Mathématiques et sciences humaines
Mathematics and social sciences

152 | Hiver 2000
Varia

Cercles vicieux, mathématiques et formalisations logiques

Vicious circles, mathematics and logic

Giuseppe Longo

Édition électronique
URL : http://journals.openedition.org/msh/2834
DOI : 10.4000/msh.2834
ISSN : 1950-6821

Éditeur
Centre d'analyse et de mathématique sociales de l'EHESS

Édition imprimée
Date de publication : 1 décembre 2000
ISSN : 0987-6936

Référence électronique
Giuseppe Longo, « Cercles vicieux, mathématiques et formalisations logiques », *Mathématiques et sciences humaines* [En ligne], 152 | Hiver 2000, mis en ligne le 10 février 2006, consulté le 19 avril 2019.
URL : http://journals.openedition.org/msh/2834 ; DOI : 10.4000/msh.2834

Math. & Sci. hum., (38e année, n° 152, *2000*, p. 5-26)

CERCLES VICIEUX, MATHÉMATIQUES ET FORMALISATIONS LOGIQUES

Giuseppe LONGO[1]

RÉSUMÉ – *Certaines formes de circularité logiques et mathématiques (auto-appartenance, auto-implication, imprédicativité,…) sont analysées comme des propriétés de fermeture de certaines structures mathématiques puisqu'on peut les interpréter comme des solutions de certains systèmes d'équations. Parallèlement, du point de vue philosophique, on met en évidence la contribution de ces circularités au pouvoir des mathématiques à rendre le monde intelligible.*

MOTS-CLÉS – Équations, Auto-référence, Auto-application, Anti-fondation, Imprédicativité.

SUMMARY– Vicious circles, Mathematics and Logic

Some forms of circularity in Logic and Mathematics (self-membership, self-application, impredicativity,□.) are analyzed as closure properties of suitable mathematical structures since they can be considered as solutions of some systems of equations. At the same time, from a philosophical point of view, we stress the contribution of these circularities to the power of mathematics in making the world intelligible.

KEYWORDS – Equations, Self-reference, Self-application, Anti-foundation, Impredicativity.

Article communiqué par P. Boldini

1. INTRODUCTION

Les phénomènes naturels, mais aussi les constructions conceptuelles, manifestent maintes formes de circularité. Il est bien difficile de les classer car elles se présentent sous des aspects et dans des contextes très différents. Examinons-en quelques-unes, en commençant par celles de la Physique.

Considérez le *plus simple* des systèmes dynamiques, celui constitué par trois corps ou plus dont le mouvement est seulement réglé par la loi newtonienne de gravitation universelle. La position, la vitesse et l'accélération d'un corps sont respectivement déterminées par les positions, vitesses et accélérations des autres corps : on ne peut pas étudier isolément le mouvement d'un corps, car celui-ci dépend du mouvement du système, dans sa globalité. Le système n'est pas *stratifié*. Ce problème était clair pour Newton lui-même et, au cours du siècle dernier, de nombreux et remarquables travaux

[1] C.N.R.S. et Département de mathématiques et informatique, École Normale Supérieure, 45 rue d'Ulm 75005 Paris, http://www.dmi.ens.fr/users/longo.

mathématiques furent consacrés au traitement de cette circularité qui est au cœur de problèmes physiques d'importance cruciale (le système solaire en fournit un bon exemple). Poincaré, vers la fin du siècle, mit en évidence le fait que la difficulté, quant à la solution des systèmes d'équations différentielles décrivant les systèmes dynamiques, provient de la circularité physique du système. Elle en est donc la contrepartie mathématique, conceptuelle.

Passons aux phénomènes du vivant. Chaque être vivant représente une *unité systémique* au moins aussi complexe que les systèmes dynamiques de la physique. On ne peut comprendre les fonctions et la nature d'une partie ou d'un organe, sans les penser dans l'unité de l'organisme, lui-même pris dans son rapport et ses maintes liaisons avec son écosystème. Des organismes différents apparaissent souvent comme liés à une unité systémique plus grande, par des phénomènes de symbiose ou d'échanges vitaux, dans lesquels on ne peut pas dire *qui vient le premier* ou *qui est venu le premier* au cours de l'évolution, par exemple.

Que dire des processus mentaux ? Le regard sur soi-même, la *conscience* de notre propre conscience… les réflexions *cognitives* sur la cognition humaine et autres jeux de mots. Tous manifestent de vrais problèmes de représentation conceptuelle.

Dans certains cas les mathématiques aident à penser ces problèmes ou, au moins, les clarifient en traitant de cas particuliers, et en représentant avec rigueur certains systèmes. Par exemple, la logique mathématique a permis l'analyse et a proposé des solutions pour certaines circularités du langage des mathématiques. Dans un premier temps, je discuterai de trois formes fondamentales de circularité traitées en logique mathématique, tout en essayant de trouver le sens de la méthode commune de solution. On verra que ces circularités syntaxiques sont résolues par la preuve de fermeture (par rapport à certaines opérations) de certaines structures algébriques ou géométriques. Dans un deuxième temps j'esquisserai quelques éléments du problème tel qu'il se pose dans d'autres secteurs des mathématiques.

La leçon, s'il y en a une, que devrait tirer le lecteur humaniste, philosophe ou simplement non-mathématicien, est que ces paradoxes apparents dans le monde, ou dans nos descriptions du monde, sont des défis lancés à nos formes de connaissance, et que les mathématiques ont su dans certains cas (très peu à vrai dire) en donner des belles explications, ou plus simplement, des représentations efficaces, instructives, quoique très spécifiques. Ceci est peut-être la trace d'un lien important entre physique, vie et pensée d'un côté, et représentation mathématique de l'autre.

2. ÉQUATIONS ET ALGÈBRE

Commençons par un cas très simple et très ancien. Un jour, ma fille revint bien triste de l'école. Elle n'avait pas su résoudre le problème suivant⊡ dans une famille, le père a quatre ans de plus que la mère, qui a 18 ans de plus que la moitié de l'âge du père. En déduire l'âge x du père et l'âge y de la mère. Ceci lui paraissait impossible : comment connaître l'âge de la mère, qui dépend de celui du père, qui dépend à son tour de celui de la mère… Ma fille ne prononça pas le mot circularité, mais il était presque sur ses lèvres.

Heureusement, dans ce cas, je pus facilement l'aider à reconstruire la solution du problème, dont elle avait, en fait, les outils. Il suffit d'écrire un petit système d'équations linéaires :

$$\begin{cases} x = y + 4 \\ y = 0{,}5x + 18 \end{cases}$$

qui lui aussi manifeste de la circularité puisque x est fonction de y qui est fonction de x.

Les mathématiques toutefois s'en sortent très bien, quoique la solution à ce problème, dans toute sa généralité, n'ait pas été immédiate. Il a fallu construire le corps des nombres rationnels, fermé par addition, soustraction, multiplication et division. Une construction qui ne fut pas évidente pour les Grecs : «peut-on diviser une grandeur par une grandeur ?» se demandèrent-ils très longtemps. Il fallut attendre l'algèbre des Arabes, Fibonacci de Pise et la théorie des nombres pour avoir des méthodes générales et uniformes de solution. C'est donc une propriété de fermeture d'une structure mathématique, le corps des rationnels, qui donne la solution du problème. En fait, cette structure a été construite justement pour résoudre ce genre de questions. Elle explique, «étale» la circularité, ou la transfère, si on veut, sur une construction d'une autre nature : la fermeture algébrique demandée est aussi une forme de circularité, mais elle est un théorème, une conséquence facile de la construction des nombres rationnels à partir des entiers, qui n'a rien de circulaire. La circularité syntaxique qui apparaît dans la définition informelle du problème, mais aussi dans sa représentation formelle (les deux équations), est expliquée par un théorème de fermeture (sémantique). Ainsi, l'interprétation fournie par la structure mathématique donne une signification au jeu circulaire des symboles.

3. ENSEMBLES NON BIEN-FONDÉS

Commençons cette fois par la fin, c'est-à-dire par des problèmes récents qui ont fortement contribué à revitaliser, en théorie des ensembles, un débat qui avait été étouffé au début du siècle.

En informatique , il existe de nombreux processus qui ne s'arrêtent jamais. Un système d'exploitation fonctionne tout le temps, on n'éteint pas les ordinateurs modernes, ils sont toujours prêts à recevoir un *input*, le traiter, donner un résultat, attendre un autre *input*… Pour rendre compte de ceci, on utilise la notion de *stream*. Par exemple, $f(n) = (n, f(n + 1))$ est le *stream* $(0, (1, (2, \dots)))$, qui définit la fonction f□ une définition de fonction tout à fait inhabituelle en mathématiques, mais d'usage commun dans certains secteurs de l'informatique théorique.

De manière générale, un système de transition x, sur un ensemble A de constantes, un système d'exploitation par exemple, produit la constante $a \in A$ puis continue à faire x. On peut formaliser ce phénomène de maintes façons ; on peut écrire□

$$x = (a, x) \qquad (1)$$

où, x est une suite de symboles, qui représentent le calcul, et a le résumé des actions à faire (lire, calculer, écrire). En général, il s'agit d'ensembles non structurés ou de listes

de symboles. La théorie des ensembles est donc le contexte privilégié pour aborder ces problèmes. Suivant la notation ensembliste de paire, la plus canonique, on écrit alors :

$$(a, x) = \{\{a\},\{a, x\}\} \tag{2}$$

Dans ce contexte notre équation devient :

$$x = \{\{a\},\{a, x\}\} \tag{3}$$

On remarque alors que l'ensemble x est défini en ses propres termes, car x est un élément d'un ensemble qui… est un élément de x. La situation est souvent plus complexe ; en informatique les processus peuvent se croiser, faire des calculs en concurrence, chacun échangeant des messages avec l'autre ou utilisant les résultats du calcul de l'autre. Ceci se formalise par le système :

$$\begin{cases} x = (a, y) \\ y = (b, x) \end{cases} \tag{4}$$

où x fait a, relance ensuite à y, qui fait b et fait appel à x. En termes ensemblistes, on écrira :

$$\begin{cases} x = \{\{a\},\{a, y\}\} \\ y = \{\{b\},\{b, x\}\} \end{cases} \tag{5}$$

Ce système ressemble beaucoup aux équations de (2.). Mais maintenant ce n'est plus la vieille crainte du géomètre grec, mal à l'aise avec le calcul algébrique, qui nous empêche de travailler, c'est plutôt l'interdit de Russell, contre les définitions circulaires, qui nous tombe sur la tête.

> *Whatever involves all of the collection must not be one of the collection*
> (B. Russell, 1908).

Sur cet interdit se sont construites, au cours de ce siècle, des théories logiques remarquables par leur richesse mathématique et leur clarté conceptuelle : le monde stratifié de Russel propageait la *certitude* du bas, des atomes, vers le haut, en les composant par niveaux bien différenciés. Le travail en théorie des ensembles et logique de Zermelo, Fraenkel, von Neumann, Bernays, Gödel et maints autres mathématiciens se focalisa autour de la théorie des types de Russell (sans toujours respecter la forme la plus stricte de stratification) ; le nom et la méthode furent aussi à l'origine des théories des types, de Church jusqu'à Martin-Löf et Girard (on verra que cette dernière viole dès sa première formulation l'interdit).

Quant à l'informatique, l'importance de la notion de type peut être comprise par analogie avec la physique mathématique. *Type*, en logique, correspond à ce qui est, en physique, le concept de *dimension*. On sait que les termes des équations de la physique (force, vitesse, accélération…) possèdent des dimensions. Voilà donc l'intérêt du typage dans les langages de programmation : le contrôle des types donne une méthode partielle, mais efficace, de contrôle de la correction d'un programme. Si le programme est bien typé, il a des bonnes chances d'être correct (bien conçu, bien écrit) ; il n'en a aucune s'il est mal typé, exactement comme pour une équation en physique, dont la dimension doit être la même, avant et après les calculs.

Cette application du typage est une des motivations les plus récentes et une des explications les plus importantes de l'actualité des théories des types. Elle est au moins aussi importante que la recherche des *certitudes stratifiées*, qui en ont motivé l'essor en logique. Le fait que les types correspondent bien aux dimensions de la physique nous confirme qu'il s'agit d'une belle construction, efficace comme la notion de force ou d'accélération en physique. Mais les mathématiques sont des constructions possibles : d'autres parcours que ceux qui en ont été à l'origine peuvent avoir des retombées au moins aussi importantes sur la compréhension du monde. Comme on le verra, on peut avoir des théories de types qui conservent leur fonctions clés (le contrôle de correction partielle, par exemple) tout en présentant des circularités fortement expressives.

Revenons à nos équations circulaires $x \in x$ et $y \in x \in y$. Comme en (2.), avec les équations linéaires, il faut construire une structure mathématique qui soit fermée par rapport à la «bonne» notion structurelle et qui corresponde à la formalisation équationnelle (et à l'intuition qui nous l'a imposée). Bref, il faut construire des univers (ensemblistes) fermés par des chaînes descendantes, car si on admet $\ldots x_n \in x_{n-1} \in \ldots \in x_0$, on a aussi $x \in x$ et $y \in x \in y$. Il s'agit de concevoir des structures fermées par ces chaînes, comme les rationnels sont fermés par les opérations impliquées dans les équations linéaires, la multiplication et la division. Si on libère son esprit des interdits des pères fondateurs, ceci n'est pas difficile à concevoir, car après tout, la notion d'appartenance «$\in$» n'est qu'un ordre partiel et rien n'empêche de concevoir des ordres (partiels) descendants : la suite des entiers relatifs, par exemple. Même si, comme un platonicien naïf, on comprend «$\in$» comme la «vraie» appartenance d'un ensemble à un autre, qu'y a-t-il d'erroné à concevoir une chaîne descendante d'ensembles… $x_n \in x_{n-1} \in \ldots \in x_0$, de plus en plus petits ? Depuis deux ou trois siècles nous avons l'habitude, en mathématiques, de concevoir des limites, des infinitésimaux, des suites *décroissantes* sans fin et des algèbres, comme celle des nombres réels, fermées par ces suites infinies. Si les nombres peuvent être de plus en plus petits, pourquoi les ensembles ne pourraient-ils pas se réduire, en se télescopant l'un l'autre, au-delà de ce qu'on peut voir avec n'importe quel microscope ? Non, pour les *purs et durs* de la stratification, les nombres, nos mesures du monde, peuvent se réduire arbitrairement, tandis que les ensembles commencent, bien visibles, au niveau des *atomes* (les *urelements* des théories des ensembles avec atomes) ou pire, démarrent avec le vide $\emptyset$ et puis, par un acte de création parenthétisée, donnent l'Univers : $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\{\{\emptyset\}\}\}$,…

3.1. AXIOMES D'ANTI-FONDATION (AFA)

Au début du siècle, les théories des ensembles de Cantor et Frege durent être sérieusement revues en raison d'un paradoxe trop connu. On pouvait s'en sortir de plusieurs façons : en restreignant le domaine de la négation, en admettant la formation d'ensembles seulement à partir d'ensembles (axiome de compréhension restreint), en stratifiant l'univers des ensembles par des types. La première solution fut privilégiée dans l'approche fonctionnelle de Church, dont on parlera en (4.) ; les deux dernières solutions furent bien plus largement retenues et développées, en ajoutant généralement une condition supplémentaire : pas de chaînes descendantes d'ensembles ou «tout ensemble est bien-fondé» (axiome de fondation, Fraenkel (1922), et von Neumann, (1925)). Seuls quelques mathématiciens isolés, comme Mirimanoff en 1917 et Finsler en 1926, eurent l'audace d'explorer des sentiers dangereux : les ensembles

«extraordinaires» de Mirimanoff n'étaient pas bien-fondés. Plus récemment on peut citer Specker, en 1957, Dana Scott, dans une note célèbre, mais non publiée de 1960, et Boffa, en 1967 : leurs travaux démontrent entre autres l'indépendance de l'axiome de fondation, en construisant des modèles non-bien-fondés des théories des ensembles plus à la mode, comme ZF, NBG (voir [1] pour une brève histoire de ces chaînes infinies en théorie des ensembles). On peut donc avoir types, ensembles et classes, comme dans ZF, NBG etc… sans axiome de fondation. En d'autres termes on peut violer l'interdit de Russell et continuer à travailler dans des cadres bien solides.

Au cours des années 70, Ennio De Giorgi[2], qui enseignait l'analyse mathématique à la Scuola Normale Superiore de Pise, animait un séminaire de logique. Dans ce séminaire, il proposa, avec l'audace et la naïveté d'un grand mathématicien, un cadre original pour les fondements de l'analyse, qu'il aimait appeler la «théorie cadre». Comme les mathématiciens n'aiment pas subir de restrictions *a priori* dans leurs constructions conceptuelles (encore moins si elles sont dictées par des logiciens en quête de certitudes), il inventa une série d'axiomes, qu'il qualifia de *libre construction*, de nature essentiellement algébrique. Parmi ces axiomes, il y avait différentes constructions possibles de chaînes descendantes. Marco Forti et Furio Honsell, qui participaient à ce séminaire, comme tout mathématicien intéressé par la logique à Pise, développèrent la *Teoria Quadro*, en ajoutant leur propres idées, [8]. Ce travail est aujourd'hui considéré comme un pivot dans l'analyse des axiomes d'anti-fondation (AFA, *anti-foundation axiom*). Des références à leurs nombreux articles se trouvent dans [1] et [5].

Voyons donc de quoi il s'agit. Un système d'équations comme :

$$\begin{cases} x = \{a, y\} \\ y = \{b, x\} \end{cases} \tag{6}$$

spécifie une fonction e de l'ensemble $X = \{x,y\}$ des variables dans l'ensemble $P(X \cup A)$ des parties de l'union de X et de $A = \{a,b\}$, a et b étant des valeurs constantes. Dans ce cas□

$$\begin{cases} e(x) = \{a, y\} \\ e(y) = \{b, x\} \end{cases} \tag{7}$$

DÉFINITION. *Un système (plat) d'équations* est un triplet $E = (X, A, e)$, où X et A sont des ensembles disjoints et e est un fonction de x dans $P(X \cup A)$. Une *solution* s est une fonction de domaine X dans l'univers des ensembles telle que :

$$s(x) = \{s(y) \mid y \in b(x)\} \cup c(x)$$

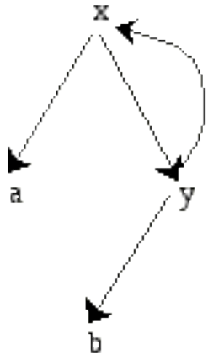
où $b(x) = e(x) \cap X$ est l'ensemble des variables dont x dépend immédiatement et $c(x) = e(x) \cap A$ est l'ensemble de constantes dont x dépend immédiatement.

[2] Ennio De Giorgi est décédé en 1997. Son enseignement, ses idées, son enthousiasme, son talent extraordinaire ont été pour moi, et pour plusieurs générations de mathématiciens italiens, le point de départ de notre travail et une référence permanente.

AXIOME. *Axiome d'Anti-Fondation (AFA)*. Tout système (plat) d'équations E a une et une seule solution s.

On peut donner un modèle simple de l'anti-fondation sur les graphes. Un arbre est un ordre partiel, avec un plus grand élément r (la racine) et tel que pour tout élément a (nœud ou feuille) de l'arbre il existe une seule chaîne $a \leq \ldots \leq r$. Les arbres sont stratifiés : ils n'ont pas de cycles. Un graphe est un ensemble de nœuds et de relations orientées entre nœuds : donc les arbres sont, en particulier, des graphes connectés, avec un élément maximum et sans cycles. Évidemment, graphes et arbres mathématiques peuvent être infinis.

Les arbres permettent d'interpréter la «bonne-fondation», si l'ordre partiel interprète «∈», dans le sens où $a \leq b$ (a est un fils de b) interprète $a \in b$. Les graphes avec cycles donnent des modèles pour l'anti-fondation. Celui représenté ci-dessous est une solution du système d'équations (6).



Plus généralement, la décoration d'un graphe est l'affectation d'un ensemble à chaque nœud du graphe, telle que les éléments de l'ensemble affecté à un nœud soient les ensembles affectés à ses fils. L'axiome AFA devient alors :

Chaque graphe a une et une seule décoration.

Il est clair que l'égalité entre ensembles (ou axiome d'extensionalité) se complique□on ne peut pas contrôler simplement si, à chaque niveau de la stratification, il y a les mêmes éléments, comme en présence de l'Axiome de Fondation. On peut toutefois définir la notion de *bisimulation*, sorte de comparaison entre ordres partiels, qui force l'égalité des ensembles. Il arrive que cette même notion, pour laquelle on renvoie à [1] et [5], est très importante en informatique (les raisons sont celles évoquées en introduction à cette section). Elle permet de comparer des processus différents qui procèdent en s'échangeant des messages, comme dans le *Calculus of Communicating Systems* [24] : en fait, c'est l'analyse sémantique du calcul de Milner qui est à l'origine des travaux de Aczel sur AFA. Notons d'ailleurs que la plupart des systèmes d'ordinateurs sont aujourd'hui distribués, concurrents, et toujours en fonction.

D'autres applications sont présentées dans [5] (sémantique de la logique modale, automates déterministes…). Ce texte donne aussi une preuve de cohérence relative de la théorie ZFA = ZFC+AFA (Zermelo-Fraenkel avec axiome de choix et AFA). On y construit en effet, à partir d'un modèle de ZFC, un modèle de ZFA.

4. DÉFINITIONS RÉCURSIVES DE FONCTIONS ET DE TYPES

En arithmétique on définit souvent des fonctions par récursion ; informellement, une fonction est définie récursivement si sa définition fait appel à elle-même. Un exemple simple de définition récursive primitive est la définition de la fonction factorielle $f(n) = n!$:

$$f(0) = 1 \quad \text{et} \quad f(n) = n \times f(n - 1)$$

Donc $n! = n \times (n - 1)! = 1 \times 2 \times 3 \ldots \times n$.

Une définition récursive peut mélanger en apparence langage et métalangage, comme dans :

$$\mathsf{expo}(x, n) = x \times x \times \ldots \times x, \quad n \text{ fois}$$

où le «n fois» de cette définition informelle reste en dehors du langage-objet (celui auquel appartiennent les symboles de fonctions et les opérations arithmétiques de base). Toutefois, en écrivant□

$$\mathsf{expo}(x, 0) = 1 \quad \text{et} \quad \mathsf{expo}(x, n + 1) = x \times \mathsf{expo}(x, n)$$

on peut traiter le problème. Ces fonctions se décrivent très bien dans maints systèmes inventés pour définir la notion de calculabilité. En particulier si on observe que $( )!$, la factorielle, et expo sont des points fixes pour certaines expressions : celles décrites à la droite des équations qui les définissent formellement.

Le premier de ces systèmes fut la logique combinatoire de Curry (1929). Inspiré par des idées de Schoenfinkel (1924) en algèbre, il se présente comme un système formel basé sur deux symboles S et K et deux axiomes□

$$\mathsf{K}MN = M \quad \text{et} \quad \mathsf{S}PQR = PR(QR)$$

qui permettent de manipuler formellement toute suite finie de S et de K. Ensuite, Herbrand et Gödel proposèrent des systèmes de fonctions, plus «mathématiques», dans leurs fameux ouvrages de 1930 et 1931. Résultat surprenant, ces différentes théories, y compris les révolutionnaires machines de Turing (1936), caractérisent la même classe de fonctions arithmétiques, les fonctions calculables ou récursives partielles ; un résultat démontré en 1936 par différents auteurs, parmi lesquels Kleene et Turing. Au cœur de la preuve d'équivalence se trouve le lambda-calcul de Church (1932), une extension[3] de la logique de Curry (voir [4]).

L'idée de Church fut d'exprimer formellement la dépendance fonctionnelle : si $f(x, y)$, par exemple, est une fonction de deux variables, on *met en évidence* la dépendance de f par rapport à y par la λ-abstraction : $\lambda y.f(x, y)$. Alors, l'application de ce nouveau terme à un argument a devient $(\lambda y.f(x, y))a = f(x, a)$. En considérant une variable à la fois, l'axiome (β) explicite l'opération de remplacement :

$$\text{Axiome } (\beta) \qquad (\lambda x.g(x))a = g(a)$$

Ici l'opérateur d'abstraction λx lie la variable libre x dans $g(x)$, comme $\{x \mid b(x)\}$ lie x dans le prédicat b. Plus formellement, les termes du λ-calcul sont des variables

[3] Les rapports entre logique combinatoire et lambda-calcul ainsi qu'entre leurs modèles sont assez subtils, voir [14].

x, y, z …, et $b(c)$, $\lambda x.b$, si *b, c* sont des termes. Observez que l'on n'a pas interdit *b(b)*. Donc $\lambda x.x(x)$ est un terme du langage. En fait, l'expressivité computationnelle du λ-calcul, provient justement de la possibilité d'exprimer dans le langage le terme :

$$\mathsf{Y} = \lambda y.\lambda x.(y(x(x)))(\lambda x.(y(x(x))))$$

fondé sur l'auto-application. Il est facile d'observer, en utilisant l'axiome (β), que $\mathsf{Y}(b) = b(\mathsf{Y}(b))$, pour tout terme *b*. Donc si on pose $f_o = \mathsf{Y}(b)$, alors $f_o = b(f_o)$. Bref, f_o est définie récursivement, en termes de *b*, c'est-à-dire que f_o est le point fixe de *b*.

Toutefois, il ne faut pas oublier que ces systèmes furent proposés pour travailler en théorie de la démonstration et pour y exprimer les mathématiques et leur logique. On voulait donc avoir dans le langage un terme qui représente la négation, appelons le neg□mais alors, pour $f_o = \mathsf{Y}(\mathsf{neg})$, on a $f_o = \mathsf{neg}(f_o)$, ce qui contredit la signification *entendue* de neg. Ceci constitue le paradoxe de Curry (1932). Remarquez comme ce paradoxe ressemble à celui de Russell en théorie des ensembles. Si on interprète $x \in x$ par $x(x)$ et *l'abstraction d'ensembles*, $\{x \mid b\}$, par l'abstraction fonctionnelle $\lambda x.b$, on obtient alors un autre terme fort intéressant, qui est Y sans les variables *y*

$$(\lambda x.x(x))(\lambda x.x(x)) \sim \{x \mid x \in x\} \in \{x \mid x \in x\}$$

Comme dans le cas de la théorie des ensembles, on peut s'en sortir de différentes façons : soit empêcher, par un interdit russellien, qu'un terme *b* s'applique à lui-même, en stratifiant les termes en différents types, soit restreindre (ou enlever) la négation du langage et conserver $b(b)$. Une conséquence de cette deuxième audace est donc l'existence, dans le langage, du terme $(\lambda x.x(x))(\lambda x.x(x))$, dont l'exécution ne se termine pas : appliquez l'axiome (β) et vous verrez que le terme entre immédiatement dans un cycle. Rien de grave, la divergence essentielle ou *non-arrêt* n'est pas un défaut, comme l'informatique le démontrera plus tard. Encore une fois un paradoxe comme celui de Russell se transforme en richesse expressive, à condition de ne pas poser d'interdits, mais de l'analyser mathématiquement. En fait, la logique combinatoire et le λ-calcul sans types ont une grande expressivité : les fonctions partielles récursives (les fonctions qui peuvent diverger) sont *strictement plus* que les fonctions totales, car il est faux que toute fonction récursive partielle admette une extension totale récursive. Et c'est ainsi que l'on arrive à calculer la même classe de fonctions que les systèmes de Herbrand, Gödel et Turing. De plus, l'absence de négation explicite dans le langage, fait qu'il n'y a pas de paradoxe, la cohérence est démontrée par le théorème de Church-Rosser[4] (1936).

4.1. SÉMANTIQUE MATHÉMATIQUE

Un problème se pose toutefois : quelle est le sens mathématique de l'auto-application, c'est-à-dire de $x(x)$ ou $f(f)$, mais aussi des SSK(SK)KK *sans signification* de la logique combinatoire ? Existe-t-il une *structure mathématique* telle que ses fonctions, ses éléments, puissent *s'appliquer* à eux-mêmes ?

Il suffirait de construire un espace *X* isomorphe à son propre espace $X \to X$ (ou X^X) de fonctions (ou endomorphismes). Ainsi un élément serait aussi une fonction (à un isomorphisme près), une fonction serait un élément et on pourrait interpréter l'application formelle, syntaxique, par l'application fonctionnelle de «tout élément à tout

[4] Un de ses corollaires nous assure que l'on ne peut pas dériver n'importe quelle égalité entre termes.

élément». On voit qu'il suffit de résoudre, comme dans les cas précédents, des équations. Ici il s'agit de l'équation :

$$X = X \to X \tag{8}$$

où «=» est l'isomorphisme dans une catégorie d'objets à construire, comme il fallut construire, à partir des entiers, les rationnels, les réels, ou, dans un modèle de ZFC, les ensembles avec des chaînes descendantes. Les mathématiques des *domaines de calculabilité* ([29]) permettent de résoudre nombre d'équations bien plus complexes, comme□

$$X = A + B \times X + X \to X \tag{9}$$

où les inconnues sont à interpréter comme des ensembles structurés ou des objets de catégories non-triviales (voir [2] pour une synthèse récente). La difficulté est claire ; sauf à prendre X égal à un singleton, aucun ensemble fini ou infini ne satisfait l'équation (1). Par ailleurs le singleton est très peu intéressant, car $X \to X$ (et donc X) doit contenir toutes les fonctions calculables.

La solution de Scott ([29], [30]) est fondée sur la construction d'une catégorie (au sens technique du terme) d'espaces topologiques dont on démontre qu'elle est fermée par les limites de certaines chaînes descendantes d'exponentielles (limites inverses) :

$$\ldots < D_n < D_{n\text{-}1} < \ldots < D_0$$

où $<$ est une *immersion isomorphe* et $D_n = D_{n\text{-}1} \to D_{n\text{-}1}$ est le domaine des endomorphismes continus sur $D_{n\text{-}1}$. À la limite, on obtient $D_\infty = D_\infty \to D_\infty$. Dans un certain sens, cela revient à montrer la structure «non-bien-fondée» de certaines catégories, par rapport à $<$, et à construire des limites.

Encore une fois, une propriété de fermeture d'une structure mathématique suffit à résoudre la circularité syntaxique. Le paradoxe apparent est interprété par un très beau théorème de fermeture ; ses développements en théorie des catégories permettent une analyse fine des différentes structures sémantiques pour la logique combinatoire, le λ-calcul et d'autres systèmes pour la calculabilité (voir [32], par exemple ; dans [23] et [18] on caractérise les modèles de la logique combinatoire, en termes catégoriques, et on classifie les modèles d'autres théories). Les applications en informatique de cette méthode ont été nombreuses. En programmation, on définit souvent les types des données (un type, en informatique , aussi bien qu'en logique, est une collection de données) par des équations du genre :

Valeurs = Constantes + Closures
Environnements = Variables → Valeurs
Closures = Variables × Expressions × Environnements

forme tout à fait similaire à celle de l'équation (8) rencontrée plus haut, bien que plus complexe (voir aussi [2]).

Les méthodes de solution de ces équations, en tant que définitions récursives de types, donnent également une signification (une solution) aux définitions récursives de fonctions. En effet, ces solutions sont données dans des catégories dont les morphismes sont des fonctions continues, ce qui fait qu'une définition récursive (de fonction) est

interprétée comme un point fixe, à la Knaster-Tarski, d'une fonction (d'une fonctionnelle) continue (voir [29], [31], [2]).

5. THÉORIES IMPRÉDICATIVES DES ENSEMBLES ET DES TYPES

5.1 ENSEMBLES

Un ensemble b est défini imprédicativement s'il est donné sous la forme :

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

l'ensemble des x tels que pour tout y dans A on a $P(x, y)$, où b peut être un élément de A, c'est-à-dire de la collection qui sert à le définir.

En fait, l'ensemble infini le plus important qui soit, les entiers $\mathbb{N}$, est défini, en logique classique de façon imprédicative :

$$\mathbb{N} = \{x \mid \forall X\ (\forall y\ (y \in X \rightarrow y + 1 \in X) \rightarrow 0 \in X\ \rightarrow x \in X)\}$$

où X «varie» sur une collection d'ensembles qui contiennent $\mathbb{N}$ (où X peut être l'ensemble $\mathbb{N}$ même que nous sommes en train de définir). Cette dernière définition est au second ordre, car elle utilise des variables (majuscules) dont on suppose qu'elles ont une signification différente de celle des variables du premier ordre (minuscules). De fait, elles varient sur des ensembles, auxquels appartiennent, en tant qu'éléments, les interprétations des variables du premier ordre. La théorie descriptive des ensembles, par exemple, fait un usage intensif des définitions imprédicatives au second ordre, comme dans l'axiome de compréhension que nous venons d'utiliser pour définir $\mathbb{N}$ (voir [25]). Le continu mathématique, avec ses bornes supérieure et inférieure, en tant que «tout» imprédicativement lié à ses parties, est aussi communément donné de façon imprédicative. La représentation de l'espace et, surtout, du temps phénoménologique y gagnent énormément (en analyse, le problème se pose depuis H. Weyl et a été traité en profondeur par maints logiciens comme Kreisel, Wang, Shutte, Feferman, Simpson…, avec des philosophies bien différentes de la nôtre, voir [19], [21]).

5.2. Types

Le système F de J.-Y. Girard est un système où l'on quantifie également au second ordre. Ainsi, si l'on comprend Types comme la collection de tous les types (ou de toutes les propositions), on admet dans le langage le type $\forall X \in \mathsf{Types}.A$, pour tout type A. Ainsi on forme un nouveau type $\forall X \in \mathsf{Types}.A$, en utilisant la quantification sur la collection de tous les types dont fait partie le type même que nous sommes en train de définir. Plus ou moins formellement cela donne :

$$(\forall X \in \mathsf{Types}.A) \in \mathsf{Types} \qquad (10)$$

Grâce à cette forte circularité le système est très expressif. Premièrement, ses termes sont tous typés, on ne perd donc pas ce contrôle partiel de correction que les types permettent (que l'on a comparé au contrôle de dimension en physique) et qui est absent dans les systèmes sans types. De plus, il permet aussi de décrire de manière interne une quantité remarquable de fonctions récursives : toutes celles

démontrablement totales dans l'arithmétique du second ordre, ce qui est vraiment beaucoup (voir [12]).

Malgré cette forte circularité, le système est démontrablement cohérent. Un théorème de normalisation difficile garantit l'impossibilité de la dérivation d'une contradiction. Les enjeux de la preuve sont, en bref, les suivants. D'abord, une forte charge inductive qui entraîne directement la normalisation forte, entre autres. En effet, dans l'induction on utilise le lemme de König qui n'est pas constructif, au sens de l'intuitionnisme orthodoxe. Il affirme que : «tout arbre infini à branchement fini possède une branche infinie». Le problème est que, même si les nœuds de l'arbre sont étiquetés et l'arbre est effectivement engendré (construit par une fonction, un processus calculable) un ordinateur ne pourrait pas trouver la branche infinie. Plus précisément : on ne peut pas donner une règle, écrire un programme, de génération de la branche infinie car l'ordinateur devrait faire des aller-retour d'exploration en effaçant et reconstruisant sa mémoire d'une façon non effective. De plus, la preuve à la Tait-Girard se base sur un axiome de compréhension du second ordre imprédicatif, comme ceux utilisés en théorie des ensembles :

$$\exists X.\forall x(x \in X \rightarrow A(x))$$

Cet axiome permet de *construire* un type à partir d'une formule A arbitraire (voir [12] pour les détails).

Sémantique mathématique des types imprédicatifs

Encore une fois il s'agit de construire des structures mathématiques, des catégories en fait, qui soient fermées pour les opérations visées. Mais quelles opérations ? Une quantification universelle, comme celle qui apparaît dans $\forall X \in \mathsf{Types}.A$, est une conjonction infinie («pour tout X, A est vrai»). Or, la signification catégorique de la conjonction logique «&» est le produit «×», le produit cartésien familier. Il faudra donc construire une catégorie qui soit fermée par produits infinis et indexés sur elle-même. Or, depuis les travaux de Lawvere, la théorie des catégories donne des notions très précises qui correspondent avec rigueur à cette intuition de produit infini, dans les cas du premier ordre comme du second ordre (voir [17], [3]).

Informellement, si la (collection des objets de la) catégorie $\mathcal{T}$ interprète (la collection) Types, il faut interpréter $\forall X \in \mathsf{Types}.A \in \mathsf{Types}$ comme la possibilité que $\mathcal{T}$ contienne le produit qui interprète $\forall X \in \mathsf{Types}.A$, disons $\Pi_{X \in \mathrm{C}} A$, un produit qui, dans le modèle, est indexé sur la catégorie $\mathcal{T}$ elle-même. Bref, il faut associer les notions formelles à gauche aux structures à droite suivant le schéma :

$$\begin{gathered}\mathsf{Types} \sim \mathcal{T} \\ \& \sim \times \\ \forall X \in \mathsf{Types}.A \sim \Pi_{X \in \mathrm{C}} A \\ \forall X \in \mathsf{Types}.A \in \mathsf{Types} \sim \Pi_{X \in \mathrm{C}} A \in \mathcal{T}\end{gathered}$$

Une catégorie avec une telle propriété de fermeture est dite *petite complète* (*small complete*). Le fait qu'une catégorie relativement simple, construite sur les sous-ensembles des nombres entiers, soit petite complète, fut remarqué en 1984 par Eugenio

Moggi[5] à Pise. Son idée a été développée par maints auteurs ([15], [27], [23]). Encore une fois, une propriété de fermeture mathématique donne un sens très solide à une notion logique, les définitions imprédicatives de la théorie des types. Depuis, évidemment, on a construit plusieurs catégories avec cette propriété de fermeture (voir [3]).

Il existe une connexion facile à démontrer entre la sémantique à la Moggi et les modèles du système sans types. Toute structure catégorique qui satisfait l'équation (8) permet de construire un modèle de $\forall X \in \mathsf{Types}.A \in \mathsf{Types}$. Il ne paraît pas possible de faire la construction inverse (il est faux que tout modèle des types imprédicatifs permette de construire un modèle du système sans types). La relation entre anti-fondation et auto-application n'est pas bien connue non plus : il n'y a pas de résultat qui permette ou interdise en général de passer d'un modèle de l'un à un modèle de l'autre.

Le système de types de Girard a connu de nombreuses applications, surtout informatiques. Certains langages de programmation sont fondés sur ce système (CLU, ML polymorphe, Quest,…). Leur sémantique a été donnée dans les termes que l'on vient d'esquisser (voir [6]). En démonstration automatique, Coq est un système construit sur une extension des types imprédicatifs (le calcul des constructions de [7]).

5.3. QUANTIFICATION UNIVERSELLE ET PREUVES

Carnap, dans un article de 1931 sur Erkenntnis, défend contre Russell l'utilisation en mathématiques des définitions imprédicatives. Brièvement résumé, son argument est le suivant. L'enjeu d'une proposition mathématique réside dans la possibilité de la démontrer (ou de pouvoir l'utiliser dans une preuve). Mais, comment pouvons-nous en mathématiques démontrer une propriété donnée sous forme imprédicative, disons $\forall X \in \mathsf{Prop}.A$? Normalement, on n'*examine* pas tous les cas possibles, c'est-à-dire qu'on ne démontre pas $[B/X]A$ pour tout B, ce qui inclurait le cas $B \equiv \forall X \in \mathsf{Prop}.A$, qui relève de la circularité. On démontre plutôt $[B/X]A$ pour B arbitraire ou générique. On voit que même pour comprendre le second ordre, on fait référence au premier ordre, parce qu'en mathématiques, on démontre une propriété $\forall x P(x)$ des nombres réels, en prouvant $P(r)$ pour r arbitraire, sans inspecter chaque réel. Le point essentiel est que l'on n'utilise dans la preuve que le type de r et aucune autre propriété (spécifique) de r. Autrement dit, la preuve utilise seulement le fait que r est un réel (son type donc).

En théorie des types, où les propositions sont des types et les preuves des termes, l'analyse des preuves est suffisamment fine pour nous permettre de mieux définir ce qu'est une preuve par rapport à un élément «générique». De plus, un résultat récent rend très solides les définitions imprédicatives données de manière interne. Dans le système de Girard, la preuve de $A[B/X]$ est un terme a tel que $a \in A[B/X]$. On dira que B est générique et a est prototype, s'il existe $a' : A$ tel que $a'[B/X] = a \in A[B/X]$ (voir [10]). Par l'axiome (β), cela nous permet d'abstraire une preuve de l'énoncé général $\lambda X \in \mathsf{Types}.a' \in (\forall X \in \mathsf{Types}.A)$ car $(\lambda X \in \mathsf{Types}.a')\, B = a'[B/X] = a \in A[B/X]$. Est-ce que la définition de preuve prototype est une bonne définition ? Est-ce qu'elle donne d'une façon canonique une preuve de $\forall X \in \mathsf{Types}.A$? Pour une simple extension de la théorie de l'égalité entre termes, on a le résultat suivant.

---

[5] Dans un message de courrier électronique (!), système d'échange d'informations qui venait de voir le jour.

THÉORÈME. (Généricité). Soit $a, a' \in \forall X \in \mathsf{Types}.A$. Si pour un type B, $a[B/X] = a'[B/X]$, on a alors $a = a'$.

La démonstration est plutôt complexe (voir [20]). Elle assure que, si pour un seul type B, a et a' coïncident, alors il sont égaux partout. Donc, dès que l'on sait que a est une preuve prototype (ce qui est décidable), on a une preuve et une seule de la proposition ou du type universel (le théorème n'est évidemment pas vrai pour la quantification au premier ordre !). En conclusion, au moins pour la théorie des types, la méthode mathématique «des preuves prototypes» sur «argument générique» est bien licite et solide, même (et surtout) dans le cas imprédicatif (voir [10]).

6. LE THÉORÈME DE KRUSKAL ET LA FORME FINIE DE FRIEDMAN

Nous montrons ici le rôle d'un principe structurel du bon ordre et sa relation à l'imprédicativité dans la preuve, grâce à un exemple relativement récent et de très grand intérêt : la version finie du théorème de Kruskal due à Friedman, connue comme FFF (Friedman's Finite Form, voir [9], [13]). FFF est un exemple récent et concret de l'incomplétude de l'arithmétique formelle. C'est-à-dire, on donne un énoncé simple formalisable dans l'arithmétique, FFF, qu'aucun principe de preuve purement syntaxique et finitaire n'arrive à démontrer. Toutefois, le travail sur les structures d'ordre des entiers, des suites finies, des arbres finis et infinis, permet de démontrer l'énoncé, comme propriété des nombres entiers. De plus, l'énoncé implique un principe essentiellement imprédicatif : le bon ordre jusqu'au premier ordinal imprédicatif.

6.1. PAS DE DÉSORDRE TOTAL CHEZ LES ARBRES

- Une relation $\leq$ est un *pré-ordre* si elle est réflexive et transitive.
- Un pré-ordre est un *ordre partiel* si il est aussi antisymétrique, c'est-à-dire si $x \leq y$ 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 suite infinie descendante (c'est-à-dire, $x_{i1} > x_{i2} > x_{i3} > \ldots$).
- 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 est un ensemble qui est donné dans un ordre (total), *i.e.* une suite dans A est une fonction $a : \omega \to A$, où l'ordinal ω représente les entiers considérés comme simple structure bien ordonnée. On note□ $a_n = a(n)$.
- On démontre facilement que tout ensemble bien ordonné réalise l'induction.

DÉFINITION 6.1.1. Un arbre fini T est un ordre partiel avec un plus petit élément, la racine, et tel que, si $a \in T$, alors $\{x \mid x \leq a\}$, la branche qui précède a, est totalement ordonnée.

DÉFINITION 6.1.2. Une immersion entre deux ordres partiels $(P, \leq)$ et $(P', \leq')$ est une fonction $h : P \to P'$ qui préserve les bornes inférieures.

Comme $h(\inf\{p,q\}) = \inf'\{h(p),h(q)\})$, h est monotone, et on note $T \leq T'$ le pré-ordre sur les arbres induit par l'immersion.

THÉORÈME 6.1.3. ([16]). Pour toute suite infinie $\{T_n \mid n < \omega\}$ d'arbres finis, il existe i et j tels que $i < i < \omega$ et $T_i \leq T_j$.

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 de comparables par immersion et dans l'ordre dans lequel la suite a été donnée. Ceci entraîne qu'il ne peut y avoir :

– (bf) de suite infinie descendante d'arbres (c'est-à-dire, $T_{i1} > T_{i2} > T_{i3} > \ldots$),

– (comp) de suite infinie d'arbres tous incomparables.

On déduit que :

COROLLAIRE 6.1.4. Tout pré-ordre qui est une extension de la relation d'immersion entre arbres finis est bien-fondé (c'est-à-dire qu'il ne contient pas de suite infinie descendante. C'est la propriété (bf) ci-dessus).

L'importance de ce simple corollaire est due aux faits suivants qui sont difficiles à démontrer. On commence par construire une fonction surjective et monotone qui a comme domaine les arbres et pour codomaine les ordinaux. Il s'en suit que 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» comme Γ_0 le premier ordinal «imprédicatif» (voir 6.3.), le théorème de Kruskal (6.1.3.) prouve la bonne fondation de ces ordinaux, en raison du corollaire 6.1.4. Or, les ordinaux forment un ordre total, donc l'absence de suites descendantes démontre qu'ils sont bien ordonnés. Ceci implique l'induction jusqu'à Γ_0, car tout ensemble bien ordonné réalise l'induction. En conclusion, 6.1.3. implique la cohérence de l'arithmétique du premier ordre, ou de Peano (PA), et de théories bien plus puissantes, ceci 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, (voir 6.3.) suffit à démontrer la cohérence de PA).

L'énoncé de 6.1.3 est clairement infinitaire, dans le sens où 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). Toutefois, sa preuve n'est pas particulièrement difficile. Elle est basée sur un résultat classique, dû à Higman, concernant les suites finies et infinies, dont on a donné, récemment une version constructive. Mais, dans la preuve de 6.1.3. on utilise un raisonnement par l'absurde pour déduire une formule existentielle ; on développe ensuite une méthode simple, mais strictement infinitaire, à savoir des comparaisons et des choix sur des suites infinies (voir [26] ou [11]). Un passage crucial de la preuve, se base sur le choix de suites de moindre longueur (lemme de Higman) et d'arbres de moindre taille (théorème de Kruskal) dans des ensembles de suites ou d'arbres. Or, puisque la longueur et la taille sont des fonctions à valeurs dans les entiers, l'existence de ces minima est assurée par l'existence d'un plus petit élément pour tout sous-ensemble des entiers.

L'idée de Friedman a été d'obtenir à partir de cet énoncé un énoncé purement finitaire, c'est-à-dire formalisable dans l'arithmétique de Peano (PA).

THÉORÈME 6.1.5. (FFF□ [9], [13]) Pour tout n, il existe un m tel que pour toute suite finie d'arbres finis $T_1, T_2, \ldots, T_m$, telle que chaque T_i ait au plus $n(i+1)$ éléments, il existe j et k tels que $j < k \leq m$ et $T_j \leq T_k$.

L'énoncé, cette fois, a la structure logique suivante : «pour tout n, il existe m suivi de $KF(n,m)$) un prédicat décidable en n et m□», ceci car on sait compter les éléments d'un arbre fini et contrôler, dans une suite finie d'arbres, s'il y en a deux de comparables (c'est donc un énoncé Π_2^0 de PA). Il affirme que, sous une petite condition sur le nombre d'éléments des arbres, même les suites finies d'arbres ne peuvent pas être totalement désordonnées. Sa preuve est une conséquence facile du théorème de Kruskal et du Lemme de König[6]. En bref, on procède par l'absurde : si «il existe un n tel que pour aucun m on a $KF(n,m)$», alors l'argument de compacité à la König donne un contre-exemple à 6.1.3.

Remarquons que ces énoncés (Kruskal, König) sont des théorèmes importants de la combinatoire infinie, car ils ont un nombre important d'applications, en particulier en logique et informatique théorique. En particulier le théorème de Kruskal qui a de nombreuses applications dans les questions de terminaison des systèmes de réécriture. Voilà donc un résultat, relié d'une façon essentielle à l'imprédicativité (le bon ordre jusqu'à Γ_0), qui fait partie des mathématiques applicables (voir aussi 7).

Ce qui est surprenant et difficile à démontrer est que FFF (6.1.5.) n'est pas démontrable dans PA. De 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 [13]). Friedman a en effet démontré que FFF suffit à donner les mêmes conséquences que 6.1.3., à savoir le bon ordre des ordinaux jusqu'à Γ_0, parce qu'il implique qu'il n'y a pas de sous-séquence descendante 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'est-à-dire l'indémontrabilité de la cohérence de PA, dans PA), FFF, qui est un énoncé de PA, n'est pas démontrable par les principes de preuve de PA (ni par des principes bien plus forts), tout en étant une propriété démontrablement vraie des nombres entiers. Notons une fois de plus que tout ceci découle de la grande puissance d'un bon-ordre qui s'étend jusqu'au premier ordinal imprédicatif.

6.2. REMARQUES

Arrêtons-nous sur deux curiosités techniques. Premièrement, FFF est un énoncé de structure syntaxique, $\forall x\, \exists y.KF(x,y)$, or, pour tout n, l'énoncé $\exists y.KF(n, y)$ est démontrable dans PA puisqu'il est vrai□ il suffit d'essayer 1, 2, 3… tôt ou tard on trouvera m tel que $KF(n, m)$, et cette procédure est une preuve, dans PA, de $\exists y.KF(n, y)$. En d'autres termes, si on fixe n, PA démontre $\exists y.KF(n, y)$. Cette preuve est un *schéma de preuve* ou une preuve *prototype* par rapport à un entier n générique (voir 5.3. pour la notion de preuve prototype). Mais on a vu qu'on ne peut pas trouver une preuve prototype dans le langage de PA, c'est-à-dire qu'il n'y a pas de preuve de «pour tout x, il existe y tel que $KF(x, y)$» dans PA, où x serait générique par rapport à tout modèle de PA. En fait, la preuve de $\exists y.KF(n, y)$ dépend strictement du type de

[6] Ce lemme s'énonce : «considérons un arbre, dont chaque élément a un nombre fini de successeurs : si toute branche est finie, il existe alors une borne uniforme pour la profondeur de l'arbre»□ Cette formulation duale de la précédente énonce une propriété de compacité. Le lemme reste tout aussi évident, bien que non-constructif.

n, c'est-à-dire du fait que n soit un entier standard : si la quantification universelle était donnée dans PA, x pourrait être interprété aussi par des entiers non-standard, tandis que, dans la preuve, on utilise explicitement n comme entier standard.

Deuxièmement, 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. On montre que cette fonction croît plus rapidement que n'importe quelle fonction démontrablement totale dans PA. De fait, elle est une des, ou la, plus «rapide» que l'on ait jamais définie, (voir [13]).

6.3. L'IMPRÉDICATIVITÉ ET LES ORDINAUX

L'énoncé FFF n'a rien d'imprédicatif, il appartient au langage de PA. Toutefois sa preuve fait intervenir l'imprédicativité profondément, en raison de la construction ordinale associée. Je vais l'esquisser très brièvement, tout juste au-delà de l'infini.

Comptons : 0, 1, 2, 3… appelons ω la limite de cette suite. Continuons : $\omega + 1$, $\omega + 2$, … $\omega + \omega = \omega 2$, et encore : $\omega 2$, $\omega 3$, … $\omega\omega = \omega^2$. La règle du jeu est claire, continuons à l'appliquer aux 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'est-à-dire $\varepsilon_0 = \phi(1, 0)$, $\varepsilon_1 = \phi(1, 1)$, …, $\varepsilon_\omega = \phi(1, \omega)$, … La fonction $\phi(1, x)$ a également des points fixes ; appelons $\phi(2, x)$ la fonction qui les dénombre… ainsi $\phi(a + 1, x)$ dénombre tout les points fixes de $\phi(a, x)$; si b est une limite, comme ω, ω^2, ω^ω, $\varepsilon_0 = \phi(1, 0)$ ou $\phi(2, 0)$, alors $\phi(b, x)$ dénombre les points fixes de $\phi(a, x)$ pour tout $a < b$.

On pourrait dire que cette construction de la suite des ordinaux n'est qu'un «jeu de symboles». Ce jeu toutefois n'est pas dépourvu de signification. à chaque niveau nous avons détecté une itération et nous avons décidé de passer à la limite. C'est la structure d'ordre des entiers que nous avons étendue en une structure mathématique, celle des ordinaux, par la double opération d'itération et de limite et… d'itération des limites. Notons bien que sa signification n'est que structurelle, car il n'y a pas d'ensembles sous-jacents : ces symboles ne sont pas en général des cardinaux, car, par exemple, il n'existe aucun ensemble X qui satisfasse l'équation $X = \omega^X$, dont ε_0 est la plus petite solution. Ainsi 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'est-à-dire qu'elle est définie pour chaque a, b énumérés de la façon que l'on vient de décrire. En outre 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 la suite qui nous intéresse particulièrement :

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

Sa limite Γ_0 satisfait l'équation $\Gamma_0 = \phi(\Gamma_0, 0)$. Le corollaire 6.1.4. implique le bon ordre des ordinaux (donc l'induction) jusqu'à Γ_0 par une immersion, relativement simple 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 symboles n'utilisait, pour une nouvelle définition, que les précédentes. Même les plus petites solutions des équations posées peuvent être atteintes par le bas, grâce à la construction basée sur la fonction $\phi(y, x)$, comme par exemple, les limites ω et ε_0 puisque $\omega = \phi(0,1)$ et $\varepsilon_0 = \phi(1,0)$. Il n'en va pas de même pour Γ_0, car pour tout $a, b < \Gamma_0$, $\phi(a, b) < \Gamma_0$.

Γ_0 échappe donc à cette construction par «itération + limite», d'une extraordinaire puissance, représentée par la fonction ϕ, fonction qui est donnée 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 fonctionnelle $\phi(y, b)$, 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 qu'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 que nous sommes en train de définir. Contrairement à ce que l'on a vu pour les $a < \Gamma_0$, on ne peut pas faire mieux, c'est-à-dire on ne peut pas atteindre Γ_0 par le bas, grâce aux opérations de l'arithmétique ordinale, voire par ϕ[7].

En conclusion, FFF est un énoncé arithmétique relativement simple et donné d'une façon tout à fait prédicative. Sa preuve toutefois demande un argument très raisonnable mais essentiellement infinitaire, car il n'y a pas de preuve dans PA. En fait, FFF implique la bonne fondation, donc l'induction, jusqu'au premier ordinal imprédicatif, ce qui implique la cohérence de PA. FFF permet de démontrer que la construction mathématique par itération et limites généralisée par les fonctions ϕ donne une structure mathématique, une structure d'ordre bien-fondée, bien que cette structure dont la construction arrive jusqu'à Γ_0 soit imprédicative.

7. THÉORIE DE LA MESURE

Les définitions imprédicatives ne sont pas un artifice de logiciens : elles font massivement partie de la pratique des mathématiques de ce siècle. Rappelons, par exemple, que les ensembles de Borel, sur un espace topologique, sont définis comme «la plus petite collection $\mathcal{B}$ d'ensembles ouverts, fermée par union infinie, intersections et complément». Il s'agit, encore une fois, d'une définition imprédicative : la classe $\mathcal{T}$ de ces collections, sur lesquelles on prend l'intersection (la plus petite dans $\mathcal{T}$, signifie l'intersection sur $\mathcal{T}$) contient la collection… que nous sommes en train de définir. Or,

[7] Cette esquisse informelle a été inspirée par les articles de Smorynski dans [13]. L'imprédicativité de Γ_0 a été démontrée en toute rigueur par Feferman et Schütte.

en théorie de la mesure, *mesurable* veut dire borélien. En fait, la mesure de Lebesgue μ sur X, est donnée par une fonction des boréliens dans les réels :

$$\mu : \mathcal{B} \rightarrow \mathcal{R} \quad \text{telle que} \quad \mu(\bigcup_i A_i) = \Sigma_i\, \mu(A_i), \quad \text{pour} \quad A_i,\, i < \omega.$$

Cette mesure est une probabilité, si on a de plus $\mu(X) = 1$.

Voici donc les notions de base de la théorie générale de l'intégration : on dit que $f : X \rightarrow \mathcal{R}$ est intégrable par rapport à μ si : $f(x) = \lim f_n(x)$ μ-presque partout (partout sauf sur un ensemble de mesure 0), où $f_n = r_0\chi_{A_0} + \ldots + r_n\chi_{A_n}$ avec $r_i \in \mathcal{R}$, et χ_{A_i} la fonction caractéristique de A_i.

On connaît l'importance de ces constructions imprédicatives pour les mathématiques modernes, ce sont elles qui permettent de définir les notions suivantes de mesure⊡

– Mesures dynamiques :

  soit $f : X \rightarrow X$ continue, $\mu : \mathcal{B} \rightarrow \mathcal{R}$ est invariante par rapport à f si $\mu(f^{-1}(A)) = \mu(A)$ pour tout ensemble mesurable A.

– Mesures ergodiques :

  pour tout ensemble mesurable A, $\mu(f^{-1}(A)) = \mu(A)$ et si $f^{-1}(A) = A$, alors $\mu(A) = 0$ ou $\mu(X\text{-}A) = 0$

(pas de $A \subset X$ invariant, comme X et μ, par rapport à f), dont font partie la mesure de Dirac et la mesure de Bowen-Ruelle-Sinai.

Dans l'introduction de cet article, nous évoquions le problème des trois corps. Quel est le rapport entre la circularité apparente de ce problème et l'imprédicativité des outils mathématiques utilisés pour son traitement ? À quel niveau des systèmes d'équations différentielles apparaît-elle ? L'enjeu est majeur, car il n'est pas possible de faire une liste complète des problèmes physiques, dont la représentation informelle et le traitement mathématique utilisent des formes de circularité si bien décrites en logique par les différentes notions rigoureuses de circularité résumées dans cet article. Voici quelques-uns de ces problèmes : les corps dans un champ gravitationnel, les avalanches, les embouteillages routiers, le frottement d'une corde sur un archet de violon, la sédimentation d'une stalactite, les turbulences fluides…

Un des succès des mathématiques de ce siècle est d'avoir pu apporter des réponses significatives à ces problèmes. Un défi pour la logique serait d'essayer de faire une analyse des outils mathématiques employés, en mettant en évidence les définitions et les théories où ces circularités sont essentielles et contribuent à l'expressivité mathématique.

8. ARGUMENTS DISCUTÉS

1. Théorie des ensembles :
   $x \in x$ (auto-appartenance)

2. Définitions récursives :
   des fonctions $f = F(f)$ (auto-application)
   des domaines $A = F(A)$

3. Théories imprédicatives :
   des ensembles $(\forall X \in \mathsf{Ens}.A) \in \mathsf{Ens}$
   des types $(\forall X \in \mathsf{Types}.A) \in \mathsf{Types}$
   Sémantique mathématique de la théorie des types
   Quantification universelle et preuves prototypes

4. Le théorème de Kruskal-Friedman :
   L'imprédicativité et les ordinaux

5. Mathématiques classiques et systèmes dynamiques :
   Théorie classique des réels (et des entiers !)
   Théorie de la mesure de Lebesgue
   Théorie générale de l'intégration
   Systèmes dynamiques

En tant que solutions des équations :

1. Théorie des ensembles :
   $x = \{y, a\}$
   $y = \{x, b\}$

2. Définitions récursives :
   fonctions : $f(n) = n \times f(n - 1)$
   domaines : $X = X + A \times X$

3. Définitions imprédicatives:
   $X = \bigcap\{Y \mid X \subseteq Y \quad \& \quad 0 \in Y \quad \& \quad \forall z(z \in Y \rightarrow z + 1 \in Y)\}$

4. Notations ordinales :
   Γ_0 est le plus petit ordinal tel que $\Gamma = \phi(\Gamma, 0)$

5. Systèmes dynamiques :
   Systèmes d'équations différentielles.

BIBLIOGRAPHIE

[1] ACZEL P., «Non-wellfounded sets», *CSLI Lecture-Notes*, 014, Stanford University, 1988.

[2] AMADIO R., CURIEN P.-L., *Domains and lambda-calculi*, Birkhuaser, 1998.

[3] ASPERTI A., LONGO G., *Categories, Types, and Structures*, MIT Press, 1991.

[4] BARENDREGT H., *The Lambda Calculus; its syntax and semantics*, Revised and expanded edition, North Holland, 1984.

[5] BARWISE J., MOSS L., «Vicious Circles: on the mathematics of non-wellfounded phenomena», *CSLI Lecture-Notes*, 060, Stanford University, 1996.

[6] CARDELLI L., LONGO G., «A semantic basis for Quest», *Journal of Functional Programming*, vol. 1, n° 2, 1991.

[7] COQUAND T., HUET G. «The Calculus of Constructions», *Information and Computation*, 76, 1988, p. 95-120.

[8] FORTI M., HONSELL F.. «Set theory with free construction principles», *Ann. Scuola Norm. Sup. Pisa*, Cl. Sci. (4) 10, 1983, p. 493-522.

[9] FRIEDMAN H., «Independence results in finite graph theory», *Technical Report*, Ohio State University, March 1981.

[10] LONGO G., «Prototype Proofs in Type Theory» [to appear in] *Mathematical Logic Quaterly*, vol. 46, n° 3, (formely: *Zeitscrift f. Math. Logik u. Grundlagen der Math.*), 2000.

[11] GALLIER J., «What is so special about Kruskal's theorem and the ordinal Γ_0?», *Ann. Pure. Appl. Logic* 53, 1991.

[12] GIRARD J.-Y., LAFONT Y., Taylor P., *Proofs and Types*, Cambridge University Press, 1989.

[13] HARRINGTON L. et al. (eds), *H. Friedman's Research on the Foundations of Mathematics*, North-Holland, 1985.

[14] HINDLEY R., LONGO G., «Lambda-calculus models and extensionally», *Zeit. Math. Logik Grund. Math.*, Vol. 26, n° 2, 1980.

[15] HYLAND M., «A small complete category», Lecture delivered at the *Conference Church's Thesis after 50 years*, Zeiss (NL), June 1986, *Ann. Pure Appl. Logic* 40, 1988.

[16] KRUSKAl J., «Well-quasi-ordering and the tree theorem», *Trans. Amer. Math. Soc.* 95, 1960.

[17] LAMBEK J., SCOTT P.J., *Introduction to higher order Categorical Logic*, Cambridge University Press, 1986.

[18] LONGO G., «Set-Theoretical Models of Lambda-Calculus: Theories, Expansions, Isomorphisms», *Annals Pure Applied Logic* 24, 1983.

[19] LONGO G. «Some aspects of impredicativity: notes on Weyl's philosophy of Mathematics and on todays Type Theory», *Logic Colloquium 87*, *Studies in Logic*, Ebbinghaus and al. (eds), North-Holland, 1989.

[20] LONGO G., MILSTED K. and SOLOVIEV S., «The genericity theorem and the notion of parametricity in the polymorphic Lambda-calculus», *Theor. Comp. Sci.*, vol. 121, 1993.

[21] LONGO G., «The mathematical continuum, from intuition to logic», *Naturalizing Phenomenology: issues in comtemporary Phenomenology and Cognitive Sciences*, J. Petitot et al. (eds.), Stanford U.P., 1999.

[22] LONGO G., MOGGI E., «A category-theoretic characterization of functional completeness», *Theor. Comp. Sci.*, vol. 70, n° 2, 1990.

[23] LONGO G., MOGGI E., «Constructive Natural Deduction and its omega-Set Interpretation», *Mathematical Structures in Computer Science*, vol. 1, n° 2, 1991.

[24] MILNER R., TOFT M., «Co-induction in relational semantics», *Theor. Comp. Sci.*, vol. 87, 1991.

[25] MOSCHOVAKIS Y.N., *Descriptive Set Theory*, North-Holland, 1980.

[26] NASH-WILLIAMS C., «On well-quasi-ordering of finite trees», *Proc. Cambridge Phil. Soc.* 59, 1963.

[27] PITTS A., «Polymorphism is Set Theoretic, constructively», *Symposium on Category Theory and Comp. Sci.*, SLNCS 283, Pitt and al. (eds.), Edinburgh, 1987.

[28] POINCARÉ H., *La Science et l'Hypothèse*, Flammarion, 1968.

[29] SCOTT D., «Outline of a mathematical theory of computation», *4th Ann. Princeton Conf. on Info. Syst. Sci.*, 1970.

[30] SCOTT D., «Continuous lattices», *Toposes, algebraic Geometry and Logic*, Lawvere (ed.), SLNM 274, Springer-Verlag, 1972, p. 97-136.

[31] SCOTT D., «Lambda-calculus, some models, some philosophy», *The Kleene Symposium*, Barwise and al. (eds.), North-Holland, 1980.

[32] SMYTH M., PLOTKIN G., «The category-theoretic solution of recursive domain equations», *SIAM Journal of Computing* 11, 1982.