Autour de la logique

Marie-Line Chabanol, Chantal Menini, Géraud Sénizergues

Institut de Mathématiques de Bordeaux/LaRRI, Université de Bordeaux

La logique : une théorie métamathématique

Objectif initial : programme de Hilbert [1905-1928]
Objet d'étude : ce qu'on peut démontrer à partir de systèmes d'axiomes et de règles de raisonnements.
Principe : formaliser les preuves.

- Les preuves deviennent vérifiables par une machine (Coq...)
- Les preuves deviennent des objets d'étude mathématique sur lesquels on peut raisonner (Gödel, etc)

Un exemple : $0 + x = x$ pour x entier

Pour le prouver, on a besoin d'axiomes, qui vont dire quelles propriétés des objets on peut utiliser, et de règles de raisonnement.

Un exemple : $0+x=x$ pour x entier

0–	$\mathrm{PA} \vdash \forall x\ x+0=x$	$(\mathtt{A4}, \mathtt{ax})$
1–	$\mathrm{PA} \vdash 0+0=0$	$(0, \forall_{\mathtt{elim}})$
2–	$\mathrm{PA}, 0+x=x \vdash \forall y,z\ (y+S(z)=S(y+z))$	$(\mathtt{A5}, \mathtt{ax})$
3–	$\mathrm{PA}, 0+x=x \vdash 0+S(x)=S(0+x)$	$(2, \forall^2_{\mathtt{elim}})$
4–	$\mathrm{PA}, 0+x=x \vdash 0+x=x$	$(\mathtt{ax})$
5–	$\mathrm{EG} \vdash \forall y,z\ y=z \to S(y)=S(z)$	$(\mathtt{COMPF}, \mathtt{ax})$
6–	$\mathrm{EG} \vdash\ 0+x=x \to S(0+x)=S(x)$	$(5, \forall^2_{\mathtt{elim}})$
7–	$\mathrm{PA}, 0+x=x \vdash\ 0+x=x \to S(0+x)=S(x)$	$(6, \mathtt{aff})$
8–	$\mathrm{PA}, 0+x=x \vdash\ S(0+x)=S(x)$	$(4, 7, \to_{\mathtt{elim}})$
9–	$\mathrm{PA}, 0+x=x \vdash\ 0+S(x)=S(0+x) \wedge S(0+x)=S(x)$	$(3, 8, \wedge_{\mathtt{intro}})$
10–	$\mathrm{EG} \vdash\ \forall y,z,t\ (y=z \wedge z=t) \to y=t$	$(\mathtt{TRANS}, \mathtt{ax})$
11–	$\mathrm{PA}, 0+x=x \vdash\ \forall y,z,t\ (y=z \wedge z=t) \to y=t$	$(10, \mathtt{aff})$
12–	$\mathrm{PA}, 0+x=x \vdash\ (0+S(x)=S(0+x) \wedge S(0+x)=S(x)) \to 0+S(x)=S(x)$	$(11, \forall^2_{\mathtt{elim}})$
13–	$\mathrm{PA}, 0+x=x \vdash\ 0+S(x)=S(x)$	$(9, 12, \to_{\mathtt{elim}})$
14–	$\mathrm{PA} \vdash\ 0+x=x \to 0+S(x)=S(x)$	$(13, \to_{\mathtt{intro}})$
15–	$\mathrm{PA} \vdash\ \forall x\ (0+x=x \to 0+S(x)=S(x))$	$(14, \forall_{\mathtt{intro}})$
16–	$\mathrm{PA} \vdash\ 0+0=0 \wedge \forall x\ (0+x=x \to 0+S(x)=S(x))$	$(1, 15, \wedge_{\mathtt{intro}})$
17–	$\mathrm{PA} \vdash\ [0+0=0 \wedge \forall x\ (0+x=x \to 0+S(x)=S(x))] \to (\forall x\ 0+x=x)$	$(\mathrm{REC}_\Phi, \mathtt{ax})$
18–	$\mathrm{PA} \vdash\ \forall x\ 0+x=x$	$(16, 17, \to_{\mathtt{elim}})$

On peut raisonner sur les preuves formelles

Les formules et les preuves sont maintenant des mots et si on les représente par des entiers :
- l'ensemble des preuves est un ensemble calculable : on peut écrire un programme qui teste si un nombre est le code d'une preuve correcte.
- l'ensemble des théorèmes d'une théorie axiomatique T, est semi-calculable : on peut écrire un programme, qui détermine si un nombre est le code d'une formule prouvable.

Un exemple : $0 + x = x$ pour x entier

Et si on enlève l'axiome de récurrence ? Il existe un autre modèle pour lequel c'est faux.

$$\begin{aligned}
\mathcal{N} &=_{\text{déf.}} (\mathbb{N} \times \{\bullet\}) \cup (\mathbb{N} \times \{\circ\}) \text{ où } \bullet \neq \circ \\
0_{\mathcal{N}} &=_{\text{déf.}} \langle 0, \bullet \rangle \\
\mathrm{S}_{\mathcal{N}} \langle p, \alpha \rangle &=_{\text{déf.}} \langle \mathrm{S}p, \alpha \rangle \text{ où } \alpha \in \{\bullet, \circ\} \\
\langle p, \alpha \rangle +_{\mathcal{N}} \langle q, \beta \rangle &=_{\text{déf.}} \langle p + q, \alpha \rangle \text{ où } \alpha, \beta \in \{\bullet, \circ\} \\
\langle p, \alpha \rangle \times_{\mathcal{N}} \langle q, \beta \rangle &=_{\text{déf.}} \langle p \times q, \beta \rangle \text{ où } \alpha, \beta \in \{\bullet, \circ\}
\end{aligned}$$

$$\mathcal{N} \models \mathrm{P}'0 \text{ et } \mathcal{N} \not\models \forall x \; 0 + x = x$$

Théorèmes de complétude/incomplétude

A-t-on eu de la chance de trouver une preuve de $0 + x = x$?
Réponse 1 : ce n'est pas un coup de chance : dès lors que la propriété était vraie dans toute structure satisfaisant PA, la preuve devait exister.

Théorème (complétude, Gödel ~ 1930)

Si la formule Φ est vraie dans toutes les structures qui satisfont l'ensemble d'axiomes $\mathscr{A}$, alors il existe une preuve de Φ à partir des axiomes de $\mathscr{A}$.

Théorèmes de complétude/incomplétude

A-t-on eu de la chance de trouver une preuve de $0 + x = x$?
Réponse 2 : le problème de savoir, étant donnés un nombre fini d'axiomes et une formule Φ, si il existe une preuve de Φ à partir de ces axiomes, est semi-décidable :
Il existe un programme qui prend en entrée les axiomes et la formule Φ et :
- soit se termine en donnant une preuve de Φ
- soit se termine en donnant une preuve de $\neg\Phi$
- soit ne se termine pas !

On verra plus loin que cette difficulté est incontournable pour PA : il n'y a pas de programme qui détermine la prouvabilité d'une formule dans PA et qui s'arrête sur toute formule.
Donc on a eu de la chance : notre programme s'est arrêté.

Théorèmes de complétude/incomplétude

Est-ce qu'on peut déterminer tout ce qui est vrai dans une structure donnée ?
En général Non.

Théorème (Gödel, Church)

Il n'y a pas d'algorithme qui permette de savoir si une formule Φ , écrite sur les symboles de l'arithmétique $+, \times, =, 0, 1$, est vraie dans la structure $\langle \mathbb{N}, +, \times, 0, 1 \rangle$.

N.B. Il n'y pas de semi-algorithme non-plus sinon, en exécutant le semi-algorithme, en parallèle, sur les formules Φ et $\neg\Phi$, on s'arrêterait au bout d'un temps fini et on saurait si Φ est vraie ou $\neg\Phi$ est vraie.

Plus généralement : que peut-on attendre d'un système logique et d'un système d'axiomes ?

- qu'il ne prouve que du vrai ?
- qu'il prouve Tout ce qui est vrai ?
- qu'il nous donne un moyen effectif (un algorithme) pour savoir si un énoncé est vrai ? pour savoir si un énoncé est prouvable ?
- est-ce que la preuve de $\exists y \Phi(x, y)$ nous donne un moyen de calculer, pour chaque valeur de x, un objet y qui satisfait $\Phi(x, y)$?
- si on fixe une structure (les réels, les entiers, les mots , etc) est-ce que le vrai dans cette structure se laisse enfermer dans un ensemble fini (ou recursivement enumerable) d'axiomes ?
- est-ce que on a une méthode physiquement réalisable pour ce faire ?

Plus généralement : que peut-on attendre d'un système logique et d'un système d'axiomes ?

1- Qu'il ne prouve que du vrai ?
Oui, c'est ce que l'on croit.
Pour les systèmes logiques : on peut le prouver, en utilisant quelques axiomes et davantage que $\mathrm{P0}$.
Pour les systèmes d'axiomes : on prouve exactement ce qui est vrai dans toutes les structures qui vérifient les axiomes.

Plus généralement : que peut-on attendre d'un système logique et d'un système d'axiomes ?

Mais est-on sûr qu'il existe de telles structures ? ? autrement dit (via le théorème de complétude) est-on sûr que le système d'axiomes est cohérent ? i.e. qu'il ne permet pas de prouver la constante "faux"($\bot$) ? ?
On croit fermement que $P0$ est cohérent.
Pourrait-on prouver que PA est cohérent en n'utilisant que $P0$?
non, on ne peut même pas le prouver en utilisant PA lui-même.

Théorème (Gödel 1931)

On peut exprimer *par une formule C de l'arithmétique la cohérence de PA. i.e. PA est cohérente ssi C est vraie dans $\langle \mathbb{N}, +, \times, 0, 1 \rangle$. La formule C n'est pas prouvable dans PA.*

Plus généralement : que peut-on attendre d'un système logique et d'un système d'axiomes ?

2- qu'il prouve Tout ce qui est vrai ?
oui : c'est le théorème de complétude.

Plus généralement : que peut-on attendre d'un système logique et d'un système d'axiomes ?

3- qu'il nous donne un moyen effectif (un algorithme) pour savoir si un énoncé est vrai ? prouvable ? en général Non :

Théorème (Church)

Si T est une théorie qui contient les axiomes de $\mathrm{P0}$ et qui est cohérente, alors l'ensemble des théorèmes de T n'est pas récursif.

"récursif : calculable par un programme (qui s'arrête !)"
Exemples :
la théorie de la structure $\langle \mathbb{N}, +, \times, 0, 1 \rangle$ (par le théorème)
la théorie des conséquences de PA (par le théorème)
la théorie des conséquences de $\mathrm{Zermelo-Fraenkel}$ (par une variante du théorème)

Plus généralement : que peut-on attendre d'un système logique et d'un système d'axiomes ?

Théorème (Incomplétude, Gödel 1931)

Si T est la théorie des conséquences d'un ensemble récursif d'axiomes, si elle contient les axiomes de $\mathrm{P0}$ *et si elle est cohérente, alors T est incomplète.*

Découle du théorème de Church.

Plus généralement : que peut-on attendre d'un système logique et d'un système d'axiomes ?

3 (suite) - qu'il nous donne un moyen effectif (un algorithme) pour savoir si un énoncé est vrai dans une structure ? prouvable dans une axiomatique ?

Pour certaines structures ou ensembles d'axiomes : oui

la théorie de la structure $\langle \mathbb{R}, +, \times, 0, 1 \rangle$

la théorie de la structure $\langle \mathbb{Q}, \leq \rangle$

la théorie de la structure $\langle \mathbb{N}, +, 0, 1 \rangle$

la théorie de la structure $\langle \mathbb{N}, \times, 0, 1 \rangle$

la théorie des conséquences de EG

la théorie des conséquences des axiomes de corps algébriquement clos de caractéristique p

Plus généralement : que peut-on attendre d'un système logique et d'un système d'axiomes ?

4- est-ce que la preuve de $\exists y \Phi(x,y)$ nous donne un moyen de calculer, pour chaque valeur de x, un objet y qui satisfait $\Phi(x,y)$?
En général Non
si la preuve est intuitionniste (système LJ), et si les axiomes sont raisonnables : oui.

Théorème (Kleene)

Si $\exists y \Phi(x,y)$ est prouvable à partir de PA , en logique intuitionniste, alors il existe une fonction calculable $f : \mathbb{N} \to \mathbb{N}$ telle que, $\forall x \in \mathbb{N}, \Phi(x, f(x))$. Un algorithme calculant f peut être "extrait" de la preuve intuitionniste.

C'est le principe implémenté dans COQ : de toute preuve on peut extraire un programme.

Plus généralement : que peut-on attendre d'un système logique et d'un système d'axiomes ?

5- si on fixe une structure (les réels, les entiers, les mots , etc) est-ce que le vrai dans cette structure se laisse enfermer dans un ensemble fini (ou récursivement énumérable) d'axiomes ?
En général Non :
si T est l' ensemble des conséquences logiques d'un ensemble récursif d'axiomes et si T est complète, alors T est décidable. La réciproque est immédiate. Donc la théorie T d'une structure est récursivement axiomatisable ssi T est récursive. On a vu plus haut que :
la théorie de la structure $\langle \mathbb{N}, +, \times, 0, 1 \rangle$ est non-récursive.
On peut montrer que :
la théorie de la structure $\langle X^*, \cdot, \varepsilon \rangle$ est non-récursive.
la théorie de la structure $\langle F(X), \cdot, \varepsilon \rangle$ est récursive.

Plus généralement : que peut-on attendre d'un système logique et d'un système d'axiomes ?

6- est-ce qu'on a une méthode physiquement réalisable pour ce faire ?

1. la théorie de la structure $\langle \mathbb{N}, +, 0, 1 \rangle$ est récursive, temps double-exponentielle. Implémentations [Klaedtke, tactique ω de COQ, ...]
2. la théorie de la structure $\langle \mathbb{R}, +, \times 0, 1 \rangle$ est récursive, temps double-exponentielle. Implémentations.
3. la théorie de la structure $\langle \mathscr{P}(X^*), (succ_x)_{x \in X}, \varepsilon, \subseteq \rangle$ est récursive. Complexité non-élémentaire. Pas de programme.

Autour de la preuve du théorème d'incomplétude de [Gödel 1931]

Ingrédient essentiel de la preuve de Gödel : "Je mens".
Echauffement : Un exemple de preuve basée sur le paradoxe du menteur :
E et $\mathscr{P}(E)$ ne sont pas en bijection.
Soit $\varphi : E \to \mathscr{P}(E)$ une application.
La partie $P := \{x \in E \mid x \notin \varphi(x)\}$ ne peut pas être de la forme $\varphi(x_0)$.
Supposons que $P = \varphi(x_0)$. Si $x_0 \in P$ alors $x_0 \notin \varphi(x_0)$, donc $x_0 \notin P$.
Si $x_0 \notin P$ alors $x_0 \in \varphi(x_0)$, donc $x_0 \in P$.
On obtient une contradiction.
Donc $\forall x \in E, P \neq \varphi(x)$: φ n'est pas surjective.
qed.
Gödel traite les énoncés et les preuves (suite de formules) comme des objets mathématiques, dans lesquels on peut considérer un énoncé qui énonce sa propre non-prouvabilité.

Autour de la preuve du théorème d'incomplétude de [Gödel 1931]

Nous considérons dans tout ce qui suit une théorie axiomatique T, qui contient $P0$, qui a un ensemble récursif d'axiomes et qui admet $\mathbb{N}$ comme modèle (i.e. tous les théorèmes de T sont vrais dans $\mathbb{N}$).
Pour construire un énoncé de T qui est auto-référent on part de plus loin.
Pour toute fonction partielle $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ on construit une formule logique $\varphi_f(n, m, p)$ qui "exprime la fonction" au sens suivant :

$$\forall n, m, p \in \mathbb{N},\ f(n, m) = p \ \Leftrightarrow\ \mathbb{N} \models \varphi_f(\overline{n}, \overline{m}, \overline{p}) \qquad (1)$$

où $\overline{n}$ est le terme qui représente l'entier n ; par exemple $\overline{3}$ est le mot $S(S(S(0)))$.

Autour de la preuve du théorème d'incomplétude de [Gödel 1931]

La formule φ_f a une forme particulièrement simple : elle commence par une suite finie de quantifications de variables , puis ce qui suit n'a plus de quantificateur :

$$\varphi_f = Q_1 x_1 Q_2 x_2 \dots Q_q x_q \cdot \varphi'(x_1, \dots, x_q, n, m, p),$$

où $Q_i x_i$ est de la forme $\exists x_i$ ou $\forall x_i \leq x_j$ (avec $j < i$) C'est pourquoi, si la formule est vraie dans $\mathbb{N}$, alors elle est prouvable dans $P0$. On a donc l'équivalence :

$$\forall n, m, p \in \mathbb{N},\ f(n, m) = p \ \Leftrightarrow\ T \vdash \varphi_f(\overline{n}, \overline{m}, \overline{p}) \qquad (2)$$

Autour de la preuve du théorème d'incomplétude de [Gödel 1931]

On considère une bijection $n \mapsto \Psi_n$ de $\mathbb{N}$ vers l'ensemble des formules à une variable libre sur le langage de l'arithmétique (N.B. les formules sont des mots sur un alphabet fini, donc on peut aisément trouver une telle bijection qui soit simple à calculer, dans les deux directions) On définit la fonction $\mathrm{PROUV} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ par :

$$\mathrm{PROUV}(n, m) = 1 \text{ si } T \vdash \Psi_n(\overline{m}).$$

$$\mathrm{PROUV}(n, m) = \text{indéfini si } T \not\vdash \Psi_n(\overline{m}).$$

Cette fonction partielle est calculable : il existe un programme qui prend en entrée le couple d'entiers (n, m) et s'arrête ssi $T \vdash \Psi_n(\overline{m})$; dans ce cas il renvoie le résultat 1.

Autour de la preuve du théorème d'incomplétude de [Gödel 1931]

La fonction *PROUV*, qui est calculable, est représentée par une formule φ_P (voir (2)) :

$$\forall n, m, p \in \mathbb{N},\ PROUV(n, m) = 1 \ \Leftrightarrow\ T \vdash \varphi_P(\overline{n}, \overline{m}, \overline{1}). \qquad (3)$$

On considère la formule

$$\theta(n) := \neg\varphi_P(n, n, \overline{1}).$$

Cette formule a un numéro n_0 pour la bijection mentionnée plus haut :

$$\theta(n) = \psi_{n_0}(n).$$

On considère alors la formule

$$\psi_{n_0}(\overline{n_0}).$$

Cette formule énonce sa non-prouvabilité au sens que :

$$\mathbb{N} \models \psi_{n_0}(\overline{n_0}) \Leftrightarrow T \not\vdash \psi_{n_0}(\overline{n_0}).$$

Autour de la preuve du théorème d'incomplétude de [Gödel 1931]

En utilisant la définition de PROUV et l'équivalence (3), on montre alors que :

si $T \vdash \psi_{n_0}(\overline{n_0})$ alors $T \not\vdash \psi_{n_0}(\overline{n_0})$ ce qui est impossible ;
si $T \vdash \neg\psi_{n_0}(\overline{n_0})$ alors $T \vdash \psi_{n_0}(\overline{n_0})$, donc T est incohérente, alors qu'elle a pour modèle $\mathbb{N}$, ce qui est impossible.

On conclut que ni $\psi_{n_0}(\overline{n_0})$, ni $\neg\psi_{n_0}(\overline{n_0})$ ne sont démontrables dans T.

Références

Références, grand public

J.P. Belna : *Histoire de la logique*, editions Ellipses, 2014

Eric Charpentier : Textes *"Cercles vicieux et paradoxes logiques"*, et *"Théorèmes d'incomplétude"* à venir sur le site CultureMaths,

G. Dowek :*Les métamorphoses du calcul :une étonnante histoire de mathématiques*, et *La logique* Editions Le Pommier

Jean-Paul Delahaye : *La logique* Editions Belin

Références, public scientifique

Bertot-Casteran : *Interactive theorem proving and program development*,Springer,2004

van Dalen : *Logic and structures*, Springer, 1980

David-Nour-Raffalli :*Introduction à la logique*, Dunod, 2003

Freek Wiedijk : Formalizing 100 Theorems,
`http://www.cs.ru.nl/~freek/100/`