LA THÉORIE DES GROUPES DE GALOIS

En 1831, un mathématicien français d'une vingtaine d'années, Évariste Galois (1811-1832), soumet à l'Académie des sciences un manuscrit sur la résolution des équations algébriques. Son manuscrit est refusé, qualifié d'inintelligible par ses examinateurs Lacroix et Poisson. Le jeune homme décède un an plus tard au cours d'un duel. Ses travaux ne seront redécouverts que dans les années 1840, par Joseph Liouville, qui les publie en 1846 dans son propre journal, intitulé *Journal de mathématiques pures et appliquées*. La théorie de Galois deviendra un élément incontournable des mathématiques modernes. De quoi s'agit-il ?

Galois a élaboré une théorie pour déterminer si une équation polynomiale de degré n à coefficients rationnels est résoluble par radicaux, c'est-à-dire à l'aide de ses coefficients et d'un nombre fini d'opérations classiques (addition, soustraction, multiplication, division et extraction de racines). Pour cela, il a associé à chaque équation un objet, qui constitue une « carte génétique » de l'équation. Cet objet est un groupe, le « groupe de l'équation » aujourd'hui baptisé « groupe de Galois ». Galois sait que si une fonction des solutions d'une équation est invariable quand on permute les solutions qu'elle renferme, elle s'exprime rationnellement à l'aide des coefficients de l'équation. Par exemple, la fonction $V(x_1, x_2)=x_1^2+x_2^2$, où x_1 et x_2 sont les solutions de l'équation du second degré $x^2+px+q=0$, est invariante par les permutations du groupe S_2, ensemble des permutations de deux éléments. Ces permutations sont l'identité, et la transposition qui échange x_1 et x_2. Pour Galois, un groupe (fini) est un ensemble où la composition de deux éléments est un élément du groupe. Cette notion n'est pas si éloignée de la conception moderne du mot groupe *(voir l'encadré page suivante)*. La fonction V s'exprime donc rationnellement à l'aide des deux coefficients p et q de l'équation. Ici, le calcul est simple : $V(x_1, x_2)=(x_1+x_2)^2-2x_1x_2$, avec $x_1+x_2=-p$ et $x_1x_2=q$.

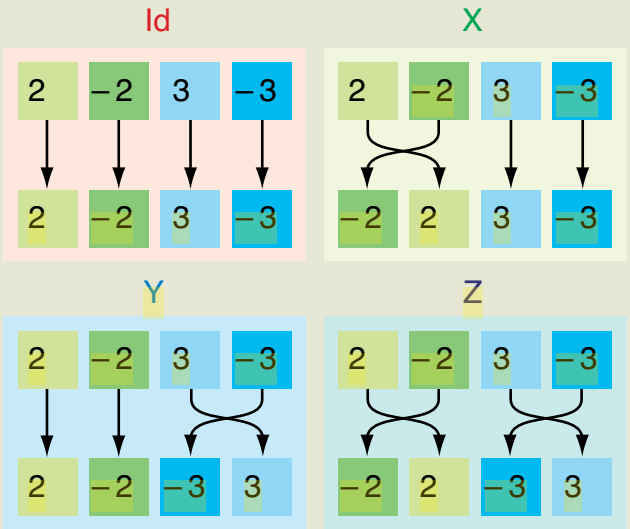
Galois étend ce résultat et démontre que toute fonction des solutions d'une équation, invariable par certaines permutations de ces solutions, mais pas toutes, s'exprime rationnellement en fonction des coefficients de l'équation.

Il démontre ensuite que les permutations des racines d'une équation qui conservent les relations rationnelles entre ces racines constituent un groupe, le groupe de Galois. Enfin, il démontre qu'à toute équation algébrique, on peut associer un tel groupe. Galois a ainsi établi une correspondance entre une fonction déterminable rationnellement et les permutations du groupe de l'équation. C'est cette correspondance entre fonctions et groupes finis, adaptée aux courbes elliptiques et aux fonctions modulaires, que Wiles utilise dans sa démonstration de la conjecture de Shimura-Taniyama-Weil. Plus précisément, il utilise la correspondance entre le groupe de Galois absolu $G_{\mathbb{Q}}$ et des sous-ensembles de points des courbes elliptiques et des fonctions modulaires *(voir l'encadré page 103)*.

Le groupe de Galois absolu réunit toutes les « cartes génétiques » des équations polynomiales à coefficients rationnels : un élément de $G_{\mathbb{Q}}$ détermine ainsi sur chaque équation une permutation particulière des racines.

Norbert Verdier, IUT de Cachan

Évariste Galois, mathématicien malheureux (1811-1832).



o	Id	X	Y	Z
Id	Id	X	Y	Z
X	X	Id	Z	Y
Y	Y	Z	Id	X
Z	Z	Y	X	Id

L'ensemble des permutations Id, X, Y, Z constitue un groupe de l'équation $x^4-5x^2+6=0$, car la composition de deux éléments donne un élément de l'ensemble (les quatre racines de l'équation sont $\pm\sqrt{2}$ et $\pm\sqrt{3}$ car l'équation s'écrit $(x^2-2)(x^2-3)=0$). En outre, en examinant la table d'opération du groupe, on remarque que l'ensemble {Id, X} est aussi un groupe : c'est un sous-groupe du groupe {Id, X, Y, Z}.

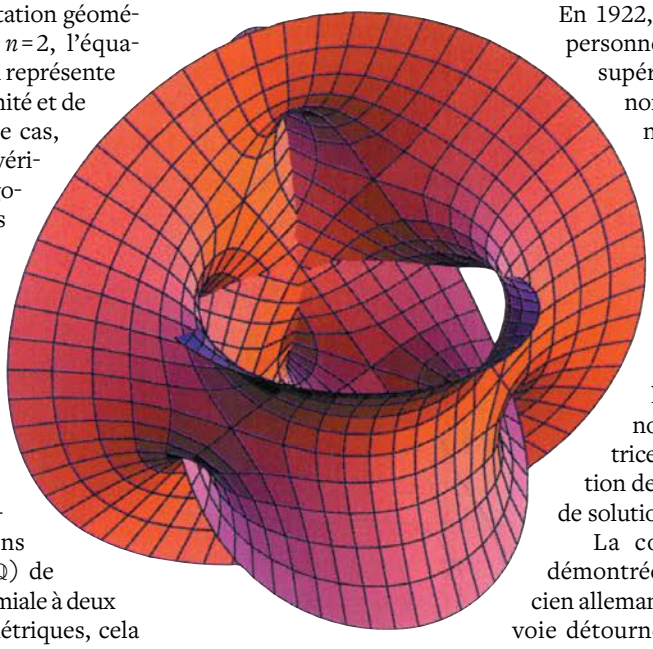
LA NOTION MODERNE DE GROUPE

La structure de groupe est centrale dans les branches les plus variées des mathématiques (groupes de Lie, géométrie algébrique, topologie algébrique et différentielle, théorie des nombres…). Un groupe est un ensemble d'éléments fermé pour une loi de composition $\times$ associative, c'est-à-dire que $(x \times y) \times z = x \times (y \times z)$ pour tous x, y, z de l'ensemble. En outre il existe un élément neutre u (unité) de l'ensemble tel que $u \times x = x \times u = x$ pour tout élément x, et chaque élément x possède un inverse x' dans l'ensemble tel que $x \times x' = x' \times x = u$. Enfin, le groupe est commutatif si pour tout couple (x, y), on a $x \times y = y \times x$. Il est aisé de vérifier que l'ensemble Z des entiers relatifs (ayant un signe) forme un groupe commutatif pour la loi de composition « addition » +; l'élément neutre est $u = 0$ et l'inverse de x est l'entier $-x$. En revanche, l'ensemble $\mathbb{N}$ des entiers naturels muni de la loi de composition + n'est pas un groupe. Cette notion abstraite de groupe fut introduite par l'Anglais Arthur Cayley en 1854.

Retour au début du XX^{e} siècle. L'examen de l'équation (1) $x^n+y^n=z^n$ montre que, pour n'importe quel n (y compris 2), lui trouver des solutions entières est équivalent à chercher des solutions rationnelles à l'équation (2) : $x^n+y^n=1$.

Quel est l'intérêt de ce décalage ? Il est avantageux de travailler sur l'équation (2) dans le corps $\mathbb{Q}$ des nombres rationnels plutôt que sur (1) dans l'anneau $\mathbb{Z}$ des entiers, car cette équation se prête à une interprétation géométrique immédiate. Ainsi, pour $n=2$, l'équation (2) devient (3) $x^2+y^2=1$, qui représente l'équation d'un cercle de rayon unité et de centre l'origine du plan. Dans ce cas, déterminer les triplets d'entiers vérifiant $x^2+y^2=z^2$ (les triplets pythagoriciens) revient à chercher les points du cercle dont les deux coordonnées sont rationnelles, ce qui est plutôt facile.

Pour $n>2$ en revanche, les courbes associées à l'équation (2) sont plus compliquées qu'un simple cercle, comme on peut déjà le voir pour $n=3$. L'énigme de Fermat devient un cas particulier du problème général de la recherche des solutions rationnelles (c'est-à-dire dans $\mathbb{Q}$) de n'importe quelle équation polynomiale à deux inconnues x, y. En termes géométriques, cela revient à déterminer les points de coordonnées rationnelles sur les courbes réelles associées à ces équations.



Surface engendrée par l'équation de Fermat $x^3+y^3=1$ quand x et y sont des variables complexes.

DES COURBES AUX SURFACES

L'intuition qui se révélera gagnante (esquissée par Euler) consiste à immerger $\mathbb{Q}$ non dans le corps $\mathbb{R}$ des nombres réels, mais dans celui des nombres complexes, $\mathbb{C}$. De cette façon, on associe non plus des courbes aux équations (2), mais des surfaces fermées et orientables nommées surfaces de Riemann. Ces surfaces furent classifiées au XIX^{e} siècle : une surface fermée, orientable et lisse est équivalente, du point de vue topologique, à une sphère avec un certain nombre d'anses (*voir la figure page 100*). Le nombre d'anses est le genre de la surface. Lorsque la surface est associée à une équation algébrique, le genre est aussi appelé genre de l'équation. Plus le genre est élevé, plus la géométrie de la surface est compliquée et plus il est difficile de trouver les points rationnels de celle-ci. Pour l'équation (2), le genre est donné par la formule $(n-1)(n-2)/2$.

Quand le genre est nul ($n=1$ ou 2), notre problème est simple. Comme nous l'avons vu dans le cas de l'équation (3), si l'équation admet une solution rationnelle, alors elle en admet un nombre infini (il existe bien sûr des équations de genre nul qui n'admettent aucune solution rationnelle, par exemple $x^2+y^2=-1$). L'affaire se complique dès lors qu'on considère une équation de genre 1 (c'est-à-dire pour $n=3$). Comme dans le cas précédent, une surface peut ne pas avoir de points rationnels. Mais si elle en a, alors ils sont en nombre fini ou, s'ils sont en nombre infini, ils peuvent être obtenus de manière canonique à partir d'un nombre fini de points rationnels appelés générateurs, comme le démontra le mathématicien anglais Louis Mordell.

En 1922, le même Mordell constate que personne n'a trouvé de courbe de genre supérieur ou égal à 2 possédant un nombre infini de points à coordonnées rationnelles. Il fait de cette constatation empirique une conjecture : aucune équation de genre supérieur ou égal à deux ne peut avoir un nombre infini de solutions « génératrices ». Dans notre contexte, la conjecture de Mordell implique que pour n supérieur ou égal à quatre, l'équation (2) a au plus un nombre fini de solutions « génératrices » et, par conséquent, que l'équation de Fermat a au plus un nombre fini de solutions primitives.

La conjecture de Mordell ne fut démontrée qu'en 1983 par le mathématicien allemand Gerd Faltings, au moyen d'une voie détournée. Qu'on en juge. En 1962, le mathématicien Igor Chafarevich avait proposé la conjecture suivante, qui prit ensuite son nom : sous certaines conditions, on peut reconstruire les solutions entières (c'est-à-dire dans $\mathbb{Z}$) d'une équation à partir de l'étude de cette équation modulo p, pour divers nombres premiers p.

En 1968, A. N. Parshin démontra que la conjecture de Chafarevich impliquait celle de Mordell. Et en 1983, Faltings s'attaqua avec succès à la conjecture de Chafarevich, prouvant comme corollaire celle de Mordell ! La