Tutorat 1

Fonctions de Weierstrass

Frédéric Chevy – chevy@lkb.ens.fr
http://www.phys.ens.fr/∼chevy/Tutorat/Tut.html

1 Notion de fonction elliptique.

Les fonctions elliptiques jouent un rôle important dans plusieurs domaines des mathématiques. Elles ont été introduites pour la première dans le calcul d'intégrales (et plus particulièrement le calcul du périmètre d'une ellipse, d'où leur nom), mais on s'est vite aperçu que leurs propriétés pouvaient être appliquées en théorie des nombres : on les utilise ainsi dans certains protocoles cryptographiques, et c'est leurs propriétés qui sont à l'origine de la démonstration du théorème de Fermat par A. Wiles. Les fonctions elliptiques sont aussi appelées fonctions doublement périodiques. En effet, soient ω_1 et ω_2 deux nombres complexes linéairement indépendants. On note $\Omega = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ le sous-groupe additif de $\mathbb{C}$ engendré par les ω_i, et on s'intéresse aux fonctions méromorphes possédant Ω comme groupe des périodes. On dit qu'une fonction f est elliptique si elle est méromorphe sur $\mathbb{C}$, sans singularité essentielle et admet Ω comme groupe de période. Pour en savoir plus, on trouvera en ligne le traité de Appell sur les fonctions elliptiques à l'adresse

`http://gallica.bnf.fr/ark:/12148/bpt6k995607.notice`

1. Rappeler le théorème de Liouville. Montrer que si f ne possède pas de pôle, alors f est constante.
2. On appelle parallélogramme de période un parallélogramme de côtés parallèles à ω_1 et ω_2. Calculer $\oint_\gamma f$, où γ est un parallélogramme de période. En déduire la somme des résidus de f. Montrer en particulier qu'une fonction elliptique possédant un unique pôle par période ne peut exister si ce dernier est d'ordre 1.
3. Relier les pôles de f'/f aux pôles et zéros de f. Calculer $\oint f'/f$ sur un parallélogramme des périodes et en déduire une relation entre le nombre de pôles et de zéros d'une fonction elliptique.
4. (a) On considère un lacet fermé $\gamma(t)$ avec $\gamma(0) = \gamma(1)$. Que peut-on dire de

$$\frac{1}{2i\pi}\int_0^1 \frac{\dot\gamma}{\gamma}dt,$$

lorsque l'on intègre sur le lacet γ. Comment se nomme cette quantité ?

(b) Soit $\gamma(t)$ un chemin tel que $\gamma(1)-\gamma(0)=\omega_i$. Que dire du chemin $f(\gamma(t))$, lorsque f est une fonction elliptique. En déduire que si I est un côté du parallélogramme des périodes,

$$\frac{1}{2i\pi}\int_I \frac{f'(z)}{f(z)}dz$$

est entier.

(c) À l'aide des questions précédentes, montrer que sur un parallélogramme des périodes

$$\frac{1}{2i\pi}\oint z\frac{f'(z)}{f(z)}dz = n_1\omega_1 + n_2\omega_2,$$

avec $(n_1, n_2) \in \mathbb{Z}^2$.

(d) En déduire que sur le parallélogramme de période centré sur l'origine, les barycentres des pôles et des zéros de f sont confondus.

2 Fonction ζ et $\mathfrak{p}$ de Weierstrass. Décomposition des fonctions elliptiques en éléments simples.

1. *Question préliminaire.* Soit Ω le sous-groupe additif de $\mathbb{C}$ engendré par ω_1 et ω_2. Montrer que la série

$$\sum_{\omega\in\Omega^*}\frac{1}{|\omega|^3}$$

est convergente.
Indication : on considérera l'ensemble des $\omega = t_1\omega_1+t_2\omega_2$ avec $(t_1,t_2)\in\mathbb{Z}^2$ et $\sup|t_i| = n$ et on sommera sur n.

2. Déduire de la question précédente que la série

$$\zeta(z) = \frac{1}{z} + \sum_{\omega\in\Omega^*}\left(\frac{1}{z-\omega}+\frac{1}{\omega}+\frac{z}{\omega^2}\right)$$

est normalement convergente sur tout compact de $\mathbb{C}$
Ω. Préciser la parité de ζ.

3. On pose $\mathfrak{p}(z) = -\zeta'(z)$. Écrire $\mathfrak{p}$ et $\mathfrak{p}'$ sous forme d'une série. En déduire que $\mathfrak{p}'$ possède Ω comme groupe de période.

4. Intégrer la condition de périodicité de $\mathfrak{p}'$ et en déduire que pour tout $\omega\in\Omega$ il existe un nombre complexe c_ω tel que pour tout $z\in\mathbb{C}$, $\mathfrak{p}(z+\omega) = \mathfrak{p}(z)+c_\omega$.

5. En considérant le cas particulier $z = -\omega/2$, montrer que $\mathfrak{p}$ est périodique.

6. Montrer que $\mathfrak{p}^{(k)}$ est une fonction elliptique et qu'en $z=0$, $\mathfrak{p}^{(k)}(z) = (-1)^k\frac{(k+1)!}{z^{k+1}}+O(1)$.

7. *Pseudo-périodicité de la fonction* ζ. On pose $\eta_i = \zeta(\omega_i/2)$ et on suppose que la base $\{\omega_1,\omega_2\}$ est directe.

(a) En vous inspirant des questions précédentes, montrer que pour $\omega \in \Omega$, $\zeta(z+\omega_i) = \zeta(z) + 2\eta_i$ (on dit que ζ est pseudo-périodique).

(b) Montrer que $\oint_\gamma \zeta(z)dz = 2\eta_1\omega_2 - 2\eta_2\omega_1$, lorsque γ est la frontière d'un parallélogramme des périodes parcourues dans le sens direct.

(c) En déduire la relation de Legendre

$$\eta_1\omega_2 - \eta_2\omega_1 = i\pi.$$

(d) Soit $A_{i=1..n}$ et $z_{i=1..n}$ $2n$ nombres complexes tels que $\sum_i A_i = 0$. Montrer que $\sum_i A_i\zeta(z - z_i)$ est une fonction elliptique.

8. *Décomposition d'une fonction elliptique en éléments simples.* Soit f une fonction elliptique possédant des pôles d'ordre $k_{i=1..n}$ en $z_{i=1..n}$. Montrer que l'on peut écrire f sous la forme

$$f(z) = \sum_{i=1}^{n}\sum_{p=1}^{k_i} A_{i,p}\zeta^{(p)}(z - z_i).$$

Indication : on pourra utiliser le théorème de Liouville.

3 Fonctions elliptiques et équations algébriques

Dans cette partie, on cherche à montrer que la fonction $\mathfrak{p}$ permet de paramétrer une courbe elliptique (cf. article).

1. Développer $\mathfrak{p}'$ en série de Laurent au voisinage de zéro et montrer que

$$\mathfrak{p}'^2 = \frac{4}{z^6} - \frac{8a_2}{z^2} - 16a_4 + o(1),$$

avec

$$\begin{aligned} a_2 &= 3\sum_{\omega\neq 0}\frac{1}{\omega^4} \\ a_4 &= 5\sum_{\omega\neq 0}\frac{1}{\omega^6}. \end{aligned}$$

2. Montrer de même que

$$\mathfrak{p}^3 = \frac{1}{z^6} + \frac{3a_2}{z^2} + 3a_4 + o(1).$$

3. À partir des questions précédentes, montrer que

$$\mathfrak{p}'^2 - 4\mathfrak{p}^3 + 20a_2\mathfrak{p} + 28a_4 = o(1).$$

4. En déduire une paramétrisation de la courbe elliptique définie par l'équation

$$y^2 = 4x^3 - 20a_2x - 28a_4, \tag{1}$$

et déduire une méthode de calcul de l'intégrale

$$\int \frac{dx}{\sqrt{4x^3 - 20a_2x - 28a_4}}.$$

5. Soient deux points P_1 et P_2 de la courbe algébrique $\mathcal{C}$ d'équation (1) définis par $P_i = (x_i, y_i) = (\mathfrak{p}(u_i), \mathfrak{p}(u_i'))$. On cherche à montrer que la droite passant par les P_i d'équation $y = ax+b$ coupe une troisième fois la courbe $\mathcal{C}$ (cf. article ci-joint). Pour cela, on considère la fonction Φ définie par

$$\Phi(z) = \mathfrak{p}'(z) - (a\mathfrak{p}(z) + b).$$

Montrer que Φ est elliptique. Quels sont ses pôles ? En déduire le nombre de zéros de Φ. Calculer le barycentre des pôles de Φ et en déduire que $\mathcal{C}$ coupe la droite (P_1, P_2) au point $Q(P_1, P_2)$ de coordonnées $(\mathfrak{p}(z_1 + z_2), -\mathfrak{p}'(z_1 + z_2))$.

6. Déduire des questions précédentes le théorème d'addition

$$\mathfrak{p}(z_1 + z_2) = -\mathfrak{p}(z_1) - \mathfrak{p}(z_2) + \frac{1}{4}\left(\frac{\mathfrak{p}'(z_1) - \mathfrak{p}'(z_2)}{\mathfrak{p}(z_1) - \mathfrak{p}(z_2)}\right).$$

En déduire que si P_1 et P_2 sont à coordonnées rationnelles, Q l'est aussi.

Fermat enfin démontré

YVES HELLEGOUARCH

La démonstration du théorème de Fermat par Andrew Wiles s'appuie sur un faisceau de méthodes mathématiques qui bouleverse le paysage de la théorie des nombres.

Vers la fin de sa vie, Pierre de Fermat (1601-1665), écrivait, dans ses *Défis aux mathématiciens* : «On sait qu'Archimède n'a pas dédaigné de travailler sur des propositions de Conon, qui étaient vraies, mais non prouvées, et qu'il a su les munir de démonstrations d'une haute subtilité. Pourquoi n'espérerais-je pas un semblable secours de vos éminents correspondants, pourquoi, Conon français, ne trouverais-je pas des Archimède anglais?»

Le 23 juin 1993, plus de 300 ans après la note marginale de Fermat, Andrew Wiles, professeur à Princeton (États-Unis), mais fils d'un professeur de théologie anglais, pensait pouvoir annoncer à l'Institut Newton, à Cambridge (Grande-Bretagne) qu'une des propositions que Fermat nous avait léguées – peut-être involontairement, car on peut se demander si la remarque qu'il avait faite en marge d'un exemplaire des *Arithmétiques* de Diophante était destinée à être publiée – était désormais munie d'une démonstration d'une haute subtilité et d'une éblouissante beauté. Il semblait que Fermat avait trouvé son Archimède anglais.

Pourtant, un des artifices d'Andrew Wiles était encore en porte-à-faux, et ce n'est que le 19 septembre 1994, à l'issue d'un labeur intense et grâce au renfort de son collègue Richard Taylor de l'Université de Cambridge, que la magnifique cathédrale édifiée par A. Wiles était enfin libérée de tout échafaudage et s'élevait triomphante dans le ciel mathématique, symbole d'un labeur de trois siècles (ce qui n'est pas exceptionnellement long pour une cathédrale). Cette dernière hésitation du destin illustre bien les mystères et les surprises recelées par le «dernier théorème de Fermat».

Position du problème

L'article de Christian Houzel du mois dernier nous a rappelé l'Histoire de la recherche des triplets pythagoriciens, les entiers x, y et z, solutions en nombres entiers de l'équation $x^2 + y^2 = z^2$ *(1)*. Ces triplets pythagoriciens sont en correspondance avec les points du cercle centré sur l'origine, de rayon unité et d'équation $u^2 + v^2 = 1$, points dont les deux coordonnées sont rationnelles, c'est-à-dire de la forme a/b où a et b sont entiers. Il suffit, pour s'en convaincre, de diviser les deux membres de l'équation *(1)* par z^2.

La résolution de cette équation *(1)*, dite diophantienne, est connue depuis fort longtemps. Pour les exposants supérieurs à 2, les équations de la forme $x^n + y^n = z^n$, la solution est radicalement différente. L'assertion de Fermat est que, pour les valeurs de l'exposant n supérieures à 2, les seules solutions entières sont «triviales» : l'un des trois nombres entiers est nul (par exemple, $x = 0$ et $y = z$), ce que l'on exprime en notant que le produit xyz est alors égal à zéro.

Revenons à l'interprétation géométrique : les courbes représentant l'équation $u^n + v^n = 1$ appartiennent à deux familles : une première famille où l'exposant est pair (n est égal à $2p$), et la seconde où l'exposant est impair (n est égal à $2p + 1$). Le cas n égal à 4 a été résolu par Fermat lui-même. Le cas où n est égal à $2p$ avec p impair résulte du cas où n est impair. En effet, en posant $u' = u^2$ et $v' = v^2$ et en remplaçant dans l'équation, on voit qu'il ne reste plus qu'à traiter le cas impair.

On peut même se limiter au cas où n est premier (et évidemment différent de 2), bien que la spécification que le nombre p doive être premier semble très restrictive. En fait cette limitation de la portée du théorème est trompeuse : si l'équation de Fermat pour le nombre p premier n'a pas de solution, alors comme $(x)^{kp}$ est égal à $(x^k)^p$ la solution n'existe pour aucun multiple de p.

Dans le cas où p est premier impair, la courbe $u^p + v^p = 1$ possède trois points rationnels triviaux, le point $(u,v) = (1,0)$, le point $(u,v) = (0,1)$, et le point à l'infini de la courbe, lequel correspond à la solution $(x,y,z) = (1,-1,0)$ de l'équation diophantienne $x^p + y^p = z^p$. L'assertion de Fermat revient à dire que si p est premier et différent de 2, la courbe $u^p + v^p = 1$ n'admet pas d'autre point rationnel : il faut démontrer qu'il n'y a que *trois* points rationnels sur la courbe.

Les derniers résultats classiques

Lorsqu'ils sont bloqués dans leurs recherches, les mathématiciens ont une stratégie particulière : ils étudient des variations du problème qu'ils présentent sous des formes différentes. Le grand mathématicien Niels Henrik Abel écrivait que l'on devait donner à un problème d'impossibilité «une forme telle qu'il soit toujours possible de le résoudre, ce que l'on peut toujours faire... Au lieu de demander une relation dont on ne sait pas si elle existe ou non, il faut (se) demander si une telle relation est en effet possible». On en déduit alors les limites de possibilité du problème original.

C'est ainsi que les algébristes italiens du XVI^e siècle ont introduits les nombres «imaginaires» pour étudier les solutions réelles des équations algébriques. Pragmatique, Newton écrivait : «il faut bien que dans les équations, il y ait des racines impossibles (entendez «imaginaires») sans quoi, dans les problèmes (physiques), cer-

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.

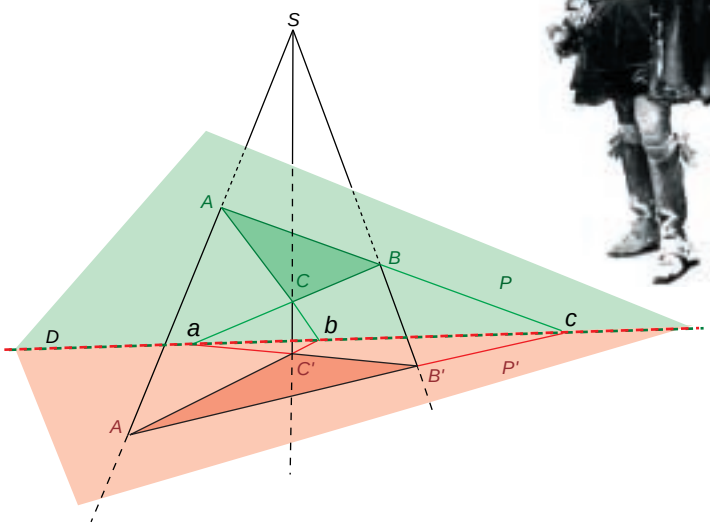
Le groupe de Galois absolu

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.

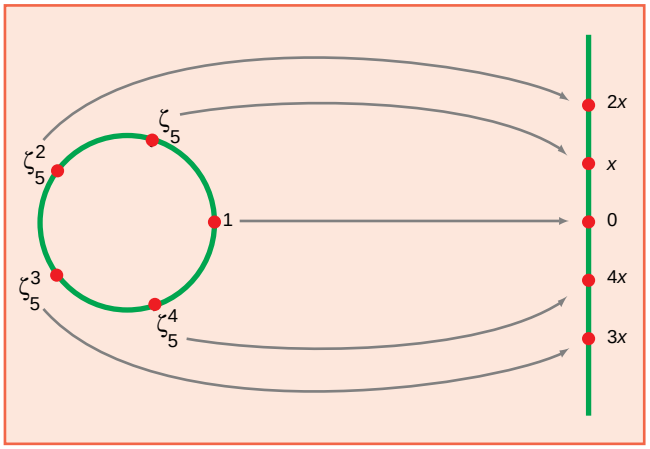
Un titre plus romantique pour ce sujet pourrait être «le corps des nombres algébriques et les représentations de son âme». En effet, la philosophie qui sous-tend ce type de question a d'abord été rêvée par Évariste Galois à la prison de Sainte-Pélagie (en 1831) avant de trouver sa consécration officielle 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

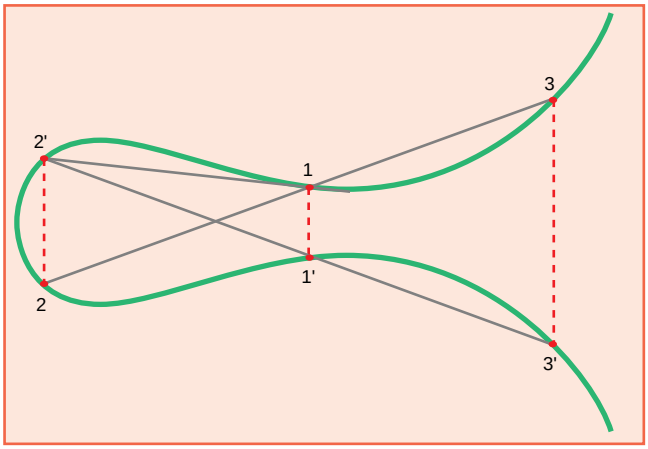
Desargues (1591-1661)



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

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.

FORMES MODULAIRES ET COURBES ELLIPTIQUES

La théorie d' Eichler-Shimura associe à la forme modulaire f :

$$f = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2$$

la courbe elliptique $y^2 - y = x^3 - x^2$.
Ceci signifie qu'en écrivant :

$$f = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + \ldots = \sum a_n q^n,$$

le nombre des points modulo p de cette courbe (y compris le "point à l'infini") est égal à $p + 1 - a_p$ (à condition que p ne divise pas 11).

Pour l premier, différent de 11, l'opérateur de Hecke T_l est défini par :

$$T_l \left(\sum a_n q^n \right) = \sum a_{ln} q^n + l \sum a_n q^{ln}$$

On vérifie que

$$T_l (f) = a_l f,$$

ce qui signifie que f est un vecteur propre de l'opérateur T_l.
La propriété de f qui lui vaut le qualificatif de "modulaire" est l'équation fonctionnelle suivante :

$$f [\exp (a\tau + b/c\tau + d)] = (c\tau + d)^2 f [\exp (\tau)],$$

où $\exp (\tau) = e^{2i\pi\tau}$, τ est un nombre complexe dont la partie imaginaire est positive, $(a,b\ ;\ c,d)$ est une matrice de quatre entiers, telle que 11 divise c et $ad - bc = 1$ (elle n'est pas évidente !).

admet un point double si et seulement si le polynôme $X(X - A)(X + B)$ admet une racine double, c'est-à-dire si et seulement si $ABC = (abc)^p = 0$.

Le reste du programme consistait à voir ce que l'on pouvait savoir des point d'ordre p de la courbe $E(A,B,C)$. J'ai constaté, en 1969, que leurs coordonnées engendraient un corps algébrique qui ressemblait beaucoup au corps cyclotomique engendré par ζ_p. Les courbes $E(A,B,C)$ ainsi associées aux solutions hypothétiques non triviales de l'équation de Fermat fourniraient, à l'aide de leurs points de p-division, des représentations du groupe de Galois absolu qui sont trop belles pour exister.

Dès leur naissance, on soupçonnait que les courbes $E(A,B,C)$ étaient des juments de Roland (dans Roland Furieux, la jument de Roland possède toute les qualités sauf l'existence). Mais comment le prouver?

C'est alors que Gerhard Frey est intervenu en 1985 : dans un manuscrit non publié intitulé «Modular Elliptic Curves and Fermat's Conjecture», il conjecturait que les courbes $E(A,B,C)$ ne pouvaient pas satisfaire la conjecture de Taniyama Weil : décidément l'Histoire aime les marges!

Les formes modulaires

On m'a rapporté une boutade du grand mathématicien M. Eichler : il aurait dit qu'il n'y avait que cinq opérations fondamentales en arithmétique : l'addition, la soustraction, la multiplication, la division et... les formes modulaires.

Les formes modulaires sont des fonctions de la variable complexe vérifiant des équations fonctionnelles *(voir l'encadré de la page 95)*. On en trouve des vestiges fragmentaires dans l'*Ars Conjectandi* de Jacques Bernoulli (1713), puis quelques beaux spécimens, dont la fonction θ dans Euler (1748), dans l'*Introductio in Analysis Infinitorum*, où apparaissent également des séries de Dirichlet et où l'on trouve aussi l'expression sous forme de produit eulérien de la fonction ζ de Riemann. On reste pantois devant la boîte de Pandore ouverte par Euler. Son *Algèbre* fourmille aussi d'équations diophantiennes, de courbes et d'intégrales elliptiques.

Peut-être est-ce dans Euler que le mathématicien allemand E. Hecke a fait ses achats. Il a relié l'équation fonctionnelle et le développement en produit de la fonction ζ de Riemann, à d'étranges propriétés de la fonction θ. Ses études joueront un rôle crucial dans la démonstration du théorème de Fermat-Wiles.

Les formes modulaires se comportent comme des organismes, leurs propriétés étant liées de manière stricte et harmonieuse par l'action d'un groupe. Celles qui nous intéressent ici sont vecteurs propres d'opérateurs très importants ici, les opérateurs de Hecke *(voir l'encadré ci-contre)*.

La conjecture de Taniyama-Weil

Depuis les années 1950, on savait associer à une courbe elliptique une série de Dirichlet, que l'on appelait la fonction L de cette courbe elliptique et qui recelait de nombreuses informations sur les points rationnels de cette courbe. Hecke avait montré, par ailleurs, comment associer à certaines séries de Dirichlet des formes modulaires de telle sorte que si les premières possèdent un produit eulérien (un produit sur les nombres premiers), les secondes sont vecteurs propres des opérateurs de Hecke. Toutefois les informations sur les fonctions L étaient trop fragmentaires pour démontrer dans le cas général l'existence de la forme modulaire.

En 1955, la voix de Taniyama s'éleva dans le désert pour annoncer que toute courbe elliptique devait provenir d'une forme modulaire. Cette prophétie, prématurée et vague, ne suscita guère d'intérêt à l'époque...

Il est bon de s'arrêter ici pour évoquer des questions de style. Un des thèmes récurrents de notre histoire est que la contribution des mathématiciens français est marquée de positivisme. Le philosophe Auguste Comte, pape du positivisme au XIX^e siècle, voyait dans le développement historique de la science trois stades successifs : le stade théologique, le stade métaphysique, et le stade positif. Dans ce dernier stade seulement la théorie est vérifiable, on dirait aujourd'hui falsifiable selon Popper. La théorie doit être suffisamment précise pour être mise en défaut si elle est imparfaite.

C'est en ce sens qu'André Weil a apporté une contribution essentielle à la conjecture de Taniyama. En s'appuyant sur la théorie d'Eichler Shimura, il a su préciser comment on devait chercher la forme modulaire associée à une courbe elliptique.

La scène était dressée pour le spectacle, mais le temps semblait avoir sus-

pendu son vol. On ne savait que faire des courbes elliptiques $E(A,B,C)$ que l'on pouvait associer à une hypothétique solution non triviale de l'équation de Fermat.

L'explosion de 1986 et le théorème de Wiles

On a dit que le coup de baguette magique fut donné en 1985 par G. Frey, alors professeur à l'Université de Sarrebruck. G. Frey conjecturait que nos courbes $E(A,B,C)$ devaient contredire la conjecture de Taniyama, et, merveille des merveilles, la communauté mathématique le crut ! Jean-Pierre Serre, d'ordinaire si prudent, tira le «coup de feu qui fit le tour du monde» en publiant de profondes conjectures dont découlait le théorème de Fermat. Peu de temps après, en 1987, B. Mazur et K. Ribet prouvèrent ces conjectures pour la représentation hypothétique du groupe de Galois absolu qui serait liée à une solution non triviale de l'équation de Fermat, mais à une condition : il fallait que la courbe $E(A,B,C)$ vérifie la conjecture de Taniyama.

Stimulé par le théorème de Ribet, le mathématicien britannique Andrew Wiles s'embarqua seul pour un long voyage sur des «océans étranges de pensée».

La navigation fut rude, et ce n'est qu'en 1991 que quelques oiseaux dans le ciel signalèrent la proximité d'une terre. En 1992, il pensait arriver près du but, et le 21 juin 1993, à l'Institut Newton, il annonça que le théorème de Fermat était démontré.

Las, l'annonce était prématurée, et les oiseaux disparurent de l'horizon. Un autre mathématicien aurait sans doute abandonné, mais A. Wiles n'écouta que son courage et son collègue R. Taylor ; celui-ci l'incitait à revenir sur sa route. C'est alors que, le 19 septembre 1994, il vit en un éclair la solution tant cherchée : un procédé découvert par Ehud de Shalit ouvrait un chemin plus direct vers la conjecture de Taniyama pour les courbes $E(A,B,C)$.

Un chef-d'œuvre est né et un mythe est mort : le théorème de Fermat est enfin démontré. De plus, le travail d'Andrew Wiles ouvre la voie à un vaste continent de recherches futures où de nombreuses conjectures restent à prouver.

Par ailleurs, la liste des équations diophantiennes abordables par la méthode des courbes $E(A,B,C)$ est loin d'être close. Pourtant les solutions d'une équation aussi voisine du théorème classique, que $x^n + y^n = 2z^n$ ne peuvent être étudiées directement par cette méthode puisque cette équation possède la solution non triviale (1,1,1). Fermat n'est sans doute pas aussi mort qu'on le suppose, et sa note marginale suscitera peut-être d'autres découvertes.

À ce stade du panorama et après deux articles portant sur le sujet, le lecteur a une idée sur le comment du théorème de Fermat. Le pourquoi de ces recherches peut lui sembler énigmatique : il nous semble que cette question ne peut être examinée en termes logiques et que le pourquoi des mathématiques reste et restera un choix artistique. Le mathématicien Emil Artin exprime avec force ce point de vue : «Nous pensons tous que les mathématiques sont un art... Certes les mathématiques sont logiques : chaque conclusion est tirée des résultats qui précédent. Cependant la totalité de l'affaire, l'œuvre d'art véritable, n'est pas linéaire ; et, ce qui est bien pire, sa perception ne peut être qu'instantanée. Nous avons tous éprouvé, en de rares occasions, une impression d'exaltation en réalisant que nous avions permis à nos auditeurs de voir, l'espace d'une seconde, l'architecture complète d'une question, et toutes ses ramifications.»

LES DIFFÉRENTES ROUTES EMPRUNTÉES DEPUIS FERMAT

LA ROUTE DES PIÉTONS

Cette route a été empruntée par Fermat lui-même pour l'exposant 4, puis par Lamé et Lebesgue pour l'exposant 7.
On se ramène à l'impossibilité de la résolution en nombres entiers des équations $t^2 = r^4 + 4s^4$ lorsque n est égal à 4, et $t^2 = r^4 - 3/4r^2s^2 + 1/7s^4$, lorsque n est égal à 7 (rst différent de zéro) et on procède par descente infinie.

LES FORMES QUADRATIQUES

On peut penser que, pour les exposants p premiers impairs, Fermat associait à son équation la forme quadratique $X^2 + (-1)^{(p+1)/2}pY^2$. C'est du moins ainsi que procédèrent Euler pour p égal à 3, puis Legendre et Dirichlet pour p égal à 5.

LES EXTENSIONS CYCLOTOMIQUES

Depuis De Moivre au XVIIIe siècle, on sait factoriser $x^p + y^p$ en produit de facteurs du premier degré en x et y, et cela conduit à considérer l'ensemble des nombres déduits par additions, soustractions et multiplications de $\zeta_p = e^{2i\pi/p}$, c'est-à-dire l'anneau des entiers cyclotomiques. C'est ainsi que Kummer parvint à démontrer l'assertion de Fermat pour tous les nombres premiers "réguliers". Malheureusement on ne sait pas démontrer qu'il existe une infinité de tels nombres.

L'APPROCHE ELLIPTIQUE

Elle est beaucoup plus récente que les précédentes (26 ans) et fait l'objet de cet article.

REMARQUES

1) Les trois premières méthodes font usage de la descente infinie pour prouver le second cas (défini dans l'article).
2) Une forme quadratique apparaît dans la route des piétons pour l'exposant 7.
3) Le nombre quadratique $((-1)^{(p-1)/2}p)^{1/2}$ apparaît implicitement dans la seconde méthode : il appartient à l'anneau des entiers cyclotomiques.
4) Finalement le corps des nombres cyclotomiques est contenu dans le corps engendré par les coordonnées des points de p-division de la courbe $E(A,B,C)$.

Yves HELLEGOUARCH est professeur de mathématiques à l'Université de Caen.

Catherine GOLDSTEIN, *Un théorème de Fermat et ses lecteurs*, Presses Universitaires de Vincennes, 1995.

Grand théorème de Fermat, in *Quadrature*, n°22, été 95.

Séminaire Bourbaki, Exposés de Jean-Pierre Serre et Joseph Oesterlé. Juin 1995.

Yves HELLEGOUARCH, *Points d'ordre $2p^h$ sur les courbes elliptiques*, in *Acta Arithmetica XXVI*, 1975.

K.A. RIBET, *Galois Representations and Modular Forms, in Bulletin of the American Society*, Octobre 1995.