Esquisse du Théorème de Galois sur le critère d'existence d'une formule pour les solutions d'une équation quintique

Enno Nagel * — Institut de Mathématiques de Jussieu

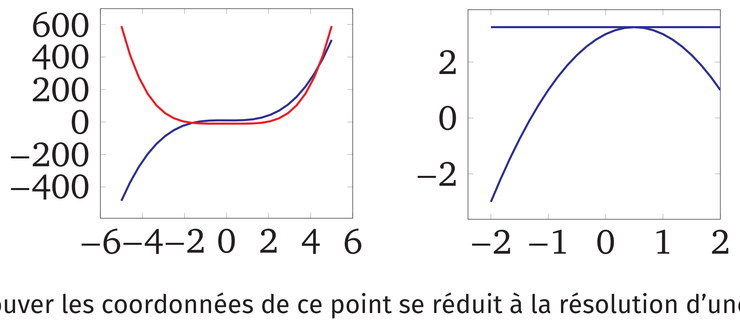
1 Solutions d'une équation polynômiale

On s'intéresse aux *polynômes* qui sont des sommes et produits en une variable inconnue X et des nombres réels qui prennent la forme

$$f(\mathrm{X}) = a_n\mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0$$

pour des nombres réels $a_n, a_{n-1}, \ldots, a_0$.

Souvent on s'intéresse au point où deux courbes données par des fonctions polynomiales se croisent ou où une tel courbe atteint son maximum :



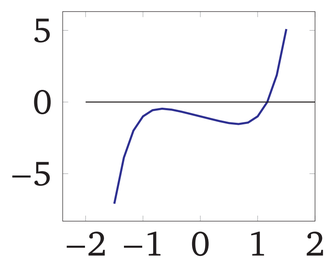
Trouver les coordonnées de ce point se réduit à la résolution d'une équation

$$f(\mathrm{X}) = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0 = 0;$$

d'où l'intérêt à une formule qui permet de calculer les *racines de* $f(\mathrm{X})$, c'est-à-dire les nombres $r_1, \ldots, r_n$ tel que $f(r_1), \ldots, f(r_n) = 0$. Nous montrerons comment résoudre cette équation polynomiale pour un degré $n = 1, 2$ et donnerons une idée pour $n = 3, 4$. Puis nous expliquons comment Evariste Galois a démontré qu'une telle formule universelle ne peut pas exister pour $n > 4$; il donné un critère quand une telle formule existe et quand non.

1.1 Les nombres complexes

Toute fonction polynomiale de degré impair $f(x) = a_{2n+1}x^{2n+1} + a_{2n}\mathrm{X}^{2n} + \cdots + a_0$ a une racine parce que pour x assez grand $f(x) > 0$ et $f(-x) < 0$. Par exemple on trouve que $f(\mathrm{X}) = x^5 - x + 1$ a une racine à $1.1673\ldots$



Pourtant l'équation

$$\mathrm{X}^2 + 1 = 0$$

reste toujours > 0. En rajoutant à $\mathbb{R}$ ses solutions $\pm\sqrt[2]{-1}$ on obtient *les nombres complexes*

$$\mathbb{C} = \{a + b\sqrt[2]{-1} : a, b \in \mathbb{R}\};$$

ainsi toutes les équations polynomiales $\mathrm{X}^2 + a\mathrm{X} + b = 0$ de degré 2 ont une solution sur $\mathbb{C}$ (comme nous verrons en tout détail en bas par la formule qui donne ses solutions).

Un théorème (d'Artin-Schreier) affirme que si tout polynôme de degré impair et tout polynôme de degré 2 a une solution, alors tout polynôme a une solution.

Dès qu'on a trouvé une solution r d'une équation polynomiale $f(x) = 0$, c'est-à-dire $f(r) = 0$, alors on peut diviser $f(x)$ par $(x - r)$ et obtient un polynôme de degré plus petit sur lequel on peut appliquer ce raisonnement de nouveau. En itérant, on voit que tout polynôme de degré n a n racines $r_1, \ldots, r_n$ dans $\mathbb{C}$.

1.2 Le degré d'un polynôme

Le plus haute la puissance maximale n de x, le plus d'ingéniosité requise pour trouver x :

- Si $n = 1$, c'est-à-dire $\mathrm{X} + a = 0$, alors $x = -a$
- (Complétion du carré) Si $n = 2$, c'est-à-dire $x^2 + px + q = 0$, alors on récrit l'équation comme $x^2 + px + q = (x + p/2)^2 - p^2/4 + q$ et obtient
$$x = -p/2 \pm \sqrt{p^2/4 - q}. \qquad (*)$$
- (Méthode de Cardan) Si $n = 3$, c'est-à-dire $x^3 + ax^2 + bx + c = 0$, alors
  1. remplace x par $\tilde{x} = x + h$ avec $h = -a/3$ qui est choisi tel que
  $$\tilde{x}^3 + p\tilde{x} + q = x^3 + ax^2 + bx + c$$
  2. remplace $\tilde{x}$ par $x' + x''$ choisis tel que $x'x'' = -p/3$, ce qui donne
  $$x'^3 + x''^3 + (x' + x'')(3x'x'' + p) + q = x'^3 + x''^3 + q.$$
  3. Alors on cherche $\mathrm{X}' = x'^3$ et $\mathrm{X}'' = x''^3$ tel que
  $$\mathrm{X}' + \mathrm{X}'' = -q \qquad \text{et} \qquad \mathrm{X}'\mathrm{X}'' = -p^3/27.$$
  Parce que $(\mathrm{X} + \alpha)(\mathrm{X} + \beta) = \mathrm{X}^2 + \alpha\beta\mathrm{X} + \alpha\beta$, les valeurs X' et X'' sont les solutions de
  $$\mathrm{X}^2 + q\mathrm{X} - p^3/27 = 0;$$
  une équation de degré 2 qu'on a résolue en haut par $(*)$ et nous donne pour $x = x' + x''$ la formule
  $$x = \sqrt[3]{-q/2 + \sqrt{q^2/4 + p^3/27}} + \sqrt[3]{-q/2 - \sqrt{q^2/4 + p^3/27}}.$$
  En remplaçant on obtient une formule de x en termes de a,b et c.
- (Méthode de Ferrari) Si $p(\mathrm{X}) = x^4 + \cdots$ est un polynôme de degré 4 alors la méthode de Ferrari montre comment réduire à une équation polynômiale de degré 3 comme en haut.

On conclut que pour toute équation polynômiale de degré jusqu'à 4 ses solutions s'expriment par les coefficients $a_0, \ldots, a_4$ de l'équation et des nombres rationnels au moyen des opérations de $+, \cdot$ et $\sqrt[n]{\cdot}$ (où $n = 2, 3, 4$).

2 Groupe de Galois

Pourtant

- la complétion du carré est connue depuis 2000 ans, et
- les méthodes de Cardan et de Ferrari datent du seizième siècle.

il fallait attendre jusqu'au 19e siècle pour s'en convaincre qu'une telle formule pour donner les racines d'une équation polynomiale de degré plus grand que 4 n'existe pas.

Pour une équation polynomiale de degré plus grand que 4, en 1834 Evariste Galois donne un critère quand une telle équation a des solutions qui peuvent s'exprimer par une formule comme en haut, en les coefficients $a_0, \ldots, a_n$ de l'équation au moyen des opérations de $+, \cdot, \cdot^n$et leurs inverses $-$, $/$ et $\sqrt[n]{\cdot}$; en particulier il montre qu'une bonne partie des polynômes de degré > 4 n'ont pas de solutions données par une formule, par exemple les zéros du polynôme $\mathrm{X}^5 - \mathrm{X} - 1$ (bien que par exemple au contraire le polynôme $\mathrm{X}^5 - 32$ a des solutions données par la formule $x = \sqrt[5]{32}$).

Soit r une racine d'un polynôme à coefficients rationnels. Parmi tous les polynômes à coefficients dans $\mathbb{Q}$ qui annulent r il y a un unique polynôme $f = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0$ du degré n minimal, c'est le *polynôme minimal de* r.

Pour savoir quand r peut être donnée par une *formule*, c'est-à-dire par des sommes $+$, soustractions $-$ et des racines $\sqrt[n]{\cdot}$ de nombres rationnels comme

$$r = \sqrt[2]{\sqrt[3]{2} + 5} - \sqrt[2]{12}$$

il faut regarder les permutations sur toutes les racines de f :

2.1 Les permutations de toutes les racines

Soit $f(\mathrm{X}) = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0$ un polynôme avec $a_{n-1}, \ldots, a_0$ dans $\mathbb{Q}$ et $r_1, \ldots, r_n$ les racines de f.

Définition

Le *groupe de Galois* de f est

$$\mathrm{G} = \{\text{ toutes les } \textit{permutations} \text{ des racines } r_1, \ldots, r_n \text{ qui } \textit{respectent l'addition et la multiplication}\ \}$$

Qu'est-ce qu'une *permutation* et que veut dire *qu'elle respecte l'addition et la multiplication* ? Par exemple soit

$$f(\mathrm{X}) = \mathrm{X}^4 - 2 = 0$$

et $\{\pm\sqrt[4]{2}, \pm\sqrt{-1}\sqrt[4]{2}\}$ ses 4 racines permutées par G. Une *permutation* permute l'ordre de toutes les racines ou, autrement dit, elle est une fonction qui envoie toute racine à une autre racine et ne jamais deux racines différentes sur la même racine, par exemple

$$\left|\begin{array}{cccc} \sqrt[4]{2} & -\sqrt[4]{2} & \sqrt{-1}\sqrt[4]{2} & -\sqrt{-1}\sqrt[4]{2} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ -\sqrt[4]{2} & \sqrt[4]{2} & -\sqrt{-1}\sqrt[4]{2} & \sqrt{-1}\sqrt[4]{2} \end{array}\right| \qquad (*)$$

Qu'est-ce que cela veut dire, qu'une permutation *respecte l'addition et la multiplication* ?

2.2 Les nombres formés par les racines

Pour cela il faut regarder le domaine de tous les nombres qui se forment comme somme des produits des racines $r_1, \ldots, r_n$ et nombres rationnels. Par exemple pour $f(\mathrm{X}) = \mathrm{X}^4 - 2$ tous ces nombres prennent la forme

$$a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{2}^2 + a_3\sqrt[4]{2}^3$$
$$+b_0\sqrt{-1} + b_1\sqrt{-1}\sqrt[4]{2} + b_2\sqrt{-1}\sqrt[4]{2}^2 + b_3\sqrt{-1}\sqrt[4]{2}^3$$

pour des nombres $a_0, \ldots, a_3$ et $b_0, \ldots, b_3$ dans $\mathbb{Q}$. Un élément typique parmi eux est par exemple

$$5 + 3\sqrt[4]{2} + 7/9\sqrt{-1}\sqrt[4]{2}^3.$$

Toutes les permutations s'étendent de toutes les racines $r_1, \ldots, r_n$ à tous ces nombres simplement en remplaçant chaque racine $r_1, \ldots, r_n$ dans une telle somme des produits des racines $r_1, \ldots, r_n$ par son image $\sigma(r_1), \ldots, \sigma(r_n)$. Par exemple si σ est la permutation définie en haut qui permute $\{\pm\sqrt[4]{2}\}$ et $\{\pm\sqrt{-1}\sqrt[4]{2}\}$, alors σ envoie $5 + 3\sqrt[4]{2} + 7/9\sqrt{-1}\sqrt[4]{2}^3$ sur $5 - 3\sqrt[4]{2} - 7/9\sqrt{-1}\sqrt[4]{2}^3$.

Définition

Une permutation *respecte l'addition et la multiplication* veut dire que pour tous les nombres x et y comme dessus, formés par les racines $r_1, \ldots, r_n$ et des nombres rationnels, la permutation σ satisfait

$$\sigma(x + y) = \sigma(x) + \sigma(y) \qquad \text{et} \qquad \sigma(x \cdot y) = \sigma(x) \cdot \sigma(y).$$

Par exemple pour $f(\mathrm{X}) = \mathrm{X}^4 - 2$ on trouve que toute permutation σ satisfait

$$0 = \sigma(0) = \sigma(\sqrt[4]{2} - \sqrt[4]{2}) = \sigma(\sqrt[4]{2}) + \sigma(-\sqrt[4]{2})$$

ce qui vaut si et seulement si $\sigma(-\sqrt[4]{2}) = -\sigma(\sqrt[4]{2})$; également on trouve $\sigma(-\sqrt{-1}\sqrt[4]{2}) = -\sigma(\sqrt{-1}\sqrt[4]{2})$. On conclut qu'entre toutes les $24 = 4 \cdot 3 \cdot 2 \cdot 1$ permutations des quatre racines $\{\pm\sqrt[4]{2}, \pm\sqrt{-1}\sqrt[4]{2}\}$de $f(\mathrm{X}) = \mathrm{X}^4 - 2$ seulement celles qui satisfont

$$\sigma(-\sqrt[4]{2}) = -\sigma(\sqrt[4]{2}) \qquad \text{et} \qquad \sigma(-\sqrt{-1}\sqrt[4]{2}) = -\sigma(\sqrt{-1}\sqrt[4]{2})$$

sont dans le groupe de Galois G de f, comme cette permutation-là donnée dans le diagramme $(*)$.

Ainsi on trouve que G contient exactement 8 permutations; c'est-à-dire toutes les conditions nécessaires sont aussi suffisantes pour qu'une permutation soit dans le groupe de Galois G. Ces 8 permutations sont données par les 4 choix pour l'image de $\sqrt[4]{2}$ et les 2 choix restants pour l'image de $\sqrt{-1}\sqrt[4]{2}$.

3. La formule d'une racine en étapes

Alors on suppose que la racine r est donnée par une *formule*, c'est-à-dire par des sommes $+$, soustractions $-$ et des racines $\sqrt[n]{\cdot}$ de nombres rationnels comme

$$r = \sqrt[2]{\sqrt[3]{2} + 5} - \sqrt[2]{12}.$$

3.1 La décomposition des racines

On observera la même particularité du groupe de Galois dans chacune des deux façons par lesquelles la racine r dans une formule est obtenue :

- Si $r = \sqrt[n]{a}$ est une racine d'un nombre obtenu par des sommes et racines dans $\mathbb{Q}$, par exemple $r = \sqrt[4]{2}$, ou
- si $r = a \pm b$ est la somme ou différence de deux nombres obtenus par des sommes et racines des nombres rationnels, par exemple $r = \sqrt{2} + \sqrt{3}$.

Le cas d'une racine

Regardons le premier cas $r = \sqrt[n]{a}$ par l'exemple $r = \sqrt[4]{2}$ dont le groupe de Galois nous venons de discuter. On observe que toutes les racines $\{\pm\sqrt[4]{2}, \pm\sqrt{-1}\sqrt[4]{2}\}$ s'expriment comme produits de deux nombres irrationnels différents : $\sqrt[4]{2}$ et $\sqrt{-1}$. Maintenant on ne regarde que toutes les permutations dans G qui fixent le facteur $\sqrt{-1}$. Une telle permutation se décrit comme

$$\left|\begin{array}{cccc} \sqrt[4]{2} & -\sqrt[4]{2} & \sqrt{-1}\sqrt[4]{2} & -\sqrt{-1}\sqrt[4]{2} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ *\sqrt[4]{2} & -*\sqrt[4]{2} & \sqrt{-1}*\sqrt[4]{2} & -\sqrt{-1}*\sqrt[4]{2} \end{array}\right|$$

où $*$ est à remplacer par une des quatre facteurs $1, -1, \sqrt{-1}$ ou $-\sqrt{-1}$.
Au contraire si on ne regarde que l'action des permutations dans G sur l'autre facteur $\sqrt{-1}$, il y en a deux possibilités :

$$\left|\begin{array}{cc} \sqrt{-1} & -\sqrt{-1} \\ \downarrow & \downarrow \\ \sqrt{-1} & -\sqrt{-1} \end{array}\right| \qquad \text{et} \qquad \left|\begin{array}{cc} \sqrt{-1} & -\sqrt{-1} \\ \downarrow & \downarrow \\ -\sqrt{-1} & \sqrt{-1} \end{array}\right|$$

Le cas d'une somme

Regardons le deuxième cas $r = a + b$ par l'exemple $r = \sqrt{2} + \sqrt{3}$. Son polynôme minimal est $\mathrm{X}^4 - 10\mathrm{X}^2 + 1$ qui a les 4 racines $\{\pm\sqrt{2} \pm \sqrt{3}\}$ et alors ses 4 permutations se décrivent par

$$\left|\begin{array}{cccc} \sqrt{2} + \sqrt{3} & -\sqrt{2} + \sqrt{3} & \sqrt{2} - \sqrt{3} & -\sqrt{2} - \sqrt{3} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ *\sqrt{2} + \dagger\sqrt{3} & *\sqrt{2} + \dagger\sqrt{3} & *\sqrt{2} + \dagger\sqrt{3} & *\sqrt{2} + \dagger\sqrt{3} \end{array}\right|$$

où $*$ et $\dagger$ sont à remplacer par une des deux facteurs 1 ou -1.

Observation

Toutes les permutations qui fixent un facteur ou additionné dans toutes les racines (par exemple le facteur $\sqrt{-1}$ dans les racines $\{\pm\sqrt[4]{2}, \pm\sqrt{-1}\sqrt[4]{2}\}$) et toutes les permutations obtenues en restreignant à ce facteur ou additionné (par exemple au facteur $\sqrt{-1}$) sont l'itération d'une seule permutation σ *engendrant*, c'est-à-dire

$$\mathrm{G} = \{\sigma, \sigma \circ \sigma, \ldots, \overbrace{\sigma \circ \cdots \circ \sigma}^{n\text{–fois}} = e\}$$

où e dénote la permutation qui fixe toute racine.

Par exemple les permutations qui fixent la racine $\sqrt{-1}$ sont toutes obtenues en appliquant la permutation σ qui envoie $\sqrt[4]{2}$ à $\sqrt{-1}\sqrt[4]{2}$ (ou aussi bien à $-\sqrt{-1}\sqrt[4]{2}$); ce diagramme montre toutes ses itérations :

$$\left|\begin{array}{cccc} \sqrt[4]{2} & -\sqrt[4]{2} & \sqrt{-1}\sqrt[4]{2} & -\sqrt{-1}\sqrt[4]{2} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ \sqrt{-1}\sqrt[4]{2} & -\sqrt{-1}\sqrt[4]{2} & -\sqrt[4]{2} & \sqrt[4]{2} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ -\sqrt[4]{2} & \sqrt[4]{2} & -\sqrt{-1}\sqrt[4]{2} & \sqrt{-1}\sqrt[4]{2} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ -\sqrt{-1}\sqrt[4]{2} & \sqrt{-1}\sqrt[4]{2} & -1\sqrt[4]{2} & \sqrt[4]{2} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ \sqrt[4]{2} & -\sqrt[4]{2} & \sqrt{-1}\sqrt[4]{2} & -\sqrt{-1}\sqrt[4]{2} \end{array}\right|$$

Les deux permutations sur $\pm\sqrt{-1}$ sont données par σ et $\sigma \circ \sigma = e$ où σ est la permutation qui change le signe de $\sqrt{-1}$ et $-\sqrt{-1}$.
On trouve de même pour les permutations des racines $\{\pm\sqrt{2} \pm \sqrt{3}\}$.

Si la racine r est donnée par une formule, alors elle est obtenue en itérant des sommes et des racines de nombres rationnels. En itérant cette observation sur son groupe de Galois (toutes les permutations de toutes les racines $r_1, \ldots, r_n$ du polynôme minimal de r) on en infère :

Corollaire

Si la racine r est donnée par une formule (avec groupe de Galois G) alors il y a des facteurs et additionnés $s_1, s_2, \ldots$ tel que pour tout $m = 1, 2, \ldots$ toutes les restrictions $\bar{\sigma}_1, \bar{\sigma}_2, \ldots$ à s_m de toutes les permutations dans G qui fixent $s_1, s_2, \ldots, s_{m-1}$ sont l'itération $\sigma, \sigma \circ \sigma, \ldots, \sigma \circ \cdots \circ \sigma = e$ d'une seule permutation σ.

Maintenant il s'avère que

- pour le groupe de toutes les permutations de 5 racines cette restriction itérative aux sous-groupes engendrés par une seule permutation n'est plus possible, et
- que l'équation polynomiale $f(\mathrm{X}) = x^5 - x + 1$ a comme groupe de Galois toutes les permutations de ses 5 racines.

Alors aucune des racines de $x^5 - x + 1$, en particulier la racine $1.1673\ldots$ dessinée au-dessus, n'est donnée par une formule.

* Plus de renseignements à www.math.jussieu.fr/~nagel