tains cas impossibles se trouveraient possibles».

En théorie des nombres, les mathématiciens varient la structure : au lieu d'examiner les solutions entières des équations, ils examinent les solutions modulo *k*. Ils regroupent dans une même classe les nombres qui ont le même reste après division par *k*. Ainsi la classe des nombres pairs est constituée par les nombres égaux à zéro modulo *2*.

Les entiers modulo *k* ont une structure d'anneau, c'est-à-dire qu'ils sont munis d'une addition et d'une multiplication reflétant l'addition et la multiplication ordinaires. Lorsque *k* est égal à 2 les restes sont 0 et 1, et l'on a :

+	0	1
0	0	1
1	1	0

ADDITION

×	0	1
0	0	0
1	0	1

MULTIPLICATION

En utilisant la loi de réciprocité quadratique due à Euler, Legendre et Gauss, le mathématicien Gérard Terjanian a su faire resplendir, en 1977, les méthodes traditionnelles d'un éclat particulier.

Il a démontré que, si *n* est égal à 2*p*, où *p* est un nombre premier impair, alors l'un des trois nombres *x*, *y*, *z* vérifiant l'équation de Fermat pour l'exposant 2*p*, est égal à zéro modulo *2p*, c'est-à-dire est divisible par *n*. C'était la première fois qu'un résultat aussi général était obtenu pour ce qu'il est convenu d'appeler le «premier cas du théorème de Fermat».

Dans les méthodes classiques, mais pas dans la méthode de A. Wiles, la démonstration de Fermat comporte toujours deux étapes. La première, que l'on appelle le «premier cas» est la plus facile ; elle consiste à démontrer, lorsque l'exposant est un nombre premier *p*, que *p* divise l'un des trois nombres *x*, *y*, *z* vérifiant l'équation de Fermat.

Donnons un exemple d'une telle démonstration. Par exemple, si *p* est égal à 3, on examine les solutions modulo 9 de l'équation $x^3 + y^3 = z^3$; on voit alors facilement que 3 divise *x*, *y* ou *z*.

En présentant les choses négativement (raisonnement par l'absurde), on prouverait le premier cas de Fermat en disant que si *p* ne divise pas *xyz*, alors l'équation $x^p + y^p = z^p$ est impossible. Comme zéro est divisible par tous les nombres, y compris *p*, les solutions triviales sont éliminées d'emblée. Cet avantage se retrouvera dans la méthode de Andrew Wiles.

Dans le second cas, beaucoup plus difficile, il s'agit de démontrer que, non seulement *p* divise *xyz*, mais que *toutes* les puissances de *p* divisent *xyz*, ce qui implique que *xyz* est égal à 0 (un nombre non nul n'étant pas indéfiniment divisible).

Fermat avait trouvé une «route tout à fait singulière» pour résoudre le second cas et d'autres problèmes de cette nature : la «descente infinie» (voir *De Diophante à Fermat*, par Christian Houzel, *Pour la Science*, janvier 1996).

La descente infinie est un ingrédient essentiel de toutes les preuves classiques du «second cas» du théorème de Fermat, alors qu'elle est inutile pour le «premier cas», comme nous l'avons vu. Ici une véritable mutation va se produire : la méthode de A. Wiles traitera d'un seul coup de baguette magique les premier et deuxième cas, et ceci pour tous les exposants à la fois.

Finalement, en 1985,au moment où l'Histoire semblait hésiter entre tradition et idées à venir, trois hardis mousquetaires, Adleman, Fouvry et Heath-Brown essayèrent de régler définitivement le sort du premier cas. S'ils échouèrent, du moins échouèrent-ils avec panache : ils démontrèrent le premier cas pour une infinité d'exposants premiers. Ce résultat fit beaucoup de bruit, mais les mathématiciens savaient qu'il s'agissait d'un combat d'arrière-garde et que les batailles futures allaient se livrer sur d'autres fronts.

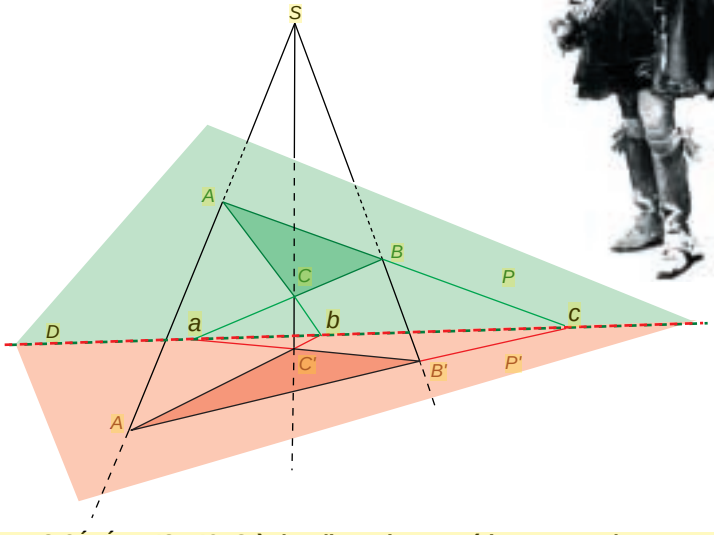
Le groupe de Galois absolu

À l'époque de Kummer déjà, les nombres algébriques avaient fait leur apparition dans l'étude du théorème de Fermat. Nous allons définir ces nombres mystérieux qui vont jouer un rôle essentiel.

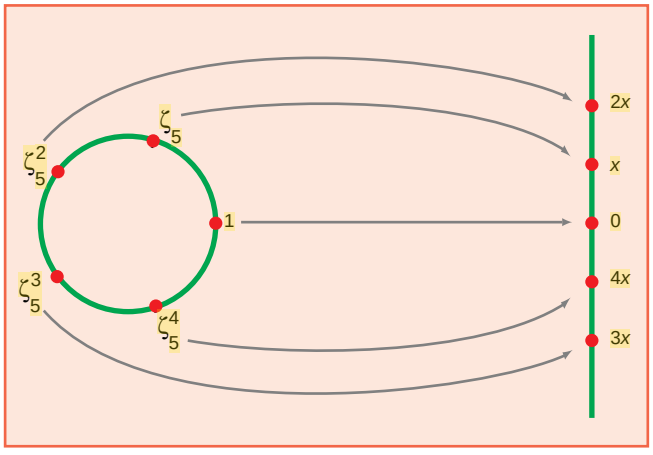
Un titre plus romantique pour ce sujet pourrait être «le corps des nombres algébriques et les représentations de son âme». En effet, la philosophie qui sous-tend ce type de question a d'abord été rêvée par Évariste Galois à la prison de Sainte-Pélagie (en 1831) avant de trouver sa consécration officielle dans le programme d'Erlangen de Félix Klein (en 1872). Cette philosophie consiste à attacher, à tout objet mathématique muni d'une structure, le groupe des transformations de cet objet qui respectent cette structure. On appelle ce groupe, le groupe des automorphismes de l'objet.

Si l'objet est l'ensemble des trois sommets d'un triangle isocèle (et non équilatéral) et sa structure la distance

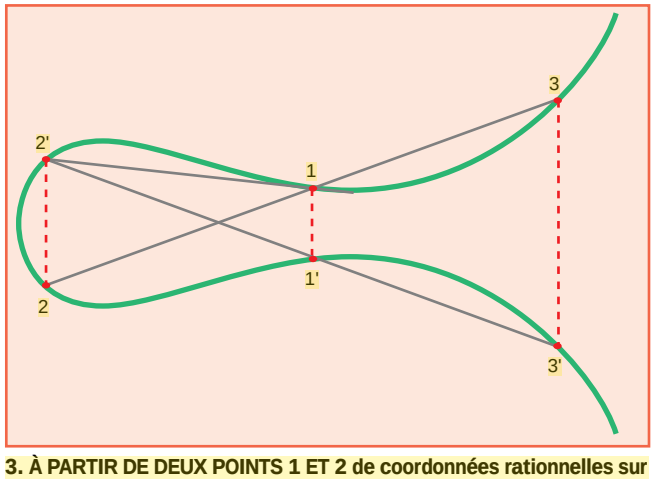
Desargues (1591-1661)



1. LES GÉNÉRALISATIONS à des dimensions supérieures sont des moyens puissants de démonstration. Ainsi des propriétés de figures planes ne sont que les ombres de propriétés de figures dans l'espace. Si *SAA', SBB', SCC'* sont alignés, alors *a, b, c* le sont aussi. Ce théorème, dû à Desargues, est démontré facilement en donnant du relief à la figure : celle-ci est considérée comme la projection plane de deux triangles en perspective dans l'espace, les triangles *ABC* et *A'B'C'*, situés dans deux plans distincts, *P* et *P'*. Alors les points *a,b,c* sur la droite d'intersection *D* des plans *P* et *P'*, sont alignés.



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