Yvon Gauthier

Logique arithmétique

L'arithmétisation de la logique

Logique de la science 王

PUL

DU MÊME AUTEUR

L'arc et le cercle. L'essence du langage chez Hegel et Hölderlin, Desclée de Brouwer et Bellarmin, Paris et Montréal, 1969.

Fondements des mathématiques. Introduction à une philosophie constructiviste, Presses de l'Université de Montréal, Montréal, 1976.

Méthodes et concepts de la logique formelle, Presses de l'Université de Montréal, Montréal, 1978, 2e éd., revue, corrigée et augmentée, 1981.

Théorétiques. Pour une philosophie constructiviste des sciences, Le Préambule, Longueuil, 1982.

De la logique interne, Vrin, Paris, 1991.

La logique interne des théories physiques, Vrin et Bellarmin, Paris et Montréal, 1992.

La philosophie des sciences. Une introduction critique, Presses de l'Université de Montréal, Montréal, 1995.

Logique et fondements des mathématiques, Diderot, Paris, 1997, 2e édition, 2000.

Logique interne. Modèles et applications, Diderot et Modulo, Paris et Montréal, 1997.

Internal Logic. Foundations of Mathematics from Kronecker to Hilbert, Kluwer, "Synthese Library", Dordrecht, Boston et London, 2002.

La logique du contenu. Sur la logique interne, L'Harmattan, Paris, 2004.

Entre science et culture. Introduction à la philosophie des sciences, Presses de l'Université de Montréal, Montréal, 2005.

Logique arithmétique

Logique de la science 王

Cette collection accueillera des ouvrages consacrés à la logique et à la philosophie des sciences entendues dans leur sens formel. La logique de la science, un titre emprunté au philosophe américain C.S. Peirce, rend compte de la logique interne du savoir qui peut se décliner en plusieurs versions et il est légitime de parler de logiques au pluriel comme on parle de sciences au pluriel. L'éventail des recherches pourra s'ouvrir pour inviter des analyses portant sur l'intersection et l'héritage commun des traditions philosophiques et scientifiques. Enfin, les travaux d'épistémologie générale ou historique dans les sciences sociales et humaines ne sauraient être exclus dans cet esprit d'ouverture qui doit caractériser l'idée d'une logique interne du discours scientifique. Si le principe de tolérance invoqué par le logicien et philosophe des sciences R. Carnap doit présider à une telle entreprise, c'est pour mieux assurer le rôle de la philosophie comme vigile du savoir.

王

Le symbole utilisé pour représenter la collection signifie la quantification «effinie» ou illimitée de la logique arithmétique et il est tiré de l'idéogramme pour «wang», roi en langue chinoise.

Yvon Gauthier

YVON GAUTHIER

Logique arithmétique

L'arithmétisation de la logique

Presses de
l'Université Laval

Les Presses de l'Université Laval reçoivent chaque année du Conseil des Arts du Canada et de la Société d'aide au développement des entreprises culturelles du Québec une aide financière pour l'ensemble de leur programme de publication.

Nous reconnaissons l'aide financière du gouvernement du Canada par l'entremise de son Programme d'aide au développement de l'industrie de l'édition (PADIÉ) pour nos activités d'édition.

Maquette de couverture : Hélène Saillant

ISBN 978-2-7637-8997-2

Dépôt légal 3e trimestre 2010

Les Presses de l'Université Laval
Pavillon Maurice-Pollack
2305, rue de l'Université, bureau 3103
Québec (Québec) G1V 0A6
CANADA
www.pulaval.com

À la mémoire de mes parents,
Blanche et Armand

Remerciements

Cet ouvrage a été publié grâce à une subvention de la Fédération canadienne des sciences humaines, de concert avec le programme d'aide à l'édition savante (PAES), dont les fonds proviennent du Conseil de recherche en sciences humaines du Canada.

Table des matières

Avant-propos

Le projet d'une logique arithmétique, c'est-à-dire d'une logique interne de l'arithmétique, n'est pas nouveau et mes travaux antérieurs l'ont exploré amplement. Je voudrais dire ici en quoi la logique arithmétique comme thèse fondationnelle diffère d'une philosophie de l'arithmétique.

Frege et Husserl, chez les logiciens et philosophes, ont conçu des philosophies de l'arithmétique sur des vues divergentes de l'arithmétique. L'entreprise du mathématicien Kronecker est plus difficile à évaluer au point de vue philosophique et peu de chercheurs se sont attaqués à la tâche d'en définir la portée fondationnelle. Dans ce contexte, le psychologisme de Husserl pourrait être contrasté avec le constructivisme de Kronecker. Husserl connaissait les travaux de Kronecker qu'il avait eu comme professeur à Berlin. Ou encore, il faudrait voir comment le logicisme de Frege s'oppose à ce que l'on peut bien appeler l'arithmétisme de Kronecker, si l'on entend par arithmétisme la thèse kroneckerienne d'une réduction de toutes les mathématiques au socle premier de l'arithmétique.

Mes travaux récents (voir [42], [43]) ont mis en évidence le clivage entre arithmétique pure ou théorie des nombres entendue au sens des arithméticiens et arithmétique formelle ou arithmétique de Peano (ou de Dedekind-Peano) qui est l'objet privilégié des logiciens et à laquelle j'oppose l'arithmétique de Fermat-Kronecker dans la tradition de la théorie des nombres (au sens de A. Weil [107]) ; l'arithmétique de Peano a pour assises la sémantique ensembliste, c'est-à-dire la théorie des ensembles de Cantor qu'il considérait comme une arithmétique transfinie.

Je suivrai dans un premier temps les destins parallèles de ces deux arithmétiques, l'arithmétique transfinie et l'arithmétique que Kronecker appelait l'arithmétique générale « *allgemeine Arithmetik* », c'est-à-dire l'arithmétique des formes ou des polynômes homogènes (cf. [73], [74]). L'arithmétique polynomiale se retrouve aujourd'hui au centre des préoccupations des mathé-

maticiens, alors que l'arithmétique transfinie est toujours le fonds commun des recherches logiques, que ce soit en théorie des modèles ou en théorie des démonstrations.

Les recherches logiques depuis Hilbert, Zermelo, Skolem, Gödel et Tarski jusqu'aux travaux récents sur les sous-systèmes de l'arithmétique et l'implantation informatique des théories logiques, e.g. la théorie intuitionniste des types dont la justification philosophique s'inspire de la théorie husserlienne, ont exploité ce fonds à satiété.

Y a-t-il un parallélisme entre arithmétique formelle et arithmétique pure ou sont-ce là des entreprises radicalement différentes ? Bien ancré dans une posture philosophique, le constructivisme logicomathématique radical que je défends depuis le début, j'essaierai de voir dans un deuxième temps si le programme de Kronecker qui a engendré le programme de Hilbert (voir [42]) n'est pas en mesure de reprendre à son compte une philosophie de l'arithmétique et, par extension, une option fondationnelle en mathématiques que l'on a associée depuis toujours au constructivisme.

Avec le bilan de la logique depuis Hilbert, il apparaît pertinent de tirer des conclusions philosophiques générales sur les fondements de la pratique logique et mathématique, particulièrement en arithmétique. Il importe aussi de revenir sur les distinctions fondamentales qu'il faut faire pour bien comprendre les enjeux de l'arithmétique pure ou théorie des nombres et l'arithmétique formelle ou l'arithmétique de Peano. Un seul exemple suffira à mesurer la distance entre les deux disciplines : alors que le logicien parlera volontiers d'ensemble dénombrable ou d'ensemble récursif (ensemble récursivement énumérable avec complément aussi bien récursivement énumérable), l'arithméticien se contentera de dire « dénombrable à l'infini », comme il dirait « à la limite » sans hypostasier cet infini ou cette limite dans une sémantique ensembliste (réaliste) avec un ordinal infini ω ou un cardinal infini $\aleph_0$. La distinction n'est pas sans effet sur la posture philosophique du mathématicien ou du logicien — et du philosophe.

En effet, mes travaux sur la logique interne ont montré que la notion de consistance — ou non contradiction — interne de l'arithmétique constructive ou arithmétique de Fermat-Kronecker est une notion qui n'est pas exclue par le résultat classique de Gödel sur les preuves de consistance de l'arithmétique de Peano (second théorème d'incomplétude de Gödel) et qu'elle peut coexister avec cette dernière sans l'invalider : l'arithmétique de Peano apparaîtrait dans ce contexte comme une extension infinitaire de l'arithmétique constructive n'obéissant pas aux mêmes contraintes formelles d'effectivité ou

de computabilité. La méthode de descente infinie de Fermat est ici opposée à l'induction complète de Peano et à l'induction transfinie de Gentzen : une preuve formelle de leur non équivalence sera le motif de l'annexe *A* du présent ouvrage. En fait, ces résultats sur la consistance interne et externe étaient acquis dans mes travaux publiés en français et en anglais depuis vingt ans (voir [35], [37], [38], [42], [44]). Dans les conférences récentes sur « The Collapse of the Hilbert Program », le philosophe et logicien américain Saul Kripke serait parvenu à des conclusions similaires récemment en utilisant l'argument de la descente infinie pour montrer l'effondrement « interne » du programme de Hilbert du point de vue oméga de Gödel dans l'arithmétique ensembliste (Peano). Comme je l'ai aussi montré (voir [36], p. 118, [38], p. 78 et [39], p.38), la descente infinie a été introduite par Mirimanoff [83] avec son idée de la descente finie pour les ensembles « ordinaires » ou transitifs qui a inspiré l'axiome de fondation et la théorie des ordinaux de von Neumann dans la structure cumulative des rangs de la théorie axiomatique des ensembles (Zermelo-Fraenkel) ; ces ensembles transitifs ont leur équivalent dans les modèles minimaux (sur les ensembles au bas de la hiérarchie) de la théorie des modèles — ces exemples sont aussi repris par Kripke. Évidemment, mon utilisation de la descente infinie va dans le sens contraire, celui d'une preuve de consistance interne pour l'arithmétique de Fermat-Kronecker et Gödel a au moins reconnu la possibilité d'une telle preuve — l'interprétation *Dialectica* va d'ailleurs dans ce sens pour l'arithmétique récursive primitive.

En réalité, c'est la logique formelle classique depuis sa création par Frege qui est ici remise en question. Je ne veux pas revoir à nouveaux frais les brèves analyses que j'ai consacrées au projet frégéen du logicisme (voir [42]), mais étayer mon hypothèse de la dualité logicisme-arithmétisme. On sait que la thèse logiciste de Frege reprise par Russell a échoué. La thèse arithmétiste, que j'attribue à Kronecker, est plus vivante que jamais avec les avancées du programme de Langlands en géométrie arithmétique et les résultats de finitude de la géométrie algébrique contemporaine, sans parler des exigences d'effectivité ou d'arithmétisation (ou encore de polynomialisation) de l'informatique théorique actuelle.

Je veux insister en particulier sur le retournement de la question de Frege : « jusqu'où peut-on aller en arithmétique par la seule voie déductive ? ». Cette question inaugurale de la logique formelle doit être révisée dans le sens de la question d'inspiration kroneckerienne : « jusqu'où peut-on aller en logique par la seule voie arithmétique ? ». C'est dans cette perspective qu'il m'apparaît légitime de parler d'arithmétisation de la logique après l'arithmétisation

de l'analyse mathématique. Les travaux récents sur Frege, ceux de G. Boolos (voir [9]) et R. Heck en particulier ont montré qu'on pouvait récupérer la consistance du système de Frege avec le principe de Hume dans une théorie axiomatique du deuxième ordre, mais qu'un tel sauvetage se faisait au profit de l'arithmétique et minait le programme logiciste. Sans défendre la thèse quinienne de la limitation de la logique aux théories du premier ordre, il est possible d'aller beaucoup plus loin et soutenir, par exemple, que la voie déductive est tout entière traduisible dans ce que j'appelle la logique polynomiale modulaire où la notion de déduction est réductible à la relation arithmétique de congruence. L'inférence logique et la notion de conséquence seraient dès lors arithmétisables et le statut indépendant du logique fortement ébranlé. L'interprétation polynomiale repose sur un isomorphisme interne entre formules logiques et polynômes, isomorphisme que je veux exploiter aux fins d'une défense et illustration de l'hypothèse arithmétiste. La preuve syntaxique de la consistance interne de l'arithmétique avec descente infinie que l'on trouvera dans l'annexe B constitue l'illustration la plus importante de l'option fondationnelle constructiviste que je défends.

Le but ultime de toutes ces analyses est de fournir une théorie fondationnelle de l'arithmétique du point de vue philosophique de la tradition constructiviste, des Grecs à Kant et aux recherches logiques contemporaines. La perspective est ici critique. Si les Grecs pensaient que l'arithmétique était au fondement de la logistique « *logistikê* », c'est-à-dire le calcul, ils n'ont pas pris toute la mesure du constructivisme et si Kant a pensé que les mathématiques étaient constructives, il a confiné leur fondement dans un *a priori* transcendantal. D'un point de vue philosophique radical, la philosophie de l'arithmétique reste à faire. Le logicisme et le formalisme ne sont plus des options fondationnelles praticables, l'intuitionnisme brouwerien et post-brouwerien n'apparaît plus que comme un semi-constructivisme ; seuls demeurent comme options viables le réalisme et le constructivisme que l'on identifie parfois à une forme d'antiréalisme. L'arithmétique peut se dispenser d'une ontologie des objets abstraits et le réaliste trouvera difficile de surimposer aux opérations du calcul quelque ciel platonicien. Le constructiviste aura la tâche de montrer que les fondements arithmétiques supportent tout l'édifice des mathématiques.

Dans cette tâche, André Weil, le grand mathématicien français de la théorie des nombres, aura été un guide. Il avait suggéré aux philosophes de pratiquer l'histoire des mathématiques plutôt que la philosophie des mathématiques et surtout la logique qui n'avait pour lui que le rôle ancillaire d'une

hygiène des mathématiques. Certains hygiénistes-logiciens n'ont pas apprécié le rôle de serviteurs ou d'adjuvants qui leur était ainsi dévolu et ont reproché amèrement à André Weil de ne pas admettre, par exemple, la méthode diagonale de Cantor comme méthode de preuve valide en théorie des nombres. On sait que la diagonalisation est au coeur des théorèmes d'incomplétude de Gödel et de maints autres résultats de la logique classique, mais la plupart des mathématiciens et plusieurs théoriciens des modèles en logique mathématique reconnaissent que le phénomène d'incomplétude n'affecte pas plus que 20% des mathématiques ou de la pratique mathématique. En théorie des modèles, des praticiens comme Hrushovski ou van den Dries et MacIntyre confessent que les travaux de André Weil en géométrie algébrique ou arithmétique ont été déterminants dans leurs résultats récents. Or il faut rappeler que la méthode privilégiée de André Weil dans ses théorèmes les plus importants était la méthode de la descente infinie de Fermat qu'il a mise en oeuvre dans la théorie des corps quadratiques ; cette méthode de preuve est constructive et n'est pas équivalente à la méthode de preuve par induction complète, comme le pensent trop souvent les logiciens éloignés de la pratique mathématique — je propose la démonstration de cette non équivalence dans l'annexe A. Il faut rappeler aussi que André Weil a été l'un des premiers à mettre l'accent sur l'importance de Kronecker en théorie des nombres et en géométrie arithmétique.

Gentzen pensait que la descente infinie était une forme déguisée de l'induction complète dans son calcul des séquents qu'il considérait comme une exemplification de sa théorie du raisonnement linéaire « *lineares Räsonieren* ». D'autres logiciens en ont tiré des variantes en théorie des preuves qui, elle, est manifestement tributaire des résultats d'incomplétude et tout empêtrée dans une sémantique ensembliste, celle des ordinaux transfinis générés eux aussi par diagonalisation ou induction transfinie. La sémantique ensembliste sur laquelle s'appuie la théorie des preuves aussi bien que la théorie des modèles ne peut transcender ou quitter l'univers infinitaire de l'ensemble $\mathbb{N}$ des nombres naturels qu'au prix de constructions comme les notions d'hyperfini ou de nombre « surnaturel » qui naviguent dans un continu non dénombrable et qui n'ont plus de fonction logique autre que celle de clôture du domaine d'un calcul. Une autre direction de la théorie des preuves semble plus fertile, la théorie des preuves appliquée(s), s'attache justement — dans ce qui avait été appelé jadis la théorie réductive des preuves — à réduire les preuves de théorèmes de l'analyse classique à leur contenu constructif, mais les méthodes logiques mises en œuvre ici pour extraire le minerai (*proof mining*)

de sa gangue non constructive ne sont souvent qu'à demi constructives, dans le mesure où l'on a recours à des techniques imprédicatives, combinatoires ou fonctionnelles — comme l'interprétation *Dialectica* de Gödel — pour la détermination des bornes du domaine d'un calcul encore cette fois (voir [69] et [45]). Herbrand avait déjà formulé l'hypothèse que tous les théorèmes en théorie des nombres ayant recours à des méthodes transcendantes devaient avoir leur pendant élémentaire, c'est-à-dire sans moyens analytiques (voir [56] et [33]). Il ne faut pas oublier non plus que les théorèmes analytiques ont leur équivalent arithmétique. Cela est évident pour le dernier théorème de Fermat et l'hypothèse de Riemann sur les zéros de la fonction ζ a sa contrepartie dans la suite raréfiée des nombres dits « surabondants » pour la somme des diviseurs d'un nombre donné, par exemple 12 est la somme de ses diviseurs $2, 4, 6$. Mais les « mathématiques expérimentales », c'est-à-dire les mathématiques de la computation à l'aide de l'ordinateur ne peuvent fournir une preuve directe dans la recherche d'un contre-exemple. En l'absence d'un contre-exemple, une instance numérique n'est qu'un « *no-no-counterexample* », comme je l'ai expliqué dans mon article de 1978 [32]. À chaque fois cependant qu'on s'éloigne du calcul, on s'éloigne de l'arithmétique et de l'idéal arithméticien. L'idée d'une logique arithmétique (polynomiale) est la poursuite de cet idéal fondationnel par des moyens logico-mathématiques, historiques et philosophiques sous le triple signe du constructivisme finitiste de Kronecker, de la logique interne inaugurée par Hilbert et de l'arithmétique de Fermat pratiquée par André Weil, dont j'ose me réclamer après qu'il m'eût encouragé à explorer la descente infinie ; par surcroît, je ne me défends pas du « bourbakisme » dont on m'a déjà accusé. Leibniz pensait que « raisonner, c'est calculer » et son impératif était « *Calculemus !* ».

Dans la perspective critique de la recherche fondationnelle, la reconstruction historique du discours mathématique, logique ou philosophique n'est pas celle de l'historien, mais plutôt celle du chercheur qui voit sa discipline du point de vue contemporain pour lequel l'histoire est récessive et les théories actuelles autant de réductions ou « réduits », au sens de l'industrie acéricole, de leur histoire. Un bel exemple est le cas de Hilbert. Nombre d'historiens vont insister sur les oscillations, vacillements ou retournements des vues de Hilbert sur la question des fondements, alors que le logicien ou le philosophe insistera sur la cohérence de la pensée d'un auteur et voudra rattacher la posture initiale à la version finale d'un projet original dans la continuité d'un programme — ici le programme de Hilbert. Ainsi la question du fondement simultané ou parallèlle de la logique et de l'arithmétique du texte hilber-

tien de 1918 « La pensée axiomatique » (*Axiomatisches Denken*) est refoulée au profit des travaux postérieurs « Sur l'infini » (*Über das Unendliche*) de 1926 et du finitisme des dernières oeuvres qui renouent avec les premières ébauches métamathématiques placées sous le signe du nombre « *ünter dem Zeichen der Zahl* » comme le dit Hilbert et dont la pierre angulaire est le chiffre « *Ziffer* », l'inscription concrète du nombre. Kronecker, pratiquement ignoré des historiens, n'a pas connu ces avatars historiques. À la fin, la trame historique que j'ai tissée de Kronecker à la géométrie arithmétique et à l'informatique théorique contemporaines n'est pas continue, mais j'ai marqué de pierres blanches le parcours que j'ai tracé de la logique formelle de Frege et Hilbert à nos jours.

Ce qu'il importe de noter dans ce contexte, c'est que la reconstruction philosophique ne sert pas les buts d'une théorie positiviste du savoir mathématique ou scientifique, mais cherche à mieux circonscrire les enjeux contemporains de l'entreprise fondationnelle. Il ne s'agit par de refaire une histoire ou de redéfinir les concepts d'une tradition de recherche, mais de leur donner un nouvel élan et de les propulser dans des labeurs futurs. Un bel exemple en est la discussion critique autour d'une oeuvre comme celle d'Ulrich Kohlenbach en théorie concrète des preuves « *applied proof theory* » qui relance le programme de Hilbert avec les nouvelles armes de la prospection fondationnelle (voir mon article *Classical Function Theory and Applied Proof Theory* [45]). Il ne s'agit aucunement de réécrire l'histoire dans ce cas, mais de montrer la filiation des idées dans la continuation d'un programme par des moyens nouveaux. C'est dans cet esprit qu'a été conçu mon travail.

Le constructivisme arithmétique doit aussi produire une théorie de la pratique mathématique qui intègre une philosophie du savoir scientifique en général couvrant aussi bien les sciences exactes que les sciences sociales. Une question fondamentale dans cette perspective est celle de l'applicabilité des mathématiques et un volet important de cette question est certainement le statut des mathématiques appliquées, en premier lieu le statut de la physique mathématique en regard de la thèse arithmétiste. Si les mathématiques doivent avoir un contenu numérique, comme le proclamait E. Bishop, un des grands promoteurs du constructivisme mathématique contemporain, on ne peut négliger d'évaluer le problème de l'applicabilité des mathématiques. Une solution frégéenne à ce problème consisterait à supposer le principe huméen de l'égalité extensionnelle — un nombre appartient à la fois à F et G, ssi F et G sont des concepts équinumériques — pour garantir l'applicabilité sémantique des mathématiques. Mais cette garantie passe par l'existence des

ensembles au sens de la sémantique ensembliste qui suppose au moins l'accessibilité de l'ensemble infini des nombres naturels ; l'appartenance des objets physiques à des ensembles infinis s'apparente à la participation platonicienne des objets sensibles aux Formes ou Idées du ciel intelligible. Le détour par la sémantique ensembliste et la théorie des modèles qui en est issue interdit la voie arithmétiste. Frege n'avait pas de notion de modèle, mais Hilbert l'avait dès 1899 avec le modèle de l'arithmétique des nombres réels dans sa preuve de consistance de la géométrie élémentaire. Ce sont les travaux de Hilbert et de son collaborateur J. von Neumann qui posent véritablement la question des fondements constructivistes de la physique mathématique avec les notions d'appareil analytique « *analytischer Apparat* » et de conditions de réalité « *Realitätsbedingungen* ». Hilbert avait même conçu l'idée d'une « logique physique » (« *physikalishe Logik* »), une idée que je voudrais explorer dans un prochain ouvrage. Ces travaux débouchent sur la notion de probabilité et on peut se demander si une théorie constructive des probabilités, comme l'a proposée E. Nelson, ne pourrait pas servir de pont entre les sciences physiques et les sciences sociales. En tout cas, c'est là tout un ensemble de problèmes que ne peut manquer d'aborder une philosophie des mathématiques soucieuse de s'intégrer à une épistémologie du savoir scientifique. La théorie constructiviste du discours scientifique est fondée sur l'hypothèse que les diverses logiques internes des savoirs particuliers sont reliées par un fonds commun de ressources et d'opérations des sujets du savoir dont on peut rendre compte dans une théorie fondationnelle d'orientation constructiviste. Ce programme est déjà en marche et s'appuie sur les assises de la logique arithmétique que j'expose dans le présent ouvrage.

J'ai rédigé l'essentiel de ce travail durant une année sabbatique (2007-2008) avec l'aide d'une subvention du CRSH que je remercie. Je remercie vivement Lawrence Deck qui a non seulement réalisé la version LaTeX de mon manuscrit, mais qui en a corrigé les nombreuses épreuves avec une vigilance et une diligence exemplaires.

Introduction. Logicisme

L'idée d'une logique interne de l'arithmétique ou logique arithmétique est inspirée par des motifs divers dans les fondements des mathématiques. Le développement de la logique mathématique au vingtième siècle, de Hilbert jusqu'à nous, semble suivre un fil continu si on l'interprète comme mouvement de l'arithmétisation de la logique. L'arithmétisation de l'analyse chez Cauchy, Weierstrass et Dedekind et l'arithmétisation de l'algèbre chez Kronecker ont abouti aux recherches fondationnelles d'un Hilbert. Les travaux de Frege sur les fondements logiques des mathématiques, de l'arithmétique avant tout, ont contribué à mettre en clair ses motifs philosophiques et bien que le logicisme de Frege n'ait pas atteint ses buts, il a donné naissance, paradoxalement pourrait-on dire, à la théorie des types de Russell et, dans une certaine mesure en vertu du même paradoxe, à la hiérarchie cumulative des rangs dans la théorie axiomatique des ensembles de Zermelo en même temps qu'il inaugurait la logique philosophique et la philosophie du langage.

Mais l'« arithmétisme » que l'on pourrait opposer au logicisme n'est pas pour autant radicalement anti-frégéen dans la mesure où l'on peut mettre côte à côte la question « Jusqu'où peut-on aller en logique avec la seule arithmétique ? » et la question frégéenne « Jusqu'où peut-on aller en arithmétique avec les seuls moyens de la logique ? ». La source première de l'arithmétisme, c'est l'arithmétique polynomiale de Kronecker et le but de l'ouvrage est d'aller jusqu'au bout d'un programme constructiviste kroneckerien dans l'arithmétisation (et l'algébrisation) de la logique au vingtième siècle – on peut voir dans ce projet la suite de mon livre *Internal Logic : Foundations of Mathematics from Kronecker to Hilbert* [42] et la continuation, si ce n'est l'achèvement, du projet d'une logique arithmétique.

Hilbert est le point de départ de l'arithmétisation de la logique ; c'est lui qui introduit la logique en mathématiques et s'il a voulu un moment fonder la logique et l'arithmétique en même temps, il s'est rendu compte plus

tard que la logique devait être arithmétisée pour avoir accès à une preuve de consistance de l'arithmétique et il a finalement adopté une posture fondationnelle finitiste qu'il a héritée de son ancien professeur, Kronecker. Skolem a aussi conçu une arithmétique finitiste et la théorie des suites de choix de Brouwer avec son assignation de nombres naturels aux membres d'une espèce (ensemble) a précédé l'arithmétisation de la syntaxe d'un système formel (l'arithmétique de Peano) chez Gödel. Les tentatives subséquentes d'une solution du problème de la consistance de l'arithmétique chez Ackermann, Herbrand, Gentzen *et alii* ont suivi la même piste. Herbrand est pourtant le seul à s'être limité aux ressources d'une arithmétique finitiste dans son essai d'une preuve de consistance de l'arithmétique, alors qu'Ackermann et Gentzen ont emprunté librement la voie de la théorie des ensembles transfinis en recourant à l'induction transfinie sur les ordinaux de la seconde classe de nombres de Cantor avec $\lim \omega = \varepsilon_0$. Le certificat de naissance de la théorie des modèles, la méthode de l'élimination des quantificateurs de Tarski, quant à elle, doit être rattachée à la méthode de substitution-élimination des indéterminées que Kronecker a élaborée dans sa théorie polynomiale. La théorie des démonstrations de l'arithmétique du premier ordre et de ses sous-systèmes témoigne encore du programme d'arithmétisation et finalement l'idée même d'algorithme et ses ramifications en théorie de la complexité, en algèbre computationnelle et en informatique théorique (langages de programmation), doit être mise au compte des gains du programme d'arithmétisation de la logique.

L'arithmétique transfinie de Cantor est partie intégrante de l'arithmétisation de l'analyse et il est facile de dépister les raisons qui ont fait déboucher l'entreprise cantorienne dans une théorie des ensembles transfinie ou transarithmétique. Mais l'analyse peut-elle être constructivisée ? Brouwer a répondu : oui, dans une certaine mesure. Bishop, inspiré davantage par Kronecker que par Brouwer, comme il l'avoue dans [6], a pensé que l'analyse pouvait être arithmétisée, c'est-à-dire que l'analyse avait un contenu numérique qu'il fallait dégager de sa gangue analytique. L'analyse non standard va encore plus loin en voulant accorder un statut arithmétique (non archimédien) aux infinitésimaux. La théorie cantorienne des ensembles est cependant devenue la sémantique standard de la logique classique et de l'arithmétique de Peano et il n'est pas aisé de défaire la syntaxe arithmétique de la sémantique ensembliste des théories logiques contemporaines, que ce soit la théorie des types constructive ou intuitionniste de Martin-Löf ou d'autres théories apparentées comme les mathématiques régressives (Friedman et Simpson) ou les mathématiques prédicatives (Feferman). L'arithmétique prédicative

de Nelson se dresse en solitaire comme programme radical, programme que plusieurs trouvent trop restrictif pour servir de guide fondationnel.

D'un point de vue philosophique, le programme ultrafinitiste d'un Yessenin-Volpin est trop éloigné de la pratique mathématique et les vues finitistes d'un Wittgenstein ne semblent pas être assez près de la logique mathématique du vingtième siècle. Ce qui est en jeu, ce n'est pas l'existence des entités logiques ou mathématiques, les éléments idéaux que Hilbert a introduits pour les éliminer ensuite à titre de simple détour, ce n'est pas non plus l'objectivité des constructions mathématiques publiques, mais bien plutôt le contenu arithmétique (computationnel ou algorithmique) d'une théorie logique ou mathématique. La réalité « objectuelle » des mathématiques se résume ultimement aux différentes façons de compter les objets physiques et les entités non physiques et au compte rendu du dénombrable et du non dénombrable, si tant est qu'il existe des nombres affectés d'un signe négatif (nombres négatifs et nombres transcendants ou non algébriques). L'attitude de Kronecker en ces matières a souvent été caricaturée et on ne peut que rappeler avec force que l'arithmétique polynomiale de Kronecker qu'il appelée arithmétique générale « *allgemeine Arithmetik* » a joué un rôle prédominant dans la genèse de l'algèbre abstraite chez les Hilbert, Noether et van der Waerden entre autres. Il faut garder à l'esprit que la géométrie algébrique ou arithmétique contemporaine a pris sa source dans les travaux de Kronecker sur les fonctions elliptiques, comme l'a montré André Weil, et que l'idéal arithméticien de Kronecker se retrouve aujourd'hui dans les vastes programmes de Langlands et de Grothendieck. La théorie algébrique des nombres a aussi bénéficié immensément de la théorie arithmétique des grandeurs algébriques — le travail classique de Kronecker en 1882 *Grundzüge einer arithmetischen Theorie algebraischen Grössen* (Traits fondamentaux d'une théorie arithmétique des grandeurs algébriques) [74] — et Hermann Weyl a mis l'accent sur les avantages que possédait la théorie kroneckerienne des domaines de rationalité « *Rationalitätsbereiche* » sur la théorie des idéaux de Dedekind.

La théorie élémentaire ou ordinaire des nombres a été l'arène des premières axiomatisations par Dedekind et Peano. Les fonctions récursives et l'idée de récurrence (Poincaré) sont apparues tôt. Dedekind est considéré comme l'initiateur de ce mode de pensée dans son ouvrage classique de 1888 « *Was sind und was sollen die Zahlen ?* » (Que sont et que doivent être les nombres ?) [20], mais la procédure est déjà exploitée chez Kronecker dans sa théorie des formes ou polynômes homogènes. Les axiomatisations de Dedekind et de Peano sont fondées sur la théorie des ensembles de Cantor et elles

sont tellement imprégnées de la sémantique ensembliste que la motivation arithmétique en est obnubilée. Hilbert sera plus conscient de l'arrière-plan arithmétique aussi bien dans son travail sur les fondements de la géométrie que dans sa métamathématique consacrée à la formalisation des mathématiques dans un système fini d'opérations arithmétiques et d'équations (et inéquations ou inégalités) polynomiales.

L'oeuvre de Kronecker est encore largement ignorée ailleurs que chez les mathématiciens et parmi les meilleurs. Logiciens et philosophes ne connaissent que son texte « *Über den Zahlbegriff* » (Sur le concept de nombre) qui n'est pas son travail le plus important et de loin. Frege, pour un, n'a mentionné le nom de Kronecker qu'une seule fois et c'était pour l'associer à Helmholtz — que Kronecker cite à la fin de son texte sur le concept de nombre — au même titre d'empiriste, le discréditant ainsi comme non logicien à ses yeux. La plupart des philosophes et des logiciens (et des mathématiciens qui ne sont pas parmi les meilleurs !) se satisfont d'attribuer à Kronecker la célèbre maxime « Dieu a créé les entiers, l'homme a créé tout le reste » sans se soucier d'en trouver la source exacte. C'est sans doute Hilbert qui, sur le ton du ressentiment, a infligé ce mot à Kronecker tout en le décrivant comme un dictateur de l'interdit « *Verbotsdiktator* » à la suite de Cantor.

L'arithmétisation de la logique s'est amorcée sans la contribution de l'algèbre de la logique avant Tarski. Boole, de Morgan, Peirce, Schröder ou plus tard Löwenheim n'ont pas été partie prenante dans le processus, à l'exception de Boole qui a influencé l'algébrisation de la logique classique élémentaire qu'il a liée à la théorie des probabilités dans son ouvrage de 1854 *An Investigation of the Laws of Thought*. Mais on devrait sans doute insister ici plutôt sur la séparation entre arithmétique et théorie des nombres. La tradition de la théories des nombres de Fermat, Euler, Gauss, Legendre, Lagrange, Dirichlet jusqu'à Kummer et Kronecker s'est développée de façon autonome — en tant que reine des sciences, comme aimait le dire Gauss. La théorie classique des nombres n'est pas sur le même pied que l'arithmétique de Dedekind-Peano et on devrait s'entendre sur le fait qu'il n'y a pas de lien historique entre la théorie des nombres et l'arithmétique formelle de la filière logique. La logique arithmétique est cependant vouée à combler le fossé entre logique et arithmétique — la « vraie » arithmétique de la théorie des nombres et non l'arithmétique ensembliste — et ce faisant a abondamment recours à la méthode de la descente infinie de Fermat toujours présente dans l'oeuvre des praticiens contemporains de la théorie des nombres de Mordell à Weil. La descente infinie combinée à l'arithmétique polynomiale de Kronecker sera

l'ingrédient essentiel dans le programme d'une logique arithmétique que je veux définir en regard de programmes alternatifs en fondements des mathématiques — on trouvera dans le second appendice les éléments essentiels de cette logique arithmétique. Du coup, je veux lier dans un seul faisceau fondationnel les questions historiques, philosophiques, logiques et mathématiques de la logique arithmétique afin de proposer un traitement unifié de la question philosophique et du problème mathématique de la consistance de l'arithmétique. Le programme de l'arithmétisation de la logique trouve sa justification finale dans la logique interne de l'arithmétique, une logique interne qui montre que l'arithmétique doit être autoconsistante si elle doit être la pierre de fondation de la logique et des mathématiques.

Chapitre 1

L'arithmétisation de l'analyse

C'est Félix Klein qui a coiffé de l'expression « arithmétisation de l'analyse » le mouvement « arithmétiste » de la fin du XIXe siècle. L'idée de l'arithmétisation de l'analyse évoque immédiatement les noms de Cauchy, Weierstrass, Cantor et Dedekind et à un moindre degré ceux de Dirichlet, Abel, Grassmann et Bolzano ; le processus de l'arithmétisation connote le besoin de rigueur dans les fondements de l'analyse en recourant à ce que Cauchy appelait l'analyse algébrique, qui devait surmonter les limites intuitives des méthodes géométriques du passé. L'histoire de l'arithmétisation de l'analyse a déjà été racontée (voir Grattan-Guinness [51]) ; ce n'est pas une histoire à sens unique, parce que la notion de rigueur avait un sens différent du nôtre et que les instruments de sa mise en application (e.g. formes quadratiques et polynômes) étaient déjà disponibles avant le XIXe siècle. La symbolisation algébrique avait déjà envahi la géométrie et la théorie des nombres (e.g. les équations diophantiennes) avec Fermat allait devenir la reine des sciences mathématiques.

1.1 Cauchy et Weierstrass

Dans l'introduction de son *Cours d'analyse* de 1821, Cauchy avertit que :

> Mais ce serait une erreur grave de penser qu'on ne trouve la certitude que dans les démonstrations géométriques de l'analyse, ou dans le témoignage des sens ([16], p. VII.)

et il propose de rechercher cette certitude dans les fondements algébriques de l'analyse ; il amorce dès lors son étude des fonctions réelles et de leurs

limites, des polynômes comme fonctions continues et des séries convergentes et divergentes. Cauchy parle toujours en termes de quantités infiniment petites ou infinitésimaux, mais il les identifie avec des limites approchées par les fonctions d'une variable réelle. Il introduit alors le produit de convolution — appelé aussi produit de Cauchy par la suite — pour les séries convergentes et les séries récurrentes ou polynômes dans l'ordre croissant ou décroissant de leurs puissances. Les résultats importants de Cauchy dans ce domaine concernent la définition précise des limites 0 et ∞ pour une quantité infinie :

> Lorsque les valeurs successivement attribuées à une même variable s'approchent indéfiniment d'une valeur fixe, de manière à finir par en différer aussi peu que l'on voudra, cette dernière est appelée la limite de toutes les autres. ([16], p. 19.)

Pour les valeurs numériques, cette limite sera appelée l'infini positif ∞ ou l'infini négatif $-\infty$; ce sont là des quantités infinies, souligne Cauchy. Weierstrass ne s'est pas contenté de la notion de variable approchant une limite. Dans son texte « *Theorie der Maxima und Minima von Functionen einer und mehreren Veränderlichen* » (Théorie des maxima et minima d'une ou plusieurs variables), Weierstrass innove avec son idée de la méthode ϵ-δ :

> Pour une fonction $f(x)$, on dit que sa valeur à $x = a$ est un minimum quand elle est inférieure pour $x = a$ à toutes les valeurs avoisinantes de x, c'est-à-dire quand une quantité positive δ peut être déterminée telle que
>
> $$f(a + h) - f(a) > 0$$
>
> avec $|h| < \delta$. Et la valeur d'une fonction $f(x)$ pour $x = a$ est appelée un maximum, quand on a pour toutes les valeurs avec la restriction $|h| < \delta$
>
> $$f(a + h) - f(a) < 0.$$
>
> ([105], vol. 7. p. 4.)

Weierstrass montre alors que pour la dérivée

$$f(a + h) - f(a) = hf'(a + \epsilon h)$$

une quantité ϵ est requise avec la condition suffisante

$$0 < \epsilon < 1\,;$$

la première condition nécessaire pour un minimum ou un maximum de $f(x)$ à $x = a$ est que $f'(a) = 0$ et la seconde condition nécessaire est que dans la suite des dérivées, la première dérivée qui ne s'annule pas pour $x = a$ doive être d'ordre pair. Weierstrass continue en généralisant ces conditions aux fonctions de plusieurs variables.

Le fait important est que Weierstrass s'exprime ici dans le langage des formes (polynômes) quadratiques : ce sont là les fondements arithmétiques par excellence dans la tradition de la théorie des nombres depuis Gauss. Bien sûr, Bolzano avait déjà démontré la propriété de continuité des polynômes et Weierstrass n'avait qu'à définir une forme définie positive dont les valeurs s'annulent comme une forme dont les variables ont toutes la valeur 0 ([105], vol. VII, p. 20). Plus loin, Weierstrass s'intéresse au théorème de Sturm sur les changements de signes dans les racines réelles d'une équation algébrique ; Kronecker s'est aussi appliqué à raffiner le théorème de Sturm par la localisation «*Isolierung*» des racines réelles d'une équation algébrique dans des intervalles définis à l'aide d'égalités et d'inégalités algébriques tout en critiquant le théorème des valeurs intermédiaires de Bolzano qu'il trouvait imprécis et même faux, puisque l'intervalle des valeurs n'était pas rigoureusement défini, même si Bolzano avait cru arithmétiser les preuves intuitives (géométriques) pour la continuité des fonctions. Bien plus, Kronecker vilipende Bolzano (voir J. Boniface et N. Schappacher [8], p. 269) pour avoir utilisé les moyens les plus frustres «*mit den rohesten Mitteln*» pour obtenir son résultat qui ne peut s'appliquer aux racines d'une fonction entière. Si Bolzano a voulu donner une preuve purement analytique (i.e. non géométrique) de son théorème, il est demeuré obsédé par l'image de la courbe qui coupe l'axe des y, mais la courbe d'une fonction trigonométrique ne se laisse pas facilement visualiser, conclut Kronecker. La version simplifiée que donne Weierstrass du théorème des valeurs intermédiaires se lit :

> Si une fonction continue $f(x)$ définie sur un intervalle est parfois positive $x > 0$ et parfois négative $x < 0$, elle doit être zéro à un point donné.

L'histoire de l'arithmétisation de l'analyse ne s'arrête pas là et Cantor et Dedekind allaient prendre un nouveau virage en prolongeant les méthodes plus ou moins constructives de leurs prédécesseurs dans des avenues qui n'avaient plus rien de constructif.

1.2 Dedekind et Cantor

Du côté de Dedekind, l'arithmétisation est une entreprise logique dans la mesure où preuve et prouvable sont entrelacés dans les constructions mathématiques ; la logique qu'il envisage est interne à l'arithmétique ou science des nombres «*Wissenschaft der Zahlen*». Les nombres irrationnels selon Dedekind doivent trouver leur fondement dans l'arithmétique, mais si les fondements sont par définition abstraits et généraux — puisque la science des nombres est *a priori* et indépendante de l'espace et du temps — il faut trouver des assises concrètes à l'arithmétique. C'est pour cette raison que Dedekind parle de choses « *Dingen* » et de système de choses « *Systeme von Dingen* »). Bien plus, ces pierres de taille seront assemblées en suivant des lignes abstraites comme les applications « *Abbildungen* » et leurs images « *Bilder* », mais les chaînes « *Kette* » demeurent les liens concrets pour les lignes d'assemblage des choses et de leurs systèmes. Dans le train de pensée de Dedekind, le point culminant est sa définition d'un système infini comme un système en bijection avec l'un de ses sous-systèmes propres (excluant le système lui-même) ; autrement un système est fini. La preuve de cet énoncé a été diversement accueillie — certains l'ont reléguée au rang de preuve psychologique ou métaphysique — ; Dedekind invoque ici le monde de mes pensées « *meine Gedankenwelt* » en tant que système infini actuel, alors qu'il dit expressément que le monde de mes pensées, c'est-à-dire la totalité des choses qui *peuvent* être l'objet de ma pensée est infinie, ce qui suggérerait un infini potentiel tout au plus (Dedekind [20], p. 14). Ce n'est pas sans raison que Dedekind note qu'il y a des considérations similaires dans les *Paradoxien des Unendlichen* (Paradoxes de l'infini) du platonisant Bolzano. On peut penser qu'il y a ici un tiraillement entre les potentialités arithmétiques et l'actualité ensembliste d'un monde transcendantal (transarithmétique). Dans l'esprit de Dedekind, le système des nombres naturels avec l'induction complète comme système bijectif $\mathbb{N} \to \mathbb{N}$ simplement infini est une construction allant de soi. Par ailleurs, la construction des nombres rationnels et irrationnels dans « *Stetigkeit und irrationale Zahlen* » (Continuité et nombres irrationnels) est effectuée dans le plus pur style arithmétique des mathématiques réelles :

> Je vois toute l'arithmétique comme une conséquence nécessaire ou à tout le moins naturelle de l'opération arithmétique la plus simple, le comptage, et le comptage lui-même comme rien de plus que la création successive de la suite illimitée des entiers positifs. ([20], II, p. 5.)

La notion de chaîne apparaît alors comme l'enchaînement des nombres dans leur succession naturelle ; les nombres rationnels, si on les met sur la droite réelle, sont situés à gauche ou à droite d'un point donné et sur une droite continue il y a une infinité de points qui ne correspondent à aucun nombre rationnel. L'essence de la continuité réside dans le principe suivant :

> Si nous coupons la droite en deux segments (classes) de telle façon à mettre tous les points du premier segment à gauche de tout point du second segment, alors il y a un seul point qui divise l'ensemble des points en deux segments de la droite. ([20], II, p. 10.)

Une coupure « *Schnitt* » (A_1, A_2) signifie que tout nombre rationnel dans A_1 est plus petit que tout nombre dans A_2 et qu'il y a un plus grand nombre dans A_1 ou un plus petit nombre dans A_2. Il s'ensuit immédiatement qu'il y a une infinité de coupures sur la droite réelle qui ne sont pas engendrées par des nombres rationnels qui, par conséquent, ne peuvent couvrir la droite continue dans sa totalité. Ainsi un nombre irrationnel comme $\sqrt{2}$ est représenté par une coupure irrationnelle. L'ordre total et la complétude au sens de Dedekind de la droite réelle sont des propriétés qui découlent directement de la construction des coupures, puisque supremum et infimum sont des conséquences du théorème stipulant qu'il n'y a qu'un seul nombre qui « coupe » en deux le système de tous les nombres réels. Dedekind a aussi supposé que sa théorie des coupures s'appliquait aisément au calcul différentiel et à l'analyse infinitésimale en vertu du rôle capital joué par le concept de continuité.

Pour nous, ce qui importe c'est l'accent que met Dedekind sur la construction arithmétique du continu réel ; pour lui, le principe recteur, en dépit de ses résonances ensemblistes, est le procès arithmétique qui permet de prolonger de façon naturelle l'arithmétique ordinaire dans l'arithmétique supérieure (théorie des nombres et algèbre) et l'analyse. Dans le même esprit arithmétique, Cantor est allé plus loin dans une arithmétique transfinie qui épuiserait non seulement les points de la droite réelle, mais l'esprit arithmétique lui-même par immersion dans l'univers ensembliste.

Au point de départ, Cantor s'est intéressé à la théorie des nombres et à l'algèbre, comme ses premiers travaux l'attestent (voir Cantor [15]). Ainsi, sa dissertation de 1867 traite des formes quadratiques et l'une de ses thèses est que les méthodes purement arithmétiques doivent prendre le pas sur les méthodes analytiques. Ces premiers écrits semblent cependant n'être que des exercices sur des problèmes soulevés par les théoriciens des nombres, de

Legendre à Kronecker (son professeur à Berlin), jusqu'au moment où il aborde le vaste terrain des fonctions trigonométriques où son talent mathématique fait ses vrais débuts. Cantor hérite de Riemann et de Heine le problème de la représentation unique (canonique) d'une fonction de variables réelles $f(x)$ par une série trigonométrique convergente pour toutes les valeurs de x. Une série trigonométrique s'écrit comme chez Cantor

$$f(x) = \frac{1}{2}a_0 + (a_1 \sin x + b_1 \cos x + \ldots + a_n \sin nx + b_n \cos nx) + \ldots$$

i.e. une expansion de Fourier d'une série trigonométrique où les a et les b sont des constantes et n un entier non négatif. Au cours de ses travaux sur la représentation canonique, Cantor a su mettre à profit des remarques de Kronecker pour la simplification de sa preuve ; la simplification consistait à évacuer des infinitésimaux à l'aide de deux expressions arithmétiques $y + x$ et $y - x$ où y est une constante afin d'annuler les coefficients infinitésimaux $\lim c_n = 0$ dans

$$\lim(c_n nx) = 0 \quad \text{pour } n = \infty.$$

Le rejet des infinitésimaux chez Cantor vient sans doute du programme d'arithmétisation de Kronecker ! Mais Cantor a vite fait de trouver un autre emploi pour les limites infinies dans sa théorie des ensembles dérivés de points. Cantor ne s'en est pas tenu longtemps en effet aux simplifications et aux restrictions arithmétiques suggérées par Kronecker et en voulant généraliser son résultat de 1872 sur les séries trigonométriques, il élabore une théorie des points limites « *Grenzpunkte* » ou points d'accumulation « *Haüfungspunkte* » d'inspiration géométrique (avec coordonnées cartésiennes), même si la théorie ressemble à l'entreprise arithmétique de Weierstrass — un autre de ses professeurs à Berlin — à première vue. L'inclination infinitaire de Cantor est visible dans sa propension à inclure l'infini aussi bien que le fini dans ses recherches mathématiques ; pour Cantor, le point limite d'un ensemble de points est un point sur la droite tel que tout voisinage de ce point contienne une infinité de points, mais à l'intérieur « *in seinem Innern* » de l'intervalle réel. Nous avons ici les linéaments de la topologie ensembliste. Cantor dénote par P' l'ensemble des points limites d'un ensemble de points P. Si ce premier ensemble dérivé P' contient un ensemble infini de points, nous avons un second ensemble dérivé de points (noté P'') et ainsi de suite jusqu'à P^ν pour le ν-ième ensemble dérivé. La construction d'une série illimitée d'ensembles dérivés de points ouvre la voie à la théorie des suites fondamentales d'ordre

arbitraire

$$\lim_{\nu\to\infty}(\alpha_{\nu+\mu}-\alpha_\nu)=0$$

et en général

$$\lim_{\nu\to\infty}\beta_\nu=\beta.$$

Ces suites fondamentales qui nous rappellent les suites de Cauchy sont en réalité des dérivées d'ordre infini et là où Cauchy voyait une limite finie, Cantor a pris ce symbole de limite comme une coupure radicale avec les vues traditionnelles. Il écrit :

> On doit attirer l'attention sur ce point cardinal dont le sens peut être facilement mal interprété dans la troisième définition du nombre réel — à l'aide des suites fondamentales comme
>
> $$\lim_{\nu\to\infty}\alpha_\nu=b$$
>
> un nombre b n'est pas défini comme la limite des parties α_ν d'une suite fondamentale (α_ν) ; ce serait là un erreur logique semblable à la discussion de notre première définition (de la limite comme somme) où l'existence de la limite
>
> $$\lim_{\nu\to\infty}\alpha_\nu$$
>
> serait seulement supposée ; c'est plutôt l'inverse que nous avons ici, puisque nos définitions antérieures du concept b avec ses propriétés et ses relations dans le système des nombres rationnels nous permettent de conclure avec certitude que la limite α_ν existe et est égale à b. Pardonnez mon insistance sur cette apparente vétille « *Kleinigkeit* ». ([15], p. 187.)

Cantor continue en affirmant que les nombres irrationnels ont droit au même statut de réalité déterminée « *bestimmte Realität* » dans notre esprit que les nombres rationnels. La limite

$$\lim_{\nu\to\infty}\alpha_\nu=b$$

existe réellement et les ordres arbitraires des suites fondamentales existent aussi bien. Dans les mots de Cantor, ce n'est pas un procès à la limite qui nous donne le nombre irrationnel, mais c'est la possession véritable de la limite (dans notre esprit) qui nous permet de comprendre ce qu'est le procès ou

l'approximation de la limite. C'est ici il me semble que Cantor rompt radicalement avec la tradition arithmétique et un mathématicien comme Poincaré objectera par la suite que ce n'est pas le procès fini qui est une approximation de l'infini, mais plutôt l'infini qui est une approximation du fini...

Je vois dans le passage cité plus haut le certificat de naissance de la théorie des ensembles transfinis avec la génération illimitée des ordres des suites fondamentales devenant des ordinaux de la seconde classe de nombres des ω définie par

$$\lim_{n\to\infty} \omega^{\omega^{\cdot^{\cdot^{\omega}}}} \Big\} \, n = \epsilon_0$$

et plus explicitement

$$\begin{aligned}
\omega &= \lim < 0, 1, 2, \ldots n > \\
\omega \cdot 2 &= \lim < \omega n > \\
\omega^2 &= \lim < \omega \cdot n > \\
\omega^\omega &= \lim < \omega^n > \\
\omega^{\omega^\omega} &= \lim < \omega^{\omega^n} > \\
\epsilon_0 &= \lim < \omega^{\omega^{\cdot^{\cdot^{\omega}}}} \Big\} \, n > .
\end{aligned}$$

Cantor a même imaginé une troisième classe de nombres

$$\epsilon_0, \epsilon_\nu, \ldots, \epsilon_\omega, \epsilon_{\omega+1}, \ldots$$

dans une hiérarchie transfinie d'ordinaux, mais la totalité Ω de tous les ordinaux, comme la totalité « *taw* » de tous les cardinaux ne serait pas un ensemble, mais une pluralité absolument inconsistante « *eine absolut inkonsistente Vielheit* ». Il n'y guère de doute cependant que Cantor a conçu sa théorie des nombres transfinis comme une extension ou un prolongement du continu arithmétique (voir Cantor [15], p. 190 et ss.). Le premier principe de génération « *Erzeugungsprinzip* », comme il l'explique, est celui de l'addition d'une unité à un nombre donné — c'est la première classe de nombres, les ordinaux finis — le second principe de génération applique simplement la même procédure aux ordinaux limites ω jusqu'à ϵ_0. En plus de ces deux principes de génération, il y a un troisième principe de limitation « *Hemmungsprinzip* » qui opère seulement sur les totalités de nombres déjà définies par les deux principes de génération : c'est un principe de clôture qui enclôt les totalités déjà complétées, permet de passer outre et d'aller plus loin encore dans le transfini. Dans le même texte de 1882 « *Über unendliche lineare Punktmannigfaltigkeiten* » (Sur les multiplicités linéaires infinies d'ensembles de

points). Cantor formulait son hypothèse du continu

$$\aleph_0 < 2^{\aleph_0} = \aleph_1$$

qu'on n'a pas réussi à démontrer jusqu'ici — on sait cependant que la cardinalité du continu c est probablement supérieure à $\aleph_1$. À cette époque, Cantor voulait sans doute construire sa propre théorie des multiplicités « *Mannigfaltigkeitslehre* » à la suite de Riemann qui avait conçu une théorie des mutiplicités n-dimensionnelles (appelées maintenant variétés) en géométrie différentielle. L'analogie est certainement présente dans l'esprit de Cantor lorsqu'il fait mention de continua n-dimensionnels ayant la même cardinalité ou la même puissance « *Mächtigkeit* » que le continu linéaire, i.e. $c = 2^{\aleph_0}$. Brouwer a montré par la suite qu'au-delà de la caractérisation ensembliste, il n'y a pas d'homéomorphisme entre continua de dimensions différentes.

Je n'ai pas le dessein de faire le tableau complet du paradis cantorien des ensembles, mais seulement de décrire les éléments essentiels qui seront toujours actifs dans la tradition ultérieure de l'arithmétisation. Nous savons que Hilbert voulait laisser la porte du paradis cantorien ouverte aux éléments idéaux et il a même espéré démontrer l'hypothèse du continu — le premier problème de sa célèbre liste de 1900 — mais il est revenu au port terrestre de Kronecker à la fin, laissant à ses élèves Ackermann et Gentzen l'induction transfinie sur les ordinaux de la deuxième classe de nombres pour la preuve de consistance de l'arithmétique. Peano de son côté a hérité du modèle ensembliste pour sa théorie axiomatique de l'arithmétique, mais a laissé à d'autres le soin de construire une logique arithmétique. Gödel a mis à profit la méthode diagonale de Cantor dans sa preuve d'incomplétude pour l'arithmétique de Peano, mais il a renoncé à l'arithmétique ordinale transfinie dans sa tentative ultérieure d'une preuve de la consistance de l'arithmétique.

J'esquisse la méthode diagonale en suivant le texte de Cantor de 1890 (Cantor [15], pp. 278-281) « *Über eine elementare Frage der Mannigfaltigkeitslehre* » (Sur une question élémentaire de la théorie des multiplicités). Cantor introduit la méthode diagonale dans la démonstration du fait que l'ensemble $P(X)$ des parties d'un ensemble infini X est strictement plus grand que X ou que card $X <$ card $P(X)$. Déjà en 1874 ([15], pp. 115-118) Cantor avait montré que l'ensemble $\mathbb{R}$ des nombres réels n'est pas dénombrable par un argument portant sur les nombres algébriques de la forme

$$a_0\omega^n + a_1\omega^{n-1} + \cdots + a_n = 0$$

— ici les ω sont simplement des nombres réels et le polynôme décrit a un degré fini n, ce qui implique que les nombres algébriques sont dénombrables. La totalité (ω) peut être mise en suite

$$\omega_1, \omega_2, \ldots, \omega_n, \ldots$$

Recourant au théorème de 1844 de Liouville sur l'existence de nombres irrationnels transcendants (non algébriques) qui ne peuvent qu'être approchés par des nombres rationnels, Cantor conclut que s'il y a autre chose et plus dans l'intervalle réel que les nombres algébriques irrationnels, ces nombres doivent être non dénombrables. La méthode diagonale semble être une méthode constructive de prime abord, mais il ne faut pas s'y méprendre. Cantor commence avec un système infini M de coordonnées dont les éléments $(x_1, x_2, \ldots, x_\nu)$ n'ont que deux « caractères » m et w et il établit une matrice infinie de suites E de ces éléments

$$\begin{aligned} E^I &= (m, m, m, m, \ldots) \\ E^{II} &= (w, w, w, w, \ldots) \\ E^{III} &= (m, w, m, w, \ldots). \end{aligned}$$

Il suppose que la totalité de ces suites n'est pas en bijection avec les suites de nombres naturels, donc n'est pas dénombrablement infinie de cardinalité $\aleph_0$. On n'a qu'à montrer que dans la matrice infinie des suites représentant les nombres naturels

$$\begin{aligned} E_1 &= (a_{1,1}, a_{1,2}, \ldots, a_{1,\nu}, \ldots) \\ E_2 &= (a_{2,1}, a_{2,2}, \ldots, a_{2,\nu}, \ldots) \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ E_\mu &= (a_{\mu,1}, a_{\mu,2}, \ldots, a_{\mu,\nu}, \ldots) \end{aligned}$$

n'épuise pas M, l'ensemble des nombres réels dans l'intervalle (m, w) ou $(0, 1)$ puisque la suite

$$E_\nu = (b_1, b_2, b_3, \ldots)$$

définie par $b_\nu \neq a_{\nu,\nu}$ ne s'y trouve pas, l'élément b_ν étant différent de tout élément a_ν dans la diagonale de E_1 à E_μ. Les éléments b_i sont pris sur l'antidiagonale ou sur la codiagonale, comme je préfère dire, puisqu'ils sont tirés du complément $\mathbb{R} - \mathbb{N}$ qui doit contenir tous les nombres naturels. Plutôt que l'expression de Liouville

$$|x - p/q| > M/q^n$$

où x est un nombre algébrique irrationnel de degré n, p, q et M étant des entiers, nous avons chez Cantor

$$\operatorname{card}\mathbb{N} < \operatorname{card}\mathbb{M}$$

pour $\mathbb{N}$ l'ensemble des nombres naturels et $\mathbb{M}$ la totalité « *Inbegriff* » des nombres réels. La méthode de Cantor n'en est pas moins existentielle ou non constructive, puisque on peut choisir librement les éléments diagonaux dans le complément $\mathbb{M} - \mathbb{N}$ qui soient différents de tous les éléments dans la liste diagonale dénombrable, d'où la conclusion $\mathbb{N} < \mathbb{M}$: les nombres réels sont plus nombreux que les nombres naturels et parmi les nombres réels les nombres transcendants sont les plus nombreux. Puisque l'élément b_ν est choisi aléatoirement dans le complément $\mathbb{M} - \mathbb{N}$, c'est un élément transcendant (comme π) en toute probabilité. À la fin de son texte de 1880, Cantor s'est senti libre de poursuivre sa quête de puissances infinies en acte de plus en plus loin $\mathbb{M}_0 < \mathbb{M}_1 < \cdots < \mathbb{M}_n$ et s'est mis à croire que leur succession constituait un ensemble bien ordonné, continuant ainsi la théorie des nombres finis par d'autres moyens...— voir Cantor [15], p. 280. Mais Cantor devait bientôt découvrir que la totalité de toutes les puissances (ou cardinaux) ne formait pas un ensemble consistant (cohérent), mais seulement une pluralité inconsistante.

La méthode diagonale a généré des paradoxes : l'antinomie ou le paradoxe de Richard, par exemple, est inspirée de ce procédé diagonal. Supposons que je veuille énumérer tous les énoncés en langue française qui désignent un nombre réel, *e.g.* le rapport entre la circonférence et le diamètre d'un cercle est π ; j'ordonne ces énoncés selon l'ordre lexicographique du dictionnaire. Appelons le $n^{\text{ième}}$ nombre réel de cette énumération le n-ième nombre de Richard

$$r_n = 0, a_{n1}a_{n2}\ldots a_{nn}\ldots$$

comme plus haut. Je définis maintenant un nombre réel par la diagonalisation : 'le nombre réel dont la n-ième décimale est 1, si la n-ième décimale du n-ième nombre de Richard n'est pas 1 et dont la n-ième décimale est 2, si la n-ième décimale du n-ième nombre de Richard est 1' ; cet énoncé définit un nombre de Richard, disons le r-ième, mais il diffère du nombre de Richard par la r-ième décimale. Nous avons donc $r_{nn} = 1$, si $a_{nn} \neq 1$ et $r_{nn} = 2$, si $a_{nn} = 1$; on a alors un nombre de Richard b_n qui diffère de tous les r_n. Il ne fait donc pas partie de l'énumération et pourtant il est défini en un

nombre fini de lettres dans l'ordre lexicographique. Gödel tirera de ce paradoxe la forme, sinon la matière, de son premier théorème d'incomplétude en extrayant de la diagonalisation un énoncé indécidable qui s'autoproclame indémontrable.

On peut encore évoquer le paradoxe de Skolem lié au théorème de Löwenheim-Skolem. Une théorie du premier ordre, par le théorème de Löwenheim-Skolem ascendant, peut avoir un modèle d'une cardinalité infinie arbitraire, c'est-à-dire non dénombrable (*e.g.* $2^{\aleph_0}$ pour la théorie axiomatique des ensembles sans supposer l'hypothèse du continu). Par exemple, le théorème de Cantor énonce que

$$\forall \alpha \left(\bar{\bar{\alpha}} \prec \bar{\bar{P}} \left(\bar{\bar{\alpha}} \right) \right)$$

pour tout ensemble, le cardinal de cet ensemble est plus petit que le cardinal de l'ensemble de ses sous-ensembles. Donc il n'y a pas de bijection entre l'ensemble des nombres naturels ω et $P(\omega)$ *dans* le modèle de la théorie du premier ordre. Comment peut-on y parler alors d'ensemble non dénombrable ? En fait, l'ensemble $P(\omega)$ est dénombrable *dans* le modèle — vu de l'extérieur — donc il y a une bijection entre ω et $P(\omega)$, mais cette bijection entre ω et $P(\omega)$ *n'est pas dans* le modèle vu de l'intérieur, autrement dit, ce n'est pas un objet du modèle. Cette situation paradoxale signifie simplement que la notion de cardinalité et les autres notions ensemblistes sont *relatives* — à un modèle — et qu'elles n'ont rien d'absolu d'un point de vue sémantique (*i.e.* du point de vue de la théorie des modèles). Remarquons que la théorie des ensembles Zermelo-Fraenkel exige une théorie du second ordre (voir [95]) pour pouvoir s'exprimer pleinement (en particulier, l'axiome de remplacement). La même remarque s'applique à la théorie des nombres ensembliste pour laquelle le postulat d'induction de Peano ne peut se formuler adéquatement qu'au second ordre où l'on quantifie sur les propriétés ou les sous-ensembles de l'ensemble $\mathbb{N}$.

En conclusion, peut-on considérer la théorie cantorienne des ordinaux transfinis comme une extension légitime du programme d'arithmétisation de l'analyse au même titre, par exemple, que l'analyse p-adique (analyse non archimédienne sur les nombres premiers) ? Ou encore doit-on admettre la théorie des nombres surréels (de Conway) comme une extension naturelle de la notion de coupure dédékindienne ? Il semble bien que les extensions et les complétions des corps de nombres n'aient pas le même statut mathématique du simple fait de leur rôle capital dans la pratique mathématique contemporaine. Une chose est sûre, un grand nombre de mathématiciens ont

renoncé au paradis cantorien et, parmi eux, ceux que l'on appelle communément les semi-intuitionnistes français, Borel et Poincaré en particulier. André Weil, l'un des grands praticiens de la théorie des nombres et de la géométrie algébrique au 20ième siècle, n'admettait pas la méthode diagonale comme méthode de preuve valide en théorie des nombres ; Weil privilégiait la méthode de descente infinie de Fermat qu'il caractérisait comme « méthode de descente finie dans les corps de nombres finis ». Pour l'arithméticien, le dénombrable est « dénombrable à l'infini » signifiant par là que la suite des nombres naturels est illimitée et ne doit pas être conçue comme une totalité infinie achevée à la manière d'un ensemble infini.

1.3 Frege, Russell et Peano

1.3.1 L'arithmétique de Frege

Le néo-logicisme a misé tellement sur le principe de Hume de l'égalité extensionnelle « *equality in extension* » pour faire revivre le logicisme de Frege que l'on en est venu à obnubiler son statut logique (voir Burgess [13]). À prime abord, le principe de Hume est un principe d'abstraction qu'on ne peut qualifier d'arithmétique dans son contexte frégéen, bien que Hume dans son *A Treatise of Human Nature* ne se soit intéressé qu'à l'égalité numérique qu'on peut exprimer

$$\forall R \forall S[(Num\,(R) = Num\,(S)) \leftrightarrow R = S]$$

pour R et S des relations numériques : le principe stipule que les relations numériques, en algèbre par exemple, sont égales si les nombres qu'elles relient sont égaux en arithmétique. Hume pensait que c'était seulement en arithmétique et en algèbre et non pas en géométrie qu'on pouvait atteindre l'exactitude parfaite « *perfect exactness* » de l'égalité (Hume [63], i, 3, 1). Le principe de Hume s'accorde parfaitement avec le procès de compter « *Zählen* » de Dedekind omniprésent dans le programme d'arithmétisation, alors que Frege traite de concepts et d'objets généraux indéterminés « *allgemeine unbestimmte Gegenstände* » dans sa loi fondamentale V des *Grundgesetze der Arithmetik* [30] (§36)

$$\forall F \forall G[Ext(F) = Ext(G) \leftrightarrow \forall x(Fx \equiv Gx)]$$

i.e. deux concepts ont la même extension, si et seulement si ils ont les mêmes « objets généraux ». La loi V donne naissance immédiatement au principe de compréhension illimitée

$$\exists x \forall y (y \in x \leftrightarrow P(y))$$

et au paradoxe de Russell lorsqu'on substitue y à x. En réalité, le néologicisme de C. Wright et G. Boolos ne réhabilite pas tant le logicisme de Frege qu'il essaie de l'adapter aux théories arithmétiques du second ordre, *e.g.* l'arithmétique de Peano, en recourant au principe de Hume. L'idée première de Frege pour une logique interne de l'arithmétique était pourtant de voir jusqu'où on pouvait aller en arithmétique par la seule déduction (logique) :

> *Wie weit man in der Arithmetik durch Schlüsse allein gelangen könnte* [20], p. X.

La consécution (conséquence) logique, comme dit Frege, doit imiter l'ordre séquentiel ou sériel de l'arithmétique avec l'addition comme paradigme assurant ainsi l'uniformité d'un procès totalement indépendant de l'intuition. C'était là aussi l'idée rectrice de son travail d'habilitation à Iéna en 1874 sur les méthodes de calcul « fondées sur l'extension du concept de quantité ». L'addition représente alors, comme chez Dedekind, l'opération première pour la fondation d'une « arithmétique conceptuelle », puisque l'arithmétique demeure l'archétype d'une théorie des concepts dans une sorte de reprise du projet leibnizien du « *calculus ratiocinator* » ; ce qui expliquerait sans doute l'intention ou la motivation de Frege dans ses travaux ultérieurs sur les notions de concept, d'objet et de fonction ou encore de sens et de référence ; la philosophie des concepts ou la philosophie du langage qui en résulte se situerait à l'intérieur d'un programme de philosophie générale fondé sur le modèle arithmétique. Cette interprétation de Frege n'est certainement pas orthodoxe, puisqu'elle évacue l'essence du logicisme comme fondation logique de l'arithmétique (et des mathématiques). Mais qu'est-ce que la logique, si ce n'est la formalisation de l'arithmétique, comme Frege nous l'enseigne ? Si Frege se réfugie dans la géométrie après sa tentative de conceptualisation d'une arithmétique formelle libérée de l'intuition et de l'empirisme, c'est qu'il croit que la géométrie est la source de la connaissance mathématique « expérimentale » et que le continuum spatio-temporel est à l'origine (comme chez Kant !) de l'idée d'infini ; il reconnaît en plus que sa notion de nombre comme extension d'un concept est un échec. On serait tenté de croire que les concepts chez Frege jouent le rôle des indéterminées de Kronecker, alors

que les nombres prennent la place des coefficients entiers dans une fonction polynomiale, la différence étant ici bien sûr que les indéterminées ne sont que des variables muettes et ne peuvent prétendre à l'existence conceptuelle ou idéale que Frege confère à ses objets généraux indéterminés ; seuls les nombres comme symboles ou numéraux subsistent sur la terre plate de l'arithmétique !

Le destin de la logique dans le projet de Frege est certainement lié à la formalisation du concept de fonction. Fonction et argument sont dérivés de la notion de fonction polynomiale et Frege est explicite là-dessus dans sa préface de la *Begriffsschrift* : sa formalisation ou « langage de formules pour la pensée pure » est modelé sur l'idée d'un langage formel pour l'arithmétique. En résumé, Frege a d'abord formé le projet d'arithmétiser la logique ordinaire (aristotélicienne), un projet qui s'est transformé en cours de route en une logicisation de l'arithmétique qui pouvait couvrir l'arithmétique jusqu'à la théorie des fonctions, i.e. sommation et intégration. Cet idéal arithmétique est exposé dans la *Begriffsschrift* où le langage formalisé a pour seule fin la traduction du langage informel de l'arithmétique ordinaire. Il n'y a pas de signe de logicisation ici, pas plus que dans les *Grundlagen der Arithmetik* de 1884 où Frege se satisfait d'une recherche logico-mathématique sur le concept de nombre. Tout cela est compatible avec le programme d'arithmétisation et avec la façon de parler non logiciste que l'on trouve chez Dedekind et Cantor.

Il semble donc que le programme logiciste d'une conceptualisation logique de l'arithmétique est d'abord et avant tout d'inspiration philosophique et ne doit pas être considéré comme une voie alternative pour les fondements arithmétiques des mathématiques au moins jusqu'aux *Grundgesetze* où le véritable programme philosophique de Frege prend forme. On pourrait toutefois penser que le propos anti-kantien ou non aprioriste de Frege n'est pas tant un impératif logiciste qu'un motif philosophique apparenté au *calculus philosophicus* ou *ratiocinator* de Leibniz. Mais l'idéal d'un formalisme notationnel ou idéographie est une extension pure et simple de l'arithmétique pour la représentation des jugements logiques classiques, comme le montrent à souhait les deux premiers chapitres de la *Begriffsschrift*, alors que la troisième partie traite d'une présentation notationnelle des suites arithmétiques qu'on pourrait étendre au calcul différentiel et même à l'*analysis situs* (topologie) et à la physique. Le rêve philosophique de Frege est alimenté par un esprit arithmétique ; il est dommage que Frege n'ait pas tenu compte d'une autre extension de l'arithmétique, l'arithmétique générale ou polynomiale de Kronecker qui est un développement purement mathématique, parce qu'on peut conclure que la logique formelle de Frege n'est rien d'autre qu'une arith-

métique générale détournée au profit d'un conceptualisme philosophique. Le fait que la formalisation de Frege (sans son système notationnel) a rendu possible la théorie russellienne des descriptions définies est un signe de sa fécondité philosophique et non de sa pertinence mathématique. Mon interprétation du logicisme ne cherche qu'à montrer que le prétendu programme logiciste de Frege est né de l'arithmétique et n'était pas destiné à fournir des fondements pour l'arithmétique et l'ensemble des mathématiques, mais plutôt à continuer l'arithmétique par d'autre moyens, comme chez Cantor...

La logique formelle est apparue avec Aristote, elle a été partiellement arithmétisée par Frege, mais le programme fort de l'arithmétisation de la logique commence avec Hilbert et son école. La logique philosophique est née avec Frege, la logique mathématique naît avec Hilbert. Entre les deux il y a Russell dont la théorie des types est une créature hybride qui a achevé et défait en même temps le programme logiciste tel qu'on le conçoit traditionnellement. Après le rejet de la tentative frégéenne d'une théorie arithmétique des concepts, l'entreprise de Russell aussi bien que les axiomatisations de Hilbert et Zermelo pourraient être perçues comme des « polynomialisations » de la logique. Après le précepte de Quine selon lequel la logique du second ordre n'est plus de la logique, mais de l'arithmétique, l'idée que la logique du second ordre avec le principe équinumérique de Hume est équivalente à l'arithmétique de Peano ne doit guère impressionner le logicien mathématicien qui ne voit pas l'astuce philosophique ; c'est pour cette raison que mon « arithmétisation » du logicisme de Frege ne devrait pas l'étonner, pas davantage que ma caractérisation du logicisme de Russell comme un calcul polynomial des degrés (ordres) de fonctions propositionnelles qui ressemblent à s'y méprendre à des fonctions polynomiales. En prime, le problème qu'a rencontré Russell dans sa théorie des types (simples ou ramifiés) aurait pu être résolu en revenant à une théorie des polynômes de degré fini comme support fini de séries de puissances infinies. Que Russell ait une vague idée de cette solution, c'est ce que je veux maintenant discuter.

1.3.2 Le logicisme de Russell

Le motif recteur pour l'invention russellienne des différentes théories des classes, la théorie zigzag, la théorie de la limitation de la taille et la théorie sans classes est assurément sa formulation du paradoxe de l'axiome V de compréhension illimitée dans les *Grundgesetze* de Frege. L'invention elle-même était plus en accord avec une simple solution arithmétique du paradoxe : il n'est pas difficile de voir que la hiérarchie des types simples avec le premier type 0 assigné aux objets ou aux individus, le second aux prédicats, le troisième aux prédicats de prédicats et ainsi de suite est définie sur une échelle arithmétique sur les nombres naturels — la théorie des types transfinis est une extension que Russell n'a pas voulu considérer, elle est l'oeuvre de ses successeurs. À ce titre, la théorie des types s'apparente à l'axiomatisation de l'arithmétique chez Peano et la mise en garde :

> Tout ce qui contient une variable apparente (liée) ne doit pas être une valeur possible de cette variable. (Russell [90], p. 163.)

n'est là que pour prémunir contre le principe du cercle vicieux générateur de contradictions. La théorie des types ramifiés est une théorie des types pour les fonctions propositionnelles dont les types dépendent des types de leurs arguments, mais aussi des types de variables liées qu'elles contiennent et qui peuvent être d'un type supérieur au type de l'argument de la fonction. Cette situation contraint à introduire la notion d'ordre et l'axiome de réductibilité qui en découle stipule que toute fonction d'ordre arbitraire n est coextensive à une fonction prédicative d'ordre $n-1$, c'est-à-dire à l'ordre égal au type de ses variables liées. Par exemple, $\forall\varphi(\psi(\varphi, y))$ où φ est une fonction du premier ordre sera une fonction du second ordre ou encore une fonctionnelle. Mais l'axiome est finalement apparu artificiel et Russell y a finalement renoncé. Si Russell avait conçu clairement les fonctions propositionnelles comme des fonctions polynomiales, il n'aurait pas eu besoin d'introduire la notion d'ordre et les types ramifiés, la notion de degré suffisant à rendre la notion de type simple : le degré (ou l'ordre) d'un polynôme est le maximum des degrés de tous les termes dans le polynôme. La même remarque s'applique à la théorie prédicative de Weyl, mais Weyl était bien conscient de l'analogie de la hiérarchie des niveaux « *Stufe* » de prédicativité avec les polynômes de degré fini. Dans son ouvrage *Das Kontinuum* [109], Weyl restreint les objets dans son « *engeres Verfahren* » aux nombres naturels et rationnels, ce sont les catégories fondamentales d'individus avec leurs propriétés (relations) et rejette les ensembles transfinis qui restent sous le coup d'une interdiction

intuitionniste. De toute façon, la théorie ramifiée était destinée à contrer les paradoxes — Russell les appelait faussetés réflexives « *reflexive falsities* » étrangères aux mathématiques — et Ramsey lui a sagement conseillé de laisser tomber la théorie ramifiée au profit de la théorie des types simples. Mais Russell devait ajouter un axiome de l'infini ; dans la théorie russellienne $\aleph_0$ doit exister comme classe des cardinaux finis, c'est-à-dire dans les mots de Russell, comme la classe de toutes les classes de classes d'individus et $2^{\aleph_0}$ existe comme le cardinal d'une classe de toutes les classes de classes de classes de classes d'individus ! L'entreprise des *Principia Mathematica* (avec A.N. Whitehead) était fondée sur la théorie des types finis et l'extension (peu utile) aux types infinis a été laissée à d'autres. Ce qui reste plutôt des efforts de Russell se trouve dans son travail logique e.g. la théorie des descriptions définies qui donne pour « l'actuel roi de France est chauve » la formulation

$$\exists x[((\varphi x) \wedge \forall y(\varphi y \rightarrow x = y)) \wedge \psi x]$$

— Russell employait ιx comme descripteur défini. Pour la logique, Russell défend toujours la thèse attribuée à Frege voulant que les mathématiques soient fondées sur la logique, comme prétendent le démontrer les *Principia Mathematica*. Mais la démonstration est dans la plupart des cas superflue. Si la logique des classes est ensembliste, la théorie des types peut être retraduite en arithmétique polynomiale. Comme pour Frege, le langage formel de la logique ne tient qu'aux connecteurs propositionnels et aux quantificateurs du premier ordre ; c'est le tout de la logique si l'on s'en tient au dogme de Quine. Lindström caractérise la logique classique du premier ordre comme un langage possédant les propriétés de compacité et de Löwenheim-Skolem : la logique classique du premier ordre consiste dans l'emploi des quantificateurs $\exists x$ (introduit par Russell) pour « *there exists* » et $\forall x$ (introduit par Gentzen) pour « *Alle* » qui signifie « tous », la logique d'ordre zéro se limitant aux seuls connecteurs $\wedge$, $\vee$, $\neg$, $\rightarrow$, $\leftrightarrow$. Le contenu propositionnel dans les deux cas est d'abord le langage ordinaire et ensuite les langages spécialisés, e.g. les mathématiques élémentaires. La logique formelle distingue les énoncés (expressions closes) des formules (expressions ouvertes) avec des constantes et des variables, liées dans le cas des énoncés, libres dans le cas des formules. Les formules bien formées, les fbfs, sont générées par des règles de formation d'un vocabulaire et les règles de transformation — dans l'idiome de Carnap — ou règles d'inférence permettent de passer des axiomes aux théorèmes, e.g. *modus ponens*.

1.3.3 Le Formulaire de Peano

Le *Formulaire* de Peano, qui a influencé si profondément Russell, semble délesté de contenu logique malgré l'emploi de la notion d'indéterminée pour les signes de variables. L'arithmétique de Peano est toujours le système fondamental de l'arithmétique pour les besoins de la logique et son postulat d'induction se lit comme suit :

> Si un ensemble S de nombres naturels contient 1 et si, contenant un nombre arbitraire a, il contient aussi son successeur, alors S contient tous les nombres naturels. ([88], p. 34.)

C'est là une formulation au second ordre et elle correspond à l'axiome de l'infini dans la théorie axiomatique des ensembles de Zermelo-Fraenkel

$$\exists x\{\emptyset \in x \wedge \forall y(y \in x \rightarrow y \cup \{y\} \in x\}$$

pour $\{y\}$ le singleton ou ensemble à un seul élément. Cette formulation relie l'arithmétique de Peano à la théorie des ensembles et à la notion ensembliste de système chez Dedekind, d'où l'appellation d'arithmétique ensembliste. L'axiomatisation de Zermelo de la théorie des ensembles avait aussi pour but d'éliminer la conséquence paradoxale, l'axiome de compréhension illimitée, de la loi V des *Grundgesetze* de Frege ; l'axiome de compréhension limitée aussi appelé axiome de séparation « *Aussonderungsaxiom* » par Zermelo

$$\forall x \exists y \forall z(z \in y \leftrightarrow z \in x \wedge A(z))$$

sépare un sous-ensemble z d'un ensemble x avec une propriété définie d'un ensemble donné y. Zermelo ne manque pas d'attaquer le *Formulaire* de Peano en l'accusant de vouloir réduire les mathématiques à la syllogistique d'Aristote et de la scholastique médiévale (Zermelo [112]). Il revient à Zermelo d'avoir renoué avec l'esprit arithmétique de l'entreprise cantorienne quand ce ne serait, comme il dit, que pour introduire certaines restrictions (Zermelo [111]) à la théorie des ensembles finis qu'il identifie à l'arithmétique élémentaire ; mais Zermelo ne pensait pas se limiter aux ensembles finis et il croyait que le principe du bon ordre pour les ensembles finis pouvait s'étendre dans le transfini (Zermelo [113]). Sa théorie axiomatique des ensembles allait cependant être retravaillée par d'autres, Skolem, Fraenkel et von Neumann surtout. C'est von Neumann qui a formulé l'axiome de fondation ou régularité ([104])

$$\forall x(x \neq \emptyset \rightarrow \exists y(y \in x \wedge y \cap x = 0)$$

ou au second ordre

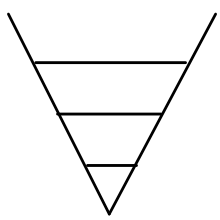
$$\forall X \forall x [X(x) \rightarrow \exists y \forall z \{X(y) \wedge [X(z) \rightarrow z \in y]\}].$$

Von Neumann cite Mirimanoff [83] qui a défini les « ensembles ordinaires » comme les ensembles qui génèrent des descentes finies seulement — il n'y a pas de suite infinie descendante d'éléments $e_1 \ni e_2 \ni e_3 \dots$ puisqu'elle doit s'arrêter à un élément indécomposable $\emptyset$ que Mirimanoff appelle « noyau ». De plus, Mirimanoff avait déjà les trois opérations (ou postulats) pour la structure cumulative des rangs, l'union, l'ensemble des parties et le postulat de remplacement ou substitution qu'il explique de la façon suivante :

> Si un ensemble $(a, b, c, \dots)$ existe, alors existe tout ensemble équivalent (E,F,G) où *E, F, G* sont des ensembles ordinaires (distincts) existant. [83]

Mirimanoff était un praticien de la méthode de la descente infinie de Fermat en théorie des nombres, comme l'était Skolem qui a traité des suites ϵ descendantes dans son texte de 1922 « *Remarques sur le fondement axiomatique de la théorie des ensembles* » ; les suites ϵ devaient aussi s'arrêter dans le fini. Dans ce même texte, Skolem insiste sur le fait que les notions ensemblistes sont relatives, ce qui devait inciter Gödel à définir des formules absolues dans un modèle intérieur minimal de la théorie des ensembles Z-F pour sa preuve de la consistance relative de l'hypothèse du continu.

La structure cumulative des rangs pour la théorie des ensembles est le résultat des efforts conjugués de Zermelo, Mirimanoff, Skolem et von Neumann. La structure cumulative des rangs a la forme suivante pour les ordinaux



$$V_\omega = \bigcup_{\beta \prec \omega} V_\beta$$
$$V_{\alpha+1} = V_\alpha \cup P(V_\alpha)$$
$$V_\alpha$$
$$V_0 = \emptyset$$

La structure a un premier rang qui correspond à l'ensemble nul ; on monte dans la hiérarchie par l'opération d'union et celle d'ensemble des parties. Chaque rang définit un ordinal et l'on peut dire que le rang ordinal détermine la taille cardinale d'un ensemble, puisque plus l'ordinal d'un ensemble est élevé, plus la place qu'il occupe dans l'univers V des ensembles est grande.

La clôture ou l'accumulation « *Haüfung* » s'opère dans le transfini, comme aurait dit Cantor, pour les opérations d'addition et d'ensemble des parties est constituée par les cardinaux inaccessibles et les cardinaux supérieurs (mesurables, compacts, supercompacts, etc.). Cette structure repose sur l'axiome de fondation. Un principe de réflexion équivalent à l'axiome de remplacement

$$Fonc(F) \rightarrow F''x \in V$$

et à l'axiome de l'infini donne une image grandeur nature d'un univers ensembliste V qui se reflète dans les niveaux transfinis de la hiérarchie ordinale. Est-ce que l'extension transfinie du monde arithmétique, sa complétion transarithmétique dans les ensembles infinis a une signification absolue ou est-ce simplement une réplique transfinie de l'arithmétique finie, comme Skolem l'a pensé ? Un mathématicien constructiviste dans la foulée de Kronecker ne peut que refuser l'existence ou la validité absolue de l'univers ensembliste plein, mais peut vouloir extraire le minerai arithmétique de cette gangue ensembliste, comme Cauchy, Weierstrass, Dedekind et Hilbert pensaient le faire avec l'analyse classique où la notion de limite était mise à l'épreuve par des méthodes arithmétiques, e.g. la théorie de l'approximation, quand elle n'était pas simplement évacuée. Ce qui s'est produit avec Cantor est une situation inverse : le concept de limite a été mis « en acte » et « ordinalisé », ce qui signifie que les ordinaux limites n'étaient pas l'objet d'une approximation, mais existaient *de facto* et *de jure* par la sanction d'un décret transcendant — Kronecker aurait ajouté que l'existence de ces entités était affaire de philosophie ou de théologie et non pas de mathématiques, ce que confirme d'ailleurs Cantor dans sa recherche de justification du transfini chez les philosophes modernes et les théologiens médiévaux.

Une attitude plus tolérante serait d'accommoder l'arithmétique transfinie comme une extension transarithmétique de l'arithmétique pour le bénéfice d'une clientèle ensembliste. Ce qui s'est produit après Cantor, c'est que sa création libre a attiré plus de clients que ne l'avait souhaité le rigoriste Kronecker. Il n'est pas question de faire plier l'échine ou de briser le cou de l'imagination mathématique, mais l'héritage de Kronecker dans les mathématiques pures, théorie des nombres et géométrie algébrique ou arithmétique, apparaît plus fécond que l'influence cantorienne, qui s'est fait sentir rapidement dans les mathématiques élémentaires, dans le langage mathématique et logique et dans les questions fondationnelles. C'est dans l'algèbre cependant comme extension propre ou naturelle de l'arithmétique que devait s'engager le développement de l'arithmétique générale au sens de Kronecker.

Chapitre 2

L'arithmétisation de l'algèbre

Il pourrait sembler paradoxal que Kronecker ait intitulé son programme « arithmétisation de l'algèbre » puisque l'algèbre est un autre nom pour l'arithmétique générale « *allgemeine Arithmetik* ». Hankel avait défini un principe général dans son texte de 1867 *Prinzip der Permanenz der formalen Gesetzen* (Principe de permanence des lois formelles) qui pouvait permettre d'étendre les lois de l'arithmétique ordinaire aux différents systèmes de nombres (e.g. les nombres complexes). Auparavant, l'Anglais Peacock avait parlé d'un principe de permanence des formes équivalentes « *principle of permanence of equivalent forms* ». L'ambition de Kronecker va plus loin. Dans une lettre à Lipschitz, il écrit :

> À cette occasion [la publication de son texte de 1882], j'ai découvert les fondements longtemps recherchés de toute ma théorie des formes qui complète d'une certaine façon l'arithmétisation de l'algèbre qui a été le but de ma vie mathématique ; il est parfaitement clair à mes yeux qu'en même temps l'arithmétique ne peut se passer de l'association des formes et que sans elle l'arithmétique ne peut que dériver dans des pensées tortueuses « *Gedankenspinste* » comme on le voit chez Dedekind où la vraie nature des choses est obscurcie plutôt qu'éclairée. ([78], pp. 181-182.)

Le texte de 1882 [74] en question est bien sûr la publication majeure de Kronecker *Grundzüge einer arithmetischen Theorie algebraischen Grössen* (Traits fondamentaux d'une théorie arithmétique des grandeurs algébriques) dans lequel il formule les fondements de sa théorie des formes ou polynômes homogènes.

Au-delà de la polémique entre Kronecker et Dedekind, leurs vues divergent sur l'arithmétique générale : Kronecker pensait que l'approche de Dedekind, la théorie des idéaux, était trop formelle et Dedekind croyait que la théorie des formes de Kronecker était trop générale, comme ses « Remarques mélangées » (*Bunte Bemerkungen*) sur le texte de 1882 de Kronecker le laissent penser (voir Edwards *et alii* [26]). Il n'y a pas de doute que Dedekind ait parfois raison de déplorer le style souvent obscur de Kronecker, mais pour un grand nombre de théoriciens des nombres et d'algébristes, de Hermann Weyl à André Weil, la supériorité de la méthode de Kronecker peut être résumée comme suit dans les mots de H. Edwards :

> Il est coutume en géométrie algébrique de considérer le corps des fonctions sur un corps algébriquement clos — le corps des nombres complexes ou le corps des nombres algébriques — plutôt que sur $\mathbb{Q}$ (le corps des rationnels). Dans l'approche kroneckerienne, on évite la construction transfinie des corps algébriquement clos par la manoeuvre de l'adjonction de nouveaux nombres algébriques à mesure qu'on les produit. ([23], p. 97.)

Ici adjoindre de nouveaux nombres algébriques signifie une extension numérique pas à pas, alors que le corps algébriquement clos est donné d'un seul coup par la quantification universelle (transfinie) sur l'ensemble des nombres naturels. Il importe de noter que le corps des fonctions algébriques à une variable dans $\mathbb{Q}$ est une extension de $\mathbb{Q}[x]$, l'anneau des polynômes à une indéterminée x avec coefficients dans le corps $\mathbb{Q}$ des nombres rationnels ; c'est une situation analogue à la relation qu'entretient le corps des nombres algébriques avec l'anneau $\mathbb{Z}$ des entiers. En ce qui touche le cadre algébrique de la théorie des formes de Kronecker, c'est ce caractère général — détaché du corps ambiant, comme on dit — qui assure sa pertinence fondationnelle. On sait par ailleurs que Kronecker était réfractaire au vocabulaire dédékindien des corps « *Körper* » qu'il trouvait trop matérialiste !

Le programme d'arithmétisation de Kronecker vise l'élaboration complète de la théorie des fonctions rationnelles et algébriques entières avec leurs systèmes modulaires (systèmes de diviseurs). Dans cette théorie complète, l'association des formes permet la conservation des lois de factorisation de telle sorte que le passage des domaines naturels aux domaines rationnels — domaines de rationalité « *Rationalitätsbereiche* » est le terme que Kronecker préfère à corps — est parfaitement uniforme. Le dessein de Kronecker est de formuler une théorie arithmétique des grandeurs algébriques et le passage

cette fois des grandeurs rationnelles aux grandeurs algébriques doit conserver les mêmes déterminations conceptuelles « *Begriffsbestimmungen* » et les opérations arithmétiques doivent garder leur sens dans les domaines d'extension. Le principe d'association ou d'adjonction permet d'annexer les indéterminées, à la condition qu'elles ne modifient pas la structure du domaine d'origine : c'est ce que nous appellerions aujourd'hui une extension conservatrice et que Kronecker désigne sous le nom d'extension de domaine de l'arithmétique « *Gebietserweiterung der Arithmetik* ». Kronecker avouera que :

> La conservation de ces déterminations conceptuelles dans le passage du cas rationnel au cas algébrique a été l'incitation qui a servi de principe recteur dans le traitement des grandeurs algébriques. ([74], p. 327.)

L'objet principal dans ces extensions est la notion d'indéterminée « *Unbestimmte* » que Kronecker emprunte à Gauss : ce sont les « *indeterminatae* » ou variables indépendantes des équations diophantiennes (équations indéterminées avec coefficients entiers)qui apparaissent dans les polynömes de la forme

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

où les a_i sont des coefficients entiers et les x_i sont des indéterminées — ils sont homogènes quand les coefficients ont le même degré comme dans

$$f(y, z) = a_0 + a_1y^{n-1}z + a_2y^{n-2}z^2 + \ldots + a_nz^n.$$

Un polynôme peut être décomposé en facteurs linéaires par le groupe de permutations de ses coefficients. Les fonctions polynomiales sont injectives dans les nombres naturels et deux polynômes (ou formes) homogènes F et F' sont équivalents s'ils ont les mêmes coefficients (i.e. le même contenu). On peut opérer des substitutions linéaires sur ces polynômes pourvu qu'on substitue aux indéterminées des coefficients entiers, i.e. des entiers — les indeterminées sont souvent appelées entiers indéterminés. Le rôle universel joué par les indéterminées procure à la théorie polynomiale la plus grande généralité et l'investit en même temps de moyens suffisants pour représenter le contenu de l'arithmétique. On peut donc affirmer que l'idée de contenu polynomial est l'outil principal de la théorie kroneckerienne et c'est cette idée que je veux exploiter rapidement dans ce qui suit.

2.1 Le contenu polynomial

Les polynômes de la forme

$$f = f_0 + f_1 x + f_1 x^2 + \ldots + f_n x^n$$

où les f_i sont les coefficients avec l'indéterminée x constituent le sous-anneau $K[x]$ de l'anneau des séries $K[[x]]$ de puissances formelles. Le degré d'un polynôme est le degré du dernier coefficient non nul ($k = n$), alors que le coefficient principal d'un polynôme f de degré k est la constante f_k et f est appelé monique si son coefficient principal est 1. Les polynômes sont donc des séries de puissances qui n'ont qu'un nombre fini de coefficients non nuls. Le produit de Cauchy ou d'involution de deux polynômes joue un rôle important ici ; nous l'écrivons

$$f \cdot g = (\sum\nolimits_m f_m x^m)(\sum\nolimits_n g_n x^n) = \sum\nolimits_m \sum\nolimits_n f_m g_n x^{m+n}.$$

La somme $f + g$ des polynômes f et g est obtenue en additionnant simplement les coefficients correspondants. Nous nous intéressons aux polynômes irréductibles, c'est-à-dire qui ne peuvent être le produit de deux polynômes de degré > 0 et premiers dans $K[x]$. Tout polynôme linéaire est irréductible. $K[x]$ a la propriété de factorisation et ce fait est crucial pour la notion kroneckerienne de contenu des formes. Une forme M est un terme dans une autre forme M' quand les coefficients de la première sont "convolutés" (combinés dans un produit de Cauchy) dans les coefficients du second. Cette idée d'un contenu « *Enthalten-Sein* » des formes se résume dans l'énoncé « le contenu du produit est le produit des contenus (de chaque forme) » qu'on peut extraire du texte des *Grundzüge* de Kronecker. Ainsi, pour qu'une forme soit contenue ou incluse dans une autre forme il suffit qu'elle soit combinée avec elle linéairement (avoir ses puissances convolutées avec les puissances de la seconde forme).

On peut adopter alors le principe général de la substitution-élimination par Kronecker. Nous énonçons le principe de substitution de la façon suivante :

> 1) Deux formes homogènes (polynômes) M et M' sont équivalentes si elles ont les mêmes coefficients.
>
> 2) Des formes peuvent se substituer aux indéterminées (variables) pourvu que la substitution (linéaire) se fasse avec des coefficients entiers.

Nous avons comme conséquence immédiate la proposition 1 (proposition X chez Kronecker) :

> Les formes linéaires homogènes qui sont équivalentes peuvent se transformer l'une dans l'autre par la substitution des coefficients entiers.

Nous avons aussi la proposition 2 (proposition X^0 chez Kronecker) :

> Deux formes M et M' sont équivalentes, si elles peuvent se transformer l'une dans l'autre.

Ces propositions sont en réalité des lemmes pour le théorème de la factorisation unique des formes que Kronecker considérait comme l'un de ses résultats les plus importants (proposition $XIII^0$ chez Kronecker)

> Toute forme algébrique entière est représentable comme produit de formes irréductibles (formes premières) de façon unique.

C'est là l'équivalent du théorème fondamental de l'arithmétique sur la factorisation unique des entiers par un produit de facteurs premiers.

La procédure de substitution est simultanément une procédure d'élimination, puisque les indéterminées sont remplacées par des coefficients entiers. Ainsi, une réserve indéfinie (ou effinie) de variables est mise à la disposition d'un système formel et réduite ensuite par la méthode de substitution-élimination à une suite descendante finie de nombres naturels par un algorithme d'Euclide sur les facteurs ou diviseurs des formes polynomiales — il s'agit d'un algorithme d'Euclide généralisé qui correspond en fait à la descente infinie de Fermat.

La théorie générale du contenu des polynômes avec sa procédure d'adjonction a soulevé quelques critiques de la part de Dedekind, comme je l'ai rappelé plus haut, mais du point de vue de la théorie des systèmes modulaires (diviseurs), la théorie kroneckerienne du contenu où « le contenu d'un produit = le produit du contenu » se retrouve dans la version moderne de Bourbaki (voir Edwards [23], part 0)

> Le contenu de fg (polynômes) est le contenu de f par le contenu de g.

Cette notion de contenu fait partie intégrante d'une théorie algorithmique de la divisibilité pour les entiers (ordinaires ou algébriques) qui est toujours actuelle. Kronecker aura donc trouvé le fondement le plus simple de sa théorie des formes qui était à ses yeux le but de son entreprise mathématique. À la

fin, l'arithmétique générale kroneckerienne est une théorie arithmétique des grandeurs algébriques qui est réductible à une théorie des fonctions entières de plusieurs variables avec coefficients entiers et indéterminées. La partie divisibilité a à voir avec la composition « *Aufbau* » ou association des formes et leur décomposition « *Zerlegung* » euclidienne ou fermatienne est la procédure de preuve principale. Nonobstant la distinction des niveaux pour les formes diverses ou leurs diviseurs, le résultat final que Kronecker réclame pour son programme d'une arithmétisation de l'algèbre est la mise au jour de fondements arithmétiques dont la vérité interne est démontrable par les moyens mêmes de la théorie « *innere Wahrheit und Folgerichtigkeit* » — voir Kronecker [74], p. 387.

Si cette prétention est justifiée, ce sont les successeurs de Kronecker qui devront la défendre. Hilbert a voulu donner une version logique (métamathématique) du problème de l'autoconsistance de l'arithmétique, mais les continuateurs de Kronecker en théorie algébrique des nombres et en géométrie algébrique n'auront de cesse de poursuivre le programme de Kronecker sans parler des logiciens, mathématiciens et philosophes qui se feront les défenseurs de l'arithmétisme kroneckerien.

2.2 La postérité du programme de Kronecker

Le programme de l'arithmétique générale a plusieurs ramifications, en particulier dans la théorie des systèmes modulaires où Kronecker remonte souvent à Gauss et à Galois comme sources de ses idées combinatoires — dans une autre tradition, la filière dédékindienne, les systèmes modulaires s'appellent idéaux de polynômes. Ce sont les concepts de congruence chez Gauss et de groupe de permutations dans la théorie des équations polynomiales chez Galois qui sont à l'origine de la théorie générale des systèmes modulaires — voir les textes de Kronecker « *Über einige Anwendungen der Modulsysteme auf elementare algebraische Fragen* » et « *Ein Fundamentalsatz der allgemeinen Arithmetik* », *Werke* II et III [73].

Les résultats obtenus par Kronecker confortent l'idée d'arithmétique générale comme théorie algorithmique de la divisibilité. C'est là un des legs principaux que Kronecker a laissés à sa postérité mathématique, Hensel, Hurwitz, Molk, König, Skolem, Vandiver, Weyl et Edwards en particulier (voir Edwards [22] et [24]). Hurwitz [64], par exemple, montre comment l'algorithme euclidien opère dans la théorie kroneckerienne des systèmes mo-

dulaires alors que l'analyse de Molk [84] propose un long résumé de la théorie des diviseurs de Kronecker. Un exemple intéressant se trouve dans le travail de Vandiver [103] sur « Constructive derivation of the decomposition-field of a polynomial ». S'appuyant sur les analyses de van der Waerden, Vandiver reconstruit le corps de décomposition par un algorithme fini pour l'extraction des facteurs irréductibles sans supposer l'existence *a priori* du corps de décomposition (ou du domaine de rationalité) d'un polynôme donné. Vandiver se réclame du programme de Kronecker quand il dit que la méthode des systèmes modulaires avec indéterminées est essentielle dans les fondements de l'algèbre commutative. Vandiver utilise une induction, en réalité la méthode de la descente infinie, pour un polynôme $\varphi(\beta, z)$ pour obtenir la décomposition du corps $F(\beta)$. Edwards, un autre adhérent du programme de Kronecker, suit la même voie avec l'accent sur les « anneaux naturels » d'entiers où il y a une méthode de descente infinie pour la factorisation des polynômes. Edwards ([23], p. 21) montre comment produire les polynômes irréductibles en supposant que si un polynôme h — une forme algébrique entière « *eine ganze algebraische Form* », dans les termes de Kronecker — n'est pas irréductible, il doit y avoir des polynômes de degré inférieur *ad infinitum* avec les mêmes propriétés que h, ce qui est impossible, et donc par *reductio ad absurdum* on arrive « en un nombre fini d'étapes » à un polynôme irréductible

$$h(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n$$

dans lequel l'ordre décroissant des puissances exhibe la descente finie à partir d'un entier n fini arbitraire, le degré du polynôme. Je pense cependant que l'exposé d'Edwards n'est pas totalement fidèle à l'esprit du programme de Kronecker quand il critique Weyl pour avoir mis l'accent dans son ouvrage *Algebraic Theory of Numbers* [110] sur la factorisation unique qui était aussi l'objectif principal de la théorie des idéaux de Dedekind. L'argument d'Edwards repose sur le fait que la factorisation dépend du corps ambiant ou local, mais il faudrait ajouter que l'un des résultats principaux de Kronecker, comme il le proclame, est la factorisation des formes dans le plus grand corps ambiant ou dans le domaine de rationalité maximal. C'est le caractère général ou universel de l'arithmétique générale englobant la théorie des formes, leur composition en termes d'association des formes et leur décomposition en termes de la divisibilité algébrique qui fait de la factorisation unique dans le corps des nombres algébriques, un point fort de l'entreprise de Kronecker.

Edwards traite aussi du théorème de Prague de Dedekind qui généralise le lemme de Gauss aux entiers algébriques ; la discussion porte sur le résultat de Dedekind en relation avec les travaux antérieurs de Kronecker ([73], II, pp. 419-424). Le lemme de Gauss dans l'une de ses versions stipule que deux polynômes primitifs — polynômes avec coefficients dans les entiers et pour lesquels le plus grand diviseur commun est l'unité — ont un produit qui est aussi primitif. Kronecker utilise ici le produit de Cauchy ou produit de convolution pour les polynômes que nous avons vu plus haut

$$\sum_h M_h U_h \cdot \sum_i M_{m+i} U^{i-1} = \sum_k M'_k U^k$$

où les M sont des formes entières et les U des indéterminées ; le produit

$$\prod_h \sum_k M'_k U_{hk}$$

est « contenu » dans la forme primitive qui résulte de la convolution et s'exprime

$$\sum_k M'_k U^k = (M_k M_{m+1})^k + (M_k M_{m+1})^{k-1} + (M_k M_{m+1})^{k-2}$$

$$+ \ldots + (M_k M_{m+1})$$

dans l'ordre décroissant des puissances du polynôme de degré k. Cette combinaison linéaire du produit de convolution et la descente finie sur des puissances indiquent simplement que les formes algébriques entières génèrent d'autres formes algébriques entières, i.e. des entiers algébriques. Ce qu'Edwards trouve difficile dans le style tortueux de Kronecker, c'est tout simplement une généralisation de la théorie kroneckerienne de 1882 qui comprend à la fois la théorie des systèmes modulaires et la théorie polynomiale. Le principe d'équivalence des formes dans le texte 1882 est appliqué ici à la théorie des diviseurs ; la notion de contenu « *Enthaltensein* » est modifié de la façon suivante : F est une forme avec indéterminées U_{hi} qui contient le produit des formes où le produit les f_i sont des fonctions entières des indéterminées U_{hi}

$$\prod\nolimits_h (f_0 U_{h0} + f_1 U_{h2} + \ldots + f_n U_{hn}).$$

Kronecker parle explicitement du contenu des polynômes primitifs dans son texte, ce qui le relie directement au lemme de Gauss dans sa version moderne :

Le produit de deux polynômes primitifs est un polynôme primitif.

En fait, Hurwitz [64] publie une preuve qui a recours au théorème d'interpolation de Lagrange plutôt qu'au produit de Cauchy : Hurwitz parle alors de l'élimination des puissances composées. Le célèbre théorème de Prague de Dedekind qui utilise aussi une forme de descente est une conséquence du théorème plus général de Kronecker sur le produit des formes, résultat dont apparemment Dedekind n'avait pas pris connaissance. Pour Kronecker, l'arène naturelle (avec la plus grande aire) de son arithmétique générale, c'est l'anneau des polynômes et le théorème de Prague de Dedekind peut être mis au compte de Kronecker, petit paradoxe qui montre en réalité que Dedekind n'était pas si éloigné de Kronecker, pas autant en tout cas que Kronecker l'eût souhaité, semble-t-il. Hermann Weyl est l'un de ceux qui ont vanté les mérites de l'approche constructive de Kronecker par rapport à l'approche plus ensembliste de Dedekind — voir son *Algebraic theory of numbers* [110].

Dans la postérité de Kronecker, il faudrait sans doute inclure des parties de Brouwer, des semi-intuitionnistes français, Borel et Poincaré surtout et jusqu'à un certain point Hadamard, qui comme Brouwer a emprunté à la théorie arithmétique des fonctions de plusieurs variables de Kronecker le nombre de rotation (qui est un entier) pour les besoins particuliers de la topologie — le nombre ou l'index de rotation est le nombre de fois qu'une courbe fermée passe autour d'un point donné p dans le plan. Les constructivistes russes comme Markov, Shanin, Kolmogorov jusqu'à Yessenin-Volpin se partagent aussi une part de l'héritage kroneckerien. Mais c'est certainement en géométrie algébrique contemporaine que l'influence de Kronecker s'est fait le plus sentir. André Weil [106] considère Kronecker comme le père de la géométrie arithmétique dans la mesure où Kronecker a été à l'origine de la théorie arithmétique des fonctions elliptiques — qui sont devenues les courbes elliptiques ou les formes modulaires de la géométrie algébrique contemporaine. Par exemple, le programme de Langlands est expressément inspiré du rêve de jeunesse « *Jugendtraum* » de Kronecker qu'on peut interpréter comme une théorie arithmétique de l'interaction entre théorie des nombres, algèbre et analyse, puisque Kronecker affirmait dans ses recherches sur les fonctions elliptiques que l'objet d'études était tiré de l'analyse (mathématique), que la démarche était algébrique et que la direction et le but étaient donnés par la théorie des nombres (voir là-dessus Gauthier [42], chap. 2.5).

Kronecker a déclaré en 1886 que son rêve de jeunesse « *Jugendtraum* » a été l'arithmétisation de l'algèbre et qu'il est parvenu à le réaliser dans sa théo-

rie des formes ou polynômes homogènes. Un bel exemple du prolongement du programme de Kronecker a été fourni récemment par le mathématicien français Laurent Lafforgue qui a réussi à démontrer une partie importante du programme de Langlands, inspiré lui aussi par le progamme de Kronecker (voir Langlands [76]). Dans les années 1970, le mathématicien russe Vladimir Drinfeld a cherché à généraliser le théorème de Kronecker-Weber qui énonce que toute extension abélienne de $\mathbb{Q}$ (corps des rationnels) appartient au corps cyclotomique $\mathbb{Q}(\xi_m)$ des racines de l'unité. Drinfeld — qui a aussi introduit la notion de groupe quantique — s'inspirant de Kronecker tente de démontrer la correspondance de Langlands sur le corps des fonctions rationnelles. C'est Lafforgue qui réussit à démontrer le cas général à l'aide d'une technique d'itération sur les « chtoukas » de Drinfeld — du russe « *chtoukas* » dérivé de l'allemand « *Stücke* » pour morceaux. Il s'agit d'une correspondance exacte entre morceaux finis de l'espace (modulaire) et points rationnels (dénombrables), alors que la formulation originale de Langlands renvoie à la correspondance entre les représentations l-adiques (nombres premiers l) du groupe de Galois G sur un corps fini F et les représentations GL_2 (transformations linéaires sur un corps de fonctions $F(X)$. Quant à Grothendieck, Jean Dieudonné a reconnu que sa notion centrale de schème pour les variétés algébriques dérivait de la notion kroneckerienne de système modulaires et bien que sa théorie « motivique » des correspondances algébriques soit considérée comme spéculative, on peut penser qu'elle s'inspire pour une part importante d'un motif kroneckerien, celui de la « polynomie » des structures algébriques.

Un autre exemple touche de plus près la logique, l'élimination des quantificateurs chez Tarski où certains ont vu l'acte de naissance de la théorie des modèles au sens de la logique mathématique ; selon van den Dries [102], la méthode s'inspire directement de la méthode de substitution-élimination de Kronecker.

2.3 L'élimination des quantificateurs

L'élimination des quantificateurs a permis à Tarski d'obtenir une solution positive au problème de la décision pour l'algèbre et la géométrie élémentaires [97] dont l'aboutissement est une forme normale disjonctive (disjonction de conjonctions de formules atomiques) proche parente du théorème de Herbrand et du théorème de Hilbert-Ackermann pour les théories ouvertes,

c'est-à-dire les théories dont les axiomes non logiques sont des formules sans quantificateur. Ici se trouve sans doute un terrain de rencontre pour la théorie des démonstrations et la théorie des modèles — cette dernière a depuis évolué de façon indépendante sous la poussée du théorème de compacité. Mais pour arriver à son résultat syntaxique, Tarski a suivi une route similaire à la théorie de l'élimination de Hilbert (ou de Hilbert-Kronecker). Le point de départ est un système de polynômes

$$\begin{aligned}
\alpha &\equiv \alpha_0 + \alpha_1\xi + \ldots + \alpha_m\xi^m \\
\beta &\equiv \beta_0 + \beta_1\xi + \ldots + \beta_n\xi^n \\
\gamma_1 &\equiv \gamma_{1,0} + \gamma_{1,1}\xi + \ldots + \gamma_{1,n_1}\xi^{n_1} \\
&\vdots \\
\gamma_r &\equiv \gamma_{r,0} + \gamma_{r,1}\xi + \ldots + \gamma_{r,n_r}\xi^{n_r}
\end{aligned}$$

pour lequel est définie une fonction T pour les formules Φ de la forme

$$\left(\underset{k}{E}\xi\right)\ [a = 0]$$

où $\underset{k}{E}\,\xi$ signifie "il y a exactement k valeurs de ξ" telles que $T(\Phi)$ est une formule sans quantificateur équivalente. La procédure d'élimination repose ici sur le théorème de Sturm sur le nombre de racines réelles d'un polynôme entre deux valeurs quelconques $f_0(x)$ et $f_1(x)$ de la variable et se réduit à l'algorithme d'Euclide pour la détermination du plus grand diviseur commun de $f_0(x)$ et $f_1(x)$ dans le décompte des variations de signe pour le polynôme en question (qui est une équation ou une inégalité). Bien que Tarski mentionne Kronecker et nonobstant les remarques de van den Dries quant à la source kroneckerienne de la théorie de l'élimination, Tarski ne s'inspire pas directement de la théorie des formes (polynômes homogènes) de Kronecker. L'arithmétique générale des quantités algébriques chez Kronecker est une théorie du contenu des polynômes et Tarski ne va utiliser une notion de contenu que dans sa théorie de l'implication et de la conséquence logique.

C'est toujours le noyau arithmétique qui est le centre d'attraction des champs de l'arithmétique, de l'algèbre et de l'analyse, comme le note avec force Kronecker dans son analyse du théorème de Dirichlet sur l'infinité des nombres premiers dans toute progression arithmétique $a + nb$ où a et b sont relativement premiers, *i.e.* sans dénominateur commun $\neq 1$. Le théorème récent de Green et Tao stipule qu'il y a des progressions arithmétiques de longueur arbitraire dans la suite des nombres premiers — le théorème utilise

la théorie ergodique (et les séries de Fourier) en plus de théorèmes combinatoires de van der Waerden, Szemerédi, Furstenberg et d'autres dont on cherche à extraire le contenu constructif. Le théorème sur la distribution asymptotique des nombres premiers et le théorème de Dirichlet sur l'infinité des nombres premiers dans toute progression arithmétique, on le sait maintenant, ont des versions élémentaires obtenues par Selberg et Erdös en 1949 et en 1950. Élémentaire signifie ici que l'on n'utilise que des méthodes arithmétiques constructives ou combinatoires comme les sommes finies sans recours aux méthodes transcendantes comme le prolongement analytique de séries infinies en analyse complexe. Je ferai remarquer que Dirichlet dans sa preuve de 1836 avouait que :

> *Es fehlt noch an gehörigen Principien, unter denen transzendente Verbindungen, welche unbestimmte ganze Zahlen enthalten, verschwinden können.* ([77], p. 326.)

notant donc qu'il manque encore les principes appropriés en vertu desquels les relations transcendantes (obtenues par les séries infinies) entre des entiers indéterminés pourraient être éliminées. À propos des séries infinies, Kronecker pensait qu'elles étaient inutiles au-delà des séries de puissances formelles considérées comme des expressions des séries finies dans leur support polynomial de degré fini ([73], III, p. 156).

Kronecker qui a édité les *Werke* de Dirichlet a proposé dans ses *Vorlesungen über Zahlentheorie* [72] d'étendre arithmétiquement un intervalle fini $(\mu \dots \nu)$ pour les entiers μ et ν afin d'y loger au moins un nombre premier $hm+r$ pour m et r relativement premiers. On pourrait voir là une anticipation des idées de Selberg qui utilise des formules asymptotiques pour la fonction logarithmique sur des segments ou intervalles finis de $\mathbb{Z}$ (voir Gauthier [42], p. 36). Le théorème sur les nombres premiers est associé à l'hypothèse de Riemann pour les zéros de la fonction $\zeta(s)$ sur la droite réelle $1/2$. Je noterai encore que l'hypothèse de Riemann est née d'une remarque marginale dans le texte de 1859 « *Über die Anzahl der Primzahlen unter einer gegebenen Grösse* » et que Riemann l'a laissée de côté « *bei Seite gelassen* » puisqu'il s'intéressait d'abord au problème de la distribution des nombres premiers.

C'est assurément le mot d'ordre « nombre fini d'étapes » que l'on trouve dans l'introduction de Kurt Hensel aux *Vorlesungen über Zahlentheorie* de Kronecker qui définit le mieux l'option constructiviste du programme de Kronecker dans les fondements des mathématiques. Hensel lui-même a appliqué la méthode kroneckerienne du pas à pas dans ce que l'on appelle le lemme de

Hensel dans la théorie des corps finis et l'analyse p-adique (p pour nombres premiers). C'est un instrument important quand on veut éviter la méthode transcendante de la complétion des corps — voir là-dessus Macintyre [80] qui en montre la pertinence en théorie des modèles contemporaine. Bon nombre de logiciens et de mathématiciens ont adopté le précepte kroneckerien, de Skolem, Goodstein, Curry et Nelson aux algébristes constructivistes et aux informaticiens qui traitent d'algorithmes et de structures finies. Sans compter des philosophes comme Kaufmann ou Wittgenstein (voir Marion [81]) qui ont emboîté le pas, sans se réclamer ouvertement de Kronecker dans bien des cas. Mais c'est Hilbert qui a suivi le premier le programme de Kronecker plus ou moins consciement et non sans réticence. Il a en tout cas amorcé dans l'ombre géante de Kronecker le programme de l'arithmétisation de la logique.

Chapitre 3

L'arithmétisation de la logique

Hilbert n'a pas créé l'expression « métamathématique », mais il a été le premier à lui donner le sens de théorie des systèmes formels destinée à dégager la logique interne « *inhaltliche Logik* » des mathématiques et c'est la logique interne de l'arithmétique, ce que j'appelle la logique arithmétique, qui a d'abord fait l'objet de ses travaux.

Il est bien connu que la métamathématique hilbertienne — théorie des systèmes formels ou théorie des démonstrations — a pour objectif la délimitation des méthodes finitaires et repose sur le finitisme dont Kronecker s'est fait le champion ; il semble que Hilbert soit parti de là, comme l'attestent ses premiers écrits sur le sujet (voir Hallett [54]).

L'ébauche de fondements de la logique et de l'arithmétique dans un même temps (Hilbert [57]) met de l'avant le concept d'équations homogènes dans l'esprit de la théorie polynomiale de Kronecker. La consistance de l'arithmétique se résume pour Hilbert à la dérivation de l'équation homogène $a = a$ ou de l'inéquation $a \neq a$. À l'époque selon le témoignage de Bernays, Hilbert était prêt à baisser les bras devant le finitiste Kronecker tout en accusant ce dernier de dogmatisme ; mais devant la menace des paradoxes, il abandonnait ses recherches fondationnelles pour s'en remettre à la perspective kroneckerienne en algèbre et en théorie des nombres. Ce n'est qu'en 1918 que Hilbert revient à ses travaux fondationnels et au finitisme, non sans polémiquer avec Kronecker à titre posthume, avec Brouwer et Weyl aussi qu'il jugeait trop près de Kronecker. La fondation simultanée de la logique et de l'arithmétique le préoccupe toujours et le recours à la notion de système formel a pour fonction de produire un mécanisme (un algorithme fini) pour l'introduction des éléments idéaux qui seront associés au système formel à la ma-

nière d'indéterminées ; la consistance de ces nouvelles associations ne pourra être que l'oeuvre d'un formalisme comparable à un algorithme polynomial de l'arithmétique générale, e.g. la méthode de la descente infinie fermatienne en tant qu'algorithme euclidien généralisé. Dans son texte de 1918 sur la pensée axiomatique « *axiomatisches Denken* », Hilbert isole les propriétés d'indépendance et de consistance comme principales caractéristiques de la méthode axiomatique. La consistance relative de la géométrie et des autres disciplines selon Hilbert repose sur la consistance de l'arithmétique, mais il n'y a pas d'autre fondement à l'arithmétique — et à la théorie des ensembles, d'ajouter Hilbert — que l'arithmétique elle-même. La consistance ou la non contradiction « *Widerspruchslosigkeit* » est une question logique et c'est à la logique (le système formel) que revient en dernière analyse le problème de la décision « *Entscheidungsproblem* » qui doit s'effectuer en « un nombre fini d'étapes » ([59], III, p. 154). Hilbert donne ici l'exemple de la théorie des invariants pour laquelle il avait produit une preuve de finitude inspirée par la méthode qu'il avait utilisée dans son résultat majeur, le théorème de la base finie. Le théorème de la base finie a été pratiquement dicté par les résultats de Kronecker dans son arithmétique générale et il est devenu aux yeux de Hilbert le cas paradigmatique de la décidabilité d'un système formel ; mais il n'y a pas de logique dans le théorème de la base finie, uniquement de l'algèbre, c'est-à-dire les fonctions algébriques du corps des invariants représentables par

$$i = A_1 J_1 + \ldots + A_m J_m$$

où les A_i sont des fonctions rationnelles entières des J_i — voir pour plus de détails Gauthier [42], chap. 2). Il n'est pas étonnant que les théories décidables soient pour la plupart des théories algébriques élémentaires (du premier ordre) et se retrouvent en théorie des modèles et non en théorie des démonstrations. La méthode tarskienne d'élimination des quantificateurs, comme nous l'avons vu dans le chapitre précédent, est un test de décidabilité et remonte à la théorie de l'élimination de Kronecker. Mais alors quel est l'intérêt logique de la méthode de décision ? C'est qu'une théorie logique est décidable en un nombre fini d'étapes et la même exigence s'applique pour une théorie consistante. Dans le cas des théories du premier ordre, géométrie et algèbre élémentaires, la logique ne joue aucun rôle spécial, puisque le calcul équationnel n'a pas besoin d'autres lois que les lois purement arithmétiques (ou combinatoires).

L'apport de la logique réside uniquement dans les extensions conserva-

trices de l'arithmétique au domaine (transfini) des éléments idéaux. Il n'en reste pas moins que même si Hilbert a espéré une justification logique des éléments idéaux, il a constamment insisté sur le fait qu'un procès ou une procédure finie est le moteur inférentiel de la consistance interne « *innere Widerspruchslosigkeit* ».

La consistance interne est obtenue par des moyens internes dans le cas de la théorie des invariants algébriques et Hilbert ne s'est pas trompé quand il réduit la consistance de l'arithmétique au calcul polynomial où la non contradiction correspond à l'équation $a = a$ et la contradiction à l'inéquation $a \neq a$. Un des outils principaux de la consistance interne pour l'arithmétique est le produit de convolution (de Cauchy) pour les polynômes qui génère des expressions polynomiales linéaires à partir d'expressions polynomiales comme dans l'arithmétique générale de Kronecker, le théorème de Prague de Dedekind ou le résultat de Hilbert en théorie des invariants algébriques — voir l'Annexe B où j'ai exploité le produit de Cauchy parmi d'autres méthodes pour une preuve de consistance interne de l'arithmétique. Le produit de Cauchy peut être appelé diagonale de Cauchy. C'est par une belle ironie de l'histoire que le programme général de Hilbert a reçu son plus dur coup par la méthode diagonale de Cantor qui est au coeur du résultat d'incomplétude de Gödel. En effet, l'accès au paradis cantorien doit emprunter la voie diagonale qui ne relève ni de la théorie des nombres, ni de l'algèbre, mais de l'arithmétique ensembliste, comme Hilbert lui-même la nommait, et c'est aussi cette voie diagonale de la théorie cantorienne des ensembles qu'il voulait « sécuriser » dans sa théorie des démonstrations : c'est là une autre situation paradoxale pour le logicien Hilbert que de voir son « programme fort » de la consistance de la théorie des ensembles et de l'analyse miné de l'intérieur par une procédure ensembliste !

Kreisel a voulu récupérer des morceaux du programme de Hilbert « modifié » ; d'autres comme Sieg, Feferman et Simpson ont mis en évidence des réalisations partielles du programme de Hilbert, mais aucun n'a voulu le reconduire à ses racines kroneckeriennes. Quoi qu'il en soit des mérites de programmes comme les « mathématiques régressives » de Friedman et Simpson, ce ne sont que des entreprises *a posteriori* qui ne peuvent servir qu'à une justification à rebours. Le programme de Weyl repris par Feferman de mathématiques prédicatives ne semble pas récupérer autant de mathématiques classiques que le programme régressif tout en rognant sur les principes constructivistes. Le programme de l'extraction de preuves « *proof mining* » mené par Kohlenbach et autres pour l'analyse classique n'a qu'une vocation

semi-constructiviste tout en restant utile pour dégager un contenu constructif partiel (sur les bornes effectives) de théorèmes non constructifs. Seul le programme de l'arithmétique prédicative de Nelson [85] semble assez radical pour raviver la source constructiviste du finitisme hilbertien, mais pour plusieurs il s'arrête trop court à la superexponentiation $2 \Uparrow 5$. Tous ces programmes ne semblent pas recouvrer l'arithmétique générale de Kronecker, l'asile sécuritaire des vraies mathématiques dans les mots de Kronecker.

Un programme fondationnel « progressif » pour la logique et les mathématiques n'est pas nécessairement restrictif, c'est une tentative pour étendre le territoire de conservation des mathématiques constructives sans renoncer aux principes fondamentaux qui ne doivent pas servir de refuge philosophique, ni de négationnisme fondationnel qu'on oppose aux crédos réalistes. L'incitation révisionniste est une invitation au travail créateur et une posture fondationnelle souple devrait permettre de concevoir la réconciliation des programmes respectifs de Kronecker et Hilbert dans la perspective de l'arithmétisation de la logique qui est en même temps une « délogicisation » de l'arithmétique.

3.1 L'arithmétisation de la logique et le calcul epsilon

Hilbert a conçu le calcul epsilon pour traduire les quantificateurs existentiel et universel et leur substituer une fonction de choix qui tient lieu d'axiome de choix, selon Bourbaki dans sa *Théorie des ensembles* [11]. Le motif plus profond de Hilbert était la réduction finitaire du problème de la consistance de l'arithmétique. C'est la faillite du programme logiciste qui a poussé Hilbert à chercher des fondements finitistes — en grande partie inspirés par Kronecker, répétons-le — pour l'arithmétique et éventuellement pour l'analyse et la théorie des ensembles. Ce n'est pas parce que le programme dans son intégrité a échoué aux yeux de plusieurs qu'il faille obnubiler l'intention première ; cette intention première, il faut sans doute la rapatrier dans son pays d'origine, l'arithmétique générale de Kronecker.

L'idée de Hilbert en introduisant le symbole ϵ était d'assurer le passage de l'arithmétique aux éléments idéaux de la théorie des ensembles et de l'analyse, c'est-à-dire d'assurer la consistance des mathématiques infinitaires à l'aide de l'arithmétique finitaire, la théorie Z de l'arithmétique classique (récursive primitive). Hilbert a conçu la fonction de choix transfinie pour combler le

fossé entre l'arithmétique finie et l'arithmétique transfinie de Cantor. Mais une fois que ce niveau supérieur de l'existence mathématique est atteint, il faut redescendre à la base finie : c'est la méthode de descente « *Methode der Zurückführung* » qui consiste en une construction « *Aufbau* » et une décomposition « *Abbau* » ou « *Zerlegung* » en termes arithmétiques. Le problème de la consistance de l'arithmétique est donc une question d'arithmétique finie qu'on doit sauvegarder par une procédure d'élimination du symbole ϵ et des formules critiques qui y sont attachées. À la question souvent posée : "Pourquoi introduire le symbole ϵ si c'est pour l'éliminer tout de suite après ?", la réponse est simplement : "Pour construire un royaume idéal et revenir ensuite aux fondements arithmétiques pour garantir l'édifice entier des mathématiques". La logique (avec la méthode axiomatique) n'est qu'un outil dans la mesure où elle s'occupe des inférences arithmétiques élémentaires et de leur vérité par l'extension consistante de ses méthodes, mais elle permet en même temps les inférences transarithmétiques.

Le premier axiome pour le symbole ϵ est

$$A(a) \to A(\epsilon_x A(x))$$

où $\epsilon(A)$ est une fonction logique de choix transfinie. Le quantificateur existentiel est défini par

$$\exists x\, Ax \equiv A(\epsilon_x\, A(x))$$

et le quantificateur universel par

$$\forall x\, Ax \equiv A(\epsilon_x \neg A(x))$$

signifiant que la quantification universelle peut être assertée si on ne peut trouver de contre-exemple après un essai fini, i.e. une itération finie de la fonction de choix transfinie.

L'introduction du symbole ϵ requiert deux théorèmes sur les formules critiques et leur élimination : le premier théorème ϵ élimine les formules critiques contenant un terme t

$$A(t) \to A(\epsilon_r\, A(r))$$

par une méthode de résolutions symboliques

$$(R) = \begin{cases} A(t_1) \to A(\epsilon_r\, A(r)) \\ \qquad\qquad \vdots \\ A(t_n) \to A(\epsilon_r\, A(r)) \end{cases}$$

qui reproduit la décomposition des polynômes, puisque termes et expressions sont ordonnés selon leur degré et leur rang ; le degré est le nombre (fini) maximal de termes dans une suite de termes ϵ et le rang d'une expression ϵ est le nombre (fini) maximal d'expressions dans une suite d'expressions ϵ. Pour les polynômes on obtient une réduction à une forme disjonctive de termes sans symbole ϵ, i.e. une expression linéaire. Le deuxième théorème ϵ applique le même procédé aux formules existentielles et à l'axiome d'identité. C'est le schéma d'induction qui crée un problème et requiert une nouvelle formule critique

$$A(t) \to A(\epsilon_r\, A(r) \neq t).$$

La substitution s'effectue ici au moyen de noms de nombres ou symboles numériques « *Ziffer* » pour les termes ϵ et la méthode devra introduire une formulation du principe d'induction à l'aide du symbole ϵ. Les formules

$$A(a) \to \epsilon_x\, A(x) \neq a'$$

et

$$a \neq 0 \to \delta(a)' = a$$

pour l'existence des successeurs et de leur récursion donnent naissance à un nouveau principe d'induction qui est formulé de la façon suivante :

«Pour tout prédicat numérique P qui s'applique à un nombre au moins, il y a un nombre correspondant à P, mais pour son prédécesseur, s'il y en a un, P ne s'applique pas ».

Ce principe est une conséquence directe du principe du plus petit nombre avec la fonction récursive générale μ

$$A(a) \to \mu_x\, A(x),$$

mais la procédure générale rappelle la décomposition polynomiale en facteurs irréductibles, i.e. l'algorithme euclidien pour le plus grand diviseur commun et sa généralisation par descente infinie pour les polynômes de degré n ou par la condition de la chaîne pour les anneaux (noéthériens) de polynômes.

Le principe de substitution prend la forme de substitutions partielles ou globales et les substitutions effectives de termes vont consister à trouver le polynôme de résolution en réduisant les substitutions d'instances de termes à des types fondamentaux de termes, c'est-à-dire des termes qui ne font pas partie d'autres termes. Le procédé reproduit la théorie générale de l'élimination chez Kronecker et la preuve de consistance se ramènera aux formules

réduites "irréductibles", comme le montre, par exemple, la preuve de consistance de Ackermann pour l'arithmétique [1]. La preuve de Ackermann repose essentiellement sur le nombre de réduction des substitutions globales « *Gesamtersetzungen* » pour les numéraux et les fonctions en recourant à la machinerie des fonctions récursives : on aboutit ainsi à une "suite normale" dont l'expression

$$n_0 \cdot 2^h + n_1 \cdot 2^{h-1} + \ldots + n_{h-1} \cdot 2 + n_h$$

pour les nombres n substitués aux termes. Le nombre de réduction a la valeur 1 ou 0 selon que la substitution globale se réduit à 0 ou à $j \neq 0$. Le nombre total de substitutions globales est 2^n lorsque le nombre de termes ϵ (de rang 1) dans la suite des formules est n, comme c'est le cas pour le nombre de coefficients dans un binôme, par exemple. Pour les rangs supérieurs, les équations récursives primitives suffisent

$$\begin{gathered}\psi(1,n) = 2^n \\ \psi(m+1,n) = 2^{n-\phi(m,n)} \cdot \psi(m,n).\end{gathered}$$

Le deuxième théorème ϵ a encore affaire aux formules critiques de la seconde espèce, i.e. la résolution symbolique des formules existentielles en éliminant le quantificateur existentiel des formules comme

$$\exists r_1 \ldots \exists r_r \, \forall n_1 \ldots \forall n_s \, A(r_1, \ldots, n_s)$$

pour obtenir une disjonction

$$\begin{gathered}A\left(t_1^{(1)}, \ldots, t_r^{(1)}, f_1(t_1^{(1)}, \ldots, t_r^{(1)}), \ldots, f_s(t_1^{(1)}, \ldots, t_r^{(1)})\right) \vee \ldots \vee \\ A\left(t_1^{(m)}, \ldots, t_r^{(m)}, f_1(t_1^{(m)}, \ldots, t_r^{(m)}), \ldots, f_s(t_1^{(m)}, \ldots, t_r^{(m)})\right)\end{gathered}$$

où les termes $t_j^{(i)}$ ne contiennent pas le symbole ϵ et les f_i sont des symboles de fonctions à r-arguments

$$f_1(c_1, \ldots, c_r), \ldots, f_s(c_1, \ldots, c_r)$$

Si un axiome d'égalité est ajouté, on obtient un pur calcul des prédicats qui ouvre le chemin à une preuve de consistance dans le style de Herbrand.

3.2 Herbrand

Dans ses travaux sur la consistance de l'arithmétique, Herbrand adopte le point de vue finitiste de Hilbert (voir [56]). Herbrand, par-delà Hilbert, revient à la posture fondationnelle de Kronecker et ce qu'il appelle argument intuitionniste est en fait une procédure constructive quand il déclare qu'il ne suppose pas qu'un objet existe sans qu'on ne puisse trouver un moyen de le construire ; de même ce qu'il appelle un champ infini n'est qu'une abréviation pour la construction itérative du « pas à pas » d'un domaine d'objets illimité ou « effini », comme je préfère le dire. Son *théorème fondamental* porte sur l'identité $a = a$ ou la non identité $a \neq a$, ce que Hilbert désignait par équation ou inéquation (inégalité). Si P est une identité, une preuve de P va nous permettre de trouver un nombre h tel que P ne puise être vraie dans tout domaine d'ordre h ; de même si P n'est pas une identité, pour tout h on peut construire un domaine d'ordre h dans lequel P est vraie. L'idée de Herbrand dans sa preuve de consistance est de se servir d'une induction sans quantificateur (sans variables liées) et de laisser libre cours à des récursives générales obtenues par substitution et récursion, comme nous le verrons plus loin. Herbrand est bien conscient qu'il n'y a pas de procédure générale ou d'algorithme pour définir toutes les fonctions récursives et que c'est la seule méthode diagonale qui permet à Gödel de passer outre pour démontrer l'incomplétude de l'arithmétique.. L'arithmétique récursive de Herbrand peut se traduire facilement en termes de polynômes où l'on remplace la notion d'ordre d'un domaine ou champ par celle de degré et il saute aux yeux qu'un polynôme de degré fini obtenu par composition récursive (substitution et récursion) est soumis à la diagonale de Cauchy et échappe à la diagonale de Cantor qui suppose une quantification sur l'ensemble des nombres naturels, ce que refuse Herbrand dans sa démarche intuitionniste ou constructiviste. C'est cependant dans sa thèse de 1930 formule son théorème sur la consistance du calcul des prédicats. Ce qui importe à nos yeux dans la démarche de Herbrand, c'est son insistance sur les méthodes finitaires et le point de vue fondationnel qui s'y rattache. Ainsi Herbrand formulera l'hypothèse suivante :

> les méthodes transcendantes ne peuvent permettre de démontrer en arithmétique de théorèmes qu'on ne puisse démontrer sans leur aide. (Herbrand 1968, p. 152.)

La conjecture de Herbrand trouve un écho dans un article récent de J. Avigad qui, sans mentionner Herbrand, attribue à Harvey Friedman la conjecture suivante qu'il appelle *Grand Conjecture* :

> Every theorem published in the *Annals of Mathematics* whose statement involves only finitary mathematical objects (i.e. what logicians call an arithmetical statement) can be proved in elementary arithmetic. [4]

Cela inclut évidemment le dernier théorème de Fermat dont la preuve par Andrew Wiles a occupé tout un numéro des *Annals of Mathematics* en 1995 — il faudrait donc dégager cette preuve de sa gangue analytique ! Le logicien contemporain entend par élémentaire un sous-système de l'arithmétique de Peano du premier ordre ou encore l'arithmétique récursive primitive avec induction bornée. Notons que des mathématiciens importants, comme Hardy et Littlewood ne croyaient pas possible une preuve élémentaire, ici sans les moyens analytiques, *i.e.* séries infinies de l'analyse complexe, de théorèmes arithmétiques comme le théorème sur la distribution asymptotique des nombres premiers ou le théorème de Dirichlet sur l'infinité des nombres premiers dans toute progression arithmétique. Comme on sait, l'histoire à donné raison à Herbrand dans ces deux cas à tout le moins, puisque Selberg (avec Erdös) a réussi a en donner des preuves élémentaires en n'utilisant que des logarithmes et sommes finies. C'est donc dans le cadre restreint des méthodes finitaires du programme de Hilbert que Herbrand formule ses théorèmes de consistance.

Le théorème de Herbrand sur la consistance du calcul des prédicats est dans cet esprit. Soit A une formule en forme prénexe

$$A \equiv \exists x \forall y \exists z \forall t R\left(x, y, z, t\right)$$

avec R sans quantificateur. On introduit deux nouvelles lettres de fonctions, f unaire et g binaire avec les termes $U_1 \ldots U_n, W_1 \ldots W_n$, alors A est démontrable dans le calcul des prédicats sous la forme

$$A \equiv B\left(U_1, f\left(U_1\right), W_1, g\left(U_1, W_1\right)\right) \vee \ldots \vee B\left(U_n, f\left(U_n\right), W_n, g\left(U_n, W_n\right)\right).$$

Cette disjonction, comme celle qu'on a vue plus haut, est dérivable dans un calcul propositionnel et peut servir de critère de réfutabilité dans une interprétation négative (voir Hilbert et Bernays [61], II, pp. 170 ss.).

La négation de A est

$$\neg A \equiv \forall x \exists y \forall z \exists t \neg B\left(x, y, z, t\right)$$

ou

$$\neg A \equiv \neg B\left(x, f\left(x\right), z, g\left(x, y\right)\right)$$

et si Herbrand a vu la consistance dans la réfutabilité dans un "champ infini" ou indéfini, Kreisel a pensé l'interprétation sans contre-exemple (abordée par Gödel dès 1938) comme une interprétation fonctionnelle sur les types supérieurs ; les fonctionnelles récursives sont de la forme

$$Bx_1 \ldots x_n \left[F_1\left(f_1, \ldots, f_n\right), \ldots, F_m\left(F_1, \ldots, F_n\right)\right]$$

avec B ouverte. Pour une formule vraie A, nous avons

$$B\left[F\left(f, g\right), f\left(F\left(f, g\right)\right), G\left(F\left(f, g\right), G\left(F, g\right)\right)\right]$$

où les F et les G sont évidemment nos nouvelles fonctionnelles récursives sur les types.

La dernière formule A est vraie s'il n'y a pas de contre-exemple de la forme

$$\neg B\left[x, f\left(x\right), z, g\left(x, y\right)\right]$$

avec f et g comme arguments des fonctionnelles récursives F et G de type supérieur ; F et G sont continues et peuvent donc être associées à des polynômes de degré arbitraire : nous pouvons définir la composition de F et G

$$F \cdot G = \left(\sum_i F_i\, x^i\right)\left(\sum_j G_j\, x^j\right) \sum_i \sum_j \left(F_i\, G_j\, x^{i+j}\right).$$

Puisque nous ne pouvons quantifier sur toutes les fonctionnelles — par diagonalisation il y a une fonctionnelle récursive qui est distincte de toutes les fonctionnelles récursives — nous devons nous restreindre aux polynômes de degré fini et utiliser la descente sur les degrés et les hauteurs de polynômes pour retrouver une version finitiste.

Remarquons que les fonctions récursives primitives peuvent se traduire aisément en fonctions polynomiales. La chose est évidente pour les fonctions constantes initiales ; la composition et la récursion sont traitées comme un produit de convolution $G \cdot H$ pour G et H de telle sorte que

$$F\left(x\right)_{\vec{n}} = G_n\left(H_1\left(a_n\right), \ \ldots \ , \ H_p\left(a_n\right)\right)$$

avec

$$H \cdot G = \sum_i \sum_j \left(G_i\, H_j\, x^{i+j}\right).$$

L'opérateur μ comme l'équivalent du principe du plus petit nombre est remplacé par la descente (finie) infinie sur les puissances décroissantes d'un polynôme de degré fini

$$F(x)_{\overleftarrow{n}} = f_0 x^n + f_1 x^{n-1} + \ldots + f_{n-1} x + f_n.$$

Selon l'idée de Hilbert d'une suite terminale de prédécesseurs pour un n donné, la descente fermatienne autorise un processus de réduction fini à la façon d'un ordre linéaire décroissant de puissances pour un polynôme donné.

3.3 De Hilbert à Kronecker

Le programme de Hilbert peut être modifié, comme l'a suggéré Kreisel. Une modification majeure consiste à refonder le programme de Hilbert sur ce que j'ai appelé le programme de Kronecker. Quand Hilbert, dans sa conférence de 1926 « *Über das Unendliche* », explique que du point de vue finitaire « *finiter Standpunkt* » il y a deux sortes de formules en mathématiques, les premières qui correspondent aux énoncés finitaires et les secondes aux structures idéales — qui ne signifient rien — il ne fait que transposer Kronecker et son langage d'une arithmétique pure ou arithmétique générale et de ses extensions indéterminées (qui recouvrent les éléments idéaux) dans le contexte de la métamathématique ou théorie des preuves qu'il veut ériger. Mais si les opérations extra-arithmétiques de la logique ne signifient rien, pas plus que les grandeurs algébriques hors d'un domaine de rationalité, et si seule l'arithmétique est interne alors que l'algèbre est formelle, le système formel des opérations logiques n'aura que le rôle d'une extension dénuée de sens de l'arithmétique, à condition que cette extension soit consistante, c'est-à-dire qu'une fois éliminées les structures idéales (ou les indéterminées), on conserve toujours la validité des lois logiques (du domaine primitif de l'arithmétique) ou l'arithmétique pure du domaine de rationalité. On voit le parallèle évident entre la démarche de Kronecker et celle de Hilbert. La parenté est si grande qu'on peut supposer que Hilbert s'inspire toujours, consciemment ou non, de l'idéal arithméticien de Kronecker.

Les objets concrets qui vont remplacer les entiers dans la métamathématique hilbertienne sont les signes et la combinatoire finie qu'ils génèrent est le pendant formel de l'arithmétique. Au commencement est le signe, c'est la devise philosophique de Hilbert dès 1902. Sur cette base finitaire, on peut

formaliser les théories mathématiques existantes en construisant ensemble logique et arithmétique. Cette logique arithmétique, comme nous pouvons l'appeler, recèle une logique interne — une métamathématique — qui, par-delà les preuves formelles des mathématiques ordinaires, doit mener à une preuve de non contradiction des mathématiques, puisque l'objet de la métamathématique est l'ensemble des preuves de la mathématique usuelle. Cette logique interne doit produire de nouveaux axiomes, alors que la logique formelle ne fait que dériver de nouveaux théorèmes des axiomes connus. La logique finitaire suffit à garantir la vérité intuitive de l'arithmétique élémentaire. On connaît la définition hilbertienne de système formel avec connecteurs et quantificateurs. Les quantificateurs universel et existentiel sont définis à l'aide d'une fonction de choix transfinie $\varepsilon(A)$ qui associe à tout prédicat un objet ou à toute fonction un nombre ; ainsi le quantificateur universel est défini par la fonction de choix qui ne peut trouver de contre-exemple au prédicat (ou à l'image de la fonction). Hilbert y ajoute l'axiome aristotélicien pour l'import existentiel du quantificateur universel et le principe du tiers exclu qui signifie que la négation du quantificateur universel implique l'existence d'un contre-exemple.

Bien que la fonction (logique) de choix ne soit pas constructive, Hilbert croyait que par son emploi réitéré un nombre fini de fois, la finitude de la procédure était assurée et qu'il était possible d'obtenir une preuve de consistance dans cette voie. Ackermann a pu ainsi obtenir une preuve de consistance de l'arithmétique en utilisant la méthode de la substitution ε élaborée par Hilbert.

On sait que l'espoir que fondait Hilbert de démontrer la consistance de l'arithmétique et au-delà, de l'analyse, ne s'est pas réalisé, sans doute parce qu'il s'éloignait trop du point de vue finitaire et qu'il voulait même justifier la théorie des ensembles transfinis de Cantor.

Le programme de Hilbert n'a pas échoué en vertu des résultats de Gödel sur l'incomplétude des systèmes formels contenant au moins l'arithmétique, il a échoué en tout cas parce qu'il a voulu aller plus loin que l'arithmétique au sens de Kronecker, arithmétique qu'on peut appeler finitaire ou prédicative et qui trouve des échos contemporains dans les travaux de E. Nelson [85]. L'arithmétique prédicative exige des bornes supérieures (ou logarithmiques) tout autant que dans la théorie des systèmes d'invariants complets qui est fondée sur la théorie des corps (ou du domaine de rationalité) des fonctions algébriques de Kronecker. L'arithmétique de Peano, de ce point de vue, n'est pas prédicative en vertu du postulat d'induction.

Le point de vue génétique de Kronecker lui a permis d'échapper à la tentation formaliste infinitaire de Hilbert qui a cru finalement à la réalité des indéterminées formelles, pourrait-on dire, parce qu'il n'a pas réussi à les réduire ou à les éliminer. Par ailleurs, le point de vue prédicatif (formaliste ou nominaliste) de Nelson est plus près de Kronecker que de Hilbert, quoi qu'en pense Nelson. En effet, l'arithmétique prédicative s'adjoint des entiers non standard (infinitésimaux) $\nu = \infty$ à la manière des indéterminées de Kronecker et il y a passage de l'interne à l'externe dans une théorie interne des ensembles, mais la théorie malheureusement n'est pas prédicative cette fois. Seule une logique prédicative de l'arithmétique prédicative semble répondre adéquatement au constructivisme de Kronecker.

Le formalisme de Hilbert ne serait donc que l'extension infinitaire (indéterministe, si l'on suit Kronecker) du point de vue finitiste « *finiter Standpunkt* » qui serait tributaire de l'intuitionnisme ou mieux du constructivisme arithmétique de Kronecker. La vérité intuitive ou interne de l'arithmétique lui confère le statut d'une véritable logique arithmétique qui est au fondement de tout l'édifice mathématique.

En dépit de ses nombreuses attaques contre l'attitude de Kronecker qu'il qualifie à plusieurs reprises de « dictateur de l'interdit » « *Verbotsdiktator* », Hilbert a fini par reconnaître en 1930 que

> Kronecker a formulé clairement une conception qu'il a explicitée dans de nombreux exemples : cette conception correspond pour l'essentiel à notre point de vue finitiste. ([59], III, p. 187)

Le finitisme de Hilbert est donc très proche par la filiation de Kronecker de l'intuitionnisme brouwerien et du semi-intuitionnisme d'un Poincaré, par exemple. Ce finitisme n'est pas touché par les résultats d'incomplétude infinitaire, c'est uniquement son extension formaliste infinitaire avec son idéal de consistance absolue qui est affectée. Il n'est pas étonnant à ce compte que ce soit l'induction infinie, le postulat d'induction dans l'arithmétique de Peano, qui constitue l'obstacle majeur. La preuve de Gentzen de la consistance de l'arithmétique fait appel à une induction transfinie jusqu'à ε_0. Le postulat d'induction de Peano n'est pas prédicatif, l'induction transfinie ne saurait l'être. La logique interne de l'arithmétique requiert une induction bornée, une suite "effinie", *i.e.* potentiellement infinie, de nombres naturels, rien de plus. Kronecker, Poincaré, Brouwer ont reconnu le caractère ouvert du procès de l'induction. Les propriétés métamathématiques de consistance, complétude, décidabilité, etc., perdent leur signification concrète, génétique

dans une théorie des démontrations « *Beweistheorie* » qui emprunte son arsenal infinitaire à la théorie des ensembles, se confondant par là avec une théorie des modèles qui est essentiellement une sémantique ensembliste des théories logiques et mathématiques.

L'idéal de la consistance est pourtant simple : accéder pour l'analyse (et la théorie des ensembles) à la même certitude « *Sicherheit* » que possède l'arithmétique finie qui est le fondement intuitif dernier ; c'est pourtant cette même certitude qui devrait guider la métamathématique et sa logique interne « *inhaltiches logisches Schliessen* », selon l'expression de Hilbert. Que cet idéal se soit dévoyé dans un programme formaliste voué à l'échec n'a rien de surprenant, puisque Hilbert n'a pas su s'en tenir au cadre finitaire de l'arithmétique et de ses extensions indéterminées à la manière de Kronecker. Entre-temps, c'est Hilbert (ou son programme) qui a engendré par coups et contrecoups, de Herbrand à Gödel et de Tarski à Robinson, la logique contemporaine. L'avenir proche de la logique, avec la théorie de la computation, les langages informatiques et la logique arithmétique (ou prédicative), verra peut-être un retour à l'inspirateur de Hilbert, Kronecker et à son idéal arithméticien.

3.4 Brouwer

Brouwer ne s'est guère intéressé à la théorie des nombres comme l'ont été Skolem et Herbrand après Hilbert et ce n'est pas en arithmétique, mais en théorie des fonctions que l'on trouvera l'essentiel de ses motifs arithmétiques. La théorie des suites de choix avec les suites régulières et les suites (absolument) irrégulières est en effet de part en part arithmétique dans la mesure où elle renvoie constamment à un contenu numérique, dont Bishop (1967) dira qu'il constitue l'essence des mathématiques intuitionnistes. On sait que la logique intuitionniste est l'affaire de Heyting, Kolmogorov et Gödel (et de leurs successeurs). Le texte séminal de Brouwer (1923) sur le principe du tiers exclu repose sur la notion de suites infiniment processives (que je nomme plutôt « effinies ») pour traduire le procès itératif de l'infini potentiel dans la suite des nombres naturels qui ne peut jamais devenir un ensemble infini, c'est-à-dire une totalité infinie achevée.

Avant de passer à la théorie des suites, il faut dire quelques mots de la notion d'espèce. La notion d'espèce est une notion analogue à celle d'ensemble, mais avec une forte connotation de propriété. On dira qu'une espèce

définit une ou plusieurs propriétés ; l'égalité intensionnelle se lit alors pour deux espèces X et Y

$$X \equiv Y$$

et leur égalité extensionnelle

$$X = Y \leftrightarrow_{df} \forall x \, (x \in X \leftrightarrow x \in Y) \, .$$

Une espèce X est habitée ou garantie si $\exists x \, (x \in X)$ et une espèce Y est détachable dans X si

$$\exists x \in X \, (x \in Y \vee x \notin Y) \, .$$

On définit aussi une relation $\#$ de séparation pour une espèce X de la façon suivante :

1) $\neg x \# y \leftrightarrow x = y$ 2) $x \# y \rightarrow y \# x$ 3) $x \# y \rightarrow x \# z \vee z \# y$.

Les espèces seront donc des totalités ouvertes de propriétés bien définies et la notion de suite consiste justement en un procès qui associe à tout nombre naturel un objet mathématique qui appartient à une espèce X quelconque. Une suite est donc une application qui fait correspondre à tout nombre naturel un objet dont les propriétés sont les éléments d'une espèce donnée. Une application injective Φ est définie comme suit :

$$\forall x \in X \forall x' \in X \, (\Phi x = \Phi x' \rightarrow x = x') \, .$$

Les principes non constructifs de la théorie des ensembles, axiomes du choix et de compréhension, ont une version intuitionniste qui limite leur champ d'application aux espèces décidables, *i.e.*

$$\forall x \, (x \in X \vee x \notin X)$$

pour une totalité constructible. Pour l'axiome du choix, on a

$$\forall x \in X \; \exists y \in Y \; A \, (x, y) \rightarrow \exists \Phi \in X \, (Y) \, \forall x A \, (x, \Phi x)$$

où X et Y sont des espèces décidables, Φ une fonction de choix et $\Phi \in X \, (Y)$ signifie $\Phi : X \rightarrow Y$; pour l'axiome de compréhension, on a

$$\forall Y \; \exists x \in X \, (Y x \leftrightarrow F \, (x))$$

où Y est une variable de second ordre (pour les sous-espèces de X). La prédicativité ou l'imprédicativité dépend de la décidabilité des espèces concernées. Ici il y a place pour des versions plus ou moins constructives de ces principes non constructifs.

Il y a diverses notions de suites : suites régulières « *lawlike* », suites irrégulières « *lawless* », suites de choix « *choice sequences* » ou « *Wahlfolge* ».

Une suite régulière est simplement une suite dont le développement est déterminé par une loi ou une règle (un algorithme), *e.g.* les fonctions récursives primitives — par exemple, la fonction de successeur. Une suite irrégulière est le pôle négatif d'une suite régulière ; elle est définie par un développement sans loi, c'est-à-dire qu'à une étape donnée du développement, nous ne connaissons que les valeurs obtenues jusqu'à ce moment et rien du développement futur, *e.g.* une suite de coup de dés (cet exemple n'est pas tout à fait juste, puisqu'on ne peut en général identifier suite aléatoire et suite irrégulière). La définition d'une suite de choix est un peu plus complexe : on peut dire, en bref, que c'est une notion intermédiaire entre suite régulière et suite irrégulière. Une suite de choix α est une suite de valeurs librement choisies $x_0, x_1, \ldots$ qu'on peut déterminer en introduisant une nouvelle suite de choix α_0 en définissant

$$\alpha = \Gamma_0 \alpha_0$$

pour laquelle Γ_0 est un opérateur continu ; on peut déterminer α encore en définissant après un certain temps

$$\alpha_0 = \Gamma_1 \alpha_1$$

et ainsi de suite.

Pour l'analyse fondée sur les suites régulières, on introduit les nombres réels à l'aide des suites fondamentales ou des suites de Cauchy de nombres rationnels : une suite de rationnels $\langle r_n \rangle_n$ est un générateur de nombres réels si

$$\forall k \exists n \forall m \left(|r_n - r_{n+m}| \prec 2^{-k} \right)$$

où $|r_n - r_{n+m}|$ exprime la différence ou la distance entre deux nombres rationnels, distance qui doit être inférieure à $\frac{1}{2}^k$, pour k un nombre naturel donné. Une suite régulière de réels $\langle x_n \rangle_n$ engendrée par une suite de rationnels $\langle r_n \rangle_n$ est une suite de Cauchy si

$$\forall k \exists n \forall m \left(|x_{n+m} - x_n| \prec 2^{-k} \right)$$

et converge si

$$\forall k \vee \exists n \forall m \left(|x - x_{n+m}| \prec 2^{-k} \right)$$

avec x pour limite ; on obtient alors le théorème classique : "Toute suite de Cauchy est convergente". On définit la continuité uniforme d'une manière analogue aux définitions classiques : une fonction de variables réelles est continue si

$$\forall k \forall x \exists m \exists y \left(|x - y| \prec 2^{-m} \rightarrow \left| fx - fy \prec 2^{-k} \right| \right)$$

et symétriquement pour la continuité uniforme

$$\forall k \vee \exists m \forall x \forall y \left(|x - y| \prec 2^{-m} \rightarrow |fx - fy| \prec 2^{-k} \right)$$

à comparer avec la définition classique pour des réels non négatifs δ et ε

$$\forall \varepsilon \succ 0, \exists \delta \succ 0 \forall x \forall y \, |x - y| \prec \delta \rightarrow |fx - fy| \prec \varepsilon.$$

On peut déjà produire des contre-exemples intuitionnistes pour des théorèmes classiques : *e.g.* on ne peut avoir pour les réels x

$$\forall x \left(x = 0 \vee x \neq 0 \right).$$

Prenons l'expansion décimale de π (qui est régulière — $\pi_m (n)$ signifie que n est le nombre de la dernière décimale de la $n$ième suite de dix chiffres 7 consécutifs dans l'expansion décimale de π. On sait que

$$\exists n \pi_1 n \vee \neg \exists n \pi_1 n$$

est encore indécidable puisqu'on n'a pas encore produit une seule suite de dix 7 consécutifs. Définissons un générateur de nombre réel $\langle r_m \rangle_m$ par

$$\begin{array}{c} \neg \exists n \leq m \left(\pi_1 n \right) \rightarrow r_m = 0 \\ \pi_1 n \forall n \leq m \rightarrow r_m = 2^{-n}; \end{array}$$

$\langle r_m \rangle_m$ est un générateur de nombre réel régulier qui définit le nombre réel x_0 : il n'est pas possible de décider

$$x_0 = 0 \vee x_0 \neq 0$$

puisque

$$x_0 = 0 \rightarrow \neg \exists n \left(\pi_1 n \right)$$

d'où

$$(x_0 = 0 \vee x_0 \neq 0) \leftrightarrow \exists n \pi_1 n \vee \neg \exists n \pi_1 n.$$

De la même façon, on ne peut affirmer que toute fonction uniformément continue sur l'intervalle $[0, 1]$ possède un élément maximal. Ces contre-exemples découlent directement du rejet du tiers exclu et de l'accent mis sur la décidabilité et la solubilité (constructive) des assertions mathématiques. Mais les théories des suites irrégulières et des suites de choix nous permettent d'aller plus loin dans la critique et la reconstruction intuitionniste des mathématiques classiques.

2. Suites irrégulières (ou absolument libres)

Les suites irrégulières ont été étudiées surtout par Kreisel. Un premier principe pour les suites irrégulières peut s'énoncer

1) $\forall n \exists \alpha \, (\alpha \in n)$

pour α une suite irrégulière et n un segment initial — un segment initial est une séquence finie de valeurs $\alpha_0, \ldots, \alpha \, (j_1 n - 1)$ où $j_1 n$ indique la longueur du segment initial. Ce premier principe affirme qu'il existe des suites irrégulières avec des segments initiaux arbitraires.

Un second principe donne l'égalité intensionnelle

2) $\forall \alpha \forall \beta \, (\alpha = \beta \vee \neg \alpha = \beta)$.

Le principe suivant est plus riche

3) $\forall \alpha \forall \alpha_1 \ldots \forall \alpha_p \forall X \, [\neq (\alpha, \alpha_1, \ldots, \alpha_p) \wedge X \, (\alpha, \alpha_1, \ldots, \alpha_p)$
$\rightarrow \forall n \, (\alpha \in n \wedge \forall \beta \in n \, (\neq (\beta, \alpha_1, \ldots, \alpha_p) \rightarrow X \, (\beta, \alpha_1, \ldots, \alpha_p)))]$

où $\neq (\alpha, \alpha_1, \ldots, \alpha_p)$ signifie que toutes les valeurs de α sont différentes de α. Le principe signifie qu'un prédicat ou une propriété X attribuée à une suite irrégulière α ne peut être attribuée à une autre suite irrégulière β que si cette dernière possède le même segment initial de valeurs. Un théorème facile à dériver de ce principe est le suivant

$$\vdash \forall \alpha \forall \beta \, [\alpha = \beta \leftrightarrow \forall x \, (\alpha x = \beta x)] \, .$$

On peut maintenant définir des fonctionnelles (ou des métasuites) sur les suites irrégulières, qui, en vertu de l'égalité intensionnelle que nous avons

définie plus haut, doivent être continues

$$\Gamma\alpha = x \leftrightarrow \exists n\,(\alpha \in n\,(\Gamma\beta = x))\,.$$

Le quatrième principe énonce plus fortement la propriété de continuité pour les fonctionnelles sur les suites irrégulières

4) $\forall X \forall \alpha \forall \alpha_1 \ldots \forall \alpha_p\,(\neq(\alpha, \alpha_1, \ldots, \alpha_p) \rightarrow \exists x X\,(x, \alpha_1, \ldots, \alpha_p))$
$\rightarrow \exists e \in K \forall \alpha_1 \ldots \forall \alpha_p\,(\neq(\alpha_1, \ldots, \alpha_p) \rightarrow X\,(e\,(\nu_p\,(\alpha_1, \ldots, \alpha_p))\,, \alpha_1, \ldots, \alpha_p))$
où K désigne la classe des fonctionnelles (constructives) continues et ν_p une énumération de $\langle \alpha_1, \ldots, \alpha_p \rangle$. Comme cas spécial de ce principe, on a

$$\forall X\,[\forall \alpha \exists x X\,(\alpha, x) \rightarrow \forall e \exists \alpha X\,(\alpha, e\,(\alpha))]\,.$$

On peut dégager la signification de ce principe en disant que si on peut trouver un objet x qui a les mêmes propriétés X que α pour les valeurs $\alpha_1, \ldots, \alpha_p$, on peut trouver une fonctionnelle constructive qui énumère les valeurs $\alpha_1, \ldots, \alpha_p$ ayant les mêmes propriétés.

Finalement, un théorème général dû à Brouwer permet de formuler un principe d'induction pour les nombres naturels : c'est le théorème de la barre « *bar-theorem* »

$$\forall \alpha \exists x X(\hat{a}x) \wedge \forall n(Xn \rightarrow \forall n \forall m(Xn \rightarrow Xn * m)) \wedge$$

$$\forall n \forall x Y(n * \breve{x}) \rightarrow \forall n Y n$$

où $\hat{a}$ signifie le segment initial de α et $*$ l'opération de concaténation ($\breve{x}$ est le singleton $\langle x \rangle$). En mots, le théorème signifie que "si une propriété est vraie pour toute suite habitée (par des valeurs initiales) et est vraie de α, si elle est vraie de $\alpha * \langle n \rangle$ pour tout n, alors elle est vraie pour toute suite dans S (le déploiement universel)". On voit donc la proche parenté de ce théorème avec le postulat d'induction (classique) de Peano — la preuve elle-même repose essentiellement sur l'induction, *i.e.* l'induction "barrée".

Il semble y avoir deux usages principaux pour les suites irrégulières : en premier lieu, elles servent à définir une classe de fonctions constructives qui n'apparaît pas réductible à la classe des fonctions récursives, ce qui met en question la thèse de Church qui affirme que les fonctions mécaniquement computables correspondent exactement aux fonctions récursives ; elles servent aussi à réfuter certains principes de la logique classique, dont ceux-ci

1) $\vdash \neg \forall \alpha \vee \exists x\,(\alpha x = 0)$

2) $\vdash \forall\alpha\neg\neg\exists x\,(\alpha x = 0)$
3) $\vdash \neg\forall\alpha\,(\exists x\,(\alpha x = 0) \vee \neg\exists x\,(\alpha x = 0))$
4) $\vdash \neg\,(\exists\alpha\neg\neg\exists x\,(\alpha = 0) \rightarrow \neg\neg\forall\alpha\exists x\,(\alpha x = 0))$
5) $\vdash \neg\exists\alpha\,(\neg\neg\exists x\,(\alpha x = 0) \rightarrow \exists x\,(\alpha x = 0))$.

Le théorème 2 réfute le principe du tiers exclu : supposons que nous ayons $\neg\exists x\,(\alpha x = 0)$. En vertu des principes déjà énoncés (les trois premiers principes pour les suites régulières), on a

$$\neg\exists x\,(\alpha x = 0) \leftrightarrow \exists n\,(\alpha \in n \wedge \forall\beta \in n\neg\exists x\,(\beta x = 0))$$

où n est, comme auparavant, un segment initial ; puisqu'il est toujours possible de trouver un $\beta \in n$ tel que $\beta x = 0$, on doit donc affirmer

$$\neg\neg\exists x\,(\alpha x = 0)\,.$$

Le théorème 5 réfute le principe de Markov qui permet de passer de la double négation à l'affirmation — à strictement parler, le principe de Markov ne s'applique qu'aux fonctions régulières, mais il est intéressant de voir que ce ne peut être un principe universel.

Brouwer a esquissé une théorie du sujet créateur ou constructeur pour supporter l'édifice des mathématiques intuitionnistes ; la théorie a ensuite été élaborée par Kreisel, mais elle a fait intervenir trop de notions ou d'axiomes extramathématiques et semble asservie à des motifs philosophiques que certains associent à la phénoménologie husserlienne. Le subjectivisme de la théorie brouwerienne réintègrerait ainsi une philosophie transcendantale n'ayant plus la pertinence critique du constructivisme kroneckerien qui demeure intramathématique. La vocation fondationnelle de l'intuitionnisme doit se limiter à des principes constructivistes qui régissent l'activité mathématique ou logicomathématique. Que Brouwer et ses successeurs ne se soient pas toujours tenus à la stricte observance de ces principes, c'est là une question de principe que j'analyse dans l'Annexe A du présent ouvrage.

3.5 Skolem

Skolem comme Herbrand a pensé l'arithmétique sous le mode récursif, c'est-à-dire en termes des opérations élémentaires itérées indéfiniment, et il s'est ouvertement réclamé de Kronecker et de son constructivisme finitiste (voir Skolem [94]). Skolem est sans doute le premier à définir rigoureusement

les fonctions récursives primitives dans un langage qui ne recourt pas aux quantificateurs ou aux domaines infinis où se logent les variables liées de la quantification sur l'ensemble infini des nombres naturels. Comme Herbrand, Skolem avait une première expérience de praticien en théorie des nombres — dans son cas les équations diophantiennes — et comme Herbrand encore il s'inspire de principes intuitionnistes, le rejet du tiers exclu au-delà des fonctions récursives primitives. Les fonctions récursives primitives sont celles qui ne font pas appel au principe du plus petit nombre μ qui n'a pas de signification proprement constructive. Les fonctions d'addition $a + b$, multiplication $a \cdot b$, la relation de divisibilité que Skolem définit comme

$$D(a, b) = \sum_x (a = bx)$$

et qu'il prend la peine de limiter à un domaine fini d'application, à la manière d'un algorithme euclidien qui couvre les notions de plus grand diviseur commun et de plus petit multiple commun. Skolem consacre un long développement à la notion de nombre premier et à la définition d'un plus petit nombre pour lequel une certaine proposition P est vraie mais sans lier (sans variables liées) cette vérité à un domaine infini où règne la quantification universelle : il est toujours décidable si $P(x)$ est vraie ou non pour un x arbitraire. C'est ce que Skolem appelle une fonction descriptive qui ne convoque pas l'infini actuel, ce qui n'est pas un défaut, puisque nous travaillons toujours en pratique avec des entiers positifs dont nous avons construit préalablement un exemplaire ou une instantiation n. La même chose vaut pour la cardinalité où nous utilisons une fonction (une application) finie pour définir le cardinal ou le nombre d'une classe d'éléments finis que nous pouvons ensuite élargir en une définition générale de la notion de cardinalité pour les classes d'objets. Skolem conclut son texte en disant qu'il doute qu'on puisse trouver une justification pour l'infini actuel ou le transfini et il réitère son adhésion à un point de vue finitiste cohérent et conforme au principe kroneckerien de la définition ou détermination « *Bestimmung* » des concepts mathématiques : une telle détermination, qu'on peut identifier à un algorithme, est une procédure qui doit s'effectuer en un nombre fini d'essais. C'est là tout le sens du finitisme kroneckerien, comme l'a défini Hensel dans son introduction aux *Vorlesungen über Zahlentheorie* de Kronecker.

3.6 L'arithmétisation de la syntaxe (du système formel)

Après Skolem et Herbrand qui ont voulu « réduire » les *Principia Mathematica* de Russell et Whitehead, Gödel qui avait pourtant des motifs intuitionnistes – il les exploitera plus tard – revient à l'arithmétique « classique » de Peano qu'il veut coucher dans une théorie arithmétique fondamentale, la théorie des fonctions récursives. Mais cette théorie, qui a des racines dans l'arithmétisation de l'analyse, notamment chez Dedekind, et l'arithmétisation de l'algèbre, la théorie des formes ou polynômes homogènes de Kronecker, avait éveillé des échos constructifs chez Herbrand et Skolem. Gödel voudra lui donner son plein essor dans l'arithmétique ensembliste de Peano et il devra en masquer les aspects constructifs dans son premier théorème d'incomplétude. Il importe de suivre ici la démarche de Gödel qui représente une étape décisive dans l'arithmétisation de la logique.

3.6.1 Gödel

Nous commençons par décrire le système formel S_2 de l'arithmétique. Nous savons que ce système était fondé sur les postulats de Peano. On a la structure suivante pour la théorie de l'arithmétique (désignée par T_2) :

$$S_2 = \langle \mathbb{N}, 0, S, =, +, \cdot \rangle$$

où $\mathbb{N}$, l'ensemble des nombres naturels, constitue l'univers de la structure, 0 le nombre zéro '0', S une fonction monadique qui signifie 'successeur de', $=$ une relation dyadique d'identité, $+$ et $\cdot$ des fonctions dyadiques qui expriment l'addition et la multiplication. Il va sans dire que les axiomes logiques (toute la syntaxe) des théories du premier ordre sont présents dans le système formel S_2 de l'arithmétique.

Les axiomes suivants sont suffisants pour caractériser axiomatiquement T_2.

1) $\forall x(x = x)$ et $\forall x\ \forall y\ ((x = y) \supset (A(x, x) \supset A(x, y)))$
2) $\forall x(Sx \neq 0)$
3) $\forall x\ \forall y(Sx = Sy \supset x = y)$
4) $\forall x\ \exists y(x = 0 \vee x = Sy)$
5) $\forall x(x + 0 = x)$

6) $\forall x\, \forall y\, (S(x+y) = x + Sy)$
7) $\forall x(x \cdot 0 = 0)$
8) $\forall x\, \forall y\, (x \cdot Sy = (x \cdot y) + x)$
9) $\forall x\, \forall y\, \forall z\, (x = y \supset (x = y \supset y = z))$
10) $\forall x_1, \ldots, \forall x_n\, [(a(0) \wedge \forall x\, (A(x) \supset A(Sx))) \supset \forall x A(x)]$ pour toute fbf $A(x)$ de S_2 ayant les variables libres $x, x_1, \ldots, x_n$.

À l'aide de ces axiomes, il est facile de démontrer tous les théorèmes de l'arithmétique concernant l'égalité, l'addition et la multiplication ; la même chose vaut pour une relation d'ordre ou une opération d'exponentiation qu'on peut définir à partir du langage déjà donné. Notons de nouveau ici que la formulation originale du postulat d'induction chez Peano (dans [88]) est au second ordre. Comme Peano le confesse, cette formulation est directement inspirée de Dedekind dans [20]. Dans cet ouvrage, Dedekind définit une notion de système Σ (multiplicité ou ensemble) qui a pour membres des choses (*Dinge*) qu'on peut ordonner en chaînes (*Kette*). Les nombres naturels constituent une telle chaîne A_0 ; tout élément de A_0 a une image par la fonction $\phi : s \to s'$ et la quantification universelle opère sur toutes les propriétés ou sous-ensembles de Σ. L'ensemble des nombres naturels est un ensemble infini, puisqu'il est en bijection avec l'un de ses sous-ensembles propres (e.g. l'ensemble des nombres pairs out l'ensemble des nombres impairs). Dans ce contexte, on peut bien parler de l'arithmétique de Dedekind-Peano. Pour les besoins de la logique classique, le postulat d'induction est formulé au premier ordre.

Remarquons que l'on peut obtenir la consistance ou l'autoconsistance pour un système plus simple, sans postulat de Peano, l'arithmétique de Robinson Q. Cette arithmétique est définie par les axiomes suivants (d'après Nelson [85]) :
1) $Sx \neq 0$
2) $Sx = Sy \to x = y$
3) $x + 0 = x$
4) $x + Sy = S(x + y)$
5) $x \cdot 0 = 0$
6) $x \cdot Sy = x \cdot y + x$
7) $Px = y \leftrightarrow Sy = x \vee (x = 0 \wedge y = 0)$.
On peut ajouter ici des axiomes pour l'associativité et la commutativité de l'addition et de la multiplication et la distributivité de la multiplication. L'axiome 7 définit la notion de prédécesseur. Cette théorie Q est ouverte

(ses axiomes n'ont pas de quantificateur) ; elle est consistante par le théorème de Hilbert-Ackermann : une théorie ouverte est inconsistante, ssi il y a une quasi-tautologie (une quasi-tautologie est une conséquence tautologique d'instances des axiomes d'identité et d'égalité) qui est une disjonction de négations d'instances des axiomes propres de la théorie (d'après Shoenfield [93]). Ce système est consistant et la preuve est finitaire, *i.e.* ne fait pas appel à la notion d'ensemble infini, comme l'exige le postulat d'induction de Peano. Gentzen a produit une preuve non finitaire de l'arithmétique de Peano en recourant à l'induction transfinie sur les ω jusqu'à ϵ_0. Cette arithmétique n'est pas prédicative, au sens où elle fait appel à l'ensemble des nombres naturels et à la quantification universelle ou quantification sur la suite infinie des nombres naturels. Une arithmétique prédicative n'utilise que la quantification bornée, ce qui suppose que les opérations arithmétiques sont limitées au domaine fini ou par extension, au domaine dénombrable. L'intérêt d'une telle théorie est fondationnel, c'est-à-dire qu'il touche à la fois à la logique et aux mathématiques et à la justification philosophique de la démarche logico-mathématique. Mais nous devons limiter notre étude ici au système formel S_2, puisque nous exposons la métathéorie (classique) de la logique classique et de l'arithmétique de Peano.

Dans la démonstration du théorème d'incomplétude de Gödel, il est essentiel de montrer qu'une certaine classe de fonctions arithmétiques, les fonctions récursives, sont représentables dans S_2. Définissons cinq cas de fonctions :
1) la fonction successeur ;

$$\forall x(Sx = x + 1)$$

2) les fonctions constantes, dont la fonction zéro

$$\forall x(Zx = 0)$$

3) les fonctions d'identité

$$\forall \vec{x} I_i^n(\vec{x}) = x_i \text{ ayant } n \text{ variables}$$

(la notation vectorielle $\vec{x}$ tient lieu de $(x_1, ..., x_n)$)
4) les fonctions obtenues par substitution (ou composition)

$$f(x, y) = g\,(x, h\,(y)) \text{ et } f(\vec{x}) = g\,(h_m(\vec{x}_n))$$

où g a originellement y_m pour variables auxquelles on substitue $h_1(\vec{x})$ et $h_m(\vec{x})$;

5) les fonctions obtenues par récursion

$$f(\vec{x}, 0) = g(\vec{x})$$

$$f(\vec{x}, y + 1) = h(\vec{x}, y, f(\vec{x}, y))$$

où g est une fonction à n variables ; la fonction f à $n + 1$ variables définie de cette façon est unique. Si l'on prend une fonction à zéro variable $f(0) = m$, alors m est un entier fixe. La fonction f est obtenue ici des fonctions g et h par récursion. Les trois premiers cas de fonctions sont des fonctions dites initiales. Une fonction est récursive primitive, si on peut l'obtenir des fonctions initiales par substitution ou par récursion ; elle est récursive générale ou simplement récursive, si l'on ajoute le cas suivant :
6) les fonctions obtenues par l'opérateur μ

$$f(\vec{x}) = \mu y(g(\vec{x}, y) = 0)$$

où μy signifie 'le plus petit nombre y tel que' ; l'équation veut donc dire que pour toute variable $\vec{x}$, il y a au moins un y tel que $g(\vec{x}, y) = 0$.

Une fois définies les fonctions récursives primitives et les fonctions récursives (générales), il faut montrer que les fonctions récursives constituent l'ensemble des fonctions représentables dans S_2 : indiquons d'abord comment toute fonction récursive est représentable dans S_2, mais il important de définir auparavant l'extension des fonctions récursives.

Disons, pour faire court, que si une fonction possède une définition descriptive (l'inverse d'une 'description définie', en quelque sorte), c'est-à-dire, une définition qui n'utilise que des symboles déjà définis dans le second membre d'une équation comme dans :

$$f(\vec{x}) = g(h_1(\vec{x}), \ldots, h_m(\vec{x}))$$

où l'on ne se sert que de variables et de symboles pour les fonctions récursives et d'opérateurs μ, alors elle est récursive. Il est clair que les fonctions initiales sont récursives et on démontre que l'on peut obtenir les autres fonctions récursives par induction sur les fonctions récursives, *e.g.* les fonctions de somme, de produit, différence, etc.

On peut aussi montrer que les fonctions qu'on obtient de relations récursives en limitant l'opérateur μ ou les quantificateurs universel et existentiel sont aussi récursives : l'opérateur μ ainsi limité

$$\mu y_{y \prec v} f(\vec{x}, y)$$

signifie le plus petit y plus petit que v, alors que les quantificateurs limités $\forall y_{y \prec v}$ ou $\exists y_{y \prec v}$ signifient que la quantification est limitée aux y plus petits que v. Donnons un exemple (mathématique) : tout nombre entier — positif — peut s'écrire de façon unique comme produit de facteurs premiers *e.g.* $220 = 2^2 \times 5 \times 11$, c'est le théorème fondamental de l'arithmétique, formellement

$$\forall x(x = n_0^{a_0} \times n_1^{a_1} \times \ldots \times n_r^{a_r})$$

Si l'on désigne par x_i le facteur n_i et si l'on définit

$$f(x) = \begin{cases} 1, \text{ ssi pour tous les } i,\ x_i = 1 \\ 0, \text{ ssi pour tous un } i \text{ quelconque},\ x_i = 0 \end{cases}$$

alors la fonction $f(x)$ est récursive primitive.

Donnons un autre exemple, pour plus de clarté : nous avons le dernier théorème de Fermat qui s'exprime

$$\forall n > 2\ \forall x\ \forall y\ \forall z(x^n + y^n \neq z^n)$$

pour n, x, y, z des entiers ; la fonction

$$f(x) = \begin{cases} 1, \text{ ssi le théorème de Fermat est vrai} \\ 0, \text{ ssi le théorème de Fermat est faux} \end{cases}$$

est récursive primitive – on sait maintenant qu'il est vrai par la preuve de Wiles (1995) !

Le théorème de représentabilité énonce simplement que 'Toute fonction récursive est représentable dans S_2' — voir Mendelson [82] pour un exposé détaillé. Pour obtenir les fonctions récursives par récursion, il suffit de procéder inductivement. Il faut pouvoir représenter les formules portant sur les suites finies de nombres naturels pour s'assurer que l'addition, la multiplication (et l'exponentiation) sont représentables dans S_2. Nous devons assigner un nombre à chaque suite finie de nombres naturels de telle sorte que les fonctions et prédicats associés soient récursifs et nous avons alors besoin de la fonction β de Gödel définie par

$$\beta(a, i)_i \text{ pour } \forall i \leq n$$

pour toute suite finie de nombres naturels $a_0, \ldots, a_n$ et pour tous les nombres naturels n.

Ainsi

$$\beta(a,i)_i \leq a \text{ div } 1$$

entraîne que

$$\beta(0,1) = 0$$

et

$$\beta(a,i) \prec a \text{ pour } a \neq 0.$$

La fonction β est une fonction de décomposition qui peut servir à exprimer la notion de reste ; par exemple, $\beta(a_0, a_1, i) =$ le reste dans

$$a_0 \text{ div } [1 + (i+1) \cdot a_1].$$

β est une fonction récursive primitive. Une fonction de décomposition correspond à un encodage de suites (pour l'exponentiation). Voyons encore une autre méthode plus générale pour encoder des suites finies de nombres naturels. Nous avons besoin des relations suivantes pour la suite : la relation $\text{div}(a,b)$ signifie que b divise a

$$\exists x(a = b \cdot x)$$

et la relation $rp(a,b)$ signifie si b divise ax pour tous les x, alors il divise x

$$\forall x(\text{div } (ax,b) \rightarrow \text{ div } (x,b)) \text{pour } x, b \neq 0$$

pour des nombres relativement premiers. Enfin la relation $rpp(a_i, b_j)$ pour tous les i, j et $(a_i, b_j) = 1$ pour des nombres relativement premiers en paires signifie qu'il n'y a pas de diviseur premier commun pour $i \neq j$ ou que 1 est leur seul diviseur premier commun. Remarquons que la notion de nombres relativement premiers en paires n'est pas la même chose que la notion de nombres premiers jumeaux (comme $\{5,7\}$, $\{11,13\}$, $\{17,19\}$, etc.) dont on ne sait pas encore s'il y en a une infinité. Nous obtenons alors le théorème du reste chinois dû à Sun Tsu (1er siècle) : il y a un nombre x qui est divisible par tous les a_i et par aucun b. L'idée est de réduire une congruence modulo a_i à un système de congruences plus simples ; une congruence est simplement définie par la relation

$$a \equiv b(m)$$

pour $a, b, m \in \mathbb{Z}$ (l'anneau des entiers) et signifie que a est congruent à b modulo m, si a et b ont le même reste quand on les divise par m ou si m divise $b - a$. Le système de congruences en question est

$$x \equiv b_1(m_1),\ x \equiv b_2(m_2),\ \ldots,\ x \equiv b_t(m_t) \text{ pour } m_1, m_2, \ldots, m_t = m$$

ce système est soluble et ses solutions diffèrent deux à deux par un multiple de m. En d'autres mots, pour les entiers positifs $m_1, \ldots, m_k$ relativement premiers en paires, les congruences

$$x \equiv b_1(m_1),\ \ldots,\ x \equiv b_k(m_k)$$

ont une solution unique modulo $m_1 \times \ldots \times m_k$.

Preuve : Soit $n_i = \frac{m}{m_i}$; nous avons $(m_i, n_i) = 1$, puisque ce sont des nombres relativement premiers en paires — ainsi y a-t-il des entiers r_i et s_i tels que $r_i m_i + s_i n_i = 1$. Posons $e_i = s_i n_i$, nous avons alors $e_i \equiv 1(m_i)$ et $e_i \equiv 0(m_j)$ pour $j \neq i$. Soit maintenant $x_0 = \sum_{i=1}^{t} b_i e_i$.

Nous avons alors $x_0 \equiv b_i e_i\,(m_i)$ et donc $x_0 \equiv b_i\,(m_i)$ qui constitue une solution de notre système de congruences. Supposons que x_i est une autre solution du système ; alors $x_1 - x_0 \equiv 0\,(m_i)$ pour $i = 1, 2, \ldots, t$. En d'autres mots, $m_1, m_2, \ldots, m_t$ divisent $x_1 - x_0$ et m divise $x_i - x_0$ (d'après Ireland et Rosen [65]).

La fonction β et le théorème du reste chinois (qui relève de la théorie des nombres) recourent à la notion de suite arbitraire de nombres naturels, *i.e.* font appel à une induction non bornée sur l'ensemble des nombres naturels et sont donc des concepts imprédicatifs qui atténuent le caractère constructif de la preuve de Gödel.

On peut utiliser une méthode plus constructive que la fonction β pour représenter les suites finies de nombres naturels. Soit $F_q[x]$ un corps fini (de nombres) avec q éléments où sont définis l'addition et la multiplication. Une suite finie d'entiers $(a_1, \ldots, a_n)$ peut être représentée par un polynôme de degré n

$$P(\bar{x}) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \quad (\text{ou} \quad P(\bar{x}) = \sum_{i=0}^{n} a_i x^i).$$

En recourant à la notion de polynôme réduit — dont le degré est plus petit que q — on obtient un monôme

$$M(\bar{x}) = a_i x_1^{i_1} a_i x_2^{i_2} \ldots a_i x_n^{i_n} \quad \text{avec} \ \sum(i_1, i_2, \ldots, i_n)$$

pour les variables x et les coefficients ou constantes a avec $n < q$ variables pour représenter la suite $(a_1, \ldots, a_n)$. On a alors un représentation polynomiale pour les suites finies de nombres naturels dans S_2 puisque tout polynôme dans $F_q[x]$ est équivalent à un polynôme réduit. Le caractère constructif

de cette interprétation vient du fait que la divisibilité est assurée par l'algorithme euclidien et que la descente infinie y opère naturellement dans le corps fini $F_q[x]$.

La méthode classique pour l'arithmétisation de la syntaxe consiste à assigner des nombres naturels (appelés nombres de Gödel) aux symboles et aux suites de symboles du système formel S_2. Cette assignation est effectivement calculable ; elle permet donc de formuler arithmétiquement des énoncés intrathéoriques et métathéoriques d'un système formel ; en plus, les énoncés arithmétiques ainsi obtenus seront de nature récursive et permettront ainsi de formuler un énoncé indécidable qui, en quelque sorte, dit de lui-même : 'Je ne suis pas un théorème de S_2' en vertu de la seule arithmétisation de la syntaxe (on voit ici la parenté avec la paradoxe du menteur d'Epiménide). On assigne des nombres de Gödel aux symboles et suites de symboles de S_2 de la façon suivante — nous présentons ici une façon parmi d'autres (celle de Mendelson [82]) : à chaque symbole, nous associons un nombre impair différent de 1, à chaque suite de symboles, nous associons un produit de facteurs premiers — qui correspond, comme nous l'avons vu, à un nombre entier unique. Ainsi, si P, Q, R ont pour nombres de Gödel correspondants $11, 13, 15$ la suite $\langle R, Q, P\rangle$ aura pour nombre

$$2^{15} \times 3^{13} \times 5^{11}.$$

On peut assigner de la même façon des nombres de Gödel à des suites de suites, *e.g.* si $e_1, e_2, \ldots, e_m$ sont des suites de symboles dont les nombres de Gödel sont $g_1, g_2, \ldots, g_m$, alors le nombre de Gödel de la suite $e_1, e_2, \ldots, e_m$ sera

$$2^{g_1} \times 3^{g_2} \times \ldots \times p_m^{g_m}$$

où p_m est le m-ième nombre premier (le nombre de Gödel d'une suite correspond donc à un entier unique par le théorème fondamental de l'arithmétique).

Il s'agit maintenant de montrer que les nombres de Gödel de différentes suites sont exprimés par des fonctions ou relations récursives.

Exemples :
1) $(= 3;\ ) = 5;\ ,= 7;\ \neg = 9;$
2) l'ensemble des nombres de Gödel des variables de S_2 ; cet ensemble est représenté par

$$[\exists z_{z \prec x}(1 \leq z \wedge x = 2^{5+8_z})]$$

où $\exists z_{z \prec x}$ est le quantificateur existentiel limité, $5 + 8_z$ $(z = 1, 2, \ldots)$ est le

nombre de Gödel de la variable x et 2^{5+8_z} le nombre de Gödel de la suite $\langle x \rangle$; nous avons donc une fonction récursive primitive ;
3) l'ensemble des nombres de Gödel des termes de S_2 ;
4) l'ensemble des nombres de Gödel des fbfs de S_2 ;
5) l'ensemble des nombres de Gödel des énoncés de S_2 ;
6) l'ensemble des nombres de Gödel des axiomes logiques de S_2.

Les autres clauses concernent les axiomes propres de substitution, d'identité, etc. Le plus important cependant, c'est que l'on ait des nombres de Gödel correspondant à des preuves dans S_2 ; ainsi, posons $A(\vec{x})$ une fbf déterminée de S_2 avec pour seules variables libres $\vec{x}$: posons encore que $Pr_A((\vec{x}, y)$ signifie que y est, dans S_2, le nombre de Gödel d'une preuve de $A(\bar{u}) - \bar{u}$; les u barrés sont des numéraux correspondant dans S_2 à des constantes substituées aux variables libres de $A(\vec{x})$; nous pouvons donc former

$$Pr_A(u, y)$$

où u est le nombre de Gödel d'une fbf $A(x_1)$ avec la seule variable libre x_1 et y le nombre de Gödel d'une preuve de $A(\bar{u})$. Cette relation est aussi récursive primitive. Nous voyons tout de suite que toutes ces relations et fonctions sont récursives primitives ou simplement récursives.

On arrive ainsi au théorème qui énonce que toute fonction $f(\vec{x})$ qui est représentable dans S_2 est récursive.

Preuve : Soit $A(\vec{x}, y)$ une fbf qui représente $f(\vec{x})$ et $\vec{p}$ des nombres naturels ; posons $f(\bar{p}) = v$, d'où $\vdash_{S_2} A(\bar{p}, \bar{v})$. Nous avons la formule $Pr_A((\bar{p}, v), y)$ où t est le nombre de Gödel d'une preuve dans S_2 de la formule $A(\bar{p}, \bar{v})$. La formule $Pr_A((\vec{x}, y), w)$ où y et w remplacent v et t est une relation récursive par

$$f(\vec{x}) = \mu y(Pr_A((\vec{x}, y), w)). \text{ C.Q.F.D.}$$

Le théorème couvre, bien entendu, les relations et les fonctions récursives.

On peut maintenant construire un énoncé indécidable dans S_2 par diagonalisation. On a vu que la relation $Pr_A((u), y)$ est récursive primitive ; Pr est représentée dans S_2 par la fbf $\underline{Pr}(\underline{x_1}, \underline{x_2})$. Prenons maintenant la formule $\forall \underline{x_2} \neg \underline{Pr}(\underline{x_1}, \underline{x_2})$ et prenons k comme nombre de Gödel de cette formule ; en substituant $\bar{k}$ à x_1 dans la formule, nous obtenons la fbf close ou l'énoncé

$$(*) \qquad \forall \underline{x_2} \neg \underline{Pr}(\bar{k}, \underline{x_2})$$

qui correspond à la relation $Pr((u), y)$. Cette formule dit en réalité qu'il n'y a pas de preuve, représentée par la variable x_2, de $\forall \underline{x_2} \neg \underline{Pr}(\bar{k}, \underline{x_2})$. Cette formule suppose le théorème du point fixe pour un énoncé k — le point fixe pour une fonction $f(x)$ est simplement $f(x) = x$

$$\vdash_{S_2} k \leftrightarrow A(\bar{k});$$

la formule $A(k)$ est obtenue en substituant dans $A(x_1)$ — qui n'a que la variable libre x_1 — le nombre de Gödel de l'énoncé k à x_1. Donc l'énoncé k dit indirectement de lui-même qu'il est vrai par l'équivalence entre l'énoncé et la formule qui exprime son nombre de Gödel. Ceci nous amène au théorème de Gödel [48] en deux parties :

1) Si S_2 est consistant, alors la fbf (*) n'est pas démontrable dans S_2.

La preuve est simple : supposons que S_2 est consistant et que $\forall \underline{x_2} \neg \underline{Pr}(\bar{k}, \underline{x_2})$. Prenons t comme le nombre de Gödel d'une preuve de cette fbf dans S_2 ; nous avons alors $\underline{Pr}(\underline{k}, \underline{t})$, d'où $\vdash_{S_2} \underline{Pr}(\bar{k}, \bar{t})$. Mais de $\forall x_2 \neg \underline{Pr}(\bar{k}, x_2)$, on tire par $E\forall$ (élimination du quantificateur universel) $\neg \underline{Pr}(\bar{k}, \bar{t})$. $\underline{Pr}(\bar{k}, \bar{t})$ et $\neg \underline{Pr}(\bar{k}, \bar{t})$ sont tous deux démontrables, d'où contradiction (puisque nous avons supposé S_2 consistant).

2) S_2 est ω-consistant, alors la négation de la fbf (*) n'est pas démontrable dans S_2.

Preuve : la ω-consistance signifie que pour toute fbf $A(x)$ et pour tous les nombres naturels n

$$\vdash_{S_2} A(\bar{n}) \rightarrow \nvdash_{S_2} \exists x \neg A(x)$$

Supposons d'abord $\neg$(*), c'est-à-dire

$$\vdash_{S_2} \neg \forall x_2 \neg Pr(\bar{k}, x_2), \quad (1)$$

j'obtiens alors

$$\vdash_{S_2} \exists x_2 Pr(\bar{k}, x_2) \quad (2)$$

mais par la consistance de S_2, j'ai

$$\nvdash_{S_2} \neg \forall x_2 \neg Pr(\bar{k}, x_2) \quad (3)$$

donc

$$\forall n(\vdash_{S_2} \neg Pr(\bar{k}, \bar{n}))$$

et par la ω-consistance de S_2, cela signifie que pour tous les nombres naturels n, n n'est pas le nombre de Gödel de (*), par conséquent

$$\nvdash_{S_2} \exists x_2 Pr(\bar{k}, x_2) \quad (4)$$

qui contredit (2). C.Q.F.D.

Ajoutons ici qu'une théorie ω-inconsistante n'est pas nécessairement inconsistante et qu'une théorie consistante peut être ω-inconsistante, bien qu'une théorie ω-consistante soit aussi consistante. La ω-incomplétude signifie que

$$\forall n(\vdash_{S_2} A(\bar{n}) \rightarrow \quad \nvdash_{S_2} \forall x Ax).$$

Une théorie consistante qui est ω-inconsistante est aussi ω-incomplète, une théorie ω-complète exigeant

$$\forall A \forall n \neg(\vdash_{S_2} A(\bar{n}) \ \wedge \ \nvdash_{S_2} \forall x Ax)$$

et l'ω-inconsistance supposant

$$\exists A \forall n \neg(\vdash_{S_2} A(\bar{n}) \ \rightarrow \ \vdash_{S_2} \exists x \neg Ax).$$

La consistance ω ou 1-consistance peut être réduite à la consistance tout court selon Rosser en utilisant cependant des itérations arbitraires de la règle ω qui suppose que l'on parcourt tous les nombres naturels pour les énoncés existentiels $\sum_1^0$ sur les nombres naturels, c'est-à-dire sur les relations primitives récursives définies pour tous les nombres naturels. Le (premier) théorème d'incomplétude de Gödel nous dit que tous les énoncés universels $(\prod_1^0)$ ne sont pas démontrables dans S_2. En supposant que S_2 est consistant, nous avons le résultat d'incomplétude qui nous assure qu'il y a au moins un énoncé (autoréférentiel) qui n'est pas démontrable, pas plus que sa négation d'ailleurs ; nous avons donc là un énoncé indécidable dans S_2. L'énoncé indécidable en question peut être ajouté à une extension S_2^+ de S_2 et devenir décidable, si l'on suppose la consistance ω puisqu'on peut ajouter l'énoncé indécidable ou sa négation comme axiome dans un système plus fort, comme Gödel le remarque en 1931. La procédure est cependant transfinie et suppose que l'ensemble des nombres naturels est une totalité infinie achevée par la quantification universelle de la consistance ω ou de la règle ω qui correspond

à l'induction infinie sur les nombres naturels et à l'induction transfinie sur les ordinaux. On voit dès lors que la procédure repose sur la décidabilité de tous les énoncés du système formel de l'arithmétique, une autre hypothèse qui est propre à la logique classique.

La formulation de Rosser [89] intègre l'énumérabilité récursive, concept dû à Church, pour générer une extension S_k de S_2 avec les énoncés suivants :

$$(\#) \quad \forall x_2 \left(Pr_1 \left(x_1, x_2\right) \supset \exists x_3 \left(x_3 \leq x_2 \wedge Pr_2 \left(x_1, x_3\right)\right)\right)$$

et

$$(\#\#) \quad \forall x_2 \left(Pr_1 \left(\bar{k}, x_2\right) \supset \exists x_3 \left(x_3 \leq x_2 \wedge Pr_2 \left(\bar{k}, x_3\right)\right)\right).$$

On a :

1) $Pr_1(k, y)$, ssi y est le nombre de Gödel d'un preuve de $(\#\#)$

ou

2) $Pr_2(k, y)$, ssi y est le nombre de Gödel d'un preuve de $\neg(\#\#)$.

Alors $Pr_1(k, y)$ est faux pour tous les nombres naturels y et j'ai

$$\vdash_{S_2} \neg Pr_1(\bar{k}, \bar{j})\forall j$$

et

$$\vdash_{S_2} \neg Pr_1(\bar{k}, \bar{0}) \wedge Pr_1(\bar{k}, \bar{1}) \wedge \ldots \wedge Pr_1(\bar{k}, \bar{r})$$

La consistance ω est réduite à la suite entière des nombres naturels dont on suppose qu'elle est récursivement énumérable, c'est-à-dire qu'elle a une longueur ω ...

L'énoncé (*) rappelle le paradoxe de Richard, comme le remarque Gödel lui-même. On peut reproduire la preuve en utilisant ce que j'appelle le nombre de Cantor (grand K). Le nombre de Cantor est le nombre diagonal

$$K = k_i = g_{i1} g_{i2} \ldots g_{ii}$$

pour la suite des nombres de Gödel des énoncés de S_2 que j'énumère ainsi

$$\begin{array}{rcl} k_1 & = & g_{11} g_{12} \ldots g_{1n} \\ k_2 & = & g_{21} g_{22} \ldots g_{2n} \\ & & \vdots \\ k_n & = & g_{n1} g_{n2} \ldots g_{nn} \end{array}$$

$K(= k_i)$ va donc être différent de tous les k. L'énoncé

$$(\#) \qquad \forall x_2 \neg Pr(\bar{K}, \underline{x_2})$$

est indémontrable dans S_2 et donc

$$\nvdash_{S_2} \exists k \ Pr((\bar{K}, k);$$

pour $\neg(\#)$, j'ai

$$\nvdash_{S_2} \forall x_2 \neg Pr(\bar{K}, x_2)$$

d'où

$$\vdash_{S_2} \exists k \ Pr(\bar{K}, k).$$

Mais $k \neq K$ pour tous les k, donc je ne peux avoir de théorème du point fixe

$$\vdash_{S_2} \underline{K} \leftrightarrow A(\bar{k})$$

et je conclus

$$\nvdash_{S_2} \exists k \ Pr(\bar{K}, k)$$

d'où contradiction. Dans S_2, le nombre de Cantor n'est équivalent à aucun nombre de Gödel

$$\forall k(k \neq K)$$

et on ne peut démontrer s'il est dénombrable ou non dénombrable, c'est l'énoncé indécidable. Ce résultat accentue encore l'incomplétude de l'arithmétique S_2, puisqu'on ne peut y démontrer que l'énoncé diagonal est décidable — s'il a un nombre de Gödel ou non. En d'autres termes, ce paradoxe évoque le paradoxe de Skolem, puisque à l'intérieur de S_2, $\bar{K}$ est non dénombrable (n'a pas de nombre de Gödel), mais vu du dehors, il doit avoir un nombre de Gödel inassignable du dedans. Il faut donc pour justifier la diagonalisation, chez Gödel comme chez Cantor, se situer au-delà des nombres naturels, dans l'univers transcendant du point de vue transfini (ou transarithmétique).

L'énoncé est vrai pour les nombres naturels, mais indémontrable dans S_2 : l'énoncé qui affirme pour tous les nombres naturels qu'il n'y a pas de preuve de lui-même est en fait indémontrable par le théorème de Gödel et est donc une assertion vraie, d'où l'incomplétude de S_2. On a bien

$$(\text{vrai}) \ \vDash \phi \ \leftrightarrow \nvdash \phi \ (\text{non prouvable})$$

puisque si l'énoncé indécidable dit « je n'ai pas de nombre de Gödel », il est vrai et si ce n'est pas le cas, c'est qu'il est faux et alors il a un nombre de Gödel (parce que décidable), donc

$$(\text{non vrai}) \ \nvDash \phi \ \leftrightarrow \vdash \phi \ (\text{prouvable})$$

d'où l'incomplétude, puisque

$$(\text{non vrai}) \ \nvDash \phi \ \leftrightarrow \nvdash \phi \ (\text{non prouvable})$$

ou plutôt

$$(\text{vrai}) \ \vDash \phi \ \nleftrightarrow \vdash \phi \ (\text{prouvable})$$

C'est là une assez curieuse situation, comme le dit Gödel dans son mémoire original. Le théorème de Gödel-Rosser affirme que toute extension axiomatisée consistante de S_2 est incomplète (*i.e.* contient un énoncé indécidable). On dit alors que S_2 est essentiellement incomplet ou n'est pas négacomplet — *i.e.* tout énoncé ou sa négation n'est pas un théorème. Remarquons qu'en vertu de la même incomplétude, on peut loger entre n et ω non seulement des énoncés indécidables, mais aussi des énoncés arithmétiques faux en plus des énoncés vrais qu'on loge dans le modèle sans qu'on puisse les démontrer dans le système formel.

Le second théorème d'incomplétude ou théorème sur les preuves de consistance de Gödel énonce que si S_2 est consistant, la fbf qui affirme cette consistance Cons_{S_2} n'est pas démontrable dans S_2, donc $\nvdash_{S_2} \text{Cons}_{S_2}$. En fait, le deuxième théorème d'incomplétude de Gödel suppose que

$$\vdash_{S_2} \text{Cons}_{S_2} \rightarrow (*)$$

mais (*) n'est pas démontrable, donc

$$\vdash_{S_2} \text{Cons}_{S_2} \rightarrow (*)$$

est un énoncé faux. Par ailleurs, si S_2 est inconsistant

$$\vdash_{S_2} \text{Cons}_{S_2} \rightarrow (*)$$

est un énoncé vrai, donc

$$\nvdash_{S_2} \text{Cons}_{S_2}.$$

Un des résultats les plus importants dans ce contexte est le théorème de Paris-Harrington sur un énoncé arithmétique, et non logique comme celui de

Gödel, qui est indécidable dans l'arithmétique de Peano. On montre qu'une extension simple du théorème de Ramsey fini

$$\alpha \to (k)^i_r$$

pour un ensemble M de cardinalité α où k est assez grand n'est pas démontrable dans l'arithmétique de Peano. L'énoncé est combinatoire puisqu'il porte sur les partitions ou sous-ensembles de M à i éléments qu'on répartit en r classes disjointes et qu'on entasse dans un sous-ensemble homogène k (de cardinalité $\bar{\bar{k}}$ relativement grande) mais la preuve utilise la version infinitaire du théorème de Ramsey et est analogue par là à la consistance ω utilisée par Gödel). G. Chaitin a d'autre part obtenu une généralisation (optimale !) du premier théorème d'incomplétude de Gödel en définissant un nombre réel Ω qui représente la probabilité qu'un programme quelconque s'arrête — nous invoquerons plus loin le problème de l'arrêt pour une machine de Turing. Le nombre Ω est un nombre aléatoire 'incompressible' : il est définissable par un algorithme, mais cet algorithme est indémontrable et il l'est de plus en plus ou entropiquement peut-on dire, puisque le nombre de bits (nombres digitaux binaires) qu'il faut pour le définir est ou devient plus grand exponentiellement que le nombre de bits du système formel qu'il faut pour le démontrer.

Feferman [28] a montré qu'il était possible de définir la consistance de S_2 dans S_2 sous certaines conditions ; mais il a reformulé le théorème de Gödel à l'aide de formules récursivement énumérables et a démontré que pour toute extension S_2' de S_2, $\nvdash_{S_2} \mathrm{Cons}_A$ pour A une formule récursivement énumérable qui exprime l'ensemble des nombres de Gödel des théorèmes de S_2. Remarquons encore que Gentzen [46] a donné une preuve de la consistance de l'arithmétique classique *i.e.* notre système S_2 en utilisant l'induction transfinie jusqu'à l'ordinal ε_0, limite de la suite des ω, *i.e.* $\lim\{\omega\} = \varepsilon_0$. Gentzen a fait correspondre des ordinaux aux dérivations pour les preuves de l'arithmétique et a pu montrer, dans son théorème dit de réduction, que toute preuve dans S_2 pouvait se réduire à une forme minimale. Il n'est pas clair cependant que l'induction transfinie jusqu'à ε_0 ait un caractère constructif et Gentzen n'a pu en fournir de justification convaincante. Notons finalement que Gödel a aussi proposé en 1958 une preuve de consistance de S_2, en utilisant des fonctionnelles (fonctions sur des fonctions) récursives primitives et l'induction sur tous les types finis et Spector a étendu cette preuve à l'analyse, mais le sens de ces constructions est loin d'être évident – voir pour ces

questions, en particulier la thèse de Church, mon ouvrage *Fondements des mathématiques* [31].

Terminons par l'énoncé de quelques résultats complémentaires : une théorie T est récursivement indécidable, ssi l'ensemble Th_t de ses théorèmes n'est pas récursif (un ensemble A est récursif, ssi A et son complément $\bar{A}$ — ici il est évident que la barre signifie la négation booléenne — sont récursivement énumérables, *i.e.* ou bien vides ou bien définis par une fonction récursive). Elle est essentiellement récursivement indécidable, ssi toutes ses extensions consistantes sont récursivement indécidables. T_2 est donc essentiellement *récursivement* indécidable. L'ensemble Thm_{S_2} des nombres de Gödel des théorèmes de S_2 n'est pas expressible dans S_2, si S_2 est consistant. Cela signifie qu'on ne peut faire mécaniquement la liste des théorèmes (et des non-théorèmes) de S_2 en vertu de la présence d'énoncés indécidables dans S_2, ce qui entraîne le fait que Thm_{S_2} n'est pas un ensemble récursif, bien que l'ensemble des nombres de Gödel des formules bien formées de calcul des prédicats de TP_1 soit récursif. Cela est une autre conséquence du fait que le système formel S_1 de TP_1 n'est pas négacomplet (pour les énoncés), pas plus qu'il n'est syntaxiquement complet, ce qui est l'équivalent de la négacomplétude pour les formules.

Le procédé de diagonalisation de Cantor permet de définir facilement une fonction g sur N^N distincte de toutes les fonctions calculables, donc une fonction qui n'est pas calculable : donnons-nous une énumération $f_0, f_1, f_2, \ldots$ de l'ensemble des fonctions f calculables et définissons par diagonalisation

$$g(n) = \begin{cases} 1, \text{ ssi } f_n(n) = 0 \\ 0, \text{ autrement} \end{cases}$$

Il est clair que g n'est pas calculable puisque si elle l'était, nous aurions pour un k arbitraire

$$g(k) = f_k(k)$$

mais

$$f_k(k) = 0, \text{ ssi } g(k) = 1$$

et

$$f_k(k) \neq 0, \text{ ssi } g(k) = 0$$

donc

$$g(k) \neq f_k(k).$$

La diagonalisation pour des prédicats unaires et binaires est encore plus explicite. Prenons Q unaire et P binaire : $P(a,b)$ est un prédicat binaire et $P(b)$ est unaire pour tous les b ; posons

$$P(b) = P(a,b).$$

Posons encore

$$Q(a) \leftrightarrow \neg P(a,a).$$

Alors Q est distinct de $P(b)$ pour tous les b.

Preuve : Si $Q = P(b)$, alors

$$P(b,b) \leftrightarrow P(b) \leftrightarrow Q(b) \leftrightarrow \neg P(b,b)$$

qui est une contradiction (voir Shoenfield [93]). On peut encore présenter la chose différemment : disons que m est autoréférentiel, si m est le nombre de Gödel d'une formule $F(x)$ et $F(\bar{m})$ est démontrable. Supposons que n est le nombre de Gödel d'une formule $G(x)$ qui énonce « x n'est pas autoréférentiel ». Si n est autoréférentiel, $G(\bar{n})$ est faux et démontrable, ce qui est impossible ; ainsi n n'est pas autoréférentiel et $G(\bar{n})$ est un énoncé vrai indémontrable (voir Boolos et Jeffrey [10]).

La thèse de Church stipule que les fonctions récursives correspondent aux fonctions effectivement calculables, mais la thèse n'est qu'une stipulation qui n'a pas encore été démontrée. La thèse de Church englobe plusieurs classes de fonctions effectivement calculables, les fonctions récursives de Herbrand-Gödel, les algorithmes de Markov, le calcul lambda de Church, les systèmes normaux de Post, les machines de Turing. Toutes ces classes sont équivalentes et nous nous intéresserons à la plus simple de ces classes, les machines de Turing qui représentent la computabilité de Turing.

3.6.2 Turing

Une machine de Turing est définie par les quatre spécifications suivantes :

1) un ruban perforé en cases — le ruban est la mémoire de la machine et elle est arbitrairement grande ou extensible ;

2) une tête lectrice capable de lire des symboles d'un ensemble fini de cases du ruban, de les effacer ou d'en écrire de nouveaux ;

3) la tête lectrice peut se déplacer d'une case à la fois, à droite ou à gauche ;

4) un ensemble fini d'états internes de la machine tel que les instructions (le programme), *e.g.* imprimer un dans la case vide immédiatement à droite (ou à gauche), sont déterminées par l'état interne de la machine et sa lecture des symboles à un moment donné.

La plupart des cases sont vides ; les autres contiennent un symbole tiré d'un alphabet fini, $S_1, \ldots, S_n$ (S_0 pour une case vide). La machine peut s'arrêter. Le problème de l'arrêt pour les machines de Turing consiste à spécifier une procédure systématique effective (un algorithme) pour calculer une fonction $h(m, n) = 1$, ssi la machine M ne s'arrête jamais, *i.e.* fait une boucle infinie, après son état initial, en commençant par lire le premier d'une suite de symboles 1 sur un ruban dont les autres cases sont vides. Le problème de l'arrêt est insoluble ou indécidable et il suffit d'un argument diagonal pour le montrer : supposons que la fonction h est calculée par une machine de Turing M_n, alors il y a une autre machine de Turing M_m qui s'arrête, ssi M_n ne s'arrête pas : il n'y a pas de semblable machine de Turing, puisqu'elle équivaut à une fonction g sur les nombres naturels

$$g\,(n) = \begin{cases} 1, \text{ ssi } h_n(n) = 0 \\ 0, \text{ autrement} \end{cases}$$

qui n'est pas calculable et ne peut donc être une machine de Turing. Remarquons qu'il existe des machines dites à accès aléatoire (non séquentielles) qui n'ont pas besoin d'une mémoire ou d'une capacité de stockage des données, mais se contentent d'une alimentation finie (codable dans un corps de nombres). La machine de Turing universelle est la machine qui simule toutes les autres machines de Turing.

Si l'on accepte la thèse de Church, le fait que S_2 soit récursivement indécidable signifie qu'il ne peut y avoir de méthode effective de décision pour S_2. Par ailleurs, le théorème de Church affirme que toute extension consistante de S_2 ne peut comporter de méthode de décision. Church a aussi montré qu'il n'y avait pas de méthode de décision pour la logique des prédicats du premier ordre et non plus pour la logique des prédicats du premier ordre ne comportant que des prédicats (sans constante et sans fonction). La preuve fait simplement intervenir le fait que l'ensemble des nombres de Gödel des théorèmes de la logique des prédicats du premier ordre n'est pas récursif puisqu'il s'agit toujours d'un ensemble A de formules vraies de cardinalité $\aleph_0$

et on montre que cet ensemble n'est pas récursif tout en étant récursivement énumérable — son complément $\bar{A}$, *i.e.*, $\aleph_0 - A$, ne l'est pas. Par ailleurs, la logique des prédicats monadiques du premier ordre est décidable. Finalement, un théorème de Tarski sur la vérité s'apparente de près au deuxième théorème d'incomplétude de Gödel. Le théorème de Tarski énonce qu'il n'y a pas de définition de la vérité de S_2 dans S_2. Pour le montrer, on n'a qu'à construire l'ensemble Vr_{S_2} des nombres de Gödel des énoncés vrais (ou logiquement valides) de S_2 équivalent à l'ensemble Th_{S_2} des nombres de Gödel des théorèmes de S_2 : $Vr_{S_2} = Thm_{S_2}$. Puisque Thm_{S_2} n'est pas récursif, comme on l'a vu, Vr_{S_2} ne l'est pas non plus. Il s'agit simplement d'appliquer la fonction g définie plus haut à l'ensemble récursivement énumérable des théorèmes de S_2 pour montrer que ce n'est pas un ensemble récursif ; on dit encore que Vr_{S_2} n'est pas arithmétique ou représentable (définissable) arithmétiquement. Remarquons que le théorème de Löb (1955) permet d'intégrer à S_2 tout énoncé de S_2 à l'aide d'un prédicat de prouvabilité : Si $Pr(y)$ est un prédicat de prouvabilité pour S_2, alors pour tout énoncé A, $\vdash_{S_2} Pr(\ulcorner A \urcorner)$ entraîne $\vdash_{S_2} A$. A est un théorème de S_2 ssi $(Pr(\ulcorner A \urcorner) \rightarrow A)$ est un théorème de S_2 ; $\ulcorner A \urcorner$ est le "nom" de A, *i.e.* son nombre de Gödel prédiqué par le prédicat de prouvabilité qui permet ainsi l'autoréférence pour un énoncé A qui affirme sa propre prouvabilité et est donc vrai. Mais la consistance de S_2 implique par le théorème de Tarski que S_2 ne contient pas son propre prédicat de vérité ou sa propre vérité par le deuxième théorème d'incomplétude de Gödel. La prouvabilité est ici un phénomène de réflexion, peut-on dire.

Vr_{S_2} n'est donc pas représentable. Le théorème de Tarski (1936) énonce que l'ensemble Vr_{S_2} n'est pas arithmétique, c'est-à-dire que l'ensemble des nombres de Gödel des formules vraies, *e.g.* les axiomes de S_2, ne peut être représenté par une formule vraie du modèle standard de l'arithmétique de Peano T_2. C'est l'équivalent sémantique de l'énoncé syntaxique pour l'incomplétude (sémantique) de S_2. De nouveau, nous avons ce jeu de miroirs entre la syntaxe et la sémantique en logique formelle classique. Si la syntaxe de l'arithmétique ensembliste de Peano nous dit qu'elle est incomplète, sa sémantique nous répète que la vérité de l'arithmétique lui échappe, c'est-à-dire qu'elle n'est pas définissable à l'intérieur de l'arithmétique (de Peano). Donc, le théorème de Tarski peut être formulé de la façon suivante : la vérité d'un système formel aussi fort que S_2 ne peut être représentée dans le même système (mais peut être représentée dans un système plus fort). C'est là l'origine de l'idée tarskienne des métalangages, que la sémantique va exploiter par la suite. Le métalangage diffère du langage-objet ; ce dernier parle

des objets alors que le métalangage parle du langage-objet et de ses propriétés. C'est ce que nous avons fait dans ce texte sur la métalogique. Si Tarski a défini la notion de métalangage pour les langages formels, la philosophie du langage lui a donné une extension que nous n'exploiterons pas ici. La métamathématique, comme Hilbert a appelé la théorie des démonstrations, n'est que le métalangage des théories mathématiques, de leur syntaxe (théorie des démonstrations) et de leur sémantique (théorie des modèles).

Par ailleurs, l'informatique traite l'information de manière automatique et le langage de l'ordinateur doit faire appel à la logique pour le traitement efficace, c'est-à-dire rapide et économique, de l'information, du simple calcul numérique aux systèmes experts où l'interaction avec l'utilisateur est l'enjeu essentiel. À l'origine, les langages informatiques n'avaient pour fonction que de coder l'information dans une langue logique.

Parmi ces langages, il y a PROLOG (*i.e.* programmation avec logique) qui joue un rôle central — d'autres langages sont aussi utilisés, comme LISP. PROLOG est un langage de programmation logique qui repose sur la logique du premier ordre (avec quantification sur des individus ou atomes). PROLOG comporte des clauses définies de la forme

$$H \leftarrow B_1 \wedge \ldots \wedge B_n$$

où H est la tête et les B_i le corps ou la queue. Le programme manipule des questions et des buts selon une hiérarchie, comme la suivante

$$\begin{array}{rcl} A_1 & \leftarrow & B_1 \\ A_2 & \leftarrow & B_2 \\ & \vdots & \\ A_n & \leftarrow & B_n \\ & \leftarrow & B_{n+1} \end{array}$$

Les questions concernent une base de données, les connaissances ou l'information positive dont on peut extraire une information particulière au moyen du moteur d'inférence constitué par les règles de la logique du premier ordre. L'information doit elle-même être soumise à certaines contraintes comme les clauses de Horn qui sont des disjonctions de littéraux (formules atomiques) positifs ou négatifs

$$A_1 \vee \ldots \vee A_m \vee \neg B_1 \vee \ldots \vee \neg B_n$$

dont chaque terme (clos) comporte au plus un littéral positif — le signe ¬ est le symbole de la négation ici. Un programme défini est un ensemble fini de clauses définies et se prête à une résolution par réfutation qui consiste à déployer un arbre d'inconsistance (à comparer aux arbres de consistance) où l'on cherche à trouver un contre-exemple pour aboutir à une clause vide qui équivaut à la réponse cherchée. Deux règles logiques sont au coeur de la démarche, le *Modus Ponens* et $E\forall$, l'élimination du quantificateur universel.

Un problème important est le traitement de la négation, puisqu'en principe un programme ne s'occupe que de connaissances positives (énoncés déclaratifs). La négation par défaut à été introduite pour contourner l'obstacle de l'information négative : si le programme échoue à démontrer en un nombre fini d'étapes, on peut inférer alors $\neg A$, pour A un terme clos.

L'information négative, *i.e.* les énoncés négatifs et l'information nouvelle sont des questions majeures en informatique théorique et en logique dynamique où l'on s'intéresse à l'information véhiculée dans le langage ordinaire. La multiplication des langages informatiques ne fait que traduire la variété des besoins qu'a entrainés l'avènement de l'ordinateur et son essor prodigieux. Du point de la logique mathématique, la création d'Automath dans les années soixante par N.G. de Brujn a généré toute une série de rejetons dont Coq (créé par T. Coquand) qui jouent le rôle d'assitants automatiques en théorie ou plutôt en pratique des démonstrations. Ces instruments hérités de la théorie des types, au sens de types ou de domaines d'objets, répondent à des besoins sémantiques par des moyens syntaxiques dont la nature fondationnelle (arithmétique) est souvent obnubilée.

Par ailleurs, l'informatique théorique pose de nouveaux défis à la logique formelle, comme l'a souligné Y. Gurevitch [52]. Ainsi la théorie des structures finies avec des cardinalités finies arbitraires n'a pas les propriétés métalogiques de complétude, compacité ou de Löwenheim-Skolem (descendant) pas plus que la logique des prédicats du second ordre. B.A. Trakhtenbrot a montré dès 1950 que la théorie des structures finies n'est pas récursivement énumérable et qu'elle ne peut prétendre à la complétude en vertu même de son caractère fini. La saturation ontologique de la sémantique ensembliste semble inappropriée pour les exigences syntaxiques de la théorie de la computation. Pour suppléer à cette carence en métathéorèmes de la logique classique, la théorie des modèles finis va recourir, par exemple, à la notion de « plus petit point fixe », $f(x) = 0$, ou encore à la notion de clôture transitive d'une relation dyadique (binaire) xRy sur un ensemble X telle qu'elle soit la plus petite relation transitive sur X qui contienne R. Ces notions sont utiles pour

définir les concepts de complexité computationnelle et de temps polynomial en fonction de la taille des problèmes et de leur résolution algorithmique. Le problème central de la théorie de la complexité demeure la question P = NP ? , c'est-à-dire le temps non polynomial non déterministe pour la résolution des problèmes est-il réductible au temps polynomial ? C'est un problème ouvert et on pense y apporter une réponse positive.

3.7 L'arithmétisation de la métamathématique

Hilbert voulait concevoir une logique de l'arithmétique qui prolongerait l'arithmétique finie en une arithmétique transfinie ; la logique arithmétique serait ainsi transformée en une logique ensembliste « externe ». L'internalisation de la logique de l'arithmétique va dans l'autre sens puisqu'elle est la continuation logique de l'arithmétisation de l'analyse et de l'algèbre.

Le 19e siècle a été le siècle de l'arithmétisation de Gauss et Cauchy à Kronecker, Weierstrass et Dedekind qui a conçu sa théorie des coupures comme une arithmétisation des nombres réels. Même Cantor peut être considéré comme un apôtre de l'arithmétisation puisqu'on peut prétendre que l'arithmétique transfinie appartient au programme finitiste « élargi » en négligeant le fait que Cantor voyait les choses d'un point de vue transcendant dans son interprétation du concept de limite. Cauchy et Weierstrass ont introduit le concept de limite finie pour approcher « infiniment » le fini – c'est certainement le sens des suites de Cauchy et du formalisme $\varepsilon - \delta$ de Weierstrass. Pour Cantor, ce n'est pas le procès de l'approche de la limite qui compte, c'est la possession dans notre esprit de la limite « par avance », par le moyen d'une sorte d'*a priori* platonicien. Le théorème de la forme normale de Cantor est en apparence seulement une sorte de descente finie sur les puissances d'un polynôme ordinal de la hiérarchie des ω :

$$\zeta = \gamma_0 \beta^{\alpha_n} + \gamma_1 \beta^{\alpha_{n-1}} + \ldots + \gamma_{n-1} \beta^{\alpha} + \gamma_n,$$

où les γ_i sont des coefficients entiers et les ω_i qui sont des puissances en termes d'ordinaux transfinis $< \varepsilon_0$; les ordinaux transfinis sont tous des ordinaux limites qui subsistent indépendamment de toute forme d'approche ou d'approximation. Cette échelle de Jacob ne touche jamais le sol de l'arithmétique finie !

Kronecker s'appuyait sur les déterminations conceptuelles « *Begriffsbestimmungen* », Dedekind et Hilbert parlaient plutôt de lois de la pensée pour

les opérations arithmétiques. Frege se demandait : « jusqu'où peut-on aller en arithmétique par le seul moyen de l'inférence logique ? » et sa réponse consistait à dire que le lien inférentiel se substituait au concept de succession dans une série « *Anordnung in einer Reihe* » au profit du concept de suite logique « *logische Folge* » (voir Gauthier [42], chap.5.2). « *Sequences or consequences* » dans un jeu de mots qu'on ne peut rendre en français. La logique frégéenne outrepasse l'arithmétique dans une théorie des concepts pour accéder à un monde platonicien d'entités subsistantes inaccessible à la pratique mathématique, mais ouvert à la spéculation philosophique et théologique (pour Cantor à tout le moins).

La logique interne de l'arithmétique contient simplement les opérations de l'arithmétique et les lois qui découlent de leur combinaison. La logique du contenu émerge du contenu lui-même et ne lui est pas imposée de l'extérieur. La logique formelle, au sens où Hilbert l'a formulée avec Frege et Russell, est étrangère à une logique du contenu , cela seul Hilbert l'a vu. Pour Hilbert la conception finitiste des mathématiques, sa métamathématique ou sa théorie des démonstrations ou encore théorie des systèmes formels devait demeurer très proche des structures inférentielles de l'arithmétique tout en conservant la logique ordinaire (aristotélicienne), en particulier la loi du tiers exclu. Mais pour Hilbert, la logique aristotélicienne ne parvenait pas à distinguer les domaines infinis des domaines finis en vertu de sa généralité et c'est pour cette raison qu'il a dû introduire des éléments idéaux où la logique aristotélicienne continuerait de s'appliquer. Le tiers exclu fait certainement partie du raisonnement finitaire, mais n'est pas un principe *a priori*, il doit découler de la logique interne de l'arithmétique, comme dans le cas d'une descente finie où l'on peut obtenir une conclusion par *reductio ad absurdum* ou encore dans le cas des suites infiniment processives de Brouwer où il ne s'applique pas.

La logique formelle ou un système formel avec son appareil axiomatique ne serait rien d'autre que la projection de la logique interne de l'arithmétique dans le monde « extérieur », le monde réel des réalistes platoniciens et de certains structuralistes. La logique polynomiale modulaire, comme je l'ai appelée (voir l'annexe B là-dessus), reflète mieux la logique interne de l'arithmétique à mon sens ; elle est inspirée directement par les travaux de Kronecker en arithmétique polynomiale (arithmétique générale) et a comme outil principal la descente infinie de Fermat qui se retrouve aussi dans la théorie de la divisibilité (systèmes modulaires) de Kronecker. Herbrand, Skolem et Gödel parmi beaucoup d'autres (e.g. Goodstein) ont fondé la logique

sur un calcul équationnel que Hilbert avait inauguré. Je désignerai ces développements de la logique arithmétique sous le terme de prolongement arithmétique en analogie avec le prolongement analytique en analyse complexe où des cercles concentriques viennent élargir progressivement le champ de validité d'une logique interne. Mais ces cercles ne s'étendent pas jusqu'au royaume transcendant des éléments idéaux ou des ordinaux transfinis. Extensions arithmétiques et algébriques s'arrêtent dans le fini et ne peuvent continuer que dans l'indéfini ou l'« effini »...

3.8 Hilbert

Hilbert [61] a eu recours à la notion de «système disparate de fonctions » dans le but explicite de produire une preuve de consistance pour le calcul « pur » des prédicats, *i.e.* sans identité ou égalité. Les fonctions dont il est question sont des fonctions arithmétiques simples qui associent un numéral à une expression numérique de telle sorte que pour un symbole numérique donné « *Ziffer* » p et un système disparate de formules

$$\phi_1, \ldots, \phi_s,$$

la disjonction $S_p^{(\phi)}$ est dérivable dans le calcul propositionnel. Un système disparate de fonctions est, par exemple (voir [61], II, 175)

$$\phi_i(n_i, \ldots, n_r) = \psi_0^1 \psi_1^{n_1} \psi_1^{n_r} \qquad (i = 1, \ldots, s)$$

où les ψ_i sont les nombres premiers initiaux $r + 1$. L'idée est d'associer, de façon disparate, à chaque r-tuple de symboles numériques un symbole numérique distinct. La procédure est analogue à une suite de choix chez Brouwer, comme le note Hilbert, et peut être prolongée indéfiniment, c'est-à-dire comme suite infiniment processive. La première étape de l'arithmétisation doit être effectuée par une reproduction de la structure grammaticale des formules ([61], II, 217) traduites par des fonctions récursives et des prédicats. Gödel a fait cette traduction pour la syntaxe de l'arithmétique de Peano. Nous savons que l'arithmétisation ne pouvait être complète dans ce dernier cas, essentiellement parce que l'induction sur un ensemble infini de nombres se prête à la procédure de diagonalisation à l'opposé de la diagonalisation chez Cauchy (le produit de convolution) que nous pouvons appliquer à l'arithmétique de Fermat (voir [19]).

Il importe de noter que l'infini potentiel des suites de choix de Brouwer, évoquées par Hilbert, permet une approche du problème de la consistance qui est compatible avec le programme de Hilbert. C'est apparemment dans son travail sur le problème du continu de Cantor que Hilbert a eu l'idée de l'arithmétisation ([61], II, 216). Le fait que la traduction de l'arithmétique transfinie dans l'arithmétique finie n'a pu être faite par Hilbert est certainement l'une des raisons du succès des résultats d'incomplétude. Le programme de Hilbert n'est pas confiné cependant à l'arithmétique ensembliste, comme l'appelle Hilbert, et je serais enclin à dire que l'idéal de l'arithmétisation survit pour la simple raison, comme Hilbert lui-même le confesse, que le programme remonte plus loin que les efforts de Hilbert et peut être retracé dans le programme kroneckerien de l'arithmétisation de l'algèbre. L'arithmétisation de la logique n'est que la conséquence d'un programme original relayé par Hilbert et repris récemment par l'arithmétique prédicative d'E. Nelson.

La théorie de l'arithmétique de R. Robinson, Q, qui est une théorie des opérations arithmétiques sans quantificateurs et sans postulat d'induction, est consistante et essentiellement indécidable. Mais la preuve de Nelson pour l'autoconsistance de Q dans [85] repose sur une notion génétique de nombre qui est à l'opposé de la notion formelle. La notion génétique se prête naturellement à l'exponentiation computable (bornée polynomialement) sous la forme

$$\begin{aligned} \sigma_0(1,n) &= \exists f \mathrm{ExpComp}(l,n,f) \\ \sigma_n &= \sigma_0(n,n). \end{aligned}$$

Le théorème pour la consistance logique d'une théorie T énonce T est tautologiquement consistant $\rightarrow T$ est σ-consistant et l'inférence

$$\sigma(b) \rightarrow \sigma(Sb)$$

est génétique puisque l'exponentiation $e(n)$ n'implique pas $\forall n\, e(n)$; l'exponentiation n'est pas totale

$$\exists n \neg \phi(n) \qquad \text{pour } \phi = e^y.$$

On peut rappeler ici l'arithmétique de Herbrand avec l'induction sur les formules sans variables libres (l'induction sans quantificateurs). La preuve de Nelson est fondée sur la preuve de consistance (Hilbert-Ackermann [60]) pour les théories ouvertes et les formules propositionnelles disjonctives auxquelles elles se réduisent peuvent être considérées comme des polynômes *de facto*, comme on l'a vu plus haut. Dans la preuve d'auto-consistance génétique de

Nelson, les nombres dénotés par les termes de la théorie arithmétisée sont bornés par les termes eux-mêmes (voir [85], 176), alors que dans le cas de l'arithmétique polynomiale, les nombres (les termes) sont bornés par le degré (et la hauteur) du polynôme de traduction. L'arithmétique polynomiale bornée serait le nom approprié de cette arithmétique. Si nous nous arrêtons à l'arithmétique récursive primitive et y ajoutons comme Hilbert ou Herbrand une forme quelconque du principe du plus petit nombre (que l'on trouve aussi chez Nelson), nous nous rapprochons d'une arithmétique que j'appelle l'arithmétique de Fermat, dans laquelle le postulat d'induction de Peano est remplacé par la méthode de la descente infinie qui n'est pas équivalente à l'induction infinie (formelle) d'un point de vue constructiviste : l'équivalent requiert une double négation sur un ensemble infini (de nombres naturels) inadmissible pour l'intuitionniste, mais tolérée par Gentzen qui n'a vu dans la descente infinie qu'une autre forme de l'induction complète et qui a fini par admettre la double négation sur l'ensemble $\aleph_0$ dans la seconde version de sa preuve de consistance. Supposer, dans ces conditions, que l'induction transfinie sur les ordinaux est la même chose que la descente infinie, comme l'a suggéré Kreisel, reflète une méconnaissance du rôle de la descente comme méthode de preuve finitaire en théorie des nombres, en algèbre et en géométrie arithmétique (algébrique). Poincaré — qui appelle récurrence la descente infinie — et Peirce sont deux auteurs qui ont mis l'accent sur cette distinction pour des raisons différentes, la principale étant à mes yeux le fait que la méthode de la descente infinie est une méthode de preuve centrale en théorie des nombres. Fermat, Euler, Lagrange, Legendre, Sophie Germain, Kummer jusqu'à Mordell et Weil ont tous utilisé la méthode pour démontrer d'importants théorèmes en théorie des nombres. Legendre, par exemple, a démontré

$$ax^2 + by^2 = cz^2$$

avec les nombres naturels a et b dont aucun n'est le carré parfait d'un autre nombre. La descente doit s'arrêter à 1 dans la substitution des coefficients de plus en plus petits et l'équation est soluble par un procédé de réduction (ou de décomposition) en conformité avec la méthode centrale de l'arithmétique de Fermat-Kronecker (F-K) avec descente infinie en théorie polynomiale — j'ai montré la consistance interne de cette arithmétique (voir l'Annexe B).

3.9 Conclusion. Consistance

Le problème de la consistance de l'arithmétique a été posé par Hilbert, mais sa solution par Gentzen, Ackermann ou Gödel fait appel à des moyens qui débordent le cadre finitiste dans lequel Hilbert avait d'abord formulé son problème. On sait que la formulation initiale de Hilbert — le programme métamathématique — voulait trop embrasser et que Gödel a montré en 1931 qu'il était irréalisable pour l'arithmétique de Peano, c'est-à-dire l'arithmétique ensembliste, dans les termes de Hilbert. Le résultat de Gödel n'exclut pas cependant, de l'aveu même de Gödel, d'autres formulations du problème de la consistance de l'arithmétique qui ne transcendent pas le programme finitiste. La formulation du problème chez Hilbert n'est pas sans ambiguïté. L'arithmétique en question est l'arithmétique des nombres réels avec un axiome de continuité qui stipule dans sa version archimédienne qu'entre deux nombres réels a et b il existe toujours un entier positif n tel que $a \prec nb$.

Dans l'esprit de Hilbert, une fois la consistance de cette arithmétique établie — c'est l'arithmétique des nombres réels qui lui avait servi de modèle pour la preuve de consistance de la géométrie euclidienne — la consistance de l'analyse (avec fonctions définies sur les réels) et la théorie des ensembles (sans inclure la hiérarchie des alephs) devait s'ensuivre. Mais Hilbert insiste sur la nature finitaire de la preuve de consistance et dans un manuscrit contemporain, cité par M. Hallett [54], Hilbert soutient qu'il s'agit pour l'arithmétique de démontrer la consistance d'"un nombre fini d'axiomes finis" et qu'il n'est aucunement question de processus infini dans cette arithmétique. Et il ajoute qu'en cela il suit Kronecker. Or, pour être en mesure de suivre Hilbert ici, il faut remonter jusqu'à Kronecker et refaire le trajet qui a mené de Kronecker à Hilbert, c'est-à-dire refonder le programme de Hilbert sur le programme de Kronecker que j'ai exposé dans le chapitre 3.

Le second théorème d'incomplétude de Gödel ou théorème sur les preuves de consistance interdit la formulation de la preuve de consistance de l'arithmétique de Peano (AP) avec les moyens de cette même arithmétique. Gödel admet dès le point de départ que ce résultat ne contredit pas le programme de Hilbert puisqu'il peut exister des preuves constructives de la consistance qui échappent au cadre ensembliste de l'arithmétique de Peano. Gödel hésitera toujours, semble-t-il, à reconnaître que son résultat de 1931 portait un coup fatal au programme de Hilbert. Quoi qu'il en soit, Gödel s'appuie dans sa preuve sur ce qu'il appelle la consistance ω et dans une note ajoutée en 1966 à la traduction de son texte de 1931 ([48], pp. 616-617), il parle de

consistance externe « *outer consistency* ». La consistance oméga ou la consistance externe est simplement la consistance du modèle ω (ω pour le premier ordinal infini) unique de l'arithmétique de Peano du premier ordre avec un ensemble infini de nombres naturels. Dans les mots de Gödel, la consistance ω est définie par les propriétés des nombres naturels. On sait que B. Rosser à réduit la consistance ω de la preuve d'incomplétude à la consistance simple au prix de l'introduction de l'énumérabilité récursive que Church avait formulée pour établir l'indécidabilité récursive de l'arithmétique de Peano et la logique des prédicats du 1er ordre (au-delà de la théorie des prédicats monadiques). En se fondant sur le résultat de Gödel et avec la diagonalisation sur tous les prédicats récursifs, Church a montré, en particulier, qu'il n'y a pas de prédicat récursif binaire qui énumère (ou binumère) tous les prédicats récursifs unaires ; en d'autres mots, on peut définir une fonction sur les entiers qui ne soit pas calculable et comme Kleene l'a répété, la notion générale de fonction récursive ne nous livre pas de procédé constructif pour définir une fonction récursive particulière. Le problème réside évidemment dans le fait que la procédure diagonale est appliquée à l'énumération totale des nombres naturels et il est facile d'exhiber en arithmétique ensembliste un ensemble récursivement énumérable qui n'est pas récursif, *i.e.* dont le complément n'est pas récursivement énumérable.

Ce qui nous importe ici, c'est de bien voir que la consistance externe de Gödel renvoie au modèle ω de l'arithmétique de Peano dont on peut dire de surcroît qu'elle est ω-complète dans ce contexte. C'est ce modèle unique extérieur au système formel qui justifie le point de vue de la sémantique ensembliste que Gödel a adopté. Tarski l'a bien vu qui remarque dans son texte [97] que la consistance ω (et la complétude ω) requiert un système "infinitiste" en acte avec une règle d'induction infinie (appelée aujourd'hui règle ω), alors que l'arithmétique classique n'est qu'un système potentiellement "infinitiste".

Gentzen voudra reprendre en 1936 le problème de la consistance là où l'avait laissé Gödel tout en poursuivant le programme de Hilbert — comme le souhaitera Herbrand qui a fourni sa preuve (incomplète) de consistance en 1931. Mais c'est en recourant à l'induction transfinie à la manière de Ackermann que Gentzen élaborera sa preuve. L'induction transfinie signifie que l'on étend l'induction complète ou infinie au-delà des ordinaux finis jusqu'aux ordinaux transfinis de la deuxième classe de nombres de Cantor limitée par l'ordinal ϵ_0. Gödel, de son côté, utilisera l'induction sur tous les types finis dans sa preuve [50] de la consistance de l'arithmétique de Peano ; c'est pour

lui une extension du point de vue finitiste, c'est-à-dire du programme finitiste de Hilbert, qui doit permettre de formuler la preuve de consistance ; il faut noter cependant que l'interprétation fonctionnelle — fonctions récursives sur les types supérieurs au type zéro des nombres naturels — va au-delà du point de vue finitiste en admettant les types comme objets abstraits dans un esprit intuitionniste. De toute évidence, il s'agit dans ce cas d'une notion très large de preuve constructive, puisque malgré le voeu d'une preuve de consistance interne d'une arithmétique réductible à l'arithmétique (abstraite) de Heyting, la quantification infinie sur l'ensemble des nombres naturels réintroduit le point de vue oméga de l'arithmétique de Peano et on doit conclure que l'arithmétique ensembliste (AP) est condamnée à une consistance externe qui repousse la limite des ordinaux finis jusqu'à la limite des ordinaux transfinis de la seconde classe de nombres de Cantor.

L'arithmétisation de la métamathématique a aujourd'hui pour objet la métamathémathique de l'arithmétique de Peano du 1er ordre (voir P. Hájek et P. Pudlák [53]) où il s'agit d'arithmétiser les fragments ou sous-systèmes de l'arithmétique de Peano, l'arithmétique de Peano elle-même étant indécidable. L'arithmétique bornée, l'arithmétique avec induction limitée, a des applications multiples en informatique théorique et fera l'objet d'un traitement spécial dans le prochain chapitre. Encore ici les systèmes formels de l'arithmétique ou des théories arithmétiques ne donnent lieu qu'à des résultats partiels et l'arithmétique de Peano formalisée ne semble pas en mesure de récupérer l'arithmétique ou la théorie des nombres classique dans son intégrité. Je forme l'hypothèse que le problème crucial est de nouveau la confusion entre descente infinie et induction complète, question qui occupe les deux annexess de la fin.

Pour espérer recouvrer la consistance interne de l'arithmétique, il faut retourner par-delà Gentzen, Gödel et Hilbert à Kronecker et Fermat « *ein Schritt zurück* », un pas si ce n'est un bond en arrière de l'infini ensembliste au fini de la descente finie dans les polynômes de degré fini de l'arithmétique de Fermat-Kronecker. Mais si selon l'adage de Poincaré l'infini est une abréviation du fini, le chemin du retour ou l'exercice de retournement n'est peut-être pas si ardu. La logique interne de l'arithmétique ou la logique arithmétique à laquelle on arrive à la fin n'est que le passage de la logique dans l'arithmétique par lequel s'achève l'arithmétisation de la logique et où la logique comme théorie de l'inférence trouve sa culmination dans une certitude et une vérité internes, comme le voulait Kronecker.

Chapitre 4

L'arithmétisation du langage

Le langage dont il s'agit ici est bien entendu l'ensemble des langages informatiques ou informatisés. On pourrait parler dans ce sens de l'arithmétisation de la logique comme langage ou encore de la logique du langage artificiel (ou de l'intelligence artificielle). Puisqu'il est question de computation, les langages artificiels (e.g. bases de données) apparaissent comme des sous-systèmes du langage ordinaire ou des langues naturelles, domaine de la linguistique qui peut être aussi computationnelle ; PROLOG le langage de programmation introduit dans le chapitre précédent a été conçu dans le contexte du langage ordinaire et l'un de ses rejetons, DATALOG, traite plutôt des bases de données emmagasinées dans un ordinateur aux fins de la spécification des programmes pour la représentation des contenus linguistiques (en entrée et en sortie). Ainsi le langage de la logique est-il un sous-système du langage ordinaire habilité à définir les structures logiques du langage en général. Ce sont les propriétés computationnelles du langage qui intéressent avant tout l'informaticien et la théorie des modèles finis est ici un modèle privilégié.

La théorie des modèles est une théorie de la classification des structures mathématiques et de leur définissabilité dans un langage du 1er ordre, *i.e.* la logique des prédicats du premier ordre. On pourrait ajouter que la théorie des catégories est aussi une théorie des structures mathématiques, mais elle s'intéresse seulement à les comparer ou à les relier à l'aide d'une théorie algébrique des fonctions (les foncteurs) sans chercher à les définir logiquement, le but ultime étant de « catégoriser » les structures et non de les caractériser. Si la théorie des modèles classiques portait d'abord sur les structures infinies, la théorie des modèles finis, comme son nom l'indique, se limite aux structures

finies et il apparaît assez tôt qu'on ne peut attribuer les mêmes propriétés aux structures finies qu'aux structures infinies. Les théorèmes classiques de la logique du 1er ordre , comme le complétude ou le théorème de Löwenheim-Skolem, ne sont plus valides en théorie des structures finies. La complétude de la logique des prédicats du 1er ordre est définie dans un modèle infini (la cardinalité infinie dénombrable $\aleph_0$ des nombres naturels) ; Gödel dit dans son texte de 1930 sur la théorème de complétude qu'une formule est « satisfaisable dans un domaine dénombrable par un système de satisfaction ou de remplissement (*Erfüllungssystem*) » ; la logique des modèles finis a des contraintes plus fortes pour la relation de satisfaction $\vdash L \leftrightarrow \models L$; ainsi on exigera que pour une collection de structures finies, l'ensemble des énoncés et la relation de satisfaction soient décidables et qu'il y ait des fonctions effectivement computables m et t de telle sorte que pour tout $\phi \in E_L$ (l'ensemble des énoncés du langage L) $m(\phi)$ soit une machine de Turing déterministe qui décide d'une requête $R(\phi)$ en un temps polynomial $n^{t(\phi)}$, c'est-à-dire que le temps de la computation ne doit pas dépasser la fonction polynomiale qui définit la taille ou la longueur (en bits) de la requête (voir E. Weinstein [108]). Un langage de requêtes (comme PASCAL) est un langage informatique qui interroge des bases de données ou des systèmes d'information et un langage de programmation théorique, comme une machine de Turing, le lambda-calcul de Church ou la logique combinatoire de Curry, formalise le calcul automatique de la machine (l'ordinateur), c'est-à-dire un algorithme. Or la théorie des modèles finis est une théorie algorithmique de la théorie des modèles finis et une théorie de la complexité algorithmique a pour limite le problème de l'arrêt pour une machine de Turing, le (premier) théorème d'incomplétude de Gödel ou le résultat d'incompressibilité de Kolmogorov-Chaitin. On sait que l'incomplétude ou le phénomène d'incomplétude et ses variantes algorithmiques n'affecte qu'une faible partie des mathématiques, les mathématiques qui sont résolument infinitaires, pourrait-on dire. La logique finitaire doit donc rester à l'intérieur des limites de la décidabilité. L'algorithme de la clôture transitive, par exemple, qui définit la plus petite clôture transitive d'une requête ou d'une relation binaire comme

$$\mathrm{CT(G)} \ \{ \ (a,b) \in S^2 : \text{il y a un chemin de } a \text{ à } b \ \}$$

pour un graphe G et des sommets S. De même l'algorithme du plus petit point fixe (pppf) pour

$$Fx = x$$

est une fonction monotone

$$Fx \leq Fy \quad \text{pour } x \leq y$$

si

$$\forall y(Fy = y \rightarrow x \leq y).$$

Un autre algorithme, comme le jeu de va et vient d'Ehrenfeucht-Fraïssé, qui assure la pleine information pour un dialogue entre « ∀bélard » et « ∃loïse », permet de définir deux structures équivalentes dans un langage du 1er ordre (voir Hodges [62], p. 95). Tous ces algorithmes ont une vocation sémantique, puisqu'ils relèvent de la théorie des modèles. Des résultats récents sur la préservation d'homomorphismes dans les modèles finis tentent de jeter des ponts entre sémantique et syntaxe.

4.1 La théorie des modèles finis

La théorie des modèles finis est née du défi de l'informatique théorique, selon Y. Gurevitch [52]. Les langages de programmation, (comme PASCAL) semblent exiger plus que la logique classique et les bases de données relationnelles ne font appel qu'à des structures finies. Gurevitch a introduit dans cette perspective la notion de machine à états abstraits (*abstract state machine*) où sont introduites des structures logiques qui évoluent en un temps fini pour l'implantation des programmes informatiques. Or, la logique classique a fait son nid dans la notion d'ensemble infini — infini dénombrable ou $\aleph_0$ pour la logique des prédicats du premier ordre — et les théorèmes de complétude, de compacité et de Löwenheim-Skolem parmi d'autres requièrent un ensemble infini et ne sont donc pas valides pour les modèles finis où la cardinalité de l'ensemble des individus doit être finie. Ainsi le résultat de B. A. Trakhtenbrot (1950) montre que la théorie des structures finies n'est pas récursivement énumérable, c'est-à dire qu'elle ne peut être complète, au sens de la sémantique classique (ensembliste).

Le concept central de faisabilité « *feasibility* » a permis de concrétiser la machine de Turing abstraite qui dispose de ressources infinies (ruban infini). La théorie des modèles finis n'a besoin que d'un segment initial de N, l'ensemble des nombres naturels, des constantes $0, FIN$ —pour fin du ruban ou nombre maximal de ses cases — la fonction partielle de successeur S ; le vocabulaire est fini (peut être vide).

Les structures finies correspondent à une syntaxe finitaire et la théorie de la complexité a défini les temps et les espaces de la computation. Pour les temps, on a la classification ou la hiérarchie temps linéaire (*Lin*), temps polynomial (*Pol*) et temps exponentiel *(Exp*) et pour les espaces, l'espace logarithmique (*Loge*), l'espace linéaire (*Line*) et l'espace polynomial (*Pole*). Le temps (*NPol*) est le temps polynomial non déterministe, c'est-à-dire le temps polynomial d'une machine aléatoire qui doit deviner le résultat à diverses étapes du calcul. Le problème principal de la théorie de la complexité se résume à

$$Pol = NPol\ ?$$

Pour *NPol*, un autre problème

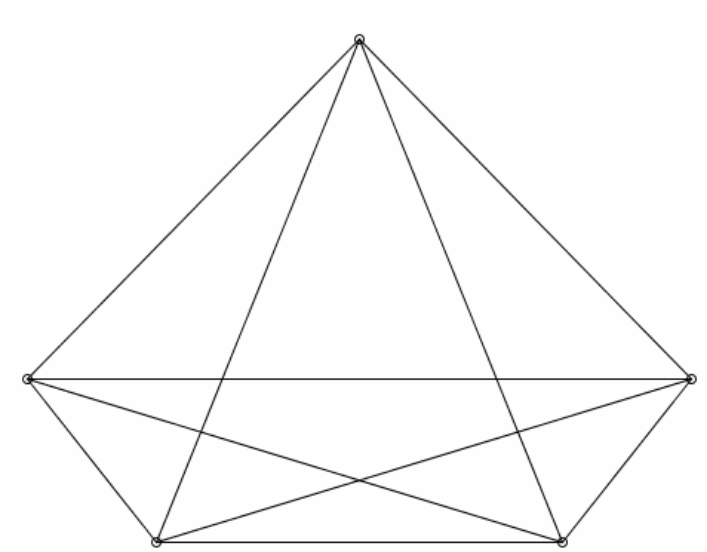
$$NPol = coNPol\ ?$$

pose la question de savoir si les compléments des ensembles *NPol* computables sont aussi *NPol* computables. Les problèmes *NPol-complets* constituent une classe d'équivalence de *NPol* problèmes et parmi eux on trouve les problèmes traités en théorie des graphes, cliques et graphes hamiltoniens, par exemple.

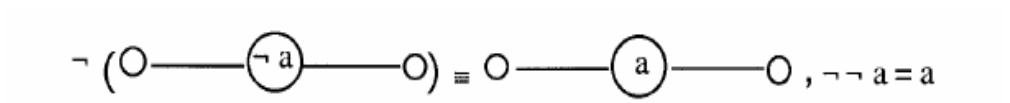
La théorie des graphes (et des hypergraphes ou graphes n-dimentionnels) est un instrument privilégié de la programmation linéaire et il n'est pas difficile d'en faire une présentation sommaire. Un graphe est un ensemble fini de points $x_l, x_2, \ldots, x_n$ appelés sommets S reliés par des arêtes A ou des arcs — les arcs ont une orientation en flèches alors que les arêtes n'en ont pas.

Un graphe est donc un couple $G = (S, A)$. Une boucle (x, x) est une chaîne de longueur 0, une chaîne de longueur $q > 0$ forme un cycle pour des arêtes $An, n > 2$ dont les sommets coïncident et un circuit est une suite de cycles telle que le sommet d'un cycle c_i coïncide avec le sommet d'un cycle c_{i+1} dans une chaîne $q > i$.

Une clique est un graphe complet — avec S et $A > 2$ — et simple, avec arête unique entre deux sommets :

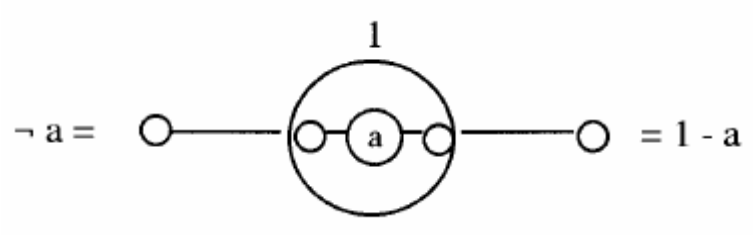


Un circuit hamiltonien passe une fois par chaque sommet du graphe. Un problème concret bien connu, celui du voyageur de commerce qui doit visiter plusieurs clients en voyageant le moins possible, est soluble dans certains cas particuliers, mais le problème général est considéré *NPol-complet* (ce vocable est dû à S. Cook). Théorie des jeux en économique et théorie des réseaux utilisent à profusion les graphes, mais du point de vue de la logique, seuls les graphes logiques ou les circuits booléens avec les sommets 0 et 1, $B = (0, 1)$ sont d'intérêt. La combinatoire géométrique des graphes logiques permet de représenter une négation non symétrique ou non booléenne dans un circuit logique. Pour la négation booléenne, on a

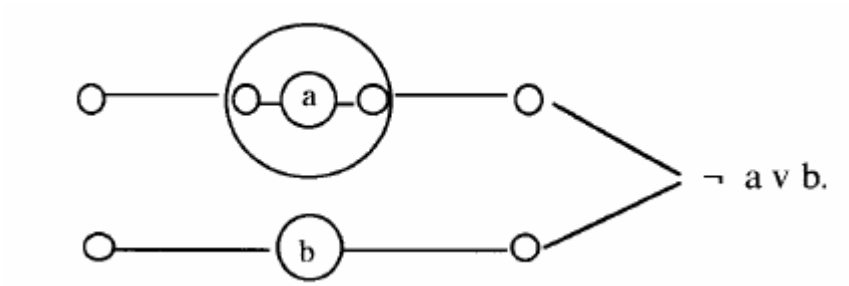


en supposant que $a = 1$ pour un circuit fermé et $a = 0$ pour un circuit ouvert.

Pour la négation locale non symétrique, on a



où nous obtenons un circuit intégré qui localise la négation de a dans un sous-circuit, e.g.



La négation locale me paraît être au coeur de la représentation linéaire de la logique et la logique des programmes, de PROLOG aux systèmes experts, en a fait un problème central.

La question de la négation est aussi cruciale en logique dynamique (non-monotone). Même si plusieurs interprétations ont été proposées pour l'introduction de la négation par défaut dans le cadre classique, c'est la version constructive qui paraît la plus plausible. Nous la comparons à une théorie de la négation locale qui a été développée dans le cadre constructiviste d'une logique arithmétique.

4.2 Des fragments de l'arithmétique à la logique prédicative

Dans son article sur « L'impossibilité d'un algorithme pour le problème de la décision dans les classes finies » (voir [98]), B.A. Trakhtenbrot montre que l'ensemble des classes finies n'est pas récursivement énumérable. Le théorème 2 est une extension du théorème de Church pour les domaines finis :

c'est l'ensemble de tous les domaines finis qui n'est pas récursivement énumérable et par conséquent la théorie de tous les modèles finis d'une théorie du premier ordre T est indécidable. La théorie des algorithmes remonte à Markov et les résultats de Church, Post, Turing, Novikov (pour le problème des mots) jusqu'à Matijasevič sur le dixième problème de Hilbert sont bien connus. L'insolubilité algorithmique repose, bien entendu, sur les concepts de récursivité, fonction récursive et fonction récursive primitive introduits par Herbrand, Skolem et Gôdel, mais on peut en retracer l'origine jusqu'à Dedekind et Kronecker. Plus que chez Dedekind, dont l'inspiration est ensembliste, pour Kronecker une suite récursive sera un algorithme et l'objet principal sera un polynôme ou une équation polynomiale comme

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x^1 + a_0 = 0$$

où n est un nombre naturel et x une indéterminée : il s'agit ici de trouver toutes les racines de l'équation. Le dixième problème de Hilbert posait la question de l'existence d'un algorithme pour les équations diophantiennes, *i.e.* avec coefficients entiers. La réponse dans le dernier cas est négative, puisque c'est un problème général et une équation diophantienne particulière peut être résoluble. La notion générale d'un algorithme se réduit à celle de machine de Turing et le problème d'un algorithme général se réduit alors au problème de l'arrêt : pour un programme quelconque, la machine s'arrête-t-elle ou forme-t-elle une boucle infinie ? La thèse de Church suppose l'équivalence des notions d'algorithme de Markov, système de Post, machine de Turing etc. et stipule que toute fonction computable est récursive. Le théorème de Church établit que toute extension consistante de l'arithmétique récursive primitive est indécidable. On voit bien que l'enjeu porte sur l'ensemble infini des nombres naturels et le premier théorème d'incomplétude de Gödel montrait par diagonalisation que le système formel qui le comprenait ne pouvait être complet tout en étant consistant.

Le noeud du problème se trouve donc dans l'induction ou la quantification sur un ensemble infini. On pourrait penser que le théorème de Trakhtenbrot sur les classes ou structures finies est de nature différente, mais là aussi la récursivité classique y joue le rôle central puisqu'on quantifie sur toutes les classes finies. Mais comment les questions sur les polynômes sont-elles d'un tout autre ordre ? Pour le comprendre, il faut penser en termes d'induction, la descente infinie de Fermat. Montrons-le par un exemple, l'algorithme d'Euclide qui est une sorte de préfiguration de la descente infinie de Fermat. L'algorithme d'Euclide est une méthode pour trouver le plus grand diviseur

commun de deux nombres entiers, on divise l'un par l'autre, ce dernier par le reste, le premier reste par le second, le second par le troisième et ainsi de suite. Une fois la division achevée, le dernier diviseur est le plus grand diviseur commun. Le même procédé s'applique aux polynômes. Euclide l'a lui-même appliqué dans la démonstration de son théorème sur l'infinité des nombres premiers et Fermat a utilisé sa méthode pour montrer l'impossibilité d'une solution pour l'équation diophantienne

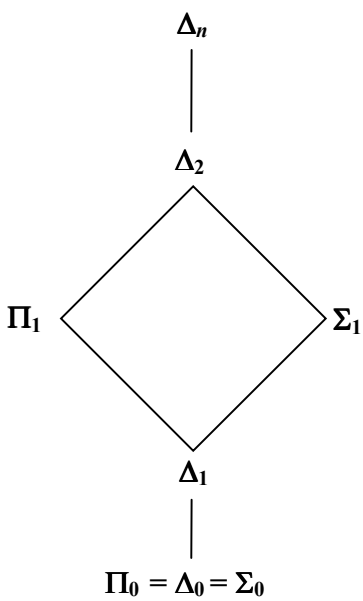
$$x^4 + y^4 = z^2$$

pour les entiers $x, y, z \neq 0$ et $z < 0$. La question initiale de la décidabilité prend un sens précis. Classiquement, une théorie est complète si et seulement si elle est consistante et décidable — si et seulement si toute formule close (énoncé) A est décidable. Le théorème de Trakhtenbrot a donc pour conséquence que la théorie des modèles finis (pour tout ordinal fini) ne peut être complète. Par ailleurs, la consistance exige que $0 \neq 1$ et il faut l'obtenir par des moyens finis. Pour une théorie ouverte on pourra même obtenir l'autoconsistance. Il faudra donc introduire nos quantificateurs finitairement et la décidabilité devra aussi être définie constructivement. L'arithmétique générale des polynômes nous fournira le cadre effectif d'une logique arithmétique dont la décidabilité sera polynomiale. Dans ce contexte, il est alors possible de définir une complétude locale ou relative qui n'a d'autre garant que la finitude du calcul.

L'étude des fragments de l'arithmétique est relativement récente ; elle a pris la relève, pourrait-on dire, de la méthode des sous-systèmes de l'analyse qui a obtenu peu de résultats concluants. Rappelons que l'examen des sous-systèmes de l'analyse avait pour but d'apprivoiser en quelque sorte le problème de la consistance de l'analyse en appliquant une théorie des démonstrations réductrice , c'est-à-dire une méthode qui consiste à réduire le problème de la consistance de l'analyse au problème de la consistance de sous-systèmes (de l'analyse). L'induction transfinie (jusqu'à ϵ_0) est au coeur du problème, puisque Gentzen avait obtenu une preuve de la consistance de l'arithmétique de Peano à l'aide de l'induction transfinie dès 1936. Ce sont donc les divers principes d'induction qui feront l'objet des recherches dans le domaine des fragments de l'arithmétique de Peano.

4.2.1 La hiérarchie arithmétique

Commençons par définir la hiérarchie arithmétique. On dit que Δ_0 est la classe de toutes les formules bornées, *i.e.* avec quantificateurs bornés $\forall x < t$ et $\exists x < t$ pour t un terme ; si la formule bornée commence avec un quantificateur $\exists x < t$, on dit qu'elle est Σ_0 et si elle commence par un quantificateur $\forall x < t$, elle sera dénotée Π_0. La hiérarchie a donc pour base $\Pi_0 = \Delta_0 = \Sigma_0$ et grimpe jusqu'à Δ_n



Σ_n, par exemple est

$$\exists x_1 \forall x_2 \exists x_3 \ldots Q x_n \phi(x_1, x_2, x_3, \ldots, x_n, y)$$

et Q est $\exists$ ou $\forall$ selon que n est impair ou pair ; Π_n est de même forme

$$\forall x_1 \exists x_2 \forall x_3 \ldots Q x_n \phi(x_1, x_2, x_3, \ldots, x_n, y).$$

On peut mettre les formules arithmétiques en forme normale prénexe

$$\theta(x) \leftrightarrow Q_1 y_1 Q_2 y_2 \ldots Q_n y_n \phi(x, y)$$

ou Q_i est $\exists$ ou $\forall$ et ϕ n'a pas de quantificateurs. On a encore une formule Σ_{n+1}, si et seulement si elle est de la forme

$$\exists x \phi(x, y) \text{ avec } \phi \in \Pi_n$$

et une formule Π_{n+1}, si et seulement si elle est de la forme

$$\forall x \phi(x, y) \text{ avec } \phi \in \Sigma_n$$

Au-delà de la hiérarchie arithmétique, les formules Δ_n^1 constituent la hiérarchie hyperarithmétique où Δ^1 signifie que l'on quantifie sur des variables fonctionnelles (au lieu des variables numériques), donc

$$\theta(f) \leftrightarrow Q_1 f_1 Q_2 f_2 \ldots Q_n f_n \phi(x, f)$$

La hiérarchie arithmétique s'étend donc encore plus loin en formules Δ_n^1 et on peut établir la correspondance suivante avec la théorie descriptive des ensembles : la hiérarchie arithmétique Δ_n^0, recouvre les ensembles finis (ω), la hiérarchie hyperarithmétique comprend les sous-ensembles récursifs de ω et la hiérarchie analytique (ou projective en n dimensions) s'étend sur les sous-ensembles récursifs de 2^ω. La première hiérarchie a donné naissance à la logique ω ; la logique β s'occupe de l'au-delà. Remarquons qu'on a d'abord les fonctions récursives primitives, puis les fonctions récursives (générales) et enfin les ordinaux (bons ordres) récursifs pour assurer la correspondance fonctionnelle. Il faut noter que l'on a

$$\Sigma_n \subseteq \Delta_{n+1} \subseteq \Sigma_{n+1}.$$

4.2.2 L'arithmétique bornée

L'arithmétique bornée (avec quantificateurs bornés) (cf. Buss [14]) aura sa hiérarchie bornée

$$\Sigma_0^b, \Sigma_1^b, \Pi_1^b, \Sigma_2^b, \Pi_2^b$$

et une induction bornée logarithmiquement

$$\Sigma_i^b \text{ LIND } : A(0) \wedge (\forall y < |x|) A(y) \rightarrow A(Sy) \rightarrow A(|x|)$$

ou

$$A(0) \wedge \forall x (A(x) \rightarrow A(Sx)) \rightarrow A(|x|)$$

pour $|x| = \lceil \log_2(x+1) \rceil$ où $\lceil\ \rceil$ signifie $\geq \log_2(x+1)$ et aussi une induction bornée polynomialement

$$\Sigma_i^b \text{ PIND } : A(0) \wedge \forall x((A(\lfloor x \rfloor) \rightarrow A(x)) \rightarrow \forall x A(x)$$

où $\lfloor\ \rfloor$ signifie $\leq x$. L'expression $|x|$ est la longueur de la représentation binaire de x et log a la définition

$$\log x = k \leftrightarrow |x|_2 = 2^k,$$

autrement $k = 0$. On a aussi une fonction dièse qui s'exprime

$$x \# y = 2^{\log x \cdot \log y}.$$

Le principe du plus petit nombre ou du minimum a également une version bornée

$$\Sigma_i^b \text{ LMIN } : \exists x A(x) \rightarrow A(0) \vee \exists x[A(x) \wedge \forall y \leq \lfloor x \rfloor \neg A(y)]$$

équivalent à Π_i^b PIND - Σ_i^b MIN est équivalent à Π_i^b IND.

L'idée d'une induction logarithmique est que la vérification d'une propriété inductive dans ce contexte peut s'effectuer en un temps polynomial et cela nous mène à la théorie de la complexité (algorithmique) où le problème principal est

$$P = NP\ ?$$

c'est-à-dire la question de savoir si le temps polynomial (d'une computation) est le même que le temps polynomial déterministe, *i.e.* un temps où sont possibles plusieurs actions (d'une machine de Turing par exemple) dans un état donné. Un autre problème est

$$NP = coNP\ ?$$

pour *coNP* le complément de *NP*. Un problème est *NP-complet*, s'il est réductible à la question $P = NP$. Prenons le cas d'un espace polynomial, *i.e.* l'ensemble des fonctions de croissance polynomiale qui peuvent êtres calculées par une machine de Turing M. Cet ensemble admet un polynôme $p(\vec{n}) - \vec{n} = (n_1, \ldots, n_n)$ — pour lequel le nombre total de cases du ruban de M pour l'entrée $\vec{x}$ (input) est toujours moindre que $p(|\vec{x}|)$, la borne logarithmique. Pour un temps exponentiel, le temps de réalisation de M sur l'entrée $\vec{x}$ est toujours inférieur à $2^{p(|x|)}$ qui est une borne polynomiale.

La hiérarchie du temps polynomial P, Σ_1^p,Π_1^p qui relaie la hiérarchie du temps linéaire est à son tour limitée par le temps exponentiel, mais la hiérarchie polynomiale ne s'effondre pas sur un niveau fini, *i.e.* est infinie. En analogie avec la hiérarchie polynomiale, la hiérarchie Δ_n des fragments de l'arithmétique de Peano est infinie et la hiérarchie

$$I\Sigma_0 \subseteq I\Sigma_0 + \Omega_1 \subseteq I\Sigma_0 + \Omega_2 \subseteq \ldots \subseteq I\Sigma_0 + \mathrm{Exp} \subseteq I\Sigma_0 + \mathrm{Superexp}$$

où I est l'induction et Ω_1 est

$$\Omega_1 = \forall x \exists y (x^{\log_2 x} = y)$$

implique que si la hiérarchie polynomiale est infinie, aucun des fragments n'est finiment axiomatisable. Les fragments $I\Delta_0$ et $I\Delta_0 + \Omega_1$ sont consistants, *i.e.* interprétables dans Q, l'arithmétique de Robinson où les axiomes d'induction sont remplacés par des suites de longueur polynomiale (voir Kaye [67]). Mais l'exponentiation ne saurait être totale

$$I\Delta_0 \vdash \forall x \forall y \exists z\, \eta(x, y, z)$$

pour $\eta = \exp : x^y = z$ et dans $I\Delta_0 + \Omega_1$, 2^xexiste si et seulement si 2^{x^2}existe de sorte que pour une formule bornée $\phi(x)$

$$I\Sigma_0 + \Omega_1 \vdash \forall x\, \phi(|x|^{(k+1)}) \forall k$$

où $|x|^{(k)}$ désigne la fonction $x \to |x|$ itérée k fois, mais

$$\vdash \neg(I\Sigma_0 + \Omega_1 + \forall x\, \phi(|x|^{(k)}))$$

implique la consistance de ϕ — par la deuxième preuve d'incomplétude de Gödel — et 2^xexiste, si et seulement si 2^{x^2}existe signifie qu'il y a une hiérarchie infinie d'applications de l'exponentiation bornée, l'exponentiation n'étant pas totale.

4.2.3 Consistance

La consistance dont il s'agit est évidemment celle de l'arithmétique de Peano (démontrée par Gentzen à l'aide de l'induction transfinie jusqu'à ϵ_0). Mais nous avons besoin pour l'arithmétique prédicative d'une preuve de consistance interne ; c'est le théorème de Hilbert-Ackermann (voir [60]) qu'on peut formuler ainsi :

> Une théorie ouverte T — où les axiomes ne comportent pas de quantificateurs — est inconsistante, si et seulement si il y a une quasi-tautologie qui est une disjonction de négations d'instances pour les axiomes nonlogiques de T.

Ici, une quasi-tautologie est une conséquence tautologique d'instances d'axiomes d'identité et d'égalité. Un théorème qui est apparenté, le théorème de Herbrand, joue un rôle important en arithmétique bornée ; nous le donnons sous la forme suivante (voir Shoenfield [93]) :

> Soit T une théorie sans axiomes non logiques et A un énoncé (formule close) en forme prénexe dans T ; alors A est un théorème de T, si et seulement si il y a une quasi-tautologie qui est une disjonction des instances de la matrice de AH.

Nous avons la formule existentielle

$$\exists x \forall y \exists z \forall w \, B[x, y, z, w]$$

et AH est

$$\exists x \exists z \, B[x, f(x), z, g(x, z)]$$

pour f unaire et g binaire. Le théorème de Herbrand est à son tour apparenté au *Hauptsatz* de Gentzen sur l'élimination des coupures, *i.e.*

$$\frac{A \vdash C \qquad C \vdash B}{A \vdash B}$$

qui correspond au *Modus Ponens*

$$\frac{A, \; A \supset B}{B}$$

ou encore à la règle d'élimination du fer à cheval en déduction naturelle ($E \supset$). Or un des problèmes centraux auxquels doit faire face une arithmétique bornée est la superexponentiation dans l'élimination des coupures ou encore la limitation de la transitivité de l'implication, *i.e.*

$$\frac{A \supset D, \; D \supset B}{A \supset B}.$$

La consistance va devoir imposer des contraintes sur la longueur des preuves, leur taux d'incompressibilité, dirait-on en termes de complexité algorithmique de Kolmogorov-Chaitin.

On sait que pour les théories ouvertes, Tarski a obtenu tôt des résultats de décidabilité — en algèbre et en arithmétique des nombres réels. Par exemple, l'arithmétique de Robinson sans quantificateurs est décidable, alors qu'elle devient essentiellement indécidable si on lui ajoute des quantificateurs. Nelson (voir [85]) a obtenu une preuve de consistance pour cette arithmétique. La formalisation du fait que n est un nombre génétique, c'est-à-dire non formel, prend la forme

$$\sigma_0(l, n) = \exists f \text{ expcomp}(l, n, f)$$

où expcomp(l, n, f) signifie que pour tous les i dans le domaine de f, $i \leq n$ et $f(0) = l$; cela entraîne pour un a quelconque explog$(f(i), a)$ pour $\text{loglog}\, a = f(i)$.

$$\sigma_n = \sigma_0(n, n)$$

— l'exponentiation est computable ou polynomialement bornée. On obtient alors le théorème de consistance tautologique :

T est tautologiquement consistant $\rightarrow$ T est σ-consistant.

Dans cette théorie, l'inférence

$$\sigma(b) \rightarrow \sigma(Sb)$$

est génétique et non formelle et l'exponentiation $e(n)$ n'entraîne pas $\forall n\ e(n)$. L'exponentiation n'est pas totale et l'on retrouve le théorème de Parikh [86] qui énonce que l'exponentiation totale ne peut être démontrée dans l'arithmétique bornée. Cependant, comme le note Nelson, la preuve de Parikh n'est pas constructive, puisqu'elle fait appel à un modèle non standard (de l'arithmétique de Peano) dans lequel on a un entier non standard

$$\forall x \exists k\ (x < \alpha^k) \text{ pour } k \text{ standard}$$

et qui génère un sous-modèle dans lequel l'arithmétique bornée est valide. Le modèle non standard abrite aussi un y non standard tel que pour $\beta = \alpha - k$, j'ai

$$\exists y\ (y \cdot \beta^k \geq 1 \cdot \alpha^k) \text{ pour } y \neq 0,$$

ce qui est impossible. Le théorème de Parikh nous dit donc qu'on a pour l'exponentiation bornée $r = x^k$

$$\forall x \exists y\ \phi(x, y) \rightarrow \forall x \exists y \leq r(x) \phi(x, y)$$

et pour le théorème de Herbrand, on a un terme $t(x)$

$$\forall x \exists y\, \phi(x, y) \rightarrow \forall x \exists t(x)\, \phi(x, t(x)).$$

Dans le contexte de l'arithmétique faisable « *feasible arithmetic* » qu'a introduite Parikh sous l'influence du finitisme de Yessenin-Volpin, il n'y a pas de preuve de

$$P^k(A) \vee P^k(\neg A)$$

pour $P(A)$ le plus petit nombre de symboles qui corresponde à une preuve de A — qui soit raisonnablement faisable — pour k suffisamment grand dans la théorie axiomatique des ensembles de Zermelo-Fraenkel. On peut ici, à la suite de Parikh, reprendre la critique de l'induction formulée par Poincaré. Cette critique montre qu'on ne saurait justifier l'induction complète (formelle) qu'en utilisant une autre induction formelle de la façon suivante : par induction ω sur tous les n, j'ai

$$[A(\bar{0})] \wedge (P[A(\bar{n})] \rightarrow P[A(\overline{Sn})]) \rightarrow P[A(\overline{n+1})] \text{ parMP}$$

donc $\forall x A(x) \equiv \forall n\, P[A(\bar{n})]$.

Les barres signifient ici que nous avons affaire à des numéraux ; on obtient l'équivalence formelle à la façon de Gödel en supposant que l'induction sur ω est une inférence logique sur $\forall x A(x)$et on revient à la critique de Nelson touchant l'induction non bornée puisque l'exponentiation inductive $e(n)$ serait sujette au second théorème de Gödel, auquel échappe l'autoconsistance de l'arithmétique de Robinson en vertu du fait que la preuve de consistance est bornée par les termes mêmes de la théorie. La critique de Poincaré révèle par ailleurs le lien entre d'une part l'imprédicativité de l'induction formelle et de l'induction complète et d'autre part entre l'inférence *MP* et l'arithmétique non bornée. On voit que Poincaré en semi-intuitionniste a anticipé en quelque sorte l'arithmétique prédicative bornée.

4.2.4 Arithmétique constructive

On peut au point de départ définir une fonction constructive de la façon suivante :

$$\forall x \exists y\, \phi(x, y) \rightarrow \exists f \forall x\, \phi(x, f(x))$$

c'est-à-dire que pour une formule $\phi(x, y)$ il existe une fonction f de x qui compute la valeur y, $f(x) = y$

$$\forall x \exists f\, \phi(x, f(x))$$

pour

$$\forall x \exists! y \, \phi(x, y).$$

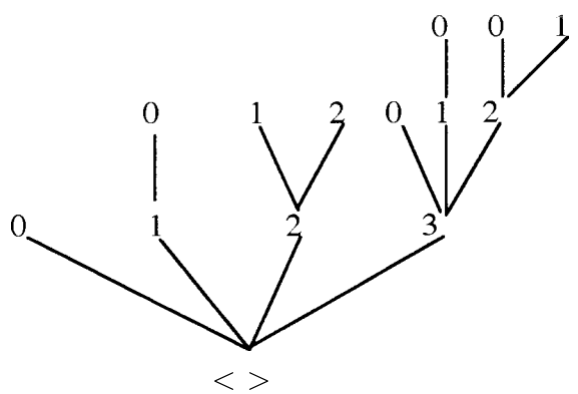
On peut poser le cadre général de cette formulation en recourant $I\Sigma$, soit un système formel pour les fonctions récursives, ou encore $I\Sigma_1^1$, un système formel pour les fonctionnelles récursives. Le théorème de Brouwer-König dans ce contexte peut être vu comme un théorème de finitude dans une direction

$$\forall x \exists F \, \phi(\vec{x}, F(\vec{x})) \rightarrow \forall n \exists F \forall x \leq n \, \phi(\vec{x}, F(\vec{x}))$$

pour $\vec{x} = \langle x_0, \ldots, x_n \rangle$ et comme théorème d'infinité dans l'autre direction

$$\forall n \exists F \forall x \leq n \, \phi(\vec{x}, F(\vec{x})) \rightarrow \forall x \exists F \, \phi(\vec{x}, F(\vec{x}))$$

Le lemme de König définit l'induction sur les arbres biens fondés



$$\forall b \in A \, \exists n \forall m \, (m > n \rightarrow b* < n >= 0) \rightarrow \exists N \forall b \, (b \leq N)$$

pour toutes les branches b (longueurs des segments initiaux) d'un arbre bien fondé et N le faîte de l'arbre (sa hauteur) : dans sa forme forte, le lemme de König stipule que si A est un arbre infini à branchement fini, il y a un sentier $S \leq A$. Remarquons qu'un bon ordre est un ordre bien fondé qui est linéaire pour x un polynôme linéaire et pour lequel $x \mapsto 2^x$. Il est évident que le lemme de König est infinitaire si l'on quantifie sur toutes les suites finies d'entiers naturels, puisqu'on a la quantification universelle du second ordre. Un ordinal est alors le nombre d'un bon ordre transitif qui est un ordre linéaire bien fondé. À tout segment initial correspond un ordinal. Le théorème de Zermelo affirme que la classe de tous les ordinaux est bien ordonnée par $\in$ $(\leq)$ et l'axiome de fondation de Z-F suppose que tous les ensembles sont bien fondés.

Enfin, l'induction transfinie repose sur la forme normale de Cantor pour les ordinaux « récursifs » jusqu'à ω_1 ; c'est une itération de l'exponentiation des ordres linéaires qui n'a pas de sens prédicatif.

Le lemme de König a une parenté évidente avec l'induction barrée de Brouwer pour les suites irrégulières — espèces bien fondées de suites finies — que nous avons vues dans le chapitre précédent.

Il serait abusif de voir dans ces divers principes une théorie de l'arithmétique bornée, mais on y perçoit certainement l'esprit constructif qui va présider à l'arithmétique finitaire. Il n'est pas facile de déterminer avec précision les aires du constructif et du non-constructif et les extensions du point de vue finitaire, selon l'expression de Gödel, débouchent souvent sur l'infini non-constructible. Pensons simplement qu'avec l'induction sur les formules bornées Δ_0 (pour les fragments de l'arithmétique) et le principe de collection (ou remplacement)

$$I\Sigma_1 \vdash \forall x \leq y \; \exists y \, \phi(x,y) \rightarrow \exists v \, \forall x \leq y \; \exists y \leq v \; \phi(x,y)$$

ou de compréhension

$$I\Sigma_1 \vdash \forall x \; \exists y, z \; \forall u \leq x \; (u \in (y,x) \equiv \phi(u))$$

on obtient l'arithmétique de Peano

$$\mathrm{AP} \; = I\Delta_0 + \mathrm{Collection}.$$

L'axiome de remplacement nous dit qu'on peut insérer un quantificateur borné dans un quantificateur borné. L'axiome de remplacement borné devra avoir la forme (voir Hájek and Pudlák [53])

$$\forall x \leq |t| \;\; \exists y \leq s \; \alpha(x,y) \rightarrow \exists w \; (\forall x \leq |t|)((w)_x \leq s \;\wedge\; \alpha(x,(w)_x))$$

où $(w)_x = w \in x$;on peut encore borner la variable w en exigeant

$$\exists w \leq t \; (s,t)$$

pour t un terme défini par

$$t(s,t) = \mathrm{borne} \; (s, 2^{|t|+1})$$

où $2^{|t|+1}$est une borne polynomiale (finie).

Nous voyons ainsi que les fragments de l'arithmétique doivent être des fragments (bornés) de l'arithmétique bornée pour parvenir à capter la notion de computabilité finie : la théorie des fonctions récursives primitives ne suffit évidemment pas, il faut définir des fonctions élémentairement computables en s'aidant, par exemple, de la notion de récursion bornée pour des fonctions $f(\vec{x})$, $g(z,\vec{x})$ et $k(y,\vec{x})$; on définit (voir [70] ; 335)

$$h(0,\vec{x}) = f(\vec{x})$$

$$h(y,\vec{x}) = \min(g(h\,\lfloor y/2\rfloor\,,\vec{x}),\vec{x}),k(y,\vec{x}))$$

où min est le plus petit élément et où $\lfloor\ \rfloor$ signifie $\frac{1}{2}y$.

Le fait que la théorie classique de la récursion soit impuissante à caractériser la notion de computabilité effective nous invite à penser que la quantification sur un ensemble infini (de nombres naturels), *i.e.* l'induction est en cause. Borner le principe d'induction revient à borner l'infini lui-même.

4.2.5 Arithmétique bornée et logique prédicative

Si l'arithmétique prédicative (de Nelson) est autoconsistante, c'est parce que les nombres dénotés par les termes de la théorie arithmétisée sont bornés par les termes eux-mêmes. L'arithmétique bornée (de Buss) possède les deux fonctions

$$|x| = \lceil \log_2(x+1) \rceil$$

pour la longueur de la représentation binaire de x et la fonction dièse

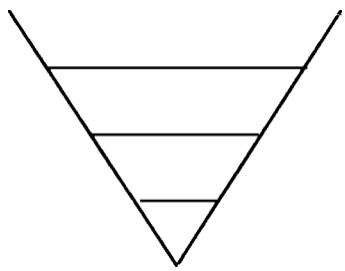
$$x\#y = 2^{\log x \cdot \log y}.$$

Rappelons que l'espace polynomial, c'est-à-dire l'ensemble des fonctions de croissance polynomiale qui peuvent être computées par une machine de Turing, admet les bornes de longueur $< p(|\vec{x}|)$où p est un polynôme et dont le temps (de computation) ne dépasse pas $2^{<p(|x|)}$. On sait que Chaitin après Kolmogorov a voulu généraliser la notion de complexité algorithmique en donnant une version « informationnelle » du premier théorème d'incomplétude de Gödel. Chaitin a produit un nombre réel aléatoire incompressible Ω qui représente la probabilité pour qu'un programme ou une machine de Turing arbitraire s'arrête et il est bien évident que cette reprise du problème de l'arrêt n'est qu'une extension (peut-être optimale) du théorème d'incomplétude et peu importe que l'on utilise la diagonalisation à la Cantor, comme

chez Gödel, ou la compression algorithmique — qui est une sorte de diagonalisation sur la complexité ou la longueur des énoncés — on dépasse les bornes de l'arithmétique polynomiale. J'ai montré (Annexe B) comment en partant de la diagonale ou le produit de convolution de Cauchy

$$\sum_{n}^{\infty} c_n x^n = (\sum_{n}^{\infty} a_n x^n)(\sum_{n}^{\infty} b_n x^n)$$

pour $c_n = a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0$,, on peut construire une arithmétique polynomiale dans laquelle la logique est traduite par la notion d'évaluateur définie de la façon suivante : un évaluateur est un entier positif qui localise la formule à laquelle il est assigné dans l'univers arithmétique



La fonction d'évaluation a la forme

$$\phi(A)[n] = 1, \text{ ssi } A_n \in \mathrm{D_n}$$

pour A une formule atomique et

$$\phi(\neg A)[n] = 0, \text{ ssi } \neg A_n \in \mathrm{D_n}$$

pour sa négation. La conjonction est traduite par $\times$, la disjonction par $+$, l'implication par une exponentiation, le quantificateur existentiel par une somme finie, le quantificateur universel par un produit fini (d'instances numériques) et finalement un nouveau quantificateur « effini » $\exists\!\!\!-x\ A(x)$ qui correspond à une suite effinie, *i.e.* avec une borne prépositionnelle mais sans borne postpositionnelle, est traduit par un produit itéré.

Cette interprétation est arithmétique, dans le sens où l'on ne déborde pas l'univers arithmétique borné par n ou par 2^n (pour un univers combinatoire). On peut aussi qualifier l'interprétation de polynomiale quand on arithmétise l'implication par un binôme de la forme

$$(\bar{a}_0 x + b_0 x)^n$$

pour $\bar{a} = 1 - a$ et une indéterminée x. Il suffit de calculer les coefficients d'un tel binôme par ses puissances décroissantes $n,\ n-1,\ n-2$ pour obtenir la suite complète des sous-formules de la formule binomiale ; on a donc ici la propriété de sous-formule de Gentzen qui permet d'éviter la superexponentiation du *Modus Ponens* ou de la formule de coupure. Le calcul sur les puissances décroissantes s'opère par la descente infinie (de Fermat) qui fait l'économie de l'induction (non bornée).

Une telle logique polynomiale est prédicative puisque le contenu polynomial des formules logiques est borné polynomialement par les termes mêmes du polynôme qu'on peut réduire finiment. Ainsi, la méthode de descente infinie dans sa forme positive qu'on peut formaliser de la façon suivante :

$$\exists\!\!\!-x\ A(x)\{([Ax \wedge \exists y\ <\ x\ A(y)] \rightarrow$$

$$\exists y\ \forall z\ <\ y\ A(z)) \rightarrow \exists z(z = 0 \text{ ou } 1)\ A(z)\} \rightarrow$$

$$\exists\!\!\!-x\ A(x)$$

avec l'arithmétique générale des indéterminées de Kronecker permet d'obtenir une preuve de consistance finitaire par une arithmétique polynomiale elle-même retraduite dans une logique arithmétique ou prédicative. Il faut donc que la logique interne de cette arithmétique soit elle-même prédicative (ou constructive) et bornée par les termes de l'arithmétique dans lesquels elle est traduite pour produire une preuve d'autoconsistance logique. La fermeture logique est alors une propriété intrinsèque d'une logique arithmétique — on trouvera dans l'Annexe B une preuve purement syntaxique qui fait l'économie de toute notion sémantique, *e.g.* univers arithmétique pour assurer le caractère finitaire de la logique arithmétique ou polynomiale.

4.3 Les bornes de l'omniscience logique

E. Bishop [6] a baptisé principe d'omniscience logique le principe du tiers exclu généralisé

$$\forall x\, P(x) \vee \exists x\, \neg P(x)$$

que Brouwer a été le premier à rejeter. Mais le principe a d'autres formes, comme celle de Parikh [87]. La relation d'accessibilité totale dans la sémantique de Kripke suppose une omniscience qui transite sur tous les mondes possibles. À l'autre extrême, le concept de nombre faisable « *feasible number* »

n'admet que l'accessibilité limitée et l'axiome principal d'un Sazonov [91] stipule que la limite est

$$\forall y(\log_2 \log_2 y < 10)$$

et donc qu'on ne peut aller au-delà de

$$2^{2^{10}} = 2^{1024} = \infty$$

L'arithmétique faisable (strictement finitiste ou encore ultra-intuitionniste) a peut-être avant tout un intérêt plus épistémologique que fondationnel. C'est ce que semble croire Parikh qui insiste sur le concept de rationalité bornée dans une théorie de la connaissance pratique dans laquelle le célèbre dilemme du prisonnier

	L	D
L	3,3	5,2
D	2,5	4,4

illustre le principe de l'équilibre de Nash d'un point de vue probabiliste et trouve son point d'application dans la théorie économique d'un agent rationnel limité. Le prisonnier loyal L (et le délateur D) ont un intérêt à ne pas trahir l'autre, mais ils ne perdent pas beaucoup à le faire, alors que le délateur gagne à agir seul. Cette situation simple n'a pas de portée mathématique, mais l'idée de rationalité bornée ou de ressources limitées a inspiré les logiciens et les philosophes. L'informatique théorique peut certainement tirer profit d'une rationalité finie d'agents interactifs tout comme le philosophe du langage ne saurait faire abstraction des capacités limitées — compétence et performance — des agents linguistiques. Mais c'est la logique interne des théories logiques et mathématiques elles-mêmes qui constitue l'enjeu fondationnel majeur. En effet, la logique classique infinitaire et l'arithmétique de Peano aussi infinitaire en vertu de la sémantique ensembliste qui leur sert de référentiel sont les deux mamelles de la science infinie, c'est-à-dire de l'omniscience qui s'étend jusqu'aux confins d'un infini dénombrable $\aleph_0$ (pour le premier ordre) et d'un au-delà non dénombrable $2^{\aleph_0}$ (pour le second ordre).

Les présupposés ontologiques de la logique et de l'arithmétique classique sont contestés par l'idée d'une logique et d'une arithmétique bornées. Des fragments de l'arithmétique à l'arithmétique prédicative et à une logique arithmétique prédicative en passant par l'arithmétique faisable, c'est à une véritable descente conceptuelle qu'est convié le logicien. Cette descente voit

défiler un paysage de plus en plus construit. L'environnement concret de l'acte constructeur du logicien invite à penser que la description des structures logiques et mathématiques (physiques, biologiques, etc ...) ne saurait reposer sur des hypothèses métaphysiques trop lourdes ou trop englobantes qui risqueraient de faire s'évaporer des généralités d'une description abstraite où s'éteint le regard. Le langage plus prosaïque du logicien constructiviste ou de l'épistémologicien cherche à creuser le sol plutôt qu'à scruter le ciel. Là sans doute réside le sens de la métaphore des fondements qui désigne une activité critique.

4.4 Conclusion

Si la théorie des modèles finis est de nature sémantique, la logique arithmétique ou logique polynomiale modulaire a un sens strictement syntaxique (ou purement arithmétique). La logique linéaire (due à J.-Y. Girard) serait d'inspiration mixte, alors que la logique positive de Yacov et Poizat sans négation mais avec une antilogie et une disjonction infinie d'ensembles vides est résolument d'origine sémantique. Selon Y. Gurevitch, la théorie des modèles finis (et métafinis) est née du besoin de se départir des structures statiques infinies en informatique théorique qui doit s'occuper d'autre part de la logique dynamique des ressources finies — pour la modélisation de langages informatiques comme PASCAL. La logique linéaire qui a aussi une vocation informatique (voir J.-Y. Girard [47]) est née de l'hybridation du calcul des séquents de Gentzen et de l'algèbre linéaire ; le calcul des séquents, fondé sur ce que Gentzen appelait le raisonnement linéaire « *lineares Räsonieren* » est le versant syntaxique, alors que le versant sémantique est la théorie des espaces linéaires ou vectoriels d'où Girard tire la notion d'espace cohérent — notion tirée de la géométrie algébrique (Grothendieck) et empruntée aussi bien par la logique catégorique (voir Gauthier [38], chap. 7.5) que par la logique positive — qui reproduit la structure d'un espace vectoriel avec addition vectorielle associative et multiplicative et multiplication scalaire. Ce sont les connecteurs propositionnels qui doivent modéliser les opérations algébriques en plus la multiplication les opérateurs modaux de la logique linéaire : ainsi la flèche linéaire $-\!\circ$ dans

$$!A-\!\circ B$$

représente l'implication matérielle $A \to B$ avec l'opérateur modal ou exponentiel ! (bien sûr A). Ces modalités doivent pallier la syntaxe appauvrie des

sous-structures du calcul des séquents de Gentzen (e.g. la règle structurale de contraction) pour dupliquer les propriétés arithmétiques de l'algèbre vectorielle en sus des opérations arithmétiques élémentaires. Il n'est pas étonnant alors que l'on doive revenir par ce détour à une logique linéaire bornée pour réintégrer le temps polynomial des ressources limitées d'une logique consumériste ! La programmation linéaire qui n'a rien à voir avec la logique linéaire comporte par ailleurs des techniques plus directes pour maximiser (dans les entiers) la distribution des biens de consommation. Au-delà ou en deçà de ses aspirations théoriques, le programme d'une logique linéaire prend au sérieux l'injonction d'une exploitation dynamique de ressources limitées sur laquelle Gurevitch a insisté, à tel point que l'on peut y voir une théorie logique de la consommation (de profits et pertes) avec tourniquet d'entrée dans les grandes surfaces de l'informatique théorique. Si la logique classique devait servir tout venant « *serving all comers* » selon le mot de Quine, la logique linéaire devrait servir tous les clients « *serving all customers* » pour continuer l'analogie ou filer la métaphore. La théorie des types n'a pas, par ailleurs, épuisé toutes ses ressources dans le proposition originale de Russell. Le calcul lambda typé avec le l'opérateur d'abstraction repris de Church, la théorie constructive ou intuitionniste des types de Martin-Löf demeurent des outils privilégiés en programmation logique. Mais ce sont là des ressources informatiques dont la nature bifide, entre syntaxe et sémantique, n'est pas parfaitement définie. En plus, leurs fondements philosophiques, dans des théories de l'abstraction ou du jugement, restent fragiles.

Une autre créature hybride est la théorie sémantique des jeux dont le lieu de naissance est la notion de jeux de dialogue « *Dialogspiele* » apparue chez Lorenzen qui voulait fournir une sémantique à la logique intuitionniste dans la lignée de la logique des problèmes de Kolmogorov pour établir un critère de constructivité dialogique (voir [79]), mais qui a été dévoyée depuis en une ludique philosophique sous des dehors logiques et mathématiques. Lorenzen appelait subjonctive « *Subjunktion* » l'implication matérielle $A \to B$ pour rendre la subordination $B \subset A$; c'est là une donnée grammaticale ou syntaxique première. D'autres joueurs sont intervenus en logique ludique ou sémantique des jeux. J. Hintikka, J. van Benthem, A. Blass, S. Abramski ont relancé la joute dialogique en ouvrant de nouvelles perspectives. Ainsi la logique computationnelle de G. Japaridze suggère une logique interne de la computation et de l'interaction entre un agent et son environnement qui renverse les rôles de la syntaxe et de la sémantique en donnant la priorité à un modèle de l'interaction machine — environnement dans une logique des

tâches qui nous ramène à Kolmogorov — où les problèmes de l'utilisateur sont résolus par les computations ou les algorithmes de la machine (voir G. Japaridze [66]). Mais ici la problématique du jeu est statique et nous perdons la dynamique des joutes qu'un Abélard disputeur adorait en des temps médiévaux où la « *disputatio* » tenait lieu de dialogue et où le dynamisme de la dialectique supplantait la logique statique d'un Aristote immobile ou impassible. L'interaction entre automates finis alternants — duo d'automates dans un état fini — est peut-être la syntaxe primitive de toute interaction, comme le suggère M. Vardi. De nouveau ici, c'est l'arithmétique qui fait bouger la logique, puisque la machine calcule, alors que le logicien ne fait que réfléchir ...

Chapitre 5

Conclusion. Arithmétisme

La question centrale de la théorie de la computabilité est le problème de la décision « *Entscheidungsproblem* » comme Hilbert l'avait désigné. Une méthode de décision pour un système formel S consiste à déterminer en un nombre fini d'étapes si un énoncé donné de S est un théorème ou non ; le problème de la décision pour le système formel en question est de trouver une méthode de décision pour S ou démontrer qu'une telle méthode n'est pas accessible (voir Shoenfield [93], p.106). Le problème de la décision est apparu tôt chez Hilbert comme je l'ai mentionné dans le chapitre 2 et ce n'est pas par retournement de l'histoire que j'ai fait remonter le problème à Kronecker et au motif recteur du « nombre fini d'étapes ». Ce n'est pas par hasard non plus que le constructivisme kroneckerien est revenu au devant de la scène avec l'informatique théorique. Rappelons le texte de Hilbert sur l'« *Entscheidungsproblem* », la méthode de la décision qui doit s'effectuer « en un nombre fini d'opérations » (Hilbert [59], III, p. 154). Ce que Hilbert appelle la consistance interne « *innere Widerspruchslosigkeit* » n'est accessible selon Hilbert qu'à l'aide de l'axiomatisation de la logique, qui doit déboucher en dernière analyse sur la question de la décidabilité « *Entscheidbarkeit* ». Hilbert donne ici l'exemple de son théorème de 1890 sur les invariants algébriques rationnels qui se réduisent à un nombre fini d'invariants générant le système entier ; cette preuve était « théologique » selon Gordan et Hilbert a produit une autre preuve en 1893 qui respecte le principe du nombre fini d'opérations inhérentes au calcul. Hilbert reconnaît à cette occasion sa dette envers Kronecker qui avait fourni les outils du calcul des invariants rationnels dans sa théorie des systèmes modulaires — voir Gauthier [42], pp 26 et ss. pour des précisions mathématiques et historiques. Ce qu'il importe de recon-

naître dans ce contexte, c'est la perpétuation du programme arithmétique de Kronecker — l'arithmétisation de l'algèbre —, de l'axiomatique hilbertienne jusqu'à l'arithmétisation des langages artificiels (ou machiniques).

Faudrait-il penser que le constructivisme doit devenir l'option fondationnelle obligée (automatique) de l'informaticien et du spécialiste de l'intelligence artificielle. Loin de là et de nombreux programmes logiques ne sont pas de teneur constructive de part en part. On n'a qu'à évoquer le lambda-calcul typé ou la théorie constructive (intuitionniste) de Martin-Löf pour l'implémentation informatique des langages de programmation pour reconnaître les limitations inhérentes aux systèmes logiques d'appartenance intuitionniste. Mais toutes les théories des types en informatique s'en remettent à une relation fondamentale entre preuves et programmes informatiques, l'isomorphisme de Curry-Howard qui établit une correspondance entre les formules et les types (ou domaines d'objets) d'un système formel. La programmation fonctionnelle signifie que l'on construit plus ou moins artificiellement des fonctions entre des programmes et des preuves, des propositions (énoncés) et des types qui les situent ou les hiérarchisent dans un univers ensembliste. Dans un contexte catégorique, ces fonctions deviennent naturellement des foncteurs qui traduisent ou compilent des structures ou des objets d'une catégorie à l'autre. Toutes ces constructions n'ont de constructif que le nom, même si à l'origine Curry (et Howard) avait des motifs constructivistes et intuitionnistes et la récupération abstraite d'un constructivisme concret à la Kronecker ne va pas dans ce sens. C'est peut-être du côté de l'algèbre constructive que l'on voit mieux encore la continuité du programme de Kronecker et à ce titre l'ouvrage récent de H.M. Edwards *Essays in Constructive Mathematics* [25] est un vibrant témoignage d'allégeance kroneckerienne, comme l'était d'ailleurs l'ouvrage *Divisor Theory* [23]. L'algèbre constructive, c'est l'arithmétique générale de Kronecker. Kant a été un des premiers avec Lambert à désigner l'algèbre comme arithmétique générale « *allgemeine Arithmetik* » et il ne faut pas s'étonner ici encore que le constructivisme mathématique de Kronecker à Brouwer se soit placé sous l'égide philosophique de Kant — Kant ne disait-il pas que les mathématiques sont une construction de concepts et que la philosophie est une analyse des concepts ?

Si la théorie des démonstrations ou la métamathématique de descendance hilbertienne est de l'arithmétique pour logiciens et la théorie des modèles de descendance tarskienne est de l'algèbre pour logiciens, comme j'ai tenté de le montrer, on pourrait sans doute supposer que l'algèbre constructive est l'arithmétique de la logique informatique ou algorithmique. Edwards in-

siste en effet après Weyl sur le caractère fini des algorithmes de l'algèbre constructive. Un bel exemple de l'algèbre informatique est la notion de base de Gröbner qui en tant qu'organe générateur d'éléments primitifs dans un anneau de polynômes fournit des algorithmes finis pour la division euclidienne des plus grands diviseurs communs ou pour l'élimination gaussienne dans la théorie des matrices ou encore pour la programmation linéaire intégrale où les variables d'un programme sont des entiers. Ce n'est plus la représentation logique (abstraite) des programmes informatiques qui est à l'avant-garde ici, mais leur implantation symbolique (concrète). Ce qui est sûr en algèbre computationnelle, comme en algèbre constructive, c'est que l'on échappe au tiers exclu dans les opérations du calcul finitaire, mieux que la logique intuitionniste ou constructive entendue au sens large — voir là-dessus l'Annexe A.

Le constructivisme strict que j'affuble du néologisme « arithmétisme » pour faire pendant au logicisme est une théorie fondationnelle critique de la pratique mathématique. L'hypothèse de départ consiste à dire que la pratique mathématique (et logique) est une activité constructive ou l'activité d'un agent constructeur : cette pratique est expérimentale dans le sens où c'est l'expérience constructive du mathématicien ou du logicien et de l'informaticien qui détermine le statut des constructions ou des objets de l'expérience mathématique. Une thèse philosophique, le pragmatisme, conviendrait sans doute pour caractériser cette attitude pratique. Frege accusait Kronecker (avec Helmholtz) d'empirisme sans doute parce qu'ils prônaient tous deux une approche expérimentale de la pratique mathématique dans une démarche du pas à pas qui ne permettait pas de saut ou de détour dans la production des vérités mathématiques. La voie directe, sans le secours du tiers exclu ou des méthodes transcendantes, est sans doute le trait principal du constructivisme logicomathématique. Kronecker pensait que sa théorie des fonctions rationnelles pour les quantités algébriques récupérait les nombres irrationnels algébriques tout en repoussant les nombres transcendants hors du domaine de l'algèbre, mais leur conservant une espèce de légitimité dans la région limitrophe des approximations rationnelles. Et si la pratique est concrète, la théorie ne peut être que générale et abstraite de quelque façon du contexte de la computation réelle. Les résultats négatifs sur la question de la décidabilité n'enseignent pas autre chose : faire progresser le plus loin possible le règne du décidable jusqu'à la frontière du non décidable, sans pour autant admettre que l'indécidable puisse se réfugier au coeur de l'arithmétique par des détours qui transcendent le royaume des nombres et du calcul.

C'est sans doute pour cette raison qu'André Weil qui pratiquait la descente (in)finie dans les corps finis jugeait que la méthode diagonale responsable des phénomènes d'incomplétude n'avait pas sa place en théorie des nombres. Cela ne signifie pas non plus que seules les méthodes constructives sont admissibles chez la reine des sciences mathématiques, comme la désignait Gauss. Les méthodes analytiques y ont bien sûr droit de cité, quand ce ne serait qu'à titre temporaire, comme le voudrait ce que j'ai appelé la conjecture de Herbrand, puisque la motivation profonde de l'arithméticien est de retrouver la part constructive de toute preuve en théorie des nombres. Cette part constructive, il est vrai, est souvent cachée loin dans la tectonique des nombres et la géométrie algébrique contemporaine travaille très fort à dégager les bas-fonds arithmétiques de la géométrie transcendante, e.g. la conjecture de Langlands (voir Langlands 1976) qui témoigne de la permanence de l'idéal arithméticien d'un Kronecker qui ne voulait rien concéder au ciel platonicien des idéalités.

Sur le plan philosophique, Poincaré s'est opposé au logicisme et il ne serait pas faux de lui attribuer l'appellation d'« arithmétiste » en vertu de son insistance sur la priorité du principe de récurrence (ou induction mathématique) au-delà ou en deçà de toute entreprise logique. Son contemporain philosophe, Léon Brunschvicg, récusera aussi bien le logicisme et pourra apparaître comme un défenseur de l'arithmétisme dans son ouvrage *Les étapes de la philosophie mathématique* (1912). Brunschvicg, inspiré par l'arithmétisme cartésien, influera par son idéalisme qu'il appellera constructif sur toute la tradition française de la philosophie des mathématiques, Bachelard, Lautman, Cavaillès, Poirier, Desanti. Herbrand le premier échappera à cette influence et se tournera vers Hilbert, dont le finitisme est aussi d'essence arithmétique.

Le logicien constructiviste, qui relaie l'arithméticien dans la recherche d'une logique interne de l'arithmétique, ne saurait se satisfaire des dogmes d'une orthodoxie classique qui relègue les visées constructivistes à la marge de l'actualité mathématicienne et logicienne. L'avènement de la méthode forte de l'informatique théorique a cependant changé la donne, si bien que les constructivistes qui conçoivent comme Bishop une mathématique à contenu numérique n'ont pas perdu espoir de voir triompher à la longue le point de vue de la rigueur et de faire partager par les autres disciplines mathématiques la certitude de l'arithmétique, comme Poincaré le disait à propos de Kronecker et Weierstrass, tous deux épousant, comme nous l'avons vu, le projet de l'arithmétisation, de l'analyse pour l'un, de l'algèbre pour l'autre.

L'arithmétisation de la logique commence avec Hilbert, mais elle n'a jamais cessé d'occuper l'esprit du logicien jusqu'à nos jours en passant par Skolem, Herbrand, Gödel, Tarski jusqu'à Feferman, Nelson et l'informatique théorique. L'intuitionnisme de Brouwer, même si ce dernier ne s'est pas intéressé à la théorie des nombres, a introduit l'arithmétique au sein même d'un continu en devenir par le moyen de la théorie des suites — dont le noyau est la suite des nombres naturels.

Que l'arithmétisation de la logique débouche sur une logique arithmétique, une logique interne de l'arithmétique, c'est là un motif personnel que j'ai tenté d'harmoniser avec les autres motifs du présent ouvrage. Si la théorie des nombres ou l'arithmétique a pour méthode principale la descente infinie de Fermat comme substitut de l'induction complète ou transfinie et si la consistance de cette méthode constructive doit être assurée à l'intérieur de l'arithmétique, alors l'arithmétique polynomiale de Kronecker comme théorie constructive de l'arithmétique générale qui englobe l'arithmétique des nombres naturels doit exhiber de façon naturelle les ressources constructives qui permettent de démontrer la consistance interne de l'arithmétique ordinaire. Or la théorie polynomiale de Kronecker enveloppe la théorie de la divisibilité (les systèmes modulaires) et du corps des rationnels, domaine de rationalité ou « *Rationalitätsbereich* », où la descente infinie trouve son régime normal en tant qu'algorithme euclidien généralisé. La logique arithmétique ou la logique polynomiale modulaire n'est que la mise en évidence de cette logique interne d'une arithmétique auto-consistante. La preuve de la consistance interne de l'arithmétique (voir l'Annexe B) s'effectue à l'aide de moyens purement arithmétiques et le rôle de la logique se limite à définir le cadre formel de la démarche démonstrative. Intuitivement, l'arithméticien et le mathématicien constructivistes n'ont jamais douté de la consistance de l'arithmétique comme fondement de l'édifice des mathématiques. La logique n'a ici qu'une fonction ancillaire, comme l'avait bien compris Hilbert, mais cette servante des mathématiques a pour seule maîtresse la certitude qui naît du calcul, c'est-à-dire de l'arithmétique et de ses extensions qui préservent sa consistance interne à la lumière de ses avancées constructives.

La logique interne de l'arithmétique, son moteur inférentiel, repose sur les opérations arithmétiques elles-mêmes. Ce qu'il faut faire, c'est traduire directement les opérateurs logiques dans leur correspondant arithmétique comme suit :

$$\begin{array}{lcl} a \wedge b & := & a \cdot b \\ a \vee b & := & a + b \\ a \rightarrow b & := & \bar{a} + b \\ \neg a & := & \bar{a} \text{ pour } 1 - a \\ \exists x & := & \sum(a_1, a_2, a_3, \ldots, a_n) \\ \forall x & := & \prod(a_1, a_2, a_3, \ldots, a_n) \\ \dot{\exists} x & := & \prod(a_1, a_2, a_3, \ldots, a_n, \ldots) \end{array}$$

pour $\dot{\exists}$ le quantificateur « effini » qui ne s'applique qu'aux suites (de nombres naturels) illimitées. Il faut traduire de nouveau les opérations arithmétiques dans l'arithmétique polynomiale modulaire e.g. pour le *Modus Ponens*, on a :

$$1 - a_0 x \equiv b_0 x \pmod{a_0 x}$$

pour $a_0 x$ et $b_0 x$ des monômes, ce qui permet de plonger ou d'immerger la logique dans un univers arithmétique expansif par un procès en devenir « *ein Prozess im Werden* », selon l'expression de Brouwer. L'idée de représenter la logique dans l'arithmétique (polynomiale) est inspirée par le constructivisme finitaire de Kronecker, mais elle est surtout l'aboutissement à mes yeux du processus d'arithmétisation de l'analyse, de l'algèbre, de la logique et finalement des langages artificiels ; la forme que doit prendre cette idée évolue elle-même et il serait téméraire de prédire l'avenir d'une arithmétisation « totale ». Il ne s'agit pas en effet de la reproduction mécanique en bits ou en qubits (bits quantiques) de l'information, qui n'est pas une représentation ou une interprétation arithmétique, mais une simple transcription électronique des messages codés en notation arithmétique. On ne fait pas de mathématiques ou de logique en binaire, on n'arithmétise ni n'algébrise, on ne fait qu'abréger un code de transmission des données. Mais il est aussi question d'écriture en logique arithmétique et là aussi les styles évoluent dans la multiplicité des options fondationnelles, puisque c'est bien de fondements qu'il s'agit en dernier ressort.

La théorie fondationnelle n'est pas « fondamentaliste », c'est une théorie critique de la pratique et la théorie constructiviste ne vise qu'à définir le socle minimal de la pratique constructive logicomathématique. Si la théorie est toujours guidée par l'idéal hilbertien de la certitude « *Sicherheit* » des constructions mathématiques, la pratique remonte à la mathématique grecque et trouve son accomplissement dans l'entreprise kroneckerienne en passant à travers l'histoire de la théorie des nombres et de l'algèbre (et de

l'analyse avec Cauchy et Weierstrass) de Fermat et Gauss jusqu'à Kummer et Kronecker. Kronecker est un point d'arrivée et en même temps un point de départ. Il n'a pas connu l'avènement de la logique en mathématiques qui devait être le fait de son élève Hilbert. Un autre élève de Kronecker, Cantor, a cependant orienté la théorie fondationnelle dans un autre sens que le constructivisme finitaire qu'avait conçu Kronecker. Mais l'arithmétisation progressive de la logique au XXe siècle et la naissance de l'informatique théorique donnent une nouvelle vigueur à l'option constructiviste qui promeut la logique arithmétisée : la logique arithmétique est le nom de ce programme. C'est là un programme qui s'ouvre sur la multiplicité des logiques qu'elle ordonne selon leurs exigences de constructivité et sur la variété des savoirs qu'elle organise dans le déploiement des gestes d'un agent constructeur qui doit rester dans l'ombre de ses propres constructions.

Annexe A

La descente infinie, l'induction transfinie et le tiers exclu [1]

La plupart des mathématiciens et des logiciens qui n'ont pas de penchant constructiviste et les philosophes, lorsqu'ils connaissent un peu de logique ou de mathématiques, ont tendance à identifier l'induction complète et la descente infinie. Parmi eux, C. S. Peirce est une exception, puisqu'il considérait la méthode de la descente infinie de Fermat comme « le plus grand exploit que l'esprit humain ait jamais accompli ». Peirce a lui-même employé la descente infinie pour faire la distinction entre une collection dénombrable — « *numerable* » est le terme qu'il utilisait — et une collection non dénombrable (« *innumerable* »). Il a même écrit à Cantor pour lui faire savoir que l'inférence fermatienne, dans ses termes, n'était pas équivalente à ce qui était selon lui improprement désigné comme « *vollständige Induktion* » ou induction complète (Eisele [27]). Peu ont eu la perspicacité de Peirce en ce domaine.

Parmi les mathématiciens, ce sont surtout les praticiens de la théorie des nombres qui font la distinction, mais ils préfèrent donner des exemples plutôt qu'une justification fondationnelle ; c'est le cas de Yves Hellegouarch dans son ouvrage *Invitation aux mathématiques de Fermat-Wiles* (Hellegouarch [55]).

André Weil, le grand théoricien des nombres, est plus explicite. Weil a eu recours à la descente infinie dans ses travaux sur l'arithmétique des courbes algébriques où une courbe elliptique dans tout corps fini n'a qu'un nombre

1. Ce texte est d'abord paru dans la revue *Dialogue*, vol. 48, no. 1 (mars 2009), pp, 1-17.

fini de points rationnels. Ici Weil s'est appuyé sur le résultat de Mordell qui a utilisé la méthode de la descente infinie pour la conjecture de Poincaré sur les propriétés arithmétiques des courbes algébriques. Poincaré parlait d'un « nombre fini d'hypothèses » pour caractériser la descente infinie alors que Weil met l'accent sur la procédure de décomposition ou réduction dans les corps finis : la descente infinie opère dans tout corps fini de nombres (idéaux ou polynômes) où le produit de deux entiers ordinaires (ou algébriques) est égal à une puissance donnée (ou degré) et leur plus grand diviseur commun s'obtient par descente finie ; c'est le cas, en particulier, pour les corps quadratiques $Q(\sqrt{N})$ des formes quadratiques binaires de discriminant N. (Weil [107] pp. 335-336).

C'est cette version de la descente infinie — qu'on pourrait caractériser comme algorithme euclidien généralisé — qui m'apparaît la plus fidèle à l'esprit fermatien et c'est à elle que je me référerai dans la suite.

Les logiciens quant à eux ont voulu identifier la descente infinie avec l'induction transfinie sur les ordinaux jusqu'à ϵ_0, la limite de la deuxième classe de nombres de Cantor :

$$\lim_{n\to\infty} \omega^{\omega^{\cdot^{\cdot^{\omega}}}} \Big\} \; n = \epsilon_0$$

Hilbert a aussi eu recours à une forme de la descente infinie dans sa procédure de réduction pour l'élimination de son symbole epsilon comme fonction de choix transfinie, mais Gentzen n'a vu dans la descente infinie qu'une forme déguisée de l'induction complète. Dans ses tentatives répétées pour justifier l'induction transfinie, qu'il tenait pour équivalente à l'induction complète, Gentzen a thématisé la notion d'accessibilité (« *Erreichbarkeit* ») pour les ordinaux (Gentzen [46]). Sa preuve de consistance pour l'arithmétique de Peano repose essentiellement sur l'emploi du principe ou du postulat de l'induction transfinie ou règle ω, comme on dit maintenant, et s'il relègue le principe au rang de théorème dans la seconde version de sa preuve de consistance, c'est que le déguisement de la descente infinie en induction complète se fait sous le couvert d'un calcul des séquents où le tiers exclu et l'élimination de la double négation apparaissent naturels dans le calcul LK. Malgré tous ses efforts pour conserver des principes constructifs, ou des inférences constructivistes, comme il dit, Gentzen n'a pas réussi à légitimer l'induction sur les ordinaux transfinis. Takeuti (Takeuti [96]) par exemple, a tenté de formuler une version récessive ou descendante pour la notion d'accessibilité de Gentzen, mais j'ai montré (Gauthier [42]) que cette descente n'était pas uni-

forme ou qu'il n'y a pas de récessibilité uniforme pour les ordinaux transfinis, contrairement à la descente infinie dans les corps finis.

On ne peut mettre en doute le caractère de méthode constructive de la descente infinie. Fermat disait que la descente est infinie ou indéfinie. En réalité, la descente doit être finie, puisque d'un nombre naturel (ou ordinal) arbitraire n, il ne peut y avoir régression à l'infini et la descente s'arrête nécessairement à 1 ou 0, si l'on prend 0 comme premier ordinal. Gentzen insistait sur l'interprétation potentialiste de la notion d'accessibilité et il voulait imaginer une traversée (« *Durchfahren* ») des ordinaux transfinis jusqu'à , qui est toujours dénombrable, d'après la doctrine ensembliste. Mais Aristote, philosophe de l'infini potentiel entre autres choses, contredit Gentzen sur ce point dans sa *Physique* en disant que l'infini ne peut être traversé (« $\alpha\delta\iota\epsilon\xi\iota\tau\eta\tau o\varsigma$ ») : il n'y a pas de chemin hors du fini — il faut le construire !

Gentzen a tenté de « potentialiser » l'infini actuel à l'aide d'un calcul finitaire dans la continuité du programme de Hilbert. Ce faisant, il oublie que l'arithmétique ensembliste de Peano n'est pas la théorie des nombres où il n'y a pas de ω comme limite de la suite illimitée (effinie) des nombres naturels ou encore de limite de la suite illimitée des nombres premiers. L'arithmétique ensembliste de Cantor, Dedekind et Peano abrite trop d'ordinaux et il y a plusieurs échelons manquants dans l'échelle qui permet de descendre de ϵ_0 à 0. L'univers actualiste de cardinalité $2^{\aleph_0}$ pour l'arithmétique de Peano du second ordre est certainement mieux rempli que le modèle standard du premier ordre de l'arithmétique de Peano, mais il y a encore plus d'entités dans ce ciel platonicien que dans le monde constructible où le tiers exclu est exclu, la décidabilité est limitée et le choix est fini.

Dans l'exercice qui suit, je veux montrer que l'induction complète (IC), l'induction transfinie (IT), la descente infinie (DI) et le principe du plus petit nombre (PPN) sont des principes équivalents du point de vue de la logique classique si l'on veut payer le plein prix du tiers exclu via la double négation pour un ensemble infini dénombrable. Je montrerai aussi que la logique intuitionniste, si elle rejette l'équivalence de l'induction transfinie avec le principe du plus petit nombre, nonobstant le rejet intuitionniste du tiers exclu, ne parvient pas à justifier l'équivalence qu'elle maintient toujours entre induction transfinie et descente infinie.

A.1 L'intuitionnisme et le tiers exclu

La logique intuitionniste (BHK pour Brouwer, Heyting et Kolmogorov) rejette en principe le tiers exclu. Dès 1923, Brouwer publie son célèbre article sur « La signification du principe du tiers exclu en mathématiques, spécialement dans la théorie des fonctions » (Brouwer [12]). Ce que Brouwer appelle le principe de réciprocité de l'espèce (ensemble) complémentaire

$$\forall x(\neg\neg Ax \to Ax)$$

ou principe de décidabilité globale pour un prédicat P

$$\forall x(Px \vee \neg Px)$$

diffère essentiellement du principe de testabilité ou décidabilité « locale »

$$\neg A \vee \neg\neg A$$

pour un élément construit $x_0 = x$ ou suite de ces éléments. Ce principe ne peut s'appliquer indifféremment aux ensembles (espèces) finis et infinis — les espèces au sens intuitionniste sont des collections de propriétés. Seule la double absurdité peut redonner un sens à la négation

$$\bot\bot a \leftrightarrow a$$

dans le fini, ce qui veut pas dire que ce qui est doublement absurde a du sens ! Puisqu'une espèce (collection de propriétés) est ou bien finie ou bien infinie, c'est dans les espèces infinies — pour Brouwer, par exemple, l'espèce infinie des points du continu — que le tiers exclu ne peut s'appliquer. C'est ainsi qu'il critique le théorème de Bolzano-Weierstrass qui affirme que toute espèce infinie bornée de points possède un point limite. Les contre-exemples que Brouwer produit alors n'ont pour effet que de montrer l'inapplicabilité du principe du tiers exclu en analyse (théorie des fonctions) intuitionniste. On peut trouver aujourd'hui dans l'analyse infinitésimale lisse un semblable rejet du tiers exclu, la logique interne de l'analyse infinitésimale lisse étant intuitionniste du point de vue de la théorie des topoi. Il est intéressant de noter que l'analyse infinitésimale lisse est un autre nom pour la géométrie différentielle synthétique dont on trouve les linéaments chez Fermat. Les petits infinis (les infinitésimaux) seraient plus réfractaires au tiers exclu que les grands infinis (les alephs), à moins que l'on plonge les premiers dans

une analyse non standard et les seconds dans une théorie des ensembles où l'hypothèse du continu vient se noyer.

Kolmogorov en 1925 dans son texte « Sur le principe *tertium non datur* » (Kolmogorov [70]) abonde dans le même sens dans sa théorie des jugements finitaires. Ce qui est obtenu par la double négation est une pseudo-vérité (*psevdoistinosti*) dans la logique des jugements de la pseudo-mathématique et le principe du tiers exclu comme la dualité booléenne $\neg\neg Ax \rightarrow Ax$ n'a de validité que dans le fini.

Si Kolmogorov avant Gödel a proposé une traduction (*la traduction négative*) des mathématiques classiques ou pseudo-mathématiques dans la mathématique intuitionniste de la double négation $A \rightarrow \neg\neg A$, cette traduction est à sens unique, à l'aller seulement, puisqu'elle n'est plus fidèle au retour. Kolmogorov montre bien que les pseudo-mathématiques font un usage illégitime du principe du tiers exclu. Il montre en plus que l'induction transfinie repose en réalité sur une application illégitime du principe du tiers exclu ou de la double négation à des collections infinies. Si Kolmogorov a anticipé la logique de Heyting et la traduction négative de Gödel, c'est en supposant que l'on peut traduire la logique classique en logique intuitionniste ou ce qu'il appelle les pseudo-mathématiques en mathématiques de la vérité, mas pas inversement. Autrement dit, la traduction négative n'est pas un billet aller-retour.

Par ailleurs si S. Artemov [3] a tenté un retour dans une sémantique constructive pour BHK en reprenant la logique des problèmes de Kolmogorov avec le vocable de logique des preuves — (*logic of proofs*) sous forme de polynômes —, ce n'est pas une logique polynomiale qu'il propose, mais une interprétation standard de la logique propositionnelle intuitionniste dont le mérite est restreint puisqu'elle se limite à donner une version classique du calcul de la prouvabilité de Gödel dans le système $S4$ de la logique modale. Même si ce dernier calcul est birectionnel d'après les résultats de Gödel, McKinsey et Tarski, c'est-à-dire dans les deux sens $\vdash$ et $\dashv$ pour la déduction, il n'est pas fidèle à la source intuitionniste ; la logique des preuves d'Artemov produit une sémantique constructive ou plutôt une sémantique des constructions pour le calcul $S4$ avec opérateur de réflexion où la prouvabilité devient un foncteur de projection oublieux (*forgetful functor*) de son origine, ce qui signifie que le retour à la logique de départ intuitionniste n'est pas assuré. À preuve la logique des preuves ne fait que rendre explicite le passage d'un problème (syntaxe) à sa solution (sémantique de la preuve) dans un cadre classique : l'intérêt de l'entreprise est plutôt épistémique que fondationnel.

Un autre mathématicien, E. Bishop (Bishop [6]), l'a compris qui a baptisé de principe d'omniscience le tiers exclu sous sa forme

$$\neg\forall x\ Ax \to \exists x\ \neg Ax$$

D'autres mathématiciens, les semi-intuitionnistes français, l'ont aussi compris. Lebesgue, Borel et Poincaré — et avec eux les prédicativistes de Hermann Weyl à Edward Nelson — abhorrent les ensembles infinis (non dénombrables). Pourtant, Brouwer a critiqué cette École de Paris en montrant que l'intégrale de Lebesgue repose sur la notion de mesurabilité où l'on a un nombre réel r avec $r = 0$, $r > 0$ ou $r < 0$, ce qui n'est pas possible si l'on n'emploie pas le principe du tiers exclu, c'est-à-dire si l'on ne suppose pas que le continu linéaire forme un ensemble ordonné de points.

Enfin, le finitisme de Hilbert et Skolem jusqu'à Wittgenstein devrait en principe n'admettre le tiers exclu que dans les situations logiques et mathématiques où l'infini (actuel) est effectivement exclu. Si Brouwer n'a pas toujours été clair sur le rejet de l'infini dénombrable (ω pour les nombres naturels et ω^2 pour les paires de nombres naturels) tout en trouvant absurde d'admettre des cardinalités non dénombrables $> \aleph_0$, la postérité logicienne de Brouwer, de Heyting à Troelstra et Kreisel, n'a pas toujours été claire elle non plus sur les principes. Alors que Brouwer insistait sur les suites infiniment processives (ou effinies) ou les suites de choix, les successeurs de Brouwer semblent admettre sans réserve l'ensemble $\aleph_0$ des nombres naturels, l'induction complète avec le postulat d'induction de Peano et l'induction transfinie en plus de sa prétendue équivalence avec la descente infinie. Voyons ce qu'il en est.

A.2 Principes d'induction

Voyons d'abord les formulations classiques de divers principes d'induction.

1. Postulat d'induction de Peano au premier ordre

$$\text{(PIP)}\quad \forall x Ax(A0 \to (\forall x Ax \to ASx)) \to \forall x Ax$$

— on remplace A par X (pour sous-ensembles) pour obtenir le postulat de Peano au second ordre.

2. Axiome de l'infini dans Z-F (correspond à PIP au deuxième ordre)

$$\text{(AI)} \quad \exists x(\oslash \in x \wedge \forall y(y \in x \to y \cup \{y\} \in x))$$

— c'est la formulation originale de Peano dans *Opere scelte* (Peano [88])
3. Induction complète

$$\text{(IC)} \quad \forall x(\forall y(y \prec x)Ay \to Ax) \to \forall x Ax$$

4. Induction transfinie

$$\text{(IT)} \quad \forall \sigma[(\forall \tau)(\tau \prec \sigma)A(\tau, \sigma) \to A(\sigma, x)] \to \forall \sigma A(\sigma, x)$$

— pour σ et τ des ordinaux.
5. Principe du plus petit nombre

$$\text{(PPN)} \quad \exists y Ay \to \exists y(Ay \wedge \forall z(z \prec y)\neg Az)$$

6. Descente infinie (ensembliste)

$$\text{(DIE)} \quad \forall x(Ax \to \exists y(y \prec x)Ay) \to \forall x \neg Ax$$

Par transformations successives (équivalences ou tautologies classiques), j'ai

$$\forall x \neg Ax \vee \exists y Ay$$

et

$$(\neg \forall x \neg Ax \wedge \neg \exists y Ay) \vee \forall x \neg Ax$$

et par

$$(\neg \forall x \neg Ax) \leftrightarrow \exists x Ax$$

j'obtiens

$$\forall x \neg Ax \vee \exists x Ax$$

i.e. le tiers exclu (ou principe d'omniscience de Bishop).

Pour cette raison, 3, 4, 5 et 6 sont équivalents au point de vue classique par contraposition (ou encore par voie indirecte), 5 et 6 ne le sont pas du point de vue intuitionniste, puisqu'il faudrait

$$\forall x Ax \leftrightarrow \neg \exists x \neg Ax,$$

mais le passage de

$$\neg\exists x\neg Ax \to \forall x Ax$$

est interdit en intuitionnisme, bien que 3 et 6 soient considérés comme équivalents, puisque l'on accepte le postulat d'induction de Peano. Si la règle de Markov permet le passage

$$\text{(RM)} \quad \neg\neg\exists x A(x,y) \to \exists x A(x,y),$$

c'est bien parce que Kolmogorov n'avait accepté le tiers exclu que pour les jugements finitaires, alors qu'il avait reconnu dans sa théorie de la *psevdoistinosti* ou pseudo-vérité que l'induction transfinie comportait le tiers exclu (Kolmogorov [70], pp. 666-667). Remarquons ici que *psevdo-istinosti* signifie littéralement vérité fausse, une belle *contradictio in terminis*. Les pseudo-mathématiques auraient-elles une logique interne dialectique ?

En toute logique intuitionniste, on devrait donc rejeter l'identification du principe d'induction transfinie avec le principe de la descente infinie parce que cette équivalence correspond à une double négation sur l'ensemble infini dénombrable ω des nombres naturels (ou des ordinaux $\omega < \epsilon_0$).

La raison de cette inconséquence dans les principes intuitionnistes tient bien sûr à la notion d'ensemble infini et à sa carence en constructivité. Les nombres naturels sont bien ordonnés dans leur suite illimitée, mais lorsque l'on veut en tirer un principe général, on s'engage dans une sémantique ensembliste.

Le principe du bon ordre dit

$$\forall S \subseteq \mathbb{N}(S \neq 0 \wedge Ax(x \in S)) \to (\exists y < x \ \wedge \ y \in S),$$

c'est-à-dire qu'il existe une suite strictement décroissante pour tous les éléments des sous-ensembles de l'ensemble $\mathbb{N}$ des nombres naturels, ce qui revient à la descente infinie ensembliste ou au principe du plus petit nombre tout aussi ensembliste et imprédicatif. La version prédicative du principe du plus petit nombre exige un quantificateur borné, comme le montre Nelson dans son ouvrage *Predicative Arithmetic* (Nelson [85]) et la version sans quantificateur de l'induction transfinie (IT) dans la preuve de Gentzen n'évite pas plus le tiers exclu puisqu'elle recourt à un bon ordre sur ω équivalent à la règle ω ou à l'induction complète sur $\mathbb{N}$ ou encore à la descente infinie au sens ensembliste.

Même une théorie bien intentionnée comme la théorie constructive (ou intuitionniste) des types de Martin-Löf, tout en voulant être prédicative, recouvre le tiers exclu par des moyens détournés via l'induction transfinie. L'ascension à petits pas de l'induction transfinie sans quantificateur veut qu'une traversée virtuelle — Gentzen disait potentielle — des omégas se rende jusqu'à ϵ_0 ; mais une fois arrivé au sommet du premier oméga ω on ne peut redescendre sans faire de faux pas ...

Voyons de façon plus précise ce que peut être une induction transfinie sans quantificateur où l'on doit recourir à une règle d'induction infinie ou règle ω qui remonte à Hilbert, mais qui a été systématiquement employée par Schütte (Schütte [92]). La règle ω stipule que si on a démontré une formule $A(x)$ pour tous les nombres naturels, on peut conclure $\forall x A(x)$, alors que l'induction transfinie non quantifiée suppose que l'on a obtenu $A(x)$ pour A sans quantificateur en parcourant un à un les ordinaux dans un ordre récursif primitif jusqu'à ϵ_0. La procédure suppose bien évidemment que l'on a parcouru tous les ordinaux finis jusqu'à ω avec une règle d'inférence pour chaque instance numérique n. Pour transformer l'induction transfinie en descente infinie ici, il suffit de supposer $\neg A(x)$ qui donne $\forall x \neg A(x)$ dans un bon ordre récursif, c'est-à-dire dans une suite strictement décroissante d'ordinaux pour arriver à une contradiction et la preuve est obtenue par *reductio ad absurdum* dans la descente infinie ensembliste

$$\text{(DIE)} \quad \forall x(Ax \to \exists y(y \prec x)Ay) \to \forall x \neg Ax.$$

Par la double négation pour $A = (0 \neq 1)$ et $\neg A = \neg(0 \neq 1)$, on obtient une preuve indirecte de la consistance de l'arithmétique de Peano. On voit à l'évidence que cette descente n'a rien d'une descente finie, le bon ordre ou l'échelle ordinale de type d'ordre ω servant en quelque sorte de marchepied à l'échelle ordinale de type d'ordre ϵ_0.

Dans sa version constructive, la méthode de la descente infinie a recours à la suite illimitée de terme général x_n, comme on dit en bourbaki, pour exprimer la quantification effinie ou illimitée

$$\exists x_n A x_n$$

pour un prédicat A et un « terme général » arbitraire.

On a alors deux versions, positive et négative, de la descente infinie :
7a. Descente infinie (positive)

$$\exists x\{([Ax \wedge \exists x(y \prec x)Ax] \rightarrow \exists y Az(z \prec y)Az) \rightarrow$$
$$\exists z(z = 0 \vee 1 \vee n)Az\} \rightarrow \exists x Ax$$

7b. Descente infinie (négative)

$$\exists x\{[Ax \wedge \exists y(y \prec x)Ay] \rightarrow \exists y \exists z(z \prec y)Az\} \rightarrow \exists x \neg Ax$$

Il ne s'agit pas ici de quantification bornée $\forall x_{x<y}$ ou $\exists x_{x<y}$, mais de quantification indéfinie sur une suite (ou sous-suite) arbitraire de nombres naturels.

La théorie des nombres classique de Fermat à Kronecker (arithmétique FK pour Fermat-Kronecker) en passant par Euler, Gauss, Lagrange, Legendre, Dirichlet, Kummer jusqu'à Mordell et Weil en géométrie arithmétique contemporaine, l'algèbre computationnelle (e.g. la théorie des bases de Gröbner) ou la théorie algorithmique (en informatique théorique) ou plus généralement encore, la théorie de la divisibilité (l'arithmétique modulaire) dans les corps finis, ne procèdent pas autrement. Dans cette perspective, la descente infinie est bien plutôt un algorithme euclidien généralisé qu'une méthode de preuve indirecte ou une réduction à l'absurde. Dans tous les cas, pour des prédicats numériques A, on a la descente

$$\begin{array}{c} Ax_n \\ Ax_{n-1} \\ \vdots \\ Ax_{n-(n-1)} \\ Ax_0 = Ax_{n-n}. \end{array}$$

C'est ainsi que la descente infinie ou indéfinie dans les termes de Fermat est en réalité une descente finie et ce n'est qu'après la descente que nous savons que $\neg(0 = 1)$. C.Q.F.D.

La voie directe nous donne

$$(0 \neq 1)$$

et la voie indirecte (*reductio ad absurdum*)

$$\neg\neg(0 \neq 1) \rightarrow (0 \neq 1)$$

ce qui est légitime ici, puisque nous sommes « descendus » dans le fini.

La morale de cette histoire, c'est que nous n'avons pas besoin de la notion d'ensemble infini de nombres naturels pour effectuer la descente « naturelle » (ou polynomiale) dans l'arithmétique de FK, pas plus que dans sa preuve sur l'infinitude des nombres premiers Euclide n'avait eu besoin de la notion d'infini (actuel).

La plupart des logiciens, qui veulent pourtant faire la théorie de la pratique mathématique, n'ont pas su apprendre cette leçon ou la retenir s'ils l'ont jamais apprise. Voyons maintenant si la logique intuitionniste peut justifier l'équivalence entre induction complète, induction transfinie et descente infinie.

A.3 La logique intuitionniste et l'induction transfinie

En logique (et mathématiques) classique, le principe du plus petit nombre (PPN) est équivalent à l'induction transfinie sur l'ensemble des ordinaux finis

$$\text{(PPN)} \quad \exists x Bx \to \exists x(Bx \wedge \forall y < x \, \neg By)$$

Il suffit de substituer $\neg Bx$ à Bx pour obtenir par contraposition

$$\text{(IT)} \quad \forall y[\forall x < y Ax \to Ay] \to \forall x Ax.$$

Du point de vue intuitionniste, PPN implique le tiers exclu pour l'arithmétique de Heyting (je suis ici Troelstra et van Dalen [101]).

Supposons que j'ai un prédicat A tel que

$$Ax = \begin{cases} 0 \wedge P \\ 1 \wedge \neg P \\ n \end{cases}$$

J'ai $\exists x Ax$; si j'avais un plus petit y tel que Ay et $y = n$, alors $\neg A0$, $\neg A1$, d'où $\neg(0 = 0 \wedge P)$ et $\neg(1 = 1 \wedge \neg P)$, ce qui donne $\neg P$ et $\neg\neg P$ (contradiction). Si $y = 0$, j'ai P et si $y = 1$, j'ai $\neg P$.

Le logicien intuitionniste a cependant un dernier recours par le principe de Markov

$$\neg\neg \exists x A(x, y) \to \exists x A(x, y)$$

et peut donc affirmer avec la double négation sur le quantificateur existentiel

$$\neg\neg[\exists x Ax \rightarrow \exists x(Ax \wedge \forall y < x\ \neg Ay)].$$

Du point de vue de la théorie des démonstrations (dans ce cas le calcul des séquents de Gentzen), on dira que le quantificateur universel est isolé des instances positives du quantificateur existentiel et de la disjonction (condition de Mints-Orevkov). On sait que la logique intuitionniste exige que dans une disjonction $(A \vee B)$, l'un des membres de la disjonction soit une instance numérique — que l'on puisse isoler — et la même exigence vaut pour le quantificateur existentiel $\exists x Ax$ qui doit pouvoir exhiber une instance numérique An.

On peut alors montrer que

$$\exists x Ax \rightarrow \neg\neg\exists x(Ax \wedge Ay < x\ \neg Ay)$$

est équivalent à

$$\forall x[Ax \rightarrow \neg\neg\exists z(Az \wedge \forall y < z\ \neg Ay)].$$

mais il faut appliquer ici le principe de l'induction transfinie dont on suppose qu'il est équivalent à l'induction complète dans l'arithmétique de Heyting. Cette même induction complète est admise par les intuitionnistes pour toutes les propriétés constructives des nombres naturels. C'est ici que le bât blesse puisqu'on peut montrer que l'équivalence entre IC et IT (et DIE) repose sur la double négation pour un ensemble infini et entraîne le tiers exclu, comme l'avait soutenu Kolmogorov. Il suffit de faire l'exercice précédent avec le principe du plus petit nombre

$$\text{(PPN)} \quad \exists y Ay \rightarrow \exists y(Ay \wedge \forall z(z \prec y)\neg Az)$$

Je substitue $\neg Ay$ à Ay

$$\neg\exists y(Ay \wedge \forall z(z \prec y \rightarrow \neg Az))$$

et j'obtiens par transformations sur les équivalences classiques et MP (*modus ponens*)

$$\forall y(\neg Ay \wedge \forall z(z \prec y \rightarrow \neg Az))$$

et

$$\forall y(\forall z(z \prec y \rightarrow \neg Az)) \rightarrow Ay$$

et

$$\forall y \neg Ay$$

qui est le conséquent de la descente avec

$$\text{(DIE)} \quad \forall y(Ay \rightarrow \exists z(z \prec y)Az) \rightarrow \forall y \neg Ay$$

obtenue classiquement de la règle d'induction

$$(A0 \text{ et } \forall y Ay \rightarrow ASy)$$

et du postulat d'induction de Peano

$$\text{(PIP)} \quad \forall x Ax(A0 \rightarrow (\forall x Ax \rightarrow ASx)) \rightarrow \forall x Ax$$

par MP.

On peut donc démontrer classiquement l'équivalence de PPN avec DI, mais PPN n'est pas déductible de IT en logique intuitionniste (à cause du principe du tiers exclu), alors que IT est équivalent à IC et à DI du point de vue intuitionniste aussi bien que classique. Il y a donc bien dilemme ou plutôt trilemme : ou bien IC, IT et DI ne sont pas équivalents en logique intuitionniste, alors PPN ne peut être obtenu ni de IT (ou IC), ni de DIE et le principe $\neg\neg[\exists x Ax \rightarrow \exists x(Ax \wedge \forall y < x\ Ay)]$ que nous pourrions appeler DIM, la « descente infinie de Markov », n'a qu'une valeur ou un portée limitée puisqu'il correspond à la recherche illimitée d'un contre-exemple.

Le principe fort de la descente infinie positive au sens de Fermat exclut nettement le tiers exclu par l'expression 7a de la descente

$$Az = \begin{cases} 0 \\ 1 \\ n \end{cases} \qquad (\text{pour } 0 \text{ ou } 1 \text{ ou } n = Ax_n \vee \ldots \vee Ax_1 \vee Ax_0)$$

selon que la descente « finie » s'arrête à 0, à 1 ou à n. C'est uniquement dans ce contexte « positif » qu'un polynôme quadratique ou une équation diophantienne peut avoir un nombre infini (*effini*) de solutions. Pour les problèmes négatifs, comme dit Fermat, la double négation aboutit dans le

fini à 0 ou 1 avec $1 \neq 0$. C'est là le sens même de la *reduction ad absurdum*, qui signifie en dernière instance réduction d'une hypothèse fausse par une procédure de preuve qui aboutit à une conclusion contradictoire en un nombre fini d'étapes, ce qui est la méthode constructive à proprement parler.

Dans son programme de réforme de l'analyse mathématique classique, Brouwer a introduit des principes intuitionnistes pour l'ordination ou le bon ordre sur les suites de choix, c'est-à-dire sur les suites de choix successifs de valeurs dans la suite ordonnée des nombres naturels ; il s'agit du théorème de la barre, du théorème de l'éventail et du théorème de continuité uniforme sur l'intervalle (compact) $[0, 1]$. On peut formuler le théorème de la barre de la façon suivante : « si une propriété est vraie pour toute suite α habitée (par des valeurs initiales) et est vraie pour le segment initial des valeurs de α, et si elle est vraie de la concaténation $\alpha* \prec n \succ$ pour tout n, alors elle est vraie pour toute suite dans S (le déploiement universel, en néerlandais « *spreiding* ») » — pour toutes ces notions je renvoie à (Gauthier [31], chap. 2) repris partiellement dans (Gauthier [38], chap. 5). On voit donc la proche parenté de ce théorème avec le postulat d'induction (classique) de Peano — la preuve elle-même repose essentiellement sur l'induction, *i.e.* l'induction "barrée". Or S.C. Kleene a montré (Kleene and Vesley [68]) que le principe général de l'induction barrée entraînait le tiers exclu et qu'il fallait donc une contrainte nouvelle , celle de la décidabilité « locale » des suites, pour valider le théorème de la barre d'un point de vue constructif — ce résultat de Kleene et d'autres sont dûment consignés dans *Elements of Intuitionism* de Dummett (Dummett [21]).

Les suites de choix sont engendrées par des choix successifs de valeurs, choix étagés par des opérations ou fonctionnelles continues qui peuvent opérer sur tout un réseau de choix antérieurs pour donner naissance à une floraison de suites de choix (voir Troelstra [99] et [100]).

Un premier principe valide pour les suites de choix est celui de la continuité intensionnelle qu'on exprime de la façon suivante

$$X\alpha \rightarrow \exists\Gamma(\exists\beta(\alpha = \Gamma\beta) \wedge \forall\beta X(\Gamma\beta))$$

i.e. si une suite de choix possède un prédicat extensionnel ou appartient à une espèce donnée, alors il est toujours possible de trouver une fonctionnelle continue opérant sur une autre suite de choix et qui correspond à cette première suite de choix, parce qu'elle possède le même prédicat extensionnel ou appartient à la même espèce (en vertu des mêmes segments initiaux).

On peut définir aussi une continuité extensionnelle (ou le principe de Brouwer pour les nombres)

$$\forall\alpha\exists x X(\alpha, x) \to \exists x\forall x\forall y\forall\beta(\bar{\alpha}x = \bar{\beta}x \to X(\beta, y)),$$

ce qui signifie que si l'on a pour une suite de choix arbitraire α une procédure qui permette de déterminer un nombre naturel x, alors pour toutes les autres suites de choix ayant les mêmes segments initiaux, on peut avoir la même procédure qui permette de déterminer un nombre naturel y, ou, en d'autres termes, l'existence d'une valeur numérique déterminée pour une suite de choix implique qu'il y a une fonctionnelle régulière continue qui détermine une telle valeur.

Une des conséquences importantes de ces principes est le théorème de l'éventail de Brouwer. Pour le discuter utilement, il faut introduire la notion de déploiement. La notion de déploiement est définie par deux lois : une loi de déploiement, qui est représentée par une fonction régulière a obéissant aux stipulations suivantes :
1) $a0 \neq 0$
2) $\forall n\forall m(a(n * m) \neq 0 \to an \neq 0)$
3) $\forall n\exists x(an \neq 0 \to a(n* \prec x \succ \neq 0))$
Une quatrième stipulation de finitude
4) $\forall n\exists z\forall x(a(n* \prec x \succ \neq 0 \to x \leq z)$
définit une loi de déploiement finitaire ou éventail (*fan*). Ici * désigne encore l'opération de concaténation et $\prec x \succ$ une suite contenant un seul élément. On peut se représenter une loi d'éventail comme un arbre dont le faîte est la suite vide

L'autre loi qui définit un déploiement est une application complémentaire ξ d'une loi de déploiement (ou d'un arbre) qui fait correspondre les objets d'une espèce donnée S aux nombres naturels positifs. Un déploiement peut être "habillé" ou "nu", selon que l'application ξ est dans une espèce ou non et une suite est élément d'un déploiement si elle suit immédiatement dans l'arbre une suite qui l'est. Le théorème de l'éventail s'énonce comme suit

$$\forall\alpha\forall x X(T_\alpha\alpha, x, \alpha_0, \ldots) \to$$

$$\exists y\forall\alpha\forall\beta(\Gamma_\alpha\alpha y = \Gamma_\beta\beta y \to X(\Gamma_\alpha\beta, x, \alpha_0, \ldots)).$$

Ce théorème est une sorte de théorème de finitude pour les suites de choix. En mots, "si à chaque élément d'un éventail α est associé un nombre naturel

x, un nombre naturel y peut être spécifié tel que x soit déterminé par les y premiers choix qui engendrent α par la loi d'éventail a". Or le lemme de König classique est la contraposée du théorème de l'éventail pour les espèces détachables, *i.e.*

$$\forall x \in X(x \in Y \vee x \notin Y)$$

pour des espèces X et Y. Le lemme de König qui stipule que tout arbre infini à branchement fini comporte une branche infinie (le tronc !) fait appel à la logique classique (tiers exclu) et à des notions non constructives (*e.g.* axiome du choix) Il faut donc affaiblir le théorème de l'éventail pour lui conserver son caractère intuitionniste.

Le théorème de l'éventail à été utilisé par Brouwer pour démontrer son important théorème en analyse intuitionniste : "Toute fonction à variables réelles définie sur l'intervalle compact $[0, 1]$ est uniformément continue". Intuitivement, on voit que toute fonction $\phi(x)$ d'une variable réelle partout définie ne peut l'être que de proche en proche — par les n premiers choix de valeurs pour $\phi(x)$ — de sorte que la différence entre deux fonctions $\phi(p)$ et $\phi(q)$ pour deux points p et q soit toujours inférieure à un nombre rationnel arbitrairement petit 2^{-n}, d'où la continuité uniforme.

Remarquons que les principes d'induction sur les ordinaux (les bons ordres) ont la même signification en logique classique et en logique intuitionniste, sauf que l'on suppose que les espèces en intuitionnisme sont décidables, *i.e.* que pour une suite (ou sous-suite) arbitraire strictement descendante F, on a $x_0 \notin F \vee x_0 \in F$ (voir Troelstra 1969). À la notion ensembliste de bon ordre sur les sous-ensembles de $\mathbb{N}$ correspond la notion intuitionniste d'arbre bien fondé pour lequel il n'y a pas de suite strictement descendante (décroissante) infinie — énoncé qui correspond à son tour à l'axiome de foundation dans la théorie des ensembles de Zermelo-Fraenkel. Dans les deux cas, pour passer à la descente infinie au sens de Fermat, en réalité une descente finie, comme nous l'avons vu — il faut utiliser la double négation sur l'ensemble infini dénombrable $\mathbb{N}$ pour la descente finie (DF)

$$\neg(\neg\mathrm{DF}) \leftrightarrow \mathrm{DF}$$

qui exclut le tiers, ici la descente indéfinie sur la suite « effinie » ou illimitée des nombres naturels.

A.4 Épilogue philosophique. Le va-et-vient entre la théorie et la pratique

Brouwer a introduit la notion de sujet créateur dans ses travaux tardifs pour accentuer le caractère subjectiviste de l'expérience mathématique. Certains ont voulu formaliser la théorie du sujet créateur, mais on a dû admettre que la théorie des constructions et des preuves qui leur sont associées était imprédicative. Une analyse phénoménologique de l'expérience mathématique peut se permettre de faire appel au sujet transcendantal dans l'esprit de Kant ou de Husserl et supposer que le destin de l'intuitionnisme a partie liée avec la phénoménologie husserlienne. Brouwer lui-même semble avoir suggéré qu'une analyse démonstrative complète ou une preuve canonique requérait une structure arborescente infinie dans le déploiement universel de toutes les suites de nombres naturels — voir là-dessus le commentaire de Dummett (Dummett [21]). Il est patent que cette idée d'une production mentale qui transcende les moyens finis de la métamathématique au sens de Hilbert va à l'encontre du constructivisme finitiste inauguré par Kronecker et que Hilbert s'est résolu à adopter après un détour par le paradis cantorien ! La justification transcendantale de théorèmes mathématiques (théorème de la barre ou théorème de l'éventail) n'est pas si éloignée en réalité des arguments philosophiques qu'un Cantor platoniste a voulu trouver chez les philosophes et théologiens médiévaux ou encore chez le Spinoza de la substance infinie. La notion hilbertienne de système formel suppose en revanche que l'on doive démontrer des propositions infinitaires par des moyens finis, la preuve se terminant avec la dernière ligne d'une dérivation formelle. C'est tout le sens de l'algorithme kroneckerien de la démonstration en un nombre fini d'étapes. La logique et les mathématiques constructives ne peuvent s'accomoder de principes et de théories qui vont au-delà de l'horizon constructif : cet horizon est récessif, mais indépassable ou intraversable tout autant que l'infini potentiel d'Aristote. La pratique mathématique d'un Leibniz pour qui l'infini mathématique est une fiction utile ou d'un Gauss pour qui l'infini du mathématicien n'est qu'une façon de parler ou encore d'un Poincaré qui pensait que l'infini est une approximation du fini et non l'inverse, toute cette tradition arithmétique se prolonge par-delà l'infinitisme cantorien aussi bien en logique et en mathématiques constructives qu'en informatique théorique. La critique fondationnelle est une théorie critique de la pratique et il importe de démonter, d'autres diraient déconstruire, le discours logique ou mathéma-

tique qui prétend rendre compte de la pratique concrète en recourant aux objets idéaux produits par un mathématicien idéal dans un univers qu'il n'a pas construit *effectivement*.

Le constructivisme intuitionniste n'obéit pas toujours aux canons de la pratique mathématique que Brouwer a voulu instaurer. En admettant l'équivalence formelle de l'induction transfinie (et de l'induction complète) avec la descente infinie, l'intuitionnisme brouwerien et post-brouwerien commet une erreur de principe, puisque le tiers exclu refusé aux ensembles infinis refait surface dans la double négation opérée sur l'ensemble dénombrable infini des nombres naturels pour redescendre l'échelle infinie de l'induction. Brouwer avait pourtant insisté sur le procès en devenir « *ein Prozess im Werden* » pour les suites infiniment processives, mais il n'a pas toujours suivi ses propres préceptes et ses successeurs n'ont pas toujours suivi l'initiateur de l'intuitionnisme. L'équivalence formelle entre induction transfinie et descente infinie est évidemment admise en logique et en mathématiques classiques au prix de principes non constructifs. Pour le montrer, il a suffi de contraster la descente infinie pratiquée en arithmétique ou théorie des nombres avec la descente infinie de la logique classique.

Un premier argument pragmatique, c'est-à-dire issu de la pratique, en faveur de la spécificité de la descente infinie au sens de Fermat, c'est qu'elle opère hors de l'atteinte de la théorie des ensembles et de la sémantique ensembliste de la logique classique, la théorie des nombres classique ayant connu un développement totalement autonome tout au long de son histoire depuis Hammourabi jusqu'à nos jours, si l'on en croit André Weil (Weil [107]). Et en pratique, l'infini constructible n'est pas absent des mathématiques constructives. On n'a qu'à rappeler le théorème d'Euclide sur l'infinité des nombres premiers où la preuve est constructive et où la notion d'infini actuel n'apparaît pas. En fait, la descente infinie que Fermat considère comme sa création peut être interprétée comme un algorithme euclidien généralisé pour la décomposition des nombres (et des polynômes) en leurs diviseurs communs ; la méthode s'applique dans de vastes domaines des mathématiques, de l'arithmétique élémentaire à la théorie algébrique des nombres (Kummer) et à l'arithmétique générale ou théorie des formes de Kronecker — on trouvera des détails sur la formulation de la méthode chez Fermat et des notes sur le programme de Kronecker dans le petit livre (Gauthier [36]) dont l'élaboration se trouve dans l'ouvrage (Gauthier [42]).

La théorie logique, la logique arithmétique ou la logique interne de l'arithmétique qui est à l'oeuvre dans la descente infinie de Fermat est par

definition une logique constructive qui ne peut tolérer le tiers exclu et les principes non constructifs comme l'axiome du choix et autres concepts infinitaires propres à l'arithmétique transfinie de Cantor sur laquelle reposent l'arithmétique ensembliste de Dedekind-Peano et la sémantique ensembliste de la logique classique. La théorie logique veut reproduire le plus fidèlement possible la démarche concrète de l'arithméticien pour retraduire la logique en termes arithmétiques, d'où le nom de logique polynomiale modulaire pour la logique arithmétique à portée computationnelle immédiate. Alors que les logiques faisables, prédicatives ou constructives de l'arithmétique de Peano (et de ses sous-systèmes) sont partie prenante de la sémantique ensembliste, la logique arithmétique est une syntaxe pure qui doit générer sa propre interprétation, *i.e.* sa consistance interne par des moyens constructifs à vocation computationnelle. La posture fondationnelle du constructivisme finitiste ou plutôt « effinitiste » cherche à mieux définir l'horizon constructif de la pratique scientifique ; c'est là une tâche philosophique à laquelle le théoricien de la pratique ne peut se soustraire.

Annexe B

La consistance interne de l'arithmétique avec descente infinie. Une preuve syntaxique [1]

B.1 Préambule

La question de la consistance [2] ou de la non contradiction de l'arithmétique est une question philosophique, celle de la certitude d'une théorie mathématique, qui est devenue un problème logique exigeant une réponse mathématique. C'est Hilbert qui est à l'origine de ce questionnement. Il a d'abord voulu montrer en 1899 la consistance de la géométrie élémentaire en la fondant sur l'arithmétique des nombres réels qu'il a supposée non contradictoire, puis il s'est interrogé sur la consistance de cette arithmétique dans

1. L'expurgation des éléments sémantiques a été faite à partir de la preuve originale "The Internal Consistency of Arithmetic with Infinite Descent" [41] et des variantes parues dans deux ouvrages récents *Internal Logic : Foundations of Mathematics from Kronecker to Hilbert* [42] et *La logique du contenu. Sur la logique interne* [43]. Pour les notions de logique utilisées dans le texte, je renvoie à mon ouvrage *Logique et fondements des mathématiques* [38].

2. Le français "cohérence" n'est pas approprié dans ce contexte, puisque l'anglais a déjà une notion logique de "coherence" qu'on ne saurait plus traduire ; une théorie logique cohérente, par exemple, est une logique qui admet des métavaluations pour lesquelles tous les théorèmes de la théorie sont des énoncés vrais (d'où complétude).

son deuxième problème de la liste de 1900 qui comportait outre les axiomes de l'arithmétique élémentaire un axiome de continuité (scindé en l'axiome d'Archimède et la complétude axiomatique). Il a voulu donner sa propre solution du problème de la consistance dans une métamathématique ou théorie des systèmes formels comme il a voulu résoudre son premier problème, celui de l'hypothèse du continu hérité de Cantor, dans les termes de la théorie cantorienne des ordinaux transfinis. C'est dans ces mêmes termes que Gentzen et d'autres à sa suite reprendront le problème après que Gödel eût montré que l'arithmétique de Peano ne pouvait contenir sa propre consistance. Skolem avait auparavant montré en 1923 qu'une preuve de consistance finitaire ne pouvait porter que sur une arithmétique finie caractérisée par des processus finis, comme le dit Skolem en s'inspirant de Kronecker. Gödel lui-même n'a pas abandonné la question de la consistance de l'arithmétique et sa propre solution l'a préoccupé à partir des années quarante jusqu'à la fin de sa vie.

Ce que Gödel a rejeté, c'est le point de vue finitiste du système formel « concret » qu'il a voulu ouvrir sur les concepts abstraits tels que les pratiquait l'intuitionnisme, e.g. la notion de fonctionnelle, c'est-à-dire une fonction de fonction ou une fonction généralisée. L'extension du point de vue finitiste signifie la généralisation d'une logique finitaire en métathéorie qui manipule en plus des objets concrets, c'est-à-dire les symboles d'un système formel, les formes plus générales d'une arithmétique qui accueille des fonctionnelles capables de couvrir l'étendue des types finis d'objets, les nombres naturels. Gödel n'a pas voulu renoncer pour autant à l'ensemble infini des nombres naturels et c'est la justification philosophique (fondationnelle) de l'extension fonctionnelle qui l'a tenaillé, jusqu'à la fin, selon son propre aveu.[3] La généralisation, plutôt que l'abstraction, que visait Gödel peut emprunter une autre voie : celle que je propose remonte au-delà de Hilbert à l'arithmétique générale « *allgemeine Arithmetik* » de Kronecker. Cette arithmétique générale traite de la théorie des formes ou polynômes homogènes qui apparaît ici comme la véritable généralisation des entiers positifs ou des nombres naturels. Au lieu donc de prolonger l'arithmétique finie dans une arithmétique transfinie cantorienne comme l'ont voulu Hilbert, Gentzen et Ackermann avec d'autres, il faut l'élargir, l'étendre — au sens de l'« *Erweiterung* » ou extension gödelienne — dans une arithmétique polynomiale qui en fait généralise les propriétés de l'arithmétique élémentaire de la façon la plus naturelle qui soit.

3. Voir [49], vol. II, p. 305.

Loin donc de contredire les résultats d'incomplétude de Gödel pour l'arithmétique de Peano, comme certains esprits peu ou mal informés ont pu le croire, la preuve de consistance tirée de l'arithmétique polynomiale les confirme plutôt à rebours, pourrait-on dire. Ces mêmes résultats ne rendaient pas non plus inopérant le programme de Hilbert, comme Gödel l'a souvent répété : c'est seulement le cadre finitaire proposé par Hilbert qu'il fallait élargir. Et pourtant Hilbert qui s'était si souvent inspiré de Kronecker et de son arithmétique générale n'a pas vu qu'une voie était ouverte dans cette même arithmétique qui pouvait mener à la consistance de l'arithmétique. Hilbert avait cependant noté dans ses travaux algébriques antérieurs à 1900 et largement inspirés des résultats de Kronecker que la décidabilité des questions mathématiques s'effectuait en un nombre fini d'étapes, ce qui anticipe clairement sur la notion de méthode axiomatique qui doit permettre la solution du problème logique de la décision en un nombre fini d'opérations. [4] Mais il faut redonner à Hilbert ce qui lui appartient en propre ; c'est lui le premier qui a formulé le problème logique de la consistance. Mieux, c'est Hilbert qui a introduit la logique en mathématiques et c'est sa théorie des démonstrations qui est la première logique mathématique. On doit en plus à Hilbert la première notion de modèle, puisque l'arithmétique des nombres réels, i.e. leurs propriétés arithmétiques élémentaires, a servi de modèle pour la preuve de consistance de la géométrie élémentaire — Tarski en montrera plus tard la décidabilité.

Ce n'est pas la sémantique ensembliste de l'arithmétique de Peano qui est en jeu au point de départ, mais bien plutôt une syntaxe primitive des opérations arithmétiques que Hilbert mettra en œuvre. Cette syntaxe est l'essence même du finitisme que Hilbert adoptera au point de départ, qu'il abandonnera par la suite pour y revenir enfin en reconnaissant ultimement son inspiration kroneckerienne. Le paradis cantorien dont Hilbert a rêvé lui est apparu inaccessible quand il s'est rendu compte à la fin qu'on ne pouvait grimper l'échelle transfinie échelon par échelon selon la méthode kroneckerienne de la progression « *Fortgang* », même si on peut la redescendre suivant la méthode fermatienne de la descente infinie ou indéfinie — en réalité finie. Les historiens, en particulier W. Sieg et V. Peckhaus, insistent sur le fait qu'il n'y a pas de fil continu dans les préoccupations fondationnelles de Hilbert, mais ils doivent admettre que le point de vue finitiste « *finiter Standpunkt* » est un thème récurrent dans l'œuvre de Hilbert. Brouwer n'est pas si éloi-

4. Voir [61], vol. III, p. 153.

gné de Hilbert là-dessus ; Brouwer connaissait peu Kronecker, si ce n'est ses travaux sur les fonctions à plusieurs variables avec la notion d'indice de rotation (*Windungszahl*) qui ont abouti à la théorie brouwerienne du point fixe, mais il partageait certainement le point de vue constructiviste. La théorie des suites régulières, suites irrégulières et suites de choix chez Brouwer relève assurément d'un esprit arithmétique apparenté à l'héritage kroneckerien. On retrouve chez le Gödel de l'extension du point de vue finitiste le motif intuitionniste des notions constructives abstraites ou générales. La convergence des entreprises fondationnelles de Hilbert, Brouwer et Gödel invite à revisiter la problématique dans la perspective d'un constructivisme ou d'un arithmétisme dont Kronecker a été l'initiateur.

L'idéal d'adéquation pour une logique interne du contenu mathématique s'accomplit dans la preuve de consistance — la complétude (sémantique) n'est qu'un dérivé illusoire et ne remplit qu'un satisfecit logico-philosophique étranger à la pensée mathématique pour laquelle la consistance équivaut à la complétude syntaxique qui n'est que l'extension maximale de la consistance ! L'équivoque de la formule qui voudrait que la consistance signifie "avoir un modèle (infini)" ne peut être levée que si l'on insiste sur l'impossible adéquation d'un calcul fini de la déduction avec l'ensemble récursivement énumérable mais toujours infini des énoncés vrais d'une théorie du premier ordre de cardinalité $\aleph_0$. Même la consistance que Gödel voudra introduire pour recouvrer l'ensemble infini des nombres naturels ne pourra rattraper une vérité "diagonalisée" qui échappera toujours au calcul, selon le point de vue transcendant adopté par Gödel. C'est sans doute aussi le point de vue transcendant qui a fait dire à Kreisel, entre autres, que la solution (par induction transfinie) au problème de la consistance suscitait plus de doutes que le problème lui-même. Encore ici, le scepticisme découle de l'adoption d'un point de vue "externaliste".

Le problème de la consistance de l'arithmétique du point de vue interne se résume à séparer les théorèmes des non-théorèmes ou les énoncés de leur négation et de montrer que seuls les théorèmes sont démontrables, i.e. $a = a$ ou $0 \neq 1$. La décidabilité pourra énumérer ces théorèmes et la complétude syntaxique dressera une liste exhaustive des axiomes de la théorie arithmétique consistante ; la complétude sémantique voudra fournir une caution externe à la consistance quand elle demandera que les théorèmes soient vrais dans les modèles de la théorie.

La forme qu'a prise la preuve de consistance que j'ai proposée dépend d'une option fondationnelle précise qui vise l'arithmétisation de la logique.

Plutôt que de prolonger l'induction infinie en induction transfinie, il s'agissait d'immerger l'anneau des entiers dans l'anneau des polynômes ou plus concrètement de plonger l'arithmétique ordinaire dans l'arithmétique générale des polynômes (formes) — que Kronecker a arithmétisée dans son état final — et de revenir dans l'arithmétique ordinaire par la méthode de la descente infinie de Fermat. C'est la traduction arithmétique ou polynomiale de la logique qui permet le passage direct de l'anneau des entiers à l'anneau des polynômes ou de l'arithmétique ordinaire à l'arithmétique générale. Le problème de la consistance est ici résolu dans l'esprit hilbertien et kroneckerien du constructivisme finitaire, l'option fondationnelle que j'ai privilégiée depuis le point de départ. Le détour par la théorie des fonctions récursives est évité grâce à la théorie polynomiale qui est à l'origine de la notion de récursivité et la métathéorie du système formel est évacuée au profit des règles génétiques du calcul gentzénien de la déduction naturelle, lui-même interprété comme théorie polynomiale. Surtout l'arithmétique de Peano dont Gödel a montré l'incomplétude et dont la consistance ne pouvait être qu'externe est réduite ou est remplacée par une arithmétique qui n'est plus ensembliste, mais numérique — au sens de la théorie des nombres. Le procédé de diagonalisation, central dans la démonstration de Gödel, ne peut opérer dans cette arithmétique de Fermat-Kronecker, puisqu'il n'y a pas d'ensemble infini de nombres naturels qu'on puisse traverser pour déboucher sur un (nombre) réel innombrable ! Du même coup, la gödelisation qui assignait des nombres naturels aux formules se trouve inversée ; dans l'interprétation polynomiale, ce sont les formules qui sont immédiatement transformées en expressions polynomiales et sont simultanément soumises à un traitement arithmétique qui les décompose par la descente infinie jusqu'à des équations ou inéquations qui traduisent numériquement les formules et leur négation en termes de polynômes de degré fini. La réduction finitaire garantit alors la consistance par l'inéquation élémentaire $0 \neq 1$.

L'idée d'une logique interne de l'arithmétique ou d'une logique arithmétique est à l'origine du présent travail remis maintes fois sur le métier depuis une vingtaine d'années. C'est d'abord la méthode de la descente infinie de Fermat découverte à la lecture de l'ouvrage d'André Weil sur l'histoire de la théorie des nombres [107] qui a orienté la recherche vers la logique arithmétique, comme en témoigne l'ouvrage *De la logique interne* [36] dont la rédaction a été amorcée en 1986 lors d'un séjour de recherche à LOMI, l'Institut de mathématiques de l'Université de Leningrad (St-Pétersbourg). Puis la lecture des *Gesammelte Abhandlungen* [57] de Hilbert en vue d'un article

pour *La revue internationale de philosophie*[5] à l'occasion du cinquantième anniversaire de la mort de Hilbert a conduit à la redécouverte de Kronecker en amont du texte de 1887 sur le concept de nombre « *Über den Zahlbegriff* ». C'est la présence de Kronecker surtout dans les travaux arithmétiques et algébriques de Hilbert qui a aiguillé la recherche sur la logique interne, comme je l'ai annoncé à la fin de l'ouvrage *De la logique interne*. Le passage de la logique interne à la logique arithmétique puis à la logique polynomiale et enfin à la logique polynomiale modulaire s'est effectué selon une logique interne proprement kroneckerienne du pas à pas. Le retour à Kronecker par-delà Hilbert « *ein Schritt zurück* », un pas en arrière, a permis de bien enraciner la vocation constructiviste de travaux menés dans les années 70 et dont les résultats, e.g. les notions de négation locale et de quantificateur « effini » en particulier, ont été consignés dans l'ouvrage *Fondements des mathématiques. Introduction à une philosophie constructiviste* [34].

La preuve de consistance de l'arithmétique avec descente infinie polynomiale s'effectue sans sémantique. Au modèle originel des domaines « effinis » de nombres naturels s'est substituée l'arithmétique polynomiale (avec indéterminées) dans laquelle est plongée naturellement l'arithmétique des entiers et la descente infinie y opère avec une égale efficacité. On peut même penser que l'arithmétique polynomiale est la sémantique « naturelle » de l'arithmétique des nombres naturels, dans le sens où l'on peut interpréter l'arithmétique et sa logique interne dans la théorie polynomiale sans recourir à des notions externes à l'arithmétique (e.g. la notion d'ensemble). La sémantique ensembliste de l'arithmétique de Peano-Dedekind avec son postulat d'induction et son univers infini est une surcharge pour l'arithmétique finitaire ; il importe délester la syntaxe de tout poids ontologique pour garantir l'effectivité générale, si abstraite soit-elle, d'une pratique démonstrative en harmonie avec la théorie constructiviste.

5. Voir "Hilbert et la logique interne des mathématiques" dans *La revue internationale de philosophie*, vol. 47, no. 186 (1993), pages 303-318, repris dans "Hilbert and the internal logic of mathematics", *Synthese*, no. 101 (1994), 1-14 ; quant au texte de la preuve originale de consistance, "The Internal Consistency of Arithmetic with Infinite Descent", il a été accepté en 1995 et publié en 2000 par la revue *Modern Logic* (voir [41]).

B.2 Introduction

L'idée de la preuve de consistance pour ce que j'ai appelé l'arithmétique de Fermat-Kronecker était de substituer la descente infinie au sens de Fermat au postulat d'induction de Peano pour l'arithmétique ensembliste. Du point de vue logique traditionnel, la descente infinie et l'induction complète sont des principes équivalents. Mais pour démontrer leur équivalence, il faut utiliser le tiers exclu (ou la double négation) sur l'ensemble infini (dénombrable) des nombres naturels, procédure que s'interdit l'option constructiviste en fondements des mathématiques. L'induction transfinie, qui n'est que l'induction complète sur les ordinaux jusqu'à la limite ($\lim \omega = \epsilon_0$) et dont on voudrait qu'elle soit l'exacte réplique de la descente infinie ne peut elle-même prétendre à ce titre qu'au prix de la voie indirecte, via le tiers exclu ou la double négation.

Un simple constat suffit cependant à disqualifier ces prétentions. La descente infinie en arithmétique ou théorie des nombres n'a pas besoin du recours à un ensemble infini de nombres naturels (ω ou $\aleph_0$) pour se déployer dans toutes ses ramifications. Fermat, Euler, Lagrange, Legendre, Dirichlet, Kummer et Kronecker, pour ne nommer que ceux-là, l'ont utilisée comme méthode élémentaire de démonstration sans jamais invoquer la totalité ensembliste des nombres naturels. Ce n'est pas seulement en théorie des nombres, mais aussi bien en algèbre (théorie des formes ou des polynômes) que la descente infinie que Fermat [19] qualifiait aussi d'indéfinie — elle s'avère à la fin être une descente finie — trouve son plus vaste champ d'application.

C'est l'algèbre des polynômes que Kronecker appelait arithmétique générale « *allgemeine Arithmetik* » — qui doit être la théorie fondatrice où l'arithmétique viendra se plonger pour assurer sa consistance. En effet, au lieu de prolonger l'arithmétique vers le haut jusque dans le transfini cantorien, comme ont voulu le faire Hilbert, Gentzen, Ackermann et leurs successeurs, il fallait plutôt représenter l'arithmétique des entiers dans une théorie générale qui reproduise la constitution et la structure de l'arithmétique dans un contexte élargi, la théorie polynomiale qui possède des propriétés essentielles de l'arithmétique élémentaire, en particulier la factorisation unique des polynômes en polynômes premiers, tout en disposant des ressources d'un calcul plus étendu. L'outil principal ici est la théorie du contenu polynomial au coeur de l'arithmétique générale de Kronecker et son principe fondamental est le principe d'équivalence des polynômes ou fonctions polynomiales dont ils sera exclusivement question ici — si deux polynômes (concrets) distincts

peuvent donner une même fonction polynomiale, une fonction polynomiale est injective dans les nombres naturels.

> Deux formes homogènes (polynômes) F et F' sont équivalentes, si elles ont les mêmes coefficients (i.e., contenu).

On peut opérer des substitutions (linéaires) sur ces formes, pourvu qu'on substitue aux variables (indéterminées) des coefficients entiers, i.e., des entiers. Le rôle universel joué par les indéterminées procure à la théorie polynomiale la plus grande généralité et l'investit en même temps de moyens suffisants pour représenter intégralement le contenu de l'arithmétique élémentaire. C'est cette notion de représentation qui est au coeur de la preuve de consistance.

La théorie de la représentation polynomiale doit faire l'économie de tout recours à la sémantique (notion de modèle ou d'interprétation) ensembliste. Les moyens syntaxiques requis sont réduits au maximum à une syntaxe logique minimale. Mais la logique minimale elle-même devra être représentée dans la théorie polynomiale où s'effectuera la preuve par réduction ou descente finie. Le terme de réduction rappelle l'algorithme d'Euclide pour la division ou la décomposition de nombres (composés). La descente infinie sera conçue ici comme un algorithme euclidien généralisé au corps $\mathbb{Q}$ des nombres rationnels.

C'est l'anneau $K[x]$ des polynômes irréductibles (premiers) avec coefficients dans le corps $k(x)$ qui sera le principal théâtre de nos opérations et $F(x)$ sera le corps fini où opère d'abord la descente infinie. Vandiver [103] s'inspirant de Kronecker a montré comment recomposer le corps de décomposition $F(x)$ d'un corps rationnel $\mathbb{Q}$ de nombres algébriques par adjonction d'indéterminées une à la fois, c'est-à-dire par un algorithme de calcul linéaire. Vandiver recompose donc (par induction finie) le corps de décomposition $\mathbb{Q}$ obtenu par descente (finie).

Ce que représente la théorie polynomiale, ce sont d'un côté les nombres de Gödel assignés aux formules logiques et de l'autre les opérations logiques qui sont responsables de la composition des formules, *i.e.*, les constantes logiques — les variables seront représentées par les indéterminées du polynôme. Tout le calcul n'a pour but que de produire une inéquation finale $0 \neq 1$ pour la consistance ou la non-contradiction de l'arithmétique. C'est donc une double bijection que l'on définit dans la représentation polynomiale, une première entre les entiers et leurs polynômes représentatifs, et une seconde entre les formules et leurs polynômes représentatifs — dans ce cas nous avons un iso-

morphisme ou une bijection de structures. C'est là un isomorphisme interne, si l'on peut dire, puisque nous demeurons dans l'arithmétique (générale), alors que l'isomorphisme de Curry-Howard entre types et formules peut être considéré comme externe.

Le programme général de l'arithmétisation de la logique inauguré par Hilbert et réalisé par Gödel pour l'arithmétique de Peano est prolongé à l'arithmétique de Fermat et à l'arithmétique générale de Kronecker.

B.3 Syntaxe

Nous avons un langage du premier ordre $L(T)$ pour une théorie du premier ordre T qui a un inventaire effini (illimité) de symboles atomiques.

a) les lettres (minuscules et majuscules) pour les formules et les énoncés, $a, b, c, \ldots A, B, C, \ldots$ avec leurs signes de ponctuation, points, virgules, parenthèses, crochets, etc.
b) les lettres de variables x_0, x_1, x_2, ...
c) les lettres de prédicats P_j^n et le symbole $=$ avec les autres symboles arithmétiques $+$, $\cdot$, -, $\neq$, $\cong$, $\equiv$, $\sum$, $\prod$ (en plus des signes de nombres naturels, 0, 1, etc. et les lettres de prédicats arithmétiques S, P) et les symboles polynomiaux P, Q, a_0, b_0, x et le symbole d'absurdité $\perp$.
d) les lettres de fonctions f_j^n — si f n'a pas d'arité (0), c'est une constante, plus les lettres de fonctions ϕ, ψ, χ.
e) les connecteurs $\wedge, \vee, \neg, \rightarrow$.
f) les quantificateurs $\forall, \exists, \dot{\exists}$.

(Remarque : les quantificateurs $\forall$ et $\exists$ portent sur les suites finies (des ensembles), alors que le quantificateur effini $\dot{\exists}$ porte sur des suites effinies, *i.e.* avec borne prépositionnelle ou terme initial, mais sans borne postpositionnelle ou terme final, comme la suite des nombres naturels, en analogie avec les suites infiniment processives de Brouwer.)

Les termes de $L(T)$ sont constitués exclusivement

1) de variables
2) de suites composées de termes et de lettres de fonctions, *e.g.* $f_j^n t_1, \ldots, t_n$ — pour les termes $t_1 \ldots t_n$.

Les formules bien formées (ou *fbfs*) sont constituées exclusivement

1) de formules atomiques composées de termes et de lettres de prédicat, e.g. $p_j^n t_1, \ldots, t_n$ — pour les termes $t_1 \ldots t_n$
2) de toute fbf construite à partir des connecteurs et des quantificateurs.

Remarques : Les énoncés sont des formules closes, c'est-à-dire que les formules sont des énoncés « ouverts » où l'on a des occurrences libres d'une variable — qui sont donc non quantifiées. Une instance ou un exemplaire $A(t_1 \dots t_n \,/\, x_1 \dots x_n)$ d'une formule A est le résultat d'une substitution de termes t pour les occurrences d'une variable libre.

L'axiome unique de cette logique minimale est l'axiome d'identité

$$A \vdash A$$

pour une formule arbitraire A.

Pour règles logiques, nous adoptons les règles intélim pour l'introduction et l'élimination des connecteurs et des quantificateurs en déduction naturelle à la Gentzen. Les règles intélim sont moins symétriques que les règles équivalentes du calcul des séquents, mais elles « collent » davantage aux déductions d'une logique constructive.

(I $\wedge$) $\dfrac{A \quad B}{A \wedge B}$ (E $\wedge$) $\dfrac{A \wedge B}{A}$ et $\dfrac{A \wedge B}{B}$

(I $\vee$) $\dfrac{A}{A \vee B}$ $\dfrac{B}{A \vee B}$ (E $\vee$) $\dfrac{A \vee B \quad \begin{array}{c}[A]\\ \vdots \\ C\end{array} \quad \begin{array}{c}[B]\\ \vdots \\ C\end{array}}{C}$

(I $\to$) $\dfrac{\begin{array}{c}[A]\\ \vdots \\ B\end{array}}{A \to B}$ (E $\to$) $\dfrac{A,\ A \to B}{B}$

(I$\neg$) $\dfrac{\begin{array}{c}[A]\\ \bot\end{array}}{\neg A}$ (E$\neg$) $\dfrac{A,\ \neg A}{\bot}$

(Remarque : $\bot$ est le symbole de l'absurdité, la logique intuitionniste admet la règle

(E$\neg$) $\dfrac{\begin{array}{c}[A]\\ \bot\end{array}}{A}$

alors que la logique classique doit supposer

$$(\mathrm{E}\neg)\quad \frac{\begin{array}{c}[\neg A]\\ \bot\end{array}}{A}$$

pour obtenir la double négation $\neg\neg A = A$).

$$(\mathrm{I}\,\forall)\quad \frac{Ax}{\forall x Ax} \qquad (\mathrm{E}\,\forall)\quad \frac{\forall x Ax}{At}$$

$$(\mathrm{I}\,\exists)\quad \frac{At}{\exists x Ax} \qquad (\mathrm{E}\,\exists)\quad \frac{\exists x A \quad \begin{array}{c}[Ax]\\ \vdots\\ B\end{array}}{B}$$

$$(\mathrm{I}\,\exists\!\!\!-)\quad \frac{Ax_n}{\exists\!\!\!-\, x Ax} \qquad (\mathrm{E}\,\exists\!\!\!-)\quad \frac{\exists\!\!\!-\, x Ax}{At_0}$$

Remarques : il est entendu que la variable de la quantification n'est pas libre, Ax_n signifie que nous avons une suite illimitée (effinie) de variables et t_0 signifie que dans l'élimination du quantificateur effini, nous revenons à un terme numérique initial. On notera que la logique minimale a les propriétés intuitionnistes de la disjonction — $A \vee B$ est prouvable signifie que A ou B est prouvable — et de l'existence numérique — $\exists x Ax$ est prouvable signifie que At est prouvable pour un terme numérique t arbitraire. En plus des propriétés intuitionnistes, cette logique minimale possède des propriétés constructives qui ne s'appliquent que localement à des suites finies (ensembles) et effinies (itérations illimitées).

De façon équivalente, dans le calcul des séquents de la forme déductive $\Gamma \vdash A$ où la suite Γ est l'antécédent et A le conséquent — unique dans le cas de la logique intuitionniste — les règles pour $\rightarrow$ prennent la forme

$$(\mathrm{I}\rightarrow)\quad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \qquad (\mathrm{E}\rightarrow)\quad \frac{\Gamma \vdash A \qquad \Gamma, B \vdash C}{\Gamma, A \rightarrow B \vdash C}$$

et la règle de coupure

$$\frac{\Gamma \vdash A \qquad \Gamma', A \vdash B}{\Gamma, \Gamma' \vdash B}$$

nous dit que si l'on a déduit A de Γ et que si l'on a déduit B d'un autre antécédent Γ' et de A, alors on peut inférer B de Γ et Γ' en « coupant » A. La règle de coupure correspond au *modus ponens* MP

$$\frac{\begin{array}{l}A \to B\\ A\end{array}}{B}$$

et le calcul des séquents a pour axiome

$$A \vdash A.$$

Quant aux règles de structure qu'on peut formuler simplement

$$\frac{\Gamma \vdash A}{\Gamma' \vdash A}$$

elles ne servent qu'à autoriser des antécédents qu'on peut ordonner selon des combinaisons diverses, soit additions, contractions ou omissions et échanges. Dans la syntaxe restreinte que nous formulons, le principe combinatoire est latent et toute permutation de l'ordre lexicographique ascendant ou descendant est permise. La symétrie des règles d'inférence dans le calcul des séquents n'est globale que dans le cas de la logique classique où l'on a la double négation

$$\frac{\vdash A, \neg A}{\neg\neg A \vdash A,}$$

et le tiers exclu par la règle de coupure. La règle de coupure n'apparaît pas non plus explicitement dans notre formulation, puisque le calcul polynomial est un calcul uniforme qui repose sur la continuité caténaire des suites polynomiales (ou séries finies) auxquelles la propriété de sous-formule est inhérente.

Enfin, il n'y a ni règle ω, ni ensemble $\aleph_0$; il n'y a pas de sémantique ensembliste et *a fortiori* pas de théorème de complétude, la complétude et autres propriétés sémantiques étant exclues pour les structures finies. L'infini n'est qu'une façon de parler, et ce n'est pas de cette façon que nous parlons ...

B.4 Arithmétique

L'arithmétique minimale de R.M. Robinson (voir E. Nelson [85], chap. 3) sert de point de départ. Elle comporte les axiomes suivants

1) $Sx \neq 0$
2) $Sx = Sy \ \rightarrow \ x = y$
3) $x + 0 = x$
4) $x + Sy = S(x + y)$
5) $x \cdot 0 = 0$
6) $x \cdot Sy = x \cdot y + x$
7) $Px = y \ \leftrightarrow \ Sy = x \vee (x = 0 \wedge y = 0)$

L'axiome du prédécesseur dû à Nelson remplace la formule de Robinson

$$x \neq 0 \ \rightarrow \ \exists y Sy = x$$

qui devient un théorème. Comme le montre Nelson, on peut se dispenser d'axiomes pour l'associativité, la distributivité et la commutativité.

Cette théorie arithmétique est une théorie ouverte, i.e., sans quantificateurs. Nous y ajoutons les quantificateurs bornés $\forall x_{x<y}$ et $\exists x_{x<y}$ qui doivent porter sur des suites finies (ensembles). Pour les suites effinies, nous introduisons le quantificateur effini qui porte sur des suites illimitées comme la suite des nombres naturels.

8) Descente infinie (positive)

$$\ddagger x\{([Ax \wedge \exists x(y \prec x)Ax] \rightarrow \exists y Az(z \prec y)Az) \rightarrow$$

$$\exists z(z = 0 \vee 1 \vee n)Az\} \rightarrow \ddagger x Ax$$

8′) Descente infinie (négative)

$$\ddagger x\{[Ax \wedge \exists y(y \prec x)Ay] \rightarrow \exists y \ddagger z(z \prec y)Az\} \rightarrow \ddagger x \neg Ax$$

Le postulat de la descente infinie est substitué ici au postulat de Peano et il est clair que les quantificateurs $\forall$ et $\exists$ ne portent que sur des suites finies (ou ensembles). Il n'y a pas de suite infinie ou d'ensemble infini dans notre axiomatisation. Le postulat de Fermat, comme nous pouvons l'appeler, permet non seulement l'induction « inverse » sur les prédécesseurs, mais en tant qu'algorithme euclidien généralisé, il permet aussi la réduction et la décomposition polynomiale en arithmétique générale (kroneckerienne) où l'exponentiation est aussi bornée par le degré fini des polynômes. Le fait que le quantificateur effini n'est pas borné autorise l'usage du postulat de Fermat comme principe d'induction en arithmétique. Mais ce principe d'induction n'est pas équivalent au principe d'induction complète, à l'induction transfinie ou au principe du plus petit nombre qui eux sont tous équivalents du point

de vue classique par la voie indirecte, c'est-à-dire la voie du tiers exclu ou de la double négation qui est impraticable pour l'arithméticien et le logicien constructiviste.

B.5 Arithmétisation de la syntaxe

Dans sa preuve classique sur l'incomplétude de l'arithmétique de Peano, Gödel [48] suppose la consistance oméga de l'arithmétique définie sur l'ensemble infini des nombres naturels. La formulation originale au deuxième ordre du postulat d'induction chez Peano était fondée sur l'existence d'un tel ensemble infini

$$\exists x\{\phi \in x \wedge \forall y(y \in x \rightarrow Sy \in x)\} \rightarrow \forall y \in x.$$

Le système formel S_2 de l'arithmétique de Peano est cependant fini au sens de la métamathématique de Hilbert et afin de représenter le système formel dans l'arithmétique de Peano, Gödel assigne des nombres naturels (les nombres de Gödel) aux signes primitifs de S_2 et aux suites finies de tels signes (les formules de S_2). Gödel écrit par exemple,

"0"...1	" "...5	"π"...9
"f"...3	"$\vee$"...7	"("...11
		")"...13 ;

la bijection entre une suite finie de nombres naturels et une suite finie de signes de $L(S_2)$, le langage du système formel, est accompagnée d'une application

$$\phi : N_s \rightarrow N$$

des suites finie de nombres naturels sur les nombres naturels qui associe bijectivement cette fois à la suite $n_1, n_2, \ldots, n_k$ le nombre

$$2^{n_1} \cdot 3^{n_2} \cdot \ldots \cdot p_k^{n_k}$$

où p_k dénote le $k$ième nombre premier. Gödel veut ainsi plonger le système formel dans l'arithmétique de Peano. Cette arithmétique est l'arithmétique des fonctions récursives primitives construites par substitution et composition (ou récursion) à partir des fonctions initiales de successeur, des fonctions constantes dont la fonction zéro

$$\forall x(Zx = 0)$$

et les fonctions d'identité. Si l'on en a en plus, comme chez Gödel, la fonction μ pour « le plus petit nombre k tel que »

$$\phi(k+1, x_2, ..., x_n) = \mu(k, \phi(k, x_2, ..., x_n), x_2, ..., x_n),$$

on obtient les fonctions récursives générales. Mais si les fonctions récursives sont des fonctions arithmétiques, elles ont pour domaine et codomaine l'ensemble dénombrable $\aleph_0$ des nombres naturels et ne se prêtent pas naturellement à un calcul fini.

Dans les mots de Gödel, la consistance ω est définie pour les propriétés $P(x)$ des nombres naturels, puisqu'elle suppose le parcours complet des valeurs d'une fonction définie sur l'ensemble des nombres naturels. La consistance simple de Rosser pour l'arithmétique de Peano ne fait que substituer à la consistance oméga le concept d'énumérabilité récursive qui lui est équivalent par le recours récursif $\aleph_0 = card\, N$.

La représentation polynomiale joue ici sur un autre plan. Prenons, par exemple, les formes quadratiques binaires $x^2 + y^2$; ce sont des polynômes homogènes du second degré (avec deux variables ici) et ils induisent des représentations équivalentes d'entiers [18]. Par l'isomorphisme entre polynômes p et entiers a

$$\sum_{k \leq n} a_k^{p_k}$$

— pour un entier a et p premier ou non — les signes et suites de signes, e.g., les formules, peuvent être représentées par des polynômes. Une polynôme réduit dans un corps fini $F_q(x)$ de q éléments est simplement un polynôme de degré moindre que q en chaque variable. Tout polynôme

$$f(x) \in F[x_1, \ldots, x_n]$$

dans ce contexte est équivalent à une polynôme réduit (voir [65]).

Si nous passons aux fonctions récursives générales avec l'opérateur μ, une voie d'évitement est assurément fournie par le polynôme réduit minimal qui est irréductible (étant linéaire ou de degré 1) ou encore si nous descendons (ou réduisons) jusqu'à 0. Puisque l'on peut utiliser le théorème du reste chinois sur les congruences, par l'algorithme d'Euclide généralisé (descente infinie), on atteint un polynôme minimal de degré 1, degré 0 (pour le polynôme constant) ou degré $-\infty$ pour le polynôme zéro (pour zéro le plus petit ordinal). Par ailleurs, le plus petit entier dans un corps fini est évidemment un entier fini et correspond au degré du polynôme minimal (de degré minimal) qui est irréductible.

On peut voir tout de suite comment opère la traduction polynomiale pour les nombres de Gödel que nous remplaçons par ce que nous pourrions bien appeler les polynômes de Gödel. Prenons la fonction β de Gödel qui servait à représenter les suites de nombres naturels (ou les énoncés portant sur ces suites). C'est une fonction un peu artificielle qui s'appuie sur le théorème du reste chinois pour obtenir une fonction récursive primitive. Pour continuer la périphrase de Gödel, on n'a qu'à introduire la notion de polynôme réduit qu'on écrit

$$P(\overline{x}) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

ou

$$P(\overline{x}) = \sum_{i=0}^{n} a_i x^i$$

pour $\overline{x}$ représentant la suite de nombres naturels $(x_1, \ldots, x_n)$. De même, au nombre de Gödel d'une suite $\overline{x}$, on substitue le monôme

$$M(\overline{x}) = a_i x_1^{i_1} a_i x_2^{i_2} \ldots a_i x_n^{i_n}$$

avec $\sum(i_1, i_2, \ldots, i_n)$.

B.6 Polynomialisation

Nous allons avoir besoin de certains faits touchant aux polynômes en une indéterminée dans la preuve de consistance. Nous passons rapidement sur les notions préliminaires (l'anneau gradué de deux ou plusieurs polynômes a le même produit de convolution, notre principal outil).

Les polynômes de la forme

$$P = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

où les a_i sont les coefficients avec l'indéterminée x constituent le sous-anneau $K[x]$ de l'anneau $K[[x]]$ des séries de puissances formelles. Le degré k d'un polynôme est le degré du dernier coefficient non nul ($k = n$), alors que le coefficient principal d'un polynôme P de degré k est la constante P_k et P est appelé monique si son coefficient principal est 1. Les polynômes sont donc des séries de puissances qui n'ont qu'un nombre fini de coefficients non nuls. Le produit de Cauchy ou d'involution de deux polynômes joue un rôle important

dans notre traduction ; nous l'écrivons

$$P \cdot Q = (\sum_m P_m x^m)(\sum_n Q_n x^n) = \sum_m \sum_n P_m Q_n x^{m+n}.$$

La somme $P + Q$ des polynômes P et Q est obtenue en additionnant simplement les coefficients correspondants. Les polynômes homogènes ont tous leurs termes non nuls du même degré et ils peuvent être mis dans la forme suivante des puissances décroissantes

$$P = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n.$$

Nous nous intéressons aux polynômes irréductibles (premiers dans $K[x]$). Tout polynôme linéaire est irréductible. $K[x]$ a la propriété de factorisation unique et ce fait est crucial pour ce qui suit.

Nous allons faire un emploi essentiel de la notion kroneckerienne de contenu des formes. Une forme M est un terme dans une autre forme M' quand les coefficients de la première sont « convolutés » (combinés dans un produit de Cauchy) dans les coefficients du second. Cette idée d'un contenu « *Enthalten-Sein* » des formes se résume dans l'énoncé « le contenu du produit est le produit des contenus (de chaque forme) » qu'on peut extraire du texte de Kronecker [73]. Ainsi, pour qu'une forme soit contenue ou incluse dans une autre forme il suffit qu'elle soit combinée avec elle linéairement (avoir ses puissances convolutées avec les puissances de la seconde forme).

On peut adopter alors le principe général de la substitution-élimination de Kronecker [73]. Nous énonçons le principe de substitution de la façon suivante :

1) Deux formes homogènes (polynômes) F et F' sont équivalentes si elles ont les mêmes coefficients (ou les mêmes diviseurs, en particulier le même plus grand commun diviseur).
2) Les formes peuvent se substituer aux indéterminées (variables) pourvu que la substitution (linéaire) se fasse avec des coefficients entiers.

Nous avons comme conséquence immédiate la proposition 1 (proposition X chez Kronecker [73]) :

> Les formes linéaires homogènes qui sont équivalentes peuvent se transformer l'une dans l'autre par la substitution de coefficients entiers.

Nous avons aussi la proposition 2 (proposition X° chez Kronecker [73]) :

> Deux formes sont absolument équivalentes quand elles se contiennent l'une l'autre.

Et Kronecker énonce ici ce qu'il considère comme un de ses résultats principaux, $XIII^{\circ}$:

> Toute forme algébrique entière est représentable comme produit de formes irréductibles (formes premières) de façon unique.

C'est là l'équivalent du théorème fondamental de l'arithmétique élémentaire sur la factorisation unique des entiers par un produit de facteurs premiers. La procédure de substitution est simultanément une procédure d'élimination, puisque les indéterminées « *Unbestimmte* » sont remplacées par des coefficients entiers. Ainsi, une réserve indéfinie (ou effinie) de variables est mise à la disposition d'un système polynomial et réduite ensuite par la méthode de substitution-élimination à une suite descendante finie de nombres naturels comme nous allons le voir ci-après.

Le procès de substitution a lieu à l'intérieur de l'arithmétique, dans le corps de Galois F^*, le corps minimal ou corps de base des polynômes qui est le lieu propre de la traduction et les indéterminées — Kronecker emprunte à Gauss ses « *indeterminatae* » — sont les outils appropriés pour la transformation des formules en polynômes. L'idée centrale est que les indéterminées dans le sens de Kronecker peuvent êtres adjointes et expulsées librement et bien que Kronecker n'ait pas toujours supposé que ses formes étaient homogènes, nous nous restreignons aux polynômes homogènes.

Nous introduisons un isomorphisme

$$\psi : Form \rightarrow Poly$$

entre les formules et les polynômes en huit clauses :

Clause 1) Une formule atomique est représentée polynomialement par l'isomorphisme

$$\psi : (A)[n] \ \cong \ a_0 x (\text{pour un } A \text{ arbitraire})$$

(où la partie a_0 est appelée la « déterminée » et la partie x « l'indéterminée »).

Ici, le coefficient a_0 correspond à un nombre naturel donné « l'évaluateur ») et 0 indique qu'il s'agit du premier membre de la suite, x étant son indéterminée associée.

Il importe de préciser que le degré du polynôme correspond à l'évaluateur indiqué par $[n]$ qui représente le nombre de Gödel de la formule A. L'abréviation $[n]$ dénote le nombre de Gödel déjà associé à la formule A. C'est donc un « polynôme de Gödel » associé à la formule A que nous pouvons identifier au degré n ; $[n]$ pourrait être, par exemple, le nombre de Gödel suivant

$$2^{107} \cdot 3^3 \cdot 5^{13} \cdot 7^7 \cdot 11^{21} \cdot 13^5 = n! \ldots$$

dans le cas d'une numération de Gödel. Nous assignons plutôt un n indéterminé aux seules formules et non à tous les symboles ; cet n indéterminé est un nombre premier dans le corps fini $F(x)$ des polynômes irréductibles où nous opérons. L'évaluateur numérique $[n]$ associé aux formules par la fonction d'évaluation

$$\phi : Form \rightarrow (0, 1)$$

doit donc être distingué nettement de l'évaluateur polynomial n correspondant au degré du polynôme par la fonction d'évaluation polynomiale

$$\chi : Poly \rightarrow (0, 1).$$

Nous identifions les polynômes par leurs premiers coefficients.

La fonction d'identité

$$I : A \rightarrow A$$

est une fonction constante. Les formules moléculaires sont constituées de monômes et leur représentation polynomiale s'effectue sur les composantes atomiques à l'aide de l'isomorphisme

$$\psi : Form \rightarrow Poly.$$

Clause 2) La négation d'une formule atomique est traduite par

$$\psi : (\neg A)[n] \ \cong \ 1 - a_0 x.$$

Ici nous pouvons introduire tout de suite la fonction d'évaluation polynomiale

$$\chi : Poly \rightarrow (0, 1)$$

qui évalue $a_0 x$ à 1 et $(1 - a_0 x)$ à 0. Au lieu d'identifier 1 à la valeur numérique du monôme, je préfère définir la valeur 1 comme polynôme unitaire $P_{(deg1)}$

(défini sur les nombres premiers) dont le degré est 1 et 0 au polynôme zéro P qui n'a pas de degré, mais est noté $-\infty$. Enfin, on peut remarquer que nous recourons ici à une notation déjà utilisée par Peirce, Schröder et Skolem pour la conjonction, la disjonction, la négation, l'implication et les quantificateurs universel et existentiel en accord avec la tradition arithmétique ou algébrique de la logique.

Clause 3) La conjonction de A et B est traduite par

$$\psi : (A \wedge B)[n] \ \cong \ ((a_0 x) \cdot (b_0 x))$$

pour le produit des monômes $(a_0 x)$ et $(b_0 x)$.

Clause 4) La disjonction A ou B est traduite par

$$\psi : (A \vee B)[n] \ \cong \ ((a_0 x) + (b_0 x)).$$

Clause 5) L'implication locale $A \rightarrow B$ est rendue par

$$\psi : (A \rightarrow B)[n] \ \cong \ (\overline{a}_0 x + b_0 x)^n$$

pour $\overline{a}_0 x = 1 - a_0 x$.

Remarques : Comment l'implication est-elle interprétée polynomialement ? Un produit développé de polynômes a la forme

$$a \cdot b = (\sum_i a_i x^i)(\sum_j b_j x^j) = \sum_i \sum_j a_i b_j x^{i+j}.$$

Pour a^b nous pourrions simplement écrire $(a+b)^n$ pour les coefficients binomiaux et mettre

$$(a_0 x + b_0 x)^n = a_0^n x + n a_1^{n-1} x b x + [n(n-1/2!)] a_2^{n-2} x^2 b_2 x^2 + b_0^n x$$

en plus court

$$(a_0 x + b_0 x)^n_{i<n} = \sum_{i+j=n} (i+j) a^i b^j x^n.$$

Le motif de cette traduction, c'est que nous voulons rendre la notion d'inclusion de a dans b par l'entrelacement ou la combinaison des coefficients

dans un produit « croisé », la somme des coefficients étant 2^n qui est aussi la somme des combinaisons de n objets différents pris r à la fois

$$\sum_{r=0}^{n} C_n^r.$$

La combinaison linéaire des coefficients est assurément de première importance du point de vue de Kronecker et un de ses résultats fondamentaux s'énonce : « Toute fonction entière d'une variable peut être représentée comme un produit de facteurs ». Kronecker se réfère au concept de congruence chez Gauss et montre qu'un système modulaire avec des éléments infinis (indéterminés) est réductible à des éléments finis. C'est là sans doute l'origine du théorème de la base de Hilbert sur le nombre fini de formes dans tout système de formes avec

$$F = A_1F_1 + A_2F_2 + \cdots + A_mF_m$$

pour des formes définies $F_1, F_2, \ldots, F_m$ du système et des formes arbitraires $A_1, A_2, \ldots, A_m$ avec des variables (indéterminées) appartenant à un corps donné ou domaine de rationalité « *Rationalitätsbereich* ». La nature combinatoire de l'implication est explicitée dans l'expansion polynomiale et est renforcée par les traits symplectiques (entrelacés) de l'inclusion locale du contenu. On peut aussi définir l'implication en analogie avec le complément relatif

$$(2^n - a_0x) + b_0x$$

où 2^n est l'univers arithmétique en expansion polynomiale jusqu'à n. D'un point de vue topologique, c'est l'ensemble des points intérieurs qui est en jeu dans ce que j'ai appelé la négation locale [42]

$$a \to b = Int((X - a) \cup b)$$

pour X un espace topologique et a et b des ensembles ouverts. L'interprétation polynomiale conserve l'asymétrie de la négation locale avec la congruence arithmétique et le signe du complément relatif ou de la différence $\overline{a}$ dans la symétrisation des coefficients du calcul polynomial, comme on le verra plus loin.

Clause 6) $\psi : (\exists x Ax)[n] \cong \sum_{0\ldots}(a_0x, b_0x, c_0x, \ldots)_{i \prec n}$
où $\sum$ est une somme itérée d'instances numériques avec a_0 comme premier membre de la suite.

Clause 7) $\psi : (\forall x A x)[n] \cong \prod_0 (a_0 x, b_0 x, c_0 x, \ldots)_{i \prec n}$.

Clause 8) $\psi : (\exists x A x)[n] \cong \prod_{0\ldots} (a_0 x, b_0 x, c_0 x, \ldots)_n$.
Remarques : La notion de quantificateur effini doit être précisée. Alors que le quantificateur universel ne s'applique qu'aux ensembles finis, le quantificateur effini est réservé aux suites infiniment processives ou suites effinies. Ce ne sont pas des ensembles et elles n'ont pas de borne postpositionnelle ; nous assignons un n à de telles suites et 2^n aux suites de suites

$$0, 1, 2, \ldots, n, \ldots, 2^n$$

en supposant que n signifie une borne arbitraire. Il faut se rappeler que Boole a aussi un univers arithmétique dans sa *Mathematical Analysis of Logic* (1847) qu'il dénote par 1 et la négation est notée $1 - a$. Le fait que le corps $K[x]$ des polynômes possède la propriété de factorisation unique révélée par la descente infinie est lié à l'algorithme de division des nombres composés chez Euclide.

Nous avons alors une formulation combinatoire

$$\prod_{0\ldots}^{n} (a_0 x b_0 x c_0 x \ldots n_n x)^n$$

pour le quantificateur effini, puisque $n! = \prod_{c \leq n}$, les combinaisons de n. J'appelle ce schéma, l'échelle absolue ou standard. Toute autre échelle est une échelle associée (d'indéterminées) et est réductible par substitution à l'échelle absolue. Par exemple, une borne supérieure comme $2^{2^n} - 1$ n'est pas démontrée par induction complète jusqu'à 2^{2^n}, mais par régression à l'échelle absolue $2^n - 1$.

Une remarque philosophique : il n'y a pas de ω. Toute échelle ordinale transnaturelle ou transarithmétique (transfinie dans la terminologie cantorienne), e.g. ϵ_0, est une échelle associée et est par définition réductible. Il est clair, d'un point de vue kroneckerien, que l'arithmétique transfinie de Cantor est une associée superflue (de compensation *indéterminée* !). L'univers arithmétique $\mathbb{N}$ est naturellement borné par 2^n.

La preuve de la consistance interne de l'arithmétique FK (pour Fermat-Kronecker) emprunte le chemin suivant : la traduction radicale de la logique dans l'arithmétique polynomiale, le plongement de l'arithmétique dans les polynômes — avec les indéterminées jouant le rôle de variables — où le degré

d'un polynôme remplace le nombre de Gödel d'une formule ou d'un énoncé donné dans l'univers arithmétique et enfin la descente infinie qui ordonne les polynômes selon l'ordre décroissant de leurs puissances jusqu'à ce qu'on atteigne les polynômes linéaires de degré 1 (irréductibles) ou le polynôme zéro lui-même. Donc $1 \neq 0$. D'où la non-contradiction par le fait que

$$\chi : P_{(deg1)} = 1$$

et donc

$$\chi : P_{(deg0)} = 0.$$

Dans la preuve, la diagonale de Cauchy (le produit de convolution) ne nous entraîne pas hors du domaine de rationalité des polynômes et la nature combinatoire de la logique est préservée dans la clôture des extensions algébriques. L'élimination de la logique dans cette réduction arithmétique n'est pas sans rappeler l'élimination des quantificateurs due à Tarski en théorie des modèles, mais elle remonte à la source, la théorie de l'élimination de Kronecker.

B.7 Réduction

La réduction des formules logiques correspondra ici à la décomposition polynomiale : il s'agira d'éliminer les règles logiques au profit de formules de congruence dans un calcul polynomial modulaire. La méthode de la réduction en théorie des nombres concerne la réduction d'une infinité de formes à un nombre fini de formes équivalentes. Lagrange a formulé la première théorie de la réduction pour les formes quadratiques (voir A. Weil [107] et Lagrange [75]). Lagrange montre comment partir d'une forme

$$Bt^2 + Ctu + Du^2$$

où B, C et D sont des entiers, t et u aussi des entiers, mais indéterminés, comme dit Lagrange. Ces formes sont des polynômes homogènes du deuxième degré et les entiers indéterminés sont simplement les indéterminées du polynôme

$$P(x, y) = ax^2 + bxy + cy^2$$

dont le discriminant est $\Delta = b^2 - 4ac$ — le discriminant est le produit des carrés des différences des racines ou solutions de l'équation polynomiale prises deux à deux [18]. Lagrange démontre que toutes les formes de discriminant

Δ peuvent être réparties dans des classes de formes équivalentes et que ces classes sont en nombre fini. C'est par un procédé de descente que Lagrange arrive à une forme réduite minimale, puisque, comme il dit ([57], p. 400), la suite des nombres décroissants « ne saurait aller à l'infini ».

La méthode de réduction allait être largement pratiquée par les arithméticiens jusqu'à aujourd'hui. Kronecker, on le sait, en a fait un usage constant et Hilbert après avoir suivi Kronecker en arithmétique et en algèbre, a été le premier à s'en servir pour les besoins de la logique.

Hilbert a formulé une méthode pour l'élimination du symbole ϵ comme nous l'avons vu au chapitre 4.2. La réduction hilbertienne est apparentée à la méthode d'élimination–substitution de Kronecker (voir le chapitre 3) puisqu'elle a recours à une méthode de résolution symbolique privilégiée par les successeurs de Kronecker, G. Study et Emmy Noether en particulier. Hilbert et Noether ont pratiqué abondamment la décomposition polynomiale pour les formes ternaires et d'ordre supérieur. Or pour la décomposition, il faut descendre jusqu'aux formes ou polynômes linéaires (irréductibles). La réduction opère sur les formules critiques contenant le symbole e et s'accompagne d'un principe de substitution pour trouver le polynôme de résolution minimal qui conduira aux formes réduites irréductibles après un nombre fini d'opérations de substitution qui visent à éliminer en dernière instance le quantificateur existentiel de formules finales sans symbole ϵ.

Enfin la méthode de réduction qu'on peut appeler aussi méthode d'élimination, a connu un autre avatar logique dans la théorie de l'élimination des quantificateurs proposée par Tarski (voir chap. 3.4) et qui tire son origine de la méthode de Kronecker, comme l'a bien vu van den Dries [102].

B.8 Élimination des constantes logiques

Les connecteurs de négation, disjonction, conjonction sont directement éliminables dans la représentation polynomiale puisqu'on peut les interpréter comme la différence, la somme et le produit de polynômes dans un nombre fini de termes (coefficients et indéterminées).

Preuve : Réécrivons les règles logiques intélim dans le langage polynomial. L'axiome unique d'identité $A \vdash A$ devient simplement l'égalité $A = A$.

(I $\wedge$) $\dfrac{A \quad B}{A \wedge B}$; $a_0x, b_0x \equiv a_0x \cdot b_0x$

(E $\wedge$) $\dfrac{A \wedge B}{A}$ et $\dfrac{A \wedge B}{B}$; $a_0x \cdot b_0x \equiv a_0x, b_0x$

(I $\vee$) $\dfrac{A}{A \vee B} \quad \dfrac{B}{A \vee B}$; $a_0x + b_0x \equiv a_0x,\ a_0x + b_0x \equiv b_0x$

(E $\vee$) $\dfrac{\begin{array}{ccc} & [A] & [B] \\ & \vdots & \vdots \\ A \vee B & C & C \end{array}}{C}$; $\begin{array}{l} a_0x + b_0x \equiv c_0x \,(\mathrm{mod}\ b_0x) \\ a_0x + b_0x \equiv c_0x \,(\mathrm{mod}\ a_0x) \end{array}$

(I $\rightarrow$) $\dfrac{\begin{array}{c}[A] \\ \vdots \\ B\end{array}}{A \rightarrow B}$; $a_0x \equiv b_0x \,(\mathrm{mod}\ a_0x + 1)$

(E $\rightarrow$) $\dfrac{A,\ A \rightarrow B}{B}$; $1 - a_0x \equiv b_0x \,(\mathrm{mod}\ a_0x)$

(I $\neg$) $\dfrac{\begin{array}{c}A \\ \bot\end{array}}{\neg A}$; $1 - a_0x \equiv 1 \,(\mathrm{mod}\ a_0x)$

(E $\neg$) $\dfrac{A,\ \neg A}{\bot}$; $1 - a_0x \equiv 0 \,(\mathrm{mod}\ a_0x)$

$$(\mathrm{I}\ \forall)\quad \frac{Ax}{\forall x Ax}\quad ;\quad \prod_n a_0 x^n \equiv a_0 x (\mathrm{mod}\ n)$$

$$(\mathrm{E}\ \forall)\quad \frac{\forall x Ax}{At}\quad ;\quad a_0 x \equiv \prod_n a_0 x^n (\mathrm{mod}\ 1)$$

$$(\mathrm{I}\ \exists)\quad \frac{At}{\exists x Ax}\quad ;\quad \sum_n a_0 x^n \equiv a_0 x (\mathrm{mod}\ 1)$$

$$(\mathrm{E}\ \exists)\quad \frac{\begin{array}{cc} & [Ax] \\ & \vdots \\ \exists x A & B \end{array}}{B}\quad ;\quad a_0 x \equiv \sum_n b_0 x^n (\mathrm{mod}\ 1)$$

$$(\mathrm{I}\ \exists\!\!\!-)\quad \frac{Ax_n}{\exists\!\!\!- x Ax}\quad ;\quad \prod_{n\ldots} a_0 x^n \equiv a_0 x (\mathrm{mod}\ n \cdot n)$$

$$(\mathrm{E}\ \exists\!\!\!-)\quad \frac{\exists\!\!\!- x Ax}{At_0}\quad ;\quad a_0 x \equiv \prod_{n\ldots} a_0 x^n (\mathrm{mod}\ 1)$$

En traduisant les formules logiques par des formes congruentes, nous voulons représenter les constantes logiques dans un langage polynomial pour opérer l'arithmétisation intégrale de la logique. Il est donc clair que dans ce contexte, la déduction, qu'elle soit exprimée par le tourniquet $A \vdash A$ ou la barre $\frac{A}{A}$ est une relation de congruence dans une calcul modulaire.

Pour l'implication, nous adoptons l'écriture

$$(\overline{a}_0 x + b_0 x)^n$$

pour $\overline{a}_0 x = 1 - a_0 x$, le complément relatif ou local (la négation locale de la logique) ; l'exposant n désigne le degré du contenu polynomial de l'implication que nous réduisons de la façon suivante en effectuant le calcul abrégé à l'aide de polynômes homogènes symétriques — avec une fonction symétrique $f(a, b) = f(b, a)$ sur les coefficients a et b.

$$(\overline{a}_0 x + b_0 x)^n$$

$$\vdots$$

$$= a_0^n x + \sum_{k=1}^{n-1} (n - 1/k - 1)\overline{a}_0^{k-1} x + (n - 1/k) a_0^k x b_0^{n-k} x + b_0^n x$$

$$\vdots$$

$$= (\overline{a}_1 x + b_1 x)(\overline{a}_1 x + b_1 x - 1)^{n-1}$$

$$\vdots$$

$$= (\overline{a}_n x + b_n x)(\overline{a}_n x + b_n x)$$

$$\vdots$$

$$= (\overline{a}_0 x + b_0 x)$$

que nous obtenons en quatre descentes successives. Le contenu combinatoire du polynôme d'implication est exhibé par la suite de longueur $n - 1$ (pour le polynôme de degré n). L'évaluation est toujours faite sur $(0, 1)$ en donnant la valeur 1 à une expression polynomiale positive et 0 à une expression polynomiale négative comme $\overline{a}_0 x = 1 - a_0 x$.

L'élimination du quantificateur effini $\exists x A x$ procède de la même manière. La décomposition polynomiale à la Kronecker est une descente infinie de la division du contenu. Le quantificateur effini s'écrit ici $\prod_{n\ldots} a_n x^n$ et pour exhiber le produit de convolution ou le produit de Cauchy

$$\sum_0^n c_n x^n = (\sum_0 a_n x^n)(\sum_0 b_n x^n)$$

où $c_n = a_0 b_n + a_1 b_{n-1} + a_n b_0$.

Nous avons $\prod_0^n (a_0 x \cdot b_0 x)^n$ que nous prenons comme produit de monômes :

$$(a_0 x)^n \cdot (b_0 x)^n$$

$$= \begin{bmatrix} a_0^n x + \prod_{i=1}^n \sum k = 1^{n-1}(n - 1/k - 1)_1 a_0^{k-1} x + (n - 1/k)_1 + b_0 x_1 \\ \vdots \\ a_0^n x + \prod_{i=1}^n \sum k = 1^{n-1}(n - 1/k - 1)_n a_0^{k-1} x + (n - 1/k)_n (a_0^k x b_0^{n-k} x)_n + b_0^n x_n \end{bmatrix}$$

que j'amène par descente à

$$\begin{aligned} &= (a_0x + b_1)_1(a_1x + b_1x - 1)_1^{n-1} \\ &\vdots \\ &= (a_1x + b_1)_n(a_1x + b_1x - 1)_n^{n-1} \end{aligned}$$

et que je ramène enfin à

$$= \begin{bmatrix} (a_0x + b_0x)_1 \\ \vdots \\ (a_0x + b_0x)_n \end{bmatrix}$$

qui est $(a_0x) \cdot (b_0x) = \prod_n^0 (a_0x + b_0x)$.

Je peux de même pratiquer une descente simultanée sur la formule générale

$$(a_0x \cdot b_0x \cdot c_0x \cdot \cdots \cdot g_0x)^n = \prod_{abc\ldots g} \sum_{pqr\ldots s} a^p b^q c^r \ldots g^s$$

qui va me donner à la fin de la descente finie :

$$(a_0x \cdot b_0x \cdot c_0x \cdot \cdots \cdot g_0x) = \prod_0^n (a_0x + b_0x + c_0x + \cdots + g_0x).$$

B.9 Conclusion : l'extension polynomiale du point de vue finitiste

La descente infinie dans les polynômes se termine à 0 ou à 1 ; si elle se termine à 1 (le degré 1), nous avons les polynômes linéaires (et par conséquent irréductibles comme les polynômes premiers). Si la descente s'arrête à 0, le polynôme zéro n'a pas de degré (que l'on note toutefois $-\infty$). Ainsi, $1 \neq 0$. Donc,

$$a_0x \not\equiv \overline{a}_0x$$

qui est $1 \neq (1 - 1 = 0)$. □

La preuve ici est en accord avec la formulation originale de Hilbert [57] du problème de la consistance en termes d'équations (polynomiales) homogènes

$$a = a$$

ou d'inéquations

$$a \neq a.$$

L'axiome 1 de Hilbert est l'axiome d'identité (ou d'égalité) que nous avons adopté et le problème de la consistance se résume à la non dérivation de

$$a \neq a,$$

ou

$$\neg(a = a)$$

en termes logiques.

Remarquons enfin que le produit de convolution polynomiale (la diagonale de Cauchy) ne permet pas de générer le paradoxe de l'autoréférence par le truchement de la diagonale de Cantor dans l'arithmétique de Peano. Gödel avoue par ailleurs dans son texte que c'est un peu par accident si une formule obtenue par la substitution diagonale se transforme en un énoncé indécidable qui dit de lui-même qu'il est indémontrable : l'autoréférence ne serait qu'un produit dérivé de la procédure diagonale. Gödel suppose en effet la consistance ω — la consistance simple de Rosser utilise la notion équivalente de fonction récursive sur $\aleph_0 = cardN$; la diagonalisation à la Cantor permet d'identifier certains énoncés portant sur le contenu arithmétique de la théorie (la théorie-objet) avec les énoncés métalogiques de la théorie. C'est ce qui se produit dans le cas de l'énoncé indécidable dans le système formel S_2 de l'arithmétique de Peano

$$\forall \underline{x}_2 \neg P_{\underline{r}}(\overline{k}, \underline{x}_2)$$

où les expressions soulignées appartiennent au système formel et où $\overline{k}$ est le nombre de Gödel de la formule

$$\forall \underline{x}_2 \neg P_{\underline{r}}(\underline{x}_1, \underline{x}_2).$$

L'énoncé indécidable dit simplement qu'il n'y a pas de preuve de lui-même dans S_2, mais l'énoncé est vrai dans T_2 (le modèle de l'arithmétique de Peano). Le jeu de la substitution n'est pas possible dans une logique interne de l'arithmétique ou une logique polynomiale puisque la substitution par diagonalisation (de Cauchy) donnerait

$$\psi : \forall x Ax[n] = \prod_n (a_0 x, b_0 x)$$

pour un énoncé A auquel est associé son nombre de Gödel $[n]$. La représentation polynomiale va faire apparaître cet n comme

$$c_n = a_0 b_n + a_1 b_{n-1} + a_n b_0$$

ou

$$\overline{c}_n \text{ pour } 1 - c_n,$$

mais il entrera dans la computation sans paradoxe. C'est parce que le $\overline{k}$ de l'arithmétique de Peano renvoie en réalité à l'ensemble des nombres naturels situés sur la codiagonale — ou antidiagonale — des énoncés niés qu'il n'est pas récupérable sans le paradoxe de l'autoréférence. La consistance externe dans l'arithmétique ensembliste $\aleph_0$ génère le paradoxe. La consistance interne de l'arithmétique générale (polynomiale) le fait s'évanouir dans le calcul.

Dans sa preuve d'incomplétude pour l'arithmétique de Peano, Gödel admet que son second résultat d'incomplétude (sur les preuves de consistance) ne contredit pas le point de vue formaliste de Hilbert, puisqu'il est possible qu'une preuve finitiste « interne » ne puisse être formulée dans le système formel de l'arithmétique de Peano ou dans des systèmes plus englobants, i.e. la théorie des ensembles ou l'analyse classique (voir [48], p. 197). Si l'on admet que les preuves de Ackermann et de Gentzen utilisent d'une façon ou d'une autre l'induction transfinie ou l'induction complète jusqu'à

$$\lim_{n\to\infty} \omega^{\omega^{\cdots^{\omega}}\}n} < \epsilon_0$$

qui ressortit de l'arithmétique ordinale transfinie de Cantor, il faut bien reconnaître qu'il ne saurait s'agir d'une preuve interne. De même l'extension du point de vue finitiste de l'interprétation *Dialectica* qui s'appuie sur une induction complète sur tous les types finis de l'interprétation fonctionnelle ne peut prétendre à une preuve interne de la consistance interne de l'arithmétique. Gödel s'est penché sur l'interprétation *Dialectica* (sans quantificateurs) pendant plus de trente ans à partir de 1941 (voir [50] et [49]). La traduction polynomiale de l'interprétation *Dialectica* fait l'objet de [40]. Sans doute faut-il retourner à l'arithmétique de Fermat-Kronecker ou l'arithmétique générale des polynômes avec descente infinie (indéfinie ou finie) pour espérer redescendre à une preuve interne finitaire, c'est-à-dire à l'intérieur du fini.

L'extension du point de vue finitiste de Hilbert, c'est ce que vise essentiellement Gödel dans cette tentative d'élargir le programme de Hilbert, puisque son second théorème d'incomplétude de 1931 ou théorème sur les preuves

de consistance ne contredit pas le programme de Hilbert, comme il l'avoue (voir [48]). Le point de vue finitiste de Hilbert opposait la logique interne « *das innere logische Schliessen* » au traitement externe « *äusseres Handeln* » du système formel, comme Hilbert l'explique dans son texte classique « Sur l'infini » (« *Über das Unendliche* ») de 1927 (voir Hilbert [58]). Hilbert devait introduire ses éléments idéaux « *Ideale Elemente* » pour pallier la finitude du système formel. Gödel propose plutôt des notions abstraites, à la manière des intuitionnistes, comme celle de fonction computable de type fini sur les entiers pour accéder à la consistance de l'arithmétique qui demeurait une consistance externe, « *outer consistency* », c'est la consistance ω encore appelée consistance 1 aujourd'hui. En d'autres termes, la consistance oméga pour le système formel S_2 de l'arithmétique de Peano

$$\vdash_{S_2} A(\overline{n}) \rightarrow \nvdash_{S_2} \exists x \neg Ax \quad \text{pour tous les } n$$

était inaccessible au système formel finitaire et le deuxième théorème d'incomplétude permettait de loger des énoncés faux dans une théorie logique pourtant consistant — entre n et ω pourrait-on dire. Tarski supposait en 1937 que la consistance ω devait être complétée par la complétude ω dans un système qui abrite un infini actuel, alors que l'arithmétique récursive primitive n'exige qu'un infini potentiel, disait-il.

La notion centrale de l'interprétation *Dialectica* est celle de fonction computable de type fini sur les nombres naturels, dont Gödel supposera qu'elle est évidente. Ici les types sont simplement définis par les clauses suivantes : la type 0 est celui des nombres naturels et la règle de génération des types stipule que si σ et $\theta_1, \ldots, \theta_n$ sont des types, alors $(\sigma, \theta_1, \ldots, \theta_n)$ l'est aussi. Ce sont en réalité des fonctions sur des arguments θ_1 à θ_n, c'est-à-dire des fonctionnelles, puisque ces fonctions s'appliquent sur d'autres fonctions pour les types > 0, i.e. au-delà des nombres naturels considérés comme les individus de l'univers des types. La logique de l'interprétation fonctionnelle est en principe intuitionniste ou constructive dans un sens large, puisque Gödel suppose que son interprétation est indépendante de la logique intuitionniste — elle n'est pas aussi abstraite ! L'idée de Gödel consiste à traduire une formule A de l'arithmétique de Heyting par une fonction computable

$$\exists x \forall y A(x, y)$$

où A est sans quantificateur. On a ainsi pour l'égalité definitionnelle

$$\begin{array}{lcl}(A \wedge B) & := & \exists xu \forall vy (A \wedge B)' \\ (A \vee B) & := & \exists zxu \forall vy (z = 0 \vee 1) \wedge (A \vee B)' \\ \forall z A z & := & \exists x \forall z y A(xz, y)' \\ \exists z A z & := & \exists zx \forall y A(z, x, y)' \\ A \to B & := & \exists UY \forall xv (A(x, Yxv) \to B(Ux, v))'\end{array}$$

Prenons pour exemple la formulation de Gödel pour deux fonctionnelles récursives

$$F' = \exists y \forall z A(y, z, x)$$

et

$$G' = \exists v \forall w B(v, w, u)$$

où les y, z, v et w sont des suites finies de variables typées. L'implication

$$(F \supset G)' = \exists V Z \forall y, w [A(y, Z(y, w), x) \supset B(V(y), w, u)]$$

exhibe deux fonctionnelles (avec leurs variables propres) qui subordonnent (« *zuordnen* ») le conséquent à l'antécédent. On peut penser ici que le produit de convolution remplit le rôle d'extractions computationnelle du contenu de façon plus directe si on traduit

$$\exists x A x \supset \exists y B y = \sum_0^n (\Sigma \overline{a}_0 x + \Sigma b_0 x)^n$$

et

$$\forall x A x \supset \forall y B y = \prod_0^n (\Pi \overline{a}_0 x \cdot \Pi b_0 x)^n$$

pour obtenir le contenu formel des formes (polynômes homogènes) au sens de l'implication ou de l'inclusion des contenus « *Enthalten-Sein* » comme le voulait Kronecker. Le calcul du contenu est-il concret ou abstrait ? Il n'y a pas de doute que le contenu polynomial est davantage extensionnel qu'intensionnel (abstrait) et qu'il satisfait aux deux exigences de la constructivité et de la finitude qui semblent être les motifs principaux de Gödel dans son interprétation *Dialectica* destinée à la preuve de la consistance interne de l'arithmétique, d'abord celle de Heyting, puis celle de Peano. Dans notre cas, c'est l'arithmétique de Fermat et l'arithmétique générale de Kronecker qui sont nos cibles et qui constituent la véritable théorie des nombres enrichie de l'arithmétique polynomiale.

L'interprétation *Dialectica* joue un rôle central dans le programme de la théorie concrète des preuves proposée par U. Kohlenbach — voir [69]. Le théorème de Herbrand (voir ci-dessus le chapitre 4.3) est aussi un outil important dans l'extraction des preuves (*proof mining*) concrètes ou effectives, mais les bornes exhibées sont parfois difficilement computables et les méthodes d'extraction ne sont pas toujours constructives. Pour Herbrand, il s'agissait de réduire la logique des prédicats du premier ordre à une logique propositionnelle avec disjonctions et conjonctions pour tenir lieu des quantificateurs dans ce qu'il appelait un champ infini ou potentiellement infini. Son théorème principal comprenait pour la logique des règles de passage (ou d'inférence) qui devaient respecter certaines propriétés A, B, C. La propriété C dans le texte de Herbrand [56] a fait l'objet de corrections de la part d'auteurs comme Dreben, Denton, Andrews et Anderea. Le lemme 3.3 dans le texte de Herbrand stipulait que :

> Une formule a la propriété C d'ordre p, ssi son expansion utilisant tous les termes du champ C est de profondeur (d'imbrication) moindre que p est une tautologie.

Une expansion de Herbrand consiste à transformer une quantification existentielle en disjonction de ses termes et une quantification universelle en une conjonction de ses termes dans le même domaine pour la logique du premier ordre. On peut produire un contre-exemple en montrant qu'une formule comme

$$\neg[\forall x \phi x \vee \neg \forall y A y] \vee \forall y_1 \phi y_1 \vee \neg \forall x_i A x_i$$

n'a pas la même profondeur d'imbrication ou le même ordre que

$$\neg \forall x [\phi x \vee \neg \forall y A y] \vee \forall y_1 \phi_1 \vee \forall x_i A x_i$$

La traduction polynomiale montre immédiatement par le passage de

$$1 - (\Pi x\, \phi(x_n) + 1 - \Pi y\, A(y_n)) + \Pi y\, \phi(y_n) + 1 - \Pi x\, A(x_i)$$

à

$$1 - \Pi x\, \phi(x_n) + 1 - \Pi y\, A(y_n) + \Pi y\, \phi(y_n) + 1 - \Pi x\, A(x_i)$$

qu'un simple calcul numérique augmente le degré du premier polynôme par la parenthétisation qui devient une somme par l'addition des coefficients — la notion de degré pour un polynôme signifie le suprémum pour les indices des coefficients et la notion d'ordre leur infimum, de sorte que les notions

de degré et d'ordre devraient être complémentaires, mais il se trouve que le produit de convolution (ou produit de Cauchy) influe directement sur le degré d'un polynôme. Le produit de convolution va doubler le degré des polynômes sommés, de sorte que si la deuxième expression est en polynômes quadratiques, la première devrait être en polynômes de quatrième degré (ou polynômes bi-quadratiques) ; d'où le fait que les deux expressions n'ont pas la même profondeur d'imbrication. S'il est permis de penser que Herbrand avait déjà une expérience < polynomiale > en théorie algébrique des nombres avec les notions de hauteur(pour les valeurs complexes d'un polynôme) et d'ordre qu'il utilise dans son texte, il suffit de conclure que le traitement polynomial des expansions de Herbrand en termes de polynômes suffit à colmater la brèche du lemme fautif. L'utilisation du théorème de Herbrand en déduction automatique et en extraction des preuves recourt à la mise en forme normale prénexe en préfixant la quantification universelle et qui correspond pour la logique à la réduction polynomiale par descente sur le degré d'un polynôme — il est clair que l'expansion de la disjonction de Herbrand correspond à l'addition des coefficients d'un polynôme réductible. Il faut cependant admettre que les calculs numériques sur les polynômes peuvent être fastidieux et que la logique à ce compte offre des raccourcis appréciables, souvent à des coûts exorbitants lorqu'il faut prendre des détours (*Umwege*), comme disait Hilbert à propos des éléments idéaux, par des voies non constructives. En tout cas pour ce qui touche l'extraction des bornes, la théorie des nombres à l'aide des diverses techniques de majoration et de minorisation avec résultats numériques aussi bien en théorie des nombres élémentaires (sans moyens analytiques) qu'en théorie algébrique des nombres et en théorie analytique des nombres et jusqu'à la géométrie arithmétique (ou algébrique), la logique extractive ne peut jouer qu'un rôle adventice. Le programme de la théorie des preuves appliquée(s) joue cependant dans le ventre de l'analyse classique en extrayant de l'information effective des preuves non constructives, de la théorie de l'approximation à la théorie ergodique.

Rappelons que l'interprétation *Dialectica* a inspiré nombre de travaux, ceux de Kreisel, Spector, Luckhardt, Scarpellini, Girard et plus récemment, ceux de Kohlenbach, Fereira et Oliva ou encore Schwichtenberg dans le programme d'extraction (de minerai constructif) des preuves de l'analyse classique. E. Bishop a repris dans [7] l'implication de Gödel ci-haut qu'il a appelée implication numérique pour en montrer le caractère constructif. Il faudrait parler plutôt d'implication polynomiale, comme je l'ai fait, puisque c'est le contenu polynomial de l'implication qui est en jeu selon l'arithmétique gé-

nérale de Kronecker — dont se réclame Bishop — et non pas seulement l'arithmétique des entiers. Notons aussi que l'interprétation *Dialectica* est apparentée au travail de Herbrand sur la consistance de l'arithmétique. L'interprétation sans contre-exemple, qui est due à Herbrand, a été reprise par Kreisel à la suite de *Dialectica* en termes de fonctionnelles de type supérieur, là ou Herbrand utilisait une interprétation *négative*, selon l'expression de Hilbert et Bernays (voir [61]) en introduisant des fonctions récursives primitives comme dans

$$\neg A \equiv \neg B(x, f(x), z, g(x, z)).$$

Kreisel [71] a voulu introduire à la suite de l'interprétation *Dialectica* l'idée d'énoncés extensionnellement définis pour une interprétation « forte » des constantes logiques dans le cadre d'une sémantique ensembliste des conditions de vérité. Ainsi, la disjonction $\vee$ aura-t-elle la forme

$$a, M, X \| B(a) \vee C(a)$$

signifie

$$a, M, X \| B(a) \quad ou \quad a, M, X \| C(a)$$

ce qui veut dire que l'on a soit $B(a)$, soit $C(a)$ dans tous les sous-modèles M_1 d'une théorie X pour les énoncés a d'une théorie des types finis à la manière de l'interprétation *Dialectica*. La tentative de Kreisel consiste essentiellement en une réinterprétation intuitionniste des constantes logiques en termes d'une sémantique ensembliste, tentative qui n'a pas porté fruit, mais on peut penser que c'est dans cette foulée de l'interprétation *Dialectica* que Cohen a introduit sa notion de « *forcing* » dans sa preuve d'indépendance de l'hypothèse du continu dans l'axiomatique de Zermelo-Fraenkel (voir [38], 88). La clause de contrainte « *forcing* » C pour la disjonction, par example, se lit

$$C \Vdash (A \vee B) \leftrightarrow_{\mathrm{df}} \; C \Vdash A \vee C \Vdash B$$

et pour l'implication $\rightarrow$

$$C \Vdash (A \rightarrow B) \leftrightarrow_{\mathrm{df}} \; C \Vdash B \vee C \Vdash \neg A$$

avec

$$C \Vdash \neg\neg A \nleftrightarrow C \Vdash A.$$

Les conditions de contrainte sont compatibles avec la logique intuitionniste, comme on le voit même si elles ont servi à un autre dessein que celui de la

consistance de l'arithmétique, le dessein original de Gödel — l'idée de Kreisel visait la complétude sémantique, le « *forcing* » de Cohen la consistance de la négation de l'hypothèse du continu dans Z-F. Gödel renouait cependant avec le projet d'une preuve de consistance de l'arithmétique telle qu'elle avait été formulée par Hilbert d'abord en 1904 puis reprise dans les années 20 [57]. Hilbert formulait la consistance en termes d'équations homogènes primitives qui doivent conserver la validité des inférences logiques dont les conséquences « *Folgerungen* » sont codées en suites « *Folgen* » homogènes gérées par l'égalité définitionelle récupérée par Gödel. Pour Hilbert, l'égalité définitionnelle rend possible la consistance par la conservation des équations polynomiales

$$x = x$$

et

$$x = y \wedge w(x) \rightarrow w(y)$$

où w est un combinaison arbitraire d'objets x et y. Hilbert parle alors de composition et de décomposition de signes numériques ou numéraux « *Auf- und Abbau der Zahlzeichen* » auxquels doit se réduire la procédure de démonstration et il invoque une sorte d'induction interne « *inhaltliche Induktion* » qu'il veut distinguer de l'induction mathématique. En réalité, l'élimination des objets idéaux et de la fonction transfinie epsilon (voir [61]) est une véritable descente « *Abstieg* » au sens où Ackermann l'utilisera dans sa preuve de consistance de l'arithmétique avec induction transfinie. Cette récurrence comme l'appellera Herbrand doit se terminer dans le fini et j'y vois là une démarche démonstrative parfaitement analogue à la descente infinie dont j'ai montré ailleurs qu'elle n'était pas équivalente à l'induction complète [42]. C'est ce fondement combinatoire que l'interprétation ou la traduction polynomiale que j'ai proposée veut recouvrer dans l'esprit hibertien de la consistance de l'arithmétique. La traduction de l'implication énoncée plus haut

$$\psi : (A \rightarrow B)[n] \cong (\overline{a}_0 x + b_0 x)^n$$

et dans sa version congruente

$$a_0 x \equiv b_0 x (\text{mod } a_0 x + 1)$$

ou dans la version fonctionnelle

$$\exists x A x \supset \exists x B y = \sum_0^n (\Sigma \overline{a}_0 x + \Sigma b_0 x)^n$$

vont au-delà de la formule ensembliste

$$a \rightarrow b = \neg a \vee b$$

et de son interprétation topologique

$$a \rightarrow b = In((X - a) \cup b)$$

pour restaurer le sens polynomial (homogène et continu) qui est à l'origine de l'idée de consistance dont Kronecker avait entrevu la teneur mathématique avant que Hilbert en fasse un problème logique. Que l'on puisse aller au-delà de l'arithmétique finie à l'arithmétique récursive primitive et à des systèmes plus forts, comme le souhaitaient Hilbert et Gödel, c'est là un problème d'extension non finitiste dans le même sens où l'on peut dire que les séries (de puissances) infinies sont une extension des polynômes finis, ce qu'un constructivisme strict ne peut admettre que comme passage à la limite, ou encore comme prolongement analytique ...

Mais il semble que ce soit de prospection philosophique ou fondationnelle qu'ait besoin le travail de Gödel qui est resté insatisfait jusqu'à la fin de ses réflexions philosophiques sur le sujet. La consistance interne de l'arithmétique doit être fondée aux yeux de Gödel sur la notion de fonctionnelle computable de type fini sur les entiers. La voie qu'avaient empruntée Gentzen, Ackermann et d'autres pour la consistance de l'arithmétique était trop spéculative et il doutait que l'on puisse aller au-delà de ω^2 dans la hiérarchie des $\omega < \epsilon_0$ qui avait servi à Gentzen, même si on ne devait monter dans l'échelle (sans quantificateurs) de l'induction transfinie des ordinaux qu'un échelon à la fois. Mais la voie des fonctionnelles sur tous les types finis demeure imprédicative, ce qui ampute considérablement son caractère constructif et du même coup « évidentiel » ou probant, malgré le souhait de Gödel. Puisque ce souhait consistait à produire une preuve de la consistance de l'arithmétique libérée de la logique, c'est-à-dire en éliminant la logique ou le système formel, la traduction polynomiale de la syntaxe arithmétique à l'aide des polynômes (de Gödel) dans l'anneau $K[x]$ des polynômes irréductibles avec coefficients dans le corps $k(x)$ va exhiber la descente infinie (ou indéfinie et en réalité finie dans les corps fini $F(x)$) qui permet d'éliminer les constantes logiques (en particulier les quantificateurs) pour en arriver à l'équation polynomiale ultime

$$deg0 \neq deg1$$

ou

$$deg - \infty \neq deg 0,$$

ce qui signifie simplement que le contenu computable d'une fonction (polynomiale) est computable en temps fini ; c'est ce que l'interprétation fonctionnelle *Dialectica* ne parvient pas à accomplir, mais que l'interprétation polynomiale a pour but de rendre possible et que les travaux récents sur l'interprétation fonctionnelle pour l'arithmétique faisable ou pour l'arithmétique bornée ne font que partiellement et par des moyens indirects (voir en particulier [5], [17], [29]). En réalité, le temps polynomial pour la complexité d'un calcul ou d'un algorithme peut être réduit arbitrairement (à un temps linéaire ou quadratique) ; ce qui importe, c'est que le cadre computationnel général puisse se prêter directement au calcul concret. La traduction polynomiale (en termes de polynômes congruents) de la logique dans une arithmétique modulaire à la Fermat-Kronecker nous fournit ce cadre général. Une belle illustration de ce fait est le résultat récent d'Agrawal, Kayal et Saxena (voir [2]) qui utilise le « petit » théorème de Fermat

$$a^{p-1} \equiv 1 \pmod{p}$$

où p est un nombre premier et a est un nombre premier relatif à p. C'est cette congruence qui fonde l'algorithme pour la factorisation des grands nombres premiers et on peut penser que le temps polynomial est dérivé d'un phénomène antérieur au programme de calcul et est enraciné dans la logique interne de l'arithmétique modulaire.

La logique polynomiale modulaire ne requiert pas de sémantique véri-conditionnelle ou ensembliste pour la vérification de a = a, seulement une syntaxe dont la correction est assurée par le calcul ou les *calculi* du latin, petits cailloux sur lesquels il fallait marcher à petits pas ou pas à pas (*Schritt zu Schritt*), selon le conseil de Kronecker. Petits calculs du castor, dira le poète (Jacques Brault), mais c'est là le labeur du castor bricoleur, ajoutera le logicien constructiviste qui aménage sous la surface le barrage de l'infini fluide.

Références bibliographiques

[1] W. Ackermann : Zur Widerspruchsfreiheit der reinen Zahlentheorie. *Mathematische Annalen*, 117(2):162–194, 1940.

[2] M. Agrawal, N. Kayal et N. Saxena : PRIMES is in P. *Annals of Mathematics*, 160:781–793, 2004.

[3] S. Artemov : Explicit provability and constructive semantics. *Bulletin of Symbolic Logic*, 7(1):1–36, 2001.

[4] J. Avigad : Number Theory and Elementary Arithmetic. *Philosophia Mathematica*, XI:257–284, 2003.

[5] J. Avigad et S.Feferman : Gödel's Functional ('Dialectica') Interpretation. *In* S.R. Buss, éditeur : *Handbook of Proof Theory*, volume 137 de *Studies in Logic and the Foundations of Mathematics*, pages 337–405. Elsevier, New York, 1998.

[6] E. Bishop : *Foundations of Constructive Analysis*. McGraw-Hill, New York, 1967.

[7] E. Bishop : Mathematics as a Numerical Language. *In Intuitionism and Proof Theory*, pages 53–71. North-Holland, Amsterdam and New-York, 1970.

[8] J. Boniface et N. Schappacher : Sur le nombre en mathématique. Cours inédit de Leopold Kronecker à Berlin en 1891. *Revue d'histoire des mathématiques*, 7:207–275, 2001.

[9] G. Boolos : *Logic, Logic and Logic*. Harvard University Press, Cambridge, Mass, 1998.

[10] G. Boolos et R. Jeffrey : *Computability and Logic*. Cambridge University Press, Cambridge, 3rd édition, 1989.

[11] N. Bourbaki : *Théorie des ensembles*. Hermann, Paris, 1970.

[12] L.E.J. Brouwer : *Collected Works, vol. I.* North-Holland, Oxford, Amsterdam, 1975.

[13] J. Burgess : *Fixing Frege.* Princeton University Press, Princeton, NJ, 2005.

[14] S. Buss : *Bounded Arithmetic.* Bibliopolis, Napoli, 1986.

[15] G. Cantor : *Abhandlungen mathematischen und philosophischen Inhalts, hrsg. v. Zermelo u. A. Fraenkel.* Gauthier-Villars, Paris, 1847.

[16] A. Cauchy : *Oeuvres complètes, IIe série, tome III.* Gauthier-Villars, Paris, 1847.

[17] S. Cook et A. Urquhart : Functional Interpretations of Feasibly Constructive Arithmetic. *Annals of Pure and Applied Logic*, 63:103–200, 1993.

[18] A. Davenport : *The Higher Arithmetic.* Chap. VI. Hutchinson University Library, London, 1968.

[19] P. de Fermat : *Oeuvres*, volume II. Gauthier-Villars, Paris, 1899.

[20] R. Dedekind : *Was sind und was sollen die Zahlen. Stetigkeit und irrationale Zahlen.* Fried. Vieweg und Sohn, Braunschweig, 1965.

[21] M. Dummett : *Elements of Intuitionism.* Oxford University Press, Oxford, 2nd édition, 2000.

[22] H. M. Edwards : An appreciation of Kronecker. *The Mathematical Intelligencer*, 9(1):28–35, 1987.

[23] H. M. Edwards : *Divisor Theory.* Birkhaüser, Basel, 1987.

[24] H. M. Edwards : Kronecker's arithmetic theory of algebraic quantities. *Jahresbericht der Deutschen Mathematiker Vereinigung*, 94(3): 130–139, 1992.

[25] H. M. Edwards : *Essays in Constructive Mathematics.* Springer, New York, 2005.

[26] H. M. Edwards, O. Neumann et W. Purkert : Dedekinds "Bunte Bemerkungen" zu Kroneckers "Grundzüge". *Archive for History of Exact Sciences*, 27(1):49–85, 1982.

[27] C. Eisele : *Studies in the Scientific and Mathematical Philosophy of C. S. Peirce.* R.M. Martin, ed. Mouton, The Hague, 1979.

[28] S. Feferman : Arithmetization of metamathematics in a general setting. *Fundamenta mathematicae*, XLIX:35–92, 1960.

[29] F. Ferreira et P. Oliva : Bounded Functional Analysis. *Annals of Pure and Applied Logic*, 135:73–112, 2005.

[30] G. Frege : *Grundgesetze der Arithmetik*. H. Pohle, Jena, 1983.

[31] Y. Gauthier : *Fondements des mathématiques. Introduction à une philosophie constructiviste*. P.U.M., Montréal, 1976.

[32] Y. Gauthier : Foundational Problems of Number Theory. *Notre Dame Journal of Formal Logic*, 19:92–100, 1978.

[33] Y. Gauthier : Le constructivisme de Herbrand. *Journal of Symbolic Logic*, 48(4):1230, 1983.

[34] Y. Gauthier : A Theory of Local Negation. The Model and Some Applications. *Archiv für mathematische Logik und Grundlagenforschung*, 25:127–143, 1985.

[35] Y. Gauthier : Finite Arithmetic with Infinite Descent. *Dialectica*, 43(4):329–337, 1989.

[36] Y. Gauthier : *De la logique interne*. Vrin, Paris, 1991.

[37] Y. Gauthier : Hilbert and the Internal Logic of Mathematics. *Synthese*, 101:1–14, 1994.

[38] Y. Gauthier : *Logique et fondements des mathématiques*. Diderot, Paris, 1997.

[39] Y. Gauthier : *La logique interne. Modèles et applications*. Diderot, Paris, 1997.

[40] Y. Gauthier : A Polynomial Translation of Gödel's Functional Interpretation. *Bulletin of the Section of Logic, University of Łódź*, 27(3):130–137, 1998.

[41] Y. Gauthier : The Internal Consistency of Arithmetic with Infinite Descent. *Modern Logic*, VIII(1/2):47–87, 2000.

[42] Y. Gauthier : *Internal Logic. Foundations of Mathematics from Kronecker to Hilbert*. Kluwer, Synthese Library, Dordrecht/Boston/London, 2002.

[43] Y. Gauthier : *La logique du contenu. Sur la logique interne*. L'Harmattan, Paris, 2004.

[44] Y. Gauthier : *Bulletin of Symbolic Logic*, 13(1):136–137, 2007.

[45] Y. Gauthier : Classical Function Theory and Applied Proof Theory. *International Journal of Pure and Applied Mathematics*, 56(2):223–233, 2009.

[46] G. Gentzen : *Collected Papers.* E. Szabo, ed. North-Holland, Amsterdam, 1969.

[47] J.-Y. Girard : Linear logic. *Theoretical Computer Science*, 50:1–101, 1987.

[48] K. Gödel : Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.

[49] K. Gödel : *Collected Works.* S. Feferman, ed., volume II, pages 217–251. Oxford University Press, New York/Oxford, 1958.

[50] K. Gödel : Über eine noch nicht benüzte Erweiterung des finiten Standpunktes. *Dialectica*, 12:230–237, 1990.

[51] I. Grattan-Guinness : *The Development of the Foundations of Mathematical Analysis from Euler to Riemann.* M.I.T. Press, Cambridge, Mass, 1970.

[52] Y. Gurevitch : *Current Trends in Theoretical Computer Science.* E. Börger, ed., chapitre Logic and the Challenge of Computer Science, pages 1–57. Computer Science Press, East Lansing, MI, 1988.

[53] P. Hájek et P. Pudlák : *Metamathematics of First-Order Logic.* Springer, Berlin, 1993.

[54] M. Hallett : Hilbert and logic. *In* M. Marion et R. S. Cohen, éditeurs : *Quebec Studies in the philosophy of science, Part I*, pages 135–187. Kluwer, Dordrecht, 1998.

[55] Y. Hellegouarch : *Invitation aux mathématiques de Fermat-Wiles.* Masson, Paris, 1997.

[56] J. Herbrand : *Écrits logiques.* J. van Heijenoort, ed. PUF, Paris, 1968.

[57] D. Hilbert : *Über die Grundlagen der Logik und Mathematik*, pages 174–185. in : A. Krazer (Hrsg.) Verhandlungen des III. Internationalen Mathematiker-Kongresses in Heidelberg vom 8. bis 13. August 1904. Leipzig, Teubner, 1904.

[58] D. Hilbert : Über das Unendliche. *Mathematische Annalen*, 95:161–190, 1926. trad. par A. Weil sous le titre « Sur l'infini », *Acta Mathematica* 48 : 91-122, 1926.

[59] D. Hilbert : *Gesammelte Abhandlungen III.* Chelsea, New York, 1932.

[60] D. Hilbert et W. Ackermann : *Grundzüge der theoretischen Logik*. Springer, Berlin, 1928.

[61] D. Hilbert et P. Bernays : *Grundlagen der Mathematik I et II*. Springer, Berlin, 2 édition, 1968–1970.

[62] W. Hodges : *Model Theory*. Cambridge University Press, Cambridge, 1993.

[63] D. Hume : *A Treatise of Human Nature.* L. A. Selby-Bigge, ed. Clarendon Press, Oxford, 1978.

[64] A. Hurwitz : *Mathematische Werke, 2 ; 198-207*. Birkhaüser, Basel, Basel, 1932–1933.

[65] K. Ireland et M. Rosen : *A Classical Introduction to Modern Number Theory*. Springer, New York/Heidelberg/Berlin, 1980.

[66] G. Japaridze : Introduction to computability logic. *Annals of Pure and Applied Logic*, 123:1–99, 2003.

[67] R. Kaye : *Models of Peano Arithmetic*. Clarendon Press, Oxford, 1991.

[68] S. C. Kleene et J. Vesley : *Foundations of Intuitionistic Mathematics*. North-Holland, Amsterdam, 1965.

[69] U. Kohlenbach : *Applied Proof Theory : Proof Interpretations and their Use in Mathematics*. Springer, Heidelberg, 2008.

[70] A. N. Kolmogorov : O Principe *tertium non datur*. *Matematicheskii sbornik*, 32:646–667, 1955.

[71] G. Kreisel : *Set-theoretic problems suggested by the notion of potential totality*, pages 103–140. in : Infinitistic Methods. Pergamon Press, Oxford, 1961.

[72] L. Kronecker : *Vorlesungen über Zahlentheorie I. K. Hensel, ed.* Teubner, Leipzig, 1901.

[73] L. Kronecker : *Werke, III Bände. K. Hensel, ed.* Teubner, Leipzig, 1968.

[74] L. Kronecker : *Werke,* éd. K. Hensel, volume III, Grundzüge einer arithmetischen Theorie der algebraischen Grössen, pages 245–387. Teubner, Leipzig, 1968.

[75] J. L. Lagrange : *Oeuvres,* éd. J.A. Serret et G. Darboux, volume III, pages 697–700. Gauthier-Villars, Paris, 1867–1892.

[76] R. P. Langlands : *Some Contemporary Problems with Origins in the Jugendtraum, Mathematical Developments arising from Hilbert's problems*. American Mathematical Society, Providence R.I., 1976.

[77] G. Lejeune-Dirichlet : *Werke I.* L. Kronecker, ed. Chelsea, New York, 1969.

[78] S. Lipschitz : *Briefwechsel mit Cantor, Dedekind, Helmholtz, Kronecker, Weierstrass*. Vieweg Verlag, Braunschveig, 1896.

[79] P. Lorenzen : Ein dialogisches Konstruktivitätskriterium. *In Infinitistic Methods*, pages 193–200. Pergamon Press, Oxford, 1961.

[80] A. Macintyre : A history of interactions between logic and number theory. *In* L. Bélair et alii, éditeurs : *Model Theory and Applications*, pages 227–272. Aracne, Napoli, 2003.

[81] M. Marion : *Wittgenstein. Finitism and the Foundations of Mathematics*. Oxford University Press, Oxford, 1998.

[82] E. Mendelson : *Introduction to Mathematical Logic*. van Nostrand, New York, 2nd édition, 1987.

[83] D. Mirimanoff : Les antinomies de Russell et Burali-forti et le problème fondamental de la théorie des ensembles. *L'enseignement mathématique*, 19:17–52, 1917.

[84] J. Molk : Sur une notion qui comprend celle de la divisibilité et sur la théorie générale de l'élimination. *Acta Mathematica*, 6:1–165, 1885.

[85] E. Nelson : *Predicative Arithmetic*. Number 32 of Mathematical Notes. Princeton University Press, Princeton, N.J., 1987.

[86] R. Parikh : Existence and feasibility in arithmetic. *Journal of Symbolic Logic*, 36:494–508, 1971.

[87] R. Parikh : Logical omniscience. *In* D. Leivant, éditeur : *Logic and Computational Complexity*, pages 22–29. Lecture Notes in Computer Science, Springer, Berlin Heidelberg, 1995.

[88] G. Peano : *Opere scelte, vol. II*. Edizione Cremonese, Roma, 1959.

[89] J. B. Rosser : Extensions of some theorems of gödel and church. *Journal of Symbolic Logic*, 1:87–91, 1936.

[90] B. Russell : Mathematical logic as based on the theory of types. *In* J. van Heijenoort, éditeur : *From Frege to Gödel*, pages 150–182. Harvard University Press, Cambridge, Mass., 1966.

[91] V. Yu. Sazonov : On feasible numbers. *In* D. Leivant, éditeur : *Logic and Computational Complexity*, pages 30–51. Lecture Notes in Computer Science, Springer, Berlin Heidelberg, 1995.

[92] K. Schütte : *Beweistheorie*. Springer, Berlin Göttingen Heidelberg, 1970.

[93] J. R. Shoenfield : *Mathematical Logic*. Addison-Wesley, Reading, Mass, 1967.

[94] T. Skolem : Begründung der elementaren Mathematik durch die rukurriende Denkweise ohne Anwendung scheinbarer Veränderlichen mit unendlichen Ausdehnungsbereich. *In* J. E. Fenstad, éditeur : *Selected Works in Logic*, pages 153–188. Universitetsforlaget, Oslo, 1970.

[95] T. Skolem : Einige Bemerkungen zur axiomatischen Begründung der Mengenlehre. *In* J. E. Fenstad, éditeur : *Selected Works in Logic*. Universitetsforlaget, Oslo, 1970.

[96] G. Takeuti : *Proof Theory*. North-Holland, Amsterdam, 1975.

[97] A. Tarski : *A Decision Method for Elementary Algebra and Geometry*. University of California Press, Berkeley and Los Angeles, 2nd édition, 1951.

[98] B. A. Trakhtenbrot : Nevozmozhnosty Algorifma dla Problemy Razreximosti Konechnyh Klassah, (L'impossibilité d'un algorithme pour le problème de la décision dans les classes finies). *Dokl. Akad. Nauk, SSSR*, 70:569–572, 1950.

[99] A. S. Troelstra : *Principles of Intuitionism*. Numéro 95 de Lectures Notes in Mathematics. Springer, Berlin Heidelberg New York, 1969.

[100] A. S. Troelstra : *Choice Sequences*. Clarendon Press, Oxford, 1976.

[101] A. S. Troelstra et D.van Dalen : *Constructivism in Mathematics. vol. I*. North-Holland, Amsterdam, 1988.

[102] L. van den Dries : Alfred Tarski's Elimination Theory for Real Closed Fields. *Journal of Symbolic Logic*, 53:7–19, 1988.

[103] H. S. Vandiver : Constructive Derivation of the Decomposition Field of a Polynomial. *Annals of Mathematics*, 37(1):1–6, 1936.

[104] J. von Neumann : *Collected Works*, volume I, chapitre Eine Axiomatisierung der Mengenlehre, pages 24–33. Pergamon Press, Oxford, 1961.

[105] K. Weierstrass : *Mathematische Werke, 7 Bände*. Mayer u. Müller, Berlin, 1894–1927.

[106] A. Weil : *Elliptic Functions according to Eisentein and Kronecker*. Springer, Berlin, 1976.

[107] A. Weil : *Number Theory. An Approach Through History. From Hammurabi to Legendre*. Birkhauser, Basel, 1984.

[108] E. Weinstein : Unifying themes in finite model theory. *In* E. *et alii* Grädel, éditeur : *Finite Model Theory*. Springer, Berlin Heidelberg New York., 2007.

[109] H. Weyl : *Das Kontinuum*. Berlin, 1917.

[110] H. Weyl : *Algebraic Theory of Numbers*. Princeton University Press, Princeton, N. J., 1940.

[111] E. Zermelo : Neuer Beweis für die Möglichkeit einer Wohlordnung. *Mathematische Annalen*, 59:107–128, 1908.

[112] E. Zermelo : Untersuchungen über die Grundlagen der Mengenlehre i. *Mathematische Annalen*, 59:261–281, 1908.

[113] E. Zermelo : Sur les ensembles finis et le principe de l'induction complète. *Acta Mathematica*, 32:185–193, 1909.

Index des noms

Index thématique

Logique arithmétique

L'arithmétisation de la logique

La logique arithmétique est la logique interne de l'arithmétique, c'est la traduction ou l'interprétation de la logique formelle dans le langage de l'arithmétique. Cette arithmétique n'est pas l'arithmétique formelle de Frege et Peano, mais l'arithmétique classique de Fermat à Kronecker jusqu'à la théorie contemporaine des nombres. L'hypothèse proposée ici suppose qu'après l'arithmétisation de l'analyse, chez Cauchy et Weierstrass, et l'arithmétisation de l'algèbre, chez Kronecker, la logique formelle a amorcé son arithmétisation avec Hilbert pour atteindre son aboutissement avec l'informatique théorique actuelle. Dans cette perspective, la méthode de la descente infinie de Fermat et l'arithmétique générale de Kronecker fournissent une critique constructiviste de l'induction transfinie en même temps qu'une preuve de consistance interne de l'arithmétique polynomiale.

La position fondationnelle défendue dans l'ouvrage se réclame du constructivisme logicomathématique et constitue les assises d'un programme qu'on peut bien appeler « logique de la science » après Peirce et Carnap. Le motif recteur des travaux formels est d'ordre philosophique et c'est dans un esprit œcuménique que l'auteur a voulu mener ces recherches.

YVON GAUTHIER est professeur de philosophie à l'Université de Montréal. Il a publié de nombreux travaux en logique formelle et en philosophie des sciences, en particulier dans le domaine des fondements des mathématiques et de la physique. Il fait ici la synthèse des travaux qu'il a menés sur les questions fondationnelles de la logique et des mathématiques.

Logique de la science 王

Illustration de la couverture :
Wassily Kandinsky, *Dans le bleu,* 1925.

Visitez les Presses
www.pulaval.com
PUL
ISBN 978-2-7637-8997-2
9 782763 789972
Presses de l'Université Laval
Philosophie