Équations et substitutions avant Galois : Lagrange et Cauchy

Massimo Galuzzi*

1 Introduction

Les célèbres *Réflexions sur la résolution algébrique des équations* et les deux mémoires publiés par Cauchy en 1815[1] sont une sorte de prémisse naturelle pour la « théorie de Galois » contenue dans le soi-disant *Premier Mémoire* de Galois.

On n'a pas encore la structure de groupe dans ces textes, mais l'usage des permutations des racines des équations algébriques fait par Lagrange pour analyser les succès (et les échecs) dans la solution de ces équations et la présence implicite de cette structure chez Cauchy, quand il considère toutes les permutations d'un nombre fini de variables qui ne modifient pas la valeur d'une fonction (rationnelle) de ces variables, sont certainement des résultats mathématiques de la plus grande importance pour l'œuvre successive de Galois.

Toutefois l'attitude de Galois envers ces deux auteurs est différente. Il cite avec soin Cauchy pour une question très simple (pour lui), mais il semble éviter toute référence à Lagrange.[2] Cette remarque, en apparence bien évidente,

*Le texte de cet exposé est provisoire. Je prie de l'utiliser seulement pour une lecture personnelle.

1. Il s'agit de (Lagrange, 1770), (Cauchy, 1815a), (Cauchy, 1815b).

2. Dans le texte du *Premier Mémoire*. Dans (Galois, 1829) il cite explicitement la méthode de Lagrange pour obtenir le développement d'une racine d'une équation algébrique en fraction continue. La référence peut être à (Lagrange, 1769), mais plus probablement elle est à (Lagrange, 1808), ou à la troisième édition (1826) curée par Poinsot. Sur l'importance pour Galois du *Commentaire* de Poinsot contenu dans cette édition on peut voir (Ehrhardt, 2007, p. 94). L'usage « scolaire »de (Lagrange, 1808) (voir sur ce point (Belhoste, 1995, p. 86)) confirme cette hypothèse.

n'est pas très commune dans l'histoire des sciences, où la continuité mathématique entre Lagrange et Galois est souvent soulignée. La question est posée en ces termes dans (Ehrhardt, 2007) :

> Un autre nom, auquel Galois ne fait aucune allusion [dans le *Premier Mémoire*] vient immanquablement à l'esprit s'agissant des inspirateurs de ses travaux : celui de Lagrange, qui a mis au point à la fin du XVIIIe siècle une méthode fondée sur les permutations et les regroupement des racines. La parenté mathématique entre deux textes [le *Premier Mémoire* et les *Réflexions*] ne suffit pas à garantir que l'un ait eu une quelque influence sur l'écriture de l'autre, étant donné qu'une telle parenté peut résulter de l'interprétation que fait le lecteur de chacune des deux textes.[3]

Dans ce qui suit je me propose d'ajouter quelques remarques sur les deux questions, par une comparaison de certaines situations mathématiques affrontées par les auteurs en question.

2 Galois cite Cauchy dans le *Premier Mémoire*

Dans la *Proposition* VII du *Premier Mémoire*, Galois montre que pour une équation irréductible d'un degré premier n soluble par radicaux « le plus petit groupe possible avant celui qui n'a qu'une seule permutation contiendra n permutations ».[4]

Il conclut de cela que « . . .un groupe de permutations d'un nombre premier n de lettres ne peut se réduire à n permutations, à moins que l'une de ces permutations ne se déduise de l'autre par une substitution de l'ordre n ».[5] Pour soutenir cette affirmation il cite un mémoire que Cauchy à publié en 1815 dans le XVII^e Cahier du *Journal de l'École* [*Polytechnique*].[6]

Dans ce Cahier, Cauchy a publie deux articles importantes sur la naissante théorie des substitutions, (Cauchy, 1815a,b).[7] La citation expéditive de

3. *Ibid.*, p. 78. Voir aussi les références données dans les notes de cette page.

4. Voir (Neumann, 2011, p. 126).

5. *Ibid.*

6. Ce résultat découle immédiatement du théorème de Cauchy contenu dans (Cauchy, 1845), mais on n'a pas besoin de toute la force de ce théorème pour le prouver.

7. Ces articles ont été l'objet de beaucoup d'analyses. Je me limite à citer (Kiernan, 1971-1972), (Dahan, 1979, 1980).

Galois ne permet pas de savoir s'il s'agit du premier ou du seconde article ni le lieu précis auquel il se réfère. Mais en tout cas les matériels contenus dans les deux articles pouvaient bien donner (à Galois) une démonstration facile.

En fait, dans (Cauchy, 1815a, p. 76) l'ordre (période) d'une substitution est introduit.

Dans (Cauchy, 1815b, p. 99-102) on a la décomposition d'une substitutions en un produit de cycles.

Que l'ordre d'une substitution soit le plus petit multiple commun des nombres qui expriment l'ordre des cycles qui la composent et que l'ordre d'une substitution contenue dans un groupe des substitutions soit un diviseur de l'ordre du groupe sont des faits presque évidents. La propriété requise en découle immédiatement.[8]

Ces considérations nous poussent à nous interroger sur la raison de cette citation. Qu'elle soit une « captatio benevolentiæ » est hors de cause. Le caractère fier et orgueilleux de Galois nous empêche de le penser à la recherche d'une quelque sorte de patronage. Il cite Cauchy parce qu'il voit en lui un mathématicien qui travaille sur sa même matière : une algèbre qui va abandonner le domaine presqu'exclusif des équations et qui va se renouveler par l'usage des *structures*.[9]

3 Galois ne cite pas Lagrange dans le *Premier Mémoire*

Une première remarque qui vient naturelle en comparant les *Réflexions* de Lagrange au *Premier Mémoire* regard les différences de style de l'expositions. Lagrange, comme le titre suggère ne donne pas un exposé structuré. Il n'y a pas des théorèmes, des lemmes de corollaires, etc. Il y a un discours qui procède dans un style que l'on pourrait définir « cartésien ».

Galois, au contraire, bien que à sa manière rapide et essentielle, structure le texte : il y a les *Principes*, le *Lemmes*, les *Propositions*, et une *Application*. C'est une première différence, peut-être suggérée par l'exigence de proposer le texte au jugement des Académiciens, mais il faut la souligner.

8. Les arguments donnés dans (Serret, 1879, p. 250-253 ; 278-281) sont évidemment à la portée de Galois.

9. Sur les rapports personnels entre Cauchy et Galois, il y a déjà, après l'essai de Taton (1971), une littérature considérable. Dans Ehrhardt (2007) il y a beaucoup de références.

Dans (Ehrhardt, 2007) on trouve la remarque suivante relative à l'usage des permutations dans (Lagrange, 1770) :

> . . .si Lagrange les avait utilisées dans ses recherches sur les équations, il s'agissait alors d'avantage d'un procédé calculatoire que d'un outil conceptuel.[10]

La comparaison de l'analyse de la résolubilité de l'équation du quatrième degré donné par Lagrange et Galois montre l'exactitude de cette remarque.

3.1 Lagrange analyse la solution de l'équation du quatrième degré

Considérons une équation du quatrième degré donnée par

$$x^4 + mx^3 + nx^2 + px + q = 0. \tag{1}$$

Dans la *Section* 30 de (Lagrange, 1770), Lagrange observe que, si les quatre racines de l'équation sont indiquées par a, b, c, d, « la combinaison $ab+cd$ des quatre racines a, b, c, d est telle qu'elle n'admet que trois variations, savoir

$$ab + cd, \quad ac + bd, \quad ad + bc. \text{ »}$$

Il s'ensuit qu'il est possible construire une équation du troisième degré, avec les coefficients dans le même domaine des quantités m, n, p, q, qui prend les valeurs $ab + cd, ac + bd, ad + bc$. L'usage du théorème sur les fonctions symétriques donne facilement l'équation

$$u^3 - nu^2 + (mp - 4q)u - (m^2 - 4n)q - p^2 = 0. \tag{2}$$

Lagrange a implicitement utilisé le fait que les permutations de a, b, c, d qui fixent la valeur $ab + cd$ sont un sous-groupe d'indice 3 du groupe totale des permutations de a, b, c, d. Et $ac + bd, ad + bc$ sont les deux autres valeurs sur les classes.

Mais à ce point son analyse ne procède plus en termes de groupes (ou des fonctions qui gardent la même valeur sur un certain sous-groupe), en opposition avec ce que nous verrons dans le texte de Galois. Il observe que, si on imagine que une racine u soit donnée par $u = ab+cd$, on a aussi $ab \cdot cd = q$, ce qui permet d'obtenir ab et cd par l'équation

$$t^2 - ut + q = 0. \tag{3}$$

10. *Ibid.* p. 61. Voir aussi (Neumann *et al.*, 1994, p. 4, 30).

L'analyse de Lagrange continue avec l'observation que, si on pose

$$ab = t', \quad cd = t''$$

on a

$$\begin{aligned} -p = ab(c+d) + cd(a+b) &= t'(c+d) + t''(a+b) \\ a+b+c+d &= -m, \end{aligned}$$

ce qui donne

$$a+b = \frac{p - mt'}{t' - t''}, \quad c+d = \frac{p - mt''}{t'' - t'}. \tag{4}$$

La connaissance de ces valeurs, et des valeurs connues précédemment, c'est à dire $ab = t', cd = t''$, permet d'obtenir les valeurs des racines a, b, c, d.

Cette analyse de Lagrange de la solution de l'équation du degré quatre est très ingénieuse, mais elle ne se fonde pas sur une méthode uniforme. Elle mélange la présence (implicite) d'un sous-groupe du groupe de permutations des racines avec des considérations sur la nature des coefficients de l'équation. On verra dans la section suivante comme l'analyse de Galois, bien que très expéditive, exploite une seule méthode.

3.2 Galois analyse la solution de l'équation du quatrième degré

Galois analyse dans un *Scholie* la solution des équations *générales* du quatrième degré.[11] Il désigne par a, b, c, d les racines et il observe qu'en adjoignant à l'équation une racine carrée (la racine carrée du discriminant, par exemple ; mais Galois ne se donne pas la peine de préciser) on se réduit à un groupe d'ordre douze, qui contient les substitutions

$$\begin{array}{cccc} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{array} \qquad \begin{array}{cccc} a & c & d & b \\ c & a & b & d \\ d & b & a & c \\ b & d & c & a \end{array} \qquad \begin{array}{cccc} a & d & b & c \\ d & a & c & b \\ b & c & a & d \\ c & b & d & a \end{array}$$

11. Voir (Neumann, 2011, p. 122-125).

Ce groupe se partage en trois groupes et « . . .par l'extraction d'un seul radical du 3^e degré » il reste simplement le groupe

$$\begin{array}{cccc} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{array} \tag{5}$$

Galois ne retient pas nécessaire d'indiquer une *fonction des racines* qui prenne trois valeurs différentes sur les trois groupes (c'est à dire en termes modernes sur le groupes et sur les classes). Il y a la fonction évidente $(a, b, c, d) \to ab + cd$, mais Galois laisse à son lecteur de trouver la fonction qu'il retienne plus adéquate. Une fois que le choix est fait, et que le groupe de l'équation est réduit à (5), on a la nouvelle partition en

$$\begin{array}{cccc} a & b & c & d \\ b & a & d & c \end{array} \qquad \begin{array}{cccc} c & d & a & b \\ d & c & b & a \end{array}$$

et une simple extraction de racine carrée donne (par exemple par le moyen de $(a, b, c, d) \to ab - cd$) le groupe

$$\begin{array}{cccc} a & b & c & d \\ b & a & d & c \end{array}$$

qui montre qu'une dernière extraction de racine carrée aboutit à la solution complète.

On voit que toute l'argumentation de Galois se réduit à analyser les structure des groupes qui sont obtenus pas après pas, et le calcul explicite des fonctions des racines qui soient invariable pour toutes le substitution des groupes obtenus est laissé au lecteur. Il se limite à observe en note que « Il suffit pour cela de choisir une fonction symétrique de divers valeurs que prend par toutes le permutations de l'un de groupes partiels [c'est a dire sur le groupe et sur les classes] une fonction qui n'est invariable pour aucune substitutions. »[12] C'est exactement ce que Lagrange a fait dans le premier pas. Mais la stratégie de Lagrange a pris ensuite une autre chemin.

12. C'est a dire une résolvante, qui prend toutes les valeurs possibles. Après (Betti, 1851) on dira une « résolvante de Galois ».

3.3 L'équation $\frac{x^n-1}{x-1}$ (n premier)

Le calcul du « groupe de Galois » de cette équation est un des deux exemple qui Galois donne, à coté de celui de l'équation générale de degré n, pour montrer explicitement comme l'on peut procéder concrètement dans certaines situations simples.[13] La *Note* XIV de (Lagrange, 1808) est une possible source d'inspiration pour Galois et, en tout cas, une comparaison entre les deux textes est intéressante.

Lagrange observe que si r est une racine quelconque de l'équation

$$x^{n-1} + x^{n-2} + \cdots + x + 1 = 0, \tag{6}$$

$$r, r^2, \ldots, r^{n-1}$$

sont toutes les racines de cette équation.[14] Il observe que

> M. *Gauss* a eu l'idée ingénieuse et heureuse de substituer à la progression arithmétique des exposants de r une progression géométrique, en vertu du fameux théorème de *Fermat*, sur les nombres premiers.[15]

Lagrange rappelle ensuite le concept de *racine primitive modulo n* et observe que, étant a une racine primitive, « si dans la série des racines

$$r, \quad r^a, \quad r^{a^2}, r^{a^3}, \quad r^{a^4}, \quad etc. \quad r^{a^{n-2}},$$

on met r^a à la place de r elle devient

$$r^a, \quad r^{a^2}, r^{a^3}, \quad r^{a^4}, \quad r^{a^5}, \quad etc. \quad r,$$

et si on y met r^{a^2} à la place de r elle devient

$$r^{a^2}, \quad r^{a^3}, r^{a^4}, \quad r^{a^5}, \quad r^{a^6}, \quad etc. \quad r, \quad r^a,$$

et ainsi de suite. »[16]

Cette propriété lui suggère d'introduire la quantité

$$t = r + \alpha r^a + \alpha^2 r^{a^2} + \cdots \alpha^{n-2} r^{a^{n-2}} \tag{7}$$

13. Voir (Neumann, 2011, p. 112-113).
14. Voir (Lagrange, 1808, p. 277). J'ai substitué, ici et ensuite, μ, du texte originale de Lagrange, par n.
15. *Ibid.*
16. *Ibid.*, p. 279.

où α est une racine de l'équation $y^{n-1} - 1 = 0$. Il s'ensuit que, si l'on pose $\theta = t^{n-1}$, « . . .en faisant attention de rabaisser les puissances de α et de r au-dessous de α^{n-1} et de r^n, par les conditions $\alpha^{n-1} = 1$ et $r^n = 1$ »[17] on a

$$t^{n-1} = \theta = \xi_0 + \alpha\xi_1 + \alpha^2\xi_2 + \cdots \alpha^{n-2}\xi_{n-2} \tag{8}$$

où les quantités ξ_j « . . .seront des fonctions rationnelles et entières de r, telles qu'elles ne changeront pas par la substitutions de $r^a, r^{a^2}, r^{a^3}, etc.$ à la place de r. »[18] La quantité θ est connue, si l'on suppose de connaître α et donc, en considérant toutes les valeurs possibles de α et en prenant les racines *n-ièmes* on arrive au calcul explicite des racines.[19]

Le but de Galois est, au contraire, simplement celui de montrer, sur cet exemple simple, comme on calcule le groupe de l'équation. Il aussi considère une *racine primitive modulo* n, qu'il nomme g, et observe que toutes les racines $a, b, c, \ldots$ de l'équation (6) peuvent être donné par $a = r, b = r^g, c = r^{g^2}, \ldots$ Il s'ensuit que r est un « élément primitif » et puisque la résolvante, dans ce cas spécial, peut être choisie comme le polynôme du premier membre de la (6), le groupe de l'équation est donné immédiatement par la table

$$\begin{array}{ccccccc} a & b & c & d & \ldots & \ldots & k \\ b & c & d & \ldots & \ldots & k & a \\ c & d & \ldots & \ldots & k & a & b \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ k & a & b & c & \ldots & \ldots & \ldots \end{array} \tag{9}$$

Puisque Galois a simplement voulu donner un exemple du calcul du groupe d'une équation particulière nous n'avons pas un texte qui poursuit en montrant comme on peut arriver au calcul explicite des racines.

Toutefois, en considérant la *Proposition* V du *Premier Mémoire* il est facile de conclure qu'il se serait simplement arrêté à la considération de la quantité (8), en laissant à son lecteur de poursuivre les calculs.[20]

17. *Ibid.*, p. 280.

18. *Ibid.*

19. Lagrange donne des autres simplifications astucieuses, mais je ne m'arrête pas sur ce point.

20. Voir (Neumann, 2011, p. 122-23) où, encore une fois, en face d'une quantité de la forme $(\theta + \alpha\theta_1 + \alpha^2\theta_2 + \cdots \alpha^{p-1}\theta_{p-1})^p$ invariable pour les substitutions cycliques, il ne voit pas la nécessité de citer Lagrange.

3.4 Le Théorème de l'élément primitif : Lagrange et Galois

Il est bien connu que la démonstration du *Lemme* III du *Premier Mémoire*, où Galois démontre sa version du « Théorème de l'Élément Primitif »,[21] a été jugée insuffisante par Poisson. Galois, y répondit par son célèbre « on jugera », en revendiquant la justesse de sa démonstration. La question a été beaucoup débattue par les historiens, qui certaines fois ont pris le parti de Galois et d'autres fois ont accepté l'avis de Poisson.[22]

L'absence de la référence au résultat contenu dans l'article 100 de (Lagrange, 1770) dans le texte du *Premier Mémoire* peut avoir une explication très simple : probablement Galois avait une connaissance indirecte de (Lagrange, 1770), donnée par le résumé fait par Lagrange lui même dans les *Notes* contenues dans (Lagrange, 1808).[23] La *Note* XIII reprend (Lagrange, 1770), mais Lagrange ne retient pas opportun de proposer de nouveau son « Théorème de l'Élément Primitif. »

Toutefois la vive réaction de Galois au jugement de Poisson montre que la question va au delà d'une absence de citation. C'est la différente attitude envers les contenus mathématiques qui est en jeu.

Puisque la question est très débattue, je me limiterai a quelques remarques.

La formulations du résultat de Lagrange est synthétisé très clairement dans (Houzel, 2002) : on a une équation algébrique $f(x) = 0$ qui a les n racines (différentes) $x_1, x_2, \ldots, x_n$. Soient $t(x_1, x_2, \ldots, x_n)$ et $y(x_1, x_2, \ldots, x_n)$ deux fonctions des racines telles que les substitutions laissant t invariant laissent aussi y invariant. Alors y est (en général) fonction rationnelle de t.

La démonstration de Lagrange consiste en un algorithme très élégant.[24]

Supposons donc que $t(x_1, x_2, \ldots, x_n)$ soit une fonction des racines et soient $t_1, t_2, \ldots, t_r$ les différentes valeurs de t qui proviennent de toutes les permutation possibles entre les racines ; soient $y_1, y_2, \ldots, y_r$ les valeurs de y qui proviennent des mêmes permutations.

Si l'on forme le polynôme

$$\theta(X) = (X - t_1)(X - t_2)\cdots(X - t_r) = a_0 + a_1 X + \cdots + a_r X^r, \qquad (10)$$

21. Voir (Neumann, 2011, p. 108-111).

22. On peut voir, par exemple, la *Note* 8 dans (Neumann, 2011, p. 142-143), ou (Edwards, 1984, p. 43, note), ou (Radloff, 2002).

23. Voir (Neumann, 2011, p.).

24. Voir (Lagrange, 1770, pp. 374-379). J'utilise pour simplicité des notations modernes.

ses coefficients a_i sont, a cause du théorème sur les fonctions symétriques, des fonctions des coefficients de l'équation proposée.

Pour la même raisons les r quantités m_k données par

$$\begin{aligned} &t_1^0 y_1 + t_2^0 y_2 + \cdots + t_r^0 y_r = m_0, \\ &t_1^1 y_1 + t_2^1 y_2 + \cdots + t_r^1 y_r = m_1, \\ &\cdots \quad \cdots \quad \cdots \\ &t_1^{r-1} y_1 + t_2^{r-1} y_2 + \cdots + t_r^{r-1} y_r = m_{r-1}, \end{aligned} \tag{11}$$

sont encore des fonctions des coefficients de la proposée.

En multipliant la première ligne par n_0, la seconde par n_1,..., la $r-1$-ième par n_{r-1} et en additionnant on a

$$\begin{aligned} &m_0 n_0 + m_1 n_1 + m_2 n_2 + \cdots + m_{r-1} n_{r-1} = \\ &= (n_0 + n_1 t_1 + n_2 t_1^2 + \cdots + n_{r-1} t_1^{r-1}) y_1 \\ &+ (n_0 + n_1 t_2 + n_2 t_2^2 + \cdots + n_{r-1} t_2^{r-1}) y_2 \\ &\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\ &+ (n_0 + n_1 t_r + n_2 t_r^2 + \cdots + n_{r-1} t_r^{r-1}) y_r. \end{aligned} \tag{12}$$

Lagrange à ce point fait usage, peut-être pour la première fois, de l'idée de son polynôme interpolateur.[25] Soit

$$\nu(X) = n_{r-1} X^{r-1} + \cdots + n_1 X + n_0,$$

ou les quantités n_k doivent être déterminées successivement.

La (12) peut être écrite comme

$$\begin{aligned} &m_0 n_0 + m_1 n_1 + \cdots + m_{r-1} n_{r-1} \\ &= \nu(t_1) y_1 + \nu(t_2) y_2 + \cdots + \nu(t_r) y_r \end{aligned}$$

On peut commencer par déterminer $\nu(X)$ afin qu'il soit

$$\nu(t_j) = 0 \quad \text{for} \quad j \neq k,$$

25. Puisque la structuration de l'algèbre linéaire est encore à venir, Lagrange n'utilise pas le caractère très simple de la matrice (de Vandermonde) du système (11). Cette idée de profiter de la nature particulière d'un système d'équations pour donner une solution « ad hoc » est très commune entre la fin du XVIII^e siècle et le commencement du XIX^e. On peut voir des exemples intéressants analysés dans (Galuzzi, 1994).

Soit donc

$$\frac{\theta(X)}{X - t_k} = \nu(X). \tag{13}$$

Il faut souligner que seulement la quantité t_k est un élément qui n'est pas connu.

Le choix de $\nu(X)$ fait par la (13) donne

$$y_k = \frac{m_0 n_0 + m_1 n_1 + \cdots + m_{r-1} n_{r-1}}{\nu(t_k)} \tag{14}$$

L'algorithme de la division permet d'expliciter la (13) :

$$\begin{aligned}
n_0 &= a_1 + a_2 t_k + \cdots + a_{r-1} t_k^{r-2} + a_r t_k^{r-1}, \\
n_1 &= a_2 + a_3 t_k + \cdots + a_r t_k^{r-2}, \\
n_2 &= a_3 + \cdots + a_r t_k^{r-3}, \\
&\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\
n_{r-1} &= a_r.
\end{aligned} \tag{15}$$

Puisque $\theta'(X) = \nu'(X)(X - t_k) + \nu(X)$ on a

$$\nu(t_k) = \theta'(t_k). \tag{16}$$

Les (15) donnent les quantités n_j en terme des quantités a_j et de t_k ; $\nu(t_k)$ est donné par la (16) et il s'agit donc simplement de substituer dans la (14) pour avoir y_k en fonction de t_k. Puisque le processus ne dépend pas du choix de k, nous avons y comme fonction de t et pour chaque k à t_k correspond exactement y_k.

On peut poser encore

$$\begin{aligned}
c_0 &= m_0 a_1 + m_1 a_2 + \cdots + m_{r-1} a_r, \\
c_1 &= m_0 a_2 + \cdots + m_{r-2} a_r, \\
&\cdots \quad \cdots \quad \cdots \\
c_{r-1} &= m_0 a_r,
\end{aligned}$$

et

$$\phi(X) = c_0 + c_1 X + \cdots + c_{r-1} X^{r-1}.$$

On conclut que, pour chaque k, on a

$$y(t_k) = \frac{\phi(t_k)}{\theta'(t_k)}. \qquad \square$$

Ce calcul de Lagrange est vraiment brillant. Un problème d'algèbre linéaire est reconduit de façon magistrale au calcul d'un polynôme interpolateur et comme solution on arrive à une fonction *calculée explicitement*. Toutefois, une certaine ambiguïté entre la nature des racines (s'agit-il d'une équation générale ou d'une équation donnée en termes numériques ?) rend problématique l'utilisation du résultat de Lagrange tel quel. Souvent dans les textes successives qui exposent la théorie de Galois comme elle va se consolider al fin du XIX^e siècle ce théorème est donné soit en termes de variables indépendants soit pour le cas des équations numériques.[26]

En tout cas Galois considère le cas le plus simple : celui ou t est une fonction qui prend toutes les valeurs possible sur les permutations des racines, c'est-à-dire le cas où le groupe des substitutions qui fixent t se réduit à l'unité.[27] Dans cette situation la démonstration de Lagrange ne pose pas des problèmes ; mais Galois préfère donner le résultat simplement pour les racines elle mêmes. Le résultat générale est un simple conséquence de sa *Proposition* III.

Soit $f(x) = 0$ une équation polynômiale qui a les racines simples

$$x_1, x_2, \ldots, x_n.$$

Galois considère donc une fonction $V(x_1, x_2, \ldots, x_n)$ qui prend $n!$ valeurs (voir la note (27)). Supposons de fixer x_1 au premier place et considérons le polynôme

$$P(t) = \prod [t - V(x_1, x_{i_2}, x_{i_3}, \ldots, x_{i_n}] \tag{17}$$

où le choix de $i_2, i_3, \ldots, i_n$ donne lieu à toutes les permutations possibles entre les nombres $2, 3, \ldots, n$.

Les coefficients de ce polynôme sont des fonctions symétriques des racines $x_2, x_3, \ldots, x_n$ et donc ils peuvent être exprimés en termes des fonctions symétriques de $x_1, x_2, x_3, \ldots, x_n$ (c'est à dire de quantité connues) et de x_1. Indiquons ce polynôme par $P(t, x_1)$ et soit V_1 la valeur de V sur la permutation fondamentale. On a identiquement $P(V_1, x_1) = 0$ et donc le polynôme $P(V_1, x)$ a la racine x_1. On voit facilement que cette racine est la seule commune entre $P(V_1, x)$ et $f(x)$ et donc le plus grand commun diviseur entre ce

26. Voir, par exemple (Bolza, 1890). Mais cette distinction est déjà dans (Dedekind, 1981).

27. Dans le *Lemme* II il a écrit que c'est un affaire de routine la construction d'une telle fonction. Mais on peut voir sur ce point (Edwards, 1984, p. 35-36).

deux polynômes doit être un polynôme du premier degré de la forme

$$A(V_1)x + B(V_1)$$

ce qui donne sur le champ

$$x_1 = -\frac{B(V_1)}{A(V_1)}. \quad \square$$

4 Betti lecteur de Galois

Aujourd'hui nous voyons les contenus du *Premier Mémoire* comme suffisamment clairs.[28] Il y a certainement quelques choses à compléter, mais l'essentiel nous semble donné en forme satisfaisante.[29]

Si donc on regard l'application finale aux équations irréductibles du premier degré solubles par radicaux, l'indépendance du texte de Galois de Lagrange semble bien justifiée, bien que réclamée, peut-être, de façon trop nette.

Mais la même chose ne devait apparaître si évidente aux contemporains ou aux successeurs immédiats de Galois et je veux conclure cet exposé en montrant que la lecture de Enrico Betti de l'œuvre de Galois la insère dans la postérité de Lagrange.

Betti a été le premier mathématicien à donner une contribution à la théorie de Galois, après la publication de Liouville.[30] Il a estimé de devoir compléter l'*Application* aux équations irréductibles de degré premier solubles par radicaux donnée par Galois à la fin du *Premier Mémoire*. Et où Galois évite toute référence à Lagrange, comme nous avons vu, il commence exactement en résumant le contenu d'une partie importante de (Lagrange, 1770).

Il observe que Lagrange a considérée une équation de la forme

$$x^\mu + px^{\mu-1} + qx^{\mu-2} + \cdots + tx + u = 0 \tag{18}$$

où μ est un nombre premier.[31] Les racines de cette équation peuvent être données comme

$$x = -\frac{p}{\mu} + \sum_{n=0}^{n=\mu-1} \sqrt[\mu]{R_n} \tag{19}$$

28. On ne peut dire la même chose pour les parties de l'œuvre de Galois qui ont un caractère plus fragmentaire. Voir, par exemple (Neumann, 1996).

29. En fait, l'exposition du Serret dans (Serret, 1879) suit pas à pas le texte de Galois.

30. dans le mémoire (Betti, 1851).

31. Ce texte est considéré aussi dans (Toti Rigatelli, 1989, pp. 54-55). Sur l'œuvre algébrique de Betti on peut voir (Mammone, 1989).

où

$$R_n = \frac{1}{\mu^\mu} \sum_{i=0}^{i=\mu-1} \left(\alpha^{in} x_i\right)^\mu \tag{20}$$

et les α^i sont les racines de l'unité. Lagrange observe aussi que les R_i sont racines d'une équation de degré $\mu - 1$

$$R^{\mu-1} + PR^{\mu-2} + QR^{\mu-3} + \cdots + SR + T = 0, \tag{21}$$

telle que les coefficients $P, Q, \ldots, S, T$ sont exprimables rationnellement par les coefficients de (18) et par la racine d'une équation de degré $\nu = (\mu - 2)!$

$$P^\nu + aP^{\nu-1} + bP^{\nu-2} + \cdots + rP + s = 0, \tag{22}$$

où $a, b, \ldots, r, s$ sont des fonctions rationnelles de $p, q, \ldots, t, u$.

Cette imposant architecture d'équations peut être simplifié, observe Betti, par un résultat d'Abel : si la (18) est irréductible et soluble par radicaux les coefficients de (21) sont des fonctions rationnelles de $p, q, \ldots, t, u$.

C'est bien ce résultat qui joue un rôle important dans le mémoire de Betti. Après un certain nombre de lemmes qui analysent la structure d'un groupe de substitutions, sous-groupe de S_n, tel que l'identité seulement peut fixer deux éléments, la forme des coefficients de (21) donnée par le théorème d'Abel et la forme des R_n donnée par (20) conduisent facilement au résultat de Galois. On voit bien que cette lecture laisse une peu dans l'ombre la remarque de Galois sur la nature de groupe cyclique qui précède l'identité. La lecture du texte de Galois est donc reconduite à Lagrange.

Il faut souligner que dans le mémoire successif (Betti, 1852) le résultat est donné dans une forme plus simple et en utilisant exactement la structure de l'avant-dernier groupe.[32] En plus dans ce mémoire les travaux de Cauchy sur les substitutions sont considérés. Toutefois la référence à Lagrange est encore dominante.

On voit donc, pour conclure, que l'indépendance de l'œuvre de Galois de celle de Lagrange n'était pas un fait escompté. Elle a eu besoin de lecteurs disponibles à un long et fatigant travail pour saisir des idées qui, a ce temps, seulement ce jeun mathématicien pouvait juger comme évidentes.

32. *Cf.* (Betti, 1852, pp. 73-74).

5 Appendice : l'article de Cauchy sur les nombre des valeurs d'une fonction de n quantités

Une analyse très claire de (Cauchy, 1815a) est donnée en beaucoup de textes. J'ai considéré surtout (Kiernan, 1971-1972) et (Dahan, 1980). Voici la formulation de Cauchy du résultat principal.

Théorème 1 *Le nombre des valeurs différentes d'une fonction de n quantités ne peut s'abaisser au-dessous du plus grand nombre premier p contenu dans n sans devenir égale à* 2 $\diamondsuit$

Proof.– Dans la démonstration je suis, avec quelques modifications, (Kiernan, 1971-1972). Soit $K = K(x_1, x_2, \ldots, x_n)$, et supposons que K prend r valeurs différentes. Il s'ensuit que $rm = n!$ and m est l'ordre du groupe G de qui ne modifient pas K.

Si $r < p$, K ne peut pas être modifié par une permutation d'ordre p. Soit π une permutation d'ordre p. Le groupe cyclique engendré par π, que Kiernan note par (π), répartit le groupe symétrique S_n en $\frac{n!}{p}$ classes. Supposons que

$$m > \frac{n!}{p}. \tag{23}$$

Il s'ensuit que G doit contenir deux éléments dans la même classe. Il doit donc contenir deux éléments σ, τ tels que $\sigma = \alpha\pi^i, \tau = \alpha\pi^j$. Par conséquence

$$\mu = \sigma^{-1}\tau = \pi^{j-i} \in (\pi).$$

Puisque p est premier $(\mu) = (\pi)$ et il s'ensuit que $\pi \in G$. Donc K n'est pas modifiée par π.

Après, Cauchy montre que si la valeur de K n'est pas modifiée par une permutation arbitraire d'ordre p elle n'est pas modifiée par un 3-cycle. En fait si l'on choisi deux permutations comme

$$\begin{pmatrix} \alpha & \beta & \gamma & \delta & \ldots & \zeta & \eta \\ \beta & \gamma & \delta & \epsilon & \ldots & \eta & \alpha \end{pmatrix} \text{ et } \begin{pmatrix} \beta & \gamma & \delta & \epsilon & \ldots & \eta & \alpha \\ \gamma & \alpha & \beta & \delta & \ldots & \zeta & \eta \end{pmatrix}, \tag{24}$$

le produit donne

$$\begin{pmatrix} \alpha & \beta & \gamma & \delta & \ldots & \eta \\ \gamma & \alpha & \beta & \delta & \ldots & \eta \end{pmatrix} = (\alpha\,\gamma\,\beta). \tag{25}$$

Enfin Cauchy démontre que, si la valeur de K n'est pas modifiée par les 3-cycle, K est symétrique ou prend seulement deux valeurs.

Cauchy appelle *transposition* une permutation de la forme

$$\begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix} \tag{26}$$

qu'il la note aussi(α, β), et observe que

$$(\alpha, \beta)(\beta, \gamma) = \begin{pmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \end{pmatrix}. \tag{27}$$

L'invariance par la substitution donnée par le produit de $(\alpha, \beta), (\beta, \gamma)$ montre que, si (α, β) change la valeur K_1 en K_2, alors (β, γ) change K_2 en K_1, et par conséquence aussi K_1 en K_2. Il s'ensuit que deux permutations qui ont un index en commun appliquées à K_1 donnent la même valeur K_2.

De l'égalité

$$(\alpha, \beta)(\beta, \gamma)(\beta, \gamma)(\gamma, \delta) = (\alpha, \beta)(\gamma, \delta) \tag{28}$$

il s'ensuit que (α, β) et (γ, δ) appliquées à K_1 donnent la même valeur K_2.

Toutes les transpositions produisent don la même valeur que $(1, 2)$ produit. Soit cette valeur K_1. Il s'ensuit que une permutation qui est le produit d'un nombre pair de transpositions ne modifie pas la valeur de K_1 pendant que une permutation qui est le produit d'un nombre impair de permutations produit la valeur K_2.

Donc si $K_1 = K_2$, la fonction K est symétrique, autrement elle prend deux valeurs.[33]

33. Kiernan observe que la démonstration de Cauchy assume que $p > 4$. Mais Cauchy considère ce cas à part : « Au reste, comme en supposant $n = 3$ ou $n = 4$, on trouve $p = 3$, on voit que le théorème précédent dans le troisième et le quatrième ordre n'exclut pas les fonctions de trois valeurs". (Cauchy, 1815a, p. 83).

Références

B. Belhoste : *Les sciences dans l'enseignement secondaire français*. Institut national de recherche pédagogique, Paris, 1995.

E. Betti : Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo. *Annali di scienze matematiche e fisiche*, II:5–19, 1851. In (Betti, 1903, pp. 31-80).

E. Betti : Sulla risoluzione delle equazioni algebriche. *Annali di scienze matematiche e fisiche*, III:49–115, 1852. In (Betti, 1903, pp. 17-27).

E. Betti : *Opere matematiche*, volume I. Hoepli, Milano, 1903.

O. Bolza : On the theory of substitutions-groups and its applications to algebraic equations. *American Journal of Mathematics*, 13:59–144, 1890.

A. L. Cauchy : Mémoire sur le nombre des valeurs qu'une fonction peut acquérir lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme. *Journal de L'École Polytechnique*, 10 (17 cahier):1–27, 1815a. *Œ uvres*, (2), 1, pp. 64-90.

A. L. Cauchy : Mémoire sur les fonctions qui ne peuvent obtenir que deux valeurs égales et de signes contraires par suite des transpositions operées sue les variables qu'elles renferment. *Journal de L'École Polytechnique*, 10 (17 cahier):29–112, 1815b. Œuvres, II, 1, 91-169.

A. L. Cauchy : Sur le nombre des valeurs égales ou inégales que peut acquerir une fonction de n variables indépendantes, quand on permute ces variables entre elles d'une manière quelconque. *Compte Rendus*, pages 779–797, 1845. *Œuvres*, (1), 9, pp. 323-341.

A. Dahan : Les récherches algébriques de Cauchy. Rapport technique, These de troisième cycle, Paris, 1979.

A. Dahan : Les travaux de Cauchy sur les substitutions. Étude de son approche du concept de groupe. *Archive for history of exact sciences*, 23:279–319, 1980.

J. W. R. Dedekind : Eine Vorlesung über Algebra. *In Scharlau (1981)*, pages 59–100, 1981.

H. M. Edwards : *Galois Theory*. Springer-Verlag, New York, etc., 1984.

C. Ehrhardt : *Évariste Galois et la théorie des groupes. Fortunes et réélaborations (1811-1910)*. Thèse de doctorat, Paris, 2007. École des hautes études en sciences sociales.

E. Galois : Démonstration d'un théorème sur les fractions continues périodiques. *Annales de mathématiques pures et appliquées*, 19:294–301, 1829.

M. Galuzzi : L'interpolazione trigonometrica in Gauss, Bessel e Cauchy. *In* C.F. Manara, G. Faliva et M. Marchi, éditeurs : *Scritti in onore di Giovanni Melzi*, pages 173–212. Vita e Pensiero, Milano, 1994.

C. Houzel : *La géométrie algébrique*. Blanchard, Paris, 2002.

B. M. Kiernan : The development of Galois theory from Lagrange to Artin. *Archive for history of exact sciences*, 8:40–154, 1971-1972.

J.-L. Lagrange : Sur la résolution des équations numériques. *Histoire de l'Académie royale des Sciences et Belles-lettres (Berlin)*, 23 (1767):311–352, 1769.

J.-L. Lagrange : Réflexions sur la résolution algébrique des équations. *Mémoires de l'Académie royale des sciences et Belles-Lettres de Berlin*, pages 205–421, 1770. Publié dans 1772. *Œuvres*, 3, 205-421.

J.-L. Lagrange : *Traité de la résolution des équations numériques de tous les degrés*. Courcier, Paris, 1808. Nouvelle édition revue et augmentée par l'auteur.

P. Mammone : Sur l'apport d'Enrico Betti en théorie de Galois. *Bollettino di storia delle scienze matematiche*, 9 (2):143–169, 1989.

O. Neumann : Die Entwicklung der Galois-Theorie zwischen Arithmetik und Topologie (1850 bis 1960). *Archive for history of exact sciences*, 50:291–329, 1996.

P. Neumann : *The mathematical writings of Évariste Galois*. The European Mathematical Society, 2011. Édition critique intégrale du texte avec traduction anglaise.

P. M. Neumann, G. A. Stoy et E. C. Thompson : *Groups and Geometry.* Oxford Science Publications, Oxford, 1994.

I. Radloff : Évariste Galois : principles and applications. *Historia Mathematica*, 29:114–137, 2002.

W. Scharlau, éditeur. *Richard Dedekind 1831-1981. Eine Würdigung zu seinem 150. Geburtstag*, Braunschweig, 1981. F. Vieweg und Sohn.

J.-A. Serret : *Cours d'algèbre supérieure*, volume 2. Gauthier-Villars, Paris, 1879. Quatrième édition. Éditions Jacques Gabay, 1992.

R. Taton : Sur les relations scientifiques d'Augustin Cauchy et d'Evariste Galois. *Revue d'histoire des sciences*, 24:123–148, 1971.

L. Toti Rigatelli : *La mente algebrica. Storia dello sviluppo della teoria di Galois nel XIX secolo.* Bramante Editrice, Busto Arsizio, 1989.