Une lettre et un extrait de lettre à Simone Weil

André Weil

Rouen, 26 mars 1940.

Quelques pensées que j'ai eues dernièrement, sur le sujet de mes travaux arithmético-algébriques, peuvent passer pour une réponse à l'une de tes lettres, où tu me questionnais sur ce qui fait pour moi l'intérêt de ces travaux. Je me décide donc à les noter, au risque que la plus grande partie te soit incompréhensible.

Les réflexions qui suivent sont de deux sortes. Les unes portent sur l'histoire de la théorie des nombres ; tu croiras peut-être en comprendre le début : tu ne comprendras rien à la suite. Les autres portent sur le rôle de l'analogie dans la découverte mathématique, examiné sur un exemple précis, et tu en auras peut-être quelque profit. Je t'avertis que tout ce qui concerne l'histoire des mathématiques, dans ce qui suit, repose sur une érudition tout à fait insuffisante, que c'est pour une bonne part une reconstitution *a priori*, et que, même si c'est ainsi que les choses ont dû être (ce qui n'est pas prouvé), je ne saurais affirmer que c'est ainsi qu'elles ont été. En mathématiques, d'ailleurs, presque autant qu'en toute autre chose, la ligne de l'histoire a des tournants.

Après ces précautions oratoires, abordons l'histoire de la théorie des nombres. Elle est entièrement dominée par la loi de réciprocité. C'est le *theorema aureum* de Gauss (? j'aurais besoin de rafraîchir ma mémoire sur ce point : Gauss aimait beaucoup les noms de ce genre, il avait aussi un *theorema egregium*, et je ne sais plus which is which), publié par lui en 1801 dans ses *Disquisitiones* qui n'ont commencé à être lues et comprises que vers 1820 par Abel, Jacobi, Lejeune Dirichlet, et qui sont restées pendant près d'un siècle la bible de l'arithméticien. Mais pour dire ce qu'est cette loi, dont l'énoncé avait été connu déjà d'Euler et de Legendre [Euler l'avait trouvée empiriquement, comme aussi Legendre ; Legendre prétendit de plus en donner une démonstration dans son Arithmétique, qui supposait vrai, paraît-il, quelque chose d'à peu près aussi difficile que le théorème ; mais il se plaignit amèrement du "vol" commis par Gauss, qui, sans connaître Legendre, retrouva, empiriquement aussi, l'énoncé, en donna deux très belles démonstrations dès les *Disquisitiones* et plus tard jusqu'à 4 ou 5 autres, toutes fondées sur des principes différents] : pour expliquer, dis-je, ce qu'est la loi de réciprocité il faut remonter plus haut.

L'algèbre à ses débuts se donnait à tâche de rechercher, à des équations données, les solutions dans un domaine également donné, qui pouvait être celui des nombres positifs, celui des nombres réels, plus tard celui des nombres complexes. On n'avait pas encore conçu cette idée si ingénieuse, caractéristique de l'algèbre moderne, de se donner l'équation et ensuite de fabriquer *ad hoc* un domaine où elle ait une solution (je ne dis pas de mal de cette idée, qui s'est montrée extrêmement féconde ; Poincaré a quelque part, d'ailleurs, de belles réflexions, à propos de résolution par radicaux, sur le processus général par lequel, après avoir cherché longtemps et vainement à résoudre tel problème par tel procédé donné à l'avance, les mathématiciens renversent les termes de la question et partent du problème pour fabriquer les méthodes adéquates). On avait donc, par les nombres

---

Transcription en Latex (Denise Vella-Chemla, mai 2024) de la lettre de 1940 d'André Weil à sa sœur, dont la référence est : André Weil, [1940a] *Une lettre et un extrait de lettre à Simone Weil*, Œuvres complètes, vol. 1, p. 244-255.

négatifs, résolu, toutes les fois que c'est possible, l'équation du second degré ; quand l'équation n'avait pas de solution, la formule habituelle en donnait d'"imaginaires", sur lesquelles on conservait beaucoup de doutes (il en fut ainsi jusqu'à Gauss, justement, et à ses contemporains) ; à cause justement de ces imaginaires, la formule dite de Cardan ou de Tartaglia, pour la résolution par radicaux de l'équation du 3^{e} degré, n'était pas sans donner quelques inquiétudes. Quoi qu'il en soit, quand Gauss, dans ses Disquisitiones, partit de la notion de congruence pour bâtir dessus un exposé systématique, il était naturel, de même, de chercher à résoudre, après les congruences du 1er degré, celles du 2^{d} (une congruence est une relation entre entiers a, b, m, qui s'écrit $a \equiv b$ modulo m, ou en abrégé $a \equiv b \pmod{m}$ ou $a \equiv b\ (m)$, et signifie que a et b ont même reste dans la division par m, ou $a - b =$ multiple de m ; une congruence du 1er degré est $ax + b = 0\ (m)$, du 2^{d} : $ax^2 + bx + c = 0\ (m)$, etc.) ; elles se ramènent (par le même procédé par lequel on ramène l'équation ordinaire du 2^{d} degré à une extraction de racine) à $x^2 = a \pmod{m}$; si celle-ci a une solution, on dit que a est résidu quadratique de m, sinon que a est non-résidu (1 et -1 sont résidus de 5, 2 et -2 non-résidus). Si ces notions étaient apparues depuis longtemps avant Gauss, ce n'est pas qu'on fût parti de la notion de congruence : mais elle se présentait d'elle-même dans les problèmes "diophantiens" (résolution d'équations en entiers ou en rationnels) qui formait l'objet des plus importants travaux de Fermat ; l'équation diophantienne du 1er degré, $ax + by = c$, équivaut à la congruence du 1er degré $ax \equiv c \pmod{b}$; les équations du 2^{d} degré des types étudiés par Fermat (décompositions en carrés, $x^2 + y^2 = a$, équations $x^2 + ay^2 = b$, etc.) ne sont pas équivalentes à des congruences, mais celles-ci, et en particulier la distinction des nombres en résidus et non-résidus, y jouent un grand rôle, qui n'apparaît pas à vrai dire chez Fermat (il est vrai qu'on ne possède pas ses démonstrations, mais il paraît avoir utilisé d'autres principes sur lesquels nous sommes à peu près renseignés), mais qui, autant que je sais (de seconde main) est déjà bien en évidence chez Euler.

La loi de réciprocité, donc, permet, étant donnés deux nombres premiers p, q, de savoir si q est, ou non, résidu (quadratique) de p, pourvu que l'on sache a) si p est, ou non, résidu de q ; b) si p et q sont respectivement $= 1$ ou $= -1$ modulo 4 (ou bien, pour $q = 2$, si p est $= 1, 3, 5$ ou 7 modulo 8). Par exemple, on a $53 \equiv 5 \equiv 1 \pmod{4}$, et 53 non-résidu de 5, *donc* 5 non-résidu de 53. Comme le problème pour les nombres non premiers se ramène aisément au problème pour les nombres premiers, cela donne un moyen facile de déterminer si a est, ou non, résidu de b dès qu'on sait les décomposer en facteurs premiers. Mais cette utilité "pratique" n'est rien. L'essentiel est qu'il y ait des *lois*. Il est évident que les résidus de m sont répartis en progressions arithmétiques de raison m, puisque si a est résidu, il en est de même de tous les $mx + a$; mais il est beau et surprenant que les nombres premiers p dont m est résidu soient précisément ceux qui appartiennent à certaines progressions arithmétiques de raison $4m$; pour les autres, m est non-résidu ; cela apparaît encore plus admirable, si l'on songe que, d'autre part, la répartition des nombres premiers dans une progression arithmétique *donnée* $Ax + B$ (on sait d'après Dirichlet qu'il y en a toujours une infinité pourvu évidemment que A, B soient premiers entre eux) n'est soumis à aucune loi connue, autre que statistique (nombre approximatif de ces nombres qui sont $\leq T$, qui, pour A donné, est le même quel que soit B premier à A) et paraît, sur chaque cas concret qu'on examine numériquement, aussi "fortuite" qu'une liste de coups sortis à la roulette.

Le reste des *Disquisitiones* contient surtout

1. la théorie définitive des formes quadratiques à 2 variables, $ax^2 + bxy + cy^2$, aboutissant *entre autres* à la résolution complète du problème qui a donné naissance à cette théorie : savoir si

$ax^2 + bxy + cy^2 = m$ a des solutions en entiers.

2. l'étude des racines n-ièmes de l'unité, et, comme nous dirions, la théorie de Galois *pour les corps engendrés par ces racines* et leurs sous-corps (le tout sans utiliser les imaginaires dans l'écriture, ni d'autres fonctions que les trigonométriques, et aboutissant à la condition nécessaire et suffisante pour que le n-gone régulier soit constructible par règle et compas), cela apparaissant comme une application de la détermination faite au début, comme préliminaire à la résolution des congruences, du groupe multiplicatif des nombres modulo m. Je ne parle pas de la théorie des formes quadratiques à plus de 2 variables, qui a eu peu d'influence jusqu'ici sur la marche générale de la théorie des nombres.

Les recherches ultérieures de Gauss ont eu surtout pour objet l'étude des résidus cubiques et bi-quadratiques (définis par $x^3 \equiv a$ et $x \equiv a \pmod{m}$) ; les derniers sont un peu plus simples ; Gauss reconnut qu'il n'y a pas de résultat simple à espérer en restant dans le domaine des entiers ordinaires et qu'il faut passer aux entiers "complexes" $a + b\sqrt{-1}$ (à propos de quoi il inventa, en même temps à peu près qu'Argand, la représentation géométrique des nombres complexes par des points du plan, par quoi furent définitivement dissipés tous les doutes touchant les "imaginaires"). Pour les résidus cubiques, il faut recourir aux "entiers" $a + bj$, a et b entiers, $j =$ racine cubique de 1. Gauss s'en aperçut aussi, et songea même (on en a la trace dans ses notes) à étudier le domaine des racines n-ièmes de l'unité, en pensant en même temps en tirer la démonstration du "théorème de Fermat" ($x^n + y^n = z^n$ impossible) qu'il entrevoyait comme une très minime application (c'est lui qui le dit) d'une telle théorie. Mais il se heurta au fait qu'il n'y a plus là décomposition unique en facteurs premiers (sauf justement pour i et j, racines 4^{e} et 3^{e} de l'unité, et je crois aussi pour les racines 5^{e}).

Voilà bien des fils épars ; il a fallu 125 ans pour les démêler et les assembler de nouveau en un même écheveau. Les grands noms sont Dirichlet (qui introduisit dans la théorie des formes quadratiques les fonctions zêta ou fonctions L, par quoi il prouva entre autres que toute progression arithmétique contient une infinité de nombres premiers ; mais surtout on n'a eu depuis qu'à se conformer à son modèle pour appliquer ce type de fonctions en théorie des nombres), Kummer (qui débrouilla les corps des racines de l'unité en inventant les facteurs "idéaux", et alla assez loin dans la théorie de ces corps pour obtenir des résultats sur le théorème de Fermat), Dedekind, Kronecker, Hilbert, Artin. Voici maintenant une esquisse du tableau d'ensemble qui se dégage de tout ça.

Je ne puis rien dire sans me servir de la notion de corps, qui, si l'on s'en tient à la définition, est assez simple (c'est un ensemble où l'on sait effectuer les "quatre opérations" élémentaires, celles-ci possédant les propriétés habituelles de commutativité, associativité, distributivité) ; d'extension algébrique d'un corps k (c'est un corps k', contenant k, dont tout élément α soit racine d'une équation algébrique $\alpha^n + c_1\alpha^{n-1} + ... + c_{n-1}\alpha + c_n = 0$ à coefficients $c_1, ..., c_n$ *dans* k) ; enfin d'extension *abélienne* d'un corps k ; cela veut dire une extension algébrique de k dont le *groupe de Galois* soit abélien c'est-à-dire commutatif. Il serait illusoire de donner de plus amples explications sur les extensions abéliennes ; il vaut mieux dire que c'est presque la même chose, mais non la même chose, qu'une extension de k obtenue par adjonction de racines n-ièmes (racines d'équations $x^n = a$, a dans k) ; si k contient, quel que soit l'entier n, n racines n-ièmes de l'unité (distinctes), alors c'est exactement la même chose (mais le plus souvent on s'intéresse à un corps qui n'a pas cette propriété). Si k contient n racines n-ièmes de l'unité (pour un n donné), alors toute extension

abélienne de degré n (c'est-à-dire pouvant être engendrée par adjonction à k d'une racine d'une équation de degré n) peut être engendrée par des racines m-ièmes (avec m diviseur de n). Cette notion s'est présentée à Abel dans ses recherches sur les équations résolubles par radicaux (Abel ne connaissait d'ailleurs pas la notion de groupe de Galois, qui éclaire toutes ces questions). Il est impossible d'indiquer ici comment ces recherches d'Abel ont été influencées par les résultats de Gauss (voir plus haut) sur la division du cercle et les racines n-ièmes de l'unité (qui engendrent une extension abélienne du corps des rationnels), ni quels rapports elles ont eus avec des travaux de Lagrange, avec les propres travaux d'Abel sur les fonctions elliptiques (dont la division donne lieu, comme l'a vu Abel, à des équations *abéliennes* [les racines engendrent des extensions abéliennes], résultat déjà connu mais non publié par Gauss tout au moins pour le cas particulier dit de la lemniscate) et sur les fonctions abéliennes, ainsi que ceux de Jacobi sur le même sujet (c'est même Jacobi qui a inventé les "fonctions abéliennes" au sens actuel et leur a donné ce nom, v. son mémoire "*De transcendentibus quibusdam abelianis*"), ni avec les travaux de Galois (qui n'ont été compris que peu à peu, et très tardivement ; il n'y a aucune trace dans Riemann qu'il en ait tiré le moindre profit, bien que (la chose est bien remarquable) Dedekind, Privatdozent à Göttingen et ami intime de Riemann, ait, dès 1855 ou 6, donc quand Riemann était en pleine production, fait un cours sur les groupes abstraits et la théorie de Galois).

Savoir si a (non multiple de p) est résidu de p (premier), c'est savoir si $x^2 - a = py$ a des solutions ; en passant au corps de $\sqrt{a}$, cela donne $(x - \sqrt{a})(x + \sqrt{a}) = py$, donc dans ce corps p n'est pas premier à $x - \sqrt{a}$ que pourtant il ne divise pas. Dans le langage des idéaux, cela revient à dire que dans ce corps p n'est pas premier, mais se décompose en deux facteurs idéaux premiers. On est donc en présence du problème : k étant un corps (ici le corps des rationnels), k' (ici, k' déduit de k par adjonction de $\sqrt{a}$) une extension algébrique de k, savoir si un idéal (ici, un nombre) premier dans k reste premier dans k' ou s'il se décompose en idéaux premiers, et comment : a étant supposé donné, la loi de réciprocité indique les p dont a est résidu, donc résout le problème pour le cas particulier en question. Ici et dans tout ce qui suit, les corps k, k', etc. sont des corps de nombres algébriques (racines d'équations algébriques à coefficients rationnels).

Lorsqu'il s'agit de résidus biquadratiques, on a affaire à un corps engendré par $\sqrt[4]{a}$; mais un tel corps n'est pas *en général* une extension abélienne du "corps de base" k à moins que l'adjonction d'une racine 4^{e} de a n'entraîne en même temps celles des trois autres, ce qui exige (puisque, si α est l'une d'elles, les autres sont $-\alpha, i\alpha, -i\alpha$) que k contienne $i = \sqrt{-1}$; c'est pourquoi on n'aura rien de simple si on prend pour corps de base le corps des rationnels, mais que tout marche bien si on prend (comme Gauss) le corps des "rationnels complexes" $r + si$ (r, s rationnels). De même pour les résidus cubiques. Dans ces cas, on étudie la décomposition, dans le corps k' obtenu par adjonction d'une racine 4^{e} (resp. 3^{e}) à partir d'un corps de base k contenant i (resp. j), d'un idéal (ici, d'un nombre) premier de k.

Eh bien[1], ce problème de la décomposition dans k' des idéaux de k est résolu complètement lorsque k' est une extension abélienne de k, et la solution est très simple et généralise directement et d'une manière évidente la loi de réciprocité. Aux progressions arithmétiques où se trouvent les nombres premiers, résidus de a, se substituent des classes d'idéaux, dont la définition est assez simple. Les

[1]Poincaré aimait beaucoup cette interjection pour commencer un paragraphe. Je ne m'y risquerais pas sans son exemple.

classes de formes quadratiques à deux variables, étudiées par Gauss, correspondent à un cas particulier de ces classes d'idéaux, comme il avait été reconnu par Dedekind ; les méthodes analytiques de Dirichlet (par les fonctions zêta ou L) pour l'étude des formes quadratiques, se transportent très aisément aux classes d'idéaux les plus générales qu'on ait à considérer en cette théorie ; par exemple, au théorème de la progression arithmétique correspondra le résultat suivant : dans chacune de ces classes d'idéaux dans k, il y a une infinité d'idéaux premiers, donc une infinité d'idéaux de k qui se décomposent d'une manière donnée dans k'. Enfin, la décomposition des idéaux de k en classes détermine k' d'une manière unique : et, par le théorème dit *loi de réciprocité d'Artin* (parce qu'il contient implicitement la loi de Gauss et toutes ses généralisations connues), il y a une correspondance (un "isomorphisme") entre le groupe de Galois de k' par rapport à k, et le "groupe" des classes d'idéaux dans k. On a donc, lorsqu'on sait ce qui se passe dans k, une connaissance complète des extensions *abéliennes* de k. Ce n'est pas qu'il n'y ait plus rien à faire sur les extensions abéliennes (par exemple, on peut engendrer celles-ci par les nombres $e^{2\pi i/n}$ si k est le corps des rationnels, donc au moyen de la fonction exponentielle ; si k est le corps de $\sqrt{-a}$, a entier positif, on sait engendrer ces extensions au moyen de fonctions elliptiques ou liées aux fonctions elliptiques ; on ne sait rien pour tout autre k). Mais ces questions sont bien débrouillées et on peut dire que *tout* ce qui a été fait en arithmétique depuis Gauss jusqu'à ces dernières années consiste en variations sur la loi de réciprocité : on est parti de celle de Gauss ; on aboutit, couronnement de tous les travaux de Kummer, Dedekind, Hilbert, à celle d'Artin, *et c'est la même*. Cela est beau, mais un peu vexant. Nous en savons un peu plus que Gauss, sans doute ; mais ce que nous savons de plus, c'est justement (ou peu s'en faut) que nous n'en savons pas plus.

Cela explique que, depuis quelque temps déjà, les mathématiciens aient mis à l'ordre du jour le problème des lois de décomposition non-abéliennes (problème sur k, k', lorsque k' est une extension quelconque, non-abélienne, de k ; il s'agit toujours de corps de nombres algébriques). Ce qu'on en sait se réduit à peu de chose ; ce peu, c'est Artin qui l'a trouvé. À chaque corps est attachée une fonction zêta, trouvée par Dedekind ; si k' est une extension de k, la fonction zêta attachée à k' se décompose en facteurs ; c'est Artin qui a découvert cette décomposition ; lorsque k' est une extension abélienne de k, ces facteurs sont identiques aux fonctions L de Dirichlet, ou plutôt à leur généralisation pour le corps k et les classes d'idéaux dans k, et l'identité entre ces facteurs et ces fonctions est (exprimée autrement) la loi de réciprocité d'Artin ; c'est même ainsi qu'Artin arriva d'abord à formuler cette loi à titre de conjecture hardie (il paraît que Landau se moqua de lui), quelque temps avant de pouvoir la démontrer (chose curieuse, sa démonstration est une simple transposition de la démonstration d'un autre résultat, parue entre temps, par Tchebotareff, qu'il ne manque pas d'ailleurs de citer ; et cependant c'est Artin, et à juste titre, qui a la gloire de la découverte). En d'autres termes, la loi de réciprocité n'est pas autre chose que la loi de formation des coefficients des séries qui représentent les facteurs d'Artin (dits eux-mêmes "fonctions L d'Artin"). Comme la décomposition en facteurs reste valable si k' est une extension non abélienne, c'est à ces facteurs, à ces "fonctions L non abéliennes" qu'il est naturel de s'attaquer pour rechercher la loi de formation de leurs coefficients. Il faut remarquer que, dans le cas abélien, on sait que les fonctions de Dirichlet, et par conséquent les fonctions d'Artin qui n'en diffèrent point, sont des fonctions entières. On ne sait rien de tel dans le cas général : il y a donc là, comme le signalait déjà Artin, un point où faire porter l'attaque (je m'excuse de la métaphore) : puisque les moyens connus de l'arithmétique ne paraissent pas permettre de démontrer que les fonctions d'Artin sont des fonctions entières, on peut espérer qu'en le démontrant on aura ouvert une brèche

qui permette d'entrer dans la place (je m'excuse de l'aggravation de la métaphore).

La brèche étant bien défendue (puisqu'elle a résisté à Artin), il faut donc passer en revue l'artillerie et les moyens de sape dont on dispose (je m'excuse, etc.[2]). Et voilà où intervient l'*analogie* annoncée dès le début, et qui, comme Tartuffe, n'apparaît qu'au 3^{e} acte.

On croit assez généralement qu'il n'y a plus rien à faire sur les fonctions algébriques d'une variable, parce que Riemann, qui a découvert sur ces fonctions à peu près tout ce que nous en savons (j'en excepte les travaux de Poincaré et Klein sur l'uniformisation, et ceux de Hurwitz et Severi sur les correspondances) ne nous a laissé l'énoncé d'aucun grand problème qui les concerne. Je suis sans doute au monde l'un de ceux qui en savent le plus sur ce sujet ; sans doute parce que j'ai eu la chance (en 1923) de l'apprendre directement dans Riemann, dont le mémoire est certes l'une des plus grandes choses que mathématicien ait jamais écrites ; il n'y en a pas un seul mot qui ne soit considérable. Le chapitre n'est d'ailleurs pas clos ; cela résulte par exemple de mon mémoire du J. de Liouville (voir l'introduction de ce mémoire). Je n'ai pas, bien entendu, la sottise de me comparer à Riemann ; mais ajouter si peu que ce soit à Riemann, c'est déjà, comme on dirait en grec, faire quelque chose, même si pour cela on s'aide (en le disant ou sans le dire) de Galois, de Poincaré et d'Artin.

Quoi qu'il en soit, vers l'époque (1875 à 1890) où Dedekind créait la théorie des idéaux dans les corps de nombres algébriques (dans les fameux "XI^{es} Suppléments" : Dedekind a publié 4 éditions des Leçons de Dirichlet sur la théorie des nombres, professées à Göttingen dans les dernières années de la vie de Dirichlet, et admirablement rédigées par Dedekind ; parmi les appendices ou "Suppléments" de ces Leçons, dont rien en apparence n'indique s'ils sont œuvre originale de Dedekind, et qui ne le sont d'ailleurs qu'en partie, figure à partir de la 2^{e} édition un exposé de la théorie des idéaux en 3 versions entièrement différentes suivant l'édition), il découvrait que des principes analogues permettent d'établir, par voie purement algébrique, les principaux résultats dits "élémentaires" de la théorie des fonctions algébriques d'une variable, obtenus par Riemann par voie transcendante ; il publia, en commun avec Weber, un exposé de ces résultats, déduit de ce principe. Jusque là, quand il était question de fonctions algébriques, il s'agissait toujours d'une fonction y d'une variable x, définie par une équation $P(x, y) = 0$ où P est un polynôme *à coefficients complexes*. Ce dernier point était essentiel pour l'application des méthodes de Riemann ; avec celles de Dedekind au contraire, on peut prendre les coefficients dans un corps (dit "corps des constantes") quelconque puisque les raisonnements sont *purement algébriques*. Ce point sera important dans un moment.

Les analogies ainsi mises en évidence par Dedekind sont d'ailleurs assez aisées à concevoir. Aux entiers se substituent les polynômes en x, à la divisibilité des entiers celle des polynômes (on sait bien, et l'on enseigne même dans les lycées, qu'il règne de part et d'autre des lois tout à fait analogues, par exemple pour la formation du p.g.c.d.), aux rationnels les fractions rationnelles, aux nombres algébriques les fonctions algébriques. À première vue, l'analogie reste superficielle ; aux problèmes les plus profonds de la théorie arithmétique (décomposition des idéaux premiers) ne correspond rien dans celle des fonctions algébriques, et inversement. Hilbert alla plus loin dans l'intelligence de

[2]Le lecteur qui aura la patience d'aller jusqu'au bout verra qu'en fait d'artillerie on dispose d'une inscription trilingue, de dictionnaires, d'un adultère, et d'un pont qui est une plaque tournante, sans parler de Dieu et du diable, qui jouent aussi leur rôle dans la comédie.

ces matières ; il vit par exemple qu'au théorème dit de Riemann-Roch correspond en arithmétique les résultats de Dedekind sur l'idéal appelé "différente" ; cette vue de Hilbert n'a été publiée par lui que dans un compte-rendu à peu près inconnu (qui m'a été signalé par Ostrowski), mais elle a été transmise par voie orale, ainsi que d'autres idées qu'il eut sur le même sujet. Les lois non écrites de la mathématique moderne interdisent absolument qu'on fasse état par écrit de pareilles vues qui ne sont susceptibles ni d'un énoncé précis ni à plus forte raison de démonstration. À vrai dire, s'il n'en était pas ainsi, l'on serait accablé d'écrits encore beaucoup plus stupides sinon plus inutiles que ceux qui se publient tous les jours dans les périodiques. Mais on aimerait que Hilbert eût fixé par écrit tout ce qu'il avait dans l'esprit là-dessus.

Examinons de plus près cette analogie. Dès qu'elle s'est traduite par la possibilité de transporter une démonstration telle quelle d'une théorie à l'autre, elle a déjà cessé sur ce point d'être féconde ; elle l'aura cessé tout à fait si un jour on arrive d'une manière sensée et non artificielle, à fondre les deux théories en une seule. De même, vers 1820, les mathématiciens (Gauss, Abel, Galois, Jacobi) se laissaient, avec angoisse et délices, guider par l'analogie entre la division du cercle (problème de Gauss) et la division des fonctions elliptiques. Aujourd'hui nous montrons, bien facilement, que l'un et l'autre problème donnent lieu à des équations abéliennes ; nous avons la théorie (je parle de la théorie purement algébrique, il ne s'agit pas d'arithmétique en cet instant) des extensions abéliennes. Finie l'analogie : finies les deux théories, finis ces troubles et délicieux reflets de l'une à l'autre, ces caresses furtives, ces brouilleries inexplicables ; nous n'avons plus, hélas, qu'une seule théorie, dont la beauté majestueuse ne saurait nous émouvoir. Rien n'est plus fécond que ces attouchements quelque peu adultères ; rien ne donne plus de plaisir au connaisseur, soit qu'il y participe, soit même qu'en historien il les contemple rétrospectivement, ce qui ne va pas néanmoins sans un peu de mélancolie. Le plaisir vient de l'illusion et du trouble des sens ; partie l'illusion, obtenue la connaissance, on atteint l'indifférence en même temps ; il y a du moins là-dessus, dans la Gîtâ, un tas de çlokas plus définitifs les uns que les autres. Mais revenons à nos fonctions algébriques.

Que ce soit dû à la tradition hilbertienne ou à l'attrait de ce sujet, les analogies entre fonctions et nombres algébriques ont occupé l'esprit de tous les grands arithméticiens de notre temps ; extensions abéliennes et fonctions abéliennes, classes d'idéaux et classes de diviseurs, il y avait là matière à bien des jeux d'esprit séduisants, dont quelques-uns risquaient d'être trompeurs (ainsi l'intervention des fonctions thêta dans l'une et l'autre théorie). Mais pour en tirer quelque chose, il y fallait deux moyens techniques d'invention assez récente. D'une part, la théorie des fonctions algébriques, celle de Riemann, repose *essentiellement* sur l'idée d'invariance birationnelle ; par exemple, s'il s'agit du corps des fonctions *rationnelles* d'une variable x, on introduit (je prends d'abord le cas du corps de constantes des nombres complexes) les points qui correspondent aux différentes valeurs complexes de x, y compris le point à l'infini, noté symboliquement par $x = \infty$, et défini par $1/x = 0$; le fait que ce point joue exactement le même rôle que tous les autres est essentiel. Soit $R(x) = a(x - \alpha_1)...(x - \alpha_m)/(x - \beta_1)...(x - \beta_n)$ une fraction rationnelle, avec sa décomposition en facteurs ; elle aura les zéros $\alpha_1, ..., \alpha_m$, les infinis $\beta_1, ..., \beta_n$, et le point ∞ comme zéro si $n > m$, comme infini si $n < m$. Dans le domaine des *nombres* rationnels, on a toujours la décomposition en facteurs premiers, $r = p_1, \ldots, p_m/q_1, \ldots, q_n$, chaque facteur premier correspondant à un facteur binome $(x - \alpha)$; mais rien en apparence ne correspond au point à l'infini. Si donc on modèle la théorie des fonctions sur la théorie des nombres algébriques, on est contraint de faire jouer un rôle tout à fait spécial, *dans les démonstrations*, au point à l'infini, quitte à l'expulser

de l'énoncé définitif des résultats : c'est ainsi que faisaient Dedekind-Weber, c'est ainsi qu'ont fait tous les auteurs qui ont écrit sur la théorie purement algébrique des fonctions algébriques d'une variable, au point que j'ai été le premier[3], il y a 2 ans, à donner (au J. de Crelle) une démonstration purement algébrique des principaux théorèmes de cette théorie, aussi birationnellement invariante (c'est-à-dire n'attribuant à aucun point un rôle spécial) que les démonstrations de Riemann ; et cela n'a pas seulement une importance méthodique. Quoi qu'il en soit, c'est bien d'avoir atteint ce résultat pour les corps de fonctions, mais il semble qu'on perde ainsi de vue notre analogie. Pour rétablir celle-ci, il faut introduire, dans la théorie des *nombres* algébriques, quelque chose qui réponde au point à l'infini de la théorie des fonctions. C'est à quoi l'on a atteint, et de la manière la plus satisfaisante, par la théorie dite des "valuations". Cette théorie, qui n'est pas difficile mais que je ne puis expliquer ici, s'appuye sur la théorie, due à Hensel, des corps p-adiques : définir un idéal premier dans un corps (celui-ci donné *abstraitement*), c'est représenter "isomorphiquement" celui-ci dans un corps p-adique : le représenter de même dans le corps des nombres réels ou complexes, c'est (dans cette théorie) définir un "idéal premier à l'infini". Cette dernière notion est due à Hasse (qui était élève de Hensel), ou peut-être à Artin, ou à tous deux. *Si on la suit dans toutes ses conséquences*, elle permet déjà, à elle seule, de rétablir l'analogie en beaucoup de points où elle semblait défaillante : elle permet même de découvrir sur les corps de nombres des résultats très simples et élémentaires, et qui pourtant étaient restés inaperçus (voir ma note de 1939 dans la Revue Rose, qui contient sur tout cela quelques détails). Ce n'est pas tant de ce point de vue qu'on s'en est servi jusqu'ici que pour donner des énoncés satisfaisants des principaux résultats de la théorie des extensions abéliennes (j'ai oublié de dire que celle-ci s'appelle le plus souvent "théorie du corps de classes"). Un point important est que le corps p-adique, ou respectivement le corps réel ou complexe, correspondant à un idéal premier, joue exactement le rôle, en arithmétique, que joue en théorie des fonctions le corps des développements en série *au voisinage d'un point* : c'est pourquoi on l'appelle *corps local*.

Avec tout cela, nous avons fait de grands progrès ; mais ce n'est pas assez. La théorie, purement algébrique, des fonctions algébriques sur un corps de constantes *quelconque* n'est pas assez riche pour qu'on puisse en tirer un enseignement utile. La théorie "classique" (c'est-à-dire Riemannienne) des fonctions algébriques sur le corps des constantes des nombres complexes l'est infiniment plus ; mais d'une part elle l'est trop, et dans la masse des faits, des analogies très réelles se brouillent ; et surtout, elle est trop loin de la théorie des nombres. On serait très embarrassé s'il n'y avait pas de pont entre les deux.

Et voilà justement que Dieu l'emporte sur le diable : ce pont existe ; c'est la théorie des corps de fonctions algébriques sur les corps de constantes finis (c'est-à-dire à un nombre fini d'éléments : dits aussi champs de Galois, et autrefois "imaginaires de Galois" parce que Galois les définit et les étudia le premier ; ce sont les extensions algébriques du corps à p éléments formé par les nombres $0, 1, 2, ..., p-1$ lorsqu'on calcule sur eux modulo p, p = nombre premier). Ils apparaissent déjà chez Dedekind. Un jeune étudiant de Göttingen, tué en 1914 ou 1915, étudia, dans sa dissertation parue en 1919 (travail entièrement personnel, dit Landau son maître) les fonctions zêta pour certains de ces corps, et montra que les méthodes ordinaires de la théorie des nombres algébriques s'y appliquent. Artin, en 1921 ou 1922, reprit la question, encore du point de vue de la fonction zêta ;

[3]Un peu excessif, parce que les démonstrations, à vrai dire très détournées, de l'école italienne (Severi surtout) sont, en principe, de cette espèce, bien que rédigées en langage classique.

F. K. Schmidt fit le pont entre ces résultats et ceux de Dedekind-Weber, en mettant la définition de la fonction zêta sous forme birationnellement invariante. Dans ces dernières années, ces corps ont formé un sujet d'étude favori pour Hasse et son école ; Hasse y a remporté quelques beaux succès.

J'ai parlé de pont ; il serait plus juste de dire plaque tournante. D'une part l'analogie avec les corps de nombres est tellement étroite et manifeste qu'il n'est pas de raisonnement ni de résultat d'arithmétique qui ne se transporte presque mot pour mot à ces corps de fonctions. En particulier, il en est ainsi pour tout ce qui concerne les fonctions zêta et les fonctions d'Artin ; et il y a plus : les fonctions d'Artin *dans le cas abélien sont des polynômes*, ce qu'on peut exprimer en disant que ces corps fournissent un modèle simplifié de ce qui se passe dans les corps de nombres ; ici, il y a donc lieu de conjecturer que les fonctions d'Artin non abéliennes sont encore des polynômes : *c'est justement de quoi je m'occupe en ce moment*, tout donnant lieu de croire que tout résultat acquis pour ces corps pourra inversement, pourvu qu'on le formule comme il convient, se transporter aux corps de nombres.

Mais d'autre part, entre ces corps de fonctions et les corps "Riemanniens", la distance n'est pas si grande qu'un patient apprentissage ne nous puisse enseigner l'art de passer de l'un à l'autre, et de profiter pour l'étude des premiers des connaissances acquises sur les seconds, et des moyens extrêmement puissants que nous offre, dans l'étude de ces derniers, le calcul intégral et la théorie des fonctions analytiques. Ce n'est pas, à beaucoup près, que tout cela soit facile ; mais on finit par apprendre à y voir quelque chose, bien qu'encore confusément. L'intuition y fait beaucoup ; je veux dire la faculté de voir un rapport entre choses en apparence tout à fait dissemblables ; elle ne laisse pas d'égarer aussi assez souvent. Quoi qu'il en soit, mon travail consiste un peu à déchiffrer un texte trilingue ; de chacune des trois colonnes je n'ai que des fragments assez décousus ; j'ai quelques notions sur chacune des trois langues : mais je sais aussi qu'il y a de grandes différences de sens d'une colonne à l'autre, et dont rien ne m'avertit à l'avance. Depuis quelques années que j'y travaille, j'ai des bouts de dictionnaire. Quelquefois c'est sur une colonne que je fais porter mes efforts, quelquefois sur l'autre. Mon grand travail du Journal de Liouville a fait avancer beaucoup la colonne en "Riemannien" ; par malheur, une grande partie du texte ainsi déchiffré n'a sûrement pas de traduction dans les deux autres langues : reste une partie, qui m'est très utile. En ce moment, je travaille sur la colonne du milieu. Tout ça est assez amusant. Ne crois pas cependant que ce travail sur plusieurs colonnes soit une chose fréquente en mathématique ; sous une forme aussi nette, c'est à peu près un cas unique. Ce genre de travail me convient d'ailleurs tout particulièrement ; il est incroyable à quel point des gens aussi distingués que Hasse et ses élèves, et qui ont fait de ce sujet la matière de leurs plus sérieuses réflexions pendant des années, ont, non seulement négligé, mais dédaigné de parti pris la voie riemannienne : c'est au point qu'ils ne savent plus lire les travaux rédigés en Riemannien (Siegel se moquait un jour de Hasse qui lui avait déclaré être incapable de lire mon mémoire de Liouville) et qu'ils ont retrouvé quelquefois avec beaucoup de peine, en leur dialecte, des résultats importants déjà connus, comme ceux de Severi sur l'anneau des correspondances, retrouvés par Deuring. Mais le rôle de ce que je nomme analogies, pour ne pas être toujours aussi net, n'en est pas moins important. Il y aurait grand intérêt à étudier ce genre de choses sur une période pour laquelle on serait bien pourvu de textes ; le choix en serait délicat.

P. S. Je t'envoie ça sans relire (...). Je crains (...) d'avoir paru faire une part à mes recherches qui

dépasse mes intentions ; c'est que, pour expliquer (suivant ton désir) comment se sont orientées ces recherches, j'ai bien été forcé d'insister sur les trous que j'ai voulu combler. En parlant des analogies entre nombres et fonctions, je ne voudrais pas avoir donné l'impression d'être le seul qui les entende : Artin y a profondément réfléchi, lui aussi, et c'est tout dire. Il est curieux de noter qu'un travail (signé par un élève d'Artin qui n'est pas autrement connu, de sorte qu'on doit, jusqu'à preuve du contraire, présumer qu'Artin en est l'auteur) paru il y a 2 ou 3 ans donne peut-être le seul exemple d'un résultat de la théorie classique, obtenu par *double* traduction à partir d'un résultat arithmétique (sur les fonctions zêta abéliennes), et qui est nouveau et intéressant. Et Hasse, dont le talent et la patience réunis finissent par lui faire une manière de génie, a eu sur ce sujet des idées très intéressantes. D'ailleurs (trait caractéristique, et qui doit t'être sympathique, de l'école algébrique moderne) tout cela se diffuse par tradition orale ou épistolaire beaucoup plus que par des publications orthodoxes de sorte qu'il est difficile de faire, dans le détail, l'histoire de tout ça.

Tu doutes, et avec quelque raison, que les axiomatiques modernes soient du travail dans une matière dure. Quand j'ai inventé (je dis bien inventé, et non découvert) les espaces uniformes, je n'avais pas du tout l'impression de travailler dans une matière dure, mais plutôt l'impression que doit avoir un sculpteur de métier qui s'amuserait à faire un bonhomme de neige. Mais tu ne vois sans doute pas que les mathématiques modernes ont pris, non seulement une étendue, mais une complexité telle qu'il est devenu urgent, si la mathématique doit subsister et ne pas se dissocier en un tas de petits bouts de recherches, d'accomplir un énorme travail d'unification, qui absorbe en quelques théories simples et générales tout le substrat commun des diverses branches de la science, supprime les inutilités et laisse intact ce qui est vraiment le détail spécifique de chaque grand problème. C'est là tout ce qu'il peut y avoir de bon (et ce n'est pas peu de chose) dans ces axiomatiques. C'est aussi tout le sens de Bourbaki. Il ne t'échappera pas du reste (pour reprendre la métaphore militaire) que dans tout cela il y a de grands problèmes de stratégie. Et il est aussi commun de savoir la tactique qu'il est rare (et beau, dirait Gondi) d'entendre la stratégie. Je comparerai donc (malgré l'incohérence des métaphores) ces grands édifices axiomatiques aux communications à l'arrière du front : on n'a jamais remporté beaucoup de gloire dans le corps de l'intendance ni dans le train des équipages, mais que ferait-on si de braves gens ne se consacraient à ces besognes subalternes (où ils gagnent d'ailleurs fort bien et assez aisément leur subsistance). Le danger n'est que trop grand que les divers fronts finissent, non par manquer de vivres (le Conseil de la Recherche est là pour ça), mais par s'ignorer les uns les autres et perdent leur temps, les uns comme les Hébreux au désert, les autres comme Hannibal à Capoue. L'organisation actuelle de la science ne tient (malheureusement, pour les sciences expérimentales ; en mathématique le dommage est beaucoup moins grand) aucun compte du fait qu'il y a extrêmement peu d'hommes capables d'embrasser tout le front d'une science, de saisir, non pas seulement les points faibles de la résistance, mais ceux qu'il importe le plus d'emporter, l'art de masser les troupes, de faire coopérer tel secteur au succès de tel autre, etc. Bien entendu, quand je parle de troupes le terme (pour le mathématicien du moins) est essentiellement métaphorique, chaque mathématicien étant à lui seul ses propres troupes. Si, sous l'impulsion donnée par certains maîtres, certaines "écoles" ont pu avoir de notables succès, le rôle de l'individu en mathématique reste prépondérant. D'ailleurs, il est devenu impossible d'appliquer des vues de ce genre à l'ensemble de la science ; il ne peut plus y avoir personne qui puisse même seulement dominer assez la mathématique et la physique à la fois pour régler leur marche alternée ou simultanée ; toute tentative de "planification" tombe dans le grotesque, et il faut s'en remettre au hasard et aux spécialistes.

Extrait d'une lettre du 29 février 1940 :

...Quant à parler à des non-spécialistes de mes recherches ou de toute autre recherche mathématique, autant vaudrait, il me semble, expliquer une symphonie à un sourd. Cela peut se faire ; on emploie des images, on parle de thèmes qui se poursuivent, qui s'entrelacent, qui se marient ou qui divorcent ; d'harmonies tristes ou de dissonances triomphantes : mais qu'a-t-on fait quand on a fini ? Des phrases, ou tout au plus un poème, bon ou mauvais, sans rapport avec ce qu'il prétendait décrire. La mathématique, de ce point de vue, n'est pas autre chose qu'un art, une espèce de sculpture dans une matière extrêmement dure et résistante (comme certains porphyres employés parfois, je crois, par les sculpteurs). Michel-Ange a exprimé, au premier quatrain d'un sonnet admirable, cette idée (que j'imagine plus ou moins platonicienne) que le bloc de marbre contient, au sortir de la carrière, l'œuvre sculptée, et que le travail de l'artiste consiste à enlever ce qui est de trop : dans ses dernières années, d'ailleurs, il a de plus en plus profité des accidents du bloc de marbre, formant l'œuvre par l'extérieur et laissant le plus possible la surface brute (colosses des jardins Boboli, aujourd'hui au musée à Florence, et surtout sa dernière œuvre que les ignorants prétendent inachevée, la Pietà (ou plutôt la descente de croix) du Palazzo Rondanini à Rome). Le mathématicien est tellement soumis au fil, au contrefil, à toutes les courbures et aux accidents mêmes de la matière qu'il travaille, que cela confère à son œuvre une espèce d'objectivité. Mais l'œuvre qui se fait (et c'est cela à quoi tu t'intéresses) est œuvre d'art et par là même inexplicable (elle seule est à elle-même son explication). Cependant, si la critique d'art est un genre vain et vide, l'histoire de l'art est peut-être possible : et l'on n'a jamais, que je sache, examiné l'histoire des mathématiques de ce point de vue (à l'exception de Dehn, autrefois à Francfort, maintenant à Trondheim en Norvège, mais qui n'a jamais rien écrit là-dessus). Et il est tout à fait vain de se lancer là-dedans sans une étude approfondie des textes : encore, vu l'absence de toute étude préparatoire, faut-il choisir une période qui s'y prête. À ce propos, connais-tu Desargues ? Dehn m'en a longuement parlé à Oslo, en mai dernier. J'ai dit une fois à Cavaillès qu'il y aurait lieu d'étudier les débuts des fonctions elliptiques (Gauss, Abel, Jacobi, et même Euler et Lagrange, et tous les auteurs mineurs), mais il faut pour cela des connaissances que tu n'as pas. Pour l'algèbre babylonienne...