Extrait de symétries Galoisiennes et renormalisation [1]

VIII. Le groupe de renormalisation et la théorie de Galois aux places archimédiennes

[...]

Commençons par une introduction très élémentaire à la théorie de Galois pour les équations algébriques.

Si la technique de résolution des équations du second degré remonte à la plus haute Antiquité (Babyloniens, Égyptiens...), elle n'a pu être étendue au troisième degré que bien plus tard, et ne sera publiée par Girolamo (Jérôme) Cardano qu'en 1545 dans les chapitres 11 à 23 de son livre *Ars magna sive de regulis algebraicis*. Bien que cela n'ait pas été reconnu avant le dix-huitième siècle, la clef de la résolution par radicaux de l'équation générale du troisième degré, $x^3+nx^2+px+q=0$, de racines a, b, c, est l'existence d'une fonction rationnelle $\alpha(a,b,c)$ de a, b, c, qui ne prend que deux déterminations différentes sous l'action des six permutations de a, b, c.

La méthode de Cardan revient à poser $\alpha=\big((1/3)(a+bj+cj^2)\big)^3$ où le nombre j est la première racine cubique de l'unité. La permutation circulaire transformant a en b, b en c et c en a laisse manifestement α inchangée et la seule autre détermination de la fonction α sous l'action des six permutations de a, b, c, est obtenue en transposant b et c par exemple, ce qui donne $\beta=\big((1/3)(a+cj+bj^2)\big)^3$.

Comme l'ensemble de ces deux nombres α et β est invariant par toutes les permutations de a, b, c, le polynôme du second degré dont α et β sont racines se calcule rationnellement en fonction des coefficients de l'équation initiale $x^3+nx^2+px+q=0$: c'est $X^2+2qX-p^3=(X+q+s)(X+q-s)$ où s est l'une des racines carrées de p^3+q^2 et où l'on a réécrit l'équation initiale sous la forme équivalente $x^3+3px+2q=0$ débarrassée du terme du deuxième degré en effectuant une translation convenable des racines et où l'on a introduit les coefficients 2 et 3 pour simplifier les formules.

Un calcul simple montre alors que chacune des racines a, b et c, de l'équation initiale s'exprime comme somme de l'une des trois racines cubiques de α et de l'une des trois racines cubiques de β, ces deux choix étant liés par le fait que leur produit doit être impérativement égal à $-p$ (il n'y a donc que trois couples de choix de ces racines à prendre en compte, ce qui est rassurant, à la place des neuf possibilités que l'on aurait pu envisager *a priori*).

C'est à l'occasion de ces formules que l'utilisation des nombres complexes s'est imposée. En effet, même dans le cas où les trois racines sont réelles, il se peut que p^3+q^2 soit négatif et que α et β soient nécessairement des nombres complexes.

Si la résolution des équations du troisième degré que nous venons d'exposer a été très longue à être mise au point (sans doute pour au moins l'un de ses cas particuliers entre 1500 et 1515 par Scipione del Ferro), celle du quatrième degré a été plus preste à la suivre puisqu'elle figure également dans l'*Ars magna* (chapitre 39) où Cardano l'attribue à son secrétaire Ludovico Ferrari qui l'aurait mise au point entre 1540 et 1545 (René Descartes en publiera une autre en 1637).

[1] https://arxiv.org/pdf/math/0211199.

Ici encore, l'on peut partir d'un polynôme débarrassé d'un coefficient, annulé par translation, disons $X^4 + pX^2 + qX + r = (X - a)(X - b)(X - c)(X - d)$.

La fonction rationnelle $\alpha(a, b, c, d)$ la plus simple[2], ne prenant que trois déterminations différentes sous l'action des vingt-quatre permutations de a, b, c et d, est $\alpha = ab + cd$. Les deux autres déterminations sont $\beta = ac + bd$, $\gamma = ad + bc$. Ce sont donc les racines d'une équation du troisième degré dont les coefficients s'expriment rationnellement en fonction de p, q et r. Un calcul simple montre que le polynôme $(X - \alpha)(X - \beta)(X - \gamma)$ est égal à $X^3 - pX^2 - 4rX + (4pr - q^2)$. Il peut donc être décomposé comme on l'a vu plus haut pour en déduire α, β et γ ; en fait, il suffit même de calculer l'une seulement de ces racines, disons α, pour pouvoir en déduire a, b, c et d (nous connaissons alors en effet la somme α et le produit r des deux nombres ab et cd, donc ces deux nombres eux-mêmes par une équation du second degré, et il ne reste plus qu'à exploiter les égalités $(a + b) + (c + d) = 0$ et $ab(c + d) + cd(a + b) = -q$ pour pouvoir en déduire $a + b$ et $c + d$, donc enfin a, b, c et d par une autre équation du second degré).

C'est à Joseph Louis Lagrange en 1770 et 1771 (publication en 1772, mais aussi, dans une moindre mesure, à Alexandre Vandermonde dans un mémoire publié en 1774 mais également rédigé vers 1770, ainsi qu'à Edward Waring dans ses *Meditationes algebricæ* de 1770 et à Francesco Malfatti) que l'on doit la mise en lumière du rôle fondamental des permutations sur les racines a, b, c... et sur les quantités auxiliaires α, β..., d'ailleurs aujourd'hui justement appelées "résolvantes de Lagrange".

Ces résolvantes ne sont pas uniques, et par exemple le choix $\alpha = (a + b - c - d)^2$ correspond à la solution de Descartes, mais elles fournissent la clef de toute les résolutions générales par radicaux. Il y en a une qui est particulièrement belle car elle est covariante pour le groupe affine, c'est à dire vérifie l'égalité,

$$\alpha(\lambda\, a + z, \lambda\, b + z, \lambda\, c + z, \lambda\, d + z) = \lambda\, \alpha(a, b, c, d) + z$$

et admet donc une interprétation géométrique.

Elle est donnée algébriquement par

$$\alpha = \frac{ad - bc}{a + d - b - c}$$

et correspond géométriquement (figure 2) au point d'intersection des cercles circonscrits aux triangles ABJ et JCD où J désigne le point d'intersection des droites AC et BD.

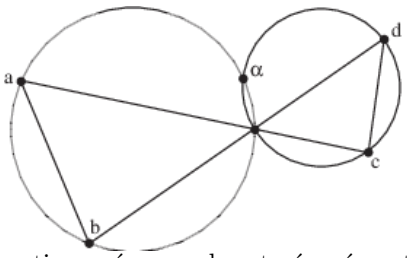

Figure 2. Le point α est fonction méromorphe et séparément homographique des quatre points A, B, C, D.

[2] *Voir [1] pour l'ubiquité de la symétrie en question, et son rôle dans l'organisation des tournois de football.*

J'ai rencontré récemment cette résolvante à propos du problème [3] de l'étoile à cinq branches (figure 3), dont elle permet une résolution algébrique que je laisse à la sagacité du lecteur.

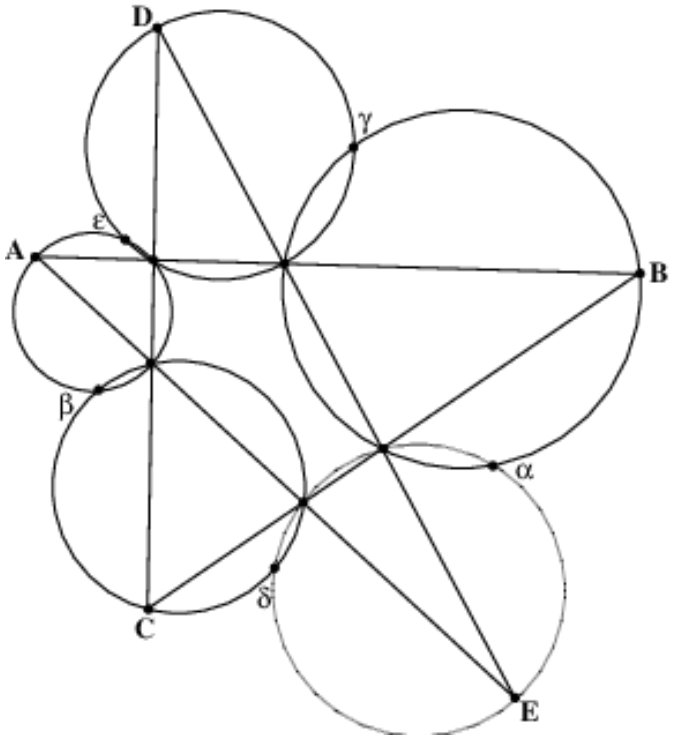

Figure 3. On donne cinq points arbitraires A,B,C,D,E. Montrer que les points d'intersection $\alpha, \beta, \gamma, \delta, \epsilon$ des cercles circonscrits aux triangles externes consécutifs de l'étoile sont situés sur un même cercle.

L'étape suivante dans la théorie des équations algébriques est évidemment celle du cinquième degré. Descartes a certainement essayé et avec lui bien des chercheurs. Elle a toujours opposé des obstacles infranchissables, et nous savons depuis Abel et Galois, aux alentours de 1830, pourquoi cette quête était vaine.

Descartes par exemple, persuadé qu'il n'existait pas de formule analogue à celle de Cardano, avait proposé en 1637, dans *La Géométrie*, une méthode graphique de résolution grâce à l'intersection de cercles et de cubiques qu'il avait inventées pour l'occasion. Entre 1799 et 1813 (date de l'édition de ses *Riflessioni intorno alla solutione delle equazioni algebraiche generali*), Paolo Ruffini a publié diverses tentatives de démonstrations, de plus en plus affinées, visant à établir l'impossiblité de résoudre l'équation générale du cinquième degré par radicaux. À toute fonction rationnelle des racines, il a eu l'idée juste d'associer le groupe des permutations de ces racines qui la laissent invariante, mais a cru à tort (d'après un rapport de Ludwig Sylow) que les radicaux intervenant dans la résolution de l'équation, comme les racines cubiques de α pour le degré trois, étaient nécessairement des fonctions rationnelles des racines.

Il faudra attendre 1824 pour que Niels Abel justifie l'intuition de Ruffini dans son *Mémoire sur les équations algébriques* et - après avoir cru trouver au contraire une méthode de résolution générale

[3] *posé par le président Chinois Jiang Zemin à la délégation de mathématiciens venue à sa rencontre en l'an 2000.*

- prouve l'impossiblité de résoudre l'équation générale du cinquième degré par radicaux, en 1826 dans le *Mémoire sur une classe particulière d'équations résolubles algébriquement*, où il amorce une théorie générale qui ne s'épanouira que dans les écrits de Galois, vers 1830. Les travaux de Galois inaugurent une ère nouvelle des mathématiques, où les calculs font place à la réflexion sur leur potentialité, et les concepts, tels celui de groupe abstrait ou d'extension algébrique, occupent le devant de la scène.

L'idée lumineuse de Galois consiste d'abord à associer à une équation arbitraire un groupe de permutations qu'il définit de la manière suivante, [2]

Soit une équation donnée, dont a, b, c,... sont les m racines.

Il y aura toujours un groupe de permutations des lettres a, b, c,... qui jouira de la propriété suivante:

1) *que toute fonction des racines, invariante par les substitutions de ce groupe, soit rationnellement connue ;*

2) *réciproquement, que toute fonction des racines, déterminée rationnellement, soit invariante par ces substitutions.*

puis à étudier comment ce groupe "d'ambiguïté" se trouve modifié par l'adjonction de quantités auxiliaires considérées comme "rationnelles".

Ainsi, dans le cas de l'équation du quatrième degré, si l'on adjoint la quantité α obtenue en résolvant l'équation auxiliaire du troisième degré, l'on réduit le groupe d'ambiguïté au sous-groupe normal formé des quatre permutations (a,b,c,d), (b,a,d,c), (c,d,a,b), (d,c,b,a). Ce groupe est le produit de deux groupes à deux éléments et l'adjonction des solutions de deux équations du second degré suffit alors pour éliminer totalement l'ambiguïté, c'est à dire résoudre l'équation initiale.

Si l'on désigne par k le corps des "quantités rationnelles" et par K celui engendré par k et par toutes[4] les racines de l'équation que l'on se propose de résoudre, le groupe de Galois, $G = \mathrm{Gal}(K : k)$ est le groupe des automorphismes de K qui fixent tous les éléments de k.

L'impossibilité de réduire l'équation du cinquième degré à des équations de degré inférieur provient alors de la "simplicité" du groupe A_5 des soixantes permutations paires (produits d'un nombre pair de transpositions) des cinq racines a, b, c, d, e d'une telle équation.

Un groupe abstrait fini est "simple" si l'on ne peut le réduire, par un homomorphisme non trivial, à un groupe plus petit.

Le groupe A_5 est le plus petit groupe simple non commutatif et il apparaît très souvent en mathématiques.

[4] *Il ne suffit pas d'adjoindre une seule de ces racines, il faut les adjoindre toutes.*

Références

[1] A. Connes, Symétries, de Galois au monde quantique, Volume en l'honneur de Louis Michel (à paraître).

[2] É. Galois, Écrits et mémoires mathématiques d'Évariste Galois. Gauthier-Villars, Paris, Londres (1962).