

UNE FAÇON DE FAIRE LA THÉORIE DES NOMBRES

ROBERT P. LANGLANDS

TABLE DES MATIÈRES

1. Introduction	1
2. Histoire	2
3. La théorie de Galois	3
4. La théorie du corps de classes	4
5. La géométrie algébrique	4
6. La cohomologie étale	5
7. Les fonctions L	7
8. Le programme dit de Langlands	8
9. Les représentations automorphes	9
10. L'avenir	10

1. INTRODUCTION

Quoiqu'elle a des conséquences concrètes facilement comprises sans rien de plus qu'une connaissance des principes mathématiques les plus élémentaires, dès son début chez les Grecs la théorie des nombres fut un sujet qui occupait une position centrale dans l'histoire des idées. Pour s'en convaincre, il suffit de jeter un coup d'œil aux livres VII et X d'Euclide, au dialogue Théétète de Platon, aux écrits du jeune Gauss ou de Galois au début du dix-neuvième siècle, ou plus récemment aux écrits des mathématiciens français André Weil et Alexander Grothendieck. Aujourd'hui même, sinon tous les spécialistes de la théorie, certainement bon nombre d'entre eux sont conscients de cette histoire et voudraient la continuer, quoique nous soyons rarement à la hauteur de nos ambitions.

Le dernier théorème de Fermat, dont la démonstration il y a une douzaine d'années est associée surtout au nom de Andrew Wiles, est toutefois la preuve que nous n'y manquons pas toujours. La preuve de ce théorème énoncé par le mathématicien Pierre de Fermat autour de 1630 fut recherchée sinon en vain, au moins avec un succès limité, pendant presque quatre siècles par des mathématiciens illustres avant que ses difficultés n'aient cédé dans les mains de Wiles aux méthodes modernes. Une forme du théorème s'énonce brièvement. Soient A , B et C des entiers différents de zéro et soit p un nombre premier impair, $p = 3, 5, 7, 11, 13, \dots$. Alors $A^p + B^p \neq C^p$. Même pour $p = 3$ la démonstration n'est pas facile.

Un des buts de cet article est d'expliquer, au moins superficiellement, la structure de sa démonstration, d'abord en utilisant des mots (en italique) encore inconnus par la plupart des lecteurs. Supposons que $A^p + B^p = C^p$, $ABC \neq 0$. Considérons l'équation algébrique $y^2 = x(x - A^p)(x - C^p)$. Il s'agit de l'équation d'une courbe, en fait d'une courbe *elliptique*

dont la *ramification* s'établit facilement. Cette ramification est petite! Ces deux mots inconnus appartiennent aux dix-huitième et dix-neuvième siècles. Une courbe elliptique définit un *motif*. À ce motif correspond une *représentation automorphe* avec la même petite ramification. Mais on démontre facilement qu'une telle représentation n'existe pas. Ces deux locutions sont l'apanage du vingtième siècle. La *correspondance* qui est la clé de la démonstration et qui est rattachée dans ce cas particulier aux noms des mathématiciens japonais Yutaka Taniyama et Goro Shimura a été démontrée par Wiles et son élève Richard Taylor.

Il me faut donc pour expliquer cette démonstration faire comprendre aux lecteurs cinq notions. Malheureusement trois d'elles — *motif*, *représentation automorphe*, *la correspondance* — ne sont pas encore comprises suffisamment même par les mathématiciens, au moins dans toutes leurs implications. Nous en savons plus que le nécessaire pour établir le théorème de Fermat, mais pas assez pour créer la grande théorie envisagée qui est le sujet de cet article. Je suis toutefois assez confiant qu'en poursuivant les questions, parfois floues, parfois précises, déjà entamées, nous arriverons inévitablement, mais tard plutôt que tôt, à une solution des difficultés centrales.

Mais à quoi servira cette théorie? À quelles questions concrètes et élémentaires semblables à celle du théorème de Fermat donnera-t-elle la réponse? Je ne sais pas et je crains que jusqu'à présent personne n'y ait pensé. Cependant son importance pour les questions plus arcanes est incontestable. Essayons de comprendre les grandes lignes de la théorie proposée ainsi que quelques obstacles majeurs. Le plus convaincant est de l'aborder du côté historique.

2. HISTOIRE

Quoique pour les fins de cet essai la théorie des nombres se réduit en principe à la résolution en nombres rationnels d'un nombre fini d'équations algébriques à un nombre fini d'inconnues, il nous faudra vite dépasser ce cadre car la théorie moderne de ces équations dites diophantiennes fait appel à la théorie des nombres algébriques et à la théorie générale des équations. La lecture de *Théétète* montre l'intérêt général de la première et celle de *La géométrie* de Descartes établit l'intérêt de la seconde.

Un nombre algébrique est une racine d'une équation de la forme

$$(1) \quad X^n + aX^{n-1} + bX^{n-2} + \cdots + f = 0$$

à une seule inconnue et à coefficients rationnels. Rappelons que la solution peut être un nombre complexe, donc un nombre de la forme $a + bi$, où a et b sont les nombres réels donnés par des points sur une ligne droite mais où i est le symbole mathématique pour une racine de $X^2 + 1 = 0$, un nombre dit imaginaire car il n'est pas donné par un point sur la ligne droite. Un nombre rationnel est un nombre donné par une fraction m/n , m et n étant des entiers. Tout nombre rationnel est réel mais tout nombre réel n'est pas rationnel, par exemple $\sqrt{2}$ ou π . L'avantage énorme des nombres complexes est que toute équation de la forme (1) à coefficients complexes a une racine complexe. Si ses coefficients sont réels, en particulier rationnels, il est possible qu'elle n'ait pas de racine réelle. La somme $a + b$ ou le produit ab de deux nombres algébriques est encore un nombre algébrique, aussi bien que leur quotient a/b si $b \neq 0$.

Une des premières grandes découvertes de la mathématique moderne était celle faite par le jeune Gauss de la symétrie cachée des $p - 1$ racines de l'équation $X^{p-1} + X^{p-2} + \cdots + X + 1$,

où p est un nombre premier. Puisque

$$(2) \quad X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \cdots + X + 1),$$

ces racines sont aussi appelées des p èmes racines de l'unité, sauf que nous excluons la racine 1. Une connaissance intime de cette symétrie a permis à Gauss de démontrer un théorème de la géométrie élémentaire que l'expérience de deux mille ans avait mené tout le monde à tenir pour faux, la possibilité de la construction n'utilisant qu'une règle et un compas d'un heptadécagone (un polynôme à dix-sept côtés) régulier. L'existence et l'importance des symétries semblables rattachées à n'importe quelle équation à une seule variable furent vite reconnues par Galois et les *groupes de Galois* occupent aujourd'hui une place centrale dans la théorie des équations diophantiennes.

Si x est un nombre algébrique, donc la racine d'une équation (1), alors $x^n = -ax^{n-1} - bx^{n-2} - \cdots - ex - f$. En multipliant cette équation par x pour obtenir $x^{n+1} = -ax^n - bx^{n-1} - \cdots$, et en substituant alors pour x^n sa valeur selon la première équation, on obtient en simplifiant une équation $x^{n+1} = a'x^{n-1} + b'x^{n-2} + \cdots$ avec des nouveaux coefficients rationnels a', b', \dots . Donc non pas seulement x^n , mais tous les nombres de la forme $a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$, m arbitrairement grand et a_0, a_1, \dots tous rationnels, sont égaux à une combinaison finie $a'_0 + a'_1x + \cdots + a'_{n-1}x^{n-1}$, où les coefficients sont encore tous rationnels. L'ensemble, noté $\mathbf{Q}(x)$, de ces nombres s'appelle un corps (de dimension finie) de nombres algébriques. Le symbole \mathbf{Q} dénote simplement l'ensemble, aussi un corps, de tous les nombres rationnels. Si le corps $\mathbf{Q}(x)$ contient les deux nombres y et y' , il contient aussi leur somme $y + y'$, leur produit yy' et, pour $y' \neq 0$, le quotient y/y' . Si le corps $F' = \mathbf{Q}(x')$ contient x alors il contient tout élément du corps $F = \mathbf{Q}(x)$ et nous disons que F' est une extension de F . En particulier, tout corps de nombres algébriques contient le corps \mathbf{Q} .

3. LA THÉORIE DE GALOIS

Elle est, en particulier, une théorie de ces extensions. Si x est un nombre algébrique et une racine du polynôme $P(X)$ à coefficients rationnels et si $P(X)$ est un produit $P(X) = R(X)S(X)$, alors $0 = P(x) = R(x)S(x)$ de sorte que $R(x) = 0$ ou $S(x) = 0$. Par conséquent, si $P(X)$ est le polynôme de plus bas degré tel que $P(x) = 0$ et tel que le coefficient de la plus grande puissance de X qui paraît dans $P(X)$ est 1, alors $P(X)$ est non seulement déterminé uniquement par x , il est en plus irréductible, c'est-à-dire qu'il n'est pas égal à un produit de deux autres polynômes.

Le principe clé de la théorie dite de Galois est que, d'un point de vue algébrique, dans ces circonstances toutes les racines du polynôme sont équivalentes. Donc si x et x' sont deux racines, les deux corps $F = \mathbf{Q}(x)$ et $F' = \mathbf{Q}(x')$ sont dits isomorphes. D'un point de vue abstrait et algébrique il est impossible de les distinguer, quoique comme nombres algébriques $x \neq x'$. On fait correspondre à n'importe quel $y = a_0 + a_1x + a_2x^2 + \cdots$ dans F , où a_0, a_1, \dots sont dans \mathbf{Q} , le nombre $y' = a_0 + a_1x' + \cdots$ dans F' . Nous écrivons soit $\phi : y \rightarrow y'$, soit $y' = \phi(y)$ et nous disons que ϕ est une application ou un isomorphisme de F sur F' , car si $\phi : z \rightarrow z'$ alors

$$\phi : y + z \rightarrow y' + z', \quad \phi : yz \rightarrow y'z'.$$

Si x'' est une troisième racine alors il y a des applications semblables ϕ' de F' à F'' et ψ de F à F'' . Observons que ψ est obtenu en composant $\phi : y \rightarrow y'$ et $\phi' : y' \rightarrow y''$. Nous l'appelons leur produit et l'écrivons $\psi = \phi' \circ \phi$. Il arrive fréquemment que pour un polynôme irréductible tous les ensembles F, F', F'', \dots sont égaux, un exemple simple étant

$P(X) = X^2 + 1$, dont les deux racines sont $x = i$ et $x = -i$. Nous disons alors que le corps F est galoisien sur le corps \mathbf{Q} . Dans ce cas les applications ϕ, ϕ', \dots sont toutes des permutations d'un seul ensemble F et elles forment son groupe de Galois, un groupe fini, donc un ensemble avec une notion de produit, qui satisfait à quelques lois simples. Il y a aussi une notion semblable pour les extensions F'/F de n'importe quel corps algébrique F aussi bien que pour son groupe de Galois, noté $\text{Gal}(F'/F)$. Observons que pour un corps de base F donné les mathématiciens parlent souvent de son groupe de Galois sans référence à une extension F' , qui implicitement est simplement assez large, même peut-être d'une dimension infinie, mais je préfère esquiver de telles questions ici.

4. LA THÉORIE DU CORPS DE CLASSES

Un groupe est dit abélien si l'égalité $\phi' \circ \phi = \phi \circ \phi'$ pour n'importe quelle couple de ses éléments. Cette égalité en apparence anodine ne l'est pas. Elle est une restriction sérieuse. La plupart des groupes ne sont pas abéliens. Le polynôme $X^{p-1} + X^{p-2} + \dots + 1$ qui est le deuxième facteur de l'équation (2) est irréductible et l'extension définie par une de ses racines est abélienne. Ce fut la connaissance de la structure de son groupe de Galois qui a permis à Gauss de construire géométriquement le heptadécagone régulier. À la suite des recherches du mathématicien allemand Kummer sur le théorème de Fermat au milieu du dix-neuvième siècle, on a découvert au seuil du vingtième siècle la possibilité d'une description précise et générale de toutes les extensions galoisiennes à groupe de Galois abélien, dites simplement abéliennes, de n'importe quel corps F de nombres algébriques. Quoique fondée par des grands mathématiciens comme Kronecker et Hilbert, cette théorie, dite du corps de classes, fut longtemps tenue pour trop difficile pour le commun des mathématiciens. Même aujourd'hui, malgré son importance reconnue pour les questions élémentaires et concrètes de la théorie des nombres, surtout pour le théorème de Fermat, elle n'est connue que par les spécialistes, dont le nombre est devenu toutefois très grand.

Quoiqu'il s'agisse d'un gros pan de mathématiques difficiles nous ne pouvons pas nous arrêter sur ce sujet. Il ne nous sert que de trampoline pour passer à un défi bien plus formidable. D'abord une description utile pour la théorie des nombres de chaque extension, galoisienne ou non, d'un corps de nombres algébriques ; ensuite une compréhension non pas seulement des racines d'une équation algébrique à une seule variable mais des courbes et des variétés de dimension plus grande définies par un nombre fini d'équations en un nombre fini de variables. Nous nous intéressons donc à la géométrie analytique ou algébrique, une géométrie entamée par Descartes, mais devenue par la suite bien plus difficile grâce à ses liens avec l'arithmétique, le calcul infinitésimal et la topologie, tous encadrés par la géométrie et liés dans elle, l'un à l'autre.

5. LA GÉOMÉTRIE ALGÉBRIQUE

Ces liens furent créés pendant deux siècles et demi par des mathématiciens comme Euler et Riemann et nous ne pouvons guère en rendre compte en quelques lignes. Mais essayons, car sans eux nous ne pouvons point comprendre l'arithmétique contemporaine. J'avoue toutefois sans ambages qu'il s'agit pour moi après plus de cinquante ans comme mathématicien d'un mystère que je ne m'attends jamais à pénétrer. Je crois d'ailleurs que tout mathématicien qui a réfléchi à ces questions a des sentiments semblables.

Les deux courbes planaires $Y^2 = X^2 - 1$ et $Y^2 = X^3 - 1$ sont différentes, mais en quoi consiste cette différence ? La première est une courbe rationnelle ; la deuxième, une courbe

elliptique. Comme courbes réelles et complexes elles sont dessinées dans la première figure. Les courbes complexes, donc l'ensemble des points à coefficients complexes dans l'une ou l'autre des deux courbes, sont plus difficiles à saisir pour un lecteur sans expérience. Si on ajoute, comme font les géomètres, les points à l'infini au nombre de deux pour la première courbe et d'un pour la deuxième, on obtient soit une sphère, soit un tore. Les points réels sont pour la première $X \leq -1$ ou $X \geq 1$, $Y = \sqrt{X^2 - 1}$, un cercle équatorial, et pour la deuxième $X \geq 1$, $Y = \sqrt{X^3 - 1}$, un cercle méridien. Ce sont les courbes complexes dont les propriétés topologiques importent à présent et de ce point de vue elles sont certainement différentes, comme les dessins le démontrent. Il est regrettable que l'ensemble des points complexes sur une courbe algébrique soit une surface difficile à visualiser, mais il n'y a pas de remède.

Une chose frappante qui est à la source de la création de la topologie, si importante aux mathématiques du vingtième siècle, est que cette différence est liée au calcul des intégrales. Par exemple, même les lycéens savent que les intégrales

$$(3) \quad \int \frac{dX}{Y} = \int \frac{dX}{\sqrt{X^2 - 1}}, \quad \int \frac{X dX}{Y} = \int \frac{X dX}{\sqrt{X^2 - 1}},$$

sur la première courbe se calculent facilement. Elles sont égales à $\ln(X + Y)$ et à Y . Pour la seconde courbe un lycéen, même une lycéenne, ne saurait pas quoi faire. Il s'agit des intégrales elliptiques,

$$(4) \quad \int \frac{dX}{Y} = \int \frac{dX}{\sqrt{X^3 - 1}}, \quad \int \frac{X dX}{Y} = \int \frac{X dX}{\sqrt{X^3 - 1}},$$

que même les mathématiciens ne rencontrent que tard dans leurs études. Les intégrales pour la première courbe possèdent chacune une propriété déplaisante. La première est une fonction, le logarithme, qui est mal défini en 0 et à l'infini. L'autre est trop simple. Elle est une fonction algébrique. Par contre les deux fonctions de (4) sont bien définies partout, et en même temps ne sont pas simplement des fonctions rationnelles en X et Y . Il n'y a essentiellement que deux telles fonctions indépendantes. La différence entre (3) et (4) est un reflet algébrique de la différence topologique entre les deux courbes. La première est une sphère, donc pour les topologues de genre $g = 0$, et la seconde un tore, donc de genre $g = 1$. Le nombre de *bonnes* intégrales indépendantes est toujours $2g$, où le genre g , du point de vue topologique, est le nombre de trous dans la surface donnée par l'ensemble des points complexes d'une courbe, qui serait une sorte de multi-tore. Par exemple la courbe $Y^2 = X^5 - 1$ correspond à l'ensemble topologique de la deuxième figure. Son genre est 2 car cet ensemble a deux trous. Les quatre bonnes intégrales indépendantes sont

$$\int \frac{dX}{Y}, \quad \int \frac{X dX}{Y}, \quad \int \frac{X^2 dX}{Y}, \quad \int \frac{X^3 dX}{Y}.$$

6. LA COHOMOLOGIE ÉTALE

Il faut s'imaginer que pour une variété algébrique de dimension (algébrique) n plus élevée, pour laquelle l'ensemble de points complexes serait maintenant une variété topologique de dimension (topologique) $2n$, il y aura une relation semblable entre les invariants topologiques et les propriétés plus algébriques des intégrales à plusieurs variables. La décrire en quelques lignes serait impossible, d'autant plus qu'il y a un lien encore plus difficile entre la topologie et non plus les intégrales algébriques mais le nombre de points, dans un sens idoine, sur les variétés qu'il faut décrire. Malgré la difficulté de sa compréhension, même pour les

mathématiciens expérimentés, il faut, à mon avis, tenir ce lien comme la grande contribution des français, surtout, mais pas seulement, celle d'André Weil et d'Alexander Grothendieck, aux mathématiques de la deuxième moitié du vingtième siècle.

Quoique nous ayons introduit le genre d'une courbe simplement comme un entier, cet entier est une dimension, la dimension d'un espace (vectoriel) appelé la *cohomologie* de la courbe en degré 1. Pour une variété quelconque, il y en a de tous les degrés, de 0 jusqu'à $2n$, sa dimension topologique. Ces espaces vectoriels peuvent être définis soit par voie topologique, soit par des intégrales, soit d'une façon purement algébrique. Cela mène à des objets différents mais, pour une variété donnée et en degré donné, tous de la même dimension. Nous n'avons pas essayé d'expliquer la façon purement algébrique qui mène à la cohomologie dite étale. Elle fait intervenir implicitement les nombres algébriques et par conséquent les groupes de Galois.

Je ne peux guère décrire cette cohomologie, mais pensons à une courbe algébrique (topologiquement une surface !) à coefficients dans le corps \mathbf{Q} de nombres rationnels. Enlevons un nombre fini de points et considérons un recouvrement de la courbe qui reste. Par exemple, si la courbe est la digne droite à paramètre X et si on enlève les points 0 et ∞ , un recouvrement possible est la courbe $Y^3 = X$, où $X \neq 0, Y \neq 0$. À chaque point $x \neq 0$ de la ligne droite sont attachés les trois points au-dessus de x , $y = x^{1/3}$, $y = ax^{1/3}$, $y = bx^{1/3}$, où $a = \cos(2\pi/3) + i \sin(2\pi/3)$ est une 3^e racine de l'unité et $b = a^2$. Le produit de deux tels recouvrements est, encore à titre d'exemple, l'ensemble des couples $\{(y_1, x), (y_2, x)\}$ de points au-dessus d'un même x est aussi un recouvrement mais à trois feuilles $y_2 = y_1$, $y_2 = ay_1$, $y_2 = by_1$. Sur chaque feuille, il y a trois points au-dessus d'un x donné. De toute façon, jouant de cette manière avec les recouvrements en général, nous pouvons introduire des configurations de recouvrements, qui auront eux-mêmes leur géométrie élémentaire. Elle sera compliquée mais nous pouvons y attacher, par les principes habituels de la topologie, les espaces de cohomologie. Les éléments du groupe de Galois agiront sur les coefficients de ces recouvrements, par exemple, sur les coefficients a et b et par conséquent sur les recouvrements, sur les configurations, et sur les espaces de cohomologie étale. Nous sommes allés très vite, mais tout expliquer exigerait un tome épais.

Comme conséquence les éléments du groupe de Galois ne sont pas que les permutations des nombres algébriques, ils sont aussi des applications des espaces de la cohomologie sur eux-mêmes. Nous arrivons maintenant à un autre principe et cette fois non pas simplement de la théorie des nombres mais de la mathématique et de la physique : l'importance capitale des représentations d'un groupe par des matrices et des structures qui s'en déduisent. Pour la physique je cite, sans essayer d'expliquer ce qu'il veut dire, la phrase du physicien-mathématicien Hermann Weyl, "*Alle Quantenzahlen sind Kennzeichen von Gruppendarstellungen*". En particulier le *spin* d'une particule, élémentaire ou non, caractérise la représentation du groupe de rotations y rattachée. La leçon que nous voulons tirer de ce dicton, "il se trouve derrière tout nombre quantique une représentation d'un groupe", c'est que tomber en mathématiques ou en physique sur les représentations d'un groupe, c'est souvent tomber sur une veine d'or à laquelle il faut tenir corps et âme. En introduisant les motifs, Grothendieck voulut introduire la possibilité de définir les "particules élémentaires" dont sont constituées les variétés algébriques. Quoique inachevées et trop difficiles pour les expliciter ici ses idées restent centrales.

Nous avons esquissé dans l'encadré l'essentiel des représentations des groupes, sans toutefois éclairer toutes les possibilités ni pour un groupe ni pour une représentation.

Soulignons simplement que les représentations, sauf exceptions malsaines, peuvent être additionnées, multipliées et décomposées en parties irréductibles. Ajoutons aussi sans explications que les représentations du groupe de Galois sur les espaces de cohomologie étale ne sont qu'un reflet des vraies représentations cherchées.

7. LES FONCTIONS L

Ces représentations du groupe de Galois sont déjà assez difficiles car elles permettent de définir la fonction zéta (ou L) rattachée à un motif ou à une variété algébrique. Elle est une fonction d'une variable complexe définie à partir de la représentation du groupe de Galois par un produit d'un nombre, malheureusement infini, de facteurs. En le calculant on observe que la plupart des facteurs sont tellement proches de 1 que leur produit aussi y est proche, de sorte que l'on calcule d'abord le produit d'une façon approximative en n'utilisant qu'un nombre fini des facteurs, pour ensuite passer à une limite. Si le corps de base est le corps de nombres rationnels \mathbf{Q} , il y a un facteur pour chaque nombre premier p et ce facteur est de la forme

$$(5) \quad \frac{1}{\left(1 - \frac{a_1}{p^s}\right) \cdots \left(1 - \frac{a_d}{p^s}\right)}, \quad a_i = a_i(M),$$

où d est la dimension de l'espace de la représentation, donc de la cohomologie du motif dont M est le symbole. Le nombre d est un entier positif ou nul et les nombres $a_1 = a_1(M), \dots, a_d = a_d(M)$, sont complexes. Ils remplacent, dans ce cadre, le spin ou nombre quantique dont parla Weyl. Enfin s est la variable dans la fonction, d'abord réelle, même positive et grande, mais ensuite complexe. La notation habituelle pour ce produit infini est

$$(6) \quad L(s, M) = \prod_p \frac{1}{\left(1 - \frac{a_1}{p^s}\right) \cdots \left(1 - \frac{a_d}{p^s}\right)}.$$

Il est difficile d'expliquer d'où viennent les coefficients a_j . À titre d'exemple considérons la variété de dimension 0, donc un ensemble fini des points, donnée par l'équation $X^2 - 3 = 0$. Sur cette variété il n'y a que deux points, $x = \pm\sqrt{3}$, tous les deux irrationnels. Cependant ce qui compte pour la fonction zéta, ou plutôt son facteur au nombre p , c'est le nombre de solutions d'une congruence $X^2 - 3 \equiv 0 \pmod{p}$. Une solution est un entier x tel que p divise $x^2 - 3$. Si x est une solution, alors tout entier $x + yp$, y entier, est aussi une solution, de sorte que l'on ne compte que les solutions x telles que $0 \leq x < p$. Pour $p = 2, 3$, il n'y en a qu'une seule. Si le reste de p après division par 12 est 1 ou 11 il y en a deux et les coefficients dans (5) sont $a_1 = a_2 = 1$; s'il est 5 ou 7 il n'y en a pas et les coefficients sont $a_1 = 1, a_2 = -1$. Expliquer le cas général serait expliquer en général le lien entre les représentations du groupe de Galois et les congruences. Ce n'est pas trop difficile si l'on n'exige pas de démonstration, mais un peu long.

Nous avons vu en esquissant la démonstration du théorème de Fermat qu'une étude de la ramification était essentielle. La ramification est une mesure du comportement exceptionnel des congruences en certains nombres premiers. Dans l'exemple simple que nous venons de décrire, la congruence est ramifiée aux nombres premiers 2 et 3. L'examen de la ramification est presque toujours fastidieux mais souvent indispensable.

Il n'a pas été prévu dans leurs définitions, mais si, par exemple, M est le motif rattaché à une variété définie par des équations à coefficients dans le corps \mathbf{Q} , toutes les indications

suggèrent que les fonctions L de (6) contiennent des renseignements importants sur l'arithmétique de M , donc non pas seulement sur les solutions des congruences y rattachées, mais sur les solutions rationnelles elles-mêmes des équations qui le définissent. Ces renseignements sont disponibles seulement si les fonctions sont prolongées de l'ensemble de nombres réels, positifs et grands à l'ensemble de tous les nombres complexes. Les prolonger d'une façon cohérente et utile (le mot technique est analytiquement) est un problème central et difficile. De toute évidence il est impossible de le résoudre sans les formes automorphes et les représentations automorphes.

8. LE PROGRAMME DIT DE LANGLANDS

Ce que j'ai proposé, quoique la forme originale du programme était plus limitée, restreinte aux motifs ou variétés de dimension 0, donc à la description des corps de nombres algébriques, ce fut de construire tout un autre édifice, un édifice aussi complexe que celui que nous venons de décrire, dont l'architecture contient les fonctions L semblables aux fonctions (6). Même le programme modeste est loin d'être achevé mais ses succès, surtout sa contribution à la démonstration du théorème de Fermat, ont dissipé le malaise et le scepticisme de la plupart des spécialistes. Ce malaise provint en grande partie des méthodes, celles de l'analyse des espaces et des représentations de dimension infinie, rédhibitoire pour bon nombre d'adeptes de la théorie des nombres classique et, malheureusement, aussi, sans doute, pour les lecteurs de cette revue.

Néanmoins, c'est en large partie grâce à deux mathématiciens, dont les noms sont rattachés étroitement à la théorie des nombres concrète, L. J. Mordell et Ramanujan, que les fonctions L ont assumé une place si large dans la théorie des formes automorphes. Ramanujan a découvert une propriété fondamentale d'une série qui porte maintenant son nom et Mordell l'a démontrée. Les idées furent poursuivies par Erich Hecke, dont l'influence a mené au cadre moderne à la suite de quelques décennies. Soit

$$\Delta(\omega) = g(x) = x \left\{ (1-x)(1-x^2) \cdots \right\}^{24} = x \left\{ \prod_{k=1}^{\infty} (1-x^k) \right\}^{24} = \sum_{n=1}^{\infty} \tau(n) x^n, \quad x = e^{2\pi i \omega}.$$

Nous supposons que $\omega = u + iv$, $v > 0$, de sorte que $|x| < 1$. Les coefficients $\tau(n)$ sont des entiers et se calculent en développant le produit infini. Par exemple, $\tau(1) = 1$, $\tau(2) = -24$, $\tau(3) = 252$. Ramanujan a proposé que $\tau(nn') = \tau(n)\tau(n')$ si n et n' n'ont pas de diviseur premier commun et que $|\tau(p)| \leq 2p^{11/2}$ pour tout nombre premier p . Par exemple $|-24| = 24 \leq 2 \times 2^{11/2}$. Mordell a vite vérifié la première hypothèse. La deuxième n'a été vérifiée que bien plus tard. C'est la première qui permet l'introduction de la série

$$(7) \quad L(s) = \prod_p \frac{1}{1 - \frac{\tau(p)}{p^s} + \frac{p^{11}}{p^{2s}}} = \prod_p \frac{1}{\left(1 - \frac{\alpha_p}{p^s}\right)\left(1 - \frac{\beta_p}{p^s}\right)},$$

où $\alpha_p + \beta_p = \tau(p)$ et $\alpha_p \beta_p = p^{11}$. Grâce aux propriétés analytiques et algébriques de la forme automorphe Δ , la prolongation de $L(s)$ à tout le plan complexe est facile.

9. LES REPRÉSENTATIONS AUTOMORPHES

Expliquons vite comment passer à une théorie plus générale et aux représentations automorphes. Soit

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

une matrice à coefficients réels à déterminant $ad - bc$ positif. C'est un élément du groupe $\mathrm{GL}(2, \mathbf{R})$ des matrices à deux lignes et deux colonnes et à coefficients réels. Alors la fonction de g ,

$$f_\Delta(g) = \frac{1}{(a+ci)^{12}} \Delta \left(\frac{b+di}{a+ci} \right),$$

satisfait aux équations

$$(8) \quad f_\Delta(hg) = f_\Delta(g),$$

pour toute matrice h dont les coefficients sont entiers et dont le déterminant est 1. De telles fonctions sont aussi appelées des formes automorphes. À n'importe quel élément k de $\mathrm{GL}(2, \mathbf{R})$ nous rattachons une application linéaire $R(k)$ de l'espace de ces formes, qui envoie la forme f sur $f' = R(k)f$, $f'(g) = f(gk)$. Avec les matrices nous avons introduit les représentations de dimension finie. Les applications $R(k)$, qui satisfont à l'équation $R(k)R(\ell) = R(k\ell)$, nous donnent des représentations de dimension infinie ! En utilisant une notion convenable d'irréductibilité pour les représentations de dimension infinie, nous distinguons, comme pour les motifs, les formes automorphes — et les représentations automorphes qu'elles définissent — auxquelles sont rattachées des fonctions L , dont la plus simple aura comme (7) la forme

$$(9) \quad \prod_p \frac{1}{\left(1 - \frac{\alpha_p}{p^s}\right)\left(1 - \frac{\beta_p}{p^s}\right)},$$

mais avec, en général, de nouveaux coefficients α_p , β_p . Encore une fois, prolonger ces fonctions au plan complexe n'est pas difficile.

Créer une théorie pareille, non pas seulement pour le groupe $\mathrm{GL}(2, \mathbf{R})$ mais en général pour $\mathrm{GL}(d, \mathbf{R})$, ne pose pas de problème sérieux. Les fonctions f sont des fonctions sur l'ensemble de matrices à d lignes et d colonnes à déterminant positif, mais l'équation (8) se lisant $f(hg) = f(g)$ pour h entier et à déterminant 1 ne change pas. Cette théorie plus générale pose toutefois un nouveau genre de problème, pas du tout facile. Pour $\mathrm{GL}(d, \mathbf{R})$ les fonctions L de base auront la forme

$$(10) \quad \prod_p \frac{1}{\left(1 - \frac{\alpha_{p,1}}{p^s}\right)\left(1 - \frac{\alpha_{p,2}}{p^s}\right) \cdots \left(1 - \frac{\alpha_{p,d}}{p^s}\right)}.$$

Supposons que la suite de couples (α_p, β_p) , $p = 2, 3, 5, \dots$ provient d'une représentation automorphe pour $\mathrm{GL}(2, \mathbf{R})$. Pour un d donné formons les suites $(\alpha_p^{d-1}, \alpha_d^{d-2}\beta_p, \dots, \alpha_p\beta_p^{d-2}, \beta_p^{d-1})$ de longueur d . Une hypothèse importante, même centrale, du programme est qu'il y a une deuxième forme (ou représentation) automorphe non pas pour le groupe $\mathrm{GL}(2, \mathbf{R})$ mais pour $\mathrm{GL}(d, \mathbf{R})$ telle que la fonction L de (10) est

$$\prod_p \frac{1}{\left(1 - \frac{\alpha_p^{d-1}}{p^s}\right)\left(1 - \frac{\alpha_p^{d-2}\beta_p}{p^s}\right) \cdots \left(1 - \frac{\alpha_p\beta_p^{d-2}}{p^s}\right)\left(1 - \frac{\beta_p^{d-1}}{p^s}\right)}.$$

Cette question est une forme du principe que j'ai nommé la fonctorialité. Il permet le transfert des formes automorphes d'un groupe à l'autre. Nous ne l'avons formulée ici que dans un cas particulier, qui est néanmoins difficile. Il s'agit de l'obstacle principal à une théorie complète au côté automorphe, en particulier un des deux obstacles qu'il faut surmonter pour arriver au genre de théorie prôné par Weyl. Le problème de fonctorialité se pose pour d'autres groupes aussi, tels les groupes de rotations dans n'importe quelle dimension, et dans d'autres formes.

10. L'AVENIR

Je crois entrevoir une façon d'aborder ce problème, mais même si j'ai raison, ce qui n'est pas évident, il s'agirait d'un travail d'exploration de longue haleine et ne serait pas le travail d'un seul chercheur. Mais après avoir établi le théorème de Fermat, les mathématiciens peuvent se permettre quelques décennies de travail plus modeste. L'outil le plus prometteur est la formule dite des traces et là on a déjà non pas seulement le travail patient et ardu de James Arthur, mais aussi les résultats frappants récents de Ngô Bào Châu à Paris. Je souligne toutefois que cette méthode ne puisse réussir sauf si elle fasse apparaître dans le cadre de la formule des traces les extensions galoisiennes finies arbitraires. Il faut attendre donc que du progrès sérieux entraînera la résolution des questions encore imprévues de la théorie des nombres.

Une fois la théorie des formes ou représentations automorphes achevée ou au moins arrivée à un stade acceptable, la dernière étape serait d'établir en général la correspondance entre ces représentations et les motifs. Des énoncés précis exigent une utilisation plus systématique de groupes et de leurs représentations et des explications plus élaborées de la fonctorialité, mais la condition de base est qu'à chaque motif irréductible sur un corps de nombres il y a une représentation automorphe d'un groupe $GL(m)$ telle que les facteurs des produits (6) et (10) sont égaux. Cela permettra la résolution d'au moins un problème : la prolongation des fonctions L rattachées aux motifs.

Pour moi la première question en ce dernier stade, à laquelle je n'ai pas encore assez réfléchi, sera la suivante : la fonctorialité acquise, les méthodes fondées — à la suite de la démonstration du théorème de Fermat — sur les idées de Wiles et de Taylor poussées à bout, quels seront les obstacles à l'établissement complet de cette correspondance qui restent ?

Compiled on November 17, 2025.