

De Galois aux corps finis

Le 25 octobre 2011 marque le bicentenaire de la naissance d'Évariste Galois. Les découvertes du fougueux jeune homme, notamment sur les structures algébriques nommées corps finis, ont profondément marqué les mathématiques.

Antoine Chambert-Loir

L'ESSENTIEL

✓ Évariste Galois était un mathématicien prodige, mais incompris. Il est mort très jeune dans des conditions tragiques.

✓ Il a découvert un important critère pour déterminer si une équation polynomiale est résoluble par radicaux.

✓ Galois est notamment à l'origine de la théorie des groupes et de celle des corps finis.

✓ Son héritage mathématique traverse de nombreux domaines et a des applications par exemple en cryptographie.

Bruno Bourgeois

Cet automne, les mathématiciens célèbrent le 200^e anniversaire de la naissance d'Évariste Galois. Au cours de sa brève et tumultueuse vie, ce mathématicien prodigieux, dont l'œuvre tient pourtant en à peine 60 pages, a fait plusieurs découvertes fondamentales relatives à la théorie des équations polynomiales. En particulier, on lui doit l'émergence des notions de groupe et de corps fini, des structures algébriques qui jouent aujourd'hui un rôle crucial dans de nombreux domaines des mathématiques et de leurs applications.

Le 200^e anniversaire de la naissance de Galois offre l'occasion de revenir sur ces travaux qui ont marqué l'histoire des mathématiques et dont la postérité reste bien vivante. Nous passerons ainsi des équations polynomiales aux équations en congruence, qui permettent d'introduire les corps finis, puis nous terminerons par l'une des applications de la théorie des corps finis, le cryptage dit asymétrique.

Commençons par les équations polynomiales. Les équations qui nous intéressent ici ont une seule inconnue, qui représente un nombre et que nous note-

rons x . Elles prennent la forme d'une relation mettant en jeu des sommes de puissances entières et positives (x , x^2 , x^3 , etc.) de ce nombre. La plus grande puissance qui apparaît dans l'équation est le « degré » de l'équation.

Les équations polynomiales de degré 1 sont élémentaires. Un exemple est l'équation $3x - 5 = 0$, dont la solution s'obtient en faisant passer le terme constant (ici, 5) dans le second membre et en divisant l'équation par le coefficient de x (ici, 3). On trouve ainsi la solution $x = 5/3$.

Existe-t-il une formule pour la solution ?

En degré 2, l'équation prend la forme $ax^2 + bx + c = 0$, où a , b et c sont trois paramètres, avec $a \neq 0$; un exemple d'une telle équation est $x^2 - x - 1 = 0$ (dont une des deux solutions est le nombre d'or). On sait résoudre toutes les équations de degré 2 depuis environ quatre siècles; la solution générale est donnée par la formule $x = (-b \pm \sqrt{b^2 - 4ac})/2a$. Cette dernière est bien connue des lycéens, et l'on peut



1. QUELQUES COURBES ELLIPTIQUES,
dans une vue d'artiste. Une addition peut être définie
entre les points d'une telle courbe, le 0 de cette
addition étant le point à l'infini (*zone brillante*).
Certaines méthodes cryptographiques sont construites
en considérant les équations de ces courbes non pas
sur le corps des nombres réels, mais sur un corps fini.

Galois, héros tragique des mathématiques

Évariste Galois, né le 25 octobre 1811 à Bourg-la-Reine, au Sud de Paris, est mort à moins de 21 ans le 31 mai 1832, tué dans un duel auquel il n'avait pu se soustraire et ce, dans des circonstances obscures. Le duel était semble-t-il lié à une « infâme coquette et [...] deux dupes de cette coquette ».

Galois s'intéresse dès l'âge de 16 ans aux mathématiques, qui deviendront l'une de ses passions, avec la politique. Mal préparé, il échoue deux fois au concours d'entrée à l'École polytechnique, la plus prestigieuse de l'époque. Il parvient



toutefois à intégrer l'École préparatoire, avatar de ce qui était et redeviendra l'École normale supérieure. Mais il en est expulsé début 1831. Peu après, il

remet à l'Académie son mémoire « Sur les conditions de résolubilité des équations par radicaux ». Ce texte est d'abord égaré par l'Académie, puis rejeté par Sylvestre Lacroix et Denis Poisson, mathématiciens qui l'examinent sans le comprendre.

L'œuvre mathématique de Galois restera dans l'ombre jusqu'à ce que Joseph Liouville, sollicité par le frère d'Évariste et par son ami Auguste Chevalier, la redécouvre et en comprenne la portée. Il la présente à l'Académie en 1843, et commence à la publier en 1846.

même dire qu'elle fait partie du patrimoine culturel ; on la trouve ainsi un peu partout dans les bandes dessinées de Marcel Gotlib, souvent en conjonction avec son personnage d'Isaac Newton. Par exemple, pour l'équation du nombre d'or, $x^2 - x - 1 = 0$, on trouve $x = (1 + \sqrt{5})/2$; le nombre d'or lui-même est la racine positive de l'équation, c'est-à-dire $(1 + \sqrt{5})/2$.

Nombres, équations, groupe de Galois

Pour la théorie des nombres, le cas où les coefficients a , b et c de l'équation sont des nombres entiers est le plus important ; on voit que les solutions sont des nombres rationnels précisément dans le cas où le discriminant $b^2 - 4ac$ est un carré parfait (le carré d'un entier). Lorsque le discriminant est négatif, cette solution fait apparaître des nombres qu'on avait, un temps seulement, qualifiés d'imaginaires (parce qu'un carré ne saurait être négatif), mais dont leur utilité est telle qu'ils ont rapidement acquis une place centrale en mathématiques et dans les sciences en général. On les nomme aujourd'hui « nombres complexes », bien qu'une fois passée la surprise de leur découverte, leur manie- ment n'ait rien de si complexe.

Décidons d'introduire un nombre i tel que $i^2 = -1$. C'est l'apanage des mathématiciens de pouvoir décréter ce genre de chose, qui ressemble au « Que la lumière soit ! » de la Bible. Cependant, comme jadis, c'est là que les choses sérieuses commencent : il faut s'assurer que l'on n'a ni créé

un chaos absolu ni tout envoyé dans le néant. Que peut-on faire avec une telle racine « imaginaire » de -1 ? On peut considérer des nombres de la forme $x + yi$ (où x et y sont des nombres réels) et les additionner : la somme de $x + yi$ et de $x' + y'i$ est égale à $(x + x') + (y + y')i$. On peut aussi les multiplier : en développant le produit $(x + yi)(x' + y'i)$ des deux nombres précédents, on trouve qu'il est égal à $xx' + (yx' + xy')i + yy'i^2$, c'est-à-dire à $(xx' - yy') + (yx' + xy')i$ puisque $i^2 = -1$.

Autrement dit, l'ensemble des nombres de la forme $x + yi$ est stable par addition et multiplication ; il est aussi stable par soustraction, et l'on peut aussi diviser par un nombre de cette forme, sauf si $x = y = 0$.

Pourquoi l'introduction des nombres complexes est-elle cruciale en mathématiques et dans beaucoup d'autres domaines scientifiques ? Parce qu'une propriété fondamentale des équations polynomiales leur est liée : toute équation polynomiale, à coefficients réels ou complexes, possède exactement autant de solutions que son degré (supposé au moins égal à 1). J'insiste : avec les nombres réels, usuels, il existe des équations très simples sans solutions, par exemple $x^2 + 1 = 0$ (dont les solutions seraient des racines carrées de -1), mais dès qu'on introduit cette racine carrée de -1 notée i , toutes les équations polynomiales ont des solutions.

Le problème persiste, en revanche, de trouver des formules pour ces solutions. En degrés 3 et 4, il existe des formules analogues à celle dont on dispose pour le degré 2, qu'ont découvertes au XVI^e siècle

les mathématiciens italiens Jérôme Cardan, Tartaglia (surnom de Niccolo Fontana), Ludovico Ferrari. Mais elles sont plus compliquées et font intervenir des racines cubiques et quartiques (du quatrième ordre).

Au XIX^e siècle, le mathématicien norvégien Niels Abel découvrit que les racines de certaines équations du cinquième degré ne peuvent pas être calculées par des formules générales semblables. L'un des apports les plus connus de Galois est d'avoir compris pourquoi il en était ainsi.

Une équation polynomiale étant donnée, Galois introduisit le groupe formé par les permutations de ses « racines » (ses solutions) qui préservent les relations algébriques satisfaites par ces racines. Cela signifie que si l'on a, par exemple, deux racines a et b vérifiant $a + b^2 = 1$, leurs images a' et b' par une permutation du groupe doivent aussi satisfaire $a' + (b')^2 = 1$. Ce groupe est aujourd'hui appelé le « groupe de Galois » de l'équation considérée.

Galois prouva que l'on peut calculer les solutions d'une équation polynomiale à l'aide de radicaux si et seulement si le groupe de Galois de l'équation possède une certaine propriété technique, nommée « résolubilité » en référence à ce résultat. Si le groupe n'est pas résoluble, il est impossible d'exprimer les solutions de l'équation à l'aide d'une formule construite avec des radicaux.

Des congruences aux corps finis

Abordons maintenant une autre découverte importante de Galois : les corps finis, que les Anglo-Saxons nomment d'ailleurs *Galois fields*. Cette découverte fait l'objet d'une petite note d'une dizaine de pages parue en 1830 et intitulée *Sur la théorie des nombres*. D'une certaine façon, Galois se proposait de combiner la théorie des équations polynomiales avec celle des congruences. Rappelons ce qu'est cette dernière.

Parmi les plus anciens ouvrages de mathématiques figure le *Sunzi Suangjing*, texte chinois du V^e siècle environ, où l'on trouve le problème suivant : « Nous avons un nombre inconnu de choses. Si nous les comptons par trois, il en reste deux ; si nous les comptons par cinq, il en reste trois, si nous les comptons par sept, il en reste deux. Trouver le nombre de ces choses. »

Appelons x l'inconnue ; c'est un nombre entier et la phrase centrale du problème affirme que x est égal à 2 plus un multiple