***Star Trek, Doctor Who, Les Simpsons*... ces trois séries ont en commun d'avoir mis à l'honneur lors d'au moins un épisode l'un des plus célèbres théorèmes mathématiques.** Quel résultat a-t-il mérité une telle récupération populaire? Le dernier théorème de Fermat, selon lequel $x^n+y^n=z^n$ n'admet pas de solution quel que soit $n>2$. L'énoncé est simple, la démonstration, beaucoup moins.

Tout commence en 1637 quand Pierre de Fermat, magistrat et mathématicien, note dans la marge de son édition des *Arithmétiques*, de Diophante: «Au contraire, il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré: j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir.» On peut douter qu'il l'ait vraiment démontré, car ce n'est qu'en 1995 qu'un autre mathématicien, l'anglais Andrew Wiles, a pu en venir à bout à l'aide d'outils mathématiques très complexes. Ce fut l'épilogue d'une longue histoire riche en détours et en rebondissements.

Remontons le cours de l'histoire, et revenons au début du XIXe siècle. À cette époque, les mathématiciens savent qu'il suffit de prouver le théorème pour les nombres premiers pour qu'il soit valide quel que soit $n$. Grâce à Ernst Kummer (1810-1893), ils savent en outre que le théorème est vrai pour les nombres premiers $p$ qu'il a qualifiés de «réguliers» (une certaine propriété liée aux racines du polynôme $x^p-1$ doit être vérifiée), et qu'il suffit donc de le démontrer pour les nombres premiers «irréguliers».

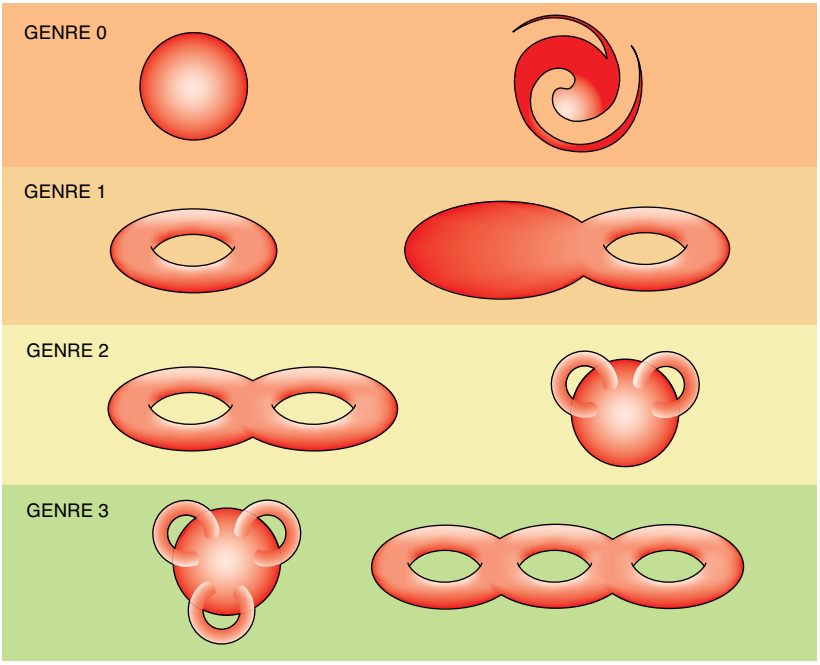
Toutefois, deux problèmes persistent. D'abord, il n'est pas facile de déterminer si un nombre premier est «régulier». Kummer a trouvé un critère permettant de déduire cette caractéristique, mais plus le nombre premier est grand, plus ce critère est lourd à déterminer. Il s'en est toutefois servi pour démontrer le théorème de Fermat pour tous les nombres premiers réguliers inférieurs à 100. Il est en revanche difficile d'aller plus loin à la main.

Ensuite, Kummer espérait qu'une infinité de nombres $p$ étaient réguliers, faisant de ceux qui ne le sont pas des exceptions. Or, en 1915, le mathématicien danois Johan Jensen montre qu'il existe une infinité de nombres irréguliers.

## UNE GOUTTE DANS L'OCÉAN

Avec l'avènement de l'informatique, le seuil des nombres premiers réguliers connus croît progressivement: les recherches sur ordinateur montrent que la plupart des nombres premiers inférieurs à un certain seuil sont réguliers et que les exceptions jouissent d'une propriété supplémentaire, une sorte de régularité faible qui fait que le théorème de Fermat s'applique aussi à ces entiers. Cela réduit d'autant le nombre de cas à traiter au-dessous d'un certain seuil pour démontrer la validité du théorème de Fermat sous ce seuil. Ainsi, en 1983, le théorème est vérifié pour $n$ inférieur à 1 million, puis, en 1992, pour $n$ inférieur à 4 millions.

Ces imposants résultats ne sont cependant qu'une goutte dans l'océan infini des nombres, et le problème de la démonstration du théorème dans sa généralité reste entier.




Dans le corps $\mathbb{C}$ des nombres complexes, l'équation de Fermat engendre une surface fermée et orientable, caractérisée par son genre, c'est-à-dire le nombre de trous qu'elle possède. Deux surfaces qui présentent le même nombre de trous sont topologiquement équivalentes: elles sont de genre égal. Si deux surfaces ont le même genre, on passe de l'une à l'autre à l'aide d'une succession de transformations continues comme les déformations d'une surface en caoutchouc.

# 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 $x_1x_2 = q$.

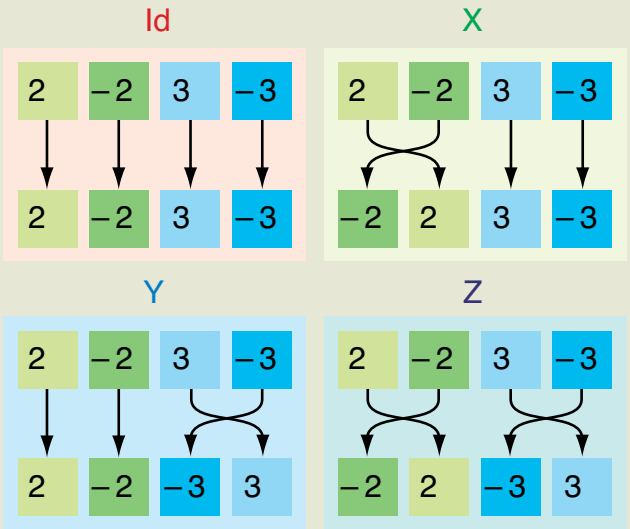
Galois étend ce résultat et démontre que toute fonction des solutions d'une équation, invariable par certaines permutations de ces solutions, mais pas toutes, s'exprime rationnellement en fonction des coefficients de l'équation.

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}.