De la logique à l'arithmétique. Pourquoi des logiques et des mathématiques constructivistes?

YVON GAUTHIER *Université de Montréal*

RÉSUMÉ : Dans cet essai informel, je veux exposer les motivations et les motifs de l'approche constructiviste en logique et en mathématiques et, au-delà, dans le savoir scientifique en général et la physique théorique en particulier. Les questions fondationnelles dans ces domaines ne relèvent pas de la philosophie, mais la critique philosophique des fondements est ici un motif recteur ou un leitmotiv dans la mesure où elle départage les options théoriques d'une pratique scientifique souvent aveugle à ses propres présupposés doctrinaux. Il s'agit dès lors de la justification d'une option ou d'une posture philosophique critique dans le champ du savoir scientifique.

ABSTRACT: In this article, I wish to discuss in an informal way the motivations and the motifs of the constructivist approach to logic and mathematics and by a natural extension to the general field of science, particularly theoretical physics. Foundational questions in those domains are not ruled by philosophical principles, but a critical philosophy of foundations could be the leitmotiv to the extent that it can be used as a criterion to decide between the theoretical options of scientific practices that are often oblivious to their own doctrinal presuppositions. My objective is to provide the justificatory reasons for a constructivist option or posture in the field of scientific knowledge.

Mots-clés : logique, mathématiques, constructivisme, arithmétique, Kronecker

1. Introduction. L'arithmétisation de la logique

La réaction spontanée de nombreux logiciens, mathématiciens, scientifiques ou philosophes devant la question du constructivisme se résume souvent à

***Dialogue* 57 (2018), 1–28.**

doi:10.1017/S0012217318000070

l'interrogation suivante : pourquoi restreindre le champ de la recherche au seul domaine des exigences et contraintes constructivistes? Pourquoi se priver, par exemple, de la théorie des ensembles transfinis de Cantor ou de la théorie axiomatique des ensembles, de la logique classique et de ses ramifications et des autres théories mathématiques, comme la théorie des catégories ou la théorie des topoi? Et pourquoi se limiter à des méthodes constructives en physique théorique où les mathématiques classiques sont omniprésentes, notamment dans des théories comme la relativité générale, la mécanique quantique ou encore les théories unifiées comme la théorie des cordes et supercordes? En un mot, pourquoi embrasser l'ascèse conceptuelle du constructivisme logico-mathématique?

Une réponse immédiate est que le but de la recherche scientifique est l'accès à un savoir certain ou savoir démonstratif selon la définition même de la science (*épistémè*) chez Aristote, que l'on reconnaît comme l'initiateur de la logique formelle. Pour les Grecs, cela signifiait un savoir fondé sur des constructions concrètes avec règle et compas pour la géométrie et algorithme de division pour l'arithmétique, comme chez Euclide. Après Aristote, c'est David Hilbert qui a posé la même question et a inauguré la logique mathématique avec sa théorie des démonstrations (*Beweistheorie*), qu'il a appelée aussi métamathématique, c'est-à-dire théorie logique des mathématiques. Bourbaki, inspiré par Hilbert dans sa construction unitaire des mathématiques sur la notion de structure, appellera cette métamathématique «mathématique formelle» dans sa *Théorie des ensembles* (1970). Soit dit en passant, une théorie des structures, comme celle de Bourbaki ou comme la théorie des catégories contemporaine, est une théorie des constructions, mais des constructions qui ont oublié leur genèse! Mais pour Hilbert, il s'agissait de construire une théorie formelle des preuves en mathématiques dans un système axiomatique finitaire afin de démontrer la consistance ou la non contradiction des théories mathématiques, en premier lieu l'arithmétique. On rappellera que Gottlob Frege avait introduit en 1879 un idiome, une idéographie (*Begriffsschrift*) pour la logique formelle avec quantification sur laquelle il voulait fonder l'arithmétique dans son programme logiciste. Mais Bertrand Russell avait détecté un paradoxe dans le système frégéen des fondements de l'arithmétique, son axiome de compréhension, qui embrassait trop large en identifiant les ensembles avec leurs propriétés logiques. Russell voudra rebâtir l'édifice logiciste, avec l'aide de Whitehead, sur la base d'une théorie des types (objets singuliers et ensembles), mais la théorie comportait des axiomes non logiques, par exemple l'axiome de l'infini qui suppose qu'il y a un ensemble infini *complété* ou actuel que l'on désigne depuis Cantor, le créateur de la théorie des ensembles, par aleph zéro, la première lettre de l'alphabet hébreu ($\aleph_0$). Cantor avait conçu sa théorie des ensembles transfinis sur le motif d'une arithmétisation de l'analyse, motif que partageaient des mathématiciens comme Dedekind et Weierstrass, alors que Kronecker a été le plus conséquent dans ce contexte en arithmétisant d'abord l'algèbre dans son arithmétique générale (*allgemeine Arithmetik*), qui visait à fonder l'ensemble

des mathématiques sur la théorie des formes (*Formenlehre*), c'est-à-dire la théorie des polynômes homogènes qui fait l'économie des séries infinies et des nombres transcendants — qui transcendent l'algèbre — que l'on retrouve partout en mathématiques, de la théorie des nombres à l'analyse fonctionnelle, de la topologie algébrique à la géométrie algébrique et à la géométrie arithmétique. Ce programme de Kronecker servira même de motivation aux programmes fondationnels contemporains des Grothendieck et Langlands (voir Gauthier, 2013a). André Weil a été l'un des premiers, si ce n'est le premier, à parler du programme de Kronecker et a montré le caractère fondateur de ce programme pour l'interaction entre théorie des nombres et géométrie algébrique, tout en déplorant la méconnaissance de la théorie kroneckerienne chez la plupart des mathématiciens (voir Weil, 1979). Hilbert, inspiré malgré lui par Kronecker qui a été son professeur, adoptera en dépit de ses réticences le point de vue finitiste et pensera qu'il faut fonder ensemble la logique et l'arithmétique sur un même socle finitaire.

On a longtemps qualifié l'entreprise de Hilbert de formalisme, mais le formalisme ne désigne que l'écriture symbolique, le support matériel du formel, alors que la motivation profonde de la théorie des démonstrations est d'ordre conceptuel : c'est le finitisme qui exige que les preuves soient des suites finies de symboles à partir des axiomes en passant par les règles d'inférence pour arriver aux théorèmes dans une démarche «pas à pas» (*Schritt zu Schritt*) en un nombre fini d'étapes — «*eine endliche Anzahl von Versuchen*», pour reprendre les mots de Kronecker —, démarche qu'avait pratiquée Kronecker dans ses travaux mathématiques. Pour Hilbert, le système formel, avec ses symboles, ses axiomes, ses règles d'inférence et ses théorèmes, ne constitue qu'un appareil externe (*äusseres Handeln*) à la mathématique, et il insistera sur le fait que la logique interne du contenu (*inhaltliche Logik*) ou la déduction logique du contenu (*das inhaltiche logische Schliessen*) des théories mathématiques n'est pas capturée par la logique formelle. C'est en introduisant des objets idéaux (*Ideale Elemente*) qu'il voudra prolonger la logique au-delà du fini pour préserver les avantages d'une théorie finitaire. L'outil formel que Hilbert privilégiera dans sa méthode axiomatique sera une fonction de choix transfinie (notée ε) utilisée pour définir le quantificateur existentiel et le quantificateur universel. Or, ici, le quantificateur universel ne s'applique que si la fonction de choix ne peut trouver de contre-exemple après un essai fini, *i.e.* une itération finie de la fonction de choix transfinie que Hilbert voudra ensuite éliminer pour redescendre sur les assises solides de l'arithmétique. Il pensera donc qu'il faut conserver le principe du tiers exclu cher à Aristote. En effet, Aristote rejetait le principe de bivalence pour les futurs contingents, mais pas le principe du tiers exclu; ce principe est essentiel en logique classique, mais les intuitionnistes comme L.E.J. Brouwer le rejetteront pour les suites infinies de nombres naturels, par exemple. Hilbert dira dans son texte capital *Sur l'infini* (1926) que la logique aristotélicienne n'a pas le caractère de la circonscriptibilité (*Übersichtlichkeit*) en ne distinguant pas le fini de l'infini, et c'est pour cette raison que

https://doi.org/10.1017/S0012217318000070 Published online by Cambridge University Press

l'on doit introduire des objets idéaux qui viennent compléter le domaine des objets concrets d'un système formel finitaire. Hilbert croira ainsi pouvoir démontrer l'hypothèse du continu de Cantor, qui stipule qu'il n'y a pas de cardinal entre le cardinal des nombres naturels et le cardinal des nombres réels — Cantor avait démontré qu'il n'y avait pas de correspondance biunivoque ou de bijection entre les deux ensembles de nombres. C'était là le premier problème de sa célèbre liste de 23 problèmes, parue en 1900. Or, c'est le deuxième problème, le problème de la consistance de l'arithmétique, qui nous intéresse ici. À la question «Pourquoi une théorie finitaire de la logique et le point de vue finitiste dans les fondements des mathématiques?», Hilbert répond que c'est la sûreté (*Sicherheit*) de nos constructions qui doit garantir la certification (*Sicherung*) de nos résultats mathématiques.

Quoi qu'il en soit du programme de Hilbert dans sa forme originale, il faut reconnaître qu'après l'arithmétisation de l'analyse par Cauchy, Weierstrass, Cantor et Dedekind et l'arithmétisation de l'algèbre par Kronecker, c'est ce programme qui a inauguré l'arithmétisation de la logique qui sera poursuivi par Herbrand, Skolem et Gödel, jusqu'aux théories algorithmiques et l'informatique théorique contemporaines (voir là-dessus Gauthier, 2010).

2. La consistance de l'arithmétique

Le problème de la consistance ou de la non contradiction 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 son propre aveu, 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 ambigüité. 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.

Dans l'esprit de Hilbert, une fois la consistance de cette arithmétique établie — c'est l'arithmétique qui lui avait servi de modèle de référence pour démontrer la consistance de la géométrie euclidienne —, la consistance de l'analyse (avec des fonctions définies sur les nombres réels) et de la théorie des ensembles devait s'ensuivre. Hilbert insiste cependant sur la nature finitaire de la preuve de consistance en soutenant qu'il s'agit pour l'arithmétique de démontrer la consistance d'«un nombre fini d'axiomes finis» (Hilbert, 1935) et qu'il n'est aucunement question de processus infini dans cette arithmétique. Il ajoute qu'en cela, il suit Kronecker. Or, pour être en mesure de comprendre 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. C'est ce que je veux m'employer à faire dans cet article en suivant la piste de la preuve de la consistance interne (*innere Widerspruchslosigkeit*) de l'arithmétique, selon l'expression originale de Hilbert.

C'est la voie que j'ai empruntée dans un article intitulé «The Internal Consistency of Arithmetic with Infinite Descent» (Gauthier, 2000) et que j'ai reformulée dans sa version finale dans *Towards an Arithmetical Logic* (Gauthier, 2015). L'arithmétique dont il s'agit n'est pas l'arithmétique ensembliste de Peano (AP), mais l'arithmétique de Fermat-Kronecker (AFK), baptisée ainsi parce que la descente infinie de Fermat y remplace le postulat d'induction de Peano et que les indéterminées de Kronecker y jouent le rôle de variables dans l'arithmétique générale des polynômes. Cette arithmétique comprend non seulement la théorie classique des nombres, mais aussi les structures abstraites de l'algèbre (corps ou domaines de rationalité) et les constructions fondamentales de la géométrie algébrique et de la géométrie arithmétique. Pour une telle arithmétique, il y a une preuve de consistance interne, que j'esquisse ici à grands traits.

Je veux auparavant refaire l'histoire du problème de la consistance depuis Gödel. 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. Ce dernier n'a d'ailleurs jamais acquiescé ouvertement au résultat de Gödel. Quoi qu'il en soit, Gödel s'appuie dans sa preuve sur ce qu'il appelle la consistance oméga (ω) et, dans une note ajoutée en 1966 à la traduction de son texte de 1931, il parle de consistance externe (outer consistency) (Gödel, 1967, p. 616-617). 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 J. B. Rosser a 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). La consistance-1 introduite par Kreisel en 1957 est un théorème de correction (voir Gauthier, 1997), qui stipule que si un énoncé est prouvable, alors il est vrai; ce théorème ne constitue que la première partie du théorème de complétude de la logique du premier ordre qui stipule que tout énoncé vrai est en même temps prouvable — d'où l'incomplétude de AP qui stipule à son tour qu'il y a au moins un énoncé vrai qui n'est pas prouvable dans cette arithmétique. 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 (pour ces résultats, voir Gauthier, 1989).

Remarquons ici que le résultat d'incomplétude de Gödel repose sur une preuve syntaxique, la consistance-ω, et sur le procédé de la diagonalisation. D'autres preuves du résultat de Gödel sont possibles qui apparemment n'utilisent pas la diagonale de Cantor. Par exemple, Gregory Chaitin utilise la notion d'incompressibilité pour la compression algorithmique d'une suite infinie caractérisée par un nombre réel aléatoire Ω (grand oméga) — c'est là un procédé diagonal déguisé, si l'on veut, puisque la preuve fait appel à l'ensemble des suites infinies de nombres naturels. D'autres preuves sont possibles, de Kreisel à Kripke, lesquelles recourent à des notions de la théorie des modèles (modèles non standard) ou encore à des concepts de la théorie de la récursion. Or, toutes ces preuves requièrent un ensemble infini (dénombrable) complété de nombres naturels. De même, si l'arithmétique minimale de Robinson Q sans quantificateurs ni postulat d'induction apparaît inoffensive du point de vue prédicatif, elle repose sur une sémantique ensembliste sous-tendue par l'ensemble infini des nombres naturels.

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 adopté par Gödel. Tarski l'a bien vu, lorsqui'il remarque (Tarski, 1933) que la consistance-ω et la complétude-ω requièrent 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. C'est toutefois en recourant à l'induction transfinie à la manière d'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, la limite des ordinaux ω. Gödel, de son côté, utilisera l'induction sur tous les types finis dans sa preuve de la consistance de l'arithmétique intuitionniste (Gödel, 1958); c'est pour lui une extension du point de vue finitiste, c'est-à-dire le 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 vœu 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 l'on doit conclure que l'arithmétique ensembliste (AP) est condamnée à une consistance externe qui repousse la limite ω des ordinaux finis jusqu'à la limite ε_0 des ordinaux transfinis de la seconde classe de nombres de Cantor. Même si ces ordinaux sont appelés constructifs, ils n'ont pas d'existence d'un point de vue constructiviste, celui que j'aborde maintenant.

3. Arithmétique

3.1. Le programme de Hilbert

Le programme de Hilbert peut être modifié, comme l'a suggéré Kreisel. La modification majeure que j'ai introduite dans un article paru en 1994 dans *Synthese* — «Hilbert and the Internal Logic of Mathematics» (repris dans Gauthier, 2002) — consiste à refonder le programme de Hilbert sur ce que j'ai appelé le programme de Kronecker après André Weil. Quand Hilbert, dans sa conférence «*Über das Unendliche*» (1926), explique que du point de vue finitiste (*finiter Standpunkt*), il y a deux sortes de formules en mathématiques, les premières qui correspondent aux énoncés finitistes 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.

Or, 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, sa signature scripturaire, pourrait-on dire. Au commencement est le signe ou le chiffre (*Ziffer*) : 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, constitue une logique interne 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 mathématiques. 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 et Bernays (voir Hilbert, 1926).

On sait que l'espoir que nourissait 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 de Peano, il a échoué en tout cas parce qu'il a voulu aller plus loin que l'arithmétique au sens de Kronecker, arithmétique que l'on peut appeler finitaire ou prédicative et qui trouve des échos contemporains dans les travaux d'Edward Nelson (1986). 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 du corps (ou du domaine de rationalité) des fonctions algébriques de Kronecker.

L'arithmétique de Peano, de ce point de vue, n'est évidemment pas prédicative en vertu du postulat d'induction infinie.

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; il y a passage

https://doi.org/10.1017/S0012217318000070 Published online by Cambridge University Press

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 (sans induction infinie) 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 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» (Hilbert, 1935, p. 487).

Le finitisme de Hilbert est donc très proche par la filiation de Kronecker de l'intuitionnisme brouwerien et du constructivisme mitigé d'un Poincaré, par exemple. Ce finitisme n'est pas touché par les résultats d'incomplétude infinitaires; 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, et Brouwer ont reconnu le caractère ouvert du procès de l'induction que Poincaré préférait appeler *récurrence*. Les propriétés métamathématiques de consistance, complétude, décidabilité, etc. perdent leur signification concrète, génétique, dans une théorie des démonstrations qui emprunte son arsenal infinitaire à la théorie des ensembles, s'associant par là à 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 la logique contemporaine par coups et contrecoups, de Herbrand à Gödel et de Tarski à Robinson. L'avenir proche de la logique, avec la théorie de la computation, les langages informatiques et la logique arithmétique, verra peut-être un retour à l'inspirateur de Hilbert, Kronecker, et à son idéal arithméticien.

La posture finitiste n'a pas suffi à Hilbert, puisqu'il reproche toujours à Kronecker en 1930 d'avoir banni les méthodes de preuve infinitaires. Or, et c'est là une curieuse ironie de l'histoire, Gödel publiait en 1931 sa preuve d'incomplétude de l'arithmétique de Peano (AP) en utilisant une méthode de preuve infinitaire, le procédé de diagonalisation de Cantor sur l'ensemble infini des nombres naturels. Le second théorème d'incomplétude stipulait qu'une preuve de consistance pour AP ne pouvait être formulée avec les moyens de AP.

Pour certains, la diagonalisation de Cantor conserve un sens constructif, même si elle comporte la quantification universelle sur l'ensemble des entiers. Puisqu'elle puise dans l'ensemble complémentaire des entiers qui ne sont pas sur la diagonale — pour cette raison je préfère parler de la *codiagonale* de Cantor —, la preuve de Gödel fait intervenir par la codiagonalisation l'ensemble des énoncés non diagonaux qui dès lors n'est pas récursivement énumérable; en fait, cet ensemble est non dénombrable puisqu'il recouvre l'ensemble des réels sur le parcours de la codiagonale, qui devient par là fonction d'une variable réelle. C'est pour cette raison que la codiagonale sur tous les nombres de Gödel des énoncés de AP produit un *nombre de Cantor* dont on ne peut savoir s'il est dénombrable ou non (pour des détails là-dessus, voir Gauthier, 1997). Cette curieuse situation, comme le disait Gödel pour l'autoréférence à propos du paradoxe du menteur, se répète ici dans le contexte du paradoxe de Skolem pour la théorie logique des prédicats du premier ordre, incapable en principe de référer à l'ensemble des sous-ensembles $P(\omega)$ d'un ensemble infini dénombrable ω. Ce paradoxe est éminemment sémantique puisqu'il relève de la logique ensembliste du théorème de Löwenheim-Skolem, corollaire du théorème de complétude pour la même logique des prédicats du premier ordre obtenu par Gödel en 1930. Par ailleurs, la diagonale de Cauchy, ou produit de convolution à l'encontre de la diagonale de Cantor, ne va pas au-delà de la suite des entiers : elle ne fait qu'entrelacer deux séries de puissances $a_n x^n$ et $b_n x^n$ dans une troisième $c_n x^n$.

Il s'agit d'un procédé nettement constructif qui ne fait appel qu'à la sommation finie de coefficients entiers. Le produit de convolution est un instrument privilégié dans la preuve finitaire de la consistance de l'arithmétique dans la mesure où la théorie des polynômes (de degré fini) constitue le support, évidemment fini, des séries de puissances infinies.

3.2. Le programme de Kronecker

La même théorie des polynômes est au coeur de l'œuvre de Kronecker, qui a élaboré une arithmétique générale (*allgemeine Arithmetik*) qui trouve son point culminant dans ses *Fondements (ou traits fondamentaux) d'une théorie arithmétique des grandeurs algébriques* (*Grundzüge einer arithmetischen Theorie der algebraischen Grössen* — voir Kronecker, 1968 [1889]). La théorie des formes, comme on l'appelait à l'époque et que Hilbert et Emmy Noether ont achevée, est une théorie des polynômes homogènes. L'objet privilégié est ici la notion d'indéterminée que Kronecker emprunte à Gauss : ce sont les «*indeterminatae*» ou variables indépendantes des équations diophantiennes, équations indéterminées

https://doi.org/10.1017/S0012217318000070 Published online by Cambridge University Press

avec coefficients entiers. L'arithmétique générale de Kronecker est un calcul des indéterminées associées à une arithmétique des entiers; le programme de Kronecker consiste essentiellement à réduire toutes les grandeurs algébriques à une arithmétique des polynômes. On n'ignore pas qu'une fonction entière — qui prend toutes ses valeurs finies — qui n'est pas un polynôme est une fonction transcendante, *i.e.* n'est pas algébrique, mais l'idée de Kronecker est d'obtenir une théorie arithmétique où même les fonctions transcendantes, par adjonction des indéterminées, se ramènent à un calcul finitaire. De là vient sans doute le mot d'esprit qu'on lui attribue : «Dieu a créé les entiers, tout le reste est l'œuvre de l'homme», mais il affirme dans ses textes que les entiers sont aussi des constructions de l'esprit humain, comme Gauss l'avait professé.

Voyons cela d'une façon un peu plus précise. Pour Kronecker, la théorie arithmétique des grandeurs algébriques se résume à la théorie des fonctions intégrales entières qui inclut la théorie des fonctions rationnelles entières, c'est-à-dire des formes ou polynômes d'un domaine de rationalité (*Rationalitätsbereich*), un terme qu'il préférait à *Körper*, une invention de Dedekind, traduit «corps» en français et «field» en anglais, parce qu'il trouvait ce dernier trop chargé matériellement.

Le but de Kronecker était de formuler une théorie arithmétique des grandeurs algébriques ou, en ses termes, d'établir les fondements de l'existence arithmétique des quantités algébriques. Le passage 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. Un 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 (extension conservatrice). Kronecker compare ses indéterminées aux nombres idéaux de Kummer et aux fonctions transcendantes de Weierstrass : pour lui, ces adjonctions n'ont pas d'existence propre, puisqu'elles ne sont qu'une extension du domaine de l'arithmétique (*Gebietserweiterung der Arithmetik*).

Soumises au calcul de l'arithmétique, les indéterminées n'ont qu'un rôle dérivé, inessentiel, et elles peuvent être éliminées. Il y a donc économie en entités réelles puisqu'on n'a pas besoin des nombres transfinis, transcendants ou irrationnels qui ne sont dès lors que des êtres idéaux gouvernés par les lois de l'arithmétique. Cette perte en idéalités mathématiques est largement compensée, aux yeux de Kronecker, par le gain constructif de l'arithmétique. Malgré ses vœux, Cantor ne pourra donner à son arithmétique transfinie le statut d'une arithmétique pure, puisqu'il devra accorder l'existence à des ordinaux-limites ou à des nombres critiques qui noient l'arithmétique dans une analyse infinie.

3.3. L'arithmétique fermatienne

Je caractérise l'arithmétique fermatienne par la méthode de la descente infinie, qui est une méthode de preuve centrale en théorie des nombres, de Fermat jusqu'à Kummer et au-delà jusqu'à Mordell, Weil et la géométrie algébrique contemporaine.

Fermat dit de la descente infinie (ou indéfinie) qu'elle est une *apagogê eis adunaton* ou une *reductio ad absurdum*. Il applique sa méthode au problème des triangles rectangles (dans les entiers rationnels) dont l'aire doit être un carré. S'il existait un tel triangle pour un nombre naturel n donné, nous dit Fermat, il devrait en exister un pour des entiers plus petits avec les mêmes propriétés; et s'il y a un second triangle, il doit y en avoir un troisième, un quatrième, et ainsi de suite, à l'infini. Or, cela est impossible, puisqu'il n'y a pas de suite descendante infinie dans les nombres naturels. Remarquons d'abord que la réduction est inoffensive ici, puisqu'elle est finitaire. En outre, la double négation qu'elle entraîne est parfaitement légitime; elle ne transcende pas le domaine du fini. La chose est plus évidente encore quand Fermat dit qu'il a appliqué sa méthode non seulement à des questions négatives, mais aussi à des problèmes positifs, comme «tout nombre premier qui est plus grand qu'un multiple de 4 d'une unité doit être composé de deux carrés». S'il y avait un tel nombre premier plus grand qu'un multiple de 4 d'une unité, mais qui ne serait pas composé de carrés, il y en aurait un plus petit de même nature et encore de plus petits, jusqu'à ce qu'on atteigne 5, qui est le plus petit nombre ayant cette propriété. On doit alors conclure par voie indirecte que le théorème est vrai, mais Fermat l'emploie dans un contexte purement arithmétique. La différence essentielle réside dans la formulation constructive de Fermat; si la descente infinie est parfaitement acceptable en tant que *reductio ad absurdum*, l'induction complète infinie obéit au principe du tiers exclu via la double négation pour un ensemble infini (par exemple N) et est donc inadmissible d'un point de vue intuitionniste et plus radicalement encore d'un point de vue constructiviste finitaire. Une telle réprobation ne s'applique pas à la descente infinie et je tenterai d'en trouver la justification fondationnelle dans la suite. C. S. Peirce et Poincaré ont insisté sur le fait que la descente infinie n'est pas équivalente à l'induction complète.

L'arithmétique de Fermat est caractérisée par la méthode de la descente infinie et je soutiens que du point de vue métamathématique, c'est-à-dire du point de vue de la théorie des démonstrations, la descente infinie remplit le rôle de l'induction sans avoir recours à la notion d'ensemble infini. Il est évident que Fermat n'avait pas à l'esprit le point de vue ω. Fermat affirme qu'il a inventé la méthode de la descente infinie ou indéfinie, mais elle est déjà *in nuce* chez Euclide. Prenons, par exemple, la proposition 31 du livre VII des *Éléments* : «tout nombre composé peut être divisé par un nombre premier». La preuve utilise une décomposition ou une réduction qui ne peut continuer indéfiniment puisque toute suite descendante de nombres naturels est finie. L'algorithme d'Euclide, qui anticipe la méthode de la descente infinie, est une méthode constructive pour trouver, par descente, le plus grand diviseur commun (p.g.d.c.) de deux entiers. On peut appliquer le même procédé aux polynômes. Le théorème d'Euclide sur l'infinité des nombres premiers, qui énonce que «[l]es nombres premiers sont plus nombreux que toute quantité définie (de nombres premiers)» — c'est la proposition 20 du livre IX des

Éléments —, découle directement de l'algorithme de division. On a donc là une preuve constructive et l'infini dont il est question n'est que potentiel, en accord avec la doctrine d'Aristote dans sa *Physique*.

Le principe de la descente infinie peut être formulé de la façon suivante : si l'existence d'une propriété pour un nombre naturel *n* implique l'existence de cette même propriété pour un nombre arbitrairement plus petit, alors cette propriété est attribuable à des nombres de plus en plus petits *ad infinitum*, ce qui est impossible puisque toute suite descendante de nombres naturels est finie. Pour justifier le principe de la méthode, on se contente de remarquer qu'il n'y a pas de descente infinie dans les nombres naturels. Mais il s'agit en réalité d'un algorithme euclidien généralisé et, comme l'a bien noté André Weil (1949, p. 335-336), 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 (ou degré), et leur plus grand diviseur commun s'obtient par descente finie. Ce principe de descente n'a pas besoin d'un quantificateur universel classique, mais d'un quantificateur *effini* pour la descente finie ou indéfinie, c'est-à-dire les suites indéfinies ou les suites infiniment processives de Brouwer.

L'arithmétique de Fermat est l'arithmétique classique avec descente infinie (sans quantification sur un ensemble infini). L'arithmétique de Peano avec postulat d'induction est l'arithmétique ensembliste — on pourrait aussi bien l'appeler arithmétique de Dedekind-Peano puisque Dedekind a été le premier à formuler l'arithmétique élémentaire en termes ensemblistes.

4. Logique

4.1. Syntaxe

La consistance est un problème logique : il faut montrer comment on ne peut avoir un énoncé et sa négation dans une même théorie ou, en termes arithmétiques, que $1 \neq 0$, *i.e.* $\neg(1 = 0)$. C'est l'autoconsistance de l'arithmétique de Fermat qui doit être démontrée; autoconsistance signifie que la preuve ne doit utiliser que des moyens internes à la théorie ou qu'elle est bornée par les termes mêmes de la théorie. Nous n'aurons donc que la quantification bornée; le quantificateur existentiel et le quantificateur universel ne s'appliquant qu'à des suites ou ensembles finis sont automatiquement bornés; en ce qui touche le quantificateur effini pour les suites effinies, il est borné naturellement par le degré (fini) du polynôme qui représente une suite effinie déterminée.

Une preuve de la consistance de l'arithmétique sans postulat d'induction est possible, qui fasse appel seulement à la descente infinie. Il n'y a pas de recours à l'induction transfinie. Nous appelons cette arithmétique l'arithmétique de Fermat (AF) pour la contraster avec l'arithmétique de Peano. L'idée principale est de traduire la logique dans l'arithmétique à l'aide d'une interprétation polynomiale avec les indéterminées (*Unbestimmte*) de Kronecker. Il s'agit donc d'une arithmétisation de la logique, c'est-à-dire d'une paramétrisation de la

logique par les polynômes avec leurs indéterminées. Le produit de convolution des polynômes sert à arithmétiser la logique. En d'autres termes, l'implication locale et la quantification locale «effinie» dans la traduction polynomiale parvient à réduire (éliminer) la logique par descente infinie de la même manière qu'on extrait le contenu des polynômes à l'aide de la descente infinie.

La logique arithmétique introduit des notions nouvelles : deux nouveaux connecteurs, la négation locale et l'implication locale, et un nouveau quantificateur appelé «quantificateur effini». Le concept fondamental de suite est scindé en suites finies qui sont des ensembles et en suites effinies qui n'en sont pas. Il n'y a pas de suites infinies. Une suite effinie n'a pas de dernier terme (open-endedness) et n'a pas de borne postpositionnelle (*e.g.* ω), mais a une borne prépositionnelle (*e.g.* 0). Une suite effinie signifie une suite potentiellement infinie ou une suite infiniment processive sans limite pré-assignée, par analogie avec le concept de suite (de choix) chez Brouwer. La suite des nombres naturels est une suite effinie. Si une suite effinie a une borne, elle devient un segment initial, *i.e.* un ensemble. Bien que minimale, la logique que nous envisagerons doit fournir un cadre naturel pour l'arithmétique, c'est-à-dire les théorèmes constructifs de la théorie des nombres, comme le théorème d'Euclide sur l'infinité des nombres premiers. Dans un sens, cette logique est une sonde finitaire pour le concept d'infinité et la logique elle-même est une «logique locale».

La syntaxe est ensuite traduite dans l'arithmétique modulaire. Pour le constructiviste, la sémantique ou la notion de modèle n'est qu'une métaphore multiforme. Le prolongement de la syntaxe dans un univers arithmétique doit donc être univoque : à chaque formule est assigné un entier positif, son «évaluateur», *i.e.* un entier qui localise la formule dans l'univers arithmétique borné où la conjonction, la disjonction et l'implication sont représentées respectivement par la multiplication, l'addition et l'exponentiation. La négation est simplement un énoncé nié dans l'univers arithmétique. Somme et produit représentent les quantificateurs existentiel et universel; un produit continué (indéfini) correspond au quantificateur effini. Une fonction d'assignation injecte les formules closes ou énoncés dans l'univers arithmétique.

4.2. La traduction polynomiale modulaire et l'élimination de la logique

Une seconde fonction, la fonction d'évaluation, va traduire les formules closes de l'univers arithmétique et leurs évaluateurs en termes de polynômes avec coefficients entiers et indéterminées. Dans cette traduction, la négation $\neg a$ sera conçue comme complément local de l'univers arithmétique selon la formule $1 - a$ et l'implication $a \rightarrow b$ correspondra à une expression modulaire $1 - a \equiv b \pmod{a}$ où la relation de congruence tient lieu de relation d'équivalence — dans le cas de l'implication, il y a un reste de la division exacte que représente l'équivalence logique ou ensembliste $a \equiv b$. Les quantificateurs existentiel et universel $\exists$ et $\forall$ deviennent des symboles de sommation et de produit Σ et Π. On a donc un contenu arithmétique ou numérique pour les constantes logiques et les quantificateurs, ce que la logique classique ne peut fournir, pas plus que la logique intuitionniste ou

d'autres logiques à prétention constructive — les logiques linéaires, les logiques combinatoires, les logiques structurales ou sous-structurales. Par exemple, la logique *indépendantiste* de Hintikka (IF, independence-friendly) veut isoler le contenu constructif du quantificateur existentiel et de la disjonction, comme le requiert la logique intuitionniste, mais comme cette dernière, et à la différence de la logique arithmétique, elle est impuissante à exhiber un contenu numérique pour ses variables (indéterminées). Cette logique polynomiale modulaire peut avoir de nombreuses applications ailleurs qu'en logique et en mathématiques, notamment en informatique théorique (calcul numérique), en théorie des probabilités et en statistiques des mégadonnées ou données massives (voir Gauthier, 2017c).

La traduction polynomiale rend compte d'un univers arithmétique ou combinatoire 2^n en expansion, mais borné dans chaque cas — dans chaque mesure — par un entier fini n, le degré d'un polynôme. La descente infinie sur les puissances décroissantes d'un polynôme fini permet d'éliminer la logique dans la traduction polynomiale en transformant toutes les formules logiques en polynômes linéaires (irréductibles), puisque la descente infinie pour les polynômes réductibles s'arrête à 1 ou à 0. Le fait que la descente infinie s'applique à l'arithmétique générale des polynômes vient du théorème fondamental de la factorisation unique des polynômes (ou forme algébrique entière, selon l'expression de Kronecker) en produit de polynômes irréductibles ou premiers (voir Kronecker, 1968 [1889]). Hermann Weyl, dans son ouvrage classique sur la théorie algébrique des nombres (Weyl, 1940), a bien vu que la factorisation unique (l'axiome de factorisation limitée) est obtenue par la condition de la chaîne descendante (anneau noethérien), qui n'est autre que la descente infinie par la généralisation de l'algorithme de division d'Euclide, puisque l'anneau des polynômes de degré fini avec plusieurs indéterminées est un anneau noethérien. Ainsi la théorie algorithmique des diviseurs, qui fait partie aussi de l'arithmétique générale de Kronecker, est-elle une généralisation de l'arithmétique finie (ou finitaire) de Fermat avec descente infinie. Les énoncés logiques sont devenus des expressions numériques générales, c'est-à-dire des polynômes, et la descente infinie réduit ces expressions numériques en formules combinatoires. La réduction de la logique est donc complète dans une logique arithmétique ou polynomiale et la consistance se résume alors à la distinction intrinsèque entre 0 et 1; pour les polynômes, la distinction est entre les polynômes linéaires (de degré 1) et les polynômes constants (de degré 0) ou encore entre les polynômes constants et le polynôme 0 (noté $-\infty$). Nous avons donc bien $\neg(0 = 1)$ et la consistance de l'arithmétique est démontrée.

Comment faire de la logique et des mathématiques sans la notion positive d'infini, c'est-à-dire sans la notion d'infini actuel? Une longue tradition mathématique, des Grecs à Fermat, de Gauss, Cauchy et Kronecker à Brouwer et Nelson, a défini le constructivisme mathématique. Heyting, Kolmogorov, Kleene, Kreisel ont formalisé la logique intuitionniste qui est une variété du constructivisme mathématique. La logique interne, d'inspiration constructiviste,

https://doi.org/10.1017/S0012217318000070 Published online by Cambridge University Press

vise à réintégrer la logique dans l'arithmétique, pierre angulaire de l'édifice mathématique, et à montrer comment les concepts d'indéfini et d'indéterminé peuvent se substituer à la notion d'infini (et de transfini dans le vocabulaire cantorien).

Descente indéfinie est l'autre nom pour la descente infinie de Fermat qui, comme nous l'avons vu, doit s'arrêter. La descente infinie ou indéfinie est donc finie en réalité et elle remplace non seulement l'induction complète sur les nombres entiers, mais aussi l'induction transfinie sur les ordinaux. Quant aux indéterminées, Kronecker, s'inspirant de Gauss, en a fait l'instrument privilégié de la théorie arithmétique des grandeurs algébriques. Une indéterminée peut même remplacer efficacement un nombre ou une grandeur transcendante dans un domaine de rationalité (ou corps au sens algébrique du terme).

Wilfrid Hodges, dans son traité de théorie des modèles (voir Hodges, 1993), reconnaît le caractère fondateur de l'arithmétique générale de Kronecker lorsqu'il dit que la théorie arithmétique des domaines de rationalité génère le modèle canonique de la théorie des corps contemporaine. Il faudrait ajouter ici que c'est la théorie des formes (polynômes) qui constitue la matrice des modèles canoniques et que cette théorie est finitaire par génération successive de ses éléments. Dans la même veine, Weyl (1940) met l'accent sur la structure algorithmique de la théorie algébrique des nombres chez Kronecker. Enfin, la théorie kroneckerienne de l'élimination a inspiré la théorie moderne de l'élimination (du quantificateur existentiel) qui a permis à Tarski d'obtenir ses résultats de décidabilité pour la géométrie et l'algèbre du premier ordre : la théorie des corps réels est par exemple une théorie décidable (voir là-dessus van den Dries, 1988). Les théories qui admettent l'élimination des quantificateurs, *i.e.* qui sont réductibles à des systèmes d'équations ou d'inéquations polynomiales sont du même coup décidables en vertu de la finitude de la procédure de réduction. Ces résultats en algèbre abstraite (les structures abstraites) ne sont pas soumis à l'incomplétude et, dans le sillage de Kronecker, on pourrait dire qu'une grande partie des mathématiques, si ce n'est la majeure partie, échappe aux limitations gödeliennes. C'est là une leçon que l'on peut tirer de la tradition constructiviste avant Brouwer et l'intuitionnisme mathématique.

Au-delà de la descente infinie de Fermat et de la théorie des indéterminées de Kronecker, il fallait concevoir, dans la preuve de consistance interne de l'arithmétique, une stratégie pour contrer ce que j'ai appelé le procédé de codiagonalisation de Cantor, qui est un ingrédient essentiel des résultats d'incomplétude de Gödel et des théorèmes d'indécidabilité (Post, Church, Rosser et Turing). La diagonale ou produit de Cauchy assurait un premier accès à la théorie des polynômes de degré fini (support des séries de puissances infinies) qui allait permettre de comprendre la théorie des formes de Kronecker comme une arithmétique polynomiale. L'expression des puissances d'un polynôme en ordre décroissant donnait prise directement à la descente infinie qui pouvait effectuer la réduction de la logique à l'arithmétique par la traduction polynomiale. Cette même traduction polynomiale a été motivée à l'origine par une logique

constructive des suites effinies (les suites infiniment processives ou potentiellement infinies de Brouwer), qui requérait l'invention d'un nouveau quantificateur, le quantificateur effini $\exists\!\!\!=\, x\, Ax$ pour les suites infiniment processives de nombres naturels.

Ce que j'ai voulu suggérer, c'est que le problème de la consistance interne de l'arithmétique avait une solution arithmétique, mais il fallait, pour y arriver, aller au-delà de Hilbert — ou plutôt en deçà — et refaire le chemin à rebours, de Hilbert à Kronecker et à Fermat, ou redescendre du paradis incertain de Cantor sur la terre ferme du fini. L'autoconsistance de l'arithmétique exige en effet le circuit fini de la preuve qui doit pouvoir énoncer les conditions de sa production, c'est-à-dire que l'autosuffisance et la minimalité des moyens de preuve doivent être garantis par la structure interne de la théorie. Or l'arithmétique polynomiale, en internalisant la logique, s'approprie les moyens de son autodétermination en vertu de la clôture de la théorie par les termes polynomiaux eux-mêmes de degré fini.

La théorie kroneckerienne de l'anneau «naturel» des entiers et du corps des entiers algébriques (extensions algébriques) fournit, en tant que théorie finitaire, un premier exemple d'autoconsistance. En s'inspirant de la théorie kroneckerienne du contenu polynomial (*Enthalten-Sein*), c'est-à-dire le contenu en coefficients entiers des formes ou polynômes homogènes, on peut conférer la notion de contenu à toute forme logique finie, c'est-à-dire à toute expression logique traduisible dans le langage de l'arithmétique polynomiale, d'où l'idée d'une logique interne du contenu arithmétique ou logique arithmétique. Pour cette logique du contenu arithmétique la descente infinie de Fermat permet de rester dans les limites de l'arithmétique «naturelle», *i.e.* l'anneau naturel des entiers et le corps naturel de ses extensions algébriques. Qu'au-delà de Cantor et en deçà de Hilbert, Kronecker ait formulé la théorie finitaire des formes algébriques, et qu'il ait pu tracer exactement la démarcation entre extensions algébriques et extensions transcendantes tout en refusant à ces dernières un statut ontologique autonome, c'est là la marque première d'un constructivisme arithmétique qui influencera Hilbert, Poincaré et Brouwer. L'arithmétique doit emprunter ce circuit dans le fini — et non pas le détour par les éléments idéaux comme chez Hilbert ou le poste d'observation externe ou transcendant le fini comme chez Gödel (de son propre aveu) — pour fermer la boucle de sa propre consistance. Poincaré ne disait-il pas que l'infini est une approximation du fini (et non l'inverse)?

La logique arithmétique, à ce titre, n'espère pas jouer au gardien des portes de la ville; elle ne cherche qu'à délimiter les territoires respectifs du constructif et du non constructif, des contenus arithmétiques et non arithmétiques. L'attitude fondationnelle peut être ici tolérante sans être béatement œcuménique et l'instinct critique n'est pas nécessairement celui du chien du garde. Sur le plan pratique, cette mise au point constitue un appel à une perspective théorique ouverte, sans dogmes et sans interdits pour un accès libre au savoir scientifique. L'arithmétisation des mathématiques et de la logique n'est pas achevée,

mais comme l'a montré Kronecker, une théorie générale, la théorie arithmétique des formes ou des polynômes, peut constituer une pièce maîtresse de l'entreprise constructiviste. À la suite de Kronecker, il est certes possible de concevoir une théorie logique qui rende compte de l'arithmétique, c'est-à-dire qui en montre la consistance interne. La logique constructive du contenu arithmétique peut montrer que la descente infinie n'est pas la même chose que l'induction complète, puisque pour montrer leur équivalence, il faut opérer une double négation sur l'ensemble infini (actuel) des nombres naturels, ce qui correspond au principe du tiers exclu, inadmissible en toute bonne logique ou mathématique constructives. Après avoir montré la consistance de l'arithmétique à l'aide de la méthode de la descente infinie à l'intérieur de l'arithmétique générale de Kronecker, il s'agit maintenant de voir jusqu'où va l'arithmétique dans ses extensions, des sous-systèmes de l'arithmétique à la théorie algébrique des corps ou «domaines de rationalité» pour Kronecker (voir Gauthier, 2010).

5. Conclusion. La logique arithmétique

5.1. Un renversement antifrégéen

Frege s'était demandé, dans son ouvrage *Lois fondamentales de l'arithmétique*, jusqu'où on pouvait aller en arithmétique avec les seuls moyens de la logique. Une réponse brutale serait que Frege n'est pas allé très loin, mais on peut retourner la question en se demandant jusqu'où on peut aller en logique avec les seules ressources de l'arithmétique, depuis l'arithmétique générale de Kronecker jusqu'à la géométrie algébrique et à la géométrie arithmétique contemporaines. Le renversement est complet si l'on peut voir qu'un calcul polynomial modulaire (la logique arithmétique) parvient à traduire toute logique en arithmétique. C'est la thèse constructiviste fondamentale que je défends dans cet essai.

La foi idéaliste du logicien «ordinaire» et du mathématicien praticien — celui qui accepte le principe qu'un énoncé logique ou mathématique est vrai ou faux en vertu des conditions de vérité édictées dans le ciel platonicien des idéalités logiques et mathématiques — ne saurait être justifiée d'un point de vue constructiviste. Pour la logique, Hilbert voudra éliminer le symbole ε après l'avoir introduit pour séparer le fini de l'infini des objets idéaux, qui n'auront servi que de détour (*Umweg*) dans le calcul finitaire d'un système formel. Si la consistance demeure l'objectif fondationnel premier, la sûreté ou la certitude (*Sicherheit*) ne peut être acquise que par les moyens finis de l'arithmétique finitaire pour fournir un contenu numérique, garant ultime de la certitude mathématique. Dans le même sens, Tarski a obtenu l'élimination des quantificateurs dans la théorie des modèles pour parvenir à des résultats finitaires de décidabilité pour l'algèbre et la géométrie élémentaires (du premier ordre). L'idée d'une logique arithmétique polynomiale et modulaire est précisément de donner un contenu numérique à la logique constructive. Le mathématicien Errett Bishop a développé une théorie fondationnelle de l'analyse mathématique (Bishop, 1967) en s'appuyant sur cette motivation d'un contenu numérique pour l'analyse : il avouera dans un

article (Bishop, 1970) que son programme est plus près de Kronecker que de Brouwer. On peut remarquer en effet que si la logique intuitionniste est fondée sur la notion de preuve, les preuves ne sont jamais dotées de contenu numérique. Brouwer, qui n'était pas un ami de la logique (ni un adepte de la théorie des nombres), a conçu les mathématiques intuitionnistes sur les notions de suite, suites régulières, suites de choix et suites irrégulières qui devaient avoir un contenu numérique intrinsèque comme suites infiniment processives — que j'appelle suites effinies. La logique intuitionniste de Heyting *et alii* a semblé perdre de vue cet objectif.

La logique arithmétique vise un contenu numérique explicite : pour un nombre naturel n arbitraire, l'univers arithmétique est limité par 2^n, l'ensemble des parties ou sous-ensembles de n — qui correspond à l'ensemble des combinaissons de n —, qui est fini par definition. Si l'arithmétique de Fermat-Kronecker avec descente infinie et arithmétique polynomiale constitue l'arrière-fond d'une logique arithmétique, c'est Gauss qui est la source première de l'arithmétique polynomiale modulaire dans ses *Disquisitiones arithmeticae*, où il introduit l'arithmétique des diviseurs et congruences avec la notion d'indéterminée (*indeterminata*) dans les expressions polynomiales — Kronecker en fera le meilleur usage dans sa théorie de diviseurs (voir Edwards, 1990) ou des systèmes modulaires (*Modulsysteme*), qui occupe une place prépondérante en théorie algébrique des nombres et en géométrie algébrique contemporaine avec ses extensions algébriques. La théorie galoisienne des ensembles de congruences de polynômes est elle aussi évidemment d'inspiration gaussienne. Pour remonter à Gauss, on peut utiliser son théorème de réciprocité quadratique (démontré à l'âge de 18 ans!) en logigue arithmétique (Gauthier, 2018); dans la même direction, on peut employer le lemme de Hensel, un élève de Kronecker, pour des résultats arithmétiques en informatique théorique et en intelligence artificielle (voir Gauthier, 2017c). Dans la grande lignée de la théorie algébrique des nombres allant de Gauss à Galois, Kummer, Kronecker et Dedekind, Hermann Weyl (Weyl, 1940) reconnaîtra la supériorité de la théorie kroneckerienne des domaines de rationalité sur la théorie des idéaux de Dedekind précisément en vertu de son caractère constructif et de son contenu numérique, et André Weil assignera à Kronecker un rôle de pionnier en géométrie algébrique pour les mêmes raisons.

La motivation d'une logique arithmétique (polynomiale modulaire) puise dans cette filiation pour proposer une preuve de consistance interne de l'arithmétique classique, celle de Fermat-Kronecker, et tirer de ce résultat la thèse d'un constructivisme logico-mathématique radical. La consistance interne de l'arithmétique de Peano et de ses sous-sytèmes ou fragments est hors de portée. De l'aveu même de Gödel, la preuve ne peut être qu'externe, c'est-à-dire d'un point de vue transcendant l'arithmétique finie, le point de vue oméga de la théorie des ensembles. De plus, selon le deuxième théorème d'incomplétude, la consistance d'une théorie du point de vue transcendant ne peut être que relative à la consistance d'une autre théorie *primitive.* Cette consistance

hypothétique stipule par exemple que si une théorie T1 est consistante (l'arithmétique de Peano au premier ordre), alors T2 est consistante (la théorie axiomatique des ensembles de Zermelo-Fraenkel). Plus d'un mathématicien, logicien ou philosophe reste dubitatif face à cette consistance itérative…

L'arithmétique de Peano est ensembliste et sa sémantique ou théorie des modèles est ensembliste de part en part jusque dans ses sous-systèmes ou fragments, et même dans l'arithmétique minimale de Robinson Q sans quantificateurs et sans postulat d'induction — bien qu'Edward Nelson en ait donné une preuve d'autoconsistance prédicative (génétique) —, puisque toutes ces arithmétiques exploitent le fonds commun d'un ensemble infini de nombres naturels. Toutes les preuves, qu'elles soient syntaxiques ou sémantiques (du théorème d'incomplétude de Gödel par exemple), ne peuvent faire abstraction de ce fondement ensembliste. La raison en est fort simple : c'est que la logique — classique du premier ordre — est assise sur un ensemble dénombrable infini et que l'arithmétique de Peano est formulée dans ce langage du premier ordre. Dans un langage du deuxième ordre où l'on quantifie non plus seulement sur les individus, mais aussi sur leurs propriétés, l'arithmétique de Peano devient l'analyse mathématique.

Des mathématiciens importants, comme E. Nelson, pensent même que l'arithmétique de Peano est inconsistante; Jack Silver, l'un des plus importants théoriciens de la théorie récente des grands cardinaux, pense que l'arithmétique de Peano au troisième ordre correspondant à l'arithmétique transfinie est inconsistante. Vladimir Voevodsky, récent médaillé Fields pour ses travaux en géométrie algébrique, admet que l'arithmétique de Peano peut être inconsistante tout en pensant que l'on peut travailler dans un cadre inconsistant, si l'on parvient à en tirer des résultats spécifiques fiables — que l'on peut tester dans un logiciel de programmation informatique comme *Coq*.

Ce que l'on peut dire là-dessus, c'est qu'il n'est pas possible de démontrer la consistance ou l'inconsistance de l'arithmétique de Peano ou de Zermelo-Fraenkel, ni d'autres théories (catégoriques ou toposiques), dès lors qu'on ne peut démontrer un énoncé infinitaire — portant sur un ensemble infini — avec des moyens finis ou même avec une extension des moyens finis comme Hilbert et Gödel l'espéraient. Si la consistance d'une théorie est un gage de certitude en logique et en mathématique, elle doit l'être aussi en physique théorique comme je l'ai montré dans des articles récents (Gauthier, 2013b et 2017b). La théorie quantique des champs regorge d'infinités qu'on parvient difficilement à éliminer à l'aide de techniques plus ou moins artificielles de renormalisation — ce qui consiste à annuler les quantités infinies (énergie ou masse) par les valeurs observées des quantités finies. Même la mécanique quantique, dans un espace de Hilbert de dimension finie, souffre de difficultés analogues lorsqu'on tient à une interprétation réaliste qui veut exploiter l'équation d'onde de Schrödinger en cardinalité du continu sans la coupure au plus dénombrable de la théorie de la mesure en termes de probabilités. Le problème apparaît aussi en relativité générale si l'on admet un *Big Bang* avec densité et énergie infinies dans une

singularité initiale. La consistance signifie encore ici l'élimination des infinités rampantes, fantômes de quantités disparues, selon l'expression de l'évèque Berkeley qui s'attaquait à l'époque au calcul infinitésimal. La théorie des multivers en cosmologie ne peut être consistante dans ce sens-là (Gauthier, 2013b). Faut-il admettre que les physiciens en général n'ont que des notions floues de l'infini? Il est intéressant de noter qu'une théorie comparable à la théorie des multivers est récemment apparue en théorie des ensembles chez des mathématiciens ensemblistes comme Hugh Woodin, Richard Laver ou Joel D. Hamkins, qui pensent en termes de multivers ensemblistes, un peu comme les univers toposiques démultipliés de Grothendieck qui n'ont pas de lien entre eux, si ce n'est dans une U-topie transcendante. Ces univers diffractés ne parviennent pas à redescendre jusqu'au «plancher des vaches» et à distinguer les ordinaux finis les uns des autres… (voir Gauthier, 2017b).

Si l'on tient à un fondement radical de nos certitudes scientifiques, il faut renoncer à l'idéal d'un réalisme intégral, plénier ou partiel et opter pour une *épistémè* qui s'alimente de nourritures terrestes plutôt que de rêver à un ciel platonicien peuplé d'idéalités inaccessibles. Le détour (*Umweg*) par les objets idéaux, comme le disait Hilbert, n'est pas interdit et on ne peut mettre un frein à la création mathématique ou bannir les créatures imaginaires de l'univers logique ou mathématique (ou même physique), mais on doit s'assurer que l'approximation du fini par l'infini, comme disait Poincaré, ne dépasse pas les bornes.

5.2. Les limites de l'infini

Gauss pensait que l'infini «n'est qu'une façon de parler en mathématiques», comme il l'exprime dans sa lettre à Schumacher du 12 juillet 1831, et que l'arithméticien, lorsqu'il dit «à l'infini», veut signifier un procès illimité, la suite des nombres naturels. L'analyste pourra dire qu'une asymptote verticale *tend* vers l'infini positif ($+\infty$), mais il parlera de limite infinie, ce qui est aussi une façon de parler. Quant aux nombres surréels (ordinaux transfinis) et hyperréels (infiniment petits), ce sont d'autres façons de parler des nombres réels qui ne le sont pas tout à fait — le seul réel infiniment petit est 0! Disons que ce sont là des façons de parler non standard, selon l'idiome particulier de la théorie des infiniment petits ou des infiniment grands qui leur sont très proches «en l'infini», comme l'usage le veut en français. Remarquons que la fonction logarithme, qui a une origine purement arithmétique, a aussi une limite «en l'infini». Il faut reconnaître qu'il y a de multiples façons de parler de l'infini en mathématiques depuis Cantor, qui s'appuyait sur des philosophes et des théologiens pour justifier son arithmétique transfinie. Même Hilbert a voulu faire un détour (*Umweg*) par ce paradis des objets idéaux (*ideale Elemente*) dans sa tentative de démonstration de l'hypothèse du continu (voir Gauthier, 2013a). Cantor pensait que les mathématiques sont une création libre de l'esprit, mais Leibniz, dans ses *Essais de théodicée* de 1710, attribuait à Dieu seul la faculté de connaître tous les possibles et de faire des combinaisons infinies — «une infinité d'infinies»,

écrivait-il. Les univers possibles ou multivers sont cependant le terrain de jeu de logiciens et mathématiciens multiversels — ou interuniversels, comme le japonais Shinichi Mochizuki dans ce qu'il appelle «géométrie interuniverselle». On ne peut rejeter d'emblée les recherches dans l'au-delà du fini, puisqu'elles visent le plus souvent des résultats de finitude. À titre d'exemple, la géométrie algébrique contemporaine trouve l'un de ses motifs principaux dans la théorie des fonctions elliptiques (devenues courbes elliptiques) — dont Kronecker a été l'un des pionniers —, qui a donné des résultats de finitude avec les travaux de Weil, Faltings, Deligne et Wiles. Dans le cas de Mochizuki, il s'agit de démontrer, par des moyens transcendant l'arithmétique, l'énoncé arithmétique élémentaire *abc* ($a + b = c$) pour des entiers positifs *a, b, c* dont le produit *d* de leurs facteurs premiers ne peut être beaucoup plus petit que la somme *c* de *a* plus *b*. La preuve d'un tel énoncé entraînerait la preuve d'un autre énoncé élémentaire, le dernier théorème de Fermat — $a^n + b^n \neq c^n$ pour *n* plus grand que 2, que Wiles a démontré en 1995 par des moyens transcendants.

Dans ce contexte, il importe de noter que Kronecker ne s'est pas abstenu de travailler la théorie analytique des fonctions elliptiques, c'est-à-dire la théorie de la multiplication complexe (dans le corps des nombres complexes *C*). Il dira dans sa conférence inaugurale à l'Académie des sciences de Berlin que l'objet de ses recherches dans ce domaine était l'analyse (mathématique); l'algèbre en était cependant le moteur et la théorie des nombres en constituait la direction et le but (voir Gauthier, 2002, p. 33). Un bel exemple de cet esprit kroneckerien est le texte séminal d'André Weil, «Number of Solutions of Equations in Finite Fields» (voir Weil, 1949). S'inspirant d'un théorème de Gauss en arithmétique élémentaire sur les congruences, Weil complète un résultat qu'il a obtenu par des moyens analytiques transcendants (en topologie) sur l'hypothèse de Riemann dans les corps de fonctions (voir Weil, 1941) et qu'il peut maintenant formuler par des moyens purement algébriques sur les courbes algébriques; ici il s'agit d'une variété algébrique, c'est-à-dire l'ensemble des racines ou solutions d'un nombre fini de polynômes en plusieurs indéterminées — un thème éminemment kroneckerien. Dans le cas d'une courbe algébrique, il s'agit d'une variété de dimension 1 où il est question de déterminer le nombre fini de points rationnels ou de points de la courbe exprimés en termes de nombres rationnels. Weil termine son article de 1949 par des conjectures sur les variétés de dimension supérieure. Il n'a jamais dénoncé cette utilisation des moyens transcendants, pas plus que Hermann Weyl dans ses travaux arithmétiques ou que Kronecker dans son programme d'arithmétisation de l'algèbre et de l'analyse : il s'agit plutôt, comme l'explique Weil (1979, p. 454), de recourir à des moyens analytiques élégants et naturels, comme la mesure de Haar pour les groupes localement compacts (dans Weil, 1995), et ensuite d'obtenir une preuve constructive sur les corps locaux par un passage à la limite facile, pour reprendre l'expression de Weil. Henri Cartan a donné en plus une preuve de ce fait mathématique sans axiome du choix.

Hermann Weyl ne s'est pas exprimé autrement à propos des méthodes transcendantes comme «construction libre» dans ses travaux en théorie des groupes

(Weyl, 1939) — là aussi on a maintenant des preuves constructives. Un autre exemple probant est le résultat *profond* (comme on dit) d'André Weil, obtenu en géométrie algébrique pour les variétés abéliennes sur les corps finis. La preuve de Weil utilisait des techniques fonctionnelles avancées et S. A. Stepanov a pu donner en 1969 une preuve élémentaire du résultat de Weil en utilisant une méthode polynomiale finitaire de comptage de points. Enrico Bombieri, médaillé Fields, a encore simplifié la méthode de Stepanov en 1972. C'est dans le même sens aussi qu'opérait Kronecker dans ses formules limites en extrayant le contenu arithmétique polynomial des séries analytiques pour les fonctions elliptiques. Cependant, l'exemple le plus fameux est la preuve transcendante de Dirichlet sur l'infinité des nombres premiers dans toute progression arithmétique, obtenue en 1836; Dirichlet confesse qu'il manque encore les principes appropriés en vertu desquels les relations transcendantes (obtenues sur les séries infinies) entre des entiers indéterminés pourraient être éliminées. Dirichlet pense donc qu'une preuve élémentaire ou constructive de son théorème est possible. Or Kronecker, qui a édité les œuvres mathématiques de Dirichlet, a proposé d'étendre arithmétiquement un intervalle fini ($\mu \ldots \upsilon$) pour des entiers μ et υ afin d'y loger au moins un nombre premier $hm + r$ pour m et r des nombres relativement premiers entre eux. On pourrait voir là une anticipation des idées de 1949 d'Atle Selberg, qui utilise des formules asymptotiques pour la fonction logarithmique sur des segments ou intervalles finis sur les entiers dans sa preuve constructive du théorème de Dirichlet. Et Kronecker d'y aller d'une déclaration de principe dans ses *Vorlesungen über Zahlentheorie* (*Leçons sur la théorie des nombres*), en disant que c'est là un cas où l'arithmétique peut aller plus loin que l'analyse… (voir là-dessus Gauthier, 2002, p. 36-37). Un autre exemple probant est le théorème de Gel'fond-Schneider en théorie des nombres transcendants. Rappelons que transcendant ici signifie «qui transcende l'algèbre» et qu'un nombre transcendant est un nombre qui n'est la solution d'aucune équation polynomiale. Le théorème démontré indépendamment par Gel'fond et Schneider en 1935 stipulait que pour un nombre algébrique α différent de 0 et 1 et β un nombre algébrique irrationnel, $\alpha\beta$ est transcendant; la preuve utilisait des ressources constructives comme les approximations logarithmiques de séries infinies, mais c'est seulement en 1962 que Gel'fond obtient une preuve constructive élémentaire en notant qu'il n'utilise qu'un outil analytique, le théorème de Rolle, qui a trait à la la dérivée d'une fonction continue de variable réelle dans l'intervalle [0, 1]. Or, Bishop (1967) a fourni une version constructive de ce théorème en définissant plus précisément les limites d'un intervalle réel [a, b] à la manière de Kronecker, dont il se réclame d'ailleurs (Bishop, 1970 — pour les détails de cette preuve, voir Gauthier, 2015, chap. 6). Disons enfin que «preuve élémentaire» ne signifie pas une preuve plus facile qu'une preuve analytique : le cas de la preuve de Dirichlet évoqué plus haut en est un exemple éclatant. Alors que la preuve de Dirichlet sur l'infinité des nombres premiers dans toute progression arithmétique utilisait les moyens transcendants des séries entières infinies sur les nombres complexes et

les notions de limites afférentes, la preuve de Selberg exploitait les propriétés arithmétiques de la fonction logarithme dans un calcul fort élaboré qui ne concède rien à la facilité pour les besoins de la rigueur. En logique mathématique, «élémentaire» signifie simplement du premier ordre où l'on quantifie seulement sur les individus ou objets individuels ou éléments d'un ensemble, alors qu'au deuxième ordre on quantifie sur les propriétés des individus, qu'au troisième ordre on quantifie sur les propriétés des propriétés, et ainsi de suite. C'est ce sens d'«élémentaire» que l'on retouve dans l'ouvrage classique de Tarski, *A Decision Method for Elementary Algebra and Geometry* (1951).

Pour revenir à André Weil, ses conjectures ont occupé pratiquement tout l'espace de la géométrie algébrique contemporaine et les meilleurs spécialistes s'y sont attaqués, de Dwork à Stepanov (pour la preuve élémentaire d'un résultat partiel), jusqu'à A. Grothendieck qui s'y est essayé sans succès et à P. Deligne qui a obtenu une preuve complète des conjectures de Weil avec des moyens transcendants, mais aussi avec un comptage fini de points rationnels. Dans le même sens, la conjecture de Shimura-Taniyama-Weil pour les courbes elliptiques sur Q, corps des nombres rationnels, qui comprend la preuve de Wiles du dernier théorème de Fermat, a été démontrée par des moyens transcendants. Cette même conjecture est un cas spécial des conjectures du mathématicien Robert Langlands, lui-même inspiré par Kronecker, tout comme Grothendieck dans sa théorie des schémas qui reprend la notion kroneckerienne de système modulaire. Remarquons enfin que la notion de motif, si chère à Grothendieck et que l'on associe au *leitmotiv* musical, s'apparente plutôt au motif cartésien : Descartes, le fondateur de la géométrie algébrique classique, parlait en effet dans sa *Dioptrique* de motifs géométriques «pour en composer la broderie», celle des courbes algébriques qu'il est le premier à introduire. Pour Grothendieck, le point géométrique est le motif recteur et cette tapisserie en pointillé du continu géométrique est bien loin de l'élégante broderie des courbes cartésiennes…

Une conjecture du logicien Jacques Herbrand, en 1930, stipule que les énoncés arithmétiques élémentaires qui sont démontrés par des moyens transcendants (par exemple en analyse réelle ou complexe) doivent être démontrés éventuellement sans ces moyens — cette conjecture a été reprise récemment comme «Grand Conjecture» par le logicien Harvey Friedman, qui apparemment ne connaissait pas la formulation de Herbrand. C'est là une des motivations centrales de la logique et des mathématiques constructives : démontrer par des moyens élémentaires (arithmétiques) des théorèmes classiques qui ont nécessité des moyens transcendant l'arithmétique. Ainsi, l'un des théorèmes de la théorie analytique des nombres, le théorème de Dirichlet sur la progression arithmétique des nombres premiers n et m entre eux — il existe une infinité de nombres premiers de la forme $1 + \lambda$ où λ est un entier positif — a été démontré par A. Selberg par des moyens élémentaires en 1949,

https://doi.org/10.1017/S0012217318000070 Published online by Cambridge University Press

comme nous l'avons vu plus haut. Il est évident que l'infinité dont il s'agit ici est une suite infiniment processive (ou effinie) de nombres naturels, comme dans le résultat non constructif récent (2008) de Green-Tao sur les suites arbitrairement longues (de longueur finie) de nombres premiers dans les progressions arithmétiques — d'aucuns parlent de suites infinies, mais il s'agit d'«abus de langage», comme on dit, ce qui arrive souvent en mathématiques! Du point de vue de la logique mathématique, on peut aussi tenter d'extraire le contenu constructif des preuves non constructives de théorèmes classiques dans des programmes de recherche comme les mathématiques à rebours (reverse mathematics) de Friedman-Simpsons ou la théorie des preuves appliquée (applied proof theory) d'U. Kohlenbach. Les théories algorithmiques de l'informatique théorique contemporaine sont les avatars les plus récents de cette conquête du constructif dans le savoir logique et mathématique — voir Gauthier (2015) pour les divers programmes de constructivisation des mathématiques classiques.

À mon sens, cette conquête du constructif commence par l'arithmétique, avec pour point de départ arbitraire le théorème de Pythagore ($c^2 = a^2 + b^2$ pour les côtés d'un triangle rectangle), et finit par l'arithmétique avec un point d'arrivée aussi arbitraire, la géométrie arithmétique contemporaine (et l'informatique théorique). Ce parcours aléatoire de l'arithmétique, qui emprunte bien des détours dans des territoires vierges (non construits), la logique arithmétique (voir Gauthier, 2015) en trace le motif recteur de l'intérieur en vertu de sa double nature constructive et de la preuve de la consistance interne de l'arithmétique qu'elle propose. Pour Poincaré, la géométrie euclidienne était une convention commode parmi toutes les géométries non euclidiennes possibles; à la question de savoir si l'arithmétique pouvait être traitée de la même façon, il répondait qu'il n'y avait qu'une seule arithmétique. Doit-on conclure qu'il n'y a qu'une seule logique arithmétique?

Remerciements : Je remercie les deux évaluateurs anonymes de *Dialogue* dont la lecture vigilante m'a permis d'apporter des précisions utiles dans un texte que j'ai voulu informel et accessible en dépit des aspects techniques de mon sujet.

Références bibliographiques

Bishop, Errett
1967 *Foundations of Constructive Analysis*, New York (NY), McGraw-Hill.

Bishop, Errett
1970 «Mathematics as a Numerical Language», dans J. Myhill, A. Kino et R.E. Vesley, dir., *Intuitionism and Proof Theory*, Amsterdam, North-Holland, p. 53–71.

Bourbaki, Nicolas
1970 *Théorie des ensembles*, Paris, Hermann.

Edwards, Harold M.
1990 *Divisor Theory*, Boston, Bikhäuser.
Gauthier, Yvon
1989 «Finite Arithmetic with Infinite Descent», *Dialectica*, vol. 43, nº 4, p. 329–337.
Gauthier, Yvon
1991 *De la logique interne*, Paris, Vrin (coll. «Mathesis»).
Gauthier, Yvon
1997 *Logique et fondements des mathématiques*, Paris, Diderot.
Gauthier, Yvon
2000 «The Internal Consistency of Arithmetic with Infinite Descent», *Modern Logic*, vol. 8, nºs 1/2, p. 47–87.
Gauthier, Yvon
2002 *Internal Logic. Foundations of Mathematics from Kronecker to Hilbert*, Dordrecht, Kluwer (coll. «Synthese Library»).
Gauthier, Yvon
2010 *Logique arithmétique. L'arithmétisation de la logique*, Québec, Presses de l'Université Laval, (coll. «Logique de la science»).
Gauthier, Yvon
2013a «Kronecker in Contemporary Mathematics. General Arithmetic as a Foundational Programme», *Reports on Mathematical Logic*, vol. 48, p. 37–65.
Gauthier, Yvon
2013b «A General No-Cloning Theorem for an Infinite Multiverse», *Reports on Mathematical Physics*, vol. 72, nº 2, p. 191–199.
Gauthier, Yvon
2015 *Towards an Arithmetical Logic. Arithmetical Foundations of Logic*. Bâle, Birkhäuser-Springer.
Gauthier, Yvon
2017a *Nouveaux entretiens sur la pluralité des mondes. Essai de cosmologie sauvage à l'usage des profanes*. Québec/Paris, Presses de l'Université Laval/Hermann.
Gauthier, Yvon
2017b «From the Local Observer in QM to the Fixed-Point Observer in GR», *Advanced Studies in Theoretical Physics*, vol. 11, nº 2, p. 687–707.
Gauthier, Yvon
2017c «Arithmetical Logic for AI Deep Learning», *International Journal of Soft Computing*, vol. 12, nº 6 (à paraître).
Gauthier, Yvon
2018 «A Quadratic Reciprocity Theorem for Arithmetical Logic», *Logica Universalis*, vol. 12, nº 2 (à paraître).
Gödel, Kurt
1958 «Über eine noch nicht benütze Erweiterung des finiten Standpunktes», *Dialectica*, vol. 12, p. 280–287.

Gödel, Kurt
1967 «On Formally Undecidable Propositions of *Principia Mathematica and Related Systems* I», dans Jean van Heijenoort, dir., *From Frege to Gödel*, Cambridge (MA), Harvard University Press, p. 616–617.

Hilbert, David
1926 «Über das Unendliche», *Mathematische Annalen*, vol. 95, p. 161–190, trad. par André Weil sous le titre «Sur l'infini», dans *Acta Mathematica*, vol. 48, n^{os} 1-2 (1926), p. 91–122.

Hilbert, David
1935 «Neubegründung der Mathematik», dans *Gesammelte Abhandlungen*, vol. 3, Berlin, Springer, p. 157–177.

Hilbert, David et Paul Bernays
1968-1970 *Grundlagen der Mathematik*, I, II, 2^{e} édition, Berlin/Heidelberg/New York, Springer.

Hodges, Wilfrid
1993 *Model Theory*, Cambridge (MA), Cambridge University Press

Kronecker, Leopold
1968 «Grundzüge einer arithmetischen Theorie der algebraischen Grössen» [1889], dans K. Hensel, dir., *Werke*, vol. III, New York (NY), Chelsea, p. 245–387.

Nelson, Edward
1986 *Predicative Arithmetic*, Princeton (NJ), Princeton University Press (coll. «Mathematical Notes»).

Tarski, Alfred
1933 «Einige Betrachtungen über die Begriffe der ω-Vollständigkeit», *Monatshefte für Mathematik und Physik*, vol. 40, p. 97–112.

Tarski, Alfred
1951 *A Decision Method for Elementary Algebra and Geometry*, 2^{e} édition, Berkeley/Los Angeles (CA), University of California Press.

Van den Driess, Lou
1988 «Alfred Tarski's Elimination Theory for Real Closed Fields», *Journal of Symbolic Logic*, vol. 53, p. 7–19.

Weil, André
1941 «On the Riemann Hypothesis in Function Fields», *Proceedings of the National Academy of Science of the United States of America*, vol. 27, n^{o} 7, p. 345–347.

Weil, André
1949 «Number of Solutions of Equations in Finite Fields», *Bulletin of the American Mathematical Society*, vol. 55, p. 497–508.

Weil, André
1979 «Number Theory and Algebraic Geometry», dans *Œuvres scientifiques. Collected Papers*, vol. III, New York (NY), Springer, p. 442–454.

Weil, André
1984 *Number Theory. An Approach through History. From Hammourabi to Legendre*, Bâle, Birkhäuser.
Weil, André
1995 *Basic Number Theory*, New York (NY), Springer.
Weyl, Hermann
1939 *The Classical Groups. Their Invariants and Representations*, Princeton (NJ), Princeton University Press.
Weyl, Hermann
1940 *Algebraic Theory of Numbers*, Princeton (NJ), Princeton University Press.