l'algèbre
à travers les équations

par Jean-Paul Cardinal

[NDLR : texte écrit d'après l'enregistrement sonore de la conférence donnée au Palais de la découverte.]

Je vais vous présenter l'algèbre sous une forme historique parce que, à mon avis, c'est à travers son développement historique qu'on peut comprendre le mieux le développement d'une science.

d'où vient le mot "algèbre"

Beaucoup de gens savent que le mot *algèbre* est d'origine arabe. Les concepts les plus primitifs se retrouvaient déjà en Inde, à Babylone, en Grèce. Dans ces trois contrées, les mathématiques remontent à des temps très anciens. Et tout a convergé après le début de l'Islam. En 830, un astronome, Mohammed Al-Khwārizmī, a écrit un livre qui s'appelle « al jabr wal muqābala », où le mot *algèbre* apparaît pour la première fois.

al jabr signifie *restaurer* et l'autre terme signifie *simplifier*. Ce sont les deux opérations de base de l'algèbre.

Restaurer ça veut dire que quand vous avez une équation qui s'écrit, par exemple :

$$x^2 - 7 = 3$$

vous pouvez la réécrire sous une forme plus intéressante :

$$x^2 = 10.$$

Qu'est-ce que vous faites ? Vous avez une balance, une égalité, et si vous enlevez quelque chose d'un côté il faut le rajouter de l'autre, ou de façon plus rigoureuse : il faut rajouter + 7 de chaque côté.

Voilà la signification première du mot *algèbre*.

Simplifier ça veut dire que quand vous avez une expression algébrique (des expressions polynomiales comme $3\,x$ … $7\,x^2$ …), dans certains développements par exemple, vous pouvez regrouper les termes. Par exemple, quand vous avez $3\,x$ d'un côté et $7\,x$ plus loin vous les regroupez, ça fait $10\,x$.

le livre d'Al-Khwārizmī

Qu'est-ce qu'on trouve dans ce livre ? On y trouve une synthèse des équations algébriques de degré 1 ou 2.

Le degré 1, ce sont les équations de la forme $ax + b = 0$ (x étant l'inconnue) ; le degré 2 c'est le trinome que certains connaissent déjà :

$$a\,x^2 + b\,x + c = 0$$

On connaissait déjà des solutions partielles à ces équations dans l'antiquité, mais dans ce livre, c'est exposé d'une façon systématique et synthétique. Voilà un exemple d'équation de degré 2, qui se trouve dans le livre en question :

$$x^2 + 10\,x = 39.$$

Si je calcule $(x + 5)$ au carré, à gauche, ça fait

$$x^2 + 10\,x + 25$$

donc il faut que je rajoute 25 au membre de droite :

$$x^2 + 10\,x + 25 = 64$$

Ensuite, vous avez un carré de chaque côté :

$$(x + 5)^2 = 64\ (= 8^2)$$

vous prenez la racine, ça fait :

$$x + 5 = 8 \text{ (ou } x + 5 = - 8)$$

d'où

$$x = 3 \text{ (ou } x = - 13).$$

Vous voyez que l'équation du second degré est relativement simple à résoudre, au moins quand on la regarde sur cet exemple.

Et puisque vous savez résoudre une équation particulière comme ça, vous pourrez sans difficulté résoudre l'équation du second degré en général, celle qui figure un peu plus haut.

notations concises

Il faut comprendre que ce n'est pas sous cette forme que se présentaient les mathématiques. Il n'y avait pas de notation symbolique, tout était écrit en mots comme dans un livre de littérature. Cette écriture symbolique que vous connaissez, remonte à beaucoup plus tard dans le temps, à François Viète qui était un mathématicien français du seizième siècle, soit sept siècles après Al-Khwārizmī.

Mais à cette époque reculée, le problème ci-dessus s'énonçait :

quel doit être le carré qui,
quand on l'augmente de dix fois sa racine,
donne un montant de trente-neuf ?

tout ça, écrit en toutes lettres ; et la solution que je vous ai écrite :

vous diminuez de moitié le nombre de racines, ce qui donne cinq (on prend 10, on divise par 2, ça donne 5), *vous multipliez ce dernier par lui-même, ce qui donne vingt-cinq* (nous, on l'a fait de façon très concise), *ajouté à trente-neuf la somme est soixante-quatre, vous prenez la racine qui est huit et vous soustrayez la moitié du nombre de racines, qui est cinq, il reste trois.*

C'était donc très long à écrire. Et on n'a adopté la notation concise qu'à partir des années 1500-1600. C'est la notation qui est restée jusqu'à nos jours.

les équations polynomiales

Les équations polynomiales ont été le point de départ de l'algèbre. Ce sont les équations de la forme :

$$a_n\,x^n + a_{n-1}\,x^{n-1} + \ldots + a_2\,x^2 + a_1\,x + a_0 = 0$$

a_0, a_1, a_2, … sont des quantités données, x étant l'inconnue, et n le degré de l'équation.

C'est une généralisation des équations de degré 1 et 2. On peut imaginer une équation de degré 3, 4, etc. Ces équations ont vraiment été le moteur de l'algèbre à travers les siècles, jusqu'au siècle dernier.

La résolution de l'équation de degré 2 est connue depuis l'antiquité bien que le problème ait été repris par ce mathématicien arabe et toute l'école arabe. Les solutions se présentent sous cette forme :

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Vous voyez apparaître une racine carrée. Pour ceux qui ont vu ça au lycée, c'est bien connu, sinon on peut la retrouver, de façon simple comme dans l'exemple traité ci-dessus.

Pendant des centaines d'années, on était limité au degré 2, on ne savait pas résoudre les équations de degrés plus élevés. Et c'est au 16ème siècle, en Italie, qu'on a enfin pu résoudre l'équation de degré 3 :

$$x^3 + p\,\mathrm{x} + q = 0.$$

Plusieurs noms de mathématiciens sont attachés à cette résolution : Ferrari, Tartaglia et Cardan. A l'époque, les chercheurs en mathématiques ne publiaient pas leurs résultats comme aujourd'hui : on faisait des mathématiques pour s'amuser, c'étaient des challenges. Untel posait un problème de mathématiques à son adversaire, et l'autre devait résoudre le problème. A la clef, il y avait des sommes d'argent, des repas au restaurant, etc.

Les problèmes qui étaient en vogue à cette époque, étaient des problèmes de degré 2 ou 3, des équations polynomiales avec des coefficients précis, par exemple $x^3 + 10\,x + 4 = 0$. Et celui qui était en face devait donner les solutions.

[C'est un problème difficile, si vous voulez essayer de le résoudre vous même, vous verrez que c'est loin d'être évident, au moins pour le degré 3.]

Et quand quelqu'un connaissait une solution générale à un problème, il se gardait bien de la divulguer ou de la diffuser. Aujourd'hui, au contraire, on est vraiment encouragé à diffuser ses résultats, à les publier. Mais à l'époque, ce n'était pas du tout le cas, les résolutions des problèmes, c'était gardé secret : ça permettait de gagner des concours.

C'est Tartaglia qui a résolu cette équation de degré 3 : on lui avait posé plusieurs dizaines d'équations de degré 3 à résoudre et comme c'était impossible à faire en tâtonnant comme c'était alors l'habitude, il a imaginé une solution, pour la première fois, ce qui était un véritable tour de force, pour résoudre l'équation générale de degré 3.

Cardan était médecin, astrologue, mathématicien. Il s'est intéressé à ces questions, et il a insisté pour que Tartaglia lui donne la solution, jusqu'alors gardée secrète. Tartaglia la lui a donnée, en lui faisant jurer de ne répéter cette solution à personne. Mais juste après avoir eu la solution de Tartaglia,

$$\boxed{\sqrt[3]{\sqrt{\frac{p^3}{27} + \frac{q^2}{4}} + \frac{q}{2}} - \sqrt[3]{\sqrt{\frac{p^3}{27} + \frac{q^2}{4}} - \frac{q}{2}}}$$

Cardan s'est empressé de la publier dans un livre … vous voyez qu'ils n'étaient pas toujours très honnêtes à l'époque.

Ce livre s'appelle *Ars Magna*, et vous voyez l'injustice des gens, puisque maintenant cette formule s'appelle *Formule de Cardan*, alors qu'évidemment, on devrait l'appeler *Formule de Tartaglia*. Ce n'est absolument pas Cardan qui a trouvé cette solution.

Vous pouvez résoudre l'équation de degré 3 en général : il vous suffit de retenir la formule encadrée, c'est l'équivalent de la formule de résolution de l'équation du second degré.

Ici vous avez quelque chose de similaire, bien qu'un peu plus compliqué, pour le degré 3. On voit apparaître des racines cubiques puisque l'équation est de degré 3.

Ce livre a eu un retentissement extraordinaire à l'époque : c'est la première fois, en 1547, qu'on a fait quelque chose de mieux que les Anciens, c'est-à-dire les Grecs.

La mathématique grecque était très développée, en géométrie, en algèbre aussi, d'une certaine façon, et là, c'est la première fois qu'il y eut une nouveauté en mathématiques, un vrai problème difficile, quinze cents ans après Jésus-Christ.

Le degré 4 a aussi été résolu à la même époque, par le domestique de Cardan. Les domestiques travaillaient avec leurs maîtres. Ferrari est entré à l'âge de quatorze ans dans la maison de Jérôme Cardan. Il s'est mis tout de suite à faire des maths et, quelques années après, il a résolu l'équation de degré 4, résolution qui figure dans ce même livre *Ars Magna*, où il est bien mentionné que la solution a été trouvée par Ludovico Ferrari.

En quelques années, on avait réussi à résoudre le degré 3 et le degré 4 !

les nombres complexes

A cette époque, il est apparu quelque chose d'un peu bizarre. Voilà un exemple. Je donne une équation de degré 3 :

$$x^3 = 15\,x + 4$$

Si je veux appliquer la formule "de Cardan", je n'ai qu'à remplacer *p* par - 15 et *q* par - 4 ; c'est très simple, on applique la formule, et on a la solution. Mais si je fais ça sur cette équation, il apparaît un nombre négatif sous la racine carrée. Prendre la racine cubique d'un nombre négatif, ça ne pose pas de problème, mais la racine carrée d'un nombre négatif … ça pose un problème.

Et pourtant, si vous traitez cette équation en tâtonnant, vous voyez qu'elle a des solutions, par exemple, x = 4 … Pour arriver à cette solution avec la formule de Cardan, il y a une espèce de tour de passe-passe, qui ne gênait pas les algébristes d'alors.

Ils se sont dit : on va chercher la racine cubique de 2 + *cette chose bizarre* $\sqrt{-121}$. Je vous la donne, cette racine cubique c'est :

$$2 + \sqrt{-1}.$$

En effet, si vous élevez au cube cette somme de deux termes, vous développez ce cube :

$$2^3 + 3.2^2.\sqrt{-1} + 3.2.(\sqrt{-1})^2 + (\sqrt{-1})^3$$

vous obtenez

$$2 + 11\sqrt{-1}$$

qui est bien $2 + \sqrt{-121}$ parce que $11^2 = 121$ et on sort de la racine le 121 qui est un carré. Donc la racine cubique de ce que je cherche, je l'ai, sans difficulté, et si j'applique la formule de Cardan, sans réfléchir, j'ai bien :

$$2 + \sqrt{-1} \;+\; 2 - \sqrt{-1}$$

et ça fait bien 4.

Ainsi, en manipulant des expressions qui n'avaient pas de sens à l'époque, comme $\sqrt{-1}$, on arrive quand même à donner les solutions.

Evidemment, beaucoup de gens ont médité sur cette question profonde. [Pour ceux qui sont maintenant en Terminale, $\sqrt{-1}$ c'est le nombre *i*, c'est un nombre complexe, un nombre imaginaire.] Pendant des siècles, on a eu du mal à accepter que ces nombres existent vraiment. Même au XVIII° siècle, il y avait des gens qui avaient du mal à l'admettre. Mais en mathématiques on est obligé de progresser comme ça, de façon audacieuse, on a besoin d'introduire des nombres nouveaux.

Vous connaissez les rationnels, les nombres relatifs, ce sont des classes de nombres qui s'emboîtent les unes dans les autres, et c'est au travers des équations algébriques que toutes ces classes ont vu le jour, ont été imaginées par les mathématiciens. Ça c'est un nouvel aspect de l'algèbre : la création de nombres nouveaux.

les systèmes de nombres et les structures algébriques

Qu'est-ce qu'un système de nombres ? Le premier système pour faire des mathématiques c'est l'ensemble des entiers, N. Les entiers : 0, 1, 2, 3, 4, 5 … Cet ensemble, lorsqu'on le munit de deux lois, une addition et une multiplication, (c'est-à-dire je peux additionner ou multiplier des nombres entre eux) on l'appelle une structure algébrique.

Une structure algébrique, c'est un ensemble muni de lois.

N, c'est le tout premier ensemble, muni des lois + et ×. Mais malheureusement, l'équation $x + 2 = 0$ n'admet pas de solution : il n'y a pas d'entier (positif) x tel que $x + 2 = 0$. C'est ce qui a conduit les gens à inventer un nouvel ensemble de nombres qui est l'ensemble des entiers relatifs, Z. Là, $x + 2 = 0$ possède une solution, c'est - 2.

Et malheureusement il y a encore d'autres équations comme $3x + 2 = 0$ qui n'ont pas de solutions dans Z. Donc, nouvel ensemble à imaginer, l'ensemble des rationnels, Q, c'est-à-dire toutes les fractions : 3/7, - 2/5, … avec ça vous pouvez résoudre toutes les équations du premier degré :

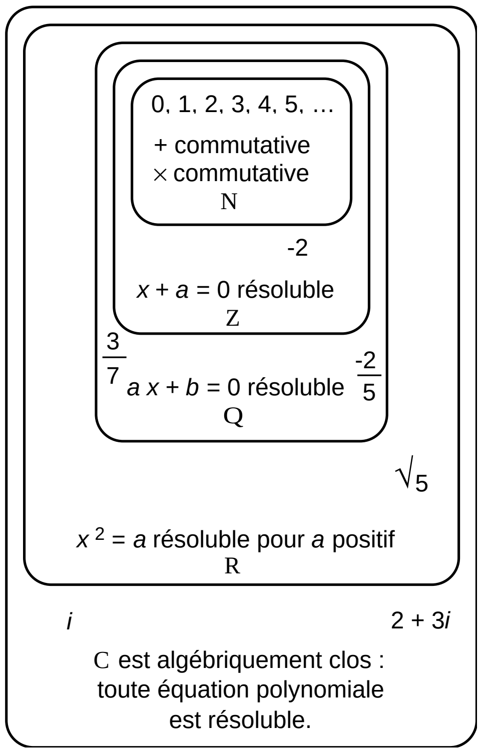
$$ax + b = 0 \ (a \in \mathrm{Q}^*, b \in \mathrm{Q}).$$

Et, pas de chance encore, une équation comme $x^2 - 5 = 0$ n'a pas de solution dans les rationnels. $\sqrt{5}$ n'est pas rationnel. On a donc inventé R, qui est un peu plus difficile à construire. Ce sont les nombres que vous avez l'habitude d'utiliser. Quand vous voyez une droite, vous pensez à R : vous placez 0 et 1 et alors vous pouvez placer n'importe quel nombre réel.

Z, avec ses deux lois, est un *anneau* (c'est une structure algébrique dont je ne donne pas le détail) ; Q est un *corps* (on peut faire des divisions, sauf par 0 ; on ne peut pas toujours diviser deux entiers entre eux, mais on peut toujours diviser deux rationnels entre eux, faire le rapport de deux fractions) ; de même, R est un corps (on peut toujours diviser comme on veut dans R, sauf par 0). En progressant de cette façon, on obtient des ensembles de plus en plus sophistiqués, de plus en plus gros.

Là encore, dans R, il y a une difficulté : l'équation $x^2 + 1 = 0$ n'a pas de solution (c'est le problème de tout à l'heure, celui de $\sqrt{-1}$). [On se demande quand on va s'arrêter …] Enfin, on construit le corps C, l'ensemble des nombres qui s'écrivent $a + i\,b$ où a et b sont des réels et i^2 vaut -1.

Et là enfin, on peut s'arrêter parce que C *est algébriquement clos*. Toutes les équations polynomiales à coefficients complexes ont des solutions. On n'a pas besoin d'aller chercher un ensemble de nombres encore plus sophistiqué. C'est ce qu'on appelle le *théorème fondamental de l'algèbre*, qui remonte à Gauss, d'Alembert. On a fait des constructions successives, et enfin, on a pu s'arrêter.



[Mais attention, il existe des équations non algébriques, comme $2^x = 0$, qui n'ont pas de solution complexe. On fait de l'algèbre, ça signifie qu'on manipule des polynômes.]

Des gens se sont amusés à construire des systèmes de nombres encore plus compliqués comme les *quaternions*. C'est comme les complexes, en un peu plus compliqué : au lieu d'avoir deux réels on en a quatre. Et il y a des règles comme $i^2 = -1$, ici c'est un peu plus compliqué, vous avez i, j, k qui obéissent à certaines règles qui ont été découvertes par Hamilton au dix-neuvième siècle.

Il y a aussi les *octonions*, les *hypernombres*, etc. On peut imaginer tout ce qu'on veut, mais il faut quand même que les choses servent dans la pratique, à résoudre des vrais problèmes scientifiques, en physique, en informatique. Les complexes, c'est universel ; les quaternions s'utilisent aussi beaucoup.

Et il y a d'autres ensembles : les *corps finis*. [Vous savez que R et C sont des corps, qui ont une infinité d'éléments.] Vous avez des *espaces vectoriels*, des *modules*, des *algèbres*, toutes sortes de structures algébriques qui sont utiles pour résoudre des problèmes scientifiques.

l'équation de degré 5

Pendant 250 années, on marque une pause. Après avoir résolu les équations de degrés 3 et 4, les gens se sont dit : on va résoudre l'équation de degré 5. Et là il y a eu un problème. De Cardan jusqu'à Lagrange, on n'a pas réussi à résoudre l'équation de degré 5. Mais personne ne doutait qu'on puisse le faire un beau jour, c'était simplement … plus compliqué.

Vers les années 1820, un jeune mathématicien norvégien a apporté une réponse tout à fait étonnante à ce problème : il a montré qu'*il n'y a pas de formule pour le degré 5*, avec des racines cubiques, des racines quatrièmes ou des racines cinquièmes … Lagrange avait déjà soupçonné qu'il y aurait un problème, mais c'est Abel qui a montré de façon précise qu'il n'y a pas de formule comme on en avait pour le degré 3. [Donc ne cherchez pas, c'est tout à fait impossible à résoudre *de façon générale*.]

Mais il y a quand même des équations particulières qui peuvent se résoudre avec des formules, comme :

$$x^5 - 1 = 0$$

et de façon générale

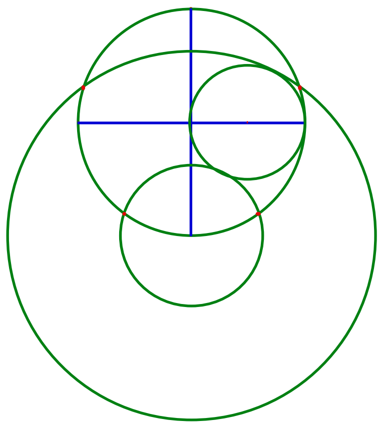
$$x^p - 1 = 0$$

Ces dernières équations se retrouvent dans un problème géométrique, celui de la construction d'un polygone régulier à la règle et au compas.

vous disposez d'une règle non graduée et d'un compas

Vous pouvez construire des objets géométriques comme une droite (plutôt un *morceau* de droite), un cercle ; pour une droite donnée, vous pouvez trouver une parallèle, une perpendiculaire. On peut faire tout ça avec une règle et un compas.

On peut construire un carré, sur une feuille non quadrillée bien sûr. C'est plus difficile, par exemple de construire un pentagone régulier. Les Grecs savaient le faire.



Mais on ne peut pas construire le polygone régulier à 7 côtés. Il y a des polygones qu'on peut construire, d'autres pas, c'est un peu difficile à comprendre. Mais on s'est aperçu à l'époque de Gauss que ce problème géométrique pouvait se réécrire en un problème algébrique.

Le problème algébrique, c'est tout simplement :

résoudre l'équation $x^p - 1 = 0$

p étant le nombre de côtés du polygone régulier à construire.

On s'est lancé dans l'exploration de ces équations, polynomiales, qu'on savait résoudre depuis l'antiquité pour $p = 3, 5, 15, 2^n$, etc. Et en 2000 ans, aucun nouveau polygone avec p premier, autre que le triangle et le pentagone, n'avait pu être construit à la règle et au compas. C'est Gauss, en 1799, qui a réussi à construire un nouveau polygone, de 17 côtés, à la règle et au compas. C'est beaucoup plus compliqué, c'est une construction très lourde.

Gauss était un des plus grands mathématiciens de tous les temps, et il a clairement compris que le problème était rattaché à un problème algébrique : il a montré qu'on pouvait construire tous les polygones réguliers où p est premier , et satisfait :

$$p = 2^{2^n} + 1$$

et on peut aussi multiplier de tels nombres entre eux, etc : mais si p est premier, il **doit** s'écrire sous cette forme.

$$2^{2^0} + 1 = 3$$
$$2^{2^1} + 1 = 5$$
$$2^{2^2} + 1 = 17$$
$$2^{2^3} + 1 = 257$$
etc ...

[mais $2^{2^5} + 1$ n'est pas premier : il est divisible par 641, et on se demande toujours s'il existe un nombre de la forme $2^{2^n} + 1$, autre que $2^{2^0}+1$, $2^{2^1}+1$, $2^{2^2}+1$, $2^{2^3}+1$ et $2^{2^4}+1$, qui soit premier lui aussi.]

On peut résoudre pour $p = 3, 5, 17$ et 257 mais pas pour 7, 11, 13, etc : il n'y a par exemple aucun moyen de construire à la règle et au compas un polygone régulier de 11 côtés.

Ça a relancé l'intérêt pour les équations algébriques : on voulait savoir quelles étaient les équations comme celles-ci qu'on pouvait résoudre.

les groupes

C'est Evariste Galois, un Français, qui est mort à 21 ans dans un duel, qui a apporté vraiment la réponse définitive à tous ces problèmes d'équations algébriques, en introduisant des concepts véritablement nouveaux et profonds comme la notion de *groupe*, ou de corps. On réécrit un problème numérique (comme une équation polynomiale) dans un langage de théorie des groupes, c'est assez abstrait mais c'est ce qui a permis de débloquer la situation complètement.

Le corps, vous en avez eu des exemples ; le groupe c'est aussi une structure algébrique, *a priori* plus simple, mais qui a vraiment pris de l'importance tardivement.

Qu'est-ce qu'un groupe ? Par exemple R muni de deux lois, c'est un corps. Mais quand je le regarde seulement muni de l'addition, c'est un groupe. Ça paraît a priori plus simple, mais en fait c'est une théorie difficile et vaste, simplement parce que, comme ils sont un peu plus simples que les corps, il en existe une grande variété. Voici un exemple :

Je considère l'équation

$$x^4 - x^2 - 2 = 0$$

C'est une équation bicarrée : il n'y a qu'un carré et une puissance 4. Je vous donne les solutions, et j'imagine que ces 4 solutions s'appellent x_1, x_2, x_3, x_4 ; la méthode de Galois, qui remonte aussi un peu à Lagrange, consiste à regarder les permutations des 4 lettres x_1, x_2, x_3, x_4 qui laissent invariantes les relations satisfaites par les racines :

$$x_1 = \sqrt{2}$$
$$x_2 = -\sqrt{2}$$
$$x_3 = i$$
$$x_4 = -i$$

Par exemple, $x_1 + x_2 = 0$, et $x_3 + x_4 = 0$. Ce sont deux relations et je vais chercher toutes les permutations qui ne changent pas ces relations. J'en donne juste une ou deux :

• La permutation identique ne change rien.

• Quand j'échange 4 et 3, je ne change pas la relation $x_3 + x_4 = 0$: si j'échange x_3 en x_4 et x_4 en x_3, ça vous donne $x_4 + x_3 = 0$, c'est la même chose.

Il y a des permutations qui changeraient les relations : si j'échange 1 et 3, ça ne marche plus. On peut échanger 1 et 2, 3 et 4, etc : il y a quelques permutations que je peux faire sans changer les deux relations qui sont données. Le groupe cherché est l'ensemble de ces huit permutations :

$$\boxed{\begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ x_1 & x_2 & x_3 & x_4 \end{array}} \qquad \boxed{\begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ x_3 & x_4 & x_1 & x_2 \end{array}}$$

id (1 3) (2 4)

$$\boxed{\begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ x_2 & x_1 & x_3 & x_4 \end{array}} \qquad \boxed{\begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ x_4 & x_3 & x_1 & x_2 \end{array}}$$

(1 2) (1 4 2 3)

$$\boxed{\begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ x_1 & x_2 & x_4 & x_3 \end{array}} \qquad \boxed{\begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ x_3 & x_4 & x_2 & x_1 \end{array}}$$

(3 4) (1 3 2 4)

$$\boxed{\begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ x_2 & x_1 & x_4 & x_3 \end{array}} \qquad \boxed{\begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ x_4 & x_3 & x_2 & x_1 \end{array}}$$

(1 2) (3 4) (1 4) (2 3)

Le groupe, c'est cet ensemble que j'appelle G, muni d'une loi : on ne peut pas ajouter des permutations, mais on peut les combiner. Si je fais une permutation, ensuite suivie d'une autre, ça me donne une nouvelle permutation. On appelle cette loi, le produit de deux permutations ; c'est noté sous forme d'un produit, qui n'est pas commutatif, attention : si vous combinez deux permutations dans un ordre et les deux mêmes dans l'autre ordre, ça ne donne pas le même résultat.

C'est donc un groupe non commutatif, il contient huit éléments, il possède une loi. Et c'est en regardant la structure de ce groupe, en comprenant bien comment il marche, comment les objets se combinent, que Galois a pu répondre à toutes les questions que se posaient les gens sur la résolution des équations par radicaux.

Dans ce petit exposé qui s'arrête vers 1830, toute l'algèbre que vous pourrez voir jusqu'au Bac et au-delà … est déjà présente. Ce que vous pouvez apprendre au lycée ou même en première année d'université, c'est … souvent des choses fondamentales, mais qui remontent à assez loin dans l'histoire de l'algèbre. Ainsi, la notion de groupe a presque 200 ans.

références :

Amy Dahan-Dalmedico et Jeanne Peiffer, *Routes et dédales*, Librairie Scientifique et Technique Albert Blanchard.

Mathématiques au fil des âges, textes choisis et commentés par J. Dhombres, A. Dahan-Dalmedico, R. Bkouche, C. Houzel et M. Guillemot, IREM, groupe épistémologie et histoire, publié chez Gauthier-Villars, © 1987.

Morris Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, New York, © 1972.

B. L. van der Waerden, *A History of Algebra*, Springer-Verlag, © 1985.