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.

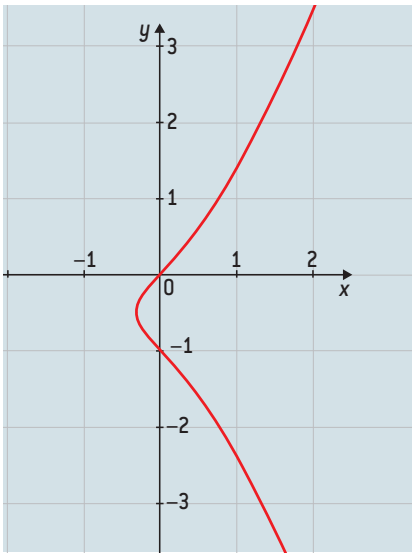
Dans sa note, Galois explique ensuite un certain nombre des propriétés de ces corps finis. Il commence par démontrer que dans un corps fini ayant p^d éléments, tout élément a vérifie $a^{(p^d)} = a$; cela généralise la congruence classique, dénommée « petit théorème de Fermat », selon laquelle $a^p \equiv a \pmod p$ 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.

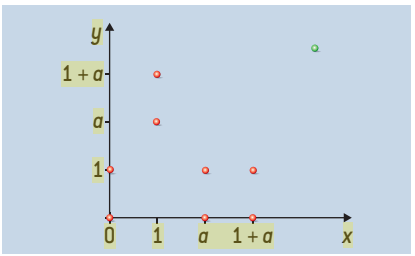
Pour construire un corps fini de « cardinal » p^d, c'est-à-dire ayant p^d éléments, par la méthode expliquée par Galois, il faut partir d'un polynôme F de degré d qui est irréductible modulo p. Galois explique alors qu'un tel polynôme est un facteur modulo p du polynôme $x^{(p^d)} - x$. Peu après, le 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).

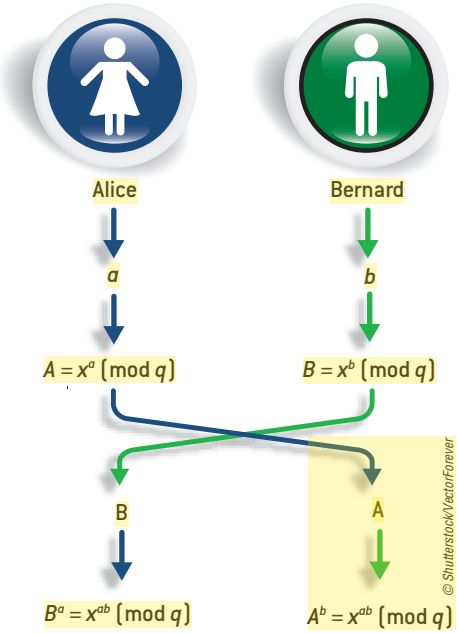
Les corps finis sont aussi au cœur des télécommunications modernes et des mécanismes intimes du réseau Internet, en particulier dans tout ce qui touche à la sécurité du commerce électronique. Lorsque vous achetez en ligne un livre, un disque ou un appareil photo, vient inévitablement le moment du paiement 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.



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.