De la fonction ζ aux travaux de Weil & Deligne

1 La fonction ζ de Riemann

Considérons la fonction h qui à s associe le nombre

$$h(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots + \frac{1}{n^s} + \dots = \sum_{n=1}^{\infty} \frac{1}{n^s} .$$

On démontre que cette écriture a un sens, c'est-à-dire que la fonction h est définie dès que s est strictement supérieur à 1. De plus on peut étendre h aux nombres complexes $s = x + iy$ en posant, selon l'habitude, $n^s = n^x \cdot e^{i(y \ln n)}$; h est alors définie dans le demi-plan complexe de partie réelle x strictement supérieure à 1.

Cette fonction h présente un intérêt majeur dans l'étude de la répartition des nombres premiers car il n'est pas trop difficile de voir que :

$$h(s) = \sum_{1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ premier}} \left(1 - \frac{1}{p^s}\right)^{-1} \qquad (1)$$

où le produit infini du membre de droite est étendu à l'ensemble de tous les nombres premiers.

Sous l'une des deux formes (1), cette fonction h n'est malheureusement pas facile à manipuler et Riemann a découvert en 1859 la fonction ζ qui prolonge la fonction h au plan complexe tout entier (sauf en 1). Il se trouve alors que ζ vérifie la relation fonctionnelle importante :

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \pi^{-\frac{1-s}{2}} \Gamma\left(\frac{1-s}{2}\right) \zeta(1-s) \qquad (2)\ *$$

où Γ n'est autre que la fonction qui prolonge la notion de factorielle $[\Gamma(n) = (n-1)!]$ et qu'on peut écrire :

$$\Gamma(x) = \lim_{n \to \infty} \frac{n!\, n^{x-1}}{x(x+1)(x+2)\dots(x+n-1)}$$

---

* Cette relation avait été conjecturée par Euler qui l'avait démontrée pour s entier et vérifiée pour quelques autres valeurs.

La relation (2) nous montre que la fonction ζ présente une certaine symétrie, plus exactement, comme les points d'affixe s et 1 – s sont symétriques par rapport au point d'affixe $\frac{1}{2}$, la fonction ζ qui n'est autre que h pour Re(s) $>$ 1 est également bien connue pour Re(s) $<$ 0 (0 est le symétrique de 1 par rapport à $\frac{1}{2}$).

Reste le cas de la bande de plan correspondant aux parties réelles comprises entre 0 et 1 et surnommée bande critique. On démontre que ζ s'annule une infinité de fois dans cette bande et on a de bonnes raisons de penser que tous les zéros non triviaux * de ζ sont de partie réelle égale à $\frac{1}{2}$. C'est ce qu'on appelle l'hypothèse de Riemann et qui permettrait (si elle était vraie) de démontrer d'excellents résultats sur la répartition des nombres premiers, par exemple le "théorème" des nombres premiers qui dit que le nombre $\varpi(x)$ des nombres premiers inférieurs à x est donné par :

$$\varpi(x) = \int_2^x \frac{dt}{\ln t} + 0(\sqrt{x}) .$$

L'avènement de l'ordinateur a permis de vérifier que l'hypothèse de Riemann est vraie pour les 3 500 000 premiers zéros ! **

Depuis 120 ans les mathématiciens se sont attaqués sans succès à l'hypothèse de Riemann. L'une des méthodes a été de construire des analogues de la fonction ζ dans d'autres corps que $\mathbb{Q}$ et d'essayer de voir ce qui se passe dans ces cas là. Différentes voies sont possibles : corps p-adiques, corps finis, corps de fonctions. C'est dans cette dernière direction qu'a travaillé A. Weil.

2 Quelques rappels d'algèbre

Avant que d'essayer de généraliser la fonction ζ nous donnerons quelques rappels sur les anneaux et les modules. Le lecteur familiarisé avec ces notions peut évidemment passer au troisième paragraphe.

a) Anneau unitaire. C'est un ensemble muni d'une addition qui en fait un groupe abelien et d'une multiplication associative, ayant un élément neutre (1) et distributive par rapport à l'addition [dans les exemples d'utilisation, l'anneau sera aussi commutatif, c'est-à-dire que la multiplication le sera] . Exemple : ($\mathbb{Z}$,+,x).

b) Idéal. C'est un sous-ensemble I de l'anneau A tel que

$$\forall a \in A \quad \forall x \in I \quad ax \in I$$

Les idéaux jouent un rôle très important en théorie des nombre et on est amené à étudier les propriétés particulières des idéaux .

---

* ζ possède une infinité de zéros triviaux qui sont les entiers négatifs pairs.
** On a même démontré qu'il y a une infinité de zéros de partie réelle égale à $\frac{1}{2}$ (mais une infinité ne veut pas dire tous !).

idéal premier : si tout élément de l'idéal de la forme ab est tel que soit a, soit b appartient à l'idéal

$$\forall x \in I \quad x = ab \implies (a \in I \quad \text{ou} \quad b \in I).$$

Dans $\mathbb{Z}$, tout idéal est principal, c'est l'ensemble des multiples d'un nombre donné ; les idéaux premiers ne sont autres que ceux engendré par les nombres premiers. Mais cette notion a l'avantage de permettre la généralisation à un anneau quelconque de la notion de nombre premier.

c) Entiers dans un corps. Dedekind avait réussi à définir la notion d'entier dans un corps de nombre (c'est-à-dire dans une extension de $\mathbb{Q}$), mais sa méthode ne pouvait pas être généralisée à un corps K quelconque. Dans ce cas il faut passer par l'intermédiaire des valuations :

valuation : on appelle valuation ν dans un corps K une application surjective de K dans $\mathbb{Z}$, telle que $\nu(\alpha \cdot \beta) = \nu(\alpha) + \nu(\beta)$ et qui vérifie la relation : $\forall \alpha \in K \ \forall \beta \in K \quad \nu(\alpha+\beta) \geqslant \min\left[\nu(\alpha), \nu(\beta)\right]$. On pose de plus $\nu(0) = +\infty$.

On démontre que l'ensemble $\mathcal{D}$ des éléments de K dont toutes les valuations sont positives ou nulles forme un anneau qu'on appelle (pour un tas de bonnes raisons) anneau des entiers de K. Tout idéal de $\mathcal{D}$ sera dit idéal entier de K. On caractérise les éléments premiers π de $\mathcal{D}$ par le fait que pour toutes les valuations $\nu(\pi) = 0$ sauf pour une pour laquelle $\nu(\pi) = 1$.

exemple : Prenons K = $\mathbb{Q}$. Soit p un nombre premier, $\frac{a}{b}$ un élément de $\mathbb{Q}$, α et β les exposants respectifs de a et b dans leur décomposition en nombre premier. Posons

$$\nu_p\left(\frac{a}{b}\right) = \alpha - \beta .$$

Il est facile de vérifier que ν_p est une valuation dans $\mathbb{Q}$ qui vaut 1 pour p, 0 pour tout autre nombre premier de $\mathbb{Z}$ et est positif ou nul pour tout nombre entier. On démontre que toutes les valuations de $\mathbb{Q}$ sont obtenues de cette façon. Il est alors facile de voir que les définitions données ci-dessus pour la notion d'entiers dans un corps K s'appliquent à $\mathbb{Q}$ et redonnent exactement $\mathbb{Z}$.

Soit alors $\mathfrak{a}$ un idéal entier de K (idéal de l'anneau $\mathcal{D}$ des entiers de K). On définit la norme de $\mathfrak{a}$ et on note $N(\mathfrak{a})$ le nombre des éléments de $\mathcal{D}/\mathfrak{a}$, ensemble quotient de $\mathcal{D}$ par la relation d'équivalence :

$$\forall \alpha \in \mathcal{D} \quad \forall \beta \in \mathcal{D} \quad \alpha \sim \beta \iff \alpha - \beta \in \mathfrak{a}$$

d) corps de fonctions. Soit K un corps et K $[x,y]$ l'ensemble des polynômes à deux variables à coefficients dans K. On sait que K $[x,y]$ est un anneau. Considérons alors l'idéal $\mathcal{Q}$ engendré par un polynôme q(x,y) ; q(x,y) = 0 peut être considéré comme l'équation d'une courbe Q et $\mathcal{Q}$ est alors l'idéal des polynômes s'annulant sur Q. L'ensemble quotient K $[x,y]/\mathcal{Q}$ (obtenu par identification de deux polynômes dont la différence est dans $\mathcal{Q}$ peut être muni d'une structure d'anneau. On construit alors son corps des fractions (de la même façon que l'on passe de $\mathbb{Z}$ à $\mathbb{Q}$) et on obtient le corps des fonctions rationnelles sur la courbe algébrique Q.

Cette construction peut être étendue à un nombre quelconque de variables. On obtient alors le corps des fonctions rationnelles sur une variété algébrique.

e) Genre d'une courbe. Soit $f(x,y) = 0$ l'équation d'une courbe Γ, où x et y sont des nombres complexes. Si on veut résoudre en y et écrire $y = \varphi(x)$ cela est en général impossible sauf à introduire des "fonctions multiformes". Pour pallier cet inconvénient on peut imaginer de démultiplier le plan complexe en autant de feuillets que nécessaires chacun correspondant à une valeur de la fonction pour que sur l'ensemble des feuillets, φ soit une "vraie" fonction. L'ensemble des feuillets forme une surface appelée surface de Riemann de la courbe Γ considérée. Du point de vue topologique, cette surface est caractérisée par son genre, c'est-à-dire par son nombre de "trous" (le tore est une surface de genre 1, la sphère de genre 0). Le genre de la surface de Riemann ne dépend que de f. On dira donc que c'est le genre de la courbe Γ définie par f. Cette notion de genre a pu être étendue à d'autres corps que $\mathbb{C}$.

3 Généralisation de la fonction ζ

Soit K un corps, on définit pour K une fonction ζ_k de $\mathbb{C}$ dans $\mathbb{C}$ (fonction ζ de Dedekind) par :

$$\zeta_k(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

où la sommation est étendue à tous les idéaux entiers $\mathfrak{a}$ de K. On démontre qu'on a encore :

$$\zeta_k(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

où le produit est étendu à tous les idéaux premiers $\mathfrak{p}$ de K.

Malgré cette définition très générale les propriétés des fonctions ζ ainsi construites dépendent du corps K. Suivant sa nature ces fonctions sont plus ou moins simples.

4 Les Travaux d'Artin, Hasse et Weil

Dans sa thèse en 1921, Artin pris comme corps une extension de degré deux d'un corps premier $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ plus exactement il prit le corps $K_D = \mathbb{F}_p\left(x, \sqrt{D(x)}\right)$ où D(x) est un polynôme à coefficients dans $\mathbb{F}_p$.

Il démontra alors que la fonction ζ associée au corps K_D est une fonction rationnelle en p^{-s}. Artin vérifia pour de petites valeurs de p et différents choix du polynôme D que "l'hypothèse de Riemann" avait bien lieu, c'est-à-dire que sa fontion ζ qui par ailleurs vérifiait une équation fonctionnelle reliant ses valeurs en s et 1 - s, ne s'annulait que pour s de partie réelle égale à 1/2. Mais ce n'est qu'en 1936 que Hasse démontra cette conjecture.

Dans la pratique, travailler dans K_D consiste à travailler dans le corps des fonctions sur la courbe $y^2 = D(x)$. Que se passe-t-il si on prend une courbe quelconque ?

Hasse put démontrer "l'hypothèse de Riemann" dans le cas d'une courbe de genre 1, mais ce n'est qu'en 1948 que Weil acheva la démonstration pour une courbe de genre quelconque. Il se mit alors à généraliser tous ces différents résultats au cas d'une variété algébrique de dimension n quelconque. Il émit à ce propos diverses conjectures :

. La fonction ζ est rationnelle en p^s et il en donnait une expression formelle.

. La fonction ζ satisfait à une équation fonctionnelle généralisant celle obtenue dans les cas classiques.

. La fonction ζ vérifie "l'hypothèse de Riemann" sur la position de ses zéros.

5 Les résultats de Grothendieck et Deligne

Au moyen de puissants instruments de topologie algébrique (cohomologie ...) qu'il n'est pas question de présenter dans cet article (j'en serais d'ailleurs bien incapable), Grothendieck, en collaboration avec Artin, prouva les deux premières conjectures de Weil en 1963. Ce n'est qu'en 1973 que Deligne démontra la troisième conjecture. Il démontre même un peu plus puisqu'il généralise le théorème de Hadamard-de la Vallée Poussin disant que la fonction ζ n'a pas de zéro de partie réelle égal à 1.

Ces différents résultats, outre leur intérêt intrinsèque, ont des applications et des retombées importantes en théorie des nombres ; par exemple le calcul du nombre de solutions dans un corps fini d'un système d'équations polynomiales (généralisation des équations diophantiennes) ; par exemple en théorie additive des nombres ; par exemple la démonstration de la conjecture de Ramanujan-Peterson...

La médaille Fields (qui avait été attribuée en son temps à Grothendieck) ne récompense donc pas un résultat précis (encore que la démonstration de la troisième conjecture de Weil suffirait sans doute à la justifier) mais un mathématicien dont les travaux en de nombreux domaines font autorité et suscitent de nombreuses recherches. N'est-il pas aussi important de savoir poser les bonnes questions que de savoir en résoudre ?

Jean LEFORT

Bibliographie

* Borevitch et Chafarevitch. Théorie des nombres (G.V. 1967)

Traite essentiellement les corps de nombres. Très complet, on y trouve des renseignement sur les valuations, sur les entiers...

* Dieudonné. Cours de géométrie algébrique (P.U.F., 1974)

Le 1er tome est lisible et très historique.

* Dieudonné (sous la direction de). Abrégé d'histoire des mathématiques 1700-1900 (Hermann 1978)

Très complet, donne beaucoup de résultats modernes malgré sa limitation à 1900.

* Fulton. Algebraic curves (Benjamin)

Permet de comprendre ce qu'est la géométrie algébrique dans un cas particulier.

* Serre. Travaux de Pierre Deligne (La Gazette des mathématiciens , n° 11 - octobre 78)

C'est le rapport de J.-P. Serre sur les travaux de Deligne en vue de l'attribution de la médaille Fields.

* Weil. Foundations of algebraic geometry (1949)

Livre de base, très théorique et qui a un peu vieilli.