Théorèmes, d'incomplétude de Gödel

Hugo Férée

25 octobre 2023

1 Contexte historique (rapide !)

Fin 18e, début du 19e siècle, de nombreux mathématiciens (Betrand Russell, Georg Cantor, Gottlob Frege, Kurt Gödel, David Hilbert) s'interrogent sur la formalisation du langage des (énoncés et des preuves) mathématiques, jusque là relativement informel : c'est le début de la **logique**. [1]

En particulier, Hilbert présente en 1900 23 problèmes ouverts, à résoudre au 20e siècle, entre autres :

2e problème : L'arithmétique est-elle cohérente ?

> **Note**
> Faux dans l'arithmétique : Gödel 1931, mais vrai avec récurrence transfinie, Gentzen 1936

10e problème : Existe-t-il un algorithme permettant de trouver une solution à une équation diphantienne.

> **Note**
> Premier problème : pas encore de définition formelle d'un algorithme. C'est une des motivations derrière les travaux de Turing ou Church par exemple.

> **Note**
> Matiiassevitch 1970 ! Indécidable, car r.e. <-> diophantien

Un des objectifs à l'époque, est de trouver une théorie permette d'exprimer les résultats existants, et qui soit *complète*. Tout énoncé est soit vrai soit faux, il suffit juste de trouver la bonne théorie qui n'énonce que des choses correctes, et qui permet de tout prouver (ou son contraire). Ça a donné plusieurs tentatives, notamment ZFC, précédée par une théorie des ensembles inconsistente (c.f. paradoxe de Russel).

1. La B.D. *Logicomix* résume de manière très accessible cette époque.

En 1931, Gödel présente ce qu'on appelle maintenant son *premier théorème d'incomplétude*, qui vient mettre fin à cette recherche (sauf pour quelques mathématiciens qui ont du mal à l'admettre).

2 Premier théorème d'incomplétude de Gödel

L'énoncé moderne, avec des hypothèses plus faibles et plus simples, est dû à Rosser quelques années plus tard.

2.1 Définitions

Définition 1 (Système formel/ théorie effective)**.** *C'est la donné d'un langage (les formules) et d'axiomes (et donc de preuves). Cela induit une notion de prouvabilité : une formule est prouvable (c'est un théorème) si elle a une preuve (finie).*

On dit que théorie est effective, si on peut décider l'application d'un axiome à une formule, et si l'ensemble des axiomes est récursivement énumérable.

En pratique, l'ensemble des théorèmes d'une théories effective est récursivement énumérable.

Exemple 1 (L'arithmétique de Péano)**.** *C'est l'arithmétique du premier ordre avec* $\{0, s, +, \cdot\}$*, et les axiomes définissant* s*,* $+$ *et* $\cdot$ *ainsi que la récurrence.*

Remarque 1. *La récurrence est en fait un schéma d'axiome : elle décrit un axiome pour chaque formule. L'arithmétique de Péano est donc récursivement axiomatisable, mais pas finiment axiomatisable (ou alors il faut passer au second ordre).*

Définition 2 (Consistence)**.** *Une théorie*[2] *est consistente s'il n'existe pas de formule* ϕ *telle que* ϕ *et* $\neg\phi$ *sont prouvables.*

Remarque 2. *Attention, prouvable* $\neq$ *vrai !*

Définition 3. *Correction Une théorie est correcte relativement à une classe de formules (et un modèle de vérité) si lorsqu'une formule dans cette classe est prouvable, alors elle est vraie (dans ce modèle).*

Par exemple, on dira qu'une théorie est Σ_1-correcte, si elle ne prouve que des énoncés Σ_1 qui sont aussi prouvables dans l'arithmétique de Péano.

Remarque 3. *En particulier, une théorie peut à la fois être cohérente et prouver des énoncés dont la négation est prouvable en arithmétique.*

Définition 4 (Complétude)**.** *Une théorie est complète si pour toute formule, elle permet de soit de la prouver, soit de prouver sa négation.*

Exemple 2. *l'arithmétique de Presburger (pour faire simple : Péano sans la multiplication) est une théorie effective, complète et correcte (relativement à l'arithmétique de Péano).*

2. qui peut définir la négation

2.2 Énoncé

Théorème 1. *Premier théorème d'incomplétude de Gödel (version Rosser) Toute théorie* ***effective, consistente*** *avec suffisamment d'arithmétique (Σ_1-correcte) est incomplète.*

2.3 Preuve originale (grandes lignes)

Gödel montre qu'il peut définir une formule qui exprime : "Cette formule n'est pas prouvable" (paradoxe du menteur). Idée : encoder les formules dans les entiers (« Gödel numbering », comme pour l'encodage des machines de Turing) [3]. On peut alors définir une formule (arithmétique) qui exprime qu'un entier encode une formule prouvable [4].

Cette formule est encodé par un nombre. On l'applique sur son propre nombre. [5]

Une théorie effective contenant suffisamment d'arithmétique permet d'énoncer cette formule. La complétude implique alors qu'on peut énumérer les preuves jusqu'à trouver une preuve de cette formule ou de sa négation. Si elle est prouvable, la correction (ω-soundness pour Gödel) implique que la formule est non prouvable, ce qui serai inconsistent. De même, si sa négation est prouvable ; contradiction.

2.4 Preuve via indécidabilité

Nous avons vu avec la hiérarchie arithmétique, qu'il existe des liens forts entre les énoncés mathématiques et la décidabilité des problèmes. En construisant sur ce que nous avons vu jusqu'ici, nous pouvons prouver plus simplement le premier théorème d'incomplétude de Gödel, avec des techniques connues. Ce type de preuve est dû à Kleene (1967) (revisitée ici par Scott Aaronson).

Lemme 1. *Toute fonction totale z satisfaisant la spécification suivante est incalculable :*
$z(< \mathcal{M} >, w) = 0$ *si* $\mathcal{M}(w) = 0$ *et* 1 *autrement.*

Preuve en exercice.

Soit $G(P, w)$ le programme qui énumère les preuves jusqu'à trouver une preuve de « $P(w) = 0$ » et retourne 1, ou de sa négation et retourne 0.

Ce programme s'arrête toujours puisque la théorie est complète. Hors, G implémente z, ce qui contredit le lemme.

3 Second théorème d'incomplétude de Gödel

Il existe aussi une preuve (laissée au lecteur curieux) du second théorème d'incomplétude utilisant la calculabilité. [6]. The Surprise Examination Paradox and the Second Incompleteness Theorem (Shira Kritchman and Ran Raz)

Cela dérive du théorème suivant.

3. un peu technique
4. très technique
5. Ça devrait vous rappeler quelque chose.
6. `http://www.ams.org/notices/201011/rtx101101454p.pdf`

Théorème 2 (théorème d'incomplétude de Chaintin)**.** *Si T est une théorie sur les entiers, correcte pour certaines affirmations sur la complexité de Kolmogorov (en particulier, "K(s) > b") ; alors il existe une constante L telle qu'aucune affirmation de la forme "K(s) > L" n'est prouvable (pour aucun s).*

Démonstration. C'est encore une fois le paradoxe de Berry (comme pour Busy-Beaver). Par l'absurde, on pourrait définir un programme qui énumère les preuves, jusqu'à trouver L plus grand que la taille de son programme et retourne le s correspondant. On aurait alors K(s) < L ; contradiction. □

Remarque 4 (Dûe à Scott Aaronson)**.** *On peut ajouter à une théorie consistente un axiome affirmant (pessimistement) qu'elle est inconsistente, et elle peut très bien rester consistente ! Au contraire, ajouter un axiome affirmant (de manière arrogante) qu'elle est consistente, la rend inconsistente.*[7]

7. C'est une leçon de vie