Fondements des mathématiques : Cantor et Gödel

Jean-Baptiste Campesato

6 janvier 2010

Cet article présente les débuts de la logique mathématique en se rattachant à l'histoire de la crise des fondements. La première partie présente le contexte historique et ne contient aucune information théorique. La seconde partie quant à elle présente les travaux de Cantor qui ont initié la théorie des ensembles, pour cela on a expliqué et démontré certains résultats fondamentaux de ce dernier de façon rigoureuse. Ensuite la troisième et dernière partie donne des démonstrations et des détails à propos des deux résultats de Gödel de 1931, ainsi que leurs conséquences en ce qui concerne les fondements des mathématiques.

1 Introduction - contexte historique

Depuis le IV^e siècle av. J.-C. et pendant plus de deux millénaires la logique, qui consiste en l'étude des règles régissant la déduction, a été considérée comme une branche propre à la philosophie et comme étant aboutie. On pensait en effet que la logique classique définie par Aristote selon les principes *d'identité*, *de non-contradiction* et *du tiers exclu* ne pouvait plus évoluer. Tout avait été dit. Cependant en 1847 George Boole publie son *Mathematical Analysis of Logic* qui marque le début de la logique étudiée d'un point de vue mathématique. Il munit la paire $\{0,1\}$ de deux lois de compositions internes + et . définies ainsi :

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

on peut vérifier qu'il définit une algèbre, que l'on nomme *algèbre de Boole* en son honneur.
En posant qu'une proposition vaut 0 dans l'algèbre de Boole si et seulement si elle est fausse, qu'elle vaut 1 si et seulement si elle est vraie et que l'on considère la loi . comme l'opérateur de conjonction (ou ET) et la loi + comme l'opérateur de disjonction (ou OU), Boole retrouve les lois de la logique classique : $x = x$ (l'identité), $x(1-x) = 0$ (la non-contradiction) et $x + (1-x) = 1$ (le tiers exclu).

$(1-x)$ définit la négation de x.

La même année Auguste De Morgan montre dans *Formal Logic or The Calculus of Inference* ses lois de dualité (que l'on nomme aujourd'hui *lois de De Morgan*) qui lient entre elles les négations de la conjonction et de la disjonction :
$(1-xy) = (1-x) + (1-y)$ et $(1-(x+y)) = (1-x)(1-y)$.
La logique symbolique était née. Cependant, ses détracteurs l'ont considérée comme limitée pour les raisons suivantes : tout comme pour la logique classique, elle part du principe que toute propriété est soit vraie, soit fausse, ce point de vue manichéen ne permet pas de décrire l'ensemble de notre monde et de plus elle est entièrement fondée sur le principe du tiers exclu. Elle va ensuite évoluer et gagner en rigueur (notamment avec l'apparition de définitions rigoureuses et de symboles) jusqu'à aboutir à de grands résultats dans les années trente. Ce sont ces résultats qui vont nous intéresser par la suite, le présent article ne développera donc pas cette évolution.
Notons de même que ce gain en rigueur va aussi donner naissance à un langage universel des mathématiques (ce qui comble une espérance de Gottfried Wilhelm Leibniz, voir sa lettre au Père Berthet de 1667 et son *Calculus Ratiocinator*).

Le XIX^e siècle est aussi marqué par une augmentation fulgurante du nombre de mathématiciens et de théories mathématiques. Le succès de la méthode axiomatique de la géométrie euclidienne (nous y reviendrons plus tard, notamment en ce qui concerne le 5^e postulat d'Euclide et les axiomes de Hilbert) qui remonte aux alentours de 300 ans av. J.-C. va se répandre et certains mathématiciens vont tenter de formaliser des théories mathématiques entières en definissant des axiomes (propriétés considérées comme vraies) dont découleront tous les autres théorèmes de la théorie par déduction logique (encore elle !). Notons cependant que la notion de système formel n'a été rigoureusement définie qu'au XX^e siècle notamment grâce aux travaux d'Alan Mathison Turing, nous y reviendrons plus tard.
On peut illustrer cet attrait pour le formalisme avec la définition axiomatique de l'ensemble des entiers naturels par Richard Julius Wilhelm Dedekind (il fut le dernier étudiant dont la thèse fut supervisée par Carl Friedrich Gauss) qui précède celle de Giuseppe Peano

Notons qu'il existe des théories alternatives à ZF(C) pour axiomatiser la théorie des ensembles, par exemple la *théorie des classes* (aussi nommée *Théorie des ensembles de von Neumann–Bernays–Gödel*).

en 1889 dans son *Arithmetices principia, nova methodo exposita* ou encore la construction axiomatique de la *théorie des ensembles* (voir ci-dessous) par Ernst Friedrich Ferdinand Zermelo en 1908 puis complétée dans les années vingt par Abraham Adolf Halevi Fraenkel et Thoralf Albert Skolem (on parle de la théorie *ZF* ou *ZFC* si on ajoute l'axiome du choix de Zermelo).

Pour finir de placer le contexte, un petit mot sur la *théorie des ensembles* sus-citée. Il s'agit d'une théorie de Georg Ferdinand Cantor introduite dans le *journal de Crelle* en 1874 et dont il fournit une introduction en six articles entre 1879 et 1884 dans l'*Acta Mathematica*. Il fournit ensuite un article en 1891 qui utilise son *argument diagonal* (nous y reviendrons et aurons de nombreuses occasions de l'utiliser dans cet article). Puis il réalise ses dernières contributions significatives en 1895 et 1897 avec un article en deux parties publié dans les *Mathematische Annalen* où il réexamine sa théorie.

Notons que Dedekind avait déjà commencé à formaliser la notion d'ensemble en mettant en avant la structure totalement ordonnée de l'ensemble des rationnels (1871) puis en construisant l'ensemble des irrationnels grâce à des coupures dans l'ensemble des rationnels (entre autres, voir une bi(bli)ographie).

Il s'agit d'une théorie visant à construire rigoureusement les objets mathématiques usuels (et jusqu'alors définis de façon intuitive) à partir de la notion d'ensemble (définie par Cantor) et d'appartenance en utilisant la logique : le principe du tiers exclu.
Cantor définit un ensemble comme *une multiplicité qui compte pour un* (Une définition très vague, il faut bien le reconnaitre... Pour information, cette traduction de la définition de Cantor, qui me plait beaucoup, est tirée du roman de Denis Guedj Villa des hommes).
Il s'intéresse notamment aux relations biunivoques (ou *bijections*) entre les ensembles et aux ensembles contenant une infinité d'éléments.
L'article initial de 1874 (*Ueber eine Eigenschaft des Inbegriffs aller reellen algebraischen Zahlen* dans le journal de Crelle, traduction disponible dans Acta Mathematica Volume 2, Number 1 / décembre 1883) met en place des résultats majeurs comme le fait que l'ensemble des nombres algébriques (racines d'un polynôme à coefficients entiers ; ou rationnels, cela revient au même en multipliant par le ppcm des dénominateurs) est dénombrable et que l'ensemble des réels ne l'est pas. Ceci amène deux résultats surprenants : d'abord il met en évidence qu'il y a « plusieurs infinis » (en effet l'ensemble des entiers est infini, l'ensemble des réels aussi, et pourtant on ne peut les mettre en bijection, il montre donc qu'« il y a plus » de réels que d'entiers) et aussi qu'« il y a plus » de nombres transcendants (c'est-à-dire non algébriques) que de nombres algébriques (et même qu'« il y en a autant » que de nombres réels), or on en connait très peu car la transcendance d'un nombre est souvent difficile à démontrer. L'article de 1891 (*Über eine elementare Frage der Mannigfaltigkeitslehre*) présente quant à lui une démonstration simple du fait que l'ensemble des réels n'est pas dénombrable en utilisant ce que l'on nomme maintenant l'*argument diagonal*, grâce auquel il démontre dans ce même article le *théorème de Cantor* (*Pour tout ensemble E, il n'y a pas de surjection de E sur l'ensemble des parties de E*) ce qui signifie qu'il y a une infinité d'ensembles infinis. Cantor va alors développer la notion de cardinalité et d'ordinalité pour quantifier le nombre d'éléments d'un ensemble et les munir d'une arithmétique, il montre alors que les *nombres transfinis* (on parle de *nombres ordinaux* désormais) forment une extension des entiers : on peut les munir d'une addition et d'une multiplication, on peut les comparer...

On dit qu'un ensemble est dénombrable si est seulement s'il existe une relation bi-univoque (ou bijection) entre cet ensemble et l'ensemble des entiers naturels.

Durant le reste de sa vie, Cantor tente de démontrer l'*hypothèse du continu* (dont il aurait aimé disposer d'une démonstration pour l'article de 1897) : il n'y a pas d'ensemble de cardinal strictement plus grand que celui des entiers et strictement plus petit que celui des réels. Nous nous intéresserons à l'hypothèse du continu dans la suite de l'article.
La théorie des ensembles a été très contreversée, d'abord pour une raison philosophique, l'existence de plusieurs infinis ne pouvait être acceptée par de nombreux mathématiciens encore très croyants et pour qui l'infini reflète dieu et doit donc être unique. Ensuite parce qu'elle va engendrer plusieurs paradoxes qui vont ébranler la logique aristotélicienne (le principe du tiers exclu) qui, comme on l'a vu au début de l'introduction, était considérée comme aboutie, parfaite... Nous y reviendrons.

À l'aube du XX^{e} siècle on peut donc distinguer trois grands mouvements mathématiques :

- Le *logicisme* soutenu par Dedekind, Cantor, Peano, Frege, Russell et Whitehead (dont nous avons cité ou citerons des travaux dans cet article). Reposant sur la logique et donc le principe du tiers exclu.
- Le *constructivisme* (ou *intuitionnisme*) où les démonstrations d'existences abstraites ne suffisent pas. Tous les objets étudiés doivent pouvoir être exhibés, l'axiome du choix y est donc proscrit. De même le principe du tiers exclu est remis en cause (Brouwer). Un exemple de théorie relativement récente due à ce mouvement est l'*analyse non standard*

de Robinson et Apery.
- Le *formalisme* qui consiste en une réunification de la multitude des champs mathématiques developpés surtout depuis le XIX^{e} siècle grâce à un système axiomatique fondamental et rigoureux valable pour toute « la » mathématique et capable d'évincer tous les paradoxes et toutes les incertitudes de la théorie des ensembles. Hilbert était un fervent partisan de ce mouvement et a placé ses espoirs dans la toute récente théorie des ensembles de Cantor. Il a ainsi affirmé que « Nul ne doit nous exclure du Paradis que Cantor a créé ». Cependant les travaux de Russel et de Gödel (théorèmes d'incomplétudes, 1931, ce sera l'aboutissement de notre article) ont démontré l'impossibilité de ce but.

Maintenant que le contexte est en place et que les grands points traités dans l'article ont été présentés (souvent par une petite note), nous allons commencer par étudier les résultats marquants de la théorie des ensembles pour ensuite présenter la notion de théorie axiomatique en logique mathématique pour aboutir aux grands résultats du XX^{e} siècle concernant le programme de Hilbert.

2 La théorie des ensembles

2.1 Les grandes démonstrations de Cantor

Les démonstrations seront données en respectant le plus possible la méthode proposée par leurs auteurs (en utilisant cependant des notations modernes pour en faciliter la compréhension).

2.1.1 L'ensemble des nombres algébriques est dénombrable

On rappelle qu'un nombre est dit *algébrique* s'il est racine d'un polynôme à coefficients entiers.

Théorème 1

L'ensemble des nombres algébriques est dénombrable.
(La formulation d'origine est que l'on peut faire correspondre l'ensemble des nombres algébriques à l'ensemble des entiers naturels. Elle ne précise cependant pas qu'il y a injection, i.e. qu'il n'y a pas de redondance, dans l'énumération des nombres algébriques obtenue, ce que l'obtient ici en plus en remarquant que tous les entiers naturels sont algébriques).

Démonstration de l'article de 1874 :

Un nombre algébrique est une solution d'une équation de la forme
$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0$ où $n \in \mathbb{N}^*$ et où $a_0, \ldots, a_n \in \mathbb{Z}$.
Sans perdre en généralité, on peut supposer que les coefficients $a_0, \ldots, a_n$ n'ont pas de diviseurs commun et que $a_0 > 0$.
On nomme hauteur de cette équation $N = a_0 + |a_1| + \ldots + |a_n| + n - 1 \in \mathbb{N}$.
Et étant donné un certain entier positif N, il existe un nombre fini d'équations de la forme ci-dessus de hauteur N (en effet on a forcément $n \leq N$ et pour chacun des n possibles $a_0 \geq 1$ et $a_1, \ldots, a_n \geq 0$).
Puis on sait que chaque équation admet au plus n solutions.
On peut donc énumérer tous les nombres algébriques résultant d'une équation de hauteur 1, puis de hauteur 2 et ainsi de suite. Comme chaque nombre algébrique résulte d'une équation de la forme ci-dessus, on les a tous énumérés.
En supprimant les redondances, et comme on sait qu'au moins chaque entier est algébrique, alors on obtient une suite de tous les nombres algébriques de la forme $(\omega_i)_{i\in\mathbb{N}}$ tel que $i \neq j \Rightarrow \omega_i \neq \omega_j$.

■

En utilisant les résultats ultérieurs de Cantor (et donc nos théories modernes), on montrerait que pour un N fixé, il y a un nombre fini d'équations de hauteur N, et que chaque équation admet un nombre fini de solutions. L'ensemble des nombres algébriques est ainsi une réunion dénombrable de parties réelles finies qui est donc au plus dénombrable, et comme chaque entier naturel est un nombre algébrique, cette réunion est bien dénombrable.

2.1.2 $\mathbb{R}$ n'est pas dénombrable

Théorème 2

L'ensemble des réels n'est pas dénombrable.
(La formulation d'origine de l'article de 1874 est que lorsque l'on a une suite de nombres réels deux à deux distincts $(u_n)_{n\in\mathbb{N}}$ et un intervalle I non vide et non restreint à un point, on peut toujours déterminer un élément η de I n'étant pas un terme de la suite. Ceci met en évidence le fait qu'il n'existe pas de surjection de $\mathbb{N}$ sur un intervalle I quelconque de $\mathbb{R}$ et donc de $\mathbb{N}$ à $\mathbb{R}$ car $I \subset \mathbb{R}$. On montre donc que $\mathbb{R}$ **est strictement plus grand que** $\mathbb{N}$ au sens de la cardinalité.)

Démonstration de l'article de 1874 :

On considère une suite de nombres réels deux à deux distincts $(u_n)_{n\in\mathbb{N}}$ et un intervalle I non vide et non restreint à un point.
On note α_0 et β_0 les bornes (éventuellement infinies, ouvertes ou fermées...) de I, avec $\alpha_0 < \beta_0$. Ensuite, on va construire les suites (finies ou non) (α_i) et (β_i) en réitérant le procédé suivant autant de fois que possible : on prend les deux premiers termes de notre suite u_k et u_l appartenant à $]\alpha_i, \beta_i[$ tels que $u_k \neq u_l$, on pose alors $\alpha_{i+1} = \min(u_k, u_l)$ et $\beta_{i+1} = \max(u_k, u_l)$.
Deux cas se présentent alors à nous :
• Soit le nombre d'intervalles $(]\alpha_i, \beta_i[)_i$ que l'on a construits est fini et s'arrête au rang n, alors il suffit de prendre un η dans $]\alpha_n, \beta_n[$.
• Soit le nombre d'intervalles est infini, alors la suite $(\alpha_i)_{i\in\mathbb{N}}$ est croissante, mais comme elle est majorée (par construction) elle est convergente, de même la suite (β_i) est décroissante et minorée, donc elle converge aussi. On note α et β leurs limites respectives. Si jamais $\alpha = \beta$ alors on pose $\eta = \alpha = \beta$ qui ne peut pas être un terme de la suite par construction, sinon si $\alpha < \beta$, il suffit de la même façon de prendre η dans $]\alpha; \beta[$.

On reconnait le théorème des segments emboîtés.

■

Démonstration de l'article de 1891 (première apparition de l'*argument diagonal*) :

La démonstration ci-dessous est présentée de façon plus moderne que dans l'article de Cantor, où il démontre en fait la non-dénombrabilité des suites binaires (à termes dans une paire d'éléments. Voir l'existence, sans unicité comme pour les développements décimaux, des développements binaires des réels), cependant cette méthode se généralise à des suites à termes dans un ensemble fini ou infini quelconque, ici dans $[\![0, 9]\!]$ (cf. [EWA2] p920).
Nous allons montrer qu'il n'y a pas de surjection de $\mathbb{N}$ sur $]0, 1[$, on pourra donc en déduire qu'il n'y a pas de surjection (et donc de bijection) de $\mathbb{N}$ sur $\mathbb{R}$.
On admet que tout réel a un unique développement décimal propre (c'est-à-dire qui ne se termine pas par une infinité de 9), donc tout réel x de $]0, 1[$ peut s'écrire sous la forme $x = 0, x_1x_2x_3\ldots$ (avec les x_i dans $[\![0, 9]\!]$ et tel qu'il n'existe pas de $N \in \mathbb{N}$ de sorte à ce que $n \geq N \Rightarrow x_n = 9$).
Supposons alors que l'on puisse énumérer les éléments de $]0, 1[$, c'est-à-dire écrire $]0, 1[= \{x_1, x_2, \ldots, x_i, \ldots\}$ avec i décrivant $\mathbb{N}$, on obtient alors :
$x_1 = 0, x_{1_1}x_{1_2}x_{1_3}x_{1_4}x_{1_5}\ldots$
$x_2 = 0, x_{2_1}x_{2_2}x_{2_3}x_{2_4}x_{2_5}\ldots$
$x_3 = 0, x_{3_1}x_{3_2}x_{3_3}x_{3_4}x_{3_5}\ldots$
$x_i = 0, x_{i_1}x_{i_2}x_{i_3}x_{i_4}x_{i_5}\ldots$

On note $[\![a, b]\!]$ l'ensemble des entiers de a à b.

Posons alors $\varphi : \begin{array}{ccc} [\![0,9]\!] & \longrightarrow & \{0,1\} \\ n & \longmapsto & \begin{cases} 0 \text{ si } n \neq 0 \\ 1 \text{ si } n = 0 \end{cases} \end{array}$ et considérons :
$y = 0, \varphi(x_{1_1})\varphi(x_{2_2})\varphi(x_{3_3})\varphi(x_{4_4})\varphi(x_{5_5})\dots$ (on remarque que l'on prend les termes diagonaux du tableau ci-dessus).
On a $y \in]0,1[$ mais pour tout $i \in \mathbb{N}$, $y \neq x_i$ car $y_i \neq x_{i_i}$.
Ce qui est contradictoire avec le fait que $]0,1[= \{x_1, x_2, \dots, x_i, \dots\}$.
Il est donc impossible de construire une surjection de $\mathbb{N}$ sur $\mathbb{R}$.

■

Notons qu'il existe aussi une démonstration de la non-dénombrabilité de $\mathbb{R}$ utilisant ce que l'on nomme *l'ensemble triadique de Cantor*.

Dans l'article de 1874 Cantor remarque qu'il retrouve grâce aux deux résultats précédents un théorème démontré par Liouville en 1851 (à savoir l'existence de nombres transcendants, c'est-à-dire non algébriques). En effet en remarquant que les nombres algébriques et que les nombres transcendants forment une partition de $\mathbb{R}$, le premier théorème permet de mettre en avant le fait que tout intervalle I non vide et non réduit à un point contient une infinité de nombres transcendants. De plus le second théorème explique pourquoi, on ne peut pas faire correspondre l'ensemble des nombres transcendants compris dans I à l'ensemble des entiers naturels, en effet, il précise qu'il n'y a pas de surjection de l'ensemble des entiers sur l'ensemble des transcendants et donc qu'il n'y a pas de bijection.

2.1.3 Un petit mot sur l'*argument diagonal* (ou *procédé diagonal*)

À la fin de l'article de 1891 Cantor précise que l'argument qu'il a utilisé est vraiment plus simple que la démonstration de 1874 mais aussi qu'il se généralise et permet de démontrer ce que l'on nomme aujourd'hui le *théorème de Cantor* (voir ci-dessous).
Par la suite l'*argument diagonal*, qui a déjà permis de démontrer la non-dénombrabilité de $\mathbb{R}$ et le théorème de Cantor, permettra encore de démontrer d'autres propriétés, dont certaines que nous allons voir ici (l'exemple à la fin de cette partie, le *paradoxe de Russel*, le *paradoxe de Richard* ou encore dans le *théorème d'incomplétude de* Gödel).

On peut considérer que l'argument consiste à étudier une fonction f définie sur le carré cartésien d'un ensemble et à s'intéresser plus particulièrement à la diagonale $f(x,x)$. Par exemple dans le cas de la non-dénombrabilité de $\mathbb{R}$ ci-dessus, on pose $f : \mathbb{N}^2 \mapsto [\![0;9]\!]$ qui à (m,n) associe la $m$ème décimale de x_n et on regarde $f(n,n)$. Dans l'exemple suivant de même, on travaille avec $f : I^2 \mapsto \{0;1\}$ qui à (m,n) associe $\left(\tilde{\Psi}^{-1}(m)\right)(n)$.
On pourra aussi s'intéresser à la formalisation de Jean-Yves Girard qui ramène l'argument diagonal à la recherche d'un point fixe, cf. [GIR] et [GBR].
Il faut noter que bien que dans ce document l'argument diagonal est souvent utilisé avec un raisonnement par l'absurde, il peut aussi être utilisé de façon « positive » dans le but de donner une démonstration constructiviste (par exemple le *théorème de Tychonov* et certains théorèmes qui découlent de ce dernier mais dont on peut se passer de certains aspects « difficiles » comme le *théorème d'Ascoli* et le *théorème de Banach-Alaoglu-Bourbaki* mais aussi dans des exemples plus accessibles comme dans ce document avec le *lemme diagonal* ou encore pour montrer qu'une partie d'un espace métrique précompacte et complète est compacte...).

Voici un exemple d'application de l'argument diagonal :

$\{0;1\}^I$ est l'ensemble des applications de I dans $\{0;1\}$.

Théorème 3

Soit I un ensemble non vide alors il n'y pas d'injection de $\{0;1\}^I$ dans I.

Démonstration :

Supposons par l'absurde l'existence d'une application injective $\Psi : \{0;1\}^I \to I$.
Nous pouvons restreindre l'ensemble d'arrivée de Ψ à son image pour obtenir une surjection et donc une bijection. Notons $\tilde{\Psi} : \{0;1\}^I \to \mathrm{Im}\Psi$ cette nouvelle application.

Soit $\varphi \in \{0;1\}^I$ défini ainsi :
$\forall i \in I,\ \varphi(i) = \begin{cases} 1 & \text{si } i \in \mathrm{Im}\Psi \text{ et } \left(\tilde{\Psi}^{-1}(i)\right)(i) = 0 \\ 0 & \text{sinon} \end{cases}$
Puis posons $m = \Psi(\varphi) \in I$, on a alors que $m \in \mathrm{Im}\Psi$ et que $\tilde{\Psi}^{-1}(m) = \varphi$ (d'après la bijectivité de $\tilde{\Psi}$).
Deux cas se présentent :
- Si $\varphi(m) = 1$ alors, par définition de φ, on a $\left(\tilde{\Psi}^{-1}(m)\right)(m) = 0$ et, par définition de m, on a $\left(\tilde{\Psi}^{-1}(m)\right)(m) = \varphi(m) = 1$. D'où une première contradiction.
- Si $\varphi(m) = 0$, comme $m \in \mathrm{Im}\Psi$, on a, par définition de φ, que $\left(\tilde{\Psi}^{-1}(m)\right)(m) = 1$ or $\left(\tilde{\Psi}^{-1}(m)\right)(m) = \varphi(m) = 0$. D'où une seconde contradiction.

Il ne peut donc y avoir d'injection de $\{0;1\}^I$ dans I.

■

On retrouve en fait le théorème de Cantor. En effet on montre que $2^{\mathrm{card}I} > \mathrm{card}I$ or $\mathrm{card}\mathfrak{P}(I) = 2^{\mathrm{card}I}$, d'où $\mathrm{card}\mathfrak{P}(I) > \mathrm{card}I$.
Ce théorème permet aussi de démontrer la non-dénombrabilité de $\mathbb{R}$ en considérant le développement binaire des réels (comme pour les développements décimaux, il faut faire attention au fait que chaque réel non nul admet deux développements binaires, voir la remarque dans la démonstration de 1891). On aura bientôt autant de démonstrations de la non-dénombrabilité de $\mathbb{R}$ que du théorème de Pythagore...

2.1.4 Le *théorème de Cantor* et ses conséquences

Une généralisation de l'argument que Cantor a utilisé dans son article de 1891 lui permet de démontrer le théorème suivant dans ce même article :

$\mathfrak{P}(E)$ est l'ensemble des parties de E.
Du fait que si E est un ensemble de cardinal fini alors $\mathrm{card}\mathfrak{P}(E) = 2^{\mathrm{card}E}$, ce qui se généralise en utilisant les fonctions caractéristiques à $\{0,1\}^E$ en bijection avec $\mathfrak{P}(E)$, on note aussi $\mathfrak{P}(E) = 2^E$.

Théorème 4: dit de Cantor

Soit E un ensemble quelconque,
alors il n'existe pas de surjection (et donc de bijection) de E sur $\mathfrak{P}(E)$.

Démonstration :

De même, que pour la première démonstration de 1891, on donne une démonstration plus moderne mais suivant le même principe que la méthode de Cantor.
Supposons par l'absurde l'existence d'une fonction f surjective de E dans $\mathfrak{P}(E)$ et considérons $\mathcal{D} = \{x \in E,\ x \notin f(x)\} \in \mathfrak{P}(E)$.
Comme f est surjective, il existe $y \in E$ tel que $f(y) = \mathcal{D}$ et alors deux cas s'offrent à nous :
- $y \in \mathcal{D}$: alors par définition de $\mathcal{D}$, $y \notin f(y) = \mathcal{D}$, contradiction.
- $y \notin \mathcal{D}$: alors cette fois $y \in f(y) = \mathcal{D}$, encore en contradiction.

Donc il ne peut exister de surjection de E sur $\mathfrak{P}(E)$.

On a obtenu : $y \in \mathcal{D} \Leftrightarrow y \notin \mathcal{D}$.

■

On déduit de ce résultat qu'il n'existe pas de plus grand cardinal, il y a donc « une infinité d'infinis » : si on se donne un ensemble E de cardinal infini alors $\mathfrak{P}(E)$ sera strictement plus grand (au sens de la cardinalité), de même $\mathfrak{P}(\mathfrak{P}(E))$ sera strictement plus grand que $\mathfrak{P}(E)$ puis $\mathfrak{P}(\mathfrak{P}(\mathfrak{P}(E)))$ que $\mathfrak{P}(\mathfrak{P}(E))$ et ainsi de suite.

On peut montrer, en acceptant l'axiome du choix (et forcément l'axiome de l'infini, c'est-à-dire que $\mathbb{N}$ est un ensemble), que $\mathbb{N}$ est le plus petit ensemble de cardinal infini (les cardinaux finis étant les entiers naturels). Une preuve est disponible à la proposition 3.49 de [GOS].
Cantor pensait qu'il n'existait pas d'ensemble de cardinal infini à la fois strictement plus grand que celui de $\mathbb{N}$ et strictement plus petit que celui de $\mathbb{R}$: l'*hypothèse du continu*. Il n'a jamais réussi à le démontrer et ce fut le premier des 23 problèmes qu'Hilbert présenta au congrès international de mathématiques de 1900 à Paris. Nous y reviendrons dans la partie 3.
On peut exhiber une bijection entre $\mathbb{R}$ et $\mathfrak{P}(\mathbb{N})$, l'hypothèse du continu revient donc à montrer qu'il n'existe pas d'ensemble de cardinal infini à la fois strictement plus grand que celui de $\mathbb{N}$

et strictement plus petit que celui de $\mathfrak{P}(\mathbb{N})$.
Il existe ainsi une hypothèse du continu généralisée : Soit E un ensemble de cardinal infini, alors il n'existe pas d'ensemble de cardinal strictement plus grand que celui de E et strictement plus petit que celui de $\mathfrak{P}(E)$.

$\mathbb{R}$ et $\mathfrak{P}(\mathbb{N})$ sont en bijection :

On considère les développements binaires et ternaires des réels :

$$\text{Soient } f : \begin{array}{ccc} \mathfrak{P}(\mathbb{N}) & \longrightarrow & \mathbb{R} \\ E & \longmapsto & \displaystyle\sum_{n\in E} \frac{1}{2^{n+1}} \end{array} \quad \text{et } g : \begin{array}{ccc} \mathfrak{P}(\mathbb{N}) & \longrightarrow & \mathbb{R} \\ E & \longmapsto & \displaystyle\sum_{n\in E} \frac{1}{3^{n+1}} \end{array}$$

(pour g on peut remplacer 3 par tout entier strictement plus grand que 2).
Alors on peut montrer que f est surjective et que g est injective.
Donc $\mathbb{R}$ et $\mathfrak{P}(\mathbb{N})$ sont en bijection.
En effet on peut montrer, avec l'axiome du choix, que pour deux ensembles A et B, il existe une injection de A dans B si et seulement s'il existe une surjection de B dans A.
Ensuite on utilise le théorème de *Cantor-Schröder-Bernstein* (démontré d'abord en utilisant, implicitement, l'axiome du choix par Cantor puis sans par Schröder et Bernstein).

■

TODO : améliorer... possible sans l'axiome du choix ?

On obtient ainsi encore une autre démonstration de la non-dénombrabilité de $\mathbb{R}$, en effet $\mathbb{R}$ est en bijection avec $\mathfrak{P}(\mathbb{N})$ qui n'est pas en bijection avec $\mathbb{N}$ d'après le théorème de Cantor.

2.2 Les premiers revers

Il convient d'abord de préciser que l'on peut définir un ensemble de deux façons différentes, soit en exhibant tous ses éléments (par exemple $\{1;6;9;45;\mathbb{R};i\}$), soit en le définissant grâce à une condition (par exemple $\{x,\ x \text{ est un entier pair}\}$) via l'*axiome de séparation* (ou *axiome de compréhension* ou *Aussonderungsaxiom*).
C'est ce second cas qui va nous intéresser ici.

Le premier paradoxe nécessite l'introduction de la notion d'ordinal (et donc de bon ordre), nous le donnons ici sans plus de précision.
Paradoxe de Burali-Forti (1897) :

Si « l'ensemble de tous les ordinaux » existe, alors son nombre ordinal serait strictement supérieur à chaque ordinal qui le compose, et donc à lui-même, ce qui est contradictoire.

■

On va s'intéresser plus longuement au *paradoxe de Russel*, basé sur un *argument diagonal* (encore... je vous avais prévenu). D'ailleurs Russel reconnait avoir trouvé ce paradoxe suite à l'étude du *théorème de Cantor*.
L'avantage de ce paradoxe est qu'il ne nécessite pas l'introduction de notions particulières (bon ordre...) et qu'il est simple à comprendre.
Russel a découvert ce paradoxe en 1901 et l'a publié en 1903. Ce paradoxe avait déjà été trouvé par Ernst Zermelo sans que ce dernier ne le publie.
Paradoxe de Russel (1901) :

Considérons l'ensemble défini ainsi : $\mathcal{E} = \{x,\ x \notin x\}$.
Deux cas se présentent alors :
• Soit $\mathcal{E} \in \mathcal{E}$, mais alors par définition de $\mathcal{E}$, $\mathcal{E} \notin \mathcal{E}$, ce qui est contradictoire avec l'hypothèse.
• Soit $\mathcal{E} \notin \mathcal{E}$, mais alors cette fois, $\mathcal{E} \in \mathcal{E}$, ce qui est toujours impossible.
D'où une contradiction : $\mathcal{E} \in \mathcal{E} \Rightarrow \mathcal{E} \notin \mathcal{E}$.

■

Ce paradoxe met en évidence le fait qu'il existe des conditions (comme ici $x \notin x$) ne permettant pas de construire un ensemble, on parle de *conditions non-collectivisantes*. *A contrario*,

les conditions permettant de définir un ensemble sont nommées *conditions collectivisantes*.
Notons qu'une variante de ce paradoxe permet de montrer que l'ensemble de tous les ensembles n'existe pas.

Attention : je suis en train de revoir entièrement cette partie qui ne me donne pas entière satisfaction...

3 Logique mathématique : Gödel

3.1 Introduction et *programme de Hilbert*

La majorité des démonstrations mathématiques un tant soit peu complexes utilisent des règles logiques de façon implicite, sans les énoncer. Ces règles découlent souvent du *bon sens* et les mathématiciens les utilisent sans se poser de question, sans s'en rendre vraiment compte, par intuition : « C'est logique ! ».
Ainsi dans le raisonnement du paradoxe de Russel on a utilisé le fait que « soit $\mathcal{E} \in \mathcal{E}$, soit $\mathcal{E} \notin \mathcal{E}$ ». Il n'y a pas d'autre cas possible, c'est intuitif. Mais avec l'avénement de la logique mathématique et la recherche d'une plus grande rigueur, on peut détailler cette intuition. Ainsi dans les théories axiomatiques usuelles on a le théorème (ou l'axiome, selon la théorie) « ou p, ou non p », où p est une variable propositionnelle, ainsi qu'une règle d'inférence dite de *substitution* selon laquelle on peut obtenir un théorème logique en remplaçant toutes les occurrences d'une variable propositionnelle dans un théorème déjà démontré par une proposition (ayant un sens dans le système considéré), ici notre proposition est « $\mathcal{E} \in \mathcal{E}$ ». On obtient ainsi notre théorème logique « soit $\mathcal{E} \in \mathcal{E}$, soit $\mathcal{E} \notin \mathcal{E}$ ».

Tout d'abord, un peu de vocabulaire. En logique formelle, une *théorie axiomatique* (ou *théorie formelle*) est formée d'un *langage formel* et d'un ensemble de *règles d'inférence* (ou *règles de déduction*) munis d'un ensemble d'*axiomes*. Les axiomes sont des *vérités nécessaires* (ou *vérités indémontrables*), des propriétés que l'on considère comme vraies, que l'on admet. Les axiomes dépendent du cadre d'étude, du contexte dans lequel on se place, il faut les choisir minutieusement, nous verrons pourquoi dans la suite. Les règles d'inférence quant à elles permettent la déduction, ce sont les règles que l'on doit appliquer pour passer d'une proposition vraie à une autre.

Un langage formel et un ensemble de règles d'inférence forment un *système formel*.

On appelle *théorème* toute propriété que l'on peut démontrer à partir des axiomes en appliquant un certain nombre de fois les règles d'inférence. Les axiomes sont donc a priori des théorèmes. Une *démonstration formelle* d'un théorème est une suite finie de propriétés débutant par un axiome (ou un théorème déjà démontré) et aboutissant au théorème de sorte à ce que l'on passe d'une propriété à la suivante en appliquant les règles d'inférence.
Remarquons que les axiomes peuvent être en nombre infini mais doivent être décidables, c'est-à-dire qu'étant donnée une propriété quelconque on doit pouvoir dire s'il s'agit ou non d'un axiome. Les règles d'inférence doivent quant à elles être « mécaniques », c'est-à-dire applicables par une machine. Ainsi une démonstration formelle étant donnée, un ordinateur doit pouvoir dire si elle est correcte ou non.
Malgré les avancées de la logique mathématique, lorsqu'ils travaillent dans des théories axiomatiques, les mathématiciens réalisent rarement des démonstrations formelles mais font toujours appel au langage courant, afin d'éviter d'avoir des démonstrations trop lourdes, trop difficiles à comprendre. Ce qui a changé c'est que maintenant ils savent qu'ils peuvent formaliser ces démonstrations.

Voici deux définitions importantes que l'on va étudier tout le long de cette partie.

Définitions

- Une théorie axiomatique est dite *consistante* (ou *cohérente*) s'il n'existe pas de proposition dont on puisse démontrer cette proposition ainsi que sa négation.
- Un théorie axiomatique est dite *complète* s'il n'existe pas de proposition dite *indécidable*, c'est-à-dire dont l'on ne peut montrer ni cette proposition ni sa négation.

Selon la nomenclature proposée par Hilbert, on nommera *métamathématiques* tout ce

que l'on fait en dehors de la théorie axiomatique considérée.
Ainsi une propriété peut être vraie à l'aide d'un raisonnement et d'arguments métamathématiques mais indémontrable dans la théorie axiomatique. Ainsi on peut reformuler la définition d'une théorie axiomatique incomplète : il s'agit d'une théorie axiomatique admettant des propriétés vraies (si une propriété est fausse il suffit de considérer sa négation) mais indémontrables.
Schématiquement on a : *propriété démontrable* $\Rightarrow$ *propriété vraie*, mais la réciproque est fausse (sauf dans le cas des théories complètes).

On a vu qu'une théorie était constituée d'un langage formel, mais de quoi s'agit-il ? Un langage formel est composé d'un ensemble de *mots* obéissant à des règles de construction strictes ainsi que d'une *sémantique* (c'est-à-dire que l'on donne un sens aux mots, qu'ils permettent d'exprimer quelque chose.).
En pratique, on se donne un ensemble (fini ou non) de signes (cet ensemble est nommé *alphabet*) que l'on souhaite utiliser et des règles de formation (il s'agit des règles définissant quelles combinaisons de signes forment un mot, il s'agit de la *grammaire formelle* du langage). Une formule respectant ces règles est dite bien formée.
Donnons un exemple pour fixer les idées. Usuellement en logique, il y a deux sortes de signes : les constantes (par exemple $\neg$ pour la négation, $\wedge$ pour la conjonction) et les variables (par exemple on peut fixer les lettres de l'alphabet). Alors $\neg a$ et $a \wedge b$ sont des mots mais $a\neg$, $a\neg b$, $\neg$ et $\wedge b$ ne le sont pas.
Remarquons aussi qu'il existe plusieurs types de variables selon la théorie axiomatique utilisée, nous en parlerons plus tard.
L'intérêt d'un langage formel est de faire abstraction de la sémantique.

Finissons l'introduction en présentant ce autour de quoi est articulé le présent article : le *programme de Hilbert*.
Il s'agit d'un projet initié par Hilbert dans le but de définir un socle sur lequel reposeraient toutes les mathématiques, d'unifier la multitude de champs mathématiques qui se sont rapidement développés. C'est en ce sens qu'il a énoncé au congrès international de mathématiques de 1900 à Paris 23 problèmes sur lesquels devaient se pencher les mathématiciens. Hilbert place ses espoirs dans la théorie des ensembles de Cantor avec la possibilité d'une théorie axiomatique valable pour toutes les mathématiques, pour « la » mathématique. Cependant ses espoirs seront ébranlés par les paradoxes de la théorie des ensembles, par la remise en cause du principe du tiers exclu (par Brouwer par exemple, qui considère que ce principe ne s'applique plus lorsque l'on manipule l'infini) et puis définitivement par les théorèmes de Gödel que nous allons présenter.
Notons que pour Hilbert, une telle théorie axiomatique des mathématiques devait être complète et consistante. Mais en plus, la consistance devait pouvoir s'obtenir par une démonstration finitiste (ne faisant pas appel à une infinité de formules ou à une infinité d'opérations sur des formules). Une telle démonstration s'obtient sans avoir à utiliser de métamathématiques (c'est-à-dire qu'elle doit s'obtenir seulement grâce à la théorie en question) et ne doit pas présupposer la consistance d'une autre théorie (il ne faut pas se ramener à la consistance d'une autre théorie).

3.2 Théorèmes de Gödel

Dans son mémoire *Über formal unentscheidbare Sätze der* Principia Mathematica *und verwandter Systeme, I.* (1931) Gödel démontre ses théorèmes dans le cas particulier d'une théorie axiomatique basée sur celle des *Principia Mathematica* de Russel et Whitehead auquel il a rajouté les axiomes de Peano pour l'arithmétique, en précisant à la fin du mémoire que cette démonstration reste valable pour un certain nombre de théories. Dans une note rajoutée en 1963 il précise que les avancées en logique (définitions claires...) doivent permettre d'obtenir une démonstration plus générale valable pour toutes les théories concernées. Nous allons donc tenter de retrouver les résultats de Gödel de façon générale, c'est-à-dire sans fixer une théorie particulière, tout en essayant de ne pas introduire trop de notions et malgré tout de rester rigoureux. Tâche ardue !

3.2.1 Paradoxe de Richard

Jules Richard présente le paradoxe suivant en 1905 dans une lettre déstinée à Louis Olivier, directeur de la *Revue générale des sciences pures et appliquées*. Elle sera publiée dans un article *Les Principes des mathématiques et le problème des ensembles* le 30 juin 1905 avec des commentaires de Jacques Hadamard (sans toutefois signer l'article). Elle sera republiée l'année suivante dans l'*Acta Mathematica*. L'article original est disponible sur le site *Gallica*, une traduction anglaise munie d'un commentaire est disponible dans [HEI]. Notons que ce paradoxe utilise lui aussi un argument diagonal.
Le paradoxe de Richard, version originale un peu modernisée :

Considérons un langage capable de définir des nombres réels, le français par exemple. On va construire la suite des phrases (ordonnée par longueur puis par ordre alphabétique) définissant un réel, c'est-à-dire l'ensemble des suites finies de mots définissant de façon rigoureuse et sans ambiguité un unique réel, où un mot est lui-même une suite finie de lettres. Richard le construit explicitement de la façon suivante :
On considère l'ensemble des 2-arrangements (c'est-à-dire que l'on choisit deux lettres parmi les lettres de l'alphabet en acceptant les répétitions de lettres et en conservant l'ordre de tirage) que l'on classe par ordre alphabétique. On fait de même à la suite avec les 3-arrangements, les 4-arrangements et ainsi de suite... Remarquons que l'on a pour l'instant une famille ordonnée et dénombrable. Ensuite on extrait les phrases définissant des réels et on obtient ainsi la suite ordonnée $(a_i)_{i\in\mathbb{N}}$ et donc une suite $(b_i)_{i\in\mathbb{N}}$, où b_i est le réel défini par a_i.
Une phrase définissant un nombre est par exemple : « Le nombre réel ayant 17 pour partie entière et tel que la $n$ème décimale vaut 1 si n est pair ou 0 sinon. » qui définit 17,01010101....
Maintenant définissons le réel $r = 0, r_0r_1r_3r_4\dots$ où r_i vaut 0 si la $i$ème décimale de b_i est différente de 0 ou 1 sinon. Alors r ne peut pas être dans notre suite par construction, cependant r peut être défini par une phrase, par exemple « Le nombre réel ayant 0 pour partie entière et telle que la $i$ème décimale vaut 0 si la $i$ème décimale de b_i est différente de 0 ou 1 sinon. ».
D'où le paradoxe. ■

Il existe aussi une version plus moderne et concernant cette fois seulement les entiers :
Le paradoxe de Richard, la notion de nombre richardien :

On construit de même la suite des phrases définissant des propriétés sur les entiers naturels. Par exemples « être premier », « être divisble par 5 » ou encore « être pair ».
On obtient ainsi la suite de phrases $(p_i)_{i\in\mathbb{N}}$.
Un entier n est alors dit richardien si et seulement si n ne vérifie pas la propriété p_n.
Cependant « être richardien » est une phrase définissant une propriété sur les entiers, c'est donc un élément de notre suite, disons p_k pour fixer les idées.
Deux cas se présentent alors :
• Soit k est richardien et alors il ne vérifie par la propriété p_k, c'est dire qu'il n'est pas richardien.
• Soit k n'est pas richardien et alors il vérifie la propriété p_k, c'est-à-dire qu'il est richardien.
D'où une contradiction et le paradoxe. ■

On retrouve donc que si k est richardien alors il ne l'est pas, et que s'il ne l'est pas alors il l'est, donc k est richardien si et seulement s'il ne l'est pas.

Notons d'abord que ce paradoxe ressemble fortement au *paradoxe du menteur*, déjà connu depuis l'Antiquité. On parle du *paradoxe du Crétois* ou encore paradoxe d'Épiménide. On peut l'énoncer ainsi : « Si un homme dit qu'il est en train de mentir. Alors s'il dit vrai, c'est que c'est faux. Mais s'il dit faux, c'est que c'est vrai. ».
Ce paradoxe est attribué à Épiménide le Crétois (VII^{e} siècle av. J.-C.) bien que le caractère paradoxal semble n'avoir été mis en avant qu'au IV^{e} siècle av. J.-C. par Eubulide dans le but de nuire à la logique d'Aristote (Déjà, bien avant Brouwer). De nombreuses solutions ont été proposées, cependant nous n'en parlerons pas plus ici, cela sort du cadre de cet article.

Une explication du paradoxe de Richard, mise en avant dès 1906 par Peano, est que l'on mélange mathématiques et métamathématiques.
Pour la deuxième version du théorème, la suite doit contenir des propriétés arithmétiques,

tacitement on parle de propriétés purement arithmétiques, que l'on peut définir dans le cadre de l'arithmétique. Or on introduit une propriété faisant intervenir notre travail antérieur : la propriété d'être richardien ou non, n'a de sens qu'après que l'on a défini notre suite. L'argument du paradoxe est donc fallacieux.
De même pour la première version, notre réel r dépend de la construction de notre suite, il ne s'agit pas d'une proposition pertinente avant la construction de la suite.

3.2.2 Nombres de Gödel

On reprend la présentation de Gödel dans son mémoire.

On rappelle que les signes de classe sont des formules ayant une variable libre.

$x = y$ est vrai si et seulement si x et y représentent la même propriété.

Le but du premier théorème de Gödel est de montrer que, sous certaines conditions, des théories axiomatiques sont forcément incomplètes. Gödel écrit lui-même dans son article de 1931 que son raisonnement est « étroitement apparenté à celui du paradoxe de Richard et au paradoxe du menteur ». Il utilise de même, sans le signaler, un argument diagonal. Voila grossièrement le raisonnement de Gödel :
On suppose que l'on peut définir dans notre théorie axiomatique $\neg$ pour la négation, $\mathrm{Dem}\, x$ qui est vrai si x est démontrable et faux sinon et $x = [y, z]$ (avec y un signe de classe et z une variable et où $[y, z]$ est la propriété obtenue en remplaçant toutes les occurrences de la variable libre de y par z).
Ensuite supposons que les signes de classe puissent être ordonnés (par exemple par longueur puis par ordre lexicographique sur les symboles du langage) et que $R(n)$ représente le $n$ème signe de classe. On peut définir une classe K de la sorte : $n \in K \Leftrightarrow \neg\mathrm{Dem}\,[R(n), n]$ (K est la classe formée des n tels que la propriété obtenue en remplaçant toutes les occurrences de la variable libre de $R(n)$ par n n'est pas démontrable). Comme cette classe est formée à partir de propriétés ayant un sens dans notre théorie, il existe un signe de classe S tel que $n \in K \Leftrightarrow [S, n]$, mais alors il existe donc un entier q tel que $S = R(q)$. Et donc on vérifie aisémment que $[R(q), q]$ n'est pas décidable (si elle est vraie alors elle est fausse, et si elle est fausse alors elle est vraie, donc elle est vraie si et seulement si elle est fausse). Donc la théorie n'est pas complète. On retrouve bien un argument diagonal avec nos $[R(n), n]$, le paradoxe du menteur puisque $[R(q), q]$ signifie (grossièrement) « Je ne suis pas démontrable » ainsi qu'une construction similaire à celle du paradoxe de Richard.
Il faut cependant prendre garde à ce que notre propriété $[R(q), q]$ ait bien un sens dans notre théorie afin d'éviter de reproduire l'erreur de Richard. Pour cela Gödel a une idée ingénieuse : il propose une application injective allant de l'ensemble des mots du langage de notre théorie à $\mathbb{N}$, il peut ainsi assigner à chaque formule ou à chaque démonstration un unique entier.

Pour présenter la notion de nombre de Gödel, nous nous plaçons dans le cas de son mémoire, c'est-à-dire avec les symboles ci-dessous.
Il commence par assigner un nombre premier à chaque symbole du langage de la théorie axiomatique considérée. Pour fixer les idées, proposons un langage ayant simplement quelques constantes et un nombre dénombrable de variables d'un certain nombre de types (ici 3 par exemple), alors on fixe un ordre pour ranger les constantes et on leurs assigne comme *nombre de Gödel* le $k$ème nombre premier (en commençant cependant par 1) pour la $k$ème constante. Supposons que l'on ait m constantes alors on ordonne les variables de chaque type et pour la $i$ème variable de type n on lui assigne le nombre p_{m+i}^n, où p_k est le $k$ème nombre premier (cependant en commençant par 1).
Par exemple :

Comme il y a une infinité dénombrable de nombres premiers, l'alphabet peut être de cardinal infini dénombrable.

Symbole	Nombre de Gödel	Signification
$\neg$	1	Négation
$\vee$	2	Disjonction
Π	3	Pour tout
0	5	0
s	7	Successeur
(	11	
)	13	
x_1	17	Première variable numérique
x_2	19	Deuxième variable numérique
x_3	23	Troisième variable numérique
	...	
y_1	17^2	Première variable propositionnelle
y_2	19^2	Deuxième variable propositionnelle
y_3	23^2	Troisième variable propositionnelle
	...	
z_1	17^3	Première variable de prédicat
z_2	19^3	Deuxième variable de prédicat
z_3	23^3	Troisième variable de prédicat

Petite explication des notations du mémoire de Gödel :
On peut substituer les variables numériques par des entiers, les variables propositionnelles par des propositions et les variables de prédicat par des prédicats.
Une formule peut avoir un certain nombre de variables libres ou liées (grossièrement on peut dire qu'une variable est libre si elle ne dépend pas d'un quantificateur (pour tout, il existe...)).
Une formule ayant n variables libres est un *signe de relation à n places*, et plus simplement si $n = 1$ on parle de *signe de classe*.

Ensuite à chaque proposition on assigne un nombre de Gödel de la même façon : on fait le produit des $p_k^{G(k)}$ où p_k est le $k$ème nombre premier (cette fois en commençant bien par 2) et $G(k)$ le nombre de Gödel du $k$ème symbole. Par exemple le nombre de Gôdel de « $\neg(x_1 \vee x_2)$ » est $2^1 \times 3^{11} \times 5^{17} \times 7^2 \times 11^{19} \times 13^{13}$.
De même pour une démonstration (on rappelle qu'il s'agit d'une suite finie de propositions) : on fait le produit des $p_k^{G(k)}$ où p_k est le $k$ème nombre premier (toujours en commençant par 2) et $G(k)$ le nombre de Gödel de la $k$ème proposition.
À partir de là, le théorème fondamental de l'arithmétique (existence et unicité de la décomposition en facteurs premiers de tout entier naturel) permet de dire si un entier n donné est un nombre de Gödel, et si oui, de préciser le symbole (ou la proposition, ou la démonstration) qui lui est associé.

On remarque qu'il faut que les théories concernées soient capables de formaliser certains rudiments d'arithmétique pour pouvoir manipuler les *nombres de Gödel* et les propriétés $[R(n), n]$ faisant intervenir des entiers (Nous clarifierons les hypothèses lors de la démonstration).
Il me semble aussi important de signaler qu'une injection dans un autre ensemble (par exemple un ensemble d'objets géométriques) permet de généraliser ce théorème à d'autres théories (par exemple capable de formaliser certains rudiments de géométrie) selon un principe similaire.

3.2.3 Quelques données supplémentaires nécessaires

On donne une définition plus générale et moins formelle que celle utilisée par Gödel.

Définition : théorie ω-consistante

Une théorie axiomatique est dite ω-consistante s'il n'existe pas de signe de classe (propriété à une seule variable libre) P tel que l'on puisse pour tout entier n démontrer « $\neg P(n)$ » et que l'on puisse aussi démontrer « $\exists y P(y)$ ».

Il ne s'agit pas d'un contre-sens, en effet ce n'est pas parce que l'on a une démonstration des propriétés « $P(n)$ » pour tout n que l'on a une démonstration de la propriété « $\forall n$, $P(n)$ ».
Notons qu'on peut vérifier qu'une théorie ω-consistante est consistante, mais qu'il ne s'agit cependant que d'une condition suffisante, en effet on peut exhiber des théories étant consistantes sans être ω-consistantes.

Notations

En plus des symboles du langage de la théorie considérée, on rajoute deux symboles « externes » permettant de rendre les démonstrations plus concises et d'éviter les répétitions :
« $p \equiv q$ » signifie que p est « équivalent » à q (permet de définir de nouveaux symboles à partir de ceux du langage pour éviter de répéter certaines formules que l'on écrira souvent dans un raisonnement).
« $\vdash p$ » signifie que p est démontrable (prouvable) dans la théorie (permet d'éviter d'écrire « est démontrable dans la théorie »).

Définition : fonction récursive

On remarque que l'on retrouve la notion de « processus mécanique » déjà nécessaire aux règles d'inférence des théories axiomatiques.

De façon imprécise, on dit qu'une fonction est récursive si elle est calculable, c'est-à-dire si elle peut être calculée à partir de ses paramètres suivant un « processus mécanique ».

Dans tout le paragraphe sur les théorèmes de Gödel, on travaillera avec des théories capables d'axiomatiser des rudiments d'arithmétique (afin de pouvoir, entre autres, manipuler les nombres de Gödel) et on notera $G(\theta)$ le nombre de Gödel associé à une formule θ bien formée pour cette théorie.
On dit qu'une théorie représente une fonction $f : \mathbb{N} \mapsto \mathbb{N}$ si et seulement s'il existe une formule « δ » dans le langage formel de cette théorie de sorte à ce que pour chaque $n \in \mathbb{N}$, on ait : $\vdash \forall y(\underline{f(n)} = y \Leftrightarrow \delta(\underline{n}, y))$.
« $\underline{n}$ » signifie que l'on considère l'entier n tel que construit dans la théorie (c'est-à-dire comme une variable numérique de cette théorie).

Le lemme suivant, qui n'était pas connu par Gödel en 1931, va nous permettre de démontrer le premier théorème de Gödel de façon plus générale. Il est nommé *lemme diagonal* du fait de sa ressemblance avec l'argument diagonal de Cantor.

Théorème 5: Lemme diagonal (ou théorème du point fixe) (Par Rudolf Carnap en 1934)

Dans toute théorie axiomatique des entiers naturels du premier ordre (calcul des prédicats) capable de représenter toutes les fonctions récursives, il existe au moins une proposition faisant référence à elle-même.
i.e. pour toute formule bien formée « ψ » à une variable libre, il existe une proposition « ϕ » tel que $\vdash \phi \Leftrightarrow \psi(\underline{G(\phi)})$

Démonstration :

Soit « ψ » une formule de la théorie à une variable libre.

$$\text{Soit } f : \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & \begin{cases} G(\theta(\underline{G(\theta)})) & \text{si } n \text{ est le nombre de Gödel d'une formule } \theta \\ & \text{ayant une variable libre.} \\ 0 & \text{sinon.} \end{cases} \end{array}.$$

f est récursive donc il existe une formule « δ » représentant f dans la théorie axiomatique.
C'est-à-dire vérifiant pour toute formule θ, $\vdash \forall y\ ((\underline{G(\theta(G(\theta)))} = y) \Leftrightarrow \delta(\underline{G(\theta)}, y))$.
Maintenant définissons la formule « β » à une variable libre ainsi :
$\beta(x) \equiv (\forall y\ (\delta(x, y) \Rightarrow \psi(y)))$.
Maintenant soit $\phi \equiv \beta(\underline{G(\beta)})$, alors on a :
$\vdash \phi \Leftrightarrow \forall y\ (\delta(\underline{G(\beta)}, y) \Rightarrow \psi(y)) \Leftrightarrow \forall y\ ((y = \underline{G(\beta(G(\beta)))}) \Rightarrow \psi(y))$

• Si « ϕ » est vraie alors pour $y \equiv G(\beta(G(\beta)))$ dans la propriété la plus à droite on a : $\vdash (\underline{G(\beta(G(\beta)))} = \underline{G(\beta(G(\beta)))}) \Rightarrow \psi(\underline{G(\beta(G(\beta)))})$.
Puis comme $\phi \equiv \beta(\underline{G(\beta)})$, on a donc que $\psi(\underline{G(\phi)})$ est vrai.

• Réciproquement supposons que « $\psi(\underline{G(\beta(G(\beta)))})$ » soit vrai. Alors la dernière propriété est vraie et donc « ϕ » l'est aussi par équivalence.

Pour une formule « ψ » à une variable libre, on a exhibé une proposition « ϕ » telle que : $\vdash \phi \Leftrightarrow \psi(\underline{G(\phi)})$.

■

Le théorème suivant va nous permettre d'utiliser le *prédicat de prouvabilité* (ou *de démontrabilité*) Dem (définie dans le cadre ci-dessous) dans le cas des théories capables de représenter toutes les fonctions récursives.
Au vu de la difficulté de cette preuve, nous ne donnerons qu'une explication informelle.
Dans son article, Gödel construit Dem en 45 étapes dans la théorie qu'il s'est fixé.

Théorème 6

Considérons la relation numérique binaire $\mathrm{Dem}(m,n)$ définie comme étant vraie si et seulement si m et n sont des nombres de Gödel et si m code une démonstration formelle de n.
Alors Dem est une fonction récursive.

Vérification informelle :

Pour vérifier si $\mathrm{Dem}(m,n)$ est vraie, on peut procéder comme suit :
On décode m, ce qui ne pose pas de souci et se fait mécaniquement.
On vérifie ensuite si m est un nombre de Gödel, si ce n'est pas le cas $\mathrm{Dem}(m,n)$ est fausse, sinon on examine si l'on obtient une formule bien formée selon la grammaire formelle du langage de notre théorie. Ce qui se fait de façon algorithmique, il n'y a toujours aucun souci.
Si ce n'est pas le cas, de même, $\mathrm{Dem}(m,n)$ est fausse. Sinon, on verifie si l'on obtient bien une démonstration formelle, c'est-à-dire s'il s'agit d'une suite de formules telle que la première formule soit un axiome (ou un théorème déjà démontré) et que l'on obtienne les formules d'après en utilisant des règles d'inférence, ce qui est décidable du fait de nos conditions dans la définition d'une théorie axiomatique (les axiomes sont décidables et les règles d'inférence sont « mécaniques »).
Si c'est le cas, il reste ensuite à vérifier que le nombre de Gödel de la dernière formule est bien n (Ce qui est décidable du fait que les théories considérées contiennent les rudiments de l'arithmétique, notamment la possibilité de tester l'égalité entre deux entiers).
Remarquons qu'une démonstration rigoureuse pourrait même montrer qu'il s'agit d'une *fonction primitive récursive* (il s'agit de fonctions récursives particulières).

■

3.2.4 Énoncés et démonstrations

Une théorie exhaustive de l'arithmétique n'est pas nécessaire, en effet le principe de récurrence sur les entiers est par exemple inutile ici. Il suffit d'avoir les rudiments d'arithmétique utiles pour les opérations sur les nombres de Gödel.

Théorème 7: Premier théorème d'incomplétude de Gödel

Dans toute théorie axiomatique du premier ordre (calcul des prédicats) ω-consistante capable de formaliser des rudiments d'arithmétique et de représenter toutes les fonctions récursives, il existe au moins une proposition indécidable.

Démonstration :

On a vu que d'après notre définition d'une *théorie axiomatique* Dem était une fonction récursive, donc d'après les hypothèses Dem est représentable dans la théorie considérée. Il existe donc une formule « $\mathcal{D}$ » à deux variables libres bien formée dans le langage de la théorie telle que si $\text{Dem}(m,n)$ est vraie alors $\vdash \mathcal{D}(\underline{m},\underline{n})$ et telle que si $\text{Dem}(m,n)$ est fausse alors $\vdash \neg\mathcal{D}(\underline{m},\underline{n})$.
Considérons alors la formule suivante ayant une unique variable libre « x » et étant bien formée dans le langage de la théorie : « $(\forall y)\neg\mathcal{D}(y,x)$ ».
Puis, comme on peut appliquer le lemme diagonal, il existe donc une formule « $\mathcal{G}$ » telle que $\vdash \mathcal{G} \Leftrightarrow ((\forall y)\neg\mathcal{D}(y,\underline{G(\mathcal{G})}))$.
On a donc obtenu notre formule signifiant « Je ne suis pas démontrable » (Paradoxe du menteur). Nous allons montrer qu'elle est indécidable.
Soit $q = G(\mathcal{G})$.

Supposons par l'absurde que « $\mathcal{G}$ » soit démontrable (i.e. $\vdash \mathcal{G}$), alors elle admet une démonstration ayant pour nombre de Gödel r et alors Dem(r, q) est vraie et donc $\vdash \mathcal{D}(\underline{r},\underline{q})$.
C'est-à-dire $\vdash \mathcal{D}(\underline{r},\underline{G(\mathcal{G})})$.
Or on a $\vdash (\forall y)\neg\mathcal{D}(y,\underline{G(\mathcal{G})})$ et donc $\vdash \neg\mathcal{D}(\underline{r},\underline{G(\mathcal{G})})$.
D'où une contradiction (car la théorie est consistante). Ainsi $\mathcal{G}$ n'est pas démontrable.

On a ainsi que pour tout entier n la relation $\text{Dem}(n,q)$ est fausse.
Donc pour tout entier n on a $\vdash \neg\mathcal{G}(\underline{n},\underline{q})$.
Du fait de l'ω-consistance, on ne peut démontrer « $(\exists y)\mathcal{G}(\underline{y},\underline{G(\mathcal{G})})$ ».

Supposons désormais par l'absurde que « $\neg\mathcal{G}$ » soit démontrable (i.e. $\vdash \neg\mathcal{G}$).
Alors $\vdash \neg((\forall y)\neg\mathcal{D}(y,\underline{G(\mathcal{G})}))$, c'est-à-dire $\vdash (\exists y)\mathcal{D}(y,\underline{G(\mathcal{G})})$.
Ce qui contredit ce que l'on vient de voir.

Donc on ne peut démontrer ni « $\mathcal{G}$ », ni « $\neg\mathcal{G}$ », on a donc exhibé une formule bien formée indécidable de notre théorie, qui est donc de ce fait, incomplète.

■

Théorème 8: Second théorème d'incomplétude de Gödel

Toute théorie axiomatique du premier ordre (calcul des prédicats) consistante capable de formaliser suffisamment d'arithmétique, de représenter toutes les fonctions récursives et vérifiant les conditions de *Löb*, ne peut démontrer elle-même sa consistance.

Avant d'entamer la démonstration, notons que GÖDEL n'a pas fourni de démonstration de ce théorème, juste une idée de démonstration. Comme pour le premier théorème, celui-ci admet de nombreuses variantes, avec différentes hypothèses. Les conditions de *Löb* peuvent être démontrées à partir des conditions de *Hilbert-Bernays* et touchent donc une large classe de théories axiomatiques.
On pose $\mathcal{B}(x) \equiv ((\exists y)\mathcal{D}(y,x))$ et alors les conditions de Löb s'énoncent ainsi :
• Pour toute formule « α », si la théorie axiomatique permet de démontrer « α » alors elle permet de démontrer « $\mathcal{B}(\underline{G(\alpha)})$ » (i.e. si $\vdash \alpha$ alors $\vdash \mathcal{B}(\underline{G(\alpha)})$).
• Pour toute formule « α », si la théorie axiomatique permet de démontrer « $\mathcal{B}(\underline{G(\alpha)}) \Rightarrow \alpha$ » alors elle permet de démontrer « α » (i.e. si $\vdash \mathcal{B}(\underline{G(\alpha)}) \Rightarrow \alpha$ alors $\vdash \alpha$).
Démonstration :

$\mathcal{B}$ pour *Beweisbar* qui est le mot allemand pour démontrable (ou prouvable).
Par définition, « $\mathcal{B}(x)$ » permet de vérifier si x admet une démonstration dans la théorie.

On définit « $\mathcal{N}$ » représentant la fonction récursive $\text{Neg}(x,y)$ étant vraie si et seulement x et y sont des nombres de Gödel et que la propriété représentée par y est la négation de la propriété représentée par x.
Considérons « $\mathcal{C}$ » (pour **c**onsistance) défini ainsi $\mathcal{C} \equiv (\forall x)(\forall y)\neg(\mathcal{N}(x,y) \wedge \mathcal{B}(x) \wedge \mathcal{B}(y))$.
Comme la théorie est consistante, par hypothèse, $\mathcal{C}$ est vraie. On va cependant voir qu'elle ne permet pas de montrer $\mathcal{C}$.
Supposons par l'absurde qu'elle le permette.
Comme $\vdash 0 \neq \underline{1}$ la première condition de Löb donne que $\vdash \mathcal{B}(\underline{G(0 \neq \underline{1})})$.

Puis par substitution dans $\mathcal{C}$:
$\vdash \neg(\mathcal{N}(\underline{G(0=\underline{1})}, \underline{G(0\neq\underline{1})}) \wedge \mathcal{B}(\underline{G(0=\underline{1})}) \wedge \mathcal{B}(\underline{G(0\neq\underline{1})}))$.
Puis par définition de « $\mathcal{N}$ », on a $\vdash \mathcal{N}(\underline{G(0=\underline{1})}, \underline{G(0\neq\underline{1})})$.
On a alors forcément $\vdash (\mathcal{B}(\underline{G(0=\underline{1})}))$.
Et comme $\vdash \neg(\mathcal{B}(\underline{G(0=\underline{1})})) \Rightarrow (0\neq\underline{1} \Rightarrow \neg(\mathcal{B}(\underline{G(0=\underline{1})})))$ (axiome ou théorème d'une théorie suffisamment élaborée).
On a par *modus ponens* $\vdash 0\neq\underline{1} \Rightarrow \neg(\mathcal{B}(\underline{G(0=\underline{1})}))$ et par contraposée $\vdash \mathcal{B}(\underline{G(0=\underline{1})}) \Rightarrow (0=\underline{1})$ (de même la théorie doit être suffisamment élaborée pour la contraposition et le modus ponens qui signifie : si $\vdash p$ et $\vdash p\Rightarrow q$ alors $\vdash q$).
La seconde condition de Löb donne donc $\vdash 0=\underline{1}$, ce qui est absurde, d'où la contradiction.
La théorie ne permet donc pas de montrer elle-même sa propre consistance, bien qu'elle soit consistante.

■

Notons cependant que Gerhard Karl Erich Gentzen (*Die Widerspruchsfreiheit der reinen Zahlentheorie*), puis Wilhelm Ackermann de façon indépendante, ont réussi à obtenir une preuve arithmétique de la consistance de l'arithmétique de Peano (respectivement en 1936 et en 1940) en utilisant une induction transfinie (incompatible avec la définition de démonstration formelle donnée dans cet article).

3.2.5 Pour approfondir

Le premier théorème d'incomplétude de Gödel peut se généraliser à des théories consistantes (plutôt qu'ω-consistantes). C'est ce qu'a montré John Barkley Rosser Sr. en 1936 en trouvant une autre formule pour la démonstration (et qui allonge un peu la démonstration, sans être toutefois trop difficile).
En 1989 George Boolos trouve une démonstration plus simple du premier théorème de Gödel en se basant sur le *paradoxe de Berry* (formulé en 1906 par Russel) plutôt que sur le paradoxe du menteur.
Tarski a montré en 1933 que la propriété arithmétique qui est vraie pour n si et seulement si n est un nombre de Gödel d'une propriété bien formée vraie (métamathématiquement) n'est pas une propriété arithmétique. La preuve est semblable, bien que plus simple, à celle du premier théorème de Gödel.
Un dernier théorème sympathique, dit de *Church-Turing* (resp. 1936 et 1937), affirme qu'il n'existe pas d'algorithme pour prédire si un théorème est démontrable...
À méditer pour les plus curieux...

Quelques résultats sur l'axiome du choix et l'hypothèse du continu :
• L'axiome du choix est une propriété indécidable de ZF.
• L'hypothèse du continu n'est pas réfutable dans ZF ou dans ZFC (Gödel 1938).
• L'hypothèse du continu ne peut se déduire des axiomes de ZF ou de ZFC (méthode du forcing par Paul Joseph Cohen en 1963).
• L'hypothèse du continu est donc une propriété indécidable de ZF(C).

3.3 Quelques exemples

3.3.1 Le calcul propositionnel (cf. [MEN])

On va démontrer la consistance et la complétude du *calcul propositionnel*, dont on va définir une théorie axiomatique très simple.
Tout d'abord le langage :

On supprime dès à présent les parenthèses quand il n'y a pas ambiguité.

Constantes		
Connecteurs propositionnels		
Symbole	Syntaxe	Signification
$\neg$	$\neg p$	Négation, NON-p
$\Rightarrow$	$p \Rightarrow q$	Implication, si p alors q
Signes des ponctuation		
(		
)		

Variables propositionnelles
p, q, p_1, p_2, $p_3 \ldots$

On se donne désormais une unique règle d'inférence relativement intuitive, la *règle de détachement* (ou *Modus ponens*) :

Si la théorie permet de démontrer p et de démontrer $(p \Rightarrow q)$ alors elle permet de démontrer q.

On a ainsi défini notre système formel, pour obtenir une théorie axiomatique il ne nous reste plus qu'à nous donner des axiomes, ils seront au nombre de 3. Les deux premiers axiomes vont permettre de démontrer le lemme de déduction et le troisième représente le raisonnement par l'absurde (ou *reductio* ou *reductio ad absurdum*).

1. $(p \Rightarrow (q \Rightarrow p))$
2. $((p_1 \Rightarrow (p_2 \Rightarrow p_3)) \Rightarrow ((p_1 \Rightarrow p_2) \Rightarrow (p_1 \Rightarrow p_3)))$
3. $(((\neg q) \Rightarrow (\neg p)) \Rightarrow (((\neg q) \Rightarrow p) \Rightarrow q))$

On a ainsi défini une théorie que l'on notera $\mathcal{T}$ dans la suite.

Avant de commencer nos démonstrations, il faut signaler que notre langage permet de définir les connecteurs propositionnels usuels : $(p \vee q) \equiv ((\neg p) \Rightarrow q)$ (disjonction) et ensuite $(p \wedge q) \equiv \neg(p \Rightarrow (\neg q))$ (conjonction). On dit que notre ensemble de connecteurs propositionnels est *complet* (à ne pas confondre avec la complétude de la théorie).

Étudions d'abord une première démonstration formelle :

Théorème 9

$\mathcal{T}$ permet de démontrer $p \Rightarrow p$ (i.e. $\vdash p \Rightarrow p$).

Démonstration :

1.	$(p \Rightarrow ((p \Rightarrow p) \Rightarrow p)) \Rightarrow ((p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p))$	Axiome 2 en substituant p_1 et p_3 par p et p_2 par $p \Rightarrow p$
2.	$p \Rightarrow ((p \Rightarrow p) \Rightarrow p)$	Axiome 1 en substituant q par $p \Rightarrow p$
3.	$(p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p)$	1, 2, Modus ponens
4.	$p \Rightarrow (p \Rightarrow p)$	Axiome 1 en substituant q par p
5.	$p \Rightarrow p$	3, 4, Modus ponens

■

Lemme : (méta-)théorème de déduction

Si en considérant « p » comme un axiome on peut démontrer « q », alors on peut démontrer « $p \Rightarrow q$ ».

Démonstration :

Soit « $p_1, p_2, \ldots, p_{k-1}, p_k \equiv q$ » une démonstration de « q » en considérant « p » vraie.
On va montrer par récurrence sur i que $\vdash p \Rightarrow p_i$ pour tout i dans $[\![1; k]\!]$.
D'après la définition de démonstration formelle, p_1 est soit un axiome ou un théorème de $\mathcal{T}$ soit p, on a donc $p \Rightarrow p_1$ en utilisant le raisonnement des deux premiers cas de l'hérédité (ne nécessitant pas d'hypothèse de récurrence).
Supposons désormais qu'il existe un certain i dans $[\![1; k-1]\!]$ tel que pour

$\forall j \in [\![1;i]\!]$, $\vdash p \Rightarrow p_i$.
• 1e cas : « p_{i+1} » est un axiome ou un théorème de $\mathcal{T}$.
Alors on a la démonstration formelle suivante :

1.	p_{i+1}	
2.	$p_{i+1} \Rightarrow (p \Rightarrow p_{i+1})$	Axiome 1 en substituant q par p et p par p_{i+1}
3.	$p \Rightarrow p_{i+1}$	1, 2, Modus ponens

• 2e cas : $p_{i+1} \equiv p$, alors on utilise le théorème précédent : $\vdash p \Rightarrow p$.
• 3e et dernier cas : « p_{i+1} » est obtenu par modus ponens sur « p_n » et « p_m » avec $n, m \leq i$ et $p_n \equiv (p_m \Rightarrow p_{i+1})$.
Donc par hypothèse de récurrence on a : $\vdash p \Rightarrow p_n$ et $\vdash p \Rightarrow (p_n \Rightarrow p_{i+1})$.
On a alors la démonstration formelle suivante :

1.	$p \Rightarrow p_n$	
2.	$p \Rightarrow (p_n \Rightarrow p_{i+1})$	
3.	$(p \Rightarrow (p_n \Rightarrow p_{i+1})) \Rightarrow ((p \Rightarrow p_n) \Rightarrow (p \Rightarrow p_{i+1}))$	Axiome 2
4.	$(p \Rightarrow p_n) \Rightarrow (p \Rightarrow p_{i+1})$	2, 3, Modus ponens
5.	$p \Rightarrow p_{i+1}$	1, 4, Modus ponens

Ce qui clôt la récurrence.

■

Ce métathéorème va nous permettre de simplifier nos démonstrations, de plus il nous autorise à rajouter des hypothèses dans la suite de propriétés d'une démonstration formelle. On ajoute alors un second sens à la notation $\vdash$: « $p_{i_1}, p_{i_2}, \ldots \vdash q$ » signifie que sous les hypothèses « $p_{i_1}, p_{i_2} \ldots$ », « q » est démontrable.
Avec cette notation le théorème devient : si $p \vdash q$ alors $\vdash (p \Rightarrow q)$.

Pour illustrer ceci remarquons que le théorème précédent se démontre désormais en une seule ligne : comme $p \vdash p$ on a par le théorème de déduction $\vdash p \Rightarrow p$.

Lemme

$\mathcal{T}$ permet de démontrer :
• $\neg p \Rightarrow (p \Rightarrow q)$

Démonstration formelle :

1.	$\neg p$	Hypothèse
2.	p	Hypothèse
3.	$p \Rightarrow ((\neg q) \Rightarrow p)$	Axiome 1 en substituant q par $\neg q$
4.	$(\neg p) \Rightarrow ((\neg q) \Rightarrow (\neg p))$	Axiome 1 en substituant q (resp. p) par $\neg q$ (resp. $\neg p$)
5.	$(\neg q) \Rightarrow p$	2, 3, Modus ponens
6.	$(\neg q) \Rightarrow (\neg p)$	1, 4, Modus ponens
7.	$(((\neg q) \Rightarrow (\neg p)) \Rightarrow (((\neg q) \Rightarrow p) \Rightarrow q))$	Axiome 3
8.	$((\neg q) \Rightarrow p) \Rightarrow q$	6, 7, Modus ponens
9.	q	5, 8, Modus ponens
10.	$(\neg p), p \vdash q$	1→9 (résumé)
11.	$(\neg p) \vdash (p \Rightarrow q)$	Théorème de déduction
12.	$\vdash (\neg p) \Rightarrow (p \Rightarrow q)$	Théorème de déduction

■

Théorème 10

$\mathcal{T}$ est consistant.

On va donner une démonstration de consistance absolue, c'est-à-dire : réalisable avec les outils de notre théorie seulement, en un nombre fini d'étapes et sans reposer sur la consistance d'une autre théorie axiomatique. Comme pour chaque démonstration mathématique correcte dans une théorie axiomatisable, il faut garder en mémoire qu'on peut en déduire une démonstration formelle (mais moins compréhensible).

Démonstration absolue de la consistance :

En substituant « p » par « $\neg p$ » dans le lemme précédent on obtient $\vdash p \Rightarrow (\neg p \Rightarrow q)$ (On reconnait : « $p \Rightarrow (p \vee q)$ »).
Supposons par l'absurde (on peut le faire sans quitter $\mathcal{T}$ d'après le troisième axiome) que $\mathcal{T}$ n'est pas consistante alors il existe « p » tel que $\vdash p$ et $\vdash \neg p$. Alors comme $\vdash \neg p$ d'après le modus ponens $\vdash (p \Rightarrow q)$ et de même comme $\vdash p$ toujours d'après le modus ponens $\vdash q$.
Donc si $\mathcal{T}$ n'est pas consistante toute formule bien formée est démontrable.

Donnons d'abord une idée d'ordre métamathématique :
On vérifie que les axiomes sont des tautologies (sinon on aurait fait un choix très mauvais...), c'est-à-dire qu'ils sont vrais quel que soient les variables propositionnelles (On dépasse légèrement du cadre de la consistance absolue en empiétant sur les métamathématiques, cependant il existe une définition de *tautologie* qui est rigoureuse et intérieure à la théorie, pour le vérifier ici, on peut dresser leurs tables de vérité).
De plus le modus ponens laisse invariant cette propriété (il faudrait pour cela voir la définition rigoureuse, cependant « c'est logique ! » : les propriétés démontrables sont des propriétés vraies).
Donc toutes les propriétés démontrables de $\mathcal{T}$ sont des tautologies.
Considérons maintenant « $p \vee q$ », il s'agit bien d'une formule bien formée mais ce n'est pas une tautologie, d'où la contradiction.

On va passer à la démonstration absolue en définissant rigoureusement ce qu'est une tautologie dans notre théorie (je me suis basé sur la définition de l'appendice 3 de [SEU1]).
On va définir deux classes K_1 et K_2 disjointes de sorte à obtenir une partition des formules bien formées :
- « $p \Rightarrow q$ » est dans K_2 si « p » est dans K_1 et « q » dans K_2, sinon elle est dans K_1.
- « $\neg p$ » est dans K_2 si « p » est dans K_1, sinon elle est dans K_1.

On dit désormais qu'une formule est une tautologie si et seulement si elle est dans K_1 quel que soient les classes (K_1 ou K_2) de ses variables libres.
Cette définition est bien indépendante de toute interprétation métamathématique.
Vérifions maintenant que nos axiomes sont des tautologies, on peut désormais alléger en toute légitimité le raisonnement à l'aide de tables de vérité (appartenir à K_1 et à K_2 est indépendant de l'aspect vrai/faux des formules, cependant le voir ainsi peut en faciliter la compréhension). Par exemple pour le premier axiome :

p	q	$q \Rightarrow p$	$p \Rightarrow (q \Rightarrow p)$
K_1	K_1	K_1	K_1
K_1	K_2	K_1	K_1
K_2	K_1	K_2	K_1
K_2	K_2	K_1	K_1

Vérifions désormais que le modus ponens conserve les tautologies. Supposons que l'on ait $\vdash p$ et $\vdash p \Rightarrow q$ où « p » et « $p \Rightarrow q$ » sont des tautologies. On a d'après le modus ponens que $\vdash q$, on doit donc vérifier que « q » est une tautologie.
On raisonne par l'absurde et on suppose qu'il ne s'agit pas d'une tautologie, alors on peut substituer les variables libres de « q » de sorte à ce qu'elle soit dans K_2. Mais alors dans ce cas, comme « p » est dans K_1, on a que « $p \Rightarrow q$ » est dans K_2. Ce qui est en contradiction avec le fait que « $p \Rightarrow q$ » soit une tautologie.
Donc toute propriété démontrable dans $\mathcal{T}$ est une tautologie.

Étudions le cas de $(p \vee q) \equiv ((\neg p) \Rightarrow q)$:

p	q	$\neg p$	$p \vee q$
K_1	K_1	K_2	K_1
K_1	K_2	K_2	K_1
K_2	K_1	K_1	K_1
K_2	K_2	K_1	K_2

Il ne s'agit donc pas d'une tautologie. On a donc exhibé rigoureusement une formule bien formée mais non démontrable.
D'où une contradiction avec l'hypothèse de la non-consistance de $\mathcal{T}$.

■

Théorème 11

$\mathcal{T}$ est complet.

Démonstration :

En rédaction...

■

Théorème 12

Les axiomes de $\mathcal{T}$ sont indépendants.
C'est-à-dire qu'aucun axiome ne peut se déduire des deux autres.

Démonstration :

En rédaction...

■

3.3.2 Le cas intéressant de la géométrie euclidienne

Dans les *Élements* d'Euclide (aux alentours de 300 av. J.-C.), la géométrie repose sur 5 postulats. Il s'agit des prémices d'une théorie axiomatique.

1. Un segment de droite peut être tracé en joignant deux points quelconques distincts.
2. Un segment de droite peut être prolongé indéfiniment en une ligne droite.
3. Étant donné un segment de droite quelconque, un cercle peut être tracé en prenant ce segment comme rayon et l'une de ses extrémités comme centre.
4. Tous les angles droits sont congruents.
5. Si deux lignes sont sécantes avec une troisième de telle façon que la somme des angles intérieurs d'un côté est strictement inférieure à deux angles droits, alors ces deux lignes sont forcément sécantes de ce côté.

Pour le 5^{e} postulat on a tendance à utiliser une proposition équivalente et plus simple : « Étant donnés une droite et un point, il existe une unique droite parallèle à la première et passant par ce point » (formulation que l'on doit à Proclos, à William Ludlam et à John Playfair).
Ce postulat semble moins évident que les 4 premiers, ainsi de nombreux mathématiciens se sont demandés s'il ne pouvait être obtenu à partir des 4 précédents (il s'agirait alors d'un théorème). Par exemple par Proclus de Lycie (*Commentaires sur le premier Livre des Éléments d'Euclide*, v^{e} siècle), par Omar Khayyâm (*Commentaires sur les postulats problématiques d'Euclide*, 1048 - ?- 1131) ou encore par Wallis (*De postulato quinto : et definitione quinta*, 1656). Cette question devient pressante au début du xix^{e} siècle. Gauss dit alors que : « Pour la théorie des parallèles, nous ne sommes pas plus avancés qu'Euclide, c'est une honte pour les mathématiques ».
S'il s'agit seulement d'un axiome, alors on pourrait tenter d'obtenir d'autres géométries où ce dernier ne figure pas comme postulat (effectivement, ce sera le cas, et on parle de géométries

non-euclidiennes. La géométrie hyperbolique est par exemple une géométrie non-euclidienne consistante et complète). Il faut noter que cette époque est marquée par une augmentation de l'abstraction mathématique du fait que les mathématiciens tentent de ne plus céder à l'intuition physique.
Notons que dès 1733 Giovanni Saccheri publie *Euclides ab omni naevo vindicatus* (Euclide lavé de toute tache) où il suppose que par un point passe une infinité de droites ne coupant pas une droite donnée (il s'agit en fait de notre géométrie hyperbolique). Il obtient ainsi des théorèmes vraisemblablement faux et pense avoir démontré par l'absurde que le 5^{e} postulat est bien un axiome et non un théorème.
Selon un raisonnement similaire Gauss (qui ne publia pas ses travaux, mais on en trouve des traces dans ses lettres), Nicolaï Ivanovitch Lobatchevski (1826) et János Bolyai (1868, *La science absolue de l'espace*) eurent la même intuition : ils obtinrent ainsi une théorie complète et consistante d'une nouvelle géométrie, la géométrie hyperbolique.

On constate très rapidement que les postulats d'Euclide ne suffisent pas à obtenir des preuves rigoureuses se passant de toute intuition géométrique. En effet Eudoxe de Cnide (408-355 av. J.-C.) et Archimède (287-212 av. J.-C.) ont déjà pressenti la nécessité d'ajouter ce que l'on nomme aujourd'hui l'*axiome d'archimède* (et qui a donné son nom à une propriété que vous connaissez bien : « $\mathbb{R}$ est archimédien »).
En 1899 Hilbert propose donc une liste de 21 axiomes (maintenant 20, du fait de la redondance d'un d'entre eux) dans le but d'obtenir une théorie axiomatique de la géométrie euclidienne (Notons que Tarski et George Birkhoff ont aussi proposé des théories axiomatiques de la géométrie euclidienne). La théorie de Hilbert repose sur 3 objets qui sont les points, les droites et les plans. Notons que celle proposée par Tarski est du premier ordre, elle ne repose que sur un seul objet.
Hilbert montre la consistance de sa théorie en se ramenant à celle des nombres réels. Ce qui met en avant le lien qui existe entre la géométrie et l'analyse. Pour cela il se donne un repère et associe à chaque point une couple de réels (ses *coordonnées*) et définit l'équation d'une droite ($ax+by+c=0$) et retrouve les axiomes à partir de calculs réels.

Théorème 13

Si la géométrie euclidienne n'est pas consistante, alors la théorie des nombres réels ne l'est pas non plus.

En 1931 (mais publié en 1951 dans *A Decision Method for Elementary Algebra and Geometry*), Tarski montre quant à lui que la géométrie euclidienne est complète (du moins pour la théorie axiomatique qu'il propose).

4 Bibliographie et ressources

4.1 Bibliographie

[SEU] Collectif, « Le théorème de Gödel », ISBN-13 : 9782020327787, chez les Éditions du Seuil (1997) :
[SEU1] Ernest Nagel, James R. Newman, « La démonstration de Gödel » (orig : « Gödel's proof » (1958)). Traduit de l'anglais par Jean-Baptiste Scherrer.
[SEU2] Kurt Gödel, « Sur les propositions formellement indécidables de *Principia Mathematica* et des systèmes apparentés I » (orig : « Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme, I. » (1931)). Traduit de l'allemand par Jean-Baptiste Scherrer.
[SEU3] Jean-Yves Girard, « Le champ du signe ou la faillite du réductionnisme ».
[MEN] Elliott Mendelson, « Introduction to Mathematical Logic », ISBN-13 : 9781584888765 5^{e} édition (2009) chez Chapman & Hall/CRC.
[EWA1] William Bragg Ewald, « From Kant to Hilbert : A Source Book in the Foundations of Mathematics, vol. I », ISBN-13 : 9780198505358, chez Oxford University Press (2004).
[EWA2] William Bragg Ewald, « From Kant to Hilbert : A Source Book in the

Foundations of Mathematics, vol. II », ISBN-13 : 9780198505365, chez Oxford University Press (2005).
[HEI] Jean van Heijenoort, « From Frege to Godel : A Source Book in Mathematical Logic, 1879-1931 », ISBN-13 : 9780674324497, nouvelle édition (1990) chez Harvard University Press.
[GOS] Bernard Gostiaux, « Cours de mathématiques spéciales, tome 1 : Algèbre », ISBN-13 : 9782130458357, chez les Presses Universitaires de France - PUF (1 août 1993).
[GIR] Jean-Yves Girard, « Le Point Aveugle : Tome 1. Cours de Logique, Vers la perfection », ISBN-13 : 9782705666330 chez Hermann (2006).
[BEL] Jean-Pierre Belna, « Histoire de la théorie des ensembles », ISBN-13 : 9782729851668 chez Ellipses (2009).

4.2 Ressources disponibles sur internet

[KLE] `http://people.umass.edu/klement/513/` Kevin C. Klement, « Phil 513 : Mathematical Logic I ».
[CHR] `http://www.chronomath.com/` Serge Mehl, « ChronoMath, une chronologie des MATHÉMATIQUES ».
[CMA] `http://www.dma.ens.fr/culturemath/` « CultureMATH ».
[GBR] `http://drame-subjectif-de-cantor.net/girardbrini.pdf` « L'argument diagonal revient à repérer un point fixe ».

Ainsi que par exemple `http://gallica.bnf.fr/` et `http://www.springerlink.com/` pour les documents anciens cités ici.