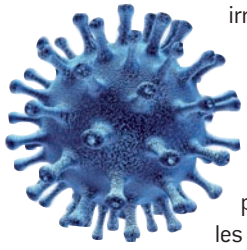
vasoconstriction créant le gradient de température entre la peau et les organes s'exerce aussi dans les bronches. Cela provoque une diminution des défenses immunitaires et mécaniques de l'organisme : d'une part, les cellules immunitaires du sang éliminent moins bien les bactéries et, d'autre part, les cils bronchiques qui nettoient en permanence les bronches ne sont plus aussi efficaces. En outre, la diminution de l'ensoleillement et de la température modifie plusieurs paramètres physiologiques ; par exemple, la concentration en vitamine D, qui participe aux défenses immunitaires et est produite par la peau sous l'effet des rayonnements ultraviolets, diminue en hiver.

D'autres facteurs environnementaux favorisent les infections hivernales. La sécheresse accompagnant le froid et les polluants atmosphériques, dont les concentrations augmentent, car les habitations sont insuffisamment ventilées, provoquent une irritation des voies nasales et bronchiques. On constate alors à la surface des cellules nasales une augmentation du nombre de protéines ICAM1, « serrures » par lesquelles les rhinovirus, responsables du rhume, entrent dans les cellules et les infectent.



Ainsi, les organismes humains sont fragilisés par le froid, qui, au contraire, permet à certains virus de persister plus longtemps dans l'air. Par exemple, le virus de la grippe se multiplie dans les cellules de la personne infectée. Les particules virales sont recouvertes d'une coque, composée d'éléments lipidiques des membranes cellulaires de l'individu infecté ; cette coque doit être assez résistante pour protéger le virus quand il est dans l'air, mais pas trop pour qu'elle puisse libérer son contenu au contact de la muqueuse nasale d'une future victime. Or la durée de vie de cette coque dans l'air et, par conséquent, celle du virus augmentent quand la température extérieure diminue : son pouvoir contagieux en est renforcé.

En outre, lors d'une épidémie, la majorité de la population est en contact à un moment ou à un autre avec l'agent infectieux, et développe une réaction immunitaire qui permet de lutter contre l'infection. Pendant quelque temps, une nouvelle épidémie avec le même agent est donc peu probable ; puis, après un délai qui dépend du type de micro-organisme, la population redevient sensible, soit par disparition de l'immunité si l'agent était peu « immunogène », soit parce que cet agent a muté, si bien qu'il n'est plus reconnu par le système immunitaire des individus exposés au premier virus. En hiver, plusieurs épidémies de virus proches peuvent apparaître par vagues. Par ailleurs, une infection détourne une grande partie des ressources immunitaires contre l'agent en cause, si bien que l'individu risque de se retrouver désarmé face à d'autres pathogènes. C'est ce qui explique qu'une personne infectée par la grippe contracte parfois une pneumonie à pneumocoques.

Enfin, l'état sanitaire général de la population est également un point important. Se défendre contre une infection mobilise des ressources physiologiques qu'il faut être capable de fournir. Certaines personnes risquent plus que d'autres de contracter une infection : les nourrissons, les femmes enceintes, les personnes âgées ou celles souffrant déjà d'une autre pathologie. Cet état sanitaire dépend bien sûr du statut socio-économique de la population et de facteurs tels que la malnutrition, voire la dénutrition.

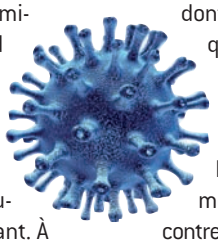
Malgré l'accumulation de données épidémiologiques et une meilleure compréhension des mécanismes physiopathologiques, notre capacité à modéliser la surmortalité par temps froid reste limitée. À la fin des années 1960, Ronald Douglas, de l'Université du Texas, et ses collègues n'ont pas réussi à relier l'infection par le rhinovirus à une simple exposition à de l'air froid, car le nombre de facteurs pouvant jouer un rôle est trop important. À l'inverse, d'autres facteurs ont été reliés au risque d'attraper un rhume, alors qu'il n'y a pas de relation de causalité directe : par exemple, un temps de sommeil inférieur à sept heures multiplie par trois ce risque (mais on ignore si le manque de sommeil diminue les défenses immunitaires ou s'il s'agit d'un biais statistique).

De surcroît, le refroidissement de l'organisme au-dessous de 37 °C, par exemple, dépend non seulement de la température extérieure, mais aussi de phénomènes d'évaporation, liés à l'humidité et à la présence de vent fort. Ainsi, une température de –10 °C avec un vent soufflant à 30 kilomètres par heure correspond à –18 °C sans vent. De même, certains déterminants, telles la pollution ou la promiscuité, sont difficiles à quantifier. Sans compter le rôle des déplacements, notamment en avion, ou de la mode vestimentaire ou encore des événements naturels, tels qu'une inondation.

Peut-on réduire les risques de contamination ?

En résumé, on « attrape froid » et on tombe malade en hiver quand les défenses de l'organisme sont affaiblies et les virus plus nombreux qu'en été. Ce sont ces paramètres, conséquences du froid, qui sont responsables de la recrudescence des maladies infectieuses en hiver.

Peut-on l'éviter ? L'écharpe ou le grog permettent-ils de se protéger par temps froid ? Probablement pas, car ils n'empêchent pas d'être en contact avec les agents infectieux, et ne suffisent pas à réchauffer l'organisme, ni l'air inspiré. En revanche, placer l'écharpe sur le nez réchauffe l'air avant son entrée dans les poumons, et évite la vasoconstriction des bronches dont nous avons évoqué les conséquences néfastes.



Enfin, n'oublions pas que la plupart des pathogènes sont transmis par les mains et que le lavage régulier est l'une des meilleures protections possibles contre les infections. Et rappelons qu'en ce début d'automne, la vaccination contre la grippe, l'utilisation de mouchoirs jetables, et le port d'un masque restent les meilleurs moyens de se protéger et de protéger les autres, en particulier les plus fragiles, contre les maladies respiratoires infectieuses. ■

Luc de SAINT-MARTIN PERNOT est médecin interniste au Centre hospitalier régional universitaire de Brest.

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 200e 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.

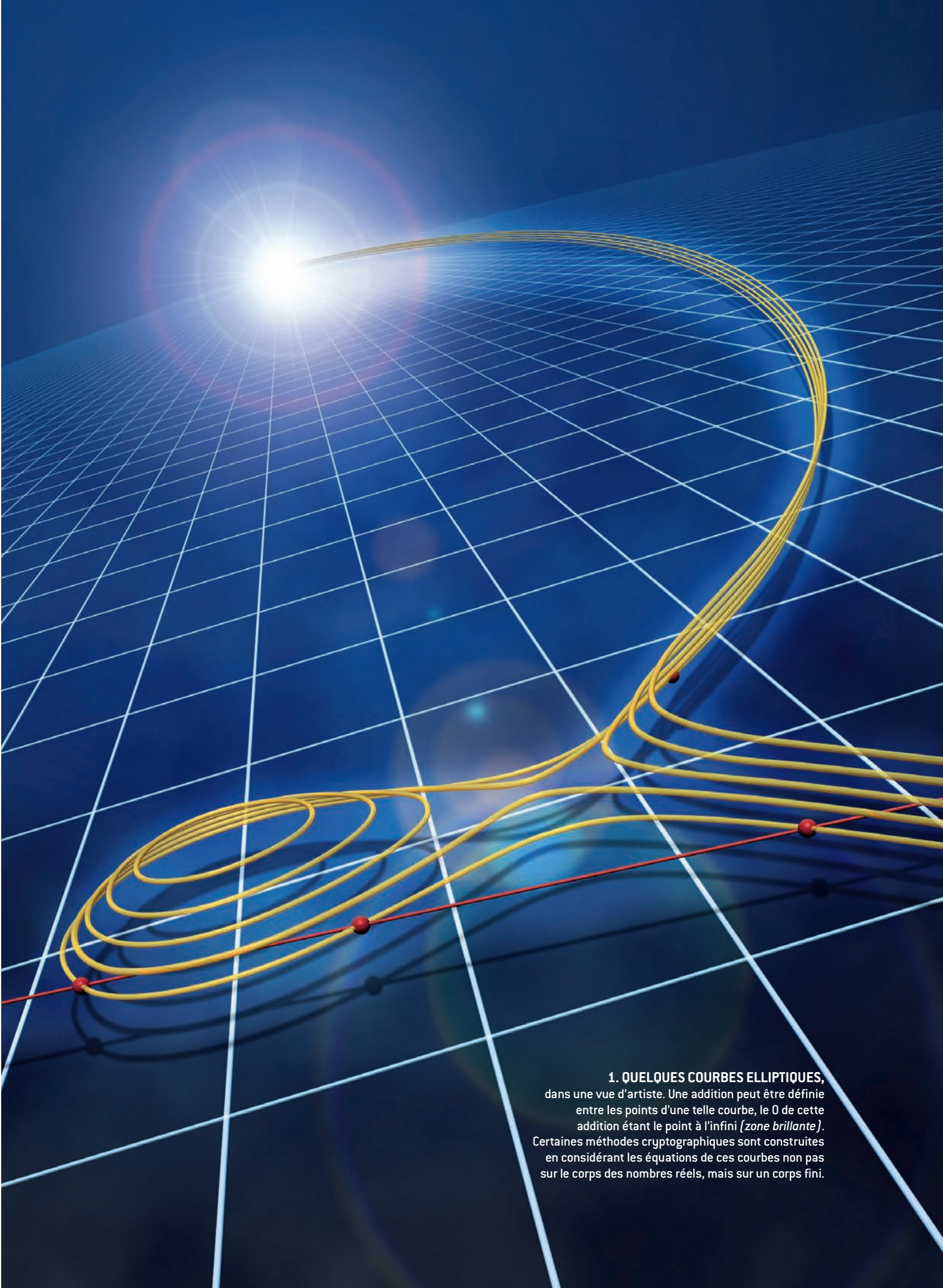
Le 200e anniversaire de la naissance de Galois offre l'occasion de revenir sur ces travaux qui ont marqué l'histoire des mathématiques et dont la postérité reste bien vivante. Nous passerons ainsi des équations polynomiales aux équations en congruence, qui permettent d'introduire les corps finis, puis 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 noterons 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 $x = (1 \pm \sqrt{5})/2$; 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).

Calculer x^a rapidement

✔ **Il existe un algorithme récursif qui permet de calculer très rapidement la puissance entière x^a d'un nombre x. Cet algorithme est fondé sur la numération binaire de l'entier a, et sur le fait que $x^a = (x^2)^{a/2}$ si a est pair, et que $x^a = x\,(x^2)^{(a-1)/2}$ si a est impair. On a par exemple $x^{19} = x\,(x^2)\,(x^{16})$, où x^{16} est calculé par quatre élévations successives au carré : $x^{16} = (((x^2)^2)^2)^2$. On obtient ainsi une méthode de calcul par récurrence qui ne demande qu'environ $2n$ multiplications pour calculer x^a, où n est le nombre de chiffres du développement binaire de a.**

modulo 7 ; or les carrés modulo 7 sont 0, 1, $2^2 = 4$, $3^2 = 9 \equiv 2$, $4^2 \equiv (-3)^2 \equiv 2$, $5^2 \equiv (-2)^2 \equiv 4$ et $6^2 \equiv (-1)^2 \equiv 1$. On constate en particulier que 3 n'est pas un carré modulo 7 et cette équation en congruence n'a donc pas de solution.

Modulo 11, on écrit plutôt :
$0 = x^2 - x - 1 \equiv x^2 - 12x - 1 \equiv$
$(x-6)^2 - 37 \equiv (x-6)^2 - 4 \pmod{11}$.
Par conséquent, $(x-6)^2 \equiv 4 \equiv 2^2$, d'où l'on déduit (comme d'habitude !) que $x - 6 = \pm 2$. On trouve ainsi deux solutions modulo 11, à savoir $x = 4$ et $x = 8$.

Équations polynomiales et congruences

Alors que ses prédécesseurs s'étaient contentés de chercher les solutions entières de congruences polynomiales, Galois s'est intéressé aux espèces de nombres complexes (ou, comme il dit, aux « quantités imaginaires ») que l'on peut définir à partir d'une congruence polynomiale, de la même façon qu'on avait créé les nombres complexes à partir d'une solution « imaginaire » de l'équation $x^2 + 1 = 0$.

Galois considère donc une raison, qui est un nombre premier p et, un polynôme arbitraire $F(x)$ de degré d et à coefficients entiers. Il fait deux hypothèses sur ce polynôme $F(x)$: d'une part, que le coefficient de x^d ne soit pas un multiple de p et, d'autre part, qu'on ne puisse pas factoriser F modulo p, c'est-à-dire qu'il n'existe pas de polynômes F_1 et F_2 tels que $F \equiv F_1 F_2 \pmod{p}$. Galois dit que la congruence $F(x) \equiv 0 \pmod{p}$ est « irréductible ». Par exemple, si $p = 13$, on ne peut pas prendre $F = x^2 + 1$, car $x^2 + 1 \equiv (x-5)(x-8) \pmod{13}$, mais on peut vérifier que le choix $p = 11$ et $F = x^2 + 1$ convient ; il en est de même du choix $p = 13$ et $F = x^2 - 2$, ou encore $p = 7$ et $F = x^2 - x - 1$.

Nous avions introduit un symbole i pour désigner une racine de l'équation $x^2 + 1 = 0$ et vu que l'on pouvait calculer naturellement avec lui. Faisons de même ici : traitons la lettre x, non plus comme une inconnue, mais comme une solution de la congruence $F(x) \equiv 0 \pmod{p}$. Cela donne lieu à un ensemble de p^d « nombres » : tous ceux de la forme :

$$a_0 + a_1 x + \ldots + a_{d-1} x^{d-1},$$

où $a_0, \ldots, a_{d-1}$ sont des entiers compris entre 0 et $p - 1$ (il y a p choix pour chacun des d coefficients, d'où p^d nombres distincts). Ces nombres peuvent être additionnés (on additionne les coefficients de type a_0, ceux de type a_1, etc., en soustrayant p si leur somme dépasse p), ou soustraits. De façon peut-être plus surprenante, on peut aussi les multiplier : si l'on développe le produit de deux nombres de la forme $a_0 + a_1 x + \ldots + a_{d-1} x^{d-1}$, on voit apparaître des puissances de x avec un exposant qui peut dépasser $d - 1$; mais la congruence $F(x) \equiv 0 \pmod{p}$ permet de remplacer x^d par un nombre admissible, x^{d+1} aussi, etc.

Par exemple, si $x^3 + 2x - 1 \equiv 0 \pmod{5}$, alors $x^4 + 2x^2 - x \equiv 0$, et par conséquent $x^4 \equiv -2x^2 + x \equiv 3x^2 + x \pmod{5}$. On en déduit que $x^5 \equiv 3x^3 + x^2 \equiv 3(3x + 1) + x^2 \equiv x^2 + 9x + 3 \equiv x^2 + 4x + 3 \pmod{5}$, etc. Enfin, et c'est là qu'intervient l'hypothèse que la congruence $F(x) \equiv 0$ est irréductible, on peut aussi diviser par tout nombre différent de 0.

On obtient ainsi un ensemble de p^d nombres avec lesquels on peut calculer de façon naturelle : addition, soustraction, multiplication, division par tout élément non nul, ces opérations obéissant aux règles usuelles (commutativité, associativité de l'addition et de la multiplication, distributivité de

L'addition dans une courbe elliptique

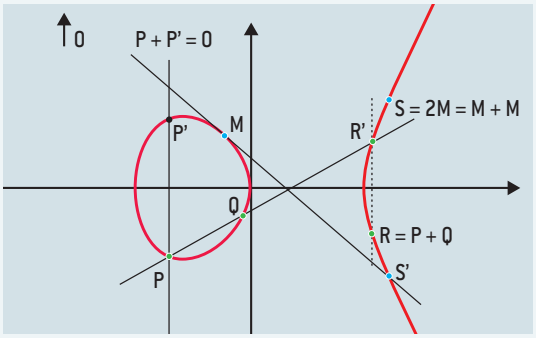
Les courbes elliptiques, qui n'ont pas du tout la forme d'une ellipse, ont été nommées ainsi parce que leurs équations ont un lien avec le calcul de la longueur d'arcs d'ellipses. Une courbe elliptique E est définie par une équation cubique qui peut être mise sous la forme $y^2 = x^3 + ux + v$, où u et v sont des nombres réels tels que $4u^3 + 27v^2$ soit non nul (sinon, la courbe a un point singulier).

Une particularité des courbes elliptiques est qu'on peut définir une addition entre leurs points. L'addition de deux points P et Q d'une courbe elliptique E est définie ainsi : si la droite passant par P et Q rencontre la courbe en un troisième point R', le point R = P + Q est le symétrique de R' par rapport à l'axe (horizontal) de symétrie de la courbe. Si la droite passant par P et Q est verticale, on considère que R est à l'infini ; le point à l'infini est défini comme étant le 0 de l'addition. Et quand Q est confondu avec P, la droite tangente à la courbe en P définit le point R = P + P = 2P. Notamment, la somme de trois points P, Q, R est égale au point 0 si et seulement si ces trois points sont alignés.

Muni de cette addition, l'ensemble des points de la courbe elliptique forme un groupe additif (structure algébrique munie d'une addition, supposée associative, où il existe un élément neutre noté 0 et où chaque élément a possède un inverse a' tel que $a + a' = 0$).

Une courbe elliptique peut aussi être considérée sur un corps F différent de celui des nombres réels *(voir la figure 2)*. Dans ce cas, les paramètres u et v sont des éléments de F et le groupe E(F) des points de la courbe elliptique E est formé des solutions (x, y) de l'équation $y^2 = x^3 + ux + v$ considérée dans le corps F, auquel on adjoint un point à l'infini 0.

Signalons que les courbes elliptiques ont joué un rôle central dans la preuve par Andrew Wiles du « grand théorème de Fermat », selon lequel il n'existe pas d'entiers strictement positifs a, b, c tels que $a^n + b^n = c^n$ pour un entier n supérieur à 2.



la multiplication sur l'addition). C'est un exemple de ce qu'on appelle en mathématiques un corps *(voir l'encadré page 27)*; et comme il n'a qu'un nombre fini d'éléments, on dit que c'est un corps fini.

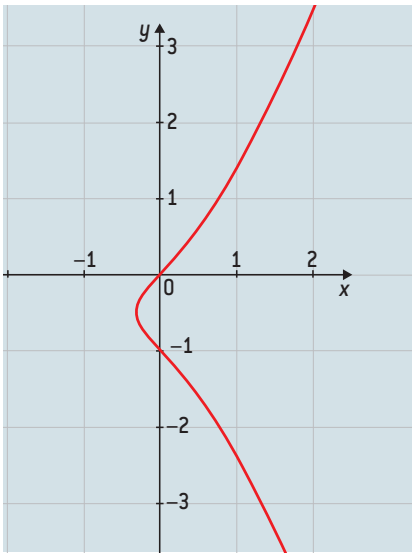
Dans sa note, Galois explique ensuite un certain nombre des propriétés de ces corps finis. Il commence par démontrer que dans un corps fini ayant p^d éléments, tout élément a vérifie $a^{(p^d)} = a$; cela généralise la congruence classique, dénommée « petit théorème de Fermat », selon laquelle $a^p \equiv a \pmod p$ pour tout entier a et tout nombre premier p. Il démontre aussi qu'il existe une « racine primitive » de cette équation $a^{(p^d)} = a$, autrement dit un élément non nul a tel que la suite 0, 1, a, a^2, ..., $a^{(p^d-2)}$ décrive exactement le corps fini.

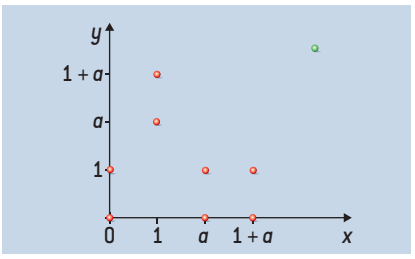
Pour construire un corps fini de « cardinal » p^d, c'est-à-dire ayant p^d éléments, par la méthode expliquée par Galois, il faut partir d'un polynôme F de degré d qui est irréductible modulo p. Galois explique alors qu'un tel polynôme est un facteur modulo p du polynôme $x^{(p^d)} - x$. Peu après, le mathématicien et astronome français Joseph Serret a démontré que l'on peut effectivement trouver un tel facteur, de sorte que, pour chaque puissance p^d d'un nombre premier p, il existe un corps fini de cardinal p^d. Et ce corps est même unique au sens où, pour deux corps finis de même cardinal (obtenus par exemple en suivant la construction de Galois pour deux polynômes F_1 et F_2), on a un dictionnaire reliant un à un les éléments des deux corps qui est compatible avec les règles de calcul (les mathématiciens disent que les deux corps sont isomorphes).

Des corps finis à la cryptographie

Dans les décennies qui ont suivi la note de Galois, plusieurs mathématiciens ont complété les travaux de Galois et formalisé la notion de corps telle qu'elle est présentée dans l'encadré page 27. À la mort de Gauss, en 1855, on a retrouvé un huitième chapitre de ses *Disquisitiones*, qu'il avait écrit en 1797 mais qui n'a été publié par le mathématicien allemand Richard Dedekind qu'en 1863. Dans ce texte, Gauss développait une théorie très proche de celle que Galois avait inventée.

La théorie des corps finis a rapidement montré son importance pour les mathématiques. C'en est aujourd'hui un outil crucial, y compris dans des domaines qui, à





2. L'ÉQUATION D'UNE COURBE plane est de la forme $f(x, y) = 0$, à l'instar de l'équation $y^2 + y = x^3 + x^2 + x$ de la courbe elliptique ci-contre. Mais une telle équation peut aussi être considérée dans un corps fini, et non sur le corps des nombres réels. Ainsi, dans le corps à $4 = 2^2$ éléments ($p = 2$, $d = 2$) formés par les polynômes 0, 1, a et $1 + a$ (où l'on a $1 + 1 = 0$ et $a^2 = a + 1$), la courbe elliptique considérée possède huit points *(graphe ci-dessus)* en plus du point 0 à l'infini *(en vert)*.

première vue, semblent ne pas relever de l'arithmétique tels que la théorie des fonctions automorphes et le programme de Langlands (un grand ensemble de conjectures techniques liant algèbre, théorie des fonctions et théorie des nombres).

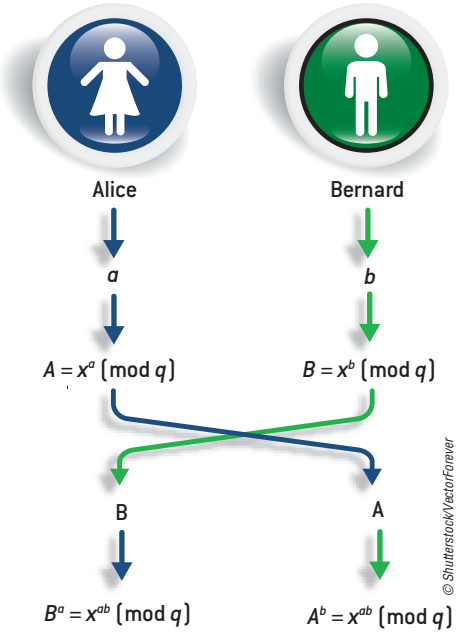
Les corps finis sont aussi au cœur des télécommunications modernes et des mécanismes intimes du réseau Internet, en particulier dans tout ce qui touche à la sécurité du commerce électronique. Lorsque vous achetez en ligne un livre, un disque ou un appareil photo, vient inévitablement le moment du paiement où il vous faut transmettre votre numéro de carte bancaire. Évidemment, vous aimeriez être certain qu'aucune personne non autorisée ne puisse obtenir ce numéro et l'utiliser à son profit. On est ainsi face à un problème classique de cryptographie : transmettre un message à son destinataire, et que seul ce dernier puisse en avoir connaissance.

Jusque vers 1975, les seuls procédés connus de cryptographie étaient symétriques. L'émetteur et le destinataire conviennent d'un code secret, lequel sert aussi bien à coder un message qu'à le décoder. Dans sa *Vie des douze Césars*, l'historien romain Suétone écrivait à propos de Jules César qu'il « y employait, pour les choses tout à fait secrètes, une espèce de chiffre qui en rendait le sens inintelligible (les lettres étant disposées de manière à ne pouvoir jamais former un mot), et qui consistait, je le dis pour ceux qui voudront les déchiffrer, à changer le rang des lettres dans l'alphabet, en écrivant la quatrième pour la première, c'est-à-dire le d pour le a, et ainsi de suite ». Comme le suggère très bien Suétone, si vous savez comment Jules César procède pour coder un message, vous êtes aussitôt en mesure de déchiffrer un message qu'il a écrit, même si vous n'en êtes pas le destinataire.

Un tel mécanisme n'est pas très utile pour le commerce en ligne puisqu'un site Web ne peut pas matériellement prendre contact avec tous ses clients potentiels et convenir, avec chacun d'entre eux, d'un tel code secret. En 1976, les Américains Whitfield Diffie, Martin Hellman et Ralph Merkle proposèrent un nouveau type de procédé, nommé aujourd'hui cryptographie asymétrique.

Dans ce schéma, n'importe qui est capable de coder des messages, mais seul son destinataire peut les décoder. Pour cela, le destinataire dispose de deux clefs ; l'une est connue de tous et permet de coder les messages, tandis que l'autre, qui permet de décoder les messages, est gardée secrète. En 1978, au MIT, Ronald Rivest, Adi Shamir et Leonard Adleman inventèrent un tel protocole, appelé depuis RSA et très largement utilisé aujourd'hui, y compris dans des consoles de jeu.

Du point de vue mathématique, on peut penser à la cryptographie comme à deux ensembles de symboles, celui des messages et celui des messages codés (un message étant alors une suite de symboles), et à deux applications, l'une qui transforme un symbole en un symbole codé et l'autre qui transforme un symbole codé en un symbole en clair. Dans le schéma de Jules César, les deux ensembles sont les lettres de l'alphabet (latin) ; la fonction qui code un message décale les lettres de trois crans vers la gauche, celle qui décode les décale de trois crans vers la droite.



© Shutterstock/VectorForever

3. LE PRINCIPE DE L'ÉCHANGE entre deux correspondants, nommés Alice et Bernard, permettant de définir en toute sécurité un secret commun représenté par $x^{ab} \pmod q$ (où q est le cardinal d'un corps fini et x une « racine primitive » de ce corps), les données x et q étant publiques.

Pour obtenir un protocole asymétrique pratique et fiable, il faut que la fonction de codage soit facile à calculer, mais qu'au contraire la fonction de décodage soit difficile à calculer si l'on ignore le code secret, même si l'on connaît la fonction de codage. Dans le cas d'une généralisation du chiffre de César où l'on permuterait les lettres d'une façon plus subtile qu'un simple décalage, il suffirait de 24 essais (le nombre de lettres de l'alphabet latin) pour savoir à quelle lettre correspond une lettre chiffrée. Cela prendrait donc juste un peu plus de temps de déchiffrer un message que de le crypter.

Mais lorsque l'ensemble des messages est très grand (10^{100} éléments, par exemple), il devient impossible de coder tous les messages possibles en espérant tomber sur un message chiffré donné : cela prendrait plus de temps que la durée de vie du Système solaire !

Face à ce problème, l'algèbre est potentiellement très utile, car se donner une formule est une façon très économique de définir une application, même entre ensembles gigantesques, et les corps finis fournissent de façon naturelle de tels ensembles tout en étant très faciles à construire.

LA THÉORIE DE GALOIS IRRIGUE

une grande partie des mathématiques d'aujourd'hui, de la théorie des nombres à celle des équations différentielles.

Dans cet ordre d'idées, expliquons comment, suivant W. Diffie et M. Hellman, deux individus, que nous appellerons Alice et Bernard, peuvent convenir d'un code secret même si Charles espionne leur conversation.

Pour cela, nos deux amis choisissent un corps fini, de cardinal q, ainsi qu'une racine primitive x (c'est-à-dire un élément x tel que la suite 0, 1, x, x^2, ..., x^{q-2} décrive tous les éléments du corps).

Alice et Bernard commencent par choisir chacun un nombre entier compris entre 1 et $q - 1$, sans le divulguer. Supposons qu'Alice ait choisi l'entier a et que Bernard ait choisi l'entier b. Alice communique alors à Bernard la valeur de x^a, tandis que Bernard communique à sa correspondante la valeur de x^b. Il est important de remarquer que, bien que x^a soit défini comme le produit de a facteurs égaux à x, un tel produit peut être calculé très rapidement *(voir page 28, en haut)*. Alice calcule alors $(x^b)^a$ dans le corps fini, et Bernard calcule $(x^a)^b$. Ainsi, les deux ont pu calculer l'élément x^{ab}, qui sera leur secret commun *(voir la figure 3)*.

Imaginons que Charles ait espionné tout l'échange entre Alice et Bernard ; il connaît donc x, x^a et x^b. L'efficacité du système repose sur le fait que personne ne sait efficacement calculer x^{ab} à partir de ces données. Une solution consisterait à retrouver la valeur de a ; c'est ce qu'on appelle le problème du « logarithme discret », a étant en quelque sorte le logarithme en base x de x^a. La méthode évidente pour ce faire consiste à calculer successivement x^2, x^3, etc., jusqu'à ce qu'apparaisse la valeur x^a ; mais, si a est choisi très grand, elle n'a aucune chance d'aboutir avant l'extinction du Soleil... Il existe cependant d'autres méthodes, plus subtiles et un peu plus efficaces. Pour que le système de communication secrète soit sûr, l'existence de ces méthodes impose que $q - 1$ ait au moins un facteur premier de très grande taille.

On gagne un peu en sécurité et en souplesse en remplaçant le calcul dans un corps fini par un calcul dans une structure algébrique plus compliquée. L'une des méthodes en vue consiste à utiliser le groupe des points d'une courbe elliptique définie sur un corps fini *(voir l'encadré page 28 et les figures 1 et 2)*. En d'autres termes, on se donne un corps fini assez grand F, une courbe elliptique E définie par une équation dont les coefficients appartiennent à F et un point P de cette courbe (dont les coordonnées appartiennent à F). L'intérêt des courbes elliptiques est que l'on peut y définir une addition entre points. Comme précédemment, Alice et Bernard choisissent des entiers a et b, calculent l'une aP et l'autre bP ; leur secret commun est le point ($a\,b$)P de la courbe E.

De tels protocoles sont implantés dans tous les systèmes de télécommunications modernes et témoignent de l'actualité de l'œuvre de Galois. Mais l'héritage de Galois est loin de se réduire au cryptage et au codage de données. Ce que l'on nomme aujourd'hui théorie de Galois est un édifice complexe qui irrigue une bonne partie des recherches mathématiques modernes, de la théorie des nombres à celle des équations différentielles, en passant par la géométrie algébrique et le programme de Langlands, dont la démonstration du célèbre théorème de Fermat constitue une retombée. ■

✔ BIBLIOGRAPHIE

N. Verdier, **Galois, le mathématicien maudit**, Belin-Pour la Science, 2011.

C. Ehrhardt, **Évariste Galois, la fabrication d'une icône mathématique**, Éditions de l'EHESS, à paraître, octobre 2011.

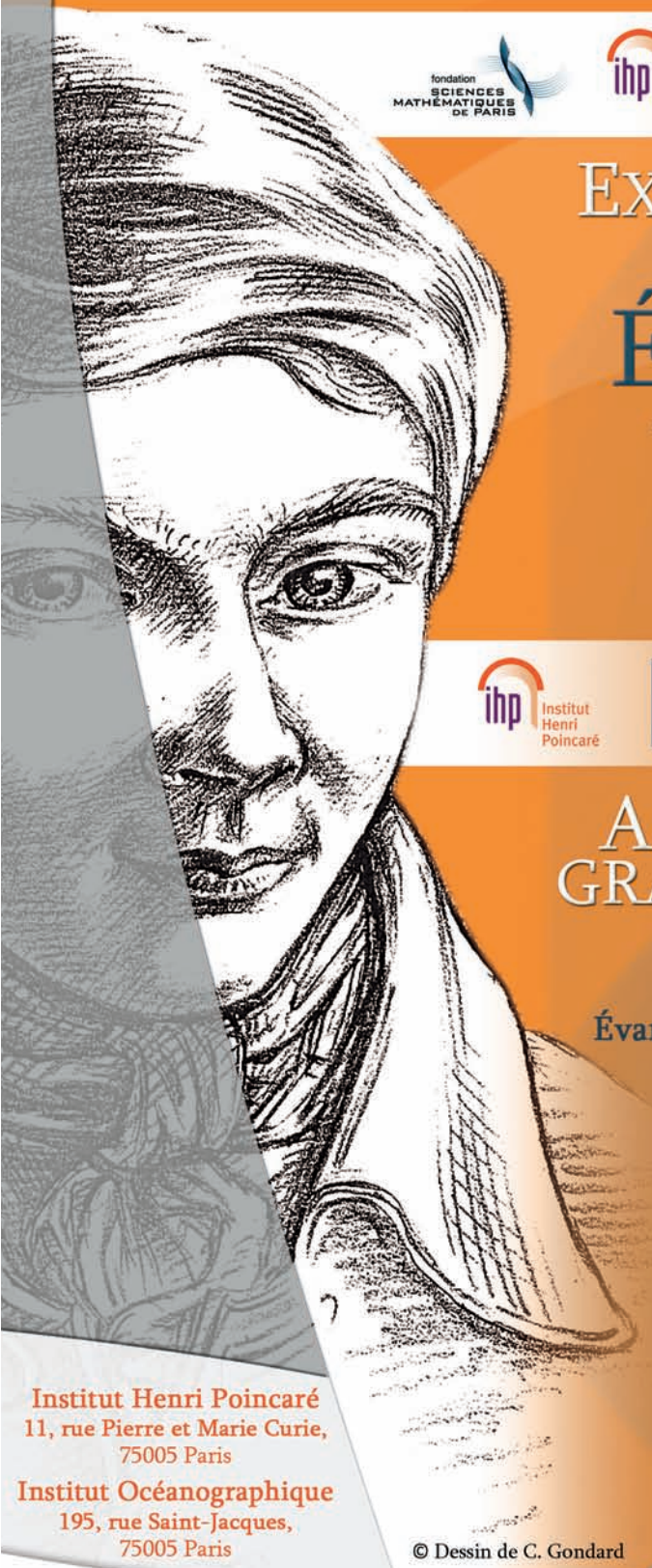
P. Pesic, **Abel, Galois et les équations algébriques**, *Pour la Science*, n° 366, avril 2008.

R. Langlands, **Le programme de Langlands**, *Pour la Science*, n° 361, novembre 2007.

A. Chambert-Loir, **Algèbre corporelle**, Éditions de l'École Polytechnique, 2005.

L'art du secret, *Dossier Pour la Science*, n° 36, juillet-octobre 2002.

Bicentenaire de la naissance d'Évariste Galois



du 17 octobre au 25 novembre 2011

EXPOSITION à la Bibliothèque de l'Institut Henri Poincaré

Évariste Galois : un mathématicien dans l'histoire

Commissaire scientifique de l'exposition : C. Ehrardt

Mercredi 26 octobre 2011

APRÈS-MIDI GRAND PUBLIC à l'Institut Océanographique

Projection du téléfilm de A. Astruc sur la vie de Galois

Exposé de B. Belhoste :
Évariste Galois, sa vie et son environnement scientifique

Exposé de V. Robert :
Les amis républicains d'Évariste Galois

Exposé de P. Cartier :
Les idées galoisiennes

Une table ronde sur le thème :
Galois et la figure du génie romantique en mathématiques

Spectacle des clowns scientifiques de la compagnie L'île logique
Pilouface, quand les clowns tombent sur la tranche...

Institut Henri Poincaré
11, rue Pierre et Marie Curie,
75005 Paris

Institut Océanographique
195, rue Saint-Jacques,
75005 Paris

© Dessin de C. Gondard

www.galois.ihp.fr

L'évolution de l'œil

Nos lointains ancêtres auraient été dotés d'un proto-œil qui captait la lumière, mais ne permettait pas de voir. Ensuite, l'œil a acquis des caractéristiques qui lui ont conféré la vision. Cette évolution aurait été très rapide : à peine 100 millions d'années.

Trevor Lamb

L'ESSENTIEL

✔ Les yeux des vertébrés sont très élaborés : ils captent la lumière et la focalisent sur la rétine, laquelle transmet des signaux qui sont traités et interprétés par le cerveau.

✔ L'étude comparative des composants de l'œil et de sa formation chez des poissons primitifs (lamproies et myxines) nous renseigne sur l'origine de cet organe complexe.

✔ Avant de devenir un organe visuel, l'œil de nos lointains ancêtres fonctionnait comme un détecteur de lumière qui imposait les rythmes circadiens.

Ci-dessus : © Shutterstock/Andrei Nekrassov

L'œil humain est un appareil photo perfectionné. Il collecte la lumière, la focalise et la convertit en signaux électriques que le cerveau traduit en images. C'est la rétine qui détecte la lumière et traite les signaux reçus au moyen de dizaines de types différents de neurones. L'œil est si élaboré que les créationnistes l'ont utilisé comme exemple du concept de « complexité irréductible », selon lequel un système si perfectionné n'a pu évoluer naturellement à partir d'une forme ancestrale. De fait, Charles Darwin lui-même, le père de la théorie de l'évolution, reconnaissait dans son ouvrage *De l'origine des espèces*, publié en 1859, qu'il pouvait paraître absurde de penser que l'œil s'était formé au gré de processus évolutifs. Toutefois, il était convaincu que l'œil s'était transformé progressivement, et ce malgré l'absence de preuves de l'existence de formes évolutives intermédiaires.

Les preuves directes se sont fait attendre. En effet, si les paléontologues peuvent étudier facilement l'évolution des os grâce aux squelettes fossilisés, c'est beaucoup plus difficile pour les tissus mous, tels les yeux, dont les fossiles sont rarissimes. Et même quand ils retrouvent des fossiles, cela ne leur permet pas de déterminer comment les structures ont évolué, car il n'y a pas assez de détails. Toutefois, les biologistes ont récemment précisé l'origine de l'œil, en étudiant comment il se développe chez les embryons et en comparant les structures de l'œil de différentes espèces ainsi que les gènes impliqués. Ils ont ainsi reconstitué le moment où sont apparues ses principales caractéristiques. Ainsi, il a fallu moins d'une centaine de millions d'années pour que l'œil des vertébrés s'élabore.

b

© Shutterstock/Waddell Images

a

© Shutterstock/Mikhail Melnikov