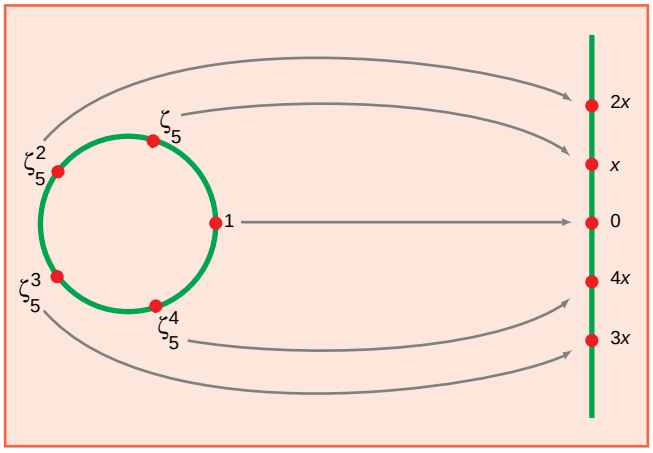
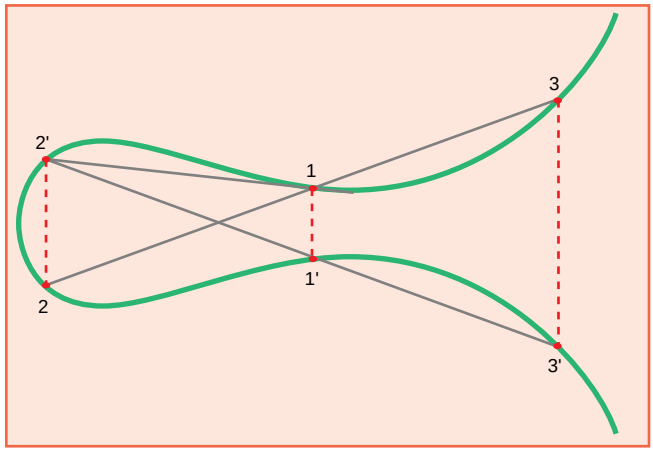


2. LES CINQ POINTS SUR LE CERCLE représentent les points de 5-division du groupe *T*. Les flèches envoient ces cinq points sur une droite dont les points sont repérés par les entiers modulo 5. Au produit de ζ^2 par ζ^4 sur le cercle, donnant le point ζ, correspond l'addition de 2*x* à 4*x*, soit 6*x* modulo 5, ou encore *x*. Pour démontrer le théorème de Fermat d'exposant *p* (ici 5), on utilise les points de *p*-division d'une courbe elliptique liée à une solution hypothétique de l'équation de Fermat.



3. À PARTIR DE DEUX POINTS 1 ET 2 de coordonnées rationnelles sur une courbe elliptique, on détermine un point 3, intersection de la droite passant par 1 et 2 avec la courbe, dont les coordonnées sont également rationnelles. Le point 3', symétrique du point 3, est le composé des points 1 et 2, et cette règle de composition définit une structure de groupe. La composition d'un point, 3 par exemple, avec le point à l'infini revient à prendre le point symétrique de 3' par rapport à l'axe de symétrie de la courbe : on retrouve le point 3 lui-même.

entre ses sommets, les transformations qui conservent l'objet et sa structure, les automorphismes, sont l'identité et la symétrie évidente.

Ainsi, lorsque l'objet est un anneau, la structure est formée par l'addition et la multiplication ; les automorphismes de l'anneau sont les transformations qui font correspondre à un élément de l'anneau un autre élément de l'anneau, en respectant ces deux lois.

Les nombres algébriques sont les nombres complexes qui sont solutions d'une équation polynomiale à coefficients fractionnaires : l'équation $3x^2 - 4$ a pour solutions $2\sqrt{3}/3$ et $-2\sqrt{3}/3$; ces nombres sont algébriques. Il est patent que les nombres rationnels sont algébriques. Le nombre π n'est solution d'aucune équation polynomiale à coefficients fractionnaires non nuls, il n'est donc pas algébrique ; on dit qu'il est transcendant.

Les mathématiciens ont démontré que les nombres algébriques constituent un corps (la somme et le produit de deux nombres algébriques sont des nombres algébriques).

Prenons par exemple un nombre complexe *z* que l'on obtient par des additions, soustractions, multiplications et divisions des nombres rationnels et du nombre complexe $\zeta_5 = e^{2i\pi/5}$. Le nombre *z* est algébrique parce que le nombre ζ_5 lui-même est algébrique. En effet, ζ_5 vérifie l'équation polynomiale à coefficients rationnels : $x^4 + x^3 + x^2 + x + 1 = 0$. Cette équation ne peut être décomposée en produits de polynômes à coefficients rationnels.

L'ensemble des nombres obtenus de la même manière que *z* forme le corps cyclotomique d'ordre 5 (ou corps de la division du cercle en cinq parties égales). C'est un sous-corps du corps de tous les nombres algébriques.

Dans notre théorie, ce corps possède un groupe d'automorphismes, le groupe des transformations de ce corps en lui-même, qui respectent l'addition et la multiplication. Ce groupe est appelé le groupe de Galois de notre corps cyclotomique.

Les automorphismes du corps des rationnels se réduisent à l'identité : ils ne sont pas très intéressants. Par chance, ζ_5 appartient à la famille des quatre frères jumeaux $e^{2i\pi/5}$ $e^{4i\pi/5}$ $e^{6i\pi/5}$ $e^{8i\pi/5}$ qui vérifient l'équation précédente. Le groupe de Galois de notre corps cyclotomique a donc quatre éléments.

La méthode utilisée par Kummer pour étudier l'équation de Fermat de degré 5 est déjà un magnifique exemple de l'utilisation de certains nombres cyclotomiques.

Le groupe des automorphismes de l'énorme corps de tous les nombres algébriques est appelé le groupe de Galois absolu. Malheureusement on ne connaît guère de caractéristiques de ce groupe de Galois absolu. C'est un objet aussi fondamental que mystérieux, mais il n'en sert pas moins de leitmotiv à la grande symphonie orchestrée par A. Wiles. Je vous entends vous exclamer : si le groupe de Galois absolu reste une notion métaphysique, comment en dire des choses positives, falsifiables ? En reprenant l'exemple ci-dessus, on voit que tout automorphisme appartenant au groupe de Galois absolu se reflète dans le groupe de Galois du corps cyclotomique bâti à partir du nombre ζ_5.

En réalité, ce que l'on fait avec le nombre 5 peut être fait avec tout entier positif *n*. Les points ζ_n ont leur image sur le cercle unité du plan complexe et ce cercle est muni naturellement d'une loi de groupe commutatif par la multiplication d'un nombre complexe. Ce groupe des nombres complexes de module 1 est désigné par *T*.

Le point ζ_5 est un élément de *T* tel que $\zeta_5^5 = 1$: on dit que c'est un point de 5-division de *T*. L'ensemble des éléments ζ qui vérifient cette condition forme un sous-groupe cyclique d'ordre 5 de *T*. Ce que l'on a étudié plus haut était l'action du groupe de Galois absolu sur ce sous-groupe. Ce sous-groupe étant isomorphe à une droite *(voir la figure 2)* sur le corps à cinq éléments F_5, on a ainsi effectué une représentation linéaire du groupe de Galois absolu sur une droite.

Les représentations du groupe de Galois absolu ont toujours fasciné J.-P. Serre ; dans les années 1970, il s'intéressait à un type analogue de représentations : celles du groupe de Galois absolu agissant sur le groupe des points de *p*-division d'une courbe elliptique dont les coefficients de l'équation sont rationnels. Nous examinerons plus loin ces courbes elliptiques.

Les points du cercle T sont paramétrés par une variable réelle modulo

2π (un angle), les points d'une courbe elliptique sont paramétrés par une variable complexe modulo deux périodes. Il en résulte que les points de p-division ne sont plus sur une droite mais dans un plan. Mais abordons, comme nous l'avions promis, les courbes elliptiques.

L'introduction des courbes elliptiques

Prenons une courbe elliptique représentée par la cubique d'équation : $y^2 = x^3 + a_2x^2 + a_4x + a_6$. La courbe est définie sur les rationnels si a_2, a_4 et a_6 sont rationnels. De plus il ne faut pas que le second membre de l'équation ait une racine double ; dans le cas contraire, la cubique possède un point multiple et n'est pas une courbe elliptique.

Comme les points de la courbe sont paramétrés par une variable complexe modulo deux périodes, ces points forment un groupe commutatif dont l'élément nul est le point de paramètre 0. Habituellement on choisit le paramétrage pour que l'élément nul du groupe soit le point à l'infini de la courbe. Les points rationnels de la courbe elliptique sont ceux dont les coordonnées sont rationnelles. Un théorème d'Abel explique comment construire le composé de deux points, et les points rationnels forment un groupe pour cette loi de composition *(voir la figure 3)*.

Pour les amateurs de courbes elliptiques, un des thèmes d'étude des années 1960 était une conjecture de Beppo Levi. Cette conjecture affirme, entre autres, que pour toutes les courbes elliptiques définies sur les rationnels, il existe un majorant de l'ordre des points rationnels. L'ordre d'un point P étant le plus petit entier n non nul tel que P composé avec lui-même n fois soit nul.

Les points rationnels d'ordre $2p^2$ doivent être particulièrement fascinants puisque B.A. Demjanenko et moi-même avons étudié ces points entre 1965 et 1970. À notre grand étonnement l'existence de ces points entraînait celle d'une solution non triviale de l'équation de Fermat d'exposant p.

En 1969, j'ai pensé à renverser l'approche : j'ai essayé de démontrer que, si l'équation de Fermat avait un triplet solution a,b,c, tous non nuls, alors la courbe elliptique dont l'équation est $Y^2 = X(X - a^p)(X + b^p)$ aurait des points d'ordre p intéressants. Si le nombre c n'apparaît pas dans cette équation c'est qu'il se déduit des deux autres par l'équation de Fermat $a^p + b^p = c^p$. La courbe sera désignée dans la suite par $E(A,B,C)$, avec $A = a^p$, $B = b^p$ et $C = -c^p$: certains auteurs la désignent sous le nom de «Courbe de Frey». Remarquons que l'on ne peut donner d'exemple de courbe $E(A,B,C)$ correspondant à une solution non triviale de l'équation de Fermat puisqu'il n'en existe pas. On peut toutefois en donner pour des équations voisines comme $x^p + y^p = 2z^p$.

Nous sommes ainsi passés du problème de Fermat de degré p à un problème sur les points d'ordre p de la courbe elliptique $E(A,B,C)$. Là encore, les mathématiciens ont élargi le problème : au point (a,b,c) ils ont fait correspondre une courbe elliptique $E(A,B,C)$, et l'on est passé ainsi d'un objet algébrique, un point $(u,v) = (a/c, b/c)$ de la courbe $u^p + v^p = 1$ à un objet «transcendant», la courbe $E(A,B,C)$.

Le passage à une dimension supérieure pour démontrer un théorème avait été utilisé avec profit par Desargues *(voir la figure 1)*. Cette démonstration fameuse par sa simplicité illustre l'intérêt de changer de «point de vue». Toutefois, une théorie plus générale que la théorie précédente n'est intéressante que si elle donne des résultats imprévus : dans le cas contraire, elle est stérile et sans portée.

Les courbes elliptiques éliminent de façon particulièrement élégante les solutions triviales de l'équation de Fermat : en effet, la courbe $E(A,B,C)$

LES FORMES MODULAIRES

La fonction thêta définie pour $|q| < 1$ par :

$$\theta(q) = \sum q^{n^2}$$

a été étudiée par Euler et Jacobi.
Si l'on pose $q(z) = e^{\pi i z}$, avec $z = x + iy$, $y > 0$, on obtient les équations fonctionnelles :

(1) $$\theta(q(z)) = \theta(q(z + 2))$$

(2) $$\theta(q(-1/z)) = (z/i)^{1/2}\, \theta(q(z))$$

La série de Dirichlet qui est associée à θ n'est autre que la célèbre fonction dzéta de Riemann :

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \quad \text{pour } \mathrm{Re}(s) > 1$$

Euler a établi que cette fonction possède un "produit eulérien", c'est-à-dire un produit ne portant que sur les nombres premiers :

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p} (1 - p^{-s})^{-1}$$

L'équation fonctionnelle de la fonction thêta conduit à celle de ζ, et le produit eulérien de ζ conduit à de nouvelles propriétés de θ !
Le 24 avril 1828, Jacobi découvrit l'identité :

$$\left(\sum q^{n^2}\right)^4 = 1 + 8 \sum A(m) z^m, \text{ où } A(m) = \sum d, \; d \text{ divisant } m \text{ et } \not\equiv 0 \bmod 4$$

qui lui permit de donner instantanément le nombre de représentations d'un entier positif comme somme de quatre carrés !
L'équation *(2)* entraîne l'équation fonctionnelle :

$$\frac{\Gamma(s/2)}{\pi^{s/2}}\, \zeta(s) = \frac{\Gamma((1 - s)/2)}{\pi^{((1 - s)/2)}}\, \zeta(1 - s)$$

publiée par B. Riemann en 1859.
La célèbre "hypothèse de Riemann" affirme que les zéros de $\zeta(s)$, qui ne sont pas -2, -4, -6, etc., se trouvent sur l'axe de symétrie de cette équation (la droite correspondant à la partie réelle de s égale à 1/2) : c'est une des grandes conjectures que notre époque lègue au prochain siècle.