

Théorie algébrique des nombres : l'envolée

L'école allemande de la fin de XIXe siècle a fourni une pléiade de mathématiciens d'exception, en particulier en théorie algébrique des nombres, cette branche de la théorie des nombres qui s'intéresse aux polynômes et à leur racines.

Au milieu du XIXe siècle, la bataille pour la démonstration du « grand théorème de Fermat » fait rage. Gauss, Dirichet, Kummer s'y lancent et font bien des avancées. Elève de Dirichet, Dedekind complète la théorie du maître et généralise celle de Kummer en introduisant les nombres algébriques, c'est-à-dire les racines des polynômes à coefficients rationnels. Elève de Kummer, Kronecker rapproche l'analyse de l'arithmétique. Riemann, élève lui aussi de Dirichet, invente une nouvelle fonction pour étudier la répartition des nombres premiers. Hurwitz, Landau, puis au XXe siècle Siegel et Hasse, tous professeurs à Göttingen, travaillent sur des théorèmes relatifs aux nombres. Hilbert, qui s'intéresse à tous les domaines mathématiques, contribue largement au développement de cette nouvelle vision de l'arithmétique qui dépasse celle de Diophante et de Fermat. L'arithmétique est devenue « théorie des nombres » et va s'étendre aux nombres algébriques. Ainsi est née la « théorie algébrique des nombres » et son développement doit beaucoup à l'école allemande de mathématiques de la fin du XIXe siècle.

Des entiers aux polynômes

Fermat avait lancé les mathématiciens européens sur la piste de l'arithmétique en les défiant de démontrer sa conjecture – à savoir qu'il n'existe pas d'entiers x, y, z non triviaux tels que $x^n + y^n = z^n$ pour $n \geq 3$ –, devenue depuis sa démonstration par Wiles en 1994, le théorème de Fermat-Wiles.

Gauss, à l'origine de presque tous les débuts de recherches mathématiques, va permettre à d'autres mathématiciens de généraliser les propriétés des entiers à des êtres mathématiques comme les polynômes, c'est-à-dire des expressions de la forme :

$P(x) = ax^n + bx^{n-1} + cx^{n-2} + \dots + 1$ où x est « l'indéterminée » et n le degré.

La 8^{ème} section de ses Disquisitiones (vers une théorie des corps finis, trouvée dans les manuscrits de Gauss, éditée après sa mort dans ses œuvres complètes) c'est à l'origine de la plupart des recherches arithmétiques de la fin du XIXe siècle. À l'image des « entiers modulo p » (voir encadré), il y considère notamment des congruences modulo un polynôme irréductible : on dit que le polynôme $q(x)$ est congru à $r(x)$ modulo $p(x)$ si $p(x)$ divise la différence $q(x) - r(x)$, ce que les mathématiciens écrivent :

$Q(x) \equiv r(x) \pmod{p(x)} \Leftrightarrow p(x) \text{ divise } (Q(x) - r(x)).$

Ceci l'amène à travailler sur des classes de polynômes à coefficients dans le corps $\mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier.

Des polynômes aux nombres idéaux.

S'intéressant au grand théorème de Fermat, Kummer cherche à factoriser en p facteurs premiers l'expression $x^n + y^n$ où p est premier. Il introduit pour cela les racines p -ièmes de l'unité. En effet, tout comme 1 a deux racines carrées, 1 et -1 , il y a trois racines cubiques dans le corps $\mathbb{C}$ des « complexes » ... et p racines p -ièmes qui s'écriront ζ^i , où i est le nombre imaginaire $\sqrt{-1}$.

Elles sont toutes des puissances de l'une d'entre elles, ζ , et s'écriront : $1, \zeta, \zeta^2, \dots, \zeta^{p-1}$.

De tels nombres ζ sont appelés « racines primitives de l'unité ». Si p est premier, toute racine p -ième sauf 1 est racine primitive. Kummer, comme l'avait fait Lagrange avant lui, arrive à :

Il étudie alors ce qu'il nomme les entiers complexes, de la forme :

..... par analogie avec les entiers complexes de Gauss s'écrivant $a+ib$ (les a_k sont entiers). Sa démonstration du théorème de Fermat repose sur une hypothèse avancée : sur les entiers complexes, la décomposition en facteurs premiers est unique. Cauchy réfutera la preuve : l'hypothèse est fausse, en prenant le contre-exemple $p=23$. Kummer développe sa théorie des nombres idéaux en partie pour palier à cette non unicité. En ajoutant aux précédents ces nombres idéaux, la factorisation devenait unique, les lois de l'arithmétique classique redevenaient valables. Par ailleurs, la théorie de Kummer restait liée aux racines de l'unité et ne permettait pas de visée générale de certains problèmes de divisibilité. Elle inspira cependant d'autres de ses collègues.

Des nombres idéaux aux nombres algébriques

La théorie des nombres algébriques de Dedekind va remplacer la théorie des nombres idéaux de Kummer. Dedekind généralise la notion d'entiers complexes de Gauss et de Kummer : il appelle nombre algébrique un nombre complexe racine d'une équation de la forme Où les a_i sont des entiers relatifs ; si $a_0=1$, on parle d'entiers algébriques. Dedekind montre que les nombres algébriques forment un corps mais s'aperçoit qu'il n'y a pas sur ces nombres non plus unicité de la décomposition de facteurs premiers. Dedekind définit également pour un nombre algébrique α , le corps de nombres $\mathbb{Q}(\alpha)$, ensemble des nombres de la forme =0 où les a_i sont des nombres rationnels. Il développe la notion d'idéal, en hommage à la terminologie de Kummer : les multiples d'un entier k forment par exemple un idéal de $\mathbb{Z}$. le couronnement de sa théorie étant le théorème : tout idéal peut être représenté de façon unique comme un produit d'idéaux premiers. Le problème de la divisibilité des entiers algébriques est ainsi solutionné, les lois de l'arithmétique classique, exprimées pour les idéaux de l'anneau, gardent ici leur validité.

Parallèlement à Dedekind, Kronecker développe une théorie des nombres algébriques en procédant par adjonction d'indéterminées aux éléments d'un corps et rejoint Dedekind en introduisant en 1882 la notion de « système modulaire » voisine de celle idéal.

Après les travaux de Kummer, Dedekind, Kronecker, la théorie des nombres algébriques devient une théorie mathématique à part entière, autonome. Hilbert, autre grand mathématicien de cette époque, qui s'est entre autre aussi intéressé à la théorie des nombres, sera le premier à proposer une synthèse des connaissances sur les corps de nombres algébriques, dans le *Zahlbericht*(1907).

Une arithmétique des classes de congruence

L'idée vient de Gauss : on peut séparer les entiers relatifs (l'ensemble noté $\mathbb{Z}$) en classes selon leurs restes dans la division par un certain nombre p : deux entiers x et y seront dans la même classe s'ils ont même reste dans la division par p , ce qu'on écrit « x est congru à y modulo p », ou encore « $x \equiv y[p]$ ». c'est-à-dire que la différence $x-y$ est divisible par p .

Ainsi, 60 est congru à 34 modulo 13 puisque tous les deux ont pour reste 8 dans la division par 13, ce qui revient à dire que leur différence, 26, est un multiple de 13.

Comme dans la division par p , les restes ne peuvent varier que de 0 à $p-1$, il y aura p classes résiduelles modulo p , qui forment l'ensemble noté $\mathbb{Z}_p$ ou $\mathbb{Z}/p\mathbb{Z}$. Gauss va définir sur cet ensemble à p éléments une vraie arithmétique, avec opérations élémentaires (addition, multiplication), et cette invention permettra de démontrer de nombreux théorèmes.

L'ensemble $\mathbb{Z}_p$ possède des propriétés supplémentaires, plus fortes, lorsque p est un nombre

premier. En particulier, toutes les classes (sauf celle de 0) y admettent un inverse : $\mathbb{Z}P$ est alors un corps.

Reperes chronologiques

Gauss (1777-1855)

Dirichlet (1805-1859)

Kummer (1810-1893)

Kronecker (1823-1891)

Riemann 1826-1866)

Dedekind (1831-1916)

Hurwiltz (1859-1919)

Hilbert (1862-1943)

Landau (1977-1938)

Siegel (1896-1981)

Hasse (1898-1972)