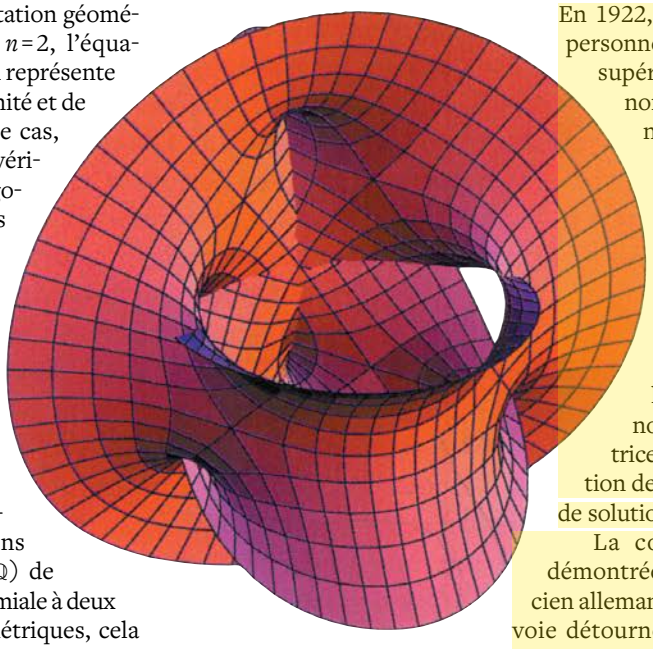
LA NOTION MODERNE DE GROUPE

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.

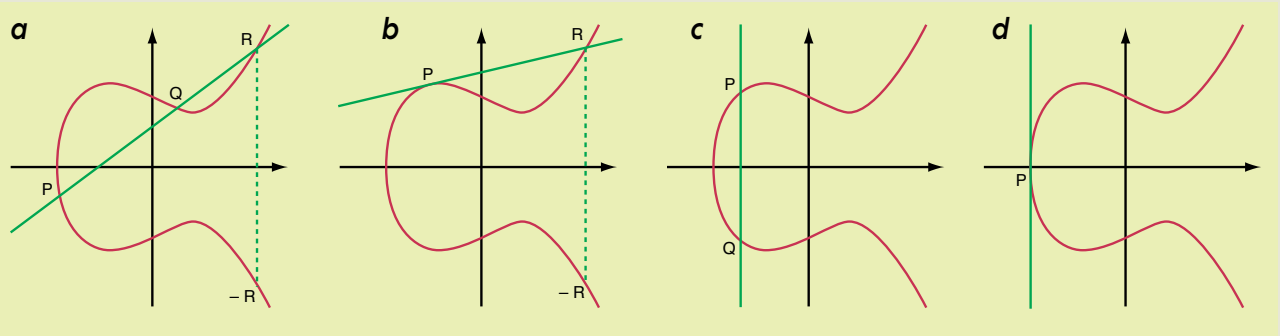
La conjecture de Mordell ne fut démontrée qu'en 1983 par le mathématicien allemand Gerd Faltings, au moyen d'une voie détournée. Qu'on en juge. En 1962, le mathématicien Igor Chafarevich avait proposé la conjecture suivante, qui prit ensuite son nom : sous certaines conditions, on peut reconstruire les 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

COURBES ELLIPTIQUES ET LOI DE GROUPE

Les courbes elliptiques sont un des outils clés de la démonstration du théorème de Fermat par Andrew Wiles. Voyons de plus près leurs caractéristiques. Une courbe elliptique E est une courbe de genre 1 dont l'équation se ramène à : $y^2+axy+by=x^3+cx^2+dx+e$, où a, b, c, d et e sont des entiers. Une telle équation définit une courbe de genre 1 si elle n'a pas de points singuliers, c'est-à-dire si les dérivées partielles par rapport à x et à y de l'équation ne s'annulent pas en même temps (ce qui impose une condition sur les coefficients). Un point de la courbe E est n'importe quel couple de nombres complexes vérifiant l'équation associée. Si certains points ont des coordonnées réelles (respectivement rationnels), on dit qu'ils sont réels (rationnels). Une propriété cruciale des courbes elliptiques est la suivante : l'ensemble de leurs points forme un groupe commutatif, et il en est de même pour l'ensemble de leurs points réels et celui de leurs points rationnels. En d'autres termes, l'« addition » ou la « soustraction » de deux points de la courbe donne un point de la courbe. Qu'est-ce que l'addition de deux points ? Considérons par exemple la courbe elliptique d'équation : $y^2=x^3-x-1$, et deux points distincts P et Q sur cette courbe *(voir la figure)*. La droite qui les joint recoupe en général la courbe en un troisième point R. On définit la somme des points P et Q comme étant le point symétrique de R par rapport à l'axe des abscisses. Si P=Q, on utilise la tangente à la courbe : le point P+P=2P est le symétrique par rapport à l'axe des abscisses du point d'intersection de la tangente en P avec la courbe. L'opposé d'un point P, noté – P, est le symétrique de P par rapport à l'axe des abscisses. Et l'élément neutre du groupe commutatif est le point , point de rencontre des verticales à l'infini. Ainsi, la somme de P et de son opposé est bien nulle, puisque la droite qui joint ces points est verticale. Autre propriété importante des courbes elliptiques : elles présentent des points de torsion, c'est-à-dire des points dont un multiple entier est nul. Pour un entier $n>2$, l'ensemble E[n] des points à coordonnées complexes de la courbe E dont le n-ième multiple est 0 (les points de n-torsion), associés au point ∞, l'élément neutre, constitue un groupe commutatif dit de n-torsion.
On montre, à partir de l'expression des coordonnées de la somme de plusieurs points, que les abscisses x des points de E[n] vérifient une équation polynomiale à coefficients rationnels. Or, par définition, le groupe de Galois absolu conserve les relations algébriques, en particulier l'équation vérifiée par les abscisses des points de E[n], et celle vérifiée par leurs ordonnées – l'équation de E. Par conséquent, il permute les points de E[n] entre eux. C'est grâce à cette propriété que l'on peut établir une correspondance entre le groupe E[n] et le groupe de Galois absolu. On a ainsi construit une représentation galoisienne des courbes elliptiques. Andrew Wiles démontra la conjecture de Shimura-Taniyama-Weil en établissant une correspondance similaire entre le groupe de Galois absolu et les fonctions modulaires, et en montrant que ces deux représentations galoisiennes sont isomorphes.

Catherine Goldstein, institut de mathématiques de Jussieu-Paris-Rive-gauche.



Différents cas d'addition de points P et Q sur la courbe elliptique d'équation $y^2=x^3-x-1$, représentée dans le plan réel. Quand P et Q sont distincts, P+Q=–R (*a*). Quand P=Q, P+P=–R (*b*). Quand P et Q ont la même abscisse (*c*), leur somme est égale au point ∞ (là où les droites verticales se rencontrent à l'infini). Quand P et Q sont confondus en un point de tangente verticale, P+P vaut le point ∞ (*d*).

démonstration de Faltings exploite la résolution, due à Pierre Deligne en 1978, de la conjecture de Weil. André Weil avait proposé en 1949 un analogue pour les corps finis de la célèbre hypothèse de Riemann, formulée à l'origine pour le corps $\mathbb{C}$ des nombres complexes (*voir L'hypothèse qui valait un million, par P. Meier, page 68*).

DÉTOUR PAR LE JAPON

Ainsi aucune équation du type (2) ne peut avoir un nombre infini de solutions génératrices pour $n>2$. Peu après, en 1985, en utilisant le résultat de Faltings, Andrew Granville et Roger Heath-Brown démontrèrent que le nombre de solutions des équations (2), s'il en existe, est une fonction décroissante de l'entier n. Ce point ne résout cependant pas l'énigme de Fermat. Il suffit en effet d'une seule solution rationnelle de l'équation (2) pour obtenir une solution entière de l'équation (1) et donc un nombre infini de solutions de celle-ci.

La solution de l'énigme de Fermat fut finalement l'œuvre d'un descendant de la vieille Angleterre émigré aux États-Unis, Andrew Wiles. Le chemin tortueux de la découverte passa par le Japon tumultueux de l'après-guerre. Revenons au cas $n=2$ du théorème, exprimé au moyen de l'équation (3) : $x^2+y^2=1$. On peut paramétriser x et y par respectivement les fonctions cosinus et sinus, qui satisfont la relation : (4) $\cos^2\alpha+\sin^2\alpha=1$.

Résoudre l'équation de Fermat pour $n=2$, c'est-à-dire déterminer les triplets de Pythagore, >