De Kronecker à Gödel via Hilbert. Les fondements arithmétiques et une crise sans fondement

Yvon Gauthier
Université de Montréal

La crise des fondements n'a pas affecté les fondements arithmétiques du constructivisme de Kronecker, Bien plutôt, c'est le finitisme kroneckerien de la théorie de l'arithmétique générale ou polynomiale qui a permis à Hilbert de surmonter la crise des fondements ensemblistes et qui a poussé Gödel, inspiré par Hilbert, à proposer une extension du point de vue finitiste pour obtenir une preuve constructive de la consistance de l'arithmétique dans son interprétation fonctionnelle « Dialectica ».

Dans ce qu'il est convenu d'appeler la crise des fondements des mathématiques du début du XX^{e} siècle, la logique formelle (Frege) et la théorie des ensembles (Cantor) avaient partie liée. Kronecker et son finitisme arithmétique y échappaient par définition. Hilbert y a échappé en se réfugiant chez Kronecker. Je veux montrer dans ce qui suit que les fondements arithmétiques de la théorie des formes ou polynômes homogènes de Kronecker ont fourni les armes nécessaires à Hilbert et ses successeurs pour ne pas être assujettis aux paradoxes logiques ou ensemblistes. L'idée de fonctionnelle polynomiale que l'on trouve chez Kronecker et que l'on retrouve chez Hilbert jusqu'à Gödel permet en effet de construire l'univers arithmétique sans le secours des notions ensemblistes et sans le recours à des constructions logiques que l'on voudra éliminer, une fois qu'on les a introduites pour faciliter l'accès au domaine purement mathématique, i.e. arithmétique. Je veux donner ici une brève idée de cette problématique que j'ai amplement développée ailleurs (voir Gauthier [1] à [7]).

Kronecker et la théorie des formes d'ordre supérieur

Dans un texte bref de 1883 « Zur Theorie der Formen höherer Stufe » ([12]), Kronecker veut compléter la théorie des formes ou polynômes homogènes qu'il a élaborée dans son œuvre majeure de 1882 ([11]) « Grundzüge einer arithmetischen Theorie der algebraischen Grössen » ou « Les éléments fondamentaux d'une théorie arithmétique des grandeurs algébriques ». Dans ce texte, Kronecker a défini la construction ou la structure générale du contenu polynomial et sa décomposition (Zerlegung) en termes de la théorie de la divisibilité : la théorie comprend en effet les formes ou polynômes homogènes et les systèmes modulaires « Modulsysteme » ou systèmes de diviseurs. Je propose ici ma propre reconstruction du schème kroneckerien en utilisant le produit de convolution (produit de Cauchy) pour les polynômes

$$f \cdot g = \left(\sum_m f_m x^m\right)\left(\sum_n g_n x^n\right) = \left(\sum_m \sum_n f_m g_n x^{m+n}\right)$$

avec addition des coefficients *m* et *n*. Kronecker ([1882] : 343) dit qu'une forme *M* est contenue dans une autre forme *M'* si les coefficients de l'une sont contenus dans les coefficients de l'autre. Il formule alors des propositions générales sur l'équivalence des formes :

> Les formes homogènes linéaires qui sont équivalentes peuvent être transformées entre elles par substitution avec des coefficients entiers.
>
> (Proposition X dans Kronecker [1882] : 345)

et

> Deux formes sont absolument équivalentes lorsqu'elles se contiennent l'une l'autre.
>
> (Proposition X^0 dans Kronecker [1882] : 351)

Kronecker énonce alors son résultat principal <*Hauptresultat*> :

> Toute forme algébrique entière au sens de l'équivalence absolue de la Proposition X^0 est représentable comme produit de formes irréductibles (premières) de façon unique.
> (Proposition $XIII^0$ dans Kronecker [1882] : 352).

et Kronecker d'ajouter que ce résultat montre que l'association des formes algébriques entières (à coefficients entiers) à l'aide de la méthode des indéterminées conserve les déterminations conceptuelles des lois élémentaires de l'arithmétique dans le passage du domaine rationnel ou du domaine des fonctions rationnelles entières au domaine des fonctions algébriques. Mais Kronecker n'est pas entièrement satisfait et revient l'année suivante avec sa théorie des formes d'ordre supérieur et introduit le produit (Kronecker[1883] : 422)

$$\sum_{h=0}^{m} M_h U_h \cdot \sum_{i=1}^{m+1} M_{m+2} U_{m+1}$$

(où $M = M_0$, M_1 , M_2 ,…, M_{n+1} sont des quantités intégrales de domaines de rationalité successifs R et les U's sont des indéterminées); on a ainsi une forme de puissance *r contenant* le produit de formes

$$\prod_{h}^{r} \sum_{k} M k' V h k.$$

Kronecker souligne que cette formulation est plus générale que sa théorie de 1882. « Être contenu » ici signifie seulement que les polynômes dans les domaines de rationalité sont inclus ou contenus dans un ordre supérieur de leurs coefficients entiers. Un système modulaire va alors décomposer cette construction en polynômes irréductibles, de sorte que les notions d'inclusion et d'équivalence (inclusion réciproque) valent aussi bien pour les formes que pour les diviseurs, i.e. la décomposition en facteurs est une technique de descente tout à fait similaire à l'algorithme de division pour les entiers ou à l'algorithme euclidien pour les polynômes.

Dans cette décomposition canonique des polynômes, la descente infinie à la Fermat permet d'arriver aux polynômes irréductibles de la même manière que la preuve d'Euclide sur la divisibilité des nombres composés par les nombres premiers. La version kroneckerienne de la décomposition canonique des polynômes repose sur les formules

$$\prod_{h=1}^{r} M_k U_{hk}$$

et

$$\prod_{i=j+k} c_i = \sum_{j+k=i} a_j b_k$$

avec $j = (0, \ldots, m)$ et $k = (0, \ldots, n)$; nous pouvons lire cette dernière formule du point de vue de la divisibilité avec $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$

$$\prod_{i=1}^{m+n} (1 + c_i x_i) = \sum_{i=0}^{m+n} \left(c_i x^{m+n-1} \right) = \sum_{m+n=1} (a_m b_n) \,.$$

La généralisation de Kronecker utilise le produit de convolution pour les polynômes

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

où les M's sont des formes entières et les U's des indéterminées comme dans le produit introduit plus haut :

$$\prod_h \sum_k M_k' U_{hk}$$

et le "contenu" du produit peut alors être exprimé par

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

dans l'ordre décroissant des puissances de la somme polynômiale. Cette combinaison linéaire par le produit de convolution et la descente (finie) des puissances montre simplement que les formes rationnelles entières génèrent des formes algébriques entières, c'est-à-dire des entiers algébriques. Ce que nous trouvons dans le texte de 1883, c'est la simple généralisation aux ordres (*Stufe*) supérieurs de la théorie des formes de 1882 qui comprend à la fois la théorie des systèmes modulaires et la théorie des polynômes. Le principe d'équivalence des formes énoncé en 1882 est valide en toute généralité et la notion de contenu ou d'inclusion « *Enthalten-sein* » s'y déploie dans la construction « *Bildung* » des formes entières qui en quelque sorte remplissent totalement l'univers arithmétique (Kronecker[1883] : 423). À mon sens, cette construction des formes d'ordre supérieur que j'appelle fonctionnelles polynomiales préside à l'idée de fonctionnelle chez Hilbert.

Hilbert et l'introduction de la notion de fonctionnelle.

C'est dans son texte de 1926 ([9]) « *Über das Unendliche* » que Hilbert introduit la notion de fonctionnelle dans sa tentative de démonstration de l'hypothèse du continu de Cantor :

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

ou dans sa forme générale

$$\forall\sigma\ (2^{\aleph_\sigma} = \aleph_{\sigma+1}).$$

Il s'agit pour Hilbert de construire une hiérarchie de fonctions de fonctions, de fonctions de fonctions de fonctions ..., c'est-à-dire de fonctionnelles pour atteindre la deuxième classe de nombres de Cantor qu'il désigne par N et qui est définie par la limite

$$\lim \omega = \varepsilon_0.$$

L'ensemble des entiers Z étant défini par

$$\lim n = \omega$$

il s'agit de faire correspondre toute fonction dans Z à un nombre de la deuxième classe de Cantor N. Les moyens élémentaires pour construire ces fonctions, nous dit Hilbert, sont la substitution des variables (*Einsetzung*) et la récurrence (*Rekursion*) qui consiste à dériver la valeur d'une fonction pour $n + 1$ de sa valeur pour n – ces moyens correspondent chez Kronecker à la substitution des indéterminées (considérées comme variables) et à la descente sur les puissances construites par le produit de convolution. Hilbert continue en disant que pour les fonctionnelles il faut introduire des paramètres d'ordre supérieur, ce sont les types de variables de hauteur (*Höhe*) croissante, mais il insiste sur le fait que c'est par itération finie en accord avec le point de vue finitiste (*finite Einstellung*) que l'on construit les fonctionnelles sur les entiers qui devront correspondre à un nombre transfini de la deuxième classe, la deuxième classe étant elle-même définie par une itération transfinie de la suite des $\omega < \varepsilon_0$. Cette tentative d'associer bijectivement les fonctionnelles dans Z avec les ordinaux de la deuxième classe de nombres de Cantor pour démontrer l'hypothèse du continu a échoué, mais les successeurs de Hilbert, Gentzen et Ackermann ont voulu utiliser l'induction transfinie jusqu'à ε_0 pour démontrer la consistance de l'arithmétique de Peano. Hilbert a donc voulu, selon mon hypothèse, prolonger jusque dans le transfini la construction des fonctionnelles polynomiales ou formes d'ordre supérieur de Kronecker tout en garantissant le point de vue finitiste d'inspiration kroneckerienne. Son programme d'arithmétisation de la logique va dans le même sens et se prolonge jusqu'à Gödel dans son extension du point de vue finitiste (l'interprétation *Dialectica*) qui reprendra l'idée de fonctionnelle de Hilbert remontant, comme j'ai voulu le montrer, au finitisme arithmétique de Kronecker.

Le programme d'arithmétisation de Hilbert

L'idée de Hilbert en introduisant le symbole epsilon ε (que nous distinguons du symbole ε_0) 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 (voir [10]). 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*> 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. A 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 symbole ε et son élimination.

Le premier axiome pour le symbole ε est

$$A(a) \ \rightarrow \ A(\varepsilon_x \ A(x))$$

où $\varepsilon(A)$ est une fonction logique de choix transfinie [9]. Le quantificateur existentiel est défini par

$$\exists x \ Ax \ \equiv \ A(\varepsilon_x \ A(x))$$

et le quantificateur universel par

$$\forall x \ Ax \ \equiv \ A(\varepsilon_x \ \neg A(x))$$

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.

Avec l'axiome aristotélicien

$$\forall x \ Ax \ \rightarrow \ A(a)$$

et le principe du tiers exclu

$$\neg\forall x \ Ax \ \rightarrow \ \exists x \ \neg A(x)$$

ces axiomes forment le cadre axiomatique pour le symbole ε et son caractère minimal devrait ouvrir le passage de l'arithmétique à l'analyse et à la théorie des ensembles en utilisant les moyens <*Hilfsmittel*> ou le détour <*Umweg*> de la logique.

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

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

par une méthode de résolutions symboliques

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

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

$$A(t) \to A(\varepsilon_r\, A(r) \neq t)$$

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

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

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 » ([10], II, 87).

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

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

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 ramènera aux formules réduites "irréductibles", comme le montre, par exemple, la preuve de consistance de Ackermann pour l'arithmétique — reproduite dans la seconde édition de Hilbert et Bernays [10], II, Supplément V, 535-555. 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

$$\psi(1,n) = 2^n$$
$$\psi(m+1,n) = 2^{n \cdot \varphi(m,n)} \cdot \psi(m,n).$$

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

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

pour obtenir une disjonction

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

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

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

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.

Le théorème de Herbrand.

La théorie de l'élimination annonce le théorème de Herbrand sur la consistance du calcul des prédicats. Voici en bref la formulation de Herbrand. Soit A une formule en forme prenexe, par exemple

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

avec R sans quantificateur. On introduit deux nouvelles lettres de fonctions, f unaire et g binaire avec les termes, 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 [10], II, 170ss.).

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 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

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

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

L'opérateur μ comme l'équivalent au 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.

L'élimination des quantificateurs.

Une autre ligne d'attaque dans le programme métamathématique de Hilbert a été conduite par Tarski et a mené à la théorie des modèles. 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 [13], 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 quantificateurs. 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 (voir [13], 31)

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

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 $T\left(\Phi\right)$. est une formule sans quantificateurs 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 $f_0\left(x\right)$ et $f_1\left(x\right)$ de la variable et se réduit à l'algorithme d'Euclide pour la détermination du plus grand diviseur commun de $f_0\left(x\right)$ et $f_1\left(x\right)$ 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 [14], 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. Dans ce contexte, le théorème de Sturm n'apparaît que comme un cas spécial de la théorie des diviseurs de Kronecker. Si Tarski conclut ([13], 53) que la méthode de la décision équivaut à une preuve de consistance et de complétude (pour les corps réels clos, par exemple), j'ai en vue plutôt l'auto-consistance de l'arithmétique. Mais auparavant, je résume l'idée chez Gödel d'une preuve de consistance interne comme une extension du point de vue finitiste.

La construction de Gödel

Gödel [8] a fait appel aux fonctionnelles sur tous les types finis en tant qu'objets abstraits distincts des nombres naturels (concrets) et c'est à Hilbert qu'il attribue la notion même de fonctionnelle dans une rare référence au texte hilbertien « Sur l'infini ». Remarquons cependant que Gödel réfère implicitement à la construction de Hilbert dans son texte de 1931 sur la complétude et la consistance (cf. « *Über Vollständigkeit und Widerspruchsfreiheit* », *Ergebnisse eines* *mathematischen Kolloquiums* 3, (1932) :13) où il suppose une suite transfinie de systèmes formels de types supérieurs, mais il est étonnant que dans sa preuve de consistance de l'arithmétique intuitionniste, i.e. l'interprétation *Dialectica*, Gödel se limite aux types finis jusqu'à ω. L'interprétation *Dialectica* qui est une extension du point de vue finitiste aux yeux de Gödel a fait l'objet de travaux par Spector, Howard et Kreisel dans l'esprit intuitionniste de l'induction barrée et de la récursion barrée. Quoique Gödel ait été animé par des motifs intuitionnistes, sa preuve de consistance pour l'arithmétique de Heyting peut être traduite pour l'arithmétique de Peano en transvidant son contenu tout en voulant éliminer la logique, comme chez Hilbert. Je propose une autre approche du problème de la consistance pour l'arithmétique, celle de Fermat (ou de Fermat-Kronecker) avec la descente infinie de Kronecker qui remplace l'induction de Peano et avec les indéterminées de Kronecker en lieu et place des variables fonctionnelles. L'"arithmétique générale" des polynômes (ou des formes, dans la terminologie kroneckerienne) est construite sur les suites "effinies" ou infiniment processives, dans la terminologie de Brouwer cette fois. Les suites finies sont des ensembles et le produit de convolution ou produit de Cauchy est conçu comme une application (fonction) de suites sur les suites dans N, alors que le degré d'un polynôme équivaut au type d'une formule, le motif étant celui d'une interprétation des formules en tant que polynômes. Gödel stipule, dans une phrase qui rappelle Gentzen, que la notion d'accessibilité <*Erreichbarkeit*> est un concept abstrait qui requiert une espèce de réflexion sur les constructions finies. Une telle notion est la notion d'une fonctionnelle computable de type fini sur les entiers que Gödel substitue aux notions abstraites d'assertion et de preuve en mathématiques intuitionnistes. Les formules comme

$$F' = \forall x \; \exists y \; A[x, y, z]$$

et

$$G' = \forall w \; \exists v \; B[v, w, u]$$

serviront à produire une interprétation consistante de l'arithmétique de Heyting : par exemple, nous avons

$$(F \supset G)' = \forall y, w \; \exists V Z \left[A(y, Z(y, w), x) \supset B(V(y), w, u)\right]$$

et

$$(\neg F)' = \forall y\, \exists \bar{Z} \quad \neg A\left(y, \bar{Z}\,(y)\,, x\right)$$

où x, y, v, w sont des suites finies de variables de type arbitraire, u est une suite de variables numériques et Y, V, Z et $\bar{Z}$ sont des variables du second ordre — A et B sont des formules sans quantificateurs. Ces formules généralisées forment l'interprétation fonctionnelle et les types finis sont définis par les trois clauses :

1. 0 est un type fini (le type des entiers)
2. si s et t sont des types finis, alors $s \times t$ (leur produit cartésien) est un type fini
3. si s et t sont des types finis, alors $s \to t$ est aussi un type fini.

Remarque : la troisième clause signifie que nous avons une application des fonctionnelles de type s aux fonctionnelles de type t.

Cette dernière transformation soulève des questions d'interprétation et la littérature là-dessus est abondante, mais je veux souligner seulement que cette application est pour moi un produit de convolution pour polynômes. Par l'isomorphisme de Curry-Howard, on peut identifier types et formules, en particulier, un produit de types est identifié à une conjonction de formules. J'étends cet isomorphisme en identifiant l'implication à une représentation par puissances. Les formules se rendent par

$$\exists x\ Ax\ \supset\ \exists y\ By\ =\ \left(\prod \bar{a}_0 x\ \cdot\ \prod b_0 x\right)^n$$

et

$$\forall x\ Ax\ \supset\ \forall y\ By\ =\ \prod_0^n \left(\prod \bar{a}_0 x\ \cdot\ \prod b_0 x\right)^n$$

où $\bar{a}_0$ est $1 - a$ avec les coefficients a et b et les indéterminées x. Mais ici nous avons un isomorphisme entre formules et polynômes qui semble plus naturel si on songe au fait qu'une théorie des types intuitionniste ou constructive (à la Martin-Löf) fondée sur l'isomorphisme admet des objets arbitraires (ou ensembles) dans un langage typifié dont la logique vient d'ailleurs et n'est pas motivée de façon interne. On peut penser aussi bien que l'induction sur tous les types finis a un caractère imprédicatif et ne répond pas aux exigences du finistisme, même « élargi » que propose Gödel dans son interprétation *Dialectica.*

Conclusion

J'ai voulu montrer qu'il y avait un fil continu du finitisme arithmétique de Kronecker qui va de Hilbert et ses successeurs jusqu'à l'extension du point de vue finitiste qu'a proposée Gödel dans sa preuve de consistance de l'arithmétique intuitionniste avec son interprétation fonctionnelle. J'estime que le programme de la théorie concrète (ou appliquée) des preuves pratiquée entre autres par U. Kohlenbach est dans la même veine puisque cette théorie recourt essentiellement aux ressources du théorème de Herbrand et de l'interprétation fonctionnelle de Gödel pour extraire le noyau constructif ou arithmétique des preuves en analyse classique (voir [7]). Kronecker a conçu le projet d'arithmétisation de l'algèbre abstraite - après le projet d'arithmétisation de l'analyse chez Cauchy, Weierstrass et Dedekind - qui a donné le projet d'arithmétisation de la logique de Hilbert à Gödel et qui se poursuit aujourd'hui en informatique théorique. J'ose penser que faire remonter ce fil conducteur de la notion de fonctionnelle polynomiale jusqu'à Kronecker, le premier tisseur de l'arithmétique générale dans les fondements des mathématiques, ne pourra que nous rasséréner dans l'analyse critique de fondements qui ne connaissent pas de crise.

Bibliographie

GAUTHIER, Y., 1991. *De la logique interne*, Paris : Vrin.

GAUTHIER, Y., 1994. « Hilbert and the Internal Logic of Mathematics », *Synthese*, 101, pp. 1-14.

GAUTHIER, Y., 1997. *De la logique interne. Modèles et applications*, Paris/Montréal : Diderot/Modulo.

GAUTHIER, Y., 2000. « The Internal Consistency of Arithmetic with Infinite Descent », *Modern Logic,* vol. 8, nos 1/2, pp. 47-87.

GAUTHIER, Y., 2002. *Internal Logic. Foundations of Mathematics from Kronecker to Hilbert*, Dordrecht-Boston-London, Kluwer, "Synthese Library".

GAUTHIER, Y., 2010. *Logique arithmétique. L'arithmétisation de la logique*, collection « Logique de la science », Québec : Presses de l'Université Laval.

GAUTHIER, Y., 2011. « Hilbert Programme and Applied Proof Theory », *Logique et Analyse,* 213, pp. 49-68.

GÖDEL, K., 1958. « Über eine noch nicht benütze Erweiterung des finiten Standpunkte s », *Dialectica*, 12, pp. 230-287. Voir aussi GÖDEL, K., *Collected Works*, vol. II, Oxford : Oxford University Press, 1990, pp. 271 et ss.

Hilbert, D., 1926. « Über das Unendliche », *Math. Ann.* 95, pp. 161-190, trad. par André Weil sous le titre "Sur l'infini" dans *Acta Mathematica*, vol 48 (1926), pp. 91-122.

HILBERT, D. et P. BERNAYS, 1968 et 1970, *Grundlagen der Mathematik I et II*, 2 Aufl., Berlin: Springer-Verlag.

KRONECKER, L., 1968. « Grundzüge einer arithmetischen Theorie der algebraischen Grössen », *Werke*, vol. III, ed. by K. Hensel, 5 vols., Chelsea : New York, pp. 245-387.

KRONECKER, L., 1965. « Zur Theorie der Formen höherer Stufe », *Werke*, vol. II, ed. by K. Hensel, 5 vols., Chelsea, New York, pp. 419-424.

TARSKI, A., 1951. *A decision method for elementary algebra and geometry*, 2e éd. revue, Berkeley et Los Angeles: University of California Press.

VAN DEN DRIES, L., 1988. « Alfred Tarski's Elimination Theory for Real Closed Fields », *JSL*, vol. 53, pp. 7-19.