

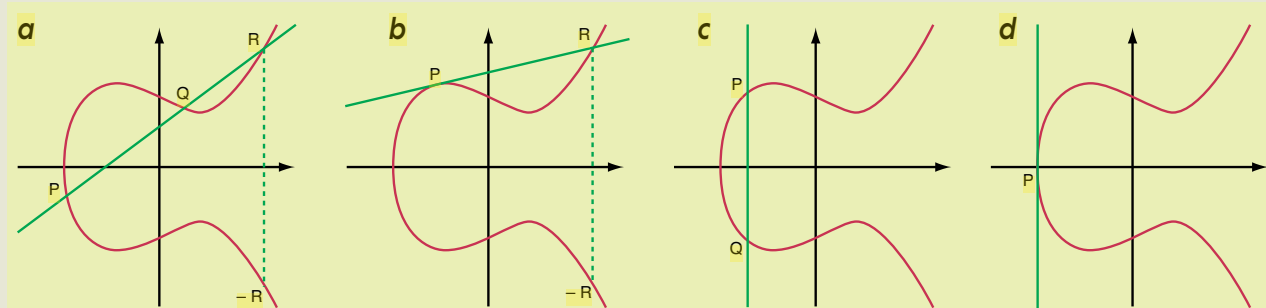
COURBES ELLIPTIQUES ET LOI DE GROUPE

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 d'ordre n .

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, >