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 $x = (1 \pm \sqrt{5})/2$; 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 maniement 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 XVIe 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 XIXe 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 Ve 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

(indéfini) de 3, à 3 plus un multiple de 5, et à 2 plus un multiple de 7. On résume ces égalités, à un multiple près de 3, 5 ou 7, par le mot « congruence ». En d'autres termes, on dit que x est congru à 2 modulo 3, à 3 modulo 5, et à 2 modulo 7, ce que l'on écrit $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$. Les entiers 3, 5 et 7 sont les « raisons » de ces congruences.

Une chinoiserie ?

Le *Sunzi Sunangjing* explique comment résoudre ces congruences, c'est-à-dire comment trouver les entiers x qui les vérifient. Ce « théorème des restes chinois », comme on le nomme parfois, dit d'ajouter 2×70, 3×21 et 2×15 (cela fait $140 + 63 + 30 = 233$) et de soustraire 105 tant que le résultat est supérieur à 106. Dans cette formule, 70, 21 et 15 ont été choisis parce que 70 est multiple de 5 et de 7 ($70 = 2 \times 5 \times 7$) et est congru à 1 modulo 3 (car $70 = 1 + 69 = 1 + 3 \times 23$), 21 est multiple de 3 et de 7 et est congru à 1 modulo 5, 15 est multiple de 3 et de 5 et est congru à 1 modulo 7. En outre, $105 = 3 \times 5 \times 7$. Dans cet exemple, on trouve donc que x est congru à 23 modulo 105 : trois congruences modulo les nombres premiers 3, 5 et 7 ont été transformées en une seule congruence ayant pour raison le produit $105 = 3 \times 5 \times 7$ de leurs raisons.

Le développement de l'algèbre a permis de comprendre que, dans le calcul des congruences, on peut négliger complètement le multiple indéfini et calculer comme si la raison était nulle. Par exemple, modulo 13, on a $6 \equiv -7$ puisque $6 - (-7) = 13 \equiv 0$; de même, $5 \times 7 \equiv 35 \equiv 3 \times 13 - 4 \equiv -4$. On peut aussi résoudre des équations en congruences ; examinons par exemple la congruence $3x - 5 \equiv 0 \pmod 7$; si l'on multiplie l'équation par 2, on trouve $6x - 10 \equiv 0 \pmod 7$. Mais $6 \equiv -1 \pmod 7$ et $-10 = -14 + 4 \equiv 4 \pmod 7$, si bien que l'équation devient $-x + 4 \equiv 0 \pmod 7$, d'où $x \equiv 4$. Inversement, si $x \equiv 4$, $3x \equiv 12 \equiv 5 \pmod 7$.

Il y a en revanche quelques subtilités nouvelles. Par exemple, 2 et 3 ne sont pas multiples de 6 (ils ne sont pas nuls modulo 6), mais leur produit l'est. Autrement dit, le produit de deux nombres peut être nul (en congruence) sans qu'aucun d'eux ne le soit.

Ce phénomène d'apparence pathologique – un produit égal à zéro alors que les facteurs sont non nuls – ne se présente pas lorsque la raison est un nombre premier, c'est-à-dire un entier positif divisible seulement par 1 et par lui-même. En effet, d'après un résultat d'Euclide, le produit de deux entiers ne peut être multiple d'un nombre premier p sans qu'au moins l'un des deux ne le soit. Pour cette raison, les congruences modulo p, où p est un nombre premier, sont les plus fondamentales en mathématiques.

Ainsi, avec le développement de la théorie des équations et celui de la théorie des nombres, est née peu à peu une théorie des équations polynomiales modulo un nombre premier. Le grand mathématicien allemand Carl Friedrich Gauss avait lui-même largement étudié ce sujet dans lequel, comme le dit Galois lui-même, il s'agit de résoudre une équation en considérant que tout multiple d'un nombre premier donné est nul.

Par exemple, comment résoudre l'équation du nombre d'or, $x^2 - x - 1 = 0$, modulo la raison 7 ou modulo la raison 11 ? On peut commencer par raisonner comme en algèbre classique. Modulo 7, on peut écrire :
$0 = x^2 - x - 1 \equiv x^2 - 8x - 1 \equiv$
$(x - 4)^2 - 17 \equiv (x - 4)^2 - 3 \pmod 7$;
s'il existe une solution entière x de cette congruence, il faut que 3 soit un carré

L'AUTEUR

Antoine CHAMBERT-LOIR est professeur de mathématiques à l'Université de Rennes 1.

✔ SUR LE WEB

Pour des détails sur les célébrations du **bicentenaire de la naissance d'Évariste Galois**, voir : http://www.galois.ihp.fr/

Qu'est-ce qu'un corps ?

Un corps est un ensemble muni d'une addition et d'une multiplication, et de deux éléments distincts notés 0 et 1, qui vérifient les axiomes suivants (a, b et c désignent ici des éléments quelconques du corps) :

- $a + b = b + a$ (commutativité de l'addition) ;
- $(a + b) + c = a + (b + c)$ (associativité de l'addition) ;
- $a + 0 = a$; pour tout a, il existe un unique élément b tel que $a + b = 0$, et on le note $-a$;
- $(a \times b) \times c = a \times (b \times c)$ (associativité de la multiplication) ;
- $a \times 1 = 1 \times a = a$; pour tout $a \neq 0$, il existe un unique élément, noté $1/a$ ou a^{-1}, tel que $a \times a^{-1} = a^{-1} \times a = 1$.
- $(a + b) \times c = a \times c + b \times c$ (distributivité de la multiplication par rapport à l'addition).

La soustraction est alors définie par la formule $a - b = a + (-b)$, la division par un élément non nul par la formule $a/b = a \times (1/b)$. Pour tout a, $a \times 0 = 0$, $a \times (-1) = -a$, etc.

Des exemples de corps sont l'ensemble des nombres rationnels (c'est le calcul des fractions appris à l'école élémentaire) ainsi que ceux des nombres réels et complexes. Ces trois corps sont infinis : ils contiennent une infinité d'éléments (par exemple 1, 2, 3, etc.).

On peut faire de l'ensemble {0, 1} un corps avec les lois d'addition et de multiplication données par les tables suivantes :
(où seule la formule $1 + 1 = 0$ n'est pas explicitement forcée par les axiomes ci-dessus). C'est donc un corps à deux éléments ; l'informatique, avec la numération binaire, lui a donné un rôle fondamental.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Plus généralement, si n est un entier supérieur ou égal à 2, on peut tenter de faire de l'ensemble $\{0, 1, \ldots, n-1\}$ un corps en disant d'abord que la somme (le produit) de deux éléments est le reste de la division par n de leur somme (de leur produit). Cela en fait un « anneau » : la seule propriété qui manque pour en faire un corps est l'existence d'un inverse pour tout élément autre que 0. Lorsque (et seulement lorsque) n est un nombre premier, l'ensemble $\{0, 1, \ldots, n-1\}$ est un corps, que Carl Friedrich Gauss avait étudié en grand détail dans ses *Disquisitiones Arithmeticae* (1798).