

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 ?

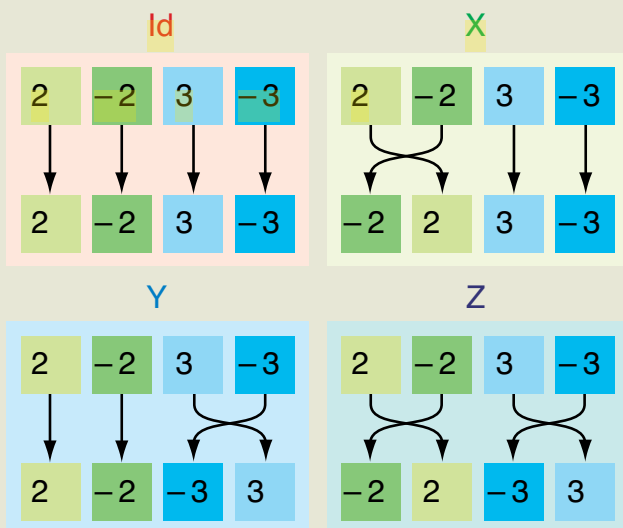
Galois a élaboré une théorie pour déterminer si une équation polynomiale de degré n à coefficients rationnels est résoluble par radicaux, c'est-à-dire à l'aide de ses coefficients et d'un nombre fini d'opérations classiques (addition, soustraction, multiplication, division et extraction de racines). 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.



Évariste Galois, mathématicien malheureux (1811-1832).

Norbert Verdier, IUT de Cachan



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}.