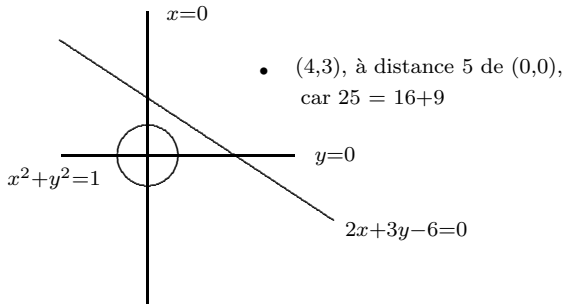
Algèbre et géométrie

La mathématique est une science cumulative. Ce que nos prédécesseurs ont découvert il y a 4000 ans _ par exemple, comment résoudre une équation du second degré _ nous reste cher, et ce qui pour les grecs était une démonstration en reste une pour nous.

"Science" n'est peut être pas le mot juste. S'il n'était péjoratif, je préférerais le mot "métaphysique". En mathématique, le critère de validité n'est pas l'expérience, mais la construction d'une démonstration, et les objets étudiés ne sont pas de ce monde: que les physiciens nous apprennent que l'espace où nous vivons n'est pas celui d'Euclide, mais est régi par la relativité générale, n'a rien à voir avec la vérité de la géométrie euclidienne; le mathématicien dira seulement que l'espace où nous vivons n'en est pas un modèle (du moins lorsque la précision requise est celle nécessaire, par exemple, aux GPS).

Les objets qu'étudie le mathématicien ont une histoire, et on peut souvent les rattacher à des idées anciennes et devenues familières. Une familiarité trompeuse, car ces notions anciennes, celle de droite par exemple, ont été maintes fois revisitées, et c'est cette multitude de points de vue, la plupart non familiers, qui fait leur force. C'est néanmoins par ce biais que je tenterai de donner une idée de ce qu'est la géométrie algébrique. C'est à elle que la plupart de mes travaux se rattachent. Il serait trop long et technique de les détailler; mon but ici est de peindre le paysage où ils s'inscrivent.

Nous sommes habitués aux graphiques, où un point du plan, rapporté à deux axes perpendiculaires, est repéré par deux nombres, et où une courbe représente une relation entre ces nombres, par exemple l'évolution d'une grandeur (température, cours de bourse, ...) avec le temps. L'usage systématique de ces "coordonnées cartésiennes" remonte à P. de Fermat (1601–1665) et R. Descartes (1596–1650). Si x et y sont deux nombres, nous dirons "point (x, y)" pour le point de coordonnées x et y. Les points (x, y) tels que x et y vérifient une équation du premier degré, par exemple $2x + 3y - 6 = 0$, sont les points d'une droite. De là le jargon "équation linéaire" pour ce type d'équation. D'après le théorème de Pythagore, le carré de la distance du point (x, y) à l'origine $(0, 0)$ est x^2+y^2. Les points tels que $x^2+y^2 = 1$ forment donc la circonférence de rayon 1 de centre l'origine.



De façon analogue, un point de l'espace, rapporté à trois axes perpendiculaires, est repéré par trois nombres, un plan correspond à une relation linéaire (= de degré 1) entre ces nombres, ...

C'est là le début d'un dictionnaire entre figures géométriques et expressions algébriques. Il permet d'appliquer aux unes l'intuition, très différente, que nous avons des autres, et d'étendre ces intuitions. Ainsi, un algébriste considérant des paires, ou des triples de nombres, n'aura aucun scrupule à considérer des quadruples ou plus généralement des systèmes de n nombres, quel que soit l'entier n. Passant au langage géométrique, il appellera point de l'espace à n dimensions un tel n^{uple}, et hyperplan l'ensemble des $(x_1, \ldots, x_n)$ vérifiant une relation linéaire. "Raisonnant juste sur des figures fausses", il pourra s'inspirer de ce qu'il voit dans le plan ou dans l'espace pour étudier, par exemple, les systèmes d'équations linéaires.

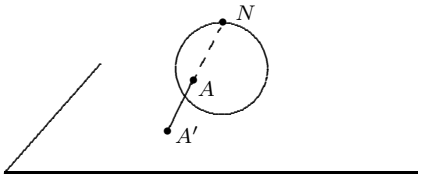
Point technique: le plan ou l'espace projectif est déduit du plan ou de l'espace euclidien en ajoutant à chaque droite un point "à l'infini", deux droites ayant le même point à l'infini si et seulement si elles sont parallèles. Il a pour source historique l'étude de la perspective, où deux droites parallèles ont pour image dans le tableau deux droites qui convergent vers un même point. Ci-dessous, c'est souvent dans le cadre "projectif" que je devrais en fait me placer.

Le va et vient entre algèbre et géométrie suggère aussi d'utiliser d'autres "systèmes de nombres" (jargon correct: corps commutatifs) que celui des nombres, dit réels, dont nous avons l'habitude, tout en gardant le langage géométrique, et l'intuition qu'il supporte. Voici des exemples. L'essentiel pour l'algèbre est qu'on dispose des 4 opérations: addition, soustraction, multiplication et division.

Les *nombres complexes* s'écrivent $a + b\sqrt{-1}$, avec a et b réels, et se manipulent comme suggéré par cette notation. Ils ont la vertu qu'une équation $z^n + az^{n-1} + \cdots + c = 0$ à coefficients $a, \ldots, c$ complexes admet toujours une solution z complexe ("théorème fondamental

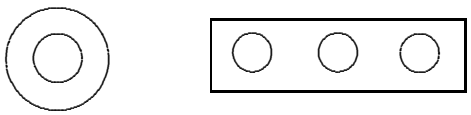
de l'algèbre"). Si on coupe la circonférence $x^2 + y^2 = 1$ par la droite $y = b$, on a 2, 1 ou 0 points d'intersection selon la valeur de b. Ce sont les points (x, b) avec $x^2 = 1 - b^2$. Si on permet à x d'être un nombre complexe, cette équation a toujours 2 solutions (exception: le cas de $x^2 = 0$, qui correspond aux tangentes $y = 1$ et $y = -1$, et où il y a intérêt à compter 2 fois l'unique solution $x = 0$). Plus généralement, dans le plan complexe, i.e. quand on permet aux coordonnées x, y d'être des nombres complexes, une droite intersecte presque toujours une circonférence en 2 points. Toute exception disparaît dans le plan projectif complexe, si on compte double les points de tangence. Bien d'autres énoncés se simplifient dans le complexe, et géométrie algébrique a souvent signifié géométrie algébrique complexe. En première approximation, celle-ci est l'étude des ensembles de points $(z_1, \ldots, z_n)$ solutions complexes d'un système d'équation polynômiales, ou des variantes dans un espace projectif. Un tel ensemble de points est ce qu'on appelle une variété algébrique complexe.

Ces variétés algébriques que nous offre l'algèbre ont un étonnant répertoire de formes, au sens de "type topologique": deux espaces ont la même "forme" si on peut les mettre en correspondance continue, un point de l'un correspondant à un et un seul point de l'autre. Premiers exemples: une droite complexe est, géométriquement, un plan (coordonnée $z = x + iy$, avec x, y réels). La droite projective complexe, qui s'en déduit par adjonction d'un point à l'infini, a la forme d'une sphère, comme le montre la projection stéréographique



(projection $A \to A'$ à partir d'un point de la sphère, N dans le dessin, où le plan tangent est parallèle au plan sur lequel on projette). Le point N correspond au point à l'infini.

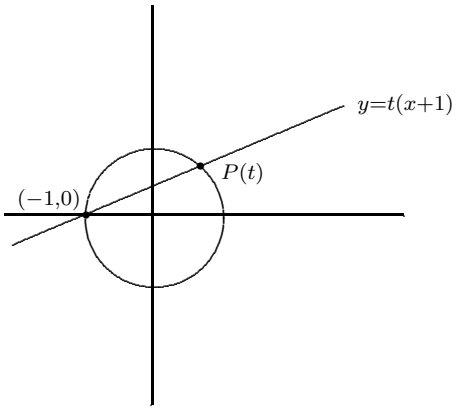
On vérifie qu'une courbe plane (projective) définie par une équation du troisième degré a en général la forme d'un tore (surface de révolution, balayée par un cercle qui tourne autour d'une droite de son plan qui ne le rencontre pas), tandis qu'une équation de degré d définit une surface de genre g, telle celle d'une brique perforée de g trous, pour $g = (d-1)(d-2)/2$. Vue d'un point de l'axe/de haut:



tore ($g = 1$) $\qquad$ $g = 3$

Un des premiers outils dont on dispose pour analyser la "forme" d'un espace est son homologie, une suite d'invariants algébriques qui lui sont associés. Dans le cas des variétés algébriques, cette homologie admet plusieurs descriptions de natures très différentes, et c'est l'un des délices du sujet.

Les *nombres rationnels* sont les fractions ordinaires a/b. Quand on travaille dans ce système de nombres, la géométrie aide à attaquer des questions d'arithmétique, où l'on cherche à résoudre des équations en nombres entiers. Soit par exemple la question d'énumérer les "triples pythagoriciens", solutions entières de l'équation $m^2 + n^2 = p^2$. Récrivant l'équation sous la forme $(m/p)^2 + (n/p)^2 = 1$, on voit qu'il s'agit de trouver les points rationnels, i.e. à coordonnées des nombres rationnels, sur la circonférence $x^2 + y^2 = 1$. Le point $(-1, 0)$ est sur cette circonférence, et la droite de pente t passant par ce point la recoupe en un autre point $P(t)$, qui, quand t varie, parcourt la circonférence. A quelques grains de sel près, ceci vaut dans tout système de nombres.



On calcule que $P(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$, et, prenant t rationnel, on paramétrise ainsi les points rationnels de $x^2 + y^2 = 1$.

Pour p un entier, les *entiers modulo p* sont déduits des entiers ordinaires, en décidant de traiter comme égaux deux entiers dont la différence est multiple de p. Il revient au même de dire que c'est le système de représentants $0, 1, 2, \ldots, p-1$, l'addition (multiplication) étant le reste quand on divise l'addition (multiplication) ordinaire par p. Les cadrans des horloges nous ont familiarisés avec le cas $p = 12$: que 4h après 10h il est 2h correspond à $10 + 4 = 2$ (modulo 12). Pour que la division (sauf par zéro) soit toujours possible, il faut supposer p premier, cas auquel nous nous limiterons. Le cas des entiers modulo 2 est particulièrement intéressant: les nombres sont 0 et 1, qu'on peut aussi appeler "pair" et "impair", et les tables d'addition et de multiplication sont les usuelles, sauf que $1 + 1 = 0$ (impair + impair

= pair). On peut penser à une suite de n 0 et 1 comme à un message, ou comme à un point de l'espace à n dimensions, à coordonnées entiers modulo 2. La géométrie algébrique fournit des codages et décodages intéressants pour communiquer de tels messages.

Il existe d'autres systèmes finis de nombres, les "*imaginaires de Galois*" (= corps finis), déduits des entiers modulo p (p un nombre premier) par des procédés réminiscents de celui qui fait passer des nombres réels aux nombres complexes. Pour chaque puissance q de p, il existe un tel système, noté $\mathbb{F}_q$, à q éléments. Il contient comme sous-système celui, $\mathbb{F}_p$, des entiers modulo p. De ce que, dans $\mathbb{F}_p$ et donc dans $\mathbb{F}_q$, on ait $p = 1+1+\cdots+1$ (p termes) $= 0$, résulte que $(x+y)^p = x^p + y^p$. Par exemple, pour $p = 2$, $(x+y)^2 = x^2 + 2xy + y^2 = x^2 + y^2$. Cette identité couplée à l'identité banale $(xy)^p = x^p y^p$ a des conséquences étonnantes:

(a) (Petit théorème de Fermat): dans $\mathbb{F}_p$, $x^p = x$. On peut le vérifier par induction: $0^p = 0$, $1^p = 1$, et si $x^p = x$, alors $(x+1)^p = x^p + 1^p = x + 1$.

(b) Réciproque: si x dans $\mathbb{F}_q$ vérifie $x^p = x$, alors x est dans $\mathbb{F}_p$: car l'équation de degré p $x^p - x = 0$ a au plus p solutions.

(c) Soit V la variété algébrique des solutions d'un système d'équations $P(x_1, \ldots, x_n) = 0$ à coefficients dans $\mathbb{F}_p$. La transformation, dite de Frobenius, $(x_1, \ldots, x_n) \mapsto (x_1^p, \ldots, x_n^p)$ transforme V en elle-même. Plus concrètement, quel que soit q, elle transforme l'ensemble des points de V à coordonnées dans $\mathbb{F}_q$ en lui-même. En effet, si $P(x_1, \ldots, x_n) = 0$, $P(x_1^p, \ldots, x_n^p) = P(x_1, \ldots, x_n)^p$ s'annule aussi.

(d) Par (a), (b), (c), les points de V à coefficients entiers modulo p apparaissent comme les points fixes de l'application de Frobenius de V dans elle-même.

L'étude et la construction de points fixes a, dans d'autres contextes, une histoire plus que centenaire. L.E.J. Brouwer a prouvé en 1910 qu'une application continue d'un disque (ou plus généralement d'une boule à n dimensions) dans lui-même laisse toujours fixe au moins un point. Le même énoncé vaut pour une transformation continue d'une sphère de dimension paire dans elle-même qui déplace peu chaque point. Si on regarde la direction dans laquelle a été déplacé chaque point comme celle dans laquelle on voudrait peigner un cheveu, ceci se traduit: "on ne peut peigner sans singularité une sphère chevelue". Exemple: si on veut en chaque point de la sphère terrestre choisir, continûment, une direction, et qu'on dise: "vers l'est", on ne sait quoi faire aux pôles.

Ces énoncés, difficiles à prouver "à mains nues", sont conséquences faciles d'une formule prouvée par S. Lefschetz reliant le nombre de points fixes, comptés judicieusement, d'une transformation T d'un espace E, et les groupes d'homologie de E déjà mentionnés.

Bien que la continuité joue ci-dessus un rôle essentiel, un formalisme analogue existe en géométrie algébrique, même quand les nombres utilisés sont les imaginaires de Galois, et bien qu'on voie mal comment penser "continu" et "fini" en même temps. Pour un système d'équations à coefficients entiers, cela implique des relations entre la "forme" de la variété des solutions complexes, et le nombre de solutions dans $\mathbb{F}_q$ (du moins une fois exclu le cas où q est puissance d'un nombre fini de nombres premiers p exceptionnels).

Voici en bref la longue histoire de la création de tels formalismes: A. Weil a commencé par traiter ce qui aujourd'hui peut être réinterprété comme le cas des courbes. En 1949, il suggère l'idée extraordinaisement hardie qu'un tel formalisme devrait exister en toute dimension. Dans les années 60, mon maître, A. Grothendieck, le construit, à la suite entre autres d'une analyse profonde de la notion d'"espace" et de celle du mot "local" qui lui est associé, et j'ai complété son oeuvre.

Un mystère subsiste, celui d'une surabondance de biens. Ce n'est pas d'une théorie de l'homologie des variétés algébriques dont on dispose, mais de nombreuses telles théories, qui semblent raconter chacune la même histoire dans une langue différente. Nous ignorons si elles sont réellement parallèles, et sommes même en peine de donner un sens à la question. Nous ne disposons que de résultats épars et de conjectures optimistes.

La géométrie algébrique est une discipline touche-à-tout, notamment parce qu'elle s'introduit naturellement partout où apparaissent les polynômes, que ce soit à propos d'intégrales d'expressions algébriques ou de nombre de solutions d'équations dans un corps fini. J'espère avoir pu donner une idée de sa splendeur.