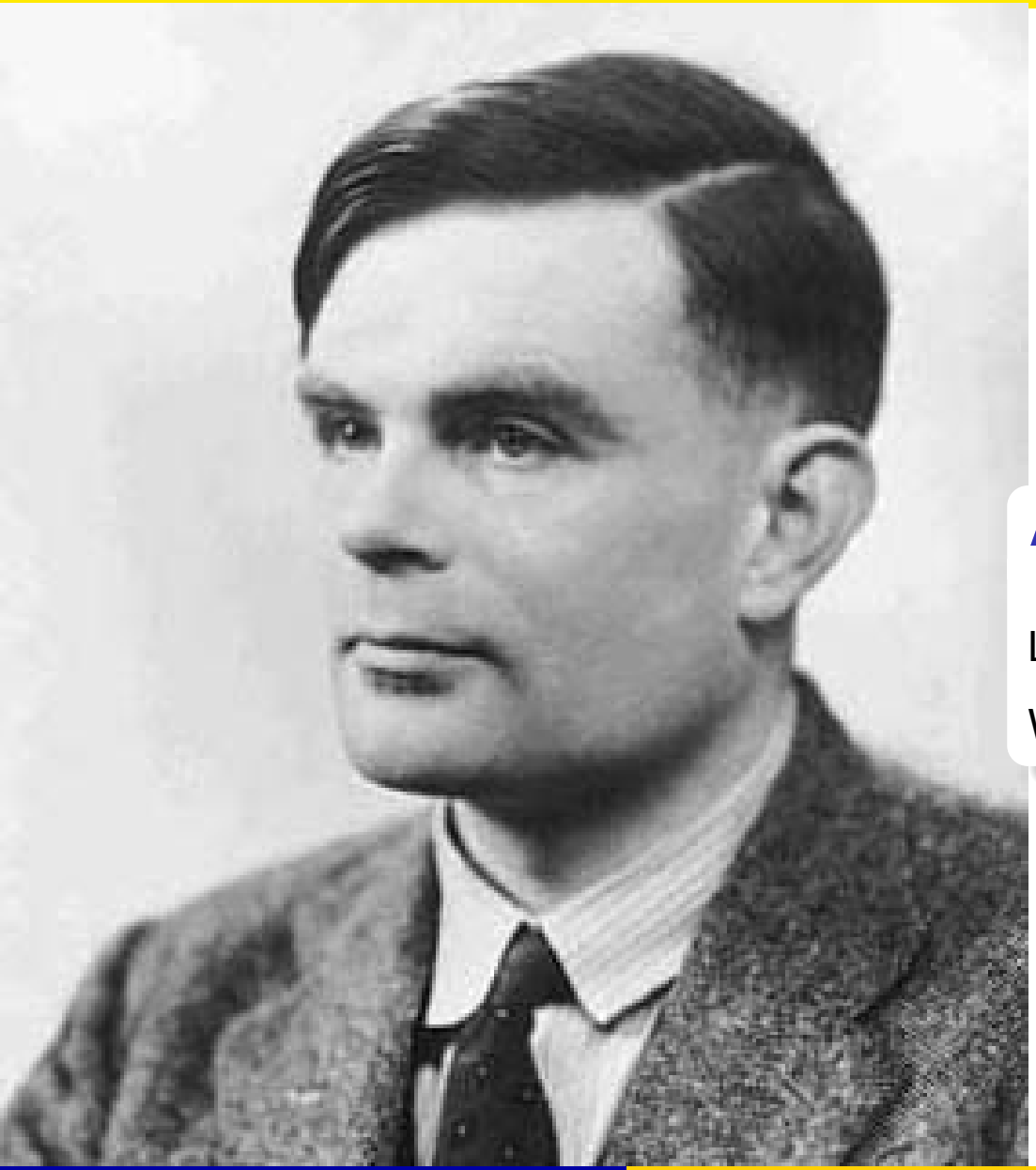
La recursivitat

El més complex dels diccionaris és el de la **representabilitat**.

Quins conjunts i funcions de l'univers dels nombres naturals poden ser «formalitzats» en el llenguatge $\mathcal{L}_{\text{ar}}$?

I Gödel els caracteritza i ho fa en l'univers conjuntista aritmètic.

Tot rau a definir les funcions [primitives] recursives i, de retruc, els conjunts recursius —que són uns subconjunts particulars del conjunt $\mathbb{N}$ dels nombres naturals. [És pura tècnica, però una tècnica genial!]



Alan Mathison Turing

Londres, (Anglaterra), 23 de juny de 1912.

Wilmslow, (Anglaterra), 14 de gener de 1978.

La recursivitat

L'any 1936 Alan Mathison Turing, i d'altres, demostrarien que les funcions **computables** coincideixen amb les recursives.

S'obre la porta als problemes de **decidibilitat** i, en particular, el que havia plantejat Hilbert en el problema 10 —relatiu a la resolubilitat de les equacions diofàntiques— i el que hem trobar a Hilbert-Ackermann —relatiu a la determinació dels teoremes.

Bibliografía

- Gödel, Kurt. «Über formal unentscheidbare Sätze der Principia Mathematica und verwandter System». *Monatshefte für Mathematik und Physik* (1931), 38, p 173-198. Traducción castellana de Jesús Mosterín: *Kurt Gödel. Obras completas*. Alianza Universidad. Madrid: 1981.
- Turing, Alan M. «On computable numbers, with an application to the Entscheidungs-problem». *Proceedings of the London Mathematical Society* (1937), 2ª serie, 42, p 230-265.
- Pla i Carrera, Josep *El Teorema de Gödel. Un análisis de la verdad matemática*. Real Sociedad Matemática Española. Ediciones Guijarro: Madrid, 2012.
- Roselló, Joan *From Foundations to Philosophy of Mathematics*. Cambridge Scholars Publishing: Cambridge, 2012.