Version préliminaire, incomplète
Commentaires très appréciés
Chapitre III

Giuseppe Longo
longo (at) di (dot) ens.fr
http://www.di.ens.fr/users/longo/

Introduction aux Théorèmes d'Incomplétude: de Gödel à Kruskal-Friedman

0. L'essentiel des chapitres précédents : la déduction minimale

Le système implicatif minimal, en termes de déduction naturelle et où $\Gamma \vdash A$ veut dire que les hypothèses Γ permettent de déduire A, a seulement deux règles de déduction de base : l'introduction de l'implication, $(\rightarrow I)$, où $[A]$ indique que A est "déchargée" (voir plus bas), et l'élimination de l'implication, $(\rightarrow E)$:

Règle d'introduction	Règle d'élimination
$(\rightarrow I)$ $\dfrac{\Gamma, [A] \vdash B}{\Gamma \vdash A \rightarrow B}$	$(\rightarrow E)$ $\dfrac{\Gamma \vdash A \qquad \Delta \vdash A \rightarrow B}{\Gamma, \Delta \vdash B}$

Dans $(\rightarrow I)$, A est déchargée, dans le sens qu'elle n'est pas une hypothèse nécessaire à la validité de $(A \rightarrow B)$, la conséquence.

La règle $(\rightarrow I)$ transfère dans le *langage* des formules la déduction *métalinguistique* $A \vdash B$. C'est-à-dire, elle affirme que de la déduction (métalinguistique) de B à partir de A, on peut déduire la formule, du langage, $(A \rightarrow B)$. Le lecteur reconnaîtra dans $(\rightarrow E)$ la règle que les ancêtres romains de l'auteur de ces notes appelaient "modus ponens": si A et A implique B, alors B.

1. Négation et premier ordre.

Le langage des mathématiques, en particulier de l'Arithmétique, est toutefois plus riche que celui basé sur les formules introduites jusqu'à présent: on a au moins besoin de la *négation* et, ce qui est bien important, des *variables*.

Une première extension permettra d'exprimer formellement la négation. Ensuite on parlera des variables, *dans les* formules (premier ordre, cette section) et *de* formules (second ordre, voir chapitre 4, en préparation), donc de *quantification*. L'intérêt de l'Arithmétique d'autre part doit être clair: elle est la Théorie (Formelle) des Nombres et cette théorie est au coeur des mathématiques et, depuis Cantor et Dedekind, fondement de l'Analyse.

Négation

Ajoutons d'abord le "**faux**", $\bot$, et la règle "ex-falso quodlibet":

$$(F) \qquad \Gamma, \bot \vdash A$$

Cette règle a des contreparties simples en Théorie des Types et en Théorie des Catégories. Toutefois, on ne développera plus ces analogies, dans cette note introductive, car leur simplicité est grande dans le cas propositionnel "positif", sans négation ni quantification, mais elle présente des difficultés techniques dans les autres[1].

On peut maintenant utiliser $\bot$ pour *définir* la négation:

$$(\neg) \qquad \neg A \equiv (A \to \bot)$$

D'où on peut dériver les deux règles suivantes, à partir de $(\to I)$ et $(\to E)$:

$$(\neg I) \quad \frac{\Gamma, [A] \vdash \bot}{\Gamma \vdash \neg A} \qquad (\neg E) \quad \frac{\Gamma \vdash A \qquad \Gamma \vdash \neg A}{\Gamma \vdash \bot}$$

Dans ce contexte, intuitionniste, on peut dériver la règle de la **contrapposition**:

(Contrap.) $A \to B \vdash (\neg B) \to (\neg A)$

ainsi que:

(Double neg.) $A \vdash \neg\neg A$

---

[1] $\bot$ est l'objet initial, en langage catégorique. La quantification correspond à des produits, fibrés ou indexés [Lambek&Scott,1989; Asperti&Longo,1991].

Exercice: complétez les preuves:

$$\dfrac{\dfrac{A \quad [\neg A]}{\bot}}{\neg\neg A}$$

$$\dfrac{\dfrac{[A] \quad A \to B}{B} \qquad \neg B}{\dfrac{\bot}{\neg A}}$$

Exercice: Réfléchir au fait que, dans la preuve de (Contrap.), à la place de $\neg A$, on aurait pu mettre "n'importe quoi", mais, dans ce cas, A n'aurait pas été effacé ... . Et dans la preuve de (Double neg.) ?
Observez que (Contrap.) implique

$$A \leftrightarrow B \ \vdash \ (\neg\neg A) \leftrightarrow (\neg\neg B).$$

Définition

- Une théorie T est **contradictoire** s'il existe une proposition A telle que $T \vdash A$ et $T \vdash \neg A$.
- Une théorie est **cohérente** s'elle n'est pas contradictoire.
- Une théorie est **complète** si pour tout A, on a $T \vdash A$ ou $T \vdash \neg A$.

Logique Classique

On passe à la logique classique, en ajoutant simplement l'axiome du "*tertium non datur*":

$$A + \neg A$$

Cet axiome est équivalent, dans notre système, à l'implication $\neg\neg A \to A$.
Notez que $\neg A \to \bot \vdash A$ est la preuve classique par absurde. En logique intuittionniste on a seulement $A \to \bot \vdash \neg A$, par définition.

Supposons $A + \neg A$. Puisque $\bot \vdash A$ et $A \vdash A$, on a

(0) $\bot + A \vdash A$ par (+E)

(1) $(A \to \bot), ((A \to \bot) \to \bot) \vdash \bot + A$ par $(\to E)$ et $(+I)$;

mais aussi $A \vdash \bot + A$ par (+I); donc

(2) $A, ((A \to \bot) \to \bot) \vdash \bot + A$.

A partir de (1), (2) et (+E), on a

$$A+(A \to \bot), ((A \to \bot) \to \bot) \vdash \bot+A.$$

Enfin (0) implique que $A + \neg A \vdash \neg\neg A \to A$.

En utilisant , $A+B \to C \vdash (A \to C)\times(B \to C)$ on démontre facilement (bon courage!) que $\neg\neg A \to A \vdash A + \neg A$. Un exercice permet de démontrer que

(Contrap.¬) $(\neg B) \to (\neg A) \vdash A \to \neg\neg B$

qui donne $(\neg B) \to (\neg A) \vdash A \to B$ dans le système classique.

Le Premier Ordre

Il n'y a pas de mathématiques sans les **variables**. Elle sont gérées, logiquement, par les **quantificateurs**, les "pour tout x ... " et "il existe x ..." habituels. Formellement, les règles pour la quantification des variables (du premier ordre ou variables d'individus) sont les suivantes:

$$(\forall I) \quad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A} \qquad (\forall E) \quad \frac{\Gamma \vdash \forall x.A}{\Gamma \vdash [t/x]A}$$

(Note: dans (∀I) il faut que x ne soit pas libre dans une proposition de Γ)

$$(\exists I) \quad \frac{\Gamma \vdash [t/x]A}{\Gamma \vdash \exists x.A} \qquad (\exists E) \quad \frac{\Gamma \vdash \exists x.A \quad \Gamma \vdash \forall x.(A \to B)}{\Gamma \vdash B}$$

(Note: dans (∃E) il faut que x ne soit pas libre dans B)

Exercice: Introduisez un nouveau symbol, "=" (égalité), et écrivez les axiomes de l'égalité.

Voila tout ce qu'il faut pour parler des variables mathématiques ordinnaires (ou "individuelles" ou du premier ordre).

2. L'Arithmétique intuitionniste et classique

Une théorie bien fondamentale du premier ordre est l'Arithmétique. Elle la "Théorie Formelle des Nombres" (et les nombres sont bien important en Mathématiques!). On l'appellera de Heyting (HA), si la logique sous-jacente est constructive, et de Peano

(PA), si la logique est classique. Elle se base sur les constantes et les axiomes propres suivants:

$0 : Nat$, $S : Nat \rightarrow Nat$ (l'entier 0 et la fonction successeur)

$\forall x.\neg(Sx = 0)$, $\forall x.\forall y.(Sx = Sy \rightarrow x = y)$ (0 est différent de 1 et S est injective)

$[0/x]A \rightarrow (\forall y.([y/x]A \rightarrow [Sy/x]A) \rightarrow \forall x.A)$ (Induction)

Exercice Définissez la somme et la multiplication sur les nombres entiers, à partir de 0 et S; e.g. $x+0 = x$ et $x+Sy = S(x+y)$ etc. ...

On écrira $HA \vdash A$, si A est un théorème dérivable à partir des axiomes de l'Arithmétique dans un cadre constructif, $PA \vdash A$ autrement.

Est-ce l'Arithmétique, HA ou PA, cohérente? On pourrait croire qu'elle l'est par un argument "élémentaire": l'ensemble (standard) des nombres entiers est un "modèle" des (vérifie les) axiomes et les règles. C'est-à-dire, on pourrait essayer de démontrer que les nombres vérifient tous les axiomes et observer que les règles d'inférence préservent la validité; donc toute proposition, démontrée dans le système, serait vrai. Ce qui entraîne qu'il ne peut pas déduire une proposition et son contraire, donc la cohérence. Mais comment le démontrer? C'est facile, on pourrait croire : par induction sur la longueur ou sur la structure des propositions, en utilisant un prédicat de vérité (e.g. en montrant, par induction, que les règles d'inférence préservent la vérité). Donc on aurait, *par induction*, une preuve de la cohérence de l'Arithmétique, dont l'axiome clé est ... *l'induction* ... (de plus, il faudrait "parler de la vérité" des propositions, tache pas moindre). Il y a là quelque chose qui cloche. Dans cette fissure logique s'infiltre le théorème de Gödel.

3. Les théorèmes d'Incomplétude de Gödel

On verra ici l'essentiel "logique" de la preuve Gödel du premier et du deuxième théorème: l'argument diagonal. On sera obligé de ne pas voir dans les détails le "lemme de représentation", pour le quel on renvoi à [Smorinski,1978]. Le raisonnement peut être entièrement développé dans un cadre constructif, pour la théorie, HA, ainsi que pour la métathéorie (ce qui n'est pas fait dans [Smorinski,1978], qui utilise un cadre classique, sauf pour le lemme de représentation: ce lemme est une *construction* par excellence). Toutefois, puisque tout résultat indépendant de PA est a fortiori

indépendant de HA, qui en est un sous-système, on démontrera l'incomplétude de PA, tout en respectant la constructivité de la preuve au niveau métalinguistique.

On partira justement de l'énoncé du lemme de représentation, qui peut être articulé en deux parties, (Rappr.1) et (Rappr.2) dessous. Pour le reste on simplifiera l'argument de Gödel (à la Rosser, 1936: cohérence au lieu de "ω–cohérence[2]"), sans conséquences, toutefois, logiques ni philosophiques (la non-utilisation de la ω–cohérence mène à un petit abus téchnique, dont le lecteur nous pardonnera : pour tous les détails nous renvoyons encore une fois à la présentation dans [Smorinski,1978]).

La première remarque importante, évidente après ce que nous avons vu, c'est que les preuves formelles sont des calculs. Plus précisément, elles sont des "fonctions calculables". Toutefois, les fonctions mathématiques ont des domaines de définition "mathématiques": les nombres entiers, les réels ... . Voila donc le premier apport technique de Gödel : pour formaliser cette idée, il donna une notion précise de fonction calculable. Mais il a fallut aussi coder avec les entiers les formules de l'Arithmétique: l'autre grande idée, la "gödelisation". Du point de vue technique, c'est très simple: associez aux symboles de bases des entiers (des nombres premiers), composez-les par des produits ou des exponentiels pour coder les formules composées, réarrangez dans l'ordre les nombres qui codent des formules et vous aurez même une correspondance bijective et effective ou calculable (on vient d'en décrire les calculs) entre entiers et formules. Bref, chaque formule bien-formée est – correspond à - un nombre (et viceversa).

Appelons $\underline{A}$ le numéro (de Gödel) de la formule A[3].

Mais alors aussi un *théorème*, une fois codé, n'est qu'un nombre que l'on obtient d'une façon effective, par des calculs (l'application des règles un nombre fini de fois), à partir des nombres qui codent les axiomes. Le travail déjà fait dans ces notes et qui a permis de voir les preuves formelles comme termes du λ–calcul (de Church, '32), devrait aider à comprendre l'effectivité de la procedure : nous avons vu que chaque preuve est un terme, en fait un programme, donc une fonction calculable. Gödel, avant Church, donne une définition de fonction calculable, ou "(partielle) recursive", exactement dans le même but, exprimer l'effectivité de la preuve. Puisque, depuis 1936, on sait que la classe de fonctions définissables par les λ–termes (non-typés) est la même

---

[2] PA est ω–cohérente s'il n'y a aucune formule $A(x)$ telle que PA démontre $\neg A(n)$ pour tout entier n, et, toutefois, PA démontre aussi $\exists x.A(x)$. Bien évidemment, tout système ω–cohérent est cohérent.

[3] Gödelization, tel que proposé par son auteur, en 1931:
Aux symboles de base de PA : 0, S, ¬, ∨, ∀, (,), ...
on associe 1, 3, 5, 7, 9, 11, 13, ... (impaires). Donc : $\underline{S} = 3$
Termes (et formules):
$\underline{1} = \underline{S(0)} = 2^3 3^{11} 5^{17^{13}}$ (exposants de nombres premiers). Et ainsi de suite.

que celle des fonctions calculable à la Gödel (partielles récursives), nous pouvons nous passer de la définition donné par Gödel et parler de *fonction calculable* sans ultérieurement spécifier dans quel système : ils sont tous équivalents.

Le lecteur devrait bien comprendre l'importance de cette démarche de Gödel. Pour un système formel donné, une *théorie* donc, la notion de déduction est une notion *metathéorique* : dans le cas de l'arithmétique formelle, Gödel encode cette notion *dans la théorie* elle-même. Pour résumer très informellement ce que l'on va voir, il donne alors un version syntactique du paradoxe du menteur ("cette phrase est fausse") en remplaçant "fausse" par "non démontrable" ("cette phrase n'est pas démontrable") et ... il démontre qu'elle n'est pas démontrable, ni elle ni sa négation. Une des conséquence de cette technique de preuve est qu'elle détruit le notion absolue de "meta", car, modulo un codage, la metathéorie finitiste (comme doit être toute metathéorie dans un cadre formel) d'une théorie qui contient PA, peut être considérer comme une sous-théorie de la théorie en question. Bref, la notion de metathéorie est bien commode, mais elle n'a pas de fondement logique ; mieux, elle n'aide en rien la discussion fondationnelle, car elle "se réduit" à la théorie qu'elle prétend analyser, voire justifier.

Soit donc PR l'ensemble des **fonctions calculables** (partielle récursives[4], donc, ou, ce qui est pareil, les fonctions calculées par le λ-calcul sans types). La première partie de la représentation dit que la procédure de démonstration est une fonction dans PR (nous avons vu, au moins pour le calcul propositionnel, qu'elle est - calculable par - un λ-terme). Le lecteur passionné peut bien suivre le parcours originel de Gödel, dans son article, où, pas à pas, il écrit dans le langage de PA des fonctions récursives neg(x), imp(x,y)… définissable donc en PA, telles que:

$$PA \vdash neg(\underline{A}) = \underline{\neg A}\ ,\ PA \vdash imp(\underline{A},\underline{B}) = \underline{A \to B}\ \ ....$$

On rappellera plus bas, aussi la définition de la function de substitution syntactique, sub ; c'est-à-dire de la function telle que : $PA \vdash sub(b,\underline{A(x)}) = \underline{[b/x]A}$.

Lemme (Rappr. 1) *Il existe une fonction th∈PR telle que:*

$$\textbf{(R1)} \quad th(\underline{A}) = 1 \ \Leftrightarrow\ PA \vdash A$$

La deuxième partie, plus difficile, assure que toute fonction calculable peut être représentée dans l'Arithmétique. Par un abus de langage, on pourra écrire

- A(x) pour mettre en évidence que x apparaît libre dans A,
- n pour S(...(S(0)...) n-fois,

[4] En fait, pour les buts du lemme de représentation, il suffit de représenter en Arithmétique les fonctions primitives récursives, une sous-classe des fonctions totales récursives. Notre travail sur le λ-calcul nous permet de concevoir des écritures formelles pour toutes les fonctions partielles récursives.

- A(n) pour [n/x]A, s'il n'y a pas d'ambiguïtés.

Comme d'habitude, f(n) = m veut dire que la fonction f est convergente (définie) sur n avec valeur m. Premier grand programmateur de l'histoire, Gödel écrit en "langage machine" (le langage de PA, avec 0, successeur…) toutes les fonctions effectives qui concernent la déduction formelle. Cette activité, d'une grande difficulté technique, s'étend facilement des fonctions récursives primitives, utilisées dans son article fondateur, à toutes le fonctions calculables (partielles recursives, PR).

Lemme (Rappr. 2) *Pour toute fonction (unaire) $f \in PR$, il existe une formule $A_f(x,y)$ de PA telle que:*

$$\textbf{(R2)} \qquad f(n) = m \quad \Leftrightarrow \quad PA \vdash A_f(n,m)$$

Une conséquence immédiate des lemmes R1 et R2 est la suivante:

Corollaire. *Il existe alors une formule Theor(x), telle que:*

$$\textbf{(R3)} \qquad PA \vdash A \quad \Leftrightarrow \quad PA \vdash Theor(\underline{A})$$

Pr. Soit th la fonction du lemme R1. En utilisant le lemme R2, posons Theor(x) $\equiv A_{th}(x,1)$[5]. ⊗

Encore une fois, cette esquisse de la preuve de Gödel, basée sur les seuls énoncés des grands lemmes de représentation, contient des abus techniques importants, dont le lecteur nous pardonnera (en se référant au texte originaire de Gödel ou à ses nombreuses présentations). D'une part, on a prétendu, en passant par le λ-calcul, de représenter en PA toutes les fonctions partielles récursives, ce qui est un abus et qui n'est pas strictement nécessaire. D'autre part, on est passé de façon cavalière sur la condition de ω-cohérence, qui, dans la version originaire de Gödel, est nécessaire à démontrer l'implication de droite à gauche en **(R3)**. Toutefois, ces abus techniques sont tous facilement réparables et ne modifient en rien les grandes lignes de la preuve ci-dessous.

La construction du prédicat Theor, qui "internalise" dans le langage de l'Arithmétique la notion métalinguistique de preuve, se fait pas à pas dans les lemmes mentionnés, en

[5] L'hypothèse de ω–cohérence est ici omise, mais elle garantie, dans la démonstration de Gödel de droite a gauche, que la preuve de Theor(A), qui est un énoncé existentiel (il *existe* - un t qui est le code de - une preuve de A) soit vrai sur les entiers (donc que l'on ait une "vrai" preuve : une extension cohérente de PA peut démontrer des énoncés existentiels faux sur les entiers standards - une conséquence justement… du théorème de Gödel).

décrivant, à l'intérieur de l'Arithmétique, les règles logiques, en fait la démontrabilité elle même. En particulier, on a:

(Int1) PA |— Theor(A)×Theor(A → B) → Theor(B)
(Int2) PA |— Theor(A) → Theor(Theor(A))
(Int3) PA |— (Theor(A) → Theor(B))×(Theor(A) → Theor(C)) →
→ (Theor(A) → Theor(B×C))

Nous avons déjà vu, grâce au λ-calcul, comme la notion de "substitution d'une variable par un terme" (l'axiome β) n'est pas seulement une opération effective, une manipulation mécanique de symbole, mais elle est "le centre du monde (de la calculabilité)": elle suffit à tout exprimer. Cette opération est aussi au coeur du théorème de Gödel; la seule différence est que l'on substituera un terme de l'arithmétique à la place d'une variable, dans une formule (modulo un codage). Comme pour le λ-calcul, avec l'axiome (β), la substitution peut être exprimée au niveau linguistique[6]: il existe donc, dans le langage de l'Arithmétique, une fonction binaire sub qui, pour tout terme b et formule A de PA, remplace toutes les occurences de la première variable libre, disons x, en A (si elle existe) par b. C'est à dire :

(sub) PA |— sub(b,A(x)) = [b/x]A .

Comme convenu, on peut aussi écrire A(b) pour [b/x]A. Notez que sub prends le premier en tant que terme et le deuxième comme (le code de) une formule; sub remplace ensuite toute occurrence de x dans la formule avec le premier et calcule le code du résultat. Tout est "effectif" et l'invention très originale de Gödel, pour son époque, reviendrait aujourd'hui à un exercice de programmation: Gödel a programmé, premier programmeur du siècle, la fonction de substitution dans le langage de l'Arithmétique ! (exercice très long et ennuyeux, mais implémentation d'une idée formidable).

On obtient, en particulier:

(R4) PA |— Theor(sub(b,A(x))) ↔ Theor([b/x]A).

On peut maintenant commencer à écrire, par une méthode diagonale, la proposition qui dit de soi même "cette formule n'est pas un théorème", en observant que sub est une fonction binaire ou de deux *variables*. Posons donc:

---

[6] Voir aussi le morphismes "eval", dans les Catégories Cartésiennes fermées définies plus haut.

$$G(x) \equiv \neg Theor(sub(x,x))$$

(Premier pas de la "diagonalisation": (x,x) est sur la "diagonale" du produit cartésien). Puisque G contient (exactement) x libre, on a écrit G(x) pour G, suivant notre convention. Soit $m = \underline{G(x)}$ (m est donc le code de G(x)). On a alors

$$G(m) \equiv \neg Theor(sub(m,m))$$

d'où :

$$G(m) \equiv \neg Theor(sub(m,\underline{G(x)}))$$

et

(R5) $PA \vdash G(m) \leftrightarrow \neg Theor(\underline{G(m)})$ par **(R4)**

G(m) est donc un "point fixe" de ¬Theor et elle sera la formule qui n'est pas démontrable. (Grâce à nos conventions, on a pu écrire $G(m) \equiv [m/x]G$, car G contient exactement x libre; en fait, G(m), en tant que point fixe de ¬Theor, peut-être comprise, *très informelement*, comme étant la formule que dit de sois même: "je ne suis pas démontrable".)

Théorème (Premier d'Incomplétude) *Si PA est cohérente, alors* $PA \not\vdash G(m)$ *et* $PA \not\vdash \neg G(m)$.

Pr. On utilisera l'hypothèse de cohérence de l'Arithmétique par contrapposition (par absurde) dans le métalangage (la règle dérivée (Contrap.)). Supposons donc que PA soit complète.

Supposons alors et d'abord, par absurde, que $PA \vdash G(m)$. Alors

$$PA \vdash G(m) \Rightarrow PA \vdash \neg Theor(\underline{G(m)}) \quad \text{par (R5).}$$

Mais aussi

$$PA \vdash G(m) \Rightarrow PA \vdash Theor(\underline{G(m)}) \quad \text{par (R3)}$$

une contradiction.

D'autre part, si l'on suppose $PA \vdash \neg G(m)$, l'autre alternative possible, on a

$PA \vdash \neg G(m) \Leftrightarrow PA \vdash \neg\neg Theor(\underline{G(m)})$ par (R5) et (Contrap) deux fois.

Or, $PA \vdash \neg\neg Theor(\underline{G(m)})$ et $PA \vdash Theor(\underline{G(m)})$ sont, classiquement, équivalents. De l'implication de droite à gauche en (R3), on déduit alors

$PA \vdash G(m)$, en contradiction avec l'hypothèse. ⊗

Par conséquent, l'Arithmétique, si elle est cohérente, est incomplète, car elle contient une proposition indécidable.

On pourrait se demander, maintenant, si $G(m) \equiv \neg Theor(sub(m,\underline{G(x)}))$ est "vraie". L'ontologie platonicienne naïve, en mathématiques et en philosophie, trouve dans G(m) un exemple de la "magie" des mathématiques: une proposition vraie, mais "indémontrable". Non, le premier théorème d'Incomplétude démontre "seulement"

qu'on ne peut pas démontrer cette proposition, ni sa négation, avec *les principes de preuve* de l'Arithmétique. C'est-à-dire, il démontre qu'elle est indécidable; en particulier, donc, G(m) n'est pas démontrable, dans PA. Aucune mention n'est faite de "vérité" quoique ce soit. Toutefois, puisque G(m) dit formellement (après beaucoup de codage) que "je ne suis pas démontrable", on pourrai déjà affirmer, naïvement, qu'on a *démontré* sa "vérité", sans qu'elle soit démontrable dans PA (!), car il est vrai que "G(m) n'est pas démontrable", dans PA (!). Plus exactement on pourrait *dériver*, une fois donnée une bonne notion de vérité, que, *si PA est cohérente* (cette hypothèse est essentielle!!), alors G(m) est vrai. Or, le deuxième théorème d'incomplétude *prouve* avec rigueur que, en hypothèse de cohérence de l'Arithmétique, G(m) est "vrai". En fait, le deuxième théorème démontre bien plus que cela : il démontre, *dans l'Arithmétique*, que G(m) est une conséquence de la cohérence. Le théorème formalise donc, dans, PA le raisonnement naïf plus haut : dérivez G(m) *à partir de* la cohérence. Par conséquent, on *démontrera*, en hypothèse de cohérence, que G(m) est vrai. Y-a-t-il d'autres méthodes pour savoir si un énoncé *mathématique* est vrai, sinon le démontrer?

Observons d'abord que la cohérence de l'Arithmétique est exprimable dans l'Arithmétique elle-même, grâce à Theor. Soit en fait

$$\mathrm{Coher}_{\mathrm{PA}} \equiv \neg \mathrm{Theor}(\bot).$$

C'est à dire, PA est cohérente, si $\bot$ (l'absurde) n'est pas un théorème. Or, par définition, l'Arithmétique est cohérente si et seulement si $\mathrm{Coher}_{\mathrm{PA}}$ est vraie[7] (comme propriété des nombres entiers).

Théorème (Deuxième d'Incomplétude) *PA* $\vdash$ $Coher_{PA} \leftrightarrow G(m)$.

Pr. ($\rightarrow$) Grâce à (Int2), on a:

$$\mathrm{PA} \vdash \mathrm{Theor}(\underline{\mathrm{G(m)}}) \rightarrow \mathrm{Theor}(\mathrm{Theor}(\underline{\mathrm{G(m)}})),$$

mais alors, par $A \vdash \neg\neg A$, (R5) et (Contrap.), avec aussi (Int1 et 2) :

(G2) $$\mathrm{PA} \vdash \mathrm{Theor}(\underline{\mathrm{G(m)}}) \rightarrow \mathrm{Theor}(\underline{\neg \mathrm{G(m)}}) .$$

Puisque, $$\mathrm{PA} \vdash \mathrm{Theor}(\underline{\mathrm{G(m)}}) \rightarrow \mathrm{Theor}(\underline{\mathrm{G(m)}}),$$

grâce à (Int3), on a :

$$\mathrm{PA} \vdash \mathrm{Theor}(\underline{\mathrm{G(m)}}) \rightarrow \mathrm{Theor}(\bot).$$

Par (Contrap.) et (R5):

$$\mathrm{PA} \vdash \neg \mathrm{Theor}(\bot) \rightarrow \mathrm{G(m)}$$

---

[7] Nous n'avons pas parlé avec rigueur d'une notion de vérité, sur des modèles mathématiques, car point nécessaire aux deux théorèmes d'incomplétudes: le lecteur peut faire confiance à son intuition de la vérité (ou, mieux, de validité sur une structure mathématique).

mais $\neg \mathrm{Theor}(\bot) \equiv \mathrm{Coher}_{PA}$.
Pour l'implication inverse, observez que

(G3) $\quad PA \vdash G(m) \rightarrow \neg \mathrm{Theor}(\underline{G(m)})$.

Or, $\vdash \bot \rightarrow G(m)$, par la règle (F) de la négation. Donc $PA \vdash \mathrm{Theor}(\underline{\bot \rightarrow G(m)})$ et
$PA \vdash \mathrm{Theor}(\bot) \rightarrow \mathrm{Theor}(\underline{G(m)})$, par (Int1). Alors, par (Contrap),

$$PA \vdash \neg \mathrm{Theor}(\underline{G(m)}) \rightarrow \neg \mathrm{Theor}(\bot)$$

donc

$$PA \vdash G(m) \rightarrow \neg \mathrm{Theor}(\bot) \qquad \otimes$$

Notez d'abord que le II théorème se base sur la preuve du I théorème. En particulier sur la construction de G dans (G2) et (G3).

Donc, si l'Arithmétique est cohérente, Coher_{PA} n'est pas démontrable dans l'Arithmétique, car G(m) ne l'est pas. Mais aussi:

Corollaire 1 (informel) *Si l'Arithmétique est cohérente, alors G(m) est "vrai".*
Pr. Conséquence immédiate du deuxième Théorème et de l'hypothèse que Coher_{PA} soit vraie. $\otimes$

Une autre conséquence du deuxième théorème est que le premier peut être *intériorisé* (pour l'ω-cohérence voir la note 2) :

Corollaire 2 $\quad PA + Coher_{PA} \vdash \neg Theor(\underline{G(m)})$.
$\quad PA + \omega\text{-}Coher_{PA} \vdash \neg Theor(\neg \underline{G(m)})$.

Pr. Pour la première dérivation : ce n'est que (→E) et (R5) appliqués à
$PA \vdash \mathrm{Coher}_{PA} \rightarrow G(m)$.
La deuxième dérivation est juste un peu plus compliquée. $\otimes$

Exercice: Démontrer les corollaires dans les détails, en sachant que la "vérité" d'une proposition sur la structure **N** des nombres entiers est une propriété "locale": on n'a pas besoin de vérifier d'avance que **N** est un "modèle" de PA. Réfléchir à leur "signification".

Où est-ce le regard du mathématicien "au dessus de l'épaule de Dieu" (Barrow) ou les effets tunnel-quantique dans le cerveau (Penrose), qui nous garantiraient la vérité de G? On vient de *démontrer* G(m), en hypothèse de cohérence.

Y-a-t-il d'autres énoncé qui "sont vrais", mais indémontrables? Oui, certainement, dans la §.4 on en verra un autre, mais, comme pour G, il faudra *démontrer* qu'il est indémontrable (en disant dans quelle théorie il est indémontrable, PA en fait) et il faudra *démontrer* qu'il est vrai, en précisant quels principes de preuve (ou "de construction", on dira) on utilise pour cette dernière preuve, quelle théorie permet de le faire. Pour démontrer (la vérité de) G, en hypothèse de cohérence, il a suffit un petit jeu syntactique, basé sur le fait que G et la cohérence, formalisée, sont donnés, les deux, en utilisant la négation du prédicat Theor. Les "bla, bla" informels que les teneurs de la vérité miraculeuse de G racontent souvent ("G dit qu'elle n'est pas démontrable ; *puisque*, de la cohérence, on dérive son indémontrabilité, *alors* elle est vrai"), sont des mauvaises paraphrases de la preuve formelle "$PA \vdash Coher_{PA} \rightarrow G(m)$".

Mais, est-ce que la cohérence est vraie? Les deux théorèmes de Gödel ne disent rien à ce sujet; ils donnent au plus des conséquences de la cohérence possible de PA, c'est-à-dire l'existence d'énoncés indécidables, *dont l'énoncé formel de la cohérence elle-même*. Encore une fois, dire que G est vrai par évidence ou par miracle équivaut à dire que la cohérence de PA est vraie par évidence ou miracle, car l'équivalence de G et $Coher_{PA}$ est bien simple. Depuis Gentzen, il y a eu 60 d'acharnement au sujet des preuves de cohérence de PA. On en verra des traces plus bas dans la discussion des énoncés concrets d'incomplétude.

Remarque principale (le rôle de la cohérence)

Rappelons encore une fois que les preuves des deux théorème d'incomplétude sont conduites à un niveau purement formel sans aucune référence à la notion de vérité, ni de "sémantique" d'aucun genre. En particulier, quant au premier théorème, on démontre :

$$(PA \vdash G(m) \Rightarrow Contrad) \textit{ et } (PA \vdash \neg G(m) \Rightarrow Contrad)$$

dont on a déduit

$$(Cohérence \Rightarrow PA \not\vdash G(m)) \textit{ et } (Cohérence \Rightarrow PA \not\vdash \neg G(m)),$$

donc

$$(Cohérence \Rightarrow (PA \not\vdash G(m) \textit{ et } PA \not\vdash \neg G(m))).$$

Dont la surprise encore plus grande du deuxième théorème, car $Coher_{PA}$ formalise la cohérence:

$$PA \vdash Coher_{PA} \rightarrow G(m).$$

Voilà l'extraordinaire calembour de Gödel : si on suppose sa cohérence, PA ne dit rien sur G. Mais si on formalise cette hypothèse de cohérence dans le langage de PA, elle *implique* G, *dans* PA (!).

Autres Remarques 1 - Le lecteur aura noté que les démonstrations n'utilisent que des règles de HA. Même au niveau de la théorie donc, elles sont intuitionnistes: toutefois, on a, d'un seul coup, démontré l'indépendance de G(m) aussi par rapport à PA (et donc HA).

2 - En effet, cette preuve s'applique à n'importe quelle théorie axiomatique qui contienne HA ou, plus précisement, à n'importe quelle théorie qui permette de representer sa métathéorie, c'est à dire, qui réalise (R3), (sub), (Int1,2,3). Bref, PA n'est pas seulement incomplète, elle est en fait *incomplétable* (PA ne possède aucune extension formelle cohérente et complète).

3 - Il doit être évidente que le raisonnement métathéorique a été toujours intuitionniste. Par exemple, la preuve du premier théorème d'incomplétude, Cohérente $\Rightarrow$ Non Complète, a été donné, dans le métalangage, par (Contrap.) à partir de Complète $\Rightarrow$ Contradictoire; plus précisement, de

$$(\text{PA} \vdash \text{G(m)} \Rightarrow \text{Contrad}) \textit{ et } (\text{PA} \vdash \neg\text{G(m)} \Rightarrow \text{Contrad})$$

on a déduit

$$(\text{Cohérence} \Rightarrow \text{PA} \not\vdash \text{G(m)}) \textit{ et } (\text{Cohérence} \Rightarrow \text{PA} \not\vdash \neg\text{G(m)}).$$

4 - On donnera, à la fin de ce cours, une démonstration de la cohérence de HA, par des principes "en dehors" de PA (et HA), mais tout à fait "constructifs".

5 - Le deuxième théorème est donc une équivalence:

$$\text{PA} \vdash \text{Coher}_{\text{PA}} \leftrightarrow \text{G(m)}.$$

Cece implique que la proposition indécidable correspond à la cohérence, à équivalence (facilement) démontrable près, ou que sa vérité est aussi forte que l'hypothèse de la cohérence de PA: on démontre l'une en supposant l'autre. Où serait alors, disions-nous, cette "évidence magique" de la vérité de G ? Elle est la même que l'évidence de la cohérence.

6 - Certains déduisent la vérité de G(m) d'une hypothèse métathéorique classique: "tout énoncé (sans variables libres) est vrais ou faux". Il s'agit d'une hypothèse forte sur la métathéorie, appelée "classique", mais pas très "mathématique", car les mathématiciens *démontrent* ce qu'ils affirment, même en dehors de PA, si nécessaire: dans ce cas, un mathématicien essayerait de démontrer l'énoncé ou de démontrer sa négation. Or, en faisant pour un instant cette hypothèse, considérons le prédicat Theor qui permet de définir $\text{G(m)} \equiv \neg\text{Theor}(\text{sub}(\text{m},\underline{\text{G(x)}}))$.

En fait, Theor(x) a la structure $\exists$yPreuve(y,x) (il existe une preuve y de x, preuve qui est codable par y en tant que suite finie de propositions). Si G(m) ou sa négation, $\neg$G(m), sont nécessairement vrais, supposons alors que $\neg$G(m) soit vrai. Puisque

$$\text{PA} \vdash \neg\text{G(m)} \leftrightarrow \neg\neg\exists\text{yPreuve}(\text{y},\underline{\text{G(m)}}) \quad \textit{et}$$
$$\text{PA} \vdash \neg\neg\exists\text{yPreuve}(\text{y},\underline{\text{G(m)}}) \leftrightarrow \exists\text{yPreuve}(\text{y},\underline{\text{G(m)}})$$

alors, la vérité de ¬G(m) équivaut à la vérité de ∃yPreuve(y,G(m)). Or, si une proposition, qui est la quantification existentielle d'un énoncé décidable, comme Preuve(y,x) qui est décidable en x et y, est vrai sur les nombres entiers, alors elle est démontrable dans PA (en fait HA) : il suffit d'énumérer les entiers l'un après l'autre et vérifier effectivement l'énoncé; s'il est vrai, tôt ou tard on le démontrera, en trouvant l'entier qui le réalise (dans PA on décrit toutes les procédures effectives, voir Lemme (Rappr.1 et 2)). Mais, puisque, *en hypothèse de cohérence,* ¬G(m) est indémontrable (premier théorème), alors ¬G(m), en tant qu'énoncé existentiel, est faux. Il ne reste, en hypothèses classiques, que la vérité de G(m).
Remarquez, toutefois que pour cette preuve, on a dû supposer la cohérence de PA. Donc, il vaut mieux utiliser directement le deuxième théorème, comme dans son corollaire, sans faire des fortes hypothèses classiques sur la "vérité".

Remarques sur le "méta".

Nous avons fait à maintes reprises une distinction, très commode, entre méta-langage (méta-théorie) et langage (théorie). Cela est bien commode, tout comme écrire des notes en rouge en marge d'un de ses propres textes pour les distinguer du récit principal. Toutefois, cette distinction n'a aucune valeur fondationnelle, elle ne fonde pas le discours mathématique, à partir d'un dehors linguistique, comme espéré dans l'approche d'Hilbert (et de Tarski). Hilbert, au début des années '20, en insistant sur cette différence fondatrice du logique, a même essayé de démontrer la cohérence de PA par méta-induction sur la profondeur des preuves. Pourquoi la méta-induction ? Une quinzaine d'années auparavant, il avait cru de pouvoir la démontrer par induction, tout en suscitant le grand rire de Poincaré : démontrer par induction la cohérence d'une théorie dont l'axiome principal est l'induction ? Voilà donc la tentative méta-théorique qui accorde, dans le cadre de tout le discours fondationnel hilbertien, ce rôle crucial au méta. Face à cette deuxième tentative, méta-théorique, ce sera « son meilleur élève », Hermann Weyl, qui lui fera remarquer que sa méta-induction… ce n'est que de l'induction (voir aussi les remarques de Wittgenstein ci-dessous).

Or, le théorème de Gödel, plus précisément sa preuve, nous dit exactement ce que Weyl (et Wittgenstein) avait saisi : la métathéorie n'est pas plus expressive que la théorie, car on peut l'encoder dans la théorie, sans perte de déductibilité (les lemmes de représentation). En plus, la cohérence, codée dans la théorie, permet de dériver G, ce qu'elle ne permet pas de faire au niveau méta-théorique. La méta-théorie de PA n'est donc qu'une sous-théorie de PA, modulo un codage. L'exact contraire de ce qu'espérait Hilbert. La preuve du théorème de normalisation de Girard (voir plus bas), en

mélangeant de façon essentielle méta-théorie et théorie dans une preuve de cohérence de l'Analyse (en tant qu'Arithmétique du II ordre), cassera ultérieurement le prétendu rôle fondationnel de cette distinction aussi commode qu'artificielle.

Des philosophies contre la "complétude".

Poincaré. Le désaccord d'Henri Poincaré avec la philosophie des mathématiques d'Hilbert est bien connu. Quelques citations permettent d'en résumer certains aspects :

1. « Pour MM. Peano et Hilbert les mathématiques sont comme le "piano raisonneur" de M. Jevons » [compte-rendu des "Fondements de la Géométrie" de Hilbert, 1899]
2. « M. Hilbert pense que les mathématiques sont comme la machine à saucisses de Chicago : on y introduit des axiomes et des porcs, et en sortent des saucisses et des théorèmes » [voir Bottazzini, 2000]
3. « Bien de fois déjà on a cru avoir résolu tous les problèmes, ou, tout au moins, avoir fait l'inventaire de ceux qui comportent une solution. Et puis le sens du mot solution s'est élargi, les problèmes insolubles sont devenus *les plus intéressants de tous* et d'autres problèmes se sont posés auxquels on n'avait pas songé » [1908].

Il y a là non seulement un désaccord sur les mathématiques, mais une différence fondamentale dans le regard sur la connaissance.

Weyl. Dans son livre *Das Kontinuum* (fin de la §. 3), Hermann Weyl, en 1918 (!) conjecture, quoi qu'en hésitant, l'incomplétude de l'Arithmétique : une remarque pas assez citée (« loup solitaire » à l'époque, comme il dira ensuite). Et cela dans un livre où maintes fois, contre le formalisme hilbertien, il souligne que l'idée de la « potentielle mecanizabilité des mathématiques les trivialise ».

Wittgenstein. Il existe un vaste débat sur la compréhension du théorème de Gödel de la part de Ludwig Wittgenstein. Citons juste quelques perles, dans des textes parfois si difficiles à déchiffrer de Wittgenstein, qui paraissent même précéder Gödel :

1. « Hilbert's metamathematics will turn out to be a disguised Mathematics» [Waismann, 1979],
2. « [A metamathematical proof] should be based on entirely different principles w.r. t. those of the proof of a proposition ... in no essential way there may exist a meta-mathematics » (voir Wittgenstein, Philo. Rem., § 153; quoted

in [Shanker,1988]) and

3. « I may play chess according to certain rules. But I may also invent a game where I play with the rules themselves. The pieces of the game are then the rules of chess and the rules of the game are, say, the rules of logic. In this case, I have *yet another game*, not a *metagame* » [Wittgenstein, 1968; p. 319]. On pourrait ajouter : on traite ce prétendu métajeu avec la même théorie des jeux, si elle s'applique.

4. Le Théorème de Kruskal et la Forme Finie de Friedman

Un ensemble (partiellement) ordonné est **bien ordonné**, si tout sous-ensemble non-vide possède un plus petit élément (voir §. 4.1). On démontre facilement que tout ensemble infini bien ordonné réalise l'induction formelle, c'est-à-dire (Ind.) de la §.2; l'implication inverse est clairement fausse, car les formules sont un ensemble dénombrable et la collection des sous-ensembles des entiers ne l'est pas.

Énoncé de cette façon, typiquement ensembliste, sur la suite infinie des nombres entiers, cet énoncé est "fortement" infinitaire : *tous* les sous-ensembles non-vides possèdent un plus petit élément (il est même imprédicatif, voir plus bas).

Pensez maintenant la suite des entiers comme bien ordonné dans votre espace mental. Sans entrer dans des réflexions cognitives, pour lesquelles on renvoi à [Bailly, Longo, 2006 ; chapitre 2], observons qu'un esprit suffisamment mathématisé voit cet ordre s'étaler vers l'infini projectif, en principe sur une droite. S'il considère un sous-ensemble *générique* non-vide, qui possède donc un élément, suite à la nature discrète de cet étalement croissant dans l'espace, il comprend bien que l'ensemble en question possède un plus petit élément (il doit y en avoir un, parmi le nombre fini qui précède l'élément qui garantit que l'ensemble est non-vide). Dans ce "jugement", qu'il est légitime d'appeler "géométrique" (on doit "voir" ou organiser l'ordre dans l'espace), la généricité de l'ensemble posé joue un rôle fondamental : comme partout en mathématique, en dehors de l'arithmétique et des ensembles inductifs, on démontre (ou on suppose) un énoncé quantifié universellement par un hypothèse de généricité (mon espace de Banach, mon triangle rectangle est *générique* – je n'ai utilisé dans la preuve que sa définition, voire il est un "invariant de la preuve" – donc mon théorème, mon hypothèse vaut pour *tous* les espaces de Banach, *tous* les triangles rectangles…).

Nous montrerons ici le rôle du principe structurel du bon ordre dans la preuve, en tant que jugement géométrique, grâce à un exemple relativement récent et de très grand intérêt: la version finie du Théorème de Kruskal due à Friedman, connue comme KF ou FFF (Friedman's Finite Form, paru en preprint en 1981, Ohio State Univ., voir [Harrington&al.,1985]). KF est un exemple récent et concret de l'incomplétude de l'Arithmétique formelle. Il est "concret", ou mathématique, car sa construction n'a pas une origine logique, comme les énoncés G ou Coher_{PA} de Gödel : il est une variante finie d'un théorème très intéressant pour les mathématiques des arbres ou graphes finis (Kruskal, 1960 ; voir plus bas).

Dans ce résultat, c'est donc la structure d'ordre, comme principe de construction mathématique, qui entre d'une façon essentielle (pour une analyse des *principes de constructions* vs. les *principes de preuve* en mathématiques et en physique, voir [Bailly, Longo, 2006]). C'est-à-dire, on donne un "simple" énoncé formalisable dans

l'Arithmétique, KF, que aucun principe de preuve purement syntactique et finitaire arrive à démontrer; toutefois, le travail sur les structures d'ordre des entiers, des arbres finis et infinis, permet de démontrer l'énoncé, comme propriété des nombres entiers. En d'autres termes, pour donner la preuve, même d'un "simple" énoncé sur les entiers, le mathématicien ne s'interdit pas de sortir du finitaire, voire de l'Arithmétique, et d'utiliser sur la structure, d'ordre dans ce cas, le bon ordre, voire des comparaisons entre suites infinies ou branches infinies d'arbres, des notions imprédicatives (voir plus bas). En bref, la "géométrie" de la droite des nombres, voire du plan (les arbres comme structures planaire), la pratique de l'infini dans la construction de suites bien ordonnées, qui s'est faite dans l'histoire, entrent d'une façon essentielle dans la construction, comme pourraient le faire maintes autres constructions possibles, les fonctions de variables complexes de la Théorie Analytique des Nombres, par exemple. Mais, dans ce cas, l'indémontrabilité formelle de l'énoncé est un théorème. Voilà donc un résultat qui se trouve dans le décalage entre principes de construction mathématiques et principes de preuve, dont on parlé pour identifier le "lieu" des théorèmes d'incomplétude.

4.1 - Pas de désordre total chez les arbres

Rappellons d'abord quelques notions sur les ensembles ordonnés. Une relation "$\leq$" est un **pre-ordre** si elle est réflexive et transitive. Un pre-ordre est un **ordre partiel** si il est aussi antisymétrique, c-à-d. $x \leq y$ et $y \leq x$ implique $x = y$. Un ordre partiel est **total**, si pour tout x et y, on a $x \leq y$ ou $y \leq x$. Il est **bien fondé** si il n'y a pas de suites infinies descendantes (c-à-d., $x_{i1} > x_{i2} > x_{i3} > \ldots$). Un **bon ordre** est un ordre total et bien fondé (ou, ce qui revient au même, tout sous-ensemble possède un plus petit élément). Une suite dénombrable est un ensemble image de l'ordre (total) ω, où ω sont les entiers ; e.g. une suite dans A est une fonction $a : \omega \rightarrow A$, avec $a_n = a(n)$.

4.1.1. Définition. *Un **arbre fini** T est un ordre partiel avec un plus petit élément, la **racine**, et tel que, si $a \in T$, alors $\{x / x \leq a\}$, la **branche** qui précède a, est totalement ordonné.*

Une **immersion** entre deux ordres partiels $(P, \leq)$ et $(P', \leq')$ est une fonction $h : P \rightarrow P'$ qui préserve les bornes inférieures (c-à-d. $h(\inf\{p,q\}) = \inf'\{h(p),h(q)\}$), donc monotone. On écrit $T \leq T'$ pour le pre-ordre sur les arbres induit par l'immersion.

4.1.2. Théorème ([Kruskal,1960]). *Pour toute suite infinie $\{T_n / n < \omega\}$ d'arbres finis, ils existent i et k tels que $i < k < \omega$ et $T_i \leq T_k$.*

Ce théorème énonce une propriété qui n'est pas du tout évidente: les arbres finis ne peuvent pas être "totalement désordonnés", car toute collection infinie en contient au moins deux "comparables", par immersion et dans l'ordre dans lequel on donne la suite. Mais alors, il ne peut pas y avoir:
- des suites infinies descendantes d'arbres (c-à-d., $T_{i1} > T_{i2} > T_{i3} > \ldots$),
- des suites infinies d'arbres tous incomparables,
et, donc, on prouve immédiatement que:

4.1.3 Corollaire. *Tout pre-ordre, qui soit une extension de la relation d'immersion entre arbres finis, est bien-fondé (c-à-d., il ne contient pas des suites infinies descendantes).*

L'importance de ce simple corollaire est due aux faits suivants, qui sont difficiles à démontrer et que nous ne traitons pas ici. En bref, il faut commencer par donner une fonction qui ait comme domaine les arbres et codomaine les ordinaux et qui soit surjective et monotone: par conséquent, l'ordre sur les ordinaux peut être vu comme une extension de celui sur les arbres. Puisque cela peut être fait sur des arbres finis à valeurs sur des ordinaux "assez grands" (Γ_0, le premier ordinal "imprédicatif", voir 4.2.3), le théorème de Kruskal, 4.1.2, prouve la bonne fondation de ces ordinaux, en raison du corollaire 4.1.3. Or, les ordinaux forment un ordre total, donc l'absence de suites descendantes démontre qu'il sont un bon ordre. Ceci implique l'induction jusqu'à Γ_0, car tout ensemble bien ordonné réalise l'induction. En conclusion, 4.1.2 implique la cohérence de l'Arithmétique du I ordre ou de Peano, PA (et de théories bien plus puissantes, en fait), en raison de résultats classiques qui remontent à Gentzen (le bon ordre ou l'induction jusqu'à ε_0, qui est bien plus petit que Γ_0, voir 4.2.3, suffit à démontrer la cohérence de PA).

L'énoncé en 4.1.2 est clairement infinitaire, dans le sens qu'il concerne des suites infinies (il est Π^1_1 dans la terminologie logique, car il commence par une quantification universelle sur des objets infinis).

L'idée de Friedman a été d'obtenir de cet énoncé un autre purement "finitaire", c'est à dire formalisable dans l'Arithmétique de Peano, PA. La preuve de son énoncé, ci-dessous, est une conséquence facile du théorème de Kruskal 4.1.2 et du Lemme de Kœnig[8]. En bref, dans la preuve, on verra que si "il existe un n tel qui pour aucun m

[8] Ce lemme dit: "pour tout arbre infini dont chaque élément a un nombre fini de successeurs, il existe une branche infini"; il est un principe infinitaire (en fait, le réciproque d'une propriété de compacité), mais il est bien évident. Il apparaît très souvent dans ce gendre de théorèmes (voir aussi la preuve de la "vérité" de l'énoncé de Paris-Harrington, pour en rester aux théorèmes d'indépendance, et maints autres résultats), car

on a KF(n,m)", alors l'argument de compacité à la Kœnig donne un contre-exemple à 4.1.2.

4.1.4 Théorème KF (Friedman, 1981) *Pour tout n, il existe un m tel que pour toute suite finie d'arbres finis $T_1, T_2, ..., T_m$, telle que chaque T_i ait au plus $n(i+1)$ éléments, ils existent j et k tels que $j < k \leq m$ et $T_j \leq T_k$.*

Pr. Disons tout d'abord, une fois fixé un n, qu'une suite finie d'arbres finis $T_1, T_2, ..., T_m$, telle que chaque T_i ait au plus $n(i+1)$ éléments, est **mauvaise** si pour tout j et k tels que $j < k \leq m$ on *n'a pas* $T_j \leq T_k$. Or, une sous-suite d'une suite mauvaise d'arbres est aussi mauvaise ; en plus, suite à la restriction sur le nombre des éléments de chaque arbre, il existe un nombre fini de suites de longueur m. On peut donc organiser les suites mauvaises dans un arbre dont

- les nœuds sont des suites d'arbres,
- la racine est la suite vide
- chaque suite mauvaise d'arbres, de longueur m, se situe à profondeur m de l'arbre et est connectée à la racine par le parcours unique donné par ses sous-suites initiales.

Puisqu'il y a un nombre fini de suites de longueur m, pour chaque m, l'arbre est infini et à branchement fini. Si donc on suppose le contraire du théorème, c'est-à-dire que pour un n donné, on a pour chaque m au moins une suite mauvaise, grâce au lemme de Kœnig, il existe une suite mauvaise *infinie* d'arbres finis, contre 4.1.2. ⊗

L'énoncé du théorème, cette fois, a la structure logique suivante: "pour tout n, il existe m" suivi d'un prédicat décidable (KF(n,m), disons), car on sait compter les éléments d'un arbre fini (ils doivent être bornés par n(i+1)) et contrôler, dans une suite finie d'arbre, si il y en a deux qui sont comparable: il est donc un énoncé Π^0_2 de PA, écrivons formellement $\forall x.\exists y.KF(x,y)$. Informellement, sous une condition qui est fonction de n sur les nombres d'éléments des arbres, le théorème KF affirme que même les suites finies de m arbres ne peuvent pas être totalement désordonnées. Il faut enfin remarquer que

---

il établie un "pont" entre fini et infini. On l'utilise pour transférer du fini à l'infini, par compacité, une propriété que, souvent, on assume par absurde: si à tout niveau fini il existe un contrexemple à notre énoncé finitaire, alors il existe aussi un contrexemple à l'énoncé infinitaire. Par ce raisonnement, un résultat infinitaire (Kruskal ou Ramsey, dans le cas de Paris-Harrington, voir l'appendice) entraîne une conséquence finitaire non évidente. Il est raisonnable de considérer aussi ce principe (appelé lemme pour des raisons historiques), un jugement géométrique : dessinez un arbre à branchement fini, qui s'étend à l'infini… il doit bien y avoir une branche infinie, même si son existence n'est pas nécessairement constructive. Elle ne l'est pas, car a chaque niveau, on "choisit" (axiome des "choix dépendants") un nœud qui *ait une infinité de successeurs*. Plus précisément : supposons qu'à un niveau donné, tous les nœuds aient un nombre fini de successeurs, alors l'arbre serait fini ; prenons donc un nœud, qui doit exister, ayant une infinité de successeurs – existence non constructive ! – et… ainsi de suite au niveau suivant.

tous ces énoncés (Kruskal, Kœnig, Ramsey, voir l'Appendice) sont des théorèmes important de la "combinatoire infinie", car ils ont un nombre important d'applications, en particulier en Logique et Informatique Théorique (Kruskal: problème de la terminaison pour les systèmes de réécriture, voir [Gallier, 1991] pour des références).

Ce qui est surprenant et difficile à démontrer formellement est que 4.1.4, KF, n'est pas démontrable dans PA (en fait, il n'est même pas démontrable dans des fragments très expressifs de l'Arithmétique du second ordre, appelée par les logiciens "Analyse", voir l'article de Simpson dans [Harrington&al.,1985]). L'exploit remarquable de Friedman a été de démontrer que KF suffit a donner les mêmes conséquences que 4.1.3, à savoir le bon ordre des ordinaux jusqu'à Γ_0, car il implique qu'il n'y a pas de sous séquences descendantes "primitives récursives", que le langage de l'Arithmétique permet de représenter et que l'on pourrait extraire de toute suite descendante. En raison du deuxième théorème d'incomplétude de Gödel (c-à-d. l'indémontrabilité de la cohérence de PA, dans PA), KF, qui est un énoncé de PA, n'est pas démontrable par les principes de preuve de PA, tout en étant une propriété démontrablement vraie des nombres entiers: pour le démontrer il faut manier le bon ordre des entiers et l'infini des arbres planaires de la preuve de Kruskal, dans une preuve rélativement simple, mais infinitaire.

4.1.5 Il existe donc une preuve, très difficile, de l'indémontrabilité de KF dans PA. Essayons maintenant de comprendre "de près", autant que cela peut se faire, qu'est-ce ce qu'il y a de non arithmétisable dans la preuve de KF : il s'agit bien d'une preuve de longueur finie, écrite avec des mots, soulignerait le formaliste computationnel (voir celle qui est dans [Harrington&al.,1985] ou [Gallier, 1991]), quel passage alors d'une ligne à une autre est-il essentiellement "infinitaire" ? Et ce passage doit bien exister, car on sait que la preuve n'est pas arithmétisable. La déduction de KF à partir du théorème de Kruskal ne pose pas vraiment de problème : le lemme de Koenig, comme hypothèse ajoutée, donne une extension conservative de PA. C'est le passage par le théorème de Kruskal qui doit contenir quelques lignes essentiellement non formalisables (dans PA[9]).

Tout d'abord, la preuve du théorème de Kruskal n'est pas particulièrement difficile. Elle se base sur un résultat classique, dû à Higman, concernant les suites finies (voir

[9] Il est évident que, étant donné un énoncé formalisé, on peut toujours trouver la théorie formelle (une extension de PA, typiquement) qui le démontre : il suffit, par exemple, de l'ajouter comme axiome. Soit-il compatible ou pas avec PA, on aurait là bien un preuve…. L'enjeu intéressant est, bien évidemment, celui de trouver des axiomatiques formelles sensées et "minimales" qui le démontrent. Il est toutefois clair que l'intérêt épistémologique de cette course poursuite (je donne un énoncé indémontrable, tu cherches une axiomatique…) n'a rien à voir avec l'hypothèse de complétude de PA (mais aussi de ZF etc) de Hilbert, qui aurait dû être une sorte de « solution finale » (ses mots) du problème de fondements. Poincaré, ayant tout autre philosophie de la connaissance, observait au contraire (Science et Méthode, 1908) : « les problèmes insolubles sont les plus intéressants » aussi puisqu'ils posent « d'autres problèmes auxquels on n'avait pas songé ». Fort heureusement, en théorie de la connaissance, il n'y a pas de « solution finale ».

[Gallier, 1991]), dont on a donné, plus récemment, aussi une version "constructive", bien plus complexe ([Rathjem, 1993]. Dans cette dernière preuve on applique la théorie, infinitaire mais intuitionistiquement acceptable – du moins pour certains intuitionnistes - des “définitions inductives” sur les ordinaux – voir §. 4.3, due à Martin-Löf.

Dans la preuve "classique" de 4.1.2, on utilise un argument par l’absurde pour démontrer qu’un certain ensemble, qui contredirait le théorème s’il était habité, est en fait vide. Plus précisément, on suppose que l’ensemble des suites mauvaises, dans le sens de la preuve de 4.1.4 mais infinies cette fois – sans borne dépendante de n, soit non-vide (on suppose donc le contraire du théorème 4.1.2). On “construit” alors une suite mauvaise minimale dans cet ensemble, en prenant, l’un après l’autre, des arbres, bien évidemment finis, de longueur minimale. On applique donc, de façon itérée, le principe du bon ordre sur les entiers (on suppose qu’il y ait une longueur minimale, parmi les entiers associé par cette mesure aux arbres finis de la suite mauvaise, qui habitent donc l’ensemble supposé non-vide). On démontre enfin que, à partir de cette suite, on peut en construire une plus petite ; cela contredit sa minimalité, un absurde (voir [Nash-Williams, 1963], [Harrington, 1985 ; p. 92], [Gallier, 1991]).

En examinant la preuve, on observe donc que la suite mauvaise minimale est obtenue en quantifiant sur un ensemble que… l’on démontrera vide, un procédure pas très effective ! En plus, cet ensemble qui résultera vide, si on le décrit formellement, est défini par un prédicat Σ^1_1, bien en dehors donc de PA (il contient une quantification sur un ensemble infini). Bref, les passages essentiellement non arithmétisables sont basés sur la définition d’un ensemble par un prédicat Σ^1_1 et sur l’utilisation, itérée, de l’existence d’un plus petit élément dans un ensemble non-vide d’entiers.

La preuve toutefois est parfaitement convaincante : si un ensemble d’entiers est non-vide, on accepte l’existence d’un plus petit élément, même si sa définition utilise un prédicat Σ^1_1. Pour le jugement géométrique du bon ordre sur la suite discrète des entiers (chaque personne mathématisé “voit” la suite croissante et discrète des entiers et que, si un sous-ensemble générique contient un élément – là-bas, quelque part, il en contient un moindre), il importe peu l’allure vers l’infini de l’ensemble en question, c’est-à-dire sa définition par le biais d’un prédicat Σ^1_1 : l’existence, sûrement non constructive du plus petit, est ici, au fini géométrique. En plus, dans notre cas, on utilise l’existence du plus petit élément, que l’on ne saurait pas construire, pour démontrer… qu’il ne peut pas exister, c’est-à-dire que l’ensemble des mauvaise suites est vide.

En dehors du langage, par une référence à un jugement géométrique aussi solide que la structure des entiers, on démontre donc un théorème sur les entiers, KF. Et, d’une façon ou d’une autre (il existe plusieurs preuves, bien évidemment), ce détour est essentiel, comme nous assure la preuve de non-démontrabilité dans PA par Friedmann.

En conclusion, cet invariant qui est le jugement géométrique du bon ordre des entiers, utilisé tous les jours par le mathématicien au travail, mais aussi par le logicien ultra-formaliste qui démontre KF (voir l'article de Simpson dans [Harrington, 1985]), *fonde*, de façon irremplaçable, PA, voire sa cohérence, ainsi que la preuve de ses théorèmes quelque peu non-formalisables. Il s'agit là d'une *gestalt*, que l'on considère ici comme étant un invariant de l'action, du geste qui ordonne dans l'espace les collections discrètes, du petit comptage que nous partageons avec certains animaux (voir [Dehaenne, 1997]) et qui abouti, par le langage, à l'itération à l'infini. Il est un invariant, car il est le résultat de nombreuses pratiques actives et de connaissance.

A cet égard, Brouwer se focalise sur la « twoness » du temps, ces instants discrets qui se succèdent, qui de un deviennent deux, l'un après l'autre, bien ordonnés. Une remarque au cœur des fondements de l'intuitionnisme brouwerien : les entiers comme donnés à et par la conscience de la suite temporelle discrète. Toutefois, l'invariance, qui donne stabilité à toute construction mathématique, voire conceptuelle, est justement établie grâce à une pluralité de « actes d'expérience », dirait H. Weyl : le concept, dans le langage, est stable car invariant par rapport à ces différentes formes de rapport au monde, constitutives de notre intelligibilité même du monde, car, par les structures mathématiques surtout, elles l'organisent. L'invariance est telle par rapport à des transformations de pratiques de vie, de contextes et de discours, humainement possibles. Au delà de Brouwer et ses « languageless mathematics », cette invariance devient alors maximale – et cela caractérise les mathématiques (le lieu de l'invariance et de la stabilité conceptuelle maximale, voir [Bailly, Longo, 2006]), grâce justement au langage, mais aussi à l'écriture et au dessin, qui permettent de la constituer/consolider dans l'intersubjectivité. Les nombres entiers, dans leur bon ordre, ne nous sont pas donnés par le Bon Dieu, mais ils sont encrés sur des activités humaines (et pré-humaines) parmi les plus anciennes de notre rapport au monde. Et l'écriture du nombre a même précédé l'écriture de langue (voir [Herrenschmidt, 2007]).

4.2 - Remarques: réductionnisme et preuves

4.2.1. On vient donc de donner un exemple purement arithmétique ou combinatoire d'énoncé qui se situe dans le décalage entre les principes de preuve (l'axiomatique formelle de PA) et principe de construction (le bon ordre des nombres et son extension aux arbres). En construisant les entiers dans l'espace, et l'ordre est une propriété spatiale, géométrique, on a montré comment la structure des nombres réalise des propriétés rélativement simple à énoncer, des jugements qui se situent au "fini géométrique", mais

qui ne sont cependant pas démontrables par des méthodes linguistico-syntactiques (finitaires et formels). Leur démonstration se base sur une analyse de la structure d'ordre des entiers et des arbres planaires.

De plus, l'énoncé de Friedman est une propriété purement *mathématique*: contrairement aux deux théorèmes d'incomplétude de Gödel, l'énoncé ne fait pas référence à une propriété métathéorique (Ier de Gödel: "cette phrase n'est pas *démontrable*"; IIème de Gödel: "la théorie est *cohérente*"). Or, le fait que les énoncés ne cachent pas de métathéorie en vertu d'un codage, comme dans les théorèmes de Gödel, est important, car il contredit l'argument du réductionnisme formaliste pour le quel les théorèmes d'incomplétude n'étaient que des accidents, des "ruses autoreférentes" (le IIème est une conséquence du Ier, qui est une version syntactique de l'argument autoreférent du menteur). Et il le contredit en jouant dans le camp adversaire: nous ne sommes pas en train de dire qu'il y a des énoncés "infinis", de la géométrie par exemple, qui échappent au formalisme linguistique, car KF est un énoncé tout à fait arithmétique et finitaire. Toutefois, le bon ordre et le concept d'infini entrent d'une façon essentielle dans sa preuve.

4.2.2 Deux aspects techniques. KF est un énoncé avec la structure formelle $\forall x.\exists y.KF(x,y)$ où $KF(x,y)$ est décidable en x et y. Or, on peut démontrer que pour tout n, l'énoncé $\exists y.KF(n,y)$ est démontrable dans PA (puisqu'il est vrai et $KF(x,y)$ est décidable, il suffit d'inspecter dans l'ordre les entiers). C'est à dire, si on fixe n, on peut donner, dans PA, une preuve de $\exists y.KF(n,y)$. Cette preuve est un "schema de preuve" ou une preuve "prototype" par rapport à un *entier* n générique (voir [Longo, 2002 ; Fruchart, Longo, 1997] pour la notion de preuve prototype). En effet, on a vu qu'on ne peut pas en trouver une preuve dans PA, c-à-d. il n'y a pas de preuve de $\forall x.\exists y.KF(x,y)$ par induction sur "x" dans le langage de PA. Donc, la preuve dépend strictement du "type" de n dans $\exists y.KF(n,y)$, c-à-d. du fait que n soit un entier standard : si la quantification universelle était donnée dans PA, n pourrait être interprété aussi par des entiers non standards, tandis que, dans la preuve, on utilise explicitement n comme entier standard (dans le branchement fini de l'arbre de Kœnig, dont la cardinalité dépend de n).

Une deuxième remarque: grâce à la décidabilité de $KF(n,m)$ en n et m, on peut définir une fonction récursive totale qui associe (choisit) un m pour tout n. Le point est que cette fonction croît plus rapidement que n'importe quelle fonction démontrablement totale en PA (en fait, elle est une des plus "rapides" que l'on connaisse, voir [Harrington&al.,1985]).

4.3 - L'imprédicativité et les Ordinaux

Une théorie logique est **imprédicative** si elle ne "stratifie" pas l'univers mathématique. Informellement, on n'en défini pas les parties, les éléments, sans faire intervenir en même temps le tout, ou un grand morceau du tout. Par exemple, en Théorie des Ensembles, une définition est imprédicative, si elle défini un ensemble b au moyen d'un ensemble A qui peut contenir b. Plus formellement, en écrivant "$\forall y$" pour "pour tout y", un ensemble b est **défini imprédicativement** si il est donné sous la forme

$$b = \{ x \mid \forall y \in A \; P(x,y) \}$$

où b peut être un élément de l'ensemble A, qui apparaît dans la définition même de b (ou: A est composé par des éléments qui, dans son entièreté, il sert à définir). La théorie généralisé de l'intégration (ou de la mesure de Lebesgue) et la Théorie des Types de J.Y. Girard sont imprédicatives[10]

Or, l'énoncé KF n'a rien d'imprédicatif, il appartient au langage de PA. Toutefois sa preuve fait intervenir l'imprédicativité profondément. On va l'esquisser très brièvement, tout juste au delà de l'infini.

Comptez: 0, 1, 2, 3 ... . Appelez ω la limite de cette suite.
Continuez: $\omega+1, \omega+2, \ldots \omega+\omega = \omega 2$. Et encore: $\omega 2, \omega 3, \ldots \omega\omega = \omega^2$.
La règle du jeu est claire, continuez à la jouer sur les puissances:

$$\omega^2, \omega^3, \ldots \omega^\omega.$$

Donc, ω puissance ω, puissance ω ... à la limite ce sera simplement ω puissance ω, ω fois. Cet ordinal s'appelle ε_0. Considérons maintenant la fonction $\phi(0, x) = \omega^x$: alors ε_0 est un point fixe de $\phi(0, x)$, car $\varepsilon_0 = \omega^{\varepsilon 0} = \phi(0, \varepsilon_0)$; en fait, ε_0 est le plus petit point fixe de $\phi(0, x)$.

Mais continuons et appelons $\phi(1, x)$ la fonction qui énumère les points fixes de $\phi(0, x)$, c-à-d. $\varepsilon_0 = \phi(1, 0)$, $\varepsilon_1 = \phi(1, 1), \ldots, \varepsilon_\omega = \phi(1, \omega), \ldots$. Aussi la fonction $\phi(1, x)$ a des points fixes; appelons $\phi(2, x)$ la fonction qui les énumère ... . Et ainsi de suite: $\phi(a+1, x)$ dénombres tout les points fixes de $\phi(a, x)$; si b est une limite, comme $\omega, \omega^2, \omega^\omega, \varepsilon_0 = \phi(1, 0)$ ou $\phi(2, 0)$, alors $\phi(b, x)$ énumères les points fixes de $\phi(a, x)$ pour tout $a < b$.

On pourrait dire que cette construction de la suite ordinal n'est qu'un "jeu de symboles". Ce jeu toutefois n'est pas dépourvu de signification. A chaque niveau nous

---

[10] Pour cette dernière, voir ce texte ou [Girard&al.,1989]. [Fruchart&Longo,1997] développe des résultats récents au sujet de son imprédicativité; [Longo,1998] des réflexions concernant le continu - en Analyse le problème se pose depuis H. Weyl et a été traité en profondeur par maints logiciens, e.g. Kreisel, Wang, Shutte, Feferman, Simpson.....

avons détecté une itération et nous avons *décidé* de "passer à la limite". C'est la *structure d'ordre des entiers* que nous avons étendu en une structure mathématique, celle des ordinaux, par la double opération, d'itération et de limite et ... d'itération des limites. Attention, sa signification n'est que structurelle, car il n'y a pas d'ensemble sous-jacents: ces symboles ne sont pas des cardinaux, en générale, car il n'existe aucun ensemble x qui satisfait, par exemple, l'équation $x = \omega^x$, dont ε_0 est la plus petite solution. On a construit, selon des principes "élémentaires", un ordre dans "l'espace mental", comme extension de celui qui va de 0 à ω.

La fonction binaire $\phi(y, x)$ est totale, c-à-d. elle est définie pour chaque a, b énuméré de la façon que l'on vient de décrire. ϕ croît très rapidement: les points fixes de $\phi(\omega, x)$, $\phi(\varepsilon_0, x)$, ... $\phi(\phi(\varepsilon_0, 0), x)$ ... sont des "monstres". On obtient une croissance encore plus forte, si on considère une suite qui nous intéresse particulièrement:

$$\gamma_0 = \phi(0,0),\ \gamma_{n+1} = \phi(\gamma_n, 0)$$

Leur limite s'appelle Γ_0 et satisfait l'équation $\Gamma_0 = \phi(\Gamma_0, 0)$. Le corollaire 4.1.3 implique le bon ordre des ordinaux (donc l'induction) jusqu'à Γ_0 par une immersion, relativement simple et qui utilise la fonction ϕ, des arbres finis dans l'ensemble des ordinaux qui précèdent Γ_0.

Observez que, jusqu'à Γ_0 nous n'étions pas sorti du dénombrable et du prédicatif: le jeu de symbole n'utilisait, pour une nouvelle définition, que les précédentes. Même les "plus petites solutions" des équations posées peuvent être atteinte par le bas, grâce à la construction basé sur la fonction $\phi(y, x)$, comme, par exemple, les limites ω et ε_0, car $\omega = \phi(0, 1)$ et $\varepsilon_0 = \phi(1, 0)$. Il n'en ait pas ainsi pour Γ_0, car pour tout $a, b < \Gamma_0$, on a $\phi(a,b) < \Gamma_0$.

Γ_0 échappe donc a cette "itération + limite", d'extraordinaire puissance, représentée par la fonction ϕ, une fonction qui est donné dans un langage dénombrable et "stratifié", à partir de la pratique du comptage naturel $1, 2, 3$ ... et du premier passage à la limite, ω. En effet, chaque fonction $\phi(a+1, x)$ est une itération "à la limite" de la fonction $\phi(a, x)$. Mais, si on fixe le *deuxième* argument, $\phi(y, b)$, comme dans la hiérarchie qui donne Γ_0, on fait une itération sur les *procès* d'itération eux-mêmes, tels qu'ils sont décrits par *toute la collection* des fonctions $\phi(a, x)$, pour tout $a < \Gamma_0$. On a donc un opérateur ou fonctionnel $\phi(y, b)$, dont la définition est bien donnée seulement quand on connaît son domaine et codomaine. Pour cette raison, Γ_0 ne peut pas être atteint par le bas, grâce aux fonctions $\phi(y, x)$: on ne peut le définir que en utilisant Γ_0 lui-même (ou la collection de tous les ordinaux, qui le contient et que nous sommes en train de définir). La définition de Γ_0 est donc essentiellement imprédicative. Pour résumer en des termes différents, Γ_0 est le plus petit ordinal tel que $\Gamma = \phi(\Gamma, 0)$, mais la collection de ces Γ contient Γ_0 lui même, que nous sommes en train de définir; contrairement à ce qu'on a

vu pour les $a < \Gamma_0$, on ne peut pas faire mieux, c-à-d. on ne peut pas atteindre Γ_0 par le bas, grâce aux opérations de l'arithmétique ordinale, voir par ϕ[11].

Or, Γ_0 entre deux fois dans KF. D'une part, la preuve d'indémontrabilité se base sur la déduction, à partir de l'énoncé combinatoire de KF, du bon-ordre jusqu'à Γ_0. D'autre part, la preuve inductive de la validité de KF sur les entiers requiert une induction jusqu'un ordinal plus grand (!) que Γ_0 (voir [Rathjem, 1993]).

5 - Conclusion

Nous avons donc un énoncé arithmétique, KF, relativement simple et donné d'une façon tout à fait prédicative. Toutefois, sa preuve demande une "pratique de l'infini" des entiers et des arbres planaires (arbres d'arbres, lemme de Kœnig, bon ordre ...), très "raisonnable" mais non-effective, voire essentiellement infinitaire, du point de vue formel, car il n'y a pas de preuve dans PA. Plus précisement, KF implique la bonne fondation, donc l'induction, jusqu'au premier ordinal imprédicatif. C'est à dire, KF permets de démontrer que la construction mathématique généralisée, par les fonctions ϕ, de l'itération et des limites, donne une structure mathématique, une structure d'ordre, bien-fondée, quoique cette structure, dont la construction arrive jusqu'à Γ_0, soit imprédicative. Par contre, la preuve inductive de KF lui-même, requiert au moins puissance imprédicative. Le formaliste-fondamentaliste n'a donc pas de choix : ou il accepte de "tirer le cou" à l'induction formelle jusqu'au delà du premier ordinal imprédicatif, ce qu'il considère le moindre mal, ou, au moins dans la preuve, il utilise de facto le jugement du bon ordre (voir les preuves citées de KF, qui passent par le théorème de Kruskal), dont le seul "fondement" est de nature cognitive.

Bien au delà de ce que peut nous dire le formidable calembour de Gödel, les résultats récents d'incomplétude "concrète", nous disent que même des "simples" énoncés combinatoires, qui s'expriment facilement en Arithmétique, peuvent faire intervenir d'une façon essentielle, dans la preuve, de l'infini et de l'espace, en tant qu'ordres structurés: ils utilisent des ordres totaux ou partiels infinis, des arbres ... . en plus, ils impliquent le bon ordre bien au-delà de ω. Des structures de l'infini et de l'espace si complexes que, si analysées formellement, elles se définissent seulement en termes d'elles mêmes (l'imprédicativité). Un décalage bien important, donc, entre principes ou pratique de la construction et de l'infini, d'un coté, et principes de preuve formels, arithmétiques (et prédicatifs), de l'autre.

---

[11] Cette esquisse informelle a été inspiré par les articles de Smorynski dans [Harrington&al.,1985]; l'imprédicativité de Γ_0 a été démontré en toute rigueur par Feferman et Schütte

La thèse que l'on a essayée d'explorer est en bref la suivante. L'analyse 'logique' de l'arithmétique humaine a proposé les notions de successeur et d'induction comme *bases opérationnelles* de la preuve formelle, mais le *fondement* de ces mêmes opérations, leur signification et justification, se trouve dans le bon ordre dans lequel nous rangeons les nombres dans nos espaces mentaux. En fait, nous concevons d'abord l'ordre (mental) des nombres et seulement ensuite sa formalisation logique (à la Peano, par exemple). C'est l'ordre et l'ordonnancement, si présents dans nos pratiques de vie et du langage, qui sont au coeur de la construction des nombres et qui les relie aux autres constructions mathématiques, comme les nombres réels, voire à la géométrie. L'hypothèse hilbertienne de complétude visait à exclure du raisonnement, au moins du raisonnement arithmétique, toute référence à la signification (en fait, à la structure sous-jacente des nombres) et à l'espace (le bon-ordre). Il s'est avéré impossible.

Le fondement de l'Arithmétique, dans sa genèse cognitive et historique, est en effet dans le comptage élémentaire et dans la construction/rangement, d'abord pratique, puis de l'infinité potentielle des nombres entiers dans nos espaces mentaux. Car le comptage, étendu par le langage, est comme simulé dans un espace mental qui devient une partie essentielle de la signification (voir ci-dessus et la référence aux représentations mentales dans [Dehaene,1997]). Et l'élément commun aux différentes organisations spatiales (et temporelle, dirait Brouwer) est justement le bon ordre. L'induction logique ou formelle, que l'on exprime dans le langage, est alors *une conséquence* non pas un fondement du monde du comptage, de l'Arithmétique, car tout ensemble bien ordonné réalise l'induction formelle. Voilà une thèse qui nous donnerait le *fondement cognitif*, et non pas logico-formel, de ce que Poincaré plaçait, justement, aux bases des mathématiques et bien en amont de la logique: *l'induction arithmétique* (" ... elle n'est que l'affirmation d'une propriété de l'esprit lui même" [Poincaré,1968], p. 42). Pour nous, l'esprit, c'est l'histoire d'une génèse cognitive.

Pour résumer, l'induction, dont la formalisation logique n'est qu'une possible représentation linguistique, bien incomplète comme on a vu, se *fonde* donc sur l'ordre (le bon-ordre), cet invariant de notre action qui organise l'espace et le temps, par les nombres, et qui leur donne une signification, dès que le langage nous permet d'aller plus loin que le comptage et l'ordonnancement élémentaire, dans cette extraordinaire construction conceptuelle que sont les mathématiques. De plus, l'extension du bon ordre au-delà de cet horizon que l'on appelle ω, permet des preuves qui ne sont pas capturées par l'induction formelle, en particulier prédicative. Le théorème KF en est un magnifique exemple.

Appendice : le Théorème de Paris-Harrington.

Énoncé informel (en "couleurs"):

> « Pour tout k, l, m il existe n si grand que, si on "colore" les sous-ensembles de k-elements de {1,...,n} avec l couleurs, il y aura alors un sous-ensemble Y de cardinalité au moins m dont tous les sous-ensembles de k-elements ont la même couleur, et tel que la cardinalité de Y est plus grand que le plus petit élément de Y. »

Cette propriété des partitions des nombres entiers, énoncée dans le langage de PA, est indémontrable dans PA. Mais elle es tune conséquence relativement simple, d'un théorème bien connu de combinatoire infinitaire, le théorème de Ramsey (ou ses variantes, voir dessous).

Plus formellement:

Notation: $[X]^n = \{Y / Y \subseteq X \text{ et } card(Y) = n\}$

Définition. Soit P une partition de $[X]^n$ en m partie, c-à-d. $P : [X]^n \to m$. On appelle alors **homogène** pour P tout sous-ensemble $Y \subseteq X$ tel que P soit constante sur $[Y]^n$ (i.e.: the n-elements subsets of Y have the same color).

Notation: pou $k \geq n$, $\mathbf{X \to (k)^n_m}$ signifie que

> "pour tout $P : [X]^n \to m$, il existe $Y \subseteq X$ homogène pour P, tel que $card(Y) \geq k$".

Théorème (de Ramsey, 1929)

- (*cas infini*) Pour tout n et m entiers, on a $\omega \to (\omega)^n_m$
- (*cas fini*) Pour tout l, n, m et p, il existe $q \geq l$, tel que $[l,q] \to (p)^n_m$.

Notation (la variante de Paris-Harrington):

$\mathbf{[l,q] \to^* (p)^n_m}$ signifie que

> "pour tout $P : [l,q]^n \to m$, il existe $Y \subseteq [l,q]$ homogène pour P, tel que $card(Y) \geq p$ et $card(Y) > min(Y)$".

Théorème 1 ([Paris-Harrington, 1978]):

$$PA \vdash \forall z \forall x \exists y.\ [x,y] \to^* (z)^z_z .$$

Pr. Paris et Harrington démontrent, par un tour de force remarquable, que

$$PA \vdash\!\!\!- (\forall z \forall x \exists y.\ [x,y] \rightarrow\!* (z)^z_z) \rightarrow Coher_{PA}$$

où $Coher_{PA}$ formalise en PA, la cohérence de PA. Donc PA ne démontre pas $\forall z \forall x \exists y.\ [x,y] \rightarrow\!* (z)^z_z$ (voir leur article dans [Barwise, 1978]). @

Toutefois, on peut demontrer que l'énoncé en question est vrai sur les entiers standards. C'est à dire, que pour tout n et m entiers, il existe p tel que $[m,p] \rightarrow\!* (n)^n_n$:

Théorème 2:

$\forall z \forall x \exists y.\ [x,y] \rightarrow\!* (z)^z_z$ est vrai (dans le modèle standard de PA).

Pr. Supposons qu'ils existent des entiers n et a tel que $\exists y.\ [a,y] \rightarrow\!* (n)^n_n$ est faux. Alors pour tout entier b, il est faux que $[a,b] \rightarrow\!* (n)^n_n$. Ou, autrement dit, pour chaque $b > a$, il existe une partition (on dira un contrexemple) $P_b : [a,b]^n \rightarrow n$, qui n'admet pas un sous-ensemble homogène Y, avec plus de n éléments, et relativement grand (i.e. tel que $card(Y) > min(Y)$).

Il est possible d'ordonner partiellement l'ensemble des partitions P_d, pour $d > a$, qui donnent des contrexemples, de la façon suivante:

$P_b \leq P_c$ ssi $b \leq c$ et $P_b = P_c \lceil [a,b]^n$ (la restriction de P_c à $[a,b]^n$).

$\{ P_d / d > a \}$ est un arbre infini, mais chaque noeud a un nombre fini de branches (ou de successeurs), car il y a un nombre fini de fonctions de $[a,d+1]^n$ dans n. Pour le lemme de Kœnig, il existe donc une branche infinie, c-à-d. une partition $P : [\omega]^n \rightarrow n$ tel que, pour tout $d > a$, la restriction de P à $[a,d]^n$ est un contrexemple.

Le cas infini du théorème de Ramsey démontre alors qu'il existe un sous-ensemble Y infini homogène pour P. Soit $e = minY + n$; choisissons alors b assez grand pour que $Z = Y \cap [a,b]$ contienne au moins e éléménts. Donc, Z est homogène pour $P_b : [a,b]^n \rightarrow n$, $card(Z) \geq n$ et Z est relativement grand, contrairement à l'hypothèse. @

En fait, on peut démontrer que, pour tout n entier,

$$PA \vdash\!\!\!- \forall x \exists y.\ [x,y] \rightarrow\!* (n)^n_n .$$

Ce qui est évidemment encore plus fort.

Bibliographie *: fichier à part.*