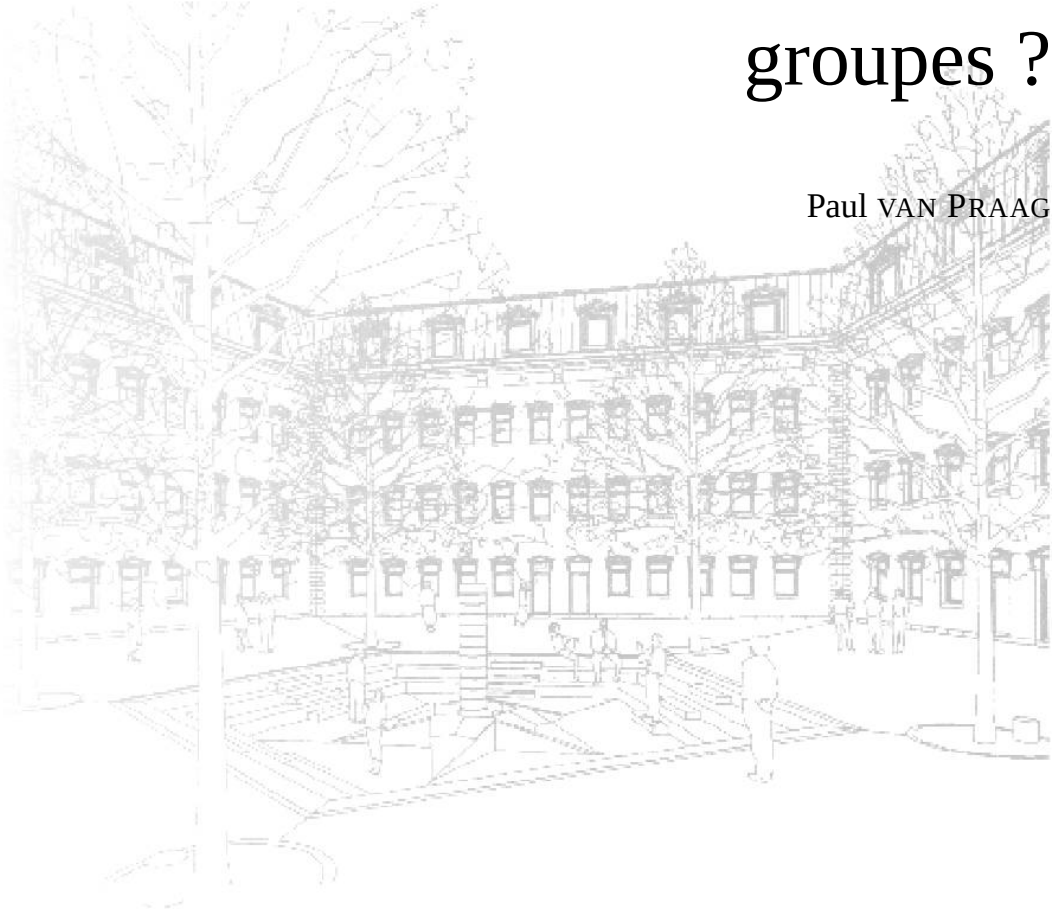
Cahier pédagodique #3
20 juin 2002

Pourquoi des nombres complexes ? Pourquoi des groupes ?

Paul VAN PRAAG



Université de Mons-Hainaut
Institut de Mathématique
Tél : +32 65 37 35 07 — Fax : +32 65 37 33 18
Web : http://www.umh.ac.be/math/institut

Pourquoi des nombres complexes ? Pourquoi des groupes ?

D'après un exposé fait le 28 mars 2002 à la Journée de Mathématique et de Sciences de l'UMH

Paul VAN PRAAG

Université de Mons-Hainaut
Institut de Mathématique
« Le Pentagone »
Avenue du Champ de Mars, 6
B-7000 Mons (Belgique)
paul.vanpraag@umh.ac.be

1 L'équation du second degré

1.1 Écrivons-la

$$x^2 + ax + b = 0 \tag{1}$$

sans trop préciser la nature des nombres a et b. On résoud des équations du premier et du second degré depuis des millénaires, en tout cas depuis les Babyloniens du début du deuxième millénaire avant Jésus-Christ, mais ce n'est que depuis les 16^{e} et 17^{e} siècles que zéro et les nombres négatifs sont traités de la même façon que les nombres (entiers ou rationnels) positifs. Ainsi il y avait une théorie pour l'équation $x^2 = ax + b$ et une autre pour l'équation $x^2 + ax = b$, a et b tous deux nombres entiers positifs ou fractions positives. Pour des motivations, voir par exemple [2].

Par la théorie d'al Khwarismi (début du 9^{e} siècle), l'équation (1) peut s'écrire successivement :

$$x^2 + 2\frac{a}{2}x + b = 0$$

$$x^2 + 2\frac{a}{2}x + \left(\frac{a}{2}\right)^2 - \left(\frac{a}{2}\right)^2 + b = 0$$

$$\left(x + \frac{a}{2}\right)^2 = \left(\frac{a}{2}\right)^2 - b$$

Pour continuer, on suppose que $(a/2)^2 \geqslant b$, puisque $(x+a/2)^2$ doit être un nombre positif.

Dès lors,

$$x+\frac{a}{2} = \pm\sqrt{\left(\frac{a}{2}\right)^2 - b}, \qquad \text{c'est-à-dire} \qquad x = -\frac{a}{2} \pm \sqrt{\left(\frac{a}{2}\right)^2 - b}. \tag{2}$$

Il y a deux racines, notons

$$x_1 := -\frac{a}{2} + \sqrt{\left(\frac{a}{2}\right)^2 - b} = \frac{1}{2}\left(-a + \sqrt{a^2-4b}\right) \tag{3}$$

$$\text{et} \quad x_2 := -\frac{a}{2} - \sqrt{\left(\frac{a}{2}\right)^2 - b} = \frac{1}{2}\left(-a - \sqrt{a^2-4b}\right). \tag{4}$$

On en déduit

$$x_1 + x_2 = -a \tag{5}$$

$$\text{et} \quad x_1 x_2 = b. \tag{6}$$

1.2 On a estimé avoir résolu l'équation (1) en écrivant (2), c'est-à-dire en exprimant les solutions de (1) à partir de nombres « connus » et de racines carrées de nombres connus, c'est-à-dire de solutions d'équations

$$x^2 = c. \tag{7}$$

Si tel est le but poursuivi, alors voici une autre façon de procéder : essayons de supprimer le terme en x dans (1) : posons $x = y + d$ et cherchons d pour lequel (1) prenne la forme (7) :

$$\begin{aligned} &(y+d)^2 + a(y+d) + b = 0, \\ &y^2 + (2d+a)y + (d^2 + ad + b) = 0 \end{aligned} \tag{8}$$

On doit donc avoir $2d + a = 0$, $d = -a/2$, et (8) devient

$$y^2 + \left(\frac{a}{2}\right)^2 - \frac{a^2}{2} + b = 0,$$

$$y^2 = \frac{a^2}{4} - b,$$

$$\left(x + \frac{a}{2}\right)^2 = \frac{a^2}{4} - b,$$

et on retrouve (2).

2 L'équation du troisième degré

Écrivons-la

$$x^3 + ax^2 + bx + c = 0. \tag{9}$$

En s'inspirant de 1.2, on peut supprimer dans (9) le terme en x^2 : on calcule qu'en posant

$$x = y - \frac{a}{3}, \tag{10}$$

l'équation (9) devient

$$y^3 + py + q = 0. \tag{11}$$

Voici une démarche des pères fondateurs (del Ferro, Tartaglia, Cardan (première moitié du 16e siècle)) : dans (10), remplaçons y par $u+v$:

$$(u+v)^3 + p(u+v) + q = 0$$
$$u^3 + 3u^2v + 3uv^2 + v^3 + p(u+v) + q = 0.$$

Si on trouve u et v pour lesquels

$$u^3 + v^3 = -q \tag{12}$$
$$\text{et} \quad 3uv + p = 0, \tag{13}$$

alors $u+v$ est solution de (11). Mais (13) implique

$$u^3v^3 = \left(\frac{-p}{3}\right)^3. \tag{14}$$

Les égalités (12) et (14) impliquent que u^3 et v^3 sont solutions de l'équation

$$z^2 + qz - \left(\frac{p}{3}\right)^3 = 0 \tag{15}$$

(en vertu de (5), (6) et (1)). On peut donc écrire :

$$u^3 = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^2} \qquad \text{et} \qquad v^3 = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^2},$$

d'où

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^2}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^2}}. \tag{16}$$

C'est la formule connue sous le nom de formule de del Ferro-Cardan-Tartaglia.

Ne nous préoccupons pas ici de la légitimité de la démarche, ni du fait que pour beaucoup de lecteurs une équation du troisième degré possède trois racines. Au 16e siècle,

on était content de présenter une solution, la solution, qui était souvent un nombre entier positif, connu à l'avance, comme nous allons le voir sur l'exemple suivant.

Cardan puis Bombelli furent interpellés par l'équation

$$x^3 = 15x + 4, \tag{17}$$

dont ils savaient que 4 est une racine. Mais si l'on veut appliquer la formule (16), alors $p = -15$ et $q = -4$, (16) donne alors

$$\sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}. \tag{18}$$

Au 16$^{\text{e}}$ siècle zéro pose un problème à beaucoup de mathématiciens, certains refusent non seulement le calcul sur les nombres négatifs mais aussi l'existence même de ces nombres. Que dire alors des racines carrées des nombres négatifs ? En 1572, Bombelli surmonte sa répulsion, écrit des nombres « a plus b (meno di memo) », aujourd'hui on écrit $a+bi$, et définit un calcul pour ces nombres : on calcule comme pour les nombres usuels, et lorsque l'on rencontre i^2, on remplace cette expression par -1.

Dès lors, par exemple,

$$(2+i)^3 = 2+11i$$
$$(2-i)^3 = 2-11i$$

d'où, en additionnant les racines cubiques,

$$4 = \sqrt[3]{2+11i} + \sqrt[3]{2-11i},$$

c'est-à-dire

$$4 = \sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}. \tag{19}$$

3 Les nombres complexes

Cette dernière démarche est l'origine des nombres complexes $a+bi$. La formule (16) avait fait ses preuves mais son application à l'équation (17) était paradoxale. Les nombres complexes résolvent le paradoxe. Mais grâce aux nombres complexes l'équation (1) possède toujours des solutions, deux si l'on compte d'une façon adéquate, même si

$$\left(\frac{a}{2}\right)^2 < b. \tag{20}$$

Sans le paradoxe, si on en était resté à l'équation du second degré et aux nombres usuels, on n'aurait probablement pas trouvé nécessaire d'inventer de nouveaux

nombres. La vie et les mathématiques sont remplies de problèmes sans solution et il suffirait de dire que sous l'hypothèse (20), l'équation (1) n'a pas de solution.

On constata qu'en acceptant les nombres complexes et en comptant les solutions d'une équation d'une façon adéquate, alors l'équation du 3^{e} degré possède 3 solutions et l'équation du 4^{e} degré, 4.

Girard conjectura au début du 17^{e} siècle qu'une équation du n^{e} degré possède n solutions. Gauss prouva cette conjecture tout à la fin du 18^{e} siècle. Dès le 18^{e} siècle, les nombres complexes s'étaient introduits dans le calcul intégral, et grâce aux développements en séries, Euler montra que ces nombres complexes permettent un lien entre la fonction exponentielle e^{x} et les fonctions trigonométriques sinus et cosinus : $e^{ix} = \cos x + i \sin x$. Il en déduisit la formule $e^{i\pi} = -1$ liant le nombre e (une aire définie par une hyperbole et liée aux logarithmes) et le nombre π (l'aire d'un cercle). À la fin du 18^{e} siècle et au début du 19^{e} siècle, ces nombres furent interprétés géométriquement : ainsi la multiplication par i s'interprète comme une rotation d'un quart de tour. Ils ont depuis lors envahi l'analyse mathématique, la géométrie et la théorie des nombres [14]. On définit proprement les nombres complexes, sous l'hypothèse d'avoir les nombres réels : ainsi pour Hamilton les nombres complexes sont les couples (a,b) de nombres réels munis des lois

$$(a,b)+(c,d) := (a+c, b+d) \quad \text{et} \quad (a,b)\cdot(c,d) := (ac-bd, ad+bc). \tag{21}$$

On vérifie que les couples $(a,0)$ se comportent comme les nombres a, et on identifie $(a,0)$ et a. Par (21) :

$$(0,1)^2 = -(1,0),$$

donc en posant $i := (0,1)$ tout nombre complexe s'écrit $a+bi$, avec $i^2 = -1$.

Cauchy montra qu'en s'intéressant aux restes de la division euclidienne du produit de deux polynômes par x^2+1, on retrouve les lois définissant les nombres complexes. Ainsi

$$(a+bx)(c+dx) = (x^2+1)bd + \big((ac-bd)+(ad+bc)x\big).$$

4 L'équation du second degré résolue dans une ambiance de bavardage

Reprenons le polynôme x^2+ax+b. Sans connaître 1.1, si l'on suppose qu'il possède deux zéros, x_1 et x_2, on peut prouver que

$$x^2+ax+b = (x-x_1)(x-x_2) = x^2-(x_1+x_2)x+x_1x_2. \tag{22}$$

On en déduit les égalités (5) et (6).

Cette déduction ne nécessite pas la connaissance des formules (3) et (4). En fait, nous aurions pu ignorer qu'il y a des racines. Nous pouvions donc ignorer s'il y a des racines, mais nous établissons que leur somme est $-a$ et leur produit b.

Les expressions x_1+x_2 et x_1x_2 sont très particulières : x_1 et x_2 y jouent exactement le même rôle : elles ne changent pas si l'on y permute x_1 et x_2. Par contre dans l'expression x_1+2x_2, x_1 et x_2 ne jouent pas le même rôle. Considérons l'expression

$$x_1-x_2. \tag{23}$$

Dans cette expression, x_1 et x_2 ne jouent pas le même rôle, mais si on y permute x_1 et x_2 elle se modifie d'une façon particulière : elle change de signe ; donc $(x_1-x_2)^2$ reste invariante par les permutations de x_1 et x_2. Remarquons alors que

$$(x_1-x_2)^2=(x_1+x_2)^2-4x_1x_2=a^2-4b \qquad \text{(par (5) et (6)).}$$

Donc

$$x_1-x_2=\pm\sqrt{a^2-4b} \tag{24}$$

Mais par (5) :

$$x_1+x_2=-a,$$

(5) et (24) forment donc un système de deux équations du premier degré à deux inconnues dont les solutions redonnent (2). On a donc retrouvé (2) en pensant à x_1-x_2 et en remarquant que si l'on y permute x_1 et x_2 cette expression bouge, mais pas trop.

5 Un procédé unique pour les équations de degré inférieur à 5.

Cherchons, comme Lagrange au 18$^{\text{e}}$ siècle (pour sa démarche originale, voir [11]), si nous pouvons pratiquer d'une façon analogue pour l'équation du troisième degré et envisageons que l'équation $x^3+px+q=0$ possède trois racines x_1, x_2 et x_3. Nous possédons à présent les nombres complexes. Puisque $x^3-1=(x-1)(x^2+x+1)$, l'équation $x^3=1$ possède trois racines : $1, \frac{1}{2}(-1+i\sqrt{3})=:\omega$, $\frac{1}{2}(-1-i\sqrt{3})=\omega^2$. Posons

$$L=x_1+\omega x_2+\omega^2 x_3,$$

en nous souvenant que l'expression x_1-x_2 est x_1+(une racine carrée bien choisie de 1)$\cdot x_2$. Regardons les valeurs que prend L lorsque l'on y permute x_1, x_2 et x_3. Tout

d'abord, quelles sont les permutations sur x_1, x_2 et x_3 ? Il y en a six : d'abord la permutation identique qui fixe chacun des x_i et que nous notons $1 := \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}$. Puis par exemple $c_1 := \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}$ qui applique x_1 sur x_2, x_2 sur x_3 et x_3 sur x_1. Puis

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix} =: c_2, \quad \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix} =: t_1, \quad \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix} =: t_2, \quad \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix} =: t_3.$$

On vérifie que par ces six permutations, L prend six valeurs. Mais introduisons

$$\Delta := (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

(qui jouera ici l'un des rôles de $x_1 - x_2$ pour l'équation du 2ème degré).

On vérifie que par les six permutations, Δ prend deux et seulement deux valeurs : Δ et $-\Delta$. Donc Δ^2 est invariant par les six permutations. On calcule (voir Appendice) que

$$\Delta^2 = -(27q^2 + 4p^3),$$

et dès lors

$$\Delta = \pm\sqrt{-(27q^2 + 4p^3)}.$$

Donc Δ a bougé, mais pas trop, et est alors une racine (carrée) d'une expression « connue » $-(27q^2 + 4p^3)$. Cherchons à présent les valeurs que prend L par les permutations sur x_1, x_2 et x_3 *qui conservent* Δ. On vérifie qu'il n'y a que trois telles permutations : 1, c_1 et c_2. Par ces trois permutations, L prend les formes :

$$L, \quad x_2 + \omega x_3 + \omega^2 x_1 = \omega^2 L, \quad \text{et} \quad x_3 + \omega x_1 + \omega^2 x_2 = \omega L.$$

On en déduit que L^3 est fixe par ces trois permutations (puisque $\omega^3 = 1$). On vérifie par un long calcul que L^3 s'exprime comme ceci en fonction de p, q et de Δ :

$$L^3 = -\frac{27}{2}q - \frac{3i}{2}\Delta.$$

Donc

$$L = \sqrt[3]{-\left(\frac{27}{2}q + \frac{3i}{2}\Delta\right)},$$

donc

$$x_1 + \omega x_2 + \omega^2 x_3 = \text{une racine cubique de quelque chose de connu.} \qquad (25)$$

On prouve de même que

$$x_1 + \omega^2 x_2 + \omega x_3 = \text{une racine cubique de quelque chose de connu.} \qquad (26)$$

Par un procédé analogue à (22), on écrit

$$x^3+px+q=(x-x_1)(x-x_2)(x-x_3)=x^3-(x_1+x_2+x_3)x^2+\cdots$$

Donc

$$x_1+x_2+x_3=0. \tag{27}$$

Les égalités (25), (26) et (27) forment un système de trois équations à trois inconnues dont la résolution donne (16). Dans cette démarche une remarque capitale est : le polynôme $(X-\Delta)(X+\Delta)$ est invariant par toutes les permutations sur $\{X_1,X_2,X_3\}$, le polynôme $(X-L)(X-\omega L)(X-\omega^2 L)$ est invariant par toutes les permutations de $\{X_1,X_2,X_3\}$ *qui laissent fixe* Δ.

Résumons ce que l'on a obtenu : par toutes les permutations de $\{X_1,X_2,X_3\}$, Δ prend deux valeurs, Δ est racine d'une équation du second degré. Par toutes les permutations de $\{x_1,x_2,x_3\}$ qui laissent Δ fixe, L prend trois valeurs, L est racine d'une équation du 3$^{\text{e}}$ degré, particulièrement bien choisie : L est racine cubique de quelque chose de « connu ». Avec cela, on résoud l'équation. Lagrange prouve alors qu'on peut procéder d'une façon analogue pour l'équation du 4$^{\text{e}}$ degré qui avait été résolue au 16$^{\text{e}}$ siècle par Ferrari.

Il avait trouvé une démarche longue mais unique pour résoudre les équations générales de degré 2, 3 et 4. Mais sa démarche ne fonctionne pas pour l'équation générale du 5$^{\text{e}}$ degré : dans ce cas l'expression analogue à L est solution d'une équation de degré 6 à coefficients connus et plus effrayante que l'équation du 5$^{\text{e}}$ degré. La **résolution par radicaux** (c'est-à-dire la recherche de formules donnant les racines et où n'interviennent que les coefficients de l'équation et les signes $+$, $-$, $\times$, $\div$, $\sqrt[p]{\ }$) de l'équation du 5$^{\text{e}}$ degré avait résisté à tous les efforts. Ce qui ne semblait pas dramatique puisque dès le 17$^{\text{e}}$ siècle étaient apparues des méthodes de résolution numérique qui donnent les solutions réelles avec l'approximation voulue.

6 Les groupes

6.1 Dans la démarche de Lagrange, nous avons vu apparaître les permutations : on étudie les valeurs que prennent certaines fonctions des racines par des permutations de ces racines. Ces permutations étaient un outil accessoire aux racines et aux fonctions sur les racines. On va maintenant étudier l'ensemble de ces permutations comme outil essentiel. Tout d'abord des notations.

Notons S_3 l'ensemble des six permutations sur $\{x_1,x_2,x_3\}$: $\{1,c_1,c_2,t_1,t_2,t_3\}$. On sait composer les permutations : si σ et τ sont des permutations, alors $\tau\circ\sigma$ est la

permutation qui applique tout x_i sur $\tau(\sigma(x_i))$. Ainsi

$$c_1 \circ t_1 = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix} \circ \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix} = t_3.$$

Lagrange s'intéressait aux permutations qui conservent une fonction des x_i, par exemple L^3. Ici, 1, c_1 et c_2 conservent L^3 ; t_1, t_2 et t_3 pas.

L'ensemble E_f des permutations qui conservent une fonction f a une propriété bien particulière : si σ et τ appartiennent à E_f, alors $\tau \circ \sigma$ aussi.

En effet :

$$\begin{aligned} \tau \circ \sigma(f) &= \tau(\sigma(f)) && \text{par définition du produit de composition des fonctions} \\ &= \tau(f) && \text{car } \sigma \in E_f \\ &= f && \text{car } \tau \in E_f \end{aligned}$$

Nous dirons *momentanément* (voir 6.3) qu'une partie E de S_3 est un *groupe de permutations* si et seulement si pour tous σ, $\tau \in E$, on a $\sigma \circ \tau \in E$.

Ainsi $\{1, c_1, c_2\}$, $\{1, t_1\}$, $\{1\}$, S_3, sont des groupes de permutations. Et $\{c_1, c_2\}$, $\{t_1\}$, $\{t_1, t_2, t_3\}$ ne sont pas des groupes de permutations.

Vers 1830, Galois associe à une équation $F = 0$ un groupe de permutations G et étudie les sous-ensembles de G qui sont des groupes. Ce sont les sous-groupes de G. Il met en évidence une propriété de certains sous-groupes de G, appelés aujourd'hui sous-groupes normaux, distingués, ou sous-groupes invariants de G et que l'on peut définir ainsi : ce sont les sous-groupes N de G pour lesquels si $n \in N$ et si $g \in G$, alors $g \circ n \circ g^{-1} \in N$. Dans les groupes étudiés par Galois, cette notion est liée à des questions très concrètes de résolubilité des équations. Il en déduit une condition sur G (l'existence de certains sous-groupes normaux) pour que l'équation $F = 0$ soit résoluble par radicaux. Lorsque cette condition est satisfaite, on retrouve comme conséquence de la théorie de Galois la démarche de Langrange, et *les sous-groupes concernés qui a priori ne sont que des sous-groupes de permutations, deviennent alors les sous-groupes de permutations qui conservent certaines fonctions.*

Galois déduit de sa théorie que pour $n > 4$, on ne peut pas « résoudre par radicaux » l'équation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, lorsque les a_i sont des « lettres ». Ce dernier résultat avait été prouvé par Abel pour $n = 5$, mais la condition de Galois est une condition nécessaire et suffisante sur G, que les a_i sont des « nombres » ou qu'ils soient des « lettres ». Ainsi on prouve par la théorie de Galois que l'équation $x^5 - 6x + 3 = 0$, qui possède bien cinq racines complexes, n'est pas résoluble par radicaux [10].

6.2 Indiscernabilité. En voulant résoudre une équation, on veut identifier chaque racine. Lorsque l'on a résolu l'équation, toutes ses racines sont discernables. Le pro-

cessus de Lagrange donne, par exemple pour l'équation du second degré la séquence suivante :
– Dans l'expression « $x_1 + x_2$ », x_1 et x_2 sont tout à fait indiscernables.
– Dans l'expression « $x_1 - x_2$ », x_1 et x_2 ne sont plus tout à fait indiscernables, mais ne sont pas totalement discernables.
– Dans les expressions « x_1 » et « x_2 » obtenues en fin de route, x_1 et x_2 sont tout à fait discernables.
Par la théorie de Galois, la séquence de Lagrange provient d'une suite de sous-groupes.

6.3 Plus haut, nous avons défini momentanément les groupes de permutations. Aujourd'hui, on appelle **groupe** un ensemble G muni d'une loi, notons-là $\cdot$,

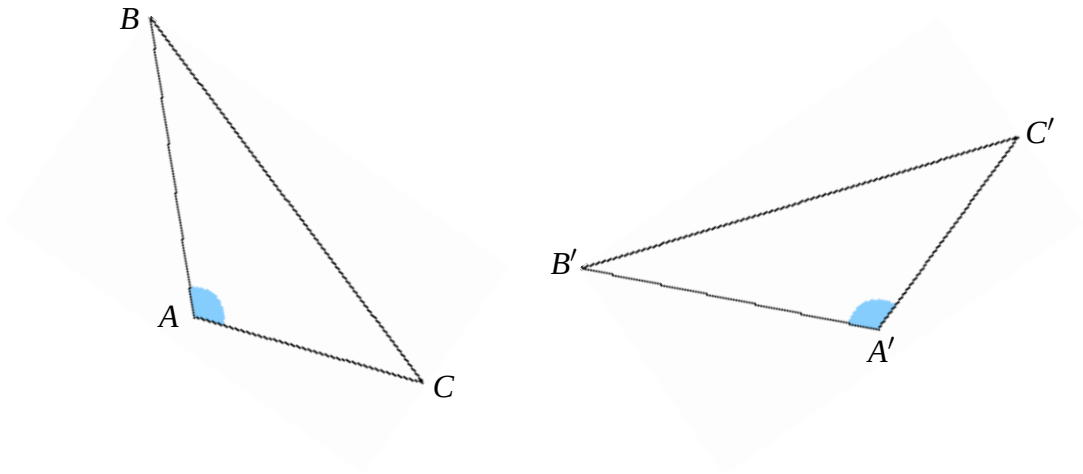
1. qui associe à tout couple (a,b) d'éléments de G un élément $a \cdot b$ de G,
2. telle que l'égalité $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ soit satisfaite pour tous les a, b, $c \in G$,
3. telle que G comprenne un élément 1 pour lequel $a \cdot 1 = a = 1 \cdot a$ pour tout $a \in G$,
4. telle que pour tout $a \in G$, il existe un unique élément $b \in G$ pour lequel $a \cdot b = 1 = b \cdot a$.

On peut prouver que si G est un ensemble de permutations sur un ensemble fini et si la loi sur G est la loi de composition $\circ$ des permutations, alors la condition 1 suffit à ce que G muni de $\circ$ soit un groupe. Mais il existe des groupes infinis de permutations (voir 7) et des groupes qui ne sont pas définis comme des groupes de permutations (mais qui le deviennent par un théorème de Cayley).

Remarque. En 4 et 5 les discussions s'effectuent dans une zone de flou : indiscernabilité des racines dont on ne sait pas très bien si elles existent, permutations sur ces racines conjecturées, expressions algébriques en des objets dont on ignore la nature, lettres et nombres. Aujourd'hui tout cela peut être défini dans un cadre considéré aujourd'hui comme clair.

7 Géométries et symétries

7.1 Changeons apparemment de sujet et plaçons-nous dans la géométrie usuelle du plan. Soient deux triangles



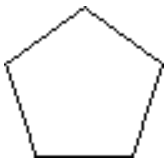
qui possèdent un angle « égal » compris entre deux côtés « égaux chacun à chacun ». Euclide (vers -300 avant J.C.) prouvait qu'ils sont « égaux » en appliquant le premier triangle sur le second. Cette pratique a été menée pendant longtemps avec mauvaise conscience : bouger le triangle, c'est faire de la physique (impure) et pas des mathématiques (pures). Il y avait d'une façon sous-jacente à cette pratique, l'idée que l'on bougeait le triangle de façon à conserver toutes les longueurs. Plus tard, on considèrera une transformation, bien choisie et bien définie mathématiquement, de tout le plan qui applique le premier triangle sur le second. Dans ce contexte, tout ce que l'on pourra dire du premier triangle, on pourra le dire du second, dans ce contexte les deux triangles sont indiscernables. On retrouve une situation où l'on a des objets indiscernables et où, lorsque deux objets sont indiscernables, une certaine permutation applique l'un sur l'autre. Cette remarque se place dans le cadre d'une découverte de Félix Klein qui avait étudié Galois.

7.2 Le programme d'Erlangen. Euclide avait codifié ce que l'on demande aux objets : points, droites, plans, circonférences, etc. pour pouvoir établir des énoncés de géométrie. Pendant des siècles des mathématiciens ont cherché à prouver que l'une des conditions demandée par Euclide dépendait des autres ; c'est l'axiome dit « des parallèles » que l'on peut énoncer comme ceci : « par un point hors d'une droite ℓ passe une et une seule droite du plan qui contient le point et ℓ, et qui ne rencontre pas ℓ ». Au 19$^{\text{e}}$ siècle, il fut prouvé (Bolyai, Lobatchevski, Riemann) que cet axiome est indépendant des autres axiomes et qu'il existe des géométries tout aussi légitimes qui ne satisfont pas à l'axiome des parallèles. Ce sont les géométries non euclidiennes [2]. Cayley réunit ces géométries et d'autres grâce à ce que l'on appelle l'espace projectif sur les nombres complexes. Félix Klein montra dans son programme d'Erlangen (1872) que la théorie des groupes pouvait permettre de comprendre autrement ces géométries et être un facteur d'unification. Il montra que toutes les géométries envisagées par Cayley pouvaient se définir par la donnée d'un ensemble E et d'un groupe G de

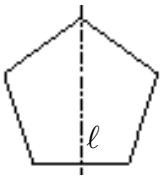
permutations de cet ensemble. Dans la situation de 7.1 E est le plan (qui peut être vu comme l'ensemble des couples de nombres réels) et G est le groupe des déplacements du plan. Les mouvements qui en 7.1 dérangeaient, apparaissent maintenant comme suffisamment importants que pour pouvoir définir la géométrie.

Par le programme d'Erlangen, au couple (E,G) qui définit une géométrie, on associe des propriétés de parties de E telles que G soit le groupe des permutations de E qui conservent ces propriétés.

7.3 Soit le pentagone représentant (le bâtiment qui contient) l'Institut de Mathématique de l'UMH :

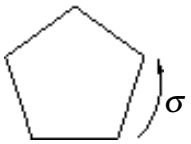


La symétrie orthogonale par rapport à la droite ℓ



applique le pentagone sur lui-même. C'est un cas particulier de ce que l'on appelle aujourd'hui une symétrie.

Pour le pentagone, la rotation σ de $\frac{360}{5}^\circ$ applique le pentagone



sur lui-même et est aussi appelée une symétrie du pentagone. Aujourd'hui, une symétrie est une permutation d'un ensemble qui conserve certaines propriétés. Plus précisément, une symétrie d'un ensemble structuré est une permutation de cet ensemble qui conserve la structure. En d'autres termes, une symétrie est ce que l'on appelle aussi un automorphisme [15, 21]. Dans l'exemple 7.1, les translations et les rotations sont des symétries du plan « usuel ». Les permutations des racines des équations rencontrées

en 4 et 5 sont des symétries d'une structure définie par ces équations. Les symétries d'une structure forment un groupe. Galois a prouvé que, pour ce dernier exemple, l'étude du groupe donnait des renseignements sur la structure. Cette démarche est devenue un guide pour la recherche, non seulement en mathématiques, mais aussi en chimie et en physique [20].

8 Conclusion

Il y avait peu de raisons utiles aux hommes pour chercher des formules de résolutions par radicaux aux équations du 3^e degré.

La formule une fois trouvée s'est révélée inutilisable. Il y avait donc encore moins de raisons de chercher une formule pour l'équation du 4^e degré. Dès que des formules efficaces de résolutions numériques furent trouvées il y eut de moins en moins de raisons de chercher une formule pour l'équation du 5^e degré. Les mathématiciens qui se sont fatigués à tirer cette question au clair savaient cela très bien. Mais ils sont ainsi faits que si une question apparemment naturelle résiste aux efforts de gens très forts, alors on se dit que derrière cette question se cache quelque chose d'important qui justifie que l'on se fatigue. Sans cette fatigue sur la résolution par radicaux des équations algébriques, aurait-on trouvé les nombres complexes qui ont envahi la plupart des domaines des mathématiques et de la physique et les groupes qui ont fait de la notion à connotation esthétique de symétrie un outil de compréhension et de prévision ?

A Appendice

A.1 Le Casus Irreductibilis. C'est, depuis Cardan, l'équation (11) lorsque $(p/3)^3 + (q/2)^2 < 0$. Un exemple est l'équation (17) qui possède au moins une solution réelle, 4, mais où l'application de la formule (16), impose comme en (18), de considérer des racines carrées de nombres négatifs. En fait, comme nous allons le voir, cette équation (17), comme toutes les équations du Casus Irreductibilis, possède trois racines réelles. On s'est demandé longtemps si pour cette équation à coefficients réels et à racines réelles, il n'existerait pas d'autres formules exprimant les racines à l'aide de radicaux $\sqrt[p]{\ }$, mais où n'interviendraient que des nombres réels. La réponse est négative (Hölder, 1890), mais sa preuve nécessite des résultats de la Théorie de Galois, contrairement à ce que nous allons prouver ici.

Un autre sujet de préoccupation fut que lorsqu'il devint admis qu'une équation du

troisième degré possède trois racines complexes (distinctes ou pas), la formule (16) semblait fournir neuf racines. L'égalité (13) implique qu'il n'en est rien.

A.2 Soient donc p et q des nombres réels, et x_1, x_2 et x_3 les racines (complexes) de l'équation (11) : $x^3+px+q=0$. Par l'égalité

$$x^3+px+q=(x-x_1)(x-x_2)(x-x_3)$$

on trouve

$$x_1+x_2+x_3=0 \tag{28}$$
$$x_1x_2+x_1x_3+x_2x_3=p \tag{29}$$
$$x_1x_2x_3=-q \tag{30}$$

Soit, comme en 4,

$$\Delta := (x_1-x_2)(x_1-x_3)(x_2-x_3) \tag{31}$$

Donc

$$\Delta \neq 0 \quad \text{si et seulement si} \quad x_1,x_2 \text{ et } x_3 \text{ sont distincts.} \tag{32}$$

Lemme 1.

$$\Delta^2 = -\left(27q^2+4p^3\right) \tag{33}$$

Démonstration. (1) L'un des $x_i=0$, soit $x_3=0$. Dès lors par (31) : $\Delta=(x_1-x_2)x_1x_2$. Or

$$(x_1-x_2)^2=(x_1+x_2)^2-4x_1x_2 \tag{34}$$

Par (27), $x_1+x_2=-x_3=0$. Par (29), $x_1x_2=p$, donc

$$(x_1-x_2)^2=-4p \quad \text{par (34)}$$

et $\Delta^2=(-4p)p^2=-4p^3$.

(2) Tous les x_i sont non nuls et par (30), $q\neq 0$. Par (34), (27) et (30) :

$$\begin{aligned}(x_1-x_2)^2 &= x_3^2+\frac{4q}{x_3}=\frac{x_3^3+4q}{x_3}\\ &= \frac{-px_3-q+4q}{x_3} \qquad \text{(par (11))}\\ &= \frac{3q}{x_3}-p\end{aligned}$$

De même

$$(x_1-x_3)^2=\frac{3q}{x_2}-p \qquad \text{et} \qquad (x_2-x_3)^2=\frac{3q}{x_1}-q.$$

D'où

$$\Delta^2 = \left(\frac{3q}{x_1} - p\right)\left(\frac{3q}{x_2} - p\right)\left(\frac{3q}{x_3} - p\right).$$

On développe le second membre, on utilise (27) et l'égalité

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = -\frac{p}{q}$$

obtenue en divisant (29) par $x_1x_2x_3$ et en utilisant (30). On en déduit (33). □

Proposition 2 (Le Casus Irreductibilis). *Les énoncés suivants sont équivalents :*

$$\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 < 0, \tag{35}$$

$$x_1, x_2 \text{ et } x_3 \text{ sont réels et distincts.} \tag{36}$$

Démonstration ([9]). (1) Soit (36). Par (31) Δ est un nombre réel non nul et Δ^2 un nombre réel positif. De (33) on déduit (35).

(2) Soit (35). Dès lors par (33) et (32), les x_i sont distincts. Toujours par (33), Δ^2 est un nombre réel positif, donc Δ est un nombre réel non nul. Par (31) :

$$x_1 - x_2 = \frac{\Delta}{(x_1 - x_3)(x_2 - x_3)}$$

Mais

$$\begin{aligned}(x_1 - x_3)(x_2 - x_3) &= x_1x_2 + x_3^2 - (x_1x_3 + x_2x_3) \\ &= x_1x_2 + x_3^2 + (x_1x_2 - p) && \text{(par (29))} \\ &= 2x_1x_2 + x_3^2 - p \\ &= -\frac{2q}{x_3} + x_3^2 - p && \text{(par (30))}\end{aligned}$$

Une équation du troisième degré à coefficients réels possède toujours au moins une racine réelle (théorème des valeurs intermédiaires). Soit $x_3 \in \mathbb{R}$. Donc

$$x_1 - x_2 = \frac{\Delta}{-\frac{2q}{x_3} + x_3^2 - p} \in \mathbb{R} \tag{37}$$

or

$$x_1 + x_2 = -x_3 \qquad \text{(par (28))}. \tag{38}$$

De (37) et (38), on déduit que x_1 et x_2 sont des nombres réels. □

A.3 On peut se donner le droit d'utiliser un peu plus les ressources de l'analyse mathématique. Étudions donc la courbe d'équation $y = x^3 + px + q$ où p et q sont des nombres réels, avec $p < 0$. Cette courbe possède un maximum, de coordonnées $\left(-\sqrt{\frac{-p}{3}}, q - \frac{4p}{3}\sqrt{\frac{-p}{3}}\right)$, et un minimum, de coordonnées $\left(\sqrt{\frac{-p}{3}}, q + \frac{2p}{3}\sqrt{\frac{-p}{2}}\right)$. En exprimant que l'ordonnée du maximum est positive et que l'ordonnée du minimum est négative, on retrouve la condition $(q/2)^2 + (p/3)^3 < 0$. Dans ce cas, il y a donc des ordonnées successivement négatives, positives, négatives puis positives, la courbe coupe donc l'axe des x en trois points (théorème des valeurs intermédiaires).

A.4 Les résolutions trigonométriques. On montre en général comme ceci qu'un nombre complexe possède une racine carrée complexe : soit $a + bi \in \mathbb{C}$, on recherche $x + iy \in \mathbb{C}$ pour lequel

$$a + bi = (x + iy)^2.$$

En développant cette dernière expression et en égalant les parties réelles, on obtient le système d'équations

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases} \tag{39}$$

Dès lors $4x^2y^2 = b^2$,

$$(x^2 + y^2)^2 = (x^2 - y^2)^2 + 4x^2y^2 = a^2 + b^2$$

Puisque $x^2 + y^2 > 0$, on a

$$x^2 + y^2 = \sqrt{a^2 + b^2}. \tag{40}$$

De (39) et (40), on déduit l'existence et le calcul des $x + iy$. Pour les racines n^{e} d'un nombre complexe ($n \geqslant 3$), on présente la méthode trigonométrique. Une raison de cette présentation exclusive est, comme nous allons le voir, que nous sommes en plein Casus Irreductibilis et dès lors la méthode algébrique ramène la recherche des racines cubiques d'un nombre complexe à la recherche des racines cubiques d'un nombre complexe. Nous allons montrer, à la suite de Viète (fin du 16^{e} siècle, début du 17^{e} siècle), que les fonctions trigonométriques permettent des formules de résolution du Casus Irreductibilis.

Lemme 3. *Si φ est un angle ou un nombre réel, alors*

$$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi.$$

Démonstration. Connue. □

Un nombre réel c est le cosinus d'un angle non nul et non plat si et seulement si $|c|<1$. Par le lemme 3, il est raisonnable d'appeler **« équation de trisection d'un angle non nul et non plat »** une équation de la forme

$$4Z^3-3Z-c=0, \qquad \text{où } |c|<1. \tag{41}$$

Les solutions de (41) sont

$$\cos\Big(\frac{\arccos c}{3}\Big), \quad \cos\Big(\frac{\arccos c}{3}+\frac{2\pi}{3}\Big) \quad \text{et} \quad \cos\Big(\frac{\arccos c}{3}+\frac{4\pi}{3}\Big).$$

Lemme 4. *Si $p<0$ et $Z=\sqrt{3/(-4p)}\,x$, alors les équations (11) et*

$$4Z^3-3Z=\frac{3q}{p}\sqrt{\frac{3}{-4p}}$$

sont équivalentes.

Démonstration. On calcule en remplaçant dans (12) X par $\sqrt{\frac{-4p}{3}}Z$. □

Lemme 5. *Soit $p<0$. Dès lors $\frac{3q}{p}\sqrt{\frac{3}{-4p}}$ est le cosinus d'un angle non nul et non plat si et seulement si*

$$27q^2+4p^3<0.$$

Démonstration. $\Big(\frac{3q}{p}\sqrt{\frac{3}{-4p}}\Big)^2<1$ si et seulement si $\frac{9q^2}{p^2}\Big(\frac{3}{-4p}\Big)<1$ si et seulement si $27q^2<-4p^3$. □

Des lemmes 4 et 5, on déduit la

Proposition 6. *L'énoncé (42) ci-après est équivalent aux énoncés (35) et (36) :*

> *$p<0$ et les $\sqrt{3/(-4p)}\,x_i$ sont les solutions d'une équation de trisection d'un angle non nul et non plat.* (42)

On a donc obtenu une *formule trigonométrique* pour les solutions de l'équation (11) lorsque $(q/2)^2+(p/3)^2<0$: ces solutions sont les

$$\sqrt{\frac{-4p}{3}}\cos\left(\frac{\arccos\frac{3q}{p}\sqrt{\frac{3}{-4p}}}{3}+\frac{2k\pi}{3}\right)$$

où $k\in\{0,1,2\}$.

Racines cubiques des nombres complexes. Mettons le nombre complexe $z = a + bi$ sous la forme $r(\cos\varphi + i\sin\varphi)$, où r est le nombre réel positif $\sqrt{a^2+b^2}$. Le nombre r possède une et une seule racine cubique réelle $\sqrt[3]{r}$, et les racines cubiques de z sont les nombres complexes $\sqrt[3]{r}\big(\cos(\frac{\varphi}{3} + \frac{2k\pi}{3})\big)$ où $k \in \{0,1,2\}$. Ces derniers cosinus sont solutions d'une équation du type (41).

Conclusion. Trouver dans le cas général le cosinus du tiers d'un angle en fonction du cosinus de cet angle, extraire la racine cubique d'un nombre complexe, et le Casus Irreductibilis, sont des problèmes équivalents.

Merci à Louis Habran qui est responsable d'une première mouture de cet exposé en septembre 2000, à Francis Buekenhout et Jean Doyen par leur aide à ma documentation, à Francis Buekenhout et Martine Oppitz pour leur lecture critique du manuscrit, à Lyane Bouchez pour le soin de sa dactylographie, et à Christophe Troestler pour la mise en page.

References

Ouvrages généraux (traitant la plupart des sujets abordés ici)

[1] W.S. Anglin et J. Lambek, *The Heritage of Thales*, Springer, (Undergraduate Texts in Mathematics), 1998.

[2] A. Dahan-Dalmedico/J. Peiffer, *Une histoire des mathématiques*, Seuil 1986.

[3] Jean Dieudonné, *Pour l'honneur de l'esprit humain*, Hachette, 1987.

[4] Enrico Giusti, *La naissance des objets mathématiques*, ellipses, 2000.

[5] Félix Klein, *Elementary mathematics from an advanced standpoint, Vol.1 : Arithmetic, Algebra, Analysis ; Vol.2 : Geometry*, Dover publications.

[6] John Stillwell, *Mathematics and Its History*, Springer-Verlag (Undergraduate Texts in Mathematics), 1991.

Équations et Théorie de Galois

[7] Gilles Godefroy, *Montons les degrés*, prépublication de l'Institut de Mathématique et d'Informatique de l'UMH, 2001, Consultable et téléchargeable sur le site web : `http://www.umh.ac.be/math/preprints/` Pour des copies « papier », s'adresser à l'Institut de Mathématique, adresse ci-dessous.

[8] Michel Lartillier, *Les tribulations de l'équation du second degré*, Mathématique et Pédagogie, 115, 43–58, 1997.

[9] Claude Mutafian, *Équations algébriques et théorie de Galois*, Vuibert, 1980.

[10] Ian Stewart, *Galois Theory*, Chapman and Hall, 1973.

[11] J.P. Tignol, *Galois'theory of algebraic equations*, New-York, Longman, 1988.

[12] B.L. van der Waerden, *A History of Algebra (from al-Khwarizmi to Emmy Noether)*, Springer-Verlag, 1985.

[13] G. Verriest, *Œuvres mathématiques d'Évariste Galois* — publiées en 1897, suivies d'une notice sur Évariste Galois et la théorie des équations algébriques, Gauthier-Villars, 1951.

Les nombres complexes

[14] IREM, *Images, Imaginaires, Imaginations, Une perspective historique pour l'introduction des nombres complexes*, ellipses, 1998.

Symétrie, groupes, géométrie et les sciences de la nature

[15] Francis Buekenhout et Jean Doyen, *Ensembles structurés et groupes de symétries*, cours de candidature, 1988. (Département de Mathématique de l'ULB, Campus Plaine, CP213, Boulevard du Triomphe, 1050 Bruxelles).

[16] Francis Buekenhout, *Le Programme d'Erlangen (1872)*, Séminaire de Géométrie Elémentaire CREM-GEPEMA-UREM, 19 novembre 1999, preprint.

[17] Alain Connes, *Symétries*, Pour la Science 292, Février 2002.

[18] Jacques Tits, *Symmetry*, Amer Math. Monthly 107, May 2000.

[19] *La symétrie aujourd'hui*, Seuil, 1989.

[20] *Les symétries de la nature*, Pour la Science, dossier, 1998.

[21] Jacques Tits, *Symétries*, Comptes Rendus de l'Acad. des Sciences, Série générale, La Vie des Sciences, Tome 2, N° 1, Janvier-Février 1985, pp. 13–25.

Cahiers pédagodiques récents

[1] Maurice BOFFA, *Fonctions récursives*, 20 avril 2001.

[2] Lucas QUARTA, *Une introduction (élémentaire) à la théorie des ondelettes*, 22 novembre 2001.

Les cahiers pédagogiques de l'*Institut de Mathématique* sont consultables et téléchargeables sur le site : `http://www.umh.ac.be/math/preprints/`. Si vous voulez recevoir des copies papier, veuillez écrire à l'adresse suivante :

Institut de Mathématique
Université de Mons-Hainaut
« Le Pentagone », 6 av. du champ de Mars
7000 Mons, Belgique