Résolubilité des équations par radicaux et premier mémoire d'Evariste Galois

par Amy DAHAN-DALMEDICO.

Ce qu'on appelle la Théorie de Galois est aujourd'hui un chapitre classique des mathématiques. Du point de vue historique et épistémologique, elle a donné lieu à de nombreuses études dont nous citons quelques-unes dans notre bibliographie.

Quant aux écrits d'Evariste Galois lui-même ils tiennent en très peu de pages qui restent difficiles d'accès. La plupart des commentateurs se sont d'ailleurs tenus éloignés du texte original, le jugeant trop peu clair (*).

Or la personnalité, la trajectoire d'Evariste Galois sont suffisamment singulières et attachantes pour qu'on éprouve le désir de se confronter à ses écrits ; non seulement sa cinglante Préface écrite à la prison Sainte-Pélagie ou sa lettre sur l'Enseignement des Sciences mais aussi ses textes mathématiques.

Evariste Galois pensait que la vérité de la science ne devait pas se présenter comme un ordre achevé et immuable mais plutôt dans le mouvement de l'invention toujours inachevée sans cesse rectifiée. Sur un point au moins, cette exigence a été entendue : l'édition critique intégrale de ses écrits (par R. Bourgne et J.P. Azra) permet le contact exceptionnel avec l'œuvre vécue, vivante du jeune mathématicien, telle qu'elle a été déchiffrée dans ses manuscrits, non séparés des ébauches, des tâtonnements de la naissance, des hésitations de l'invention, marquée par les circonstances impitoyables de sa vie. Cette édition constitue un exemple absolument unique et priviligié d'œuvre mathématique non divorcée de son auteur qui n'a pas pu et pas voulu s'effacer de ses travaux.

Nous nous sommes donc fixé comme objectif de faciliter la lecture directe de Galois, au moins celle du "Premier Mémoire" de 1831, refusé par Poisson.

Pour cela, après avoir dans un premier temps retracé les grandes lignes de l'histoire de la résolubilité des équations par radicaux, nous proposons une lecture du Mémoire, très proche des termes mêmes de Galois, que nous avons quelquefois traduits dans la formulation contemporaine que permet la théorie profonde sous-jacente telle qu'elle s'est révélée par phases successives jusqu'à Artin près d'un siècle plus tard.

Ce parti pris, inévitablement un peu lourd et filandreux, suscitera — nous l'espérons — un mouvement vers l'œuvre de Galois elle-même ; car comme le dit si bien R. Bourgne : "*ce qu'elle apporte c'est ce qu'aucun exposé doctrinal n'apportera ; car c'est la marque du créateur que de dire ce que personne ne dira comme il le dit, tant il est vrai que l'eau aura toujours un autre goût à sa source que dans une cruche*".

(*) C'est en particulier le cas de Verriest au début du siècle dont l'analyse sert de trame à bien d'autres analyses ultérieures, notamment celle de M. Kline et celle, très profonde, de J. Vuillemin.

Première partie : La problématique de la résolubilité des équations par radicaux

INTRODUCTION

A l'origine — chez les Babyloniens et les Grecs — l'algèbre ne se distingue guère de l'arithmétique, elle-même dans un état très primitif. Puis, très lentement, le processus historique d'élaboration des règles du calcul algébrique abstrait — calcul portant sur des expressions contenant une inconnue — mûrit et se développe, très lié à celui de l'élaboration de l'arithmétique. L'objet presque exclusif de cette discipline reste jusqu'au début du XIX^{e} siècle, les équations.

La théorie des équations du second degré, du moins dans l'ensemble des rationnels positifs, est acquise dans le *Précis sur le calcul de al-jabr et al-muquabala* d'Al Khwarizmi (1ère moitié du IX^{e} siècle).

Puis la résolution des équations du troisième degré arrête les mathématiciens très longtemps. Ibn Al-Haythan, Al-Khayyam (XI^{e} siècle) et d'autres tentent surtout la construction géométrique des racines des équations du 3^{e} degré, en particulier par l'intersection de deux coniques.

Enfin au cours du XVI^{e} siècle, les algébristes italiens de la Renaissance — Scipione del Ferro, Tartaglia, Cardan, Ferrari, Bombelli — donnent les formules de résolution par radicaux des équations des 3^{e} et 4^{e} degrés.

Pendant plus de deux siècles, les mathématiciens chercheront toujours des méthodes de résolution des équations de degré quelconque. Faute de les trouver, ils étudient des méthodes de résolution numérique, règles pour séparer les racines, trouver le nombre des racines réelles (Descartes, puis Stirling et De Gua au XVIII^{e} siècle), règles pour déterminer les signes des racines, méthodes d'approximation de Newton, de Lagrange, etc.

Mais la résolution algébrique des équations de degré supérieur à quatre, c'est-à-dire le fait de trouver une expression algébrique composée avec les coefficients d'une équation donnée et qui, substituée à l'inconnue, satisfasse identiquement à cette équation, reste un point noir crucial de la théorie des équations.

Les premières tentatives sérieuses de résolution viennent de la part d'un ami de Leibniz, Tchirnhaus (1651-1708) qui s'efforce en 1689 de ramener toute équation algébrique, par un certain changement de variable, à une équation binôme de la forme $x^n - C = 0$, que Cotes et De Moivre avaient résolue par division des arcs, c'est-à-dire :

$$x_k = C^{1/n}\left(\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}\right).$$

Tchirnhaus part de l'équation de degré n , $P(x) = 0$, et pose $y = Q(x)$, où Q est un polynôme de degré $n - 1$ à coefficients indéterminés. Il élimine x entre les deux équations :

$$P(x) = 0$$

et

$$Q(x) - y = 0$$

et cherche à déterminer les coefficients du polynôme Q de façon à faire disparaître de l'équation résultante en y , certains ou tous les termes intermédiaires. La méthode réussit fort bien pour $n = 3$, mais pour $n = 5$ la recherche des coefficients de Q conduit à une équation du 24e degré qui ne peut s'abaisser. Euler et Bezout étudieront le même problème au XVIIIe siècle par des procédés assez voisins mais en ne progressant guère.

En 1770, paraissent deux mémoires très importants de Van der Monde et Lagrange sur le sujet. Ils mettent fin à la période de recherche plus ou moins empirique des méthodes de résolution. Celui de Lagrange surtout aura une influence considérable sur les fondateurs de la nouvelle algèbre.

LE MÉMOIRE DE LAGRANGE

"*Je me propose,* déclare Lagrange, *d'examiner les différentes méthodes que l'on a trouvées jusqu'à présent pour la résolution algébrique des équations, de les réduire à des principes généraux et de faire voir a priori pourquoi ces méthodes réussissent pour le 3e et le 4e degré et sont en défaut pour les degrés ultérieurs*".

L'analyse de Lagrange porte davantage sur les méthodes que sur les équations ; il examine toutes les tentatives de ses prédécesseurs Scipione del Ferro, Tartaglia, Cardan, Ferrari, Descartes, Tchirnhaus, Euler, De Moivre, établit le bilan systématique de leurs entreprises puis compare les méthodes entre elles afin d'en déduire leur portée et leurs limites.

Au terme de cet examen, Lagrange montre qu'elles reviennent toutes au fond à faire dépendre la résolution de l'équation proposée de celle d'une autre équation auxiliaire — la "*réduite*" — dont les racines y_k sont composées linéairement des racines x_h de l'équation donnée et des puissances d'une racine nième de l'unité.

Ces expressions $y_k = \sum_{h=1}^{n} w_k^h x_h$, $1 \leqslant k \leqslant n$

où w_k prend successivement comme valeurs celles des n racines nièmes de l'unité, sont appelées les *résolvantes de Lagrange*. On aura évidemment progressé dans la résolution de l'équation initiale si l'équation auxiliaire obtenue peut s'abaisser à un degré inférieur à celui de la proposée.

Lagrange montre clairement que la résolubilité de l'équation cubique est liée à l'existence d'une fonction de trois variables, ne prenant que deux valeurs distinctes par permutation de ces variables au lieu des six valeurs que l'on pouvait théoriquement prévoir puisqu'il y a six permutations possibles de trois objets. En effet, si l'équation du 3e degré a pour racines x_1, x_2, x_3 , l'expression $(x_1 + w x_2 + w^2 x_3)^3$ où w est une racine cubique non réelle de l'unité ne prend que deux valeurs qui sont $(x_1 + wx_2 + w^2x_3)^3$ et $(x_1 + w^2x_2 + wx_3)^3$ par permutation des lettres ; l'équation auxiliaire réduite est ici une équation du second degré ayant pour racines les deux résolvantes $x_1 + wx_2 + w^2x_3$ et $x_1 + w^2x_2 + wx_3$.

Quand on passe au cas de l'équation du 4e degré, la situation est analogue : la résolubilité par radicaux est liée à l'existence d'une fonction de quatre variables et ne prenant que trois valeurs distinctes par permutation de ces variables ; il s'agit ici de l'expression $\frac{1}{2}(x_1 x_2 + x_3 x_4)$. Dans la méthode de Ferrari, ces trois valeurs distinctes sont les racines de la réduite qui est du 3e degré. Dans les méthodes de Descartes et de Tchirnhaus, la réduite est du 6e degré mais s'abaisse immédiatement au troisième.

Ensuite, dans un deuxième moment de son mémoire, Lagrange montre que les racines de l'équation initiale s'expriment comme fonctions rationnelles des racines de l'équation auxiliaire (c'est-à-dire les résolvantes) et des coefficients de l'équation initiale. Cela permet à Lagrange de ne pas se satisfaire de l'analyse a posteriori des méthodes existantes mais de reconstruire par un procédé direct et a priori, les équations auxiliaires réduites en utilisant les propriétés des résolvantes et des racines primitives de l'unité. Il montre qu'au-delà du 4e degré, l'équation auxiliaire est de degré supérieur à celui de l'équation initiale donnée et ne paraît pas susceptible d'abaissement.

Les conclusions auxquelles aboutit Lagrange ne sont donc pas définitives. Du moins éviteront-elles des tentatives inutiles. Il conclut : "*Si la résolution algébrique des équations de degrés supérieurs au quatrième n'est pas possible, elle doit dépendre de quelques fonctions des racines, différentes de la précédente*". De plus ces résultats ont permis de "*donner à cette occasion les vrais principes et pour ainsi dire la vraie métaphysique de la résolution des équations du troisième et du quatrième degré*".

Chemin faisant, Lagrange a démontré les premières propositions que l'on peut rattacher à la théorie des groupes :

— d'une part : le nombre des valeurs distinctes que peut prendre une fonction de n variables par permutation de ces variables, est un diviseur de n! ; ceci, avec le même raisonnement que l'on suit aujourd'hui pour montrer que l'ordre d'un sous-groupe divise l'ordre du groupe. En effet n! est l'ordre du groupe symétrique S_n de toutes les permutations de n lettres et le nombre des valeurs distinctes est l'indice dans S_n du sous-groupe des permutations qui laissent la fonction inchangée.

— d'autre part un théorème profond sur les fonctions "semblables" de racines, qu'on peut rattacher à la future théorie de Galois. De quoi s'agit-il ? : quand une fonction donnée de n lettres ne change pas quand on y effectue une certaine substitution, on dit que cette fonction *admet* cette substitution ; et deux fonctions de n lettres seront dites *semblables* si les groupes de substitutions laissant les deux fonctions invariantes sont identiques.

La première proposition de Lagrange affirme que si une fonction $\phi(x_1, x_2, \ldots, x_n)$ des racines d'une équation de degré n admet toutes les substitutions admises par une autre fonction $\psi(x_1, x_2, \ldots, x_n)$ de ces racines (et éventuellement d'autres que ψ n'admet pas), alors la fonction ϕ peut s'exprimer rationnellement par la fonction ψ et les coefficients de l'équation.

En particulier si ϕ et ψ sont semblables, chacune s'exprime rationnellement en fonction de l'autre et des coefficients de l'équation. La démonstration donnée par Lagrange fournit en même temps une méthode pour construire l'expression de ϕ en fonction de ψ .

La seconde proposition de Lagrange (dont la première devient un cas limite avec $r = 1$) dit que si une fonction $\phi(x_1, x_2, \ldots, x_n)$ des racines d'une équation n'admet pas toutes les substitutions admises par une fonction $\psi(x_1, x_2, \ldots, x_n)$ mais si elle prend, par les substitutions qu'admet ψ , r valeurs distinctes, alors ϕ est racine d'une équation de degré r dont les coefficients sont des expressions rationnelles de ψ et des coefficients de l'équation initiale donnée.

La méthode de Lagrange, quand il utilise ces théorèmes, revient à construire une suite de fonctions des racines $x_1, \ldots, x_n$, dont la première ϕ_0 doit être une fonction symétrique (par exemple l'une des fonctions symétriques élémentaires égales à un coefficient de l'équation) et dont la dernière est une racine, par exemple x_1 ; ainsi :

$$\phi_0(x_1, \ldots, x_n), \phi_1(x_1, \ldots, x_n), \phi_2(x_1, \ldots, x_n), \ldots,$$
$$\phi_{k-1}(x_1, \ldots, x_n), \phi_k(x_1, \ldots, x_n) = x_1$$

ϕ_0 admet les n! substitutions. ϕ_1 n'en admet qu'un certain nombre et donc prend par ces n! substitutions r valeurs distinctes ; ϕ_1 sera donc racine d'une équation de degré r dont les coefficients sont des expressions rationnelles de ϕ_0 et des coefficients de l'équation initiale donnée; de même ϕ_2 prend s valeurs distinctes par les substitutions qu'admet ϕ_1 et sera donc racine d'une équation de degré s dont les coefficients sont des expressions rationnelles de ϕ_1 et des coefficients de l'équation initiale donnée. Ces coefficients seront donc connus dès que l'équation de degré r dont ϕ_1 est racine, est résolue.

On continue ainsi de proche en proche jusqu'à former une équation dont la dernière fonction $\phi_k = x_1$ est racine. On obtient ainsi une série de k équations auxiliaires et si par exemple on peut choisir $\phi_0, \phi_1, \ldots, \phi_k$ en sorte qu'elles soient toutes racines d'équations binômes, on aura résolu algébriquement l'équation initiale proposée. Mais pour l'équation du 5e degré, Lagrange ne réussit pas à trouver des fonctions ϕ qui donnent lieu à des équations auxiliaires binômes. En fait, ces théorèmes anticipent l'idée galoisienne de suite de composition.

Le Mémoire de Lagrange remarquable par sa construction et sa démarche, représente un bilan méthodologique de toutes les recherches algébriques antérieures. Si la question centrale reste la solution des équations, bien des notions nouvelles et profondes relatives à la théorie des substitutions y affleurent.

RÉSOLUBILITÉ DE L'ÉQUATION $x^{17} - 1 = 0$

En 1801, paraissent les *Disquisitiones Arithmeticae* de Gauss, admirable œuvre de jeunesse qui constitue l'acte de naissance de la théorie moderne des nombres et détermine ses directions principales jusqu'à nos jours. Cet ouvrage est très riche de nombreuses structures implicites qui y sont à l'œuvre.

Mais c'est surtout la dernière section consacrée à la constructibilité à la règle et au compas du polygone régulier à 17 côtés qui nous intéresse ici. En effet, déjà Van der Monde avait étudié la résolubilité par radicaux des équations $x^p - 1 = 0$, dites cyclotomiques ou de division du cercle. On a vu que leurs racines s'écrivent

$$x_k = \cos \frac{2k\pi}{p} + i \sin \frac{2k\pi}{p}, \quad k = 0, 1, 2, \ldots, p-1 ;$$

mais une telle solution trigonométrique n'est pas forcément algébrique. Van der Monde avait résolu l'équation $x^{11} - 1 = 0$, mais son mémoire, difficile à suivre, n'a pas eu d'impact immédiat.

Gauss, lui, applique brillamment la même idée de méthode que celle de Van der Monde au cas de l'équation $x^{17} - 1 = 0$. La proposition qui se trouve à la base du raisonnement est la suivante : si les fonctions symétriques de n variables sont dans un corps donné K , alors ces n variables sont racines d'une équation à coefficients dans ce corps.

Si $r = e^{2i\pi/17}$, les racines de l'équation s'écrivent : $1, r, r^2, \ldots, r^{16}$

et l'on a $1 + r + r^2 + \ldots + r^{16} = 0$.

L'idée est de trouver des sous-sommes disjointes $\sigma_1, \sigma_2 \ldots, \sigma_e$ (avec $e < 17$) de la somme des racines, de façon que les fonctions symétriques des σ_i soient toutes rationnelles. D'après la proposition que l'on vient d'énoncer, les σ_i seront racines d'une équation de degré $e < p$, à coefficients rationnels. On considère ensuite comme connues ces quantités σ_i — Galois dira justement qu'on les a "*adjointes*" au corps des coefficients rationnels — et on essaie de trouver des sous-sommes disjointes $\tau_1, \tau_2, \ldots, \tau_{e'}$, de certaines des σ_i dont les fonctions symétriques peuvent s'exprimer comme fonctions rationnelles de $\sigma_1, \sigma_2, \ldots, \sigma_e$. Dans ce cas, les τ_i seront racines d'une équation de degré e' , dont les coefficients sont des fonctions rationnelles des σ_i . Et on répètera le processus en considérant cette fois connues les τ_i . L'idée est d'aboutir à des sous-sommes w_i réduites éventuellement à un seul terme, et donc racines de l'équation initiale, mais qui soient racines d'une équation de degré inférieur à p et dont les coefficients soient des fonctions rationnelles des sous-sommes précédentes.

Gauss utilise des propriétés arithmétiques finies pour effectuer la division en sous-sommes successives et résout l'équation $x^{17} - 1 = 0$ au moyen de quatre équations quadratiques successives ; ainsi les racines sont dans une extension de Q de degré 2^4 et donc sont constructibles à la règle et au compas.

Nous verrons que le procédé de Gauss, lui aussi, contient dans un cas particulier et de manière implicite l'idée galoisienne de suite de composition du groupe d'une équation.

LES PREMIERS TRAVAUX DE CAUCHY SUR LES SUBSTITUTIONS

En 1815, le jeune Augustin-Louis Cauchy publie deux mémoires dans lesquels il traite du problème suivant, issu de la théorie des équations : chercher le *Nombre des valeurs qu'une fonction peut acquérir lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme.* C'est d'ailleurs le titre du premier mémoire. Cauchy démontre que pour une fonction de n lettres, ce nombre ne peut être inférieur à n , prouvant définitivement qu'il ne fallait donc pas espérer trouver une fonction de 5 lettres prenant moins de 5 valeurs distinctes (sauf si elle en prenait 2) ; la problématique de Lagrange conduisait donc à une impasse dans le cas de l'équation du 5e degré.

Mais surtout, alors que Lagrange ne possédait aucune notation maniable pour la notion de permutation, et que sur ce point son exposé est très fastidieux à suivre, Cauchy invente une notation en deux lignes pour les substitutions, l'image de toute lettre se lisant sur la deuxième ligne en dessous de cette lettre ; notation qu'il abrège encore en $\binom{A}{B}$. Cette notation est déjà significative car elle permet une manipulation algébrique sans appel aux lettres elles-mêmes et conduit à la définition du produit de deux substitutions, à la notion d'ordre d'une substitution comme étant la plus petite puissance d'une substitution $\binom{A}{B}$ telle que $\binom{A}{B}^n$ soit l'identité. Cauchy étudie ce que nous appelons le groupe cyclique engendré par une substitution donnée d'ordre n . Mais il n'y a pas encore de notion générale d'un ensemble de substitutions fermé pour la loi du produit, ce que Galois appellera groupe ou que Cauchy nommera plus tard, en 1844, système de substitutions conjuguées.

Abel et Galois liront ce mémoire de Cauchy qui jette les bases d'une théorie autonome des substitutions et lui emprunteront plusieurs éléments, dont le résultat central.

ABEL ET L'IRRÉSOLUBILITÉ DE L'ÉQUATION DU 5e DEGRÉ

L'impossibilité de résoudre par radicaux les équations générales de degré supérieur ou égal à cinq, fut finalement démontrée en 1826 par le jeune mathématicien norvégien Niels Heinrik Abel (1802-1829) dans un mémoire très technique et calculatoire, bien dans la tradition du XVIIIe siècle.

Puisque résoudre algébriquement une équation c'est exprimer ses racines par des fonctions algébriques des coefficients, Abel commence par une recherche de la forme générale des fonctions algébriques qu'il classifie très minutieusement suivant le nombre de radicaux qu'elles contiennent et leur agencement dans l'expression.

Puis Abel examine à quelles conditions doit satisfaire par sa nature une équation résolue algébriquement, c'est-à-dire qui admet comme racine une fonction algébrique, déterminée et classifiée précédemment. Et cette deuxième question se précise : quelles sont les relations qui existent en cas de résolubilité d'une équation entre une racine et les autres ?

Abel aboutit au fait que, dans ce cas, on peut toujours "*donner à la racine une forme telle que toutes les fonctions algébriques dont elle est composée puissent s'exprimer par des fonctions rationnelles des racines de l'équation proposée*". Au terme d'un très long calcul, Abel prouve que toute expression rationnelle de cinq quantités qui prend cinq valeurs distinctes, doit être de la forme

$$r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4$$

où les r_i sont des expressions symétriques de ces cinq quantités et x l'une d'elles. Il peut enfin conclure à l'irrésolubilité par radicaux de l'équation générale du 5e degré.

Le mémoire d'Abel relativement ancien dans sa technique et dans sa forme, résolvait néanmoins une question que se posaient les géomètres depuis des siècles, et ouvrait de nouvelles voies de recherches : caractériser les classes d'équations résolubles. Abel devait lui-même étudier les équations qui proviennent de la division de la lemniscate, par analogie avec les équations cyclotomiques, qui sont équivalentes à la division du cercle en n arcs égaux. et aboutir aux équations dites abéliennes, qui sont résolubles par radicaux.

Avec ce mémoire, le long chapitre de l'algèbre classique se termine : en effet, la théorie des équations, sous sa forme traditionnelle, est pour l'essentiel épuisée.

Deuxième partie : L'écrit de Galois

Le problème essentiel traité par Galois est donc celui de la résolubilité des équations par radicaux, non seulement cette fois le cas de l'équation générale du 5e degré ou celle de degré n , mais son objectif est bien de déterminer un critère pour toutes les équations algébriques particulières. Nous allons suivre son Mémoire, en nous tenant le plus près de ses écrits, mais en faisant néanmoins appel à certains concepts explicitement absents de l'œuvre de Galois mais qui y fonctionnent largement. Précisons encore que la lecture de Galois n'est pas chose allant de soi : la rédaction est concise à l'extrême, les références sont laconiques, les raisonnements à peine esquissés ; d'ailleurs de nombreuses démonstrations lacunaires seront entièrement reconstruites par Camille Jordan. Enfin nous analyserons séparément les difficultés spécifiques liées aux aspects structuraux de la théorie des groupes.

Galois commence par éclaircir la notion de quantité *rationnelle* par rapport à d'autres quantités. Il la définit en ces termes : "*... on pourra convenir de regarder comme rationnelle toute fonction rationnelle d'un certain nombre de quantités déterminées, supposées connues à priori ; par exemple, on pourra choisir une certaine racine d'un nombre entier, et regarder comme rationnelle, toute fonction rationnelle de ce radical.*

Lorsque nous conviendrons de regarder ainsi comme connues de certaines quantités, nous dirons que nous les ADJOIGNONS à l'équation qu'il s'agit de résoudre. Nous dirons que ces quantités sont ADJOINTES à l'équation.

Cela posé, nous appellerons RATIONNELLE toute quantité qui s'exprimera en fonction rationnelle des coefficients de l'équation et d'un certain nombre de quantités ADJOINTES à l'équation et convenues arbitrairement.

Quand nous nous servirons d'équations auxiliaires, elles seront rationnelles si leurs coefficients sont rationnels en notre sens''.

Ces notions de quantité rationnelle et d'adjonction déjà entrevues dans le Mémoire de Van der Monde et surtout chez Gauss, sont ici tout à fait explicites et Galois approche par ce biais le concept de corps engendré par un ensemble de nombres algébriques. De plus, la considération des quantités adjointes relativise la notion de quantité rationnelle puisque les quantités adjointes sont traitées comme connues quoique irrationnelles. Galois souligne : ''*on voit au surplus que les propriétés et les difficultés d'une équation peuvent être tout à fait différentes suivant les quantités qui lui sont adjointes. Par exemple, l'adjonction d'une quantité peut rendre réductible une équation irréductible*''. Galois donne l'exemple de l'équation cyclotomique $x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$ (avec p premier), irréductible sur le corps Q des rationnels. Mais si l'on adjoint à ce corps la racine $p^{ième}$ primitive de l'unité ($\theta = e^{2i\pi/p}$), elle se factorise en $(x - \theta)(x - \theta^2) \ldots (\chi - \theta^{p-1}) = 0$ et est donc réductible sur le corps $Q(\theta)$.

Ainsi, dès les premières lignes de son mémoire, la résolubilité d'une équation cesse pour Galois d'être un problème absolu qui appelle d'emblée une réponse définitive. Elle va être conçue comme un lien entre un certain être algébrique, l'équation, et son ''milieu'', le corps ou domaine de rationnalité auquel on la rapporte. La résolubilité devient relative à ce domaine.

Vient ensuite une série de lemmes préparatoires :

— Premièrement, il existe une fonction rationnelle V des racines qui prend des valeurs toutes distinctes quand on effectue sur les racines toutes les permutations possibles ; Galois la détermine en prenant une combinaison linéaire des racines à coefficients entiers distincts. V étant choisie, toutes les racines de l'équation proposée sont fonctions rationnelles de V. Galois redémontre ce résultat à partir de propriétés de divisibilité de polynômes, mais il découle aussi de la première proposition de Lagrange sur les fonctions semblables, évoquée dans la première partie, comme devait d'ailleurs le noter Poisson, rapporteur du Mémoire. En langage actuel, on dit que V est l'élément primitif de l'extension/corps des racines, au dessus du corps des coefficients.

— Deuxièmement, soit $P = 0$ l'équation irréductible dont V est racine, que Galois suppose connue. Si $a = f(V)$ est une racine de l'équation initiale proposée, et si V' est une autre racine de $P = 0$, alors $b = f(V')$ sera aussi racine de l'équation proposée. Et la démonstration relève des mêmes idées que le précédent.

Ensuite Galois introduit le concept-clé de ''groupe de l'équation'' : ''*soit une équation donnée dont a, b, ... 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, invariable par les substitutions de ce groupe soit rationnellement connue ;

2) réciproquement, que toute fonction des racines déterminable rationnellement soit invariable par ces substitutions''.

Le groupe d'une équation de degré n sur un corps donné, qui est le plus petit corps contenant les coefficients, n'est donc pas le groupe de toutes les permutations entre les n racines — c'est-à-dire le groupe symétrique S_n d'ordre n! — mais un sous-groupe de ce groupe, formé des substitutions qui laissent invariantes toutes les relations entre les racines, donc qui conservent les expressions polynômiales des racines dont la valeur appartient au corps de base K. En langage moderne, la première propriété de Galois définissant le groupe de l'équation exprime que le corps des coefficients est le corps des invariants du groupe G ; la deuxième indique que les éléments de G définissent un groupe de K-automorphismes du corps des racines.

Considérons par exemple l'équation $x^4 - x^2 - 2 = 0$. Elle peut se mettre sous la forme $(x^2 - 2)(x^2 + 1) = 0$ et ne peut pas se réduire davantage sur le corps Q. Elle admet quatre racines :

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

On a les relations :

$x_1 x_2 = -2$, $x_1 + x_2 = 0$, $x_3 x_4 = +1$, $x_3 + x_4 = 0$.

Le groupe de cette équation comprendra quatre substitutions seulement : l'identité, la substitution S qui échange x_1 et x_2 et laisse fixes x_3 et x_4, la substitution T qui échange x_3 et x_4 et laisse fixes x_1 et x_2 et la substitution ST qui échange à la fois x_1 et x_2 d'une part, x_3 et x_4 d'autre part. (En effet, la relation $x_1 + x_2 = 0$ ne serait pas conservée par une autre de ces substitutions).

Ainsi Galois se sert du groupe d'une équation comme d'un miroir dans lequel se reflètent les difficultés de résolution de celle-ci. Le groupe permet de mesurer ce que Verriest a, par la suite, appelé ''l'indiscernabilité'' des racines sur le corps. Sur notre exemple, par rapport au corps des coefficients qui est le corps des rationnels, les deux couples (x_1, x_2) et (x_3, x_4) sont indiscernables, et au sein de chaque couple les racines sont aussi indiscernables. Mais l'adjonction à Q de l'élément $\sqrt{2}$ détermine les racines x_1 et x_2, sans permettre de distinguer encore x_3 et x_4. Sur le corps $Q(\sqrt{2})$, le groupe de l'équation se réduit à l'identité et la substitution qui échange x_3 et x_4.

Mais d'une certaine façon cette analyse de la résolubilité d'une équation, par les extensions successives du domaine de rationalité qui vont de pair avec le procédé de décomposition du groupe en sous-groupes emboîtés, est une analyse a posteriori quand on suppose connues les racines.

Le problème que se pose Galois une fois la définition du groupe donnée, est d'examiner *a priori* comment peut se réduire le groupe de l'équation. Le centre d'intérêt se déplace donc de l'équation elle-même, vers son groupe.

Quand une équation n'est pas résolue, il n'existe pas de moyen de déterminer à coup sûr l'élément primitif du corps des racines. Dans les propositions II, III, IV du Mémoire, Galois envisage d'adjoindre "la racine r d'une équation auxiliaire irréductible (R = 0) de degré premier", c'est-à-dire la valeur r numérique d'une certaine fonction rationnelle ϕ_1 des racines. Il énonce le théorème :

"1°) Il arrivera de deux choses l'une : ou bien le groupe de l'équation ne sera pas changé ; ou bien il se partagera en p *groupes appartenant chacun à l'équation proposée quand on lui adjoint respectivement chacune des racines de l'équation auxiliaire ;*

2°) Ces groupes jouiront de la propriété remarquable que l'on passera de l'un à l'autre en opérant dans toutes les permutations du premier une même substitution de lettres".

Quelle est la signification de ce théorème ?

Si on considère les substitutions de G (groupe de l'équation) qui n'altèrent pas la valeur numérique de la fonction rationnelle ϕ_1, soit il s'agit du groupe G lui-même et l'adjonction de r n'a pas rendu l'équation réductible et n'a rien fait avancer, soit elles forment un sous-groupe H_1 de G et l'adjonction de r a réduit précisément le groupe de l'équation à H_1. G s'écrit : $H_1 + H_1 b + \ldots + H_1 k$ qu'on peut encore noter $\sum_{i=0}^{p-1} H_1 \sigma_i$.

L'équation P(x) = 0 devient réductible et s'écrit :

$$P(x) = f(x, r) \cdot f(x, r_1) \ldots f(x, r_{p-1})$$

où chaque $r_i = \sigma_i r$.

$$\text{et} \quad f(x, r) = \prod_{\sigma \in H_1} (x - \sigma r)$$

En général, la décomposition de G en classes à gauche suivant H_1, ne coïncide pas avec celle en classes à droite.

Si l'on adjoint maintenant une autre racine r_i de l'équation R = 0, r_i s'écrit $\sigma_i r$ et le groupe de l'équation proposée se réduira au groupe des substitutions laissant fixe r_i, soit le groupe $\sigma_i H_1 \sigma_i^{-1}$ qui est un groupe conjugué de H_1 (c'est ce qu'exprime la condition 2°) du théorème de Galois). En effet on obtient les permutations de ce deuxième groupe en changeant V en $\sigma_i V$ dans celles du premier (cf. la troisième partie).

Ensuite Galois envisage (Proposition III) un autre mode de décomposition du groupe :
"si l'on adjoint toutes les racines d'une équation auxiliaire, les groupes dont il est question jouiront de plus de la propriété que les substitutions sont les mêmes dans chaque groupe". Or ce qui se passe dans ce cas, c'est que le groupe de l'équation devient le groupe des substitutions laissant fixes toutes les racines r_i d'une équation auxiliaire ;

G se réduit donc à $I = \bigcap_{\sigma_i \in G} \sigma_i H_1 \sigma_i^{-1}$ et un tel sous-groupe I est distingué dans G.

Galois insistera particulièrement dans sa lettre à Auguste Chevalier, sur la différence entre adjoindre à une équation une des racines d'une équation auxiliaire ou les adjoindre toutes simultanément. Seule, cette dernière façon fait apparaître un sous-groupe normal, ce que Galois nomme une "*décomposition propre*".

On peut démontrer, comme le feront Serret en 1866 dans son Cours d'Algèbre Supérieure (3e édition) ou C. Jordan que, dans le cas où l'équation auxiliaire irréductible est telle que ses racines sont exprimables rationnellement en fonction de l'une d'entre elles et de quantités connues, alors cette fois l'adjonction d'une racine ou celle de toutes les racines de cette équation auxiliaire sont équivalentes et réduisent le groupe G à un sous-groupe distingué de G. C'est d'ailleurs le cas quand l'équation auxiliaire est de la forme $x^p = A$ et que les racines pièmes de l'unité ont été précédemment adjointes.

C'est ainsi que la question de la résolubilité de l'équation par radicaux se trouve posée, et la proposition V du Mémoire de Galois y répond en donnant un critère.

Galois va transcrire en termes de groupes l'idée énoncée par Abel que les solutions doivent être exprimables uniquement à l'aide des opérations d'addition, de multiplication et d'extraction de racine pième (où l'on peut toujours supposer p premier car si p = nq l'extraction d'une racine pième est l'extraction successive de racines qième et nième). La condition s'énonce alors : par adjonctions successives de racines d'équations binômes, le groupe doit se réduire à l'identité car alors les racines sont "rationnellement" connues.

Si donc l'équation est soluble par radicaux, Galois considère p le plus petit nombre premier pour lequel une extraction de degré p réduit le groupe. Il remarque qu'on peut toujours supposer les racines pièmes de l'unité déjà adjointes car ceci ne change pas le groupe de l'équation. D'après les propositions précédentes, Galois conclut que "*le groupe de l'équation devra se décomposer en* p *groupes jouissant les uns par rapport aux autres de cette double propriété : 1°) que l'on passe de l'un à l'autre par une seule et même substitution ; 2°) que tous contiennent les mêmes substitutions*". Comme nous le détaillons dans la troisième partie, ceci veut dire qu'on a fait apparaître un sous-groupe H distingué et d'indice p dans G.

La réciproque de cette propriété est démontrée par Galois : s'il existe dans G un tel sous-groupe H, Galois utilise une résolvante de Lagrange pour construire effectivement une racine pième dont l'adjonction réduira le groupe de G à H. Pour cela, Galois prend une fonction θ des racines invariantes par H et H seulement. Soit σ une substitution de G, n'appartenant pas à H. Soient :

$$\theta_1 = \sigma\theta \quad , \quad \theta_2 = \sigma^2\theta, \ldots, \theta_{p-1} = \sigma^{p-1}\theta$$

et α une racine pième de l'unité.

Galois considère la résolvante :

$r = \theta + \alpha\theta_1 + \alpha^2\theta_2 + \ldots + \alpha^{p-1}\theta_{p-1}$.

D'une part r est évidemment invariante par H, et d'autre part les substitutions de G qui ne sont pas dans H induisent une permutation circulaire sur $\theta, \theta_1, \ldots, \theta_{p-1}$, et donc multiplient r par une puissance de α et laissent invariante r^p .

Finalement r^p est invariante par toutes les substitutions de G et r^p est rationnellement connue. En adjoignant la quantité r, on réduit le groupe G de l'équation à un sous-groupe d'indice p dans G auquel on appliquera le même raisonnement.

La condition nécessaire et suffisante à laquelle aboutit Galois, mais qui n'a été explicitée que par Jordan, pour qu'une équation soit soluble par radicaux est que "*son groupe puisse être considéré comme dérivant d'une échelle de substitutions* 1, a, b, ..., f, g *telles : 1) que chacune d'elles soit permutable au groupe dérivé des précédentes ; 2) que la première de ses puissances successives qui sont contenues dans le dit groupe soit de degré premier*" (*).

Ceci traduit la condition appelée aujourd'hui de "résolubilité" pour le groupe de l'équation : il possède une suite de sous-groupes emboîtés

$$\{1\} \subset H_k \subset H_{k-1} \subset \ldots \subset H_1 \subset G \quad ,$$

chacun étant un sous-groupe distingué maximal dans le suivant, dont l'indice dans celui-ci soit un nombre premier.

EXEMPLE D'APPLICATION DE LA THÉORIE DE GALOIS

Soit l'équation $x^4 - 3 = 0$; elle est irréductible sur le corps Q et elle admet les quatre racines distinctes r, ir, $-r$, $-ir$ avec $i = \sqrt{-1}$ et $r = \sqrt[4]{3}$.

Le corps des racines ou corps de décomposition de l'équation est obtenu par adjonction à Q de deux quantités r et i, soit $N = Q(r,i)$ qui est aussi obtenu par adjonction de l'élément primitif $r + ir$.

Tout élément de N s'écrit comme combinaison linéaire des 8 éléments suivants : $1, r, r^2, r^3, i, ir, ir^2, ir^3$.

Après l'injection des idées de linéarisation dans la théorie des corps, à partir des travaux de Dedekind jusqu'à ceux d'Artin, on considérera N comme un espace vectoriel de dimension 8 sur Q ; on dira que N est une extension de degré 8 sur Q .

Les éléments du groupe de l'équation seront déterminés dès qu'on connaît l'image de i et celle de r . Or chacune de ces deux racines ne peut être appliquée que sur l'une de ses *"conjuguées"* (de façon générale, on dit que deux éléments u et v du corps N des racines sont *conjugués* sur Q si et seulement si u et v sont tous deux racines du même polynôme irréductible sur Q). Donc i ne peut donc être appliqué que sur $+i$ et $-i$ et r sur l'un des quatre éléments r, $-r$, ir, $-ir$.

En combinant ces conditions, il y a donc huit éléments dans le groupe de Galois G (huit automorphismes du corps N). Les voici déterminés par leurs effets sur les générateurs i et r :

	I	S	S^2	S^3	T	ST	S^2T	S^3T
Image de i	i	i	i	i	$-i$	$-i$	$-i$	$-i$
Image de r	r	ir	$-r$	$-ir$	r	ir	$-r$	$-ir$

On peut vérifier que ces automorphismes conservent les relations polynomiales $i^2 = -1$, $r^4 = 3$.

G contient le sous-groupe $H = \{I, S, S^2, S^3\}$ engendré par S qui lui-même contient le sous-groupe plus petit $L = \{I, S^2\}$ engendré par S^2 . Chaque automorphisme du groupe H laisse i fixe ; il laisse donc fixe tout élément du sous-corps Q(i) .

Le sous-groupe L plus petit est formé des automorphismes qui laissent fixes tous les éléments du sous-corps plus grand $Q(i, r^2)$. Ainsi à la chaîne descendante des sous-groupes $G \supset H \supset L \supset I$ correspond la chaîne ascendante des sous-corps $Q \subset Q(i) \subset Q(i,r^2) \subset Q(i,r) = N$.

La chaîne ascendante des sous-corps fournit une méthode de résolution de l'équation donnée, par adjonctions successives des racines d'équations plus simples $x^2 = -1$, $y^2 = 3$, $z^2 = \sqrt{3}$.

La dernière partie du Premier Mémoire de 1831 est consacrée aux équations irréductibles de degré premier et Galois donne la structure du groupe de l'équation quand celle-ci est soluble par radicaux : le groupe ne renferme que des substitutions de la forme (x_k, x_{ak+b}) , les indices k et $ak+b$ étant pris modulo p . C'est ainsi que l'on voit apparaître une idée très chère à Galois qu'il appelle la présentation analytique des substitutions.

En effet, si une telle équation irréductible de degré p est soluble par radicaux, c'est qu'elle est résolue par l'adjonction d'un radical d'indice p égal à son degré, et donc le plus petit groupe avant l'identité qui intervient dans la décomposition, est d'ordre p . C'est donc le groupe cyclique G_1 des permutations circulaires d'ordre p des p racines.

Ces substitutions de G_1 sont de la forme (x_k, x_{k+c}), les indices étant pris modulo p . Ensuite Galois cherche à déterminer les groupes qui peuvent admettre ce sous-groupe comme sous-groupe normal. Il est intéressant de noter ici que du point de vue heuristique, c'est le sous-groupe qui apparaît en premier lieu et Galois cherche des normalisteurs possibles ; l'agilité dans la manipulation simultanée des deux notions est tout à fait remarquable. Soit alors G_2 le groupe précédant G_1 et τ une substitution de G_2 , n'appartenant pas à G_1 . τ est définie par une certaine fonction f . Pour toute substitution σ de G_1 , $\sigma\tau\sigma^{-1}$ doit être dans G_1 . Donc, il existe C indépendant de k , tel que

$$f(k + C) = f(k) + C$$

on peut alors déduire que $f(k) = ak + b$. Le seul groupe qui puisse admettre le groupe cyclique — formé des substitutions (x_k, x_{k+c}) — comme sous-groupe normal est le groupe formé des substitutions (x_k, x_{ak+b}) . Et Galois indique qu'il faut raisonner sur ce sous-groupe comme sur le précédent.

L'idée de la notation $(x_k, x_{f(k)})$ pour désigner une substitution se trouvait déjà de façon très embryonnaire chez Cauchy en 1815. Mais Galois va très vite sur la façon de déterminer pour une substitution donnée, sa fonction caractéristique, qui nécessite l'appel à la formule d'interpolation de Lagrange.

En effet, si les valeurs de l'indice z sont les p nombres $0, 1, 2, \ldots, p-1$ et que ces mêmes nombres sont dans un ordre différent $a, b, c, \ldots, k$; et soit la fonction

$F(z) = z(z-1)\ldots(z-p+1)$ et $F'(z)$ sa dérivée

alors la fonction

$$f(z) = \frac{a\,F(z)}{z\,F'(0)} + \frac{b\,F(z)}{(z-1)\,F'(1)} + \ldots + \frac{k\,F(z)}{(z-p+1)\,F'(p-1)}$$

est propre à représenter la substitution $\begin{pmatrix} 0 & 1 & 2 & \ldots & p-1 \\ a & b & c & \ldots & k \end{pmatrix}$.

(*) Jordan - Traité des Substitutions - Ed. Blanchard, ch. IV, § 523, p. 389. Il est intéressant de lire les démonstrations de Jordan dans le livre IV du Traité car il n'était pas question ici de reconstruire toute la théorie.

Cette idée prend un très grand développement dans le Deuxième Mémoire et le conduira à la notion de représentation linéaire, d'abord sur les corps F_p puis sur des corps finis quelconques F_q (où $q = p^\nu$).

D'une certaine façon, la dernière proposition (VIII) qui clôt ce mémoire : "*Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il faut et il suffit que deux quelconques des racines étant données, les autres s'en déduisent rationnellement*" constitue un pas en arrière par rapport à la précédente, puisque ce critère rapporte la résolubilité à des conditions sur l'équation et ses coefficients plutôt qu'aux propriétés du groupe de l'équation. Pourtant ce fut dans un premier temps la proposition la plus remarquée du Mémoire : celle que cite Galois dans la préface à son mémoire, celle dont parle Liouville quand, en 1843, il annonce à l'Académie l'imminente publication des écrits de Galois ; sans doute correspondait-elle mieux à ce que pouvait recevoir le monde mathématique de l'époque et se rapprochait-elle des formes d'énoncés obtenus par Abel, dans l'étude particulière des classes d'équations résolubles.

On peut évidemment comprendre pourquoi le théorème d'Abel sur l'irrésolubilité par radicaux de l'équation générale de degré n est une application de la théorie de Galois. L'équation "*générale*" de degré n , $a_0x^n + \ldots + a_n = 0$ a des coefficients littéraux indépendants. Son groupe de Galois est donc le groupe symétrique S_n . Or on peut démontrer que pour n supérieur à 4 , le groupe S_n n'a qu'un seul sous-groupe distingué, le groupe alterné A_n d'ordre $\frac{n!}{2}$ et ce dernier est "*simple*", c'est-à-dire qu'il n'a pas d'autres sous-groupes distingués. La condition de la théorie de Galois n'est pas vérifiée ; S_n n'est pas "*résoluble*".

Troisième partie : Aspects structuraux de théorie des groupes

Nous devons ici éclaircir un certain nombre de difficultés du texte de Galois, liées aux notions de groupe de permutations, de sous-groupes conjugués, de sous-groupe normal, et expliquer les périphrases qui les désignent faute de définitions et de notations précises.

Une fois élucidé le cœur de la théorie de Galois, ces questions peuvent paraître assez élémentaires ; pourtant, historiquement, elles ont considérablement freiné la compréhension et la diffusion de sa théorie et peuvent encore gêner la lecture directe de ses mémoires.

Pour Galois, comme pour Cauchy en 1815, une permutation est un arrangement donné de lettres (conception statique) et une substitution est le passage

d'une permutation à une autre, c'est-à-dire une opération. Et bien qu'il sache parfaitement qu'en ce qui concerne le produit — la loi de composition — il faut utiliser les substitutions, Galois hésite beaucoup entre les deux termes. Les ratures et les rajouts se superposent. Par exemple, une rature : "*Il n'y a d'important que la substitution*" ; plus loin une note en marge, elle-même biffée : "*mettre partout à la place du mot permutation le mot substitution*".

De plus, Galois dans tous les exemples développés dans ses travaux, n'utilise jamais l'écriture en deux lignes d'une substitution ; il doit raisonner de tête pour les calculs et n'écrit que les permutations d'arrivée, sans toujours préciser la permutation initiale.

Le fait que Galois applique le terme de groupe aux permutations induit une certaine instabilité dans son utilisation : si l'on rapporte ces permutations à une permutation initiale, on aura tantôt un ensemble de substitutions possédant la propriété de clôture, c'est-à-dire constituant un groupe au sens actuel, et tantôt une suite de substitutions qui sont en fait les classes à gauche ou à droite suivant un sous-groupe.

Examinons le cas développé par Galois du groupe de l'équation générale du 4e degré (S_4) (*). Galois indique qu'en adjoignant à l'équation la 1ère racine carrée qui intervient dans la formation de la résolvante du 3e degré, "le groupe de l'équation qui contenait en tout 24 substitutions, se décompose en deux qui n'en contiennent que douze.

En désignant par a, b, c, d les racines, voici l'un de ces groupes :

Tableau 1 :

a b c d	a c d b	a d b c
b a d c	c a b d	d a c b
c d a b	d b a c	b c a d
d c b a	b d c a	c b d a

Maintenant ce groupe se partage lui-même en trois groupes..." dont Galois écrit "*qu'ils sont semblables et identiques*". Galois dit aussi "*que l'on passe de l'un de ces groupes à l'autre par une même substitution*".

En effet, si l'on note ϕ la substitution :

$$\phi = \begin{pmatrix} a & b & c & d \\ a & c & d & b \end{pmatrix} = (a)\,(b, c, d)$$

et si on applique ϕ à chaque permutation d'un "groupe" de Galois (c'est-à-dire une des colonnes du tableau 1), on obtient la permutation située à la même ligne et à la colonne suivante.

Ecrivons le tableau des substitutions déduit du tableau 1 de Galois en partant de la permutation arbitraire a b c d ; nous obtenons le groupe alterné A_4, que Galois a "partagé" implicitement comme suit :

(*) Galois a présenté cet exemple dans le Mémoire de janvier 31 et on le trouve aussi traité dans un Fragment. Ed. Bourgne-Azra, p. 63 et p. 99.

Tableau 2 :

$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$	$\begin{pmatrix} a & b & c & d \\ a & c & d & b \end{pmatrix}$	$\begin{pmatrix} a & b & c & d \\ a & d & b & c \end{pmatrix}$
$\begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$	$\begin{pmatrix} a & b & c & d \\ c & a & b & d \end{pmatrix}$	$\begin{pmatrix} a & b & c & d \\ d & a & c & b \end{pmatrix}$
$\begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}$	$\begin{pmatrix} a & b & c & d \\ d & b & a & c \end{pmatrix}$	$\begin{pmatrix} a & b & c & d \\ b & c & a & d \end{pmatrix}$
$\begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}$	$\begin{pmatrix} a & b & c & d \\ b & d & c & a \end{pmatrix}$	$\begin{pmatrix} a & b & c & d \\ c & b & d & a \end{pmatrix}$

et que l'on peut aussi transcrire sous la forme postérieure des produits de cycles ; ainsi :

Tableau 3 :

(a)(b)(c)(d)	(a)(b)(c)(d)	(a)(b, d, c)
(a, b) (c, d)	(a, c, b) (d)	(a, d, b) (c)
(a, c) (b, d)	(a, d, c) (b)	(a, b, c) (d)
(a, d) (b, c)	(a, b, d) (c)	(a, c, d) (b)

Pour nous, il est bien clair que nous avons affaire à un sous-groupe H du groupe $G (= A_4)$ des douze substitutions de départ, qui est la 1ère colonne de gauche, et de ses classes (à gauche, par exemple) dans G .

Si on appelle H′ et H″ les deuxième et troisième colonnes de ce tableau 3, on a :

$$H' = \phi H$$
$$H'' = (a)\,(b, d, c)\,H = \phi^2 H = \phi H'$$

Galois écrira dans sa lettre à A. Chevalier :

$$G = H + \phi H + \phi^2 H .$$

Pour Galois, H, ϕ H et ϕ^2 H sont désignés par le même terme de groupe. La reconnaissance par Galois qu'une même substitution applique successivement chaque colonne sur la suivante renvoie au caractère cyclique du groupe quotient de G par H . Et ce caractère cyclique s'explique lui-même par le fait que l'ordre de G/H est égal au degré p premier de l'équation binôme dont l'adjonction de la racine a permis de réduire le groupe G à H .

On voit donc que des "*groupes semblables et identiques de permutations*" pour Galois n'impliquent pas une quelconque propriété analogue pour les ensembles respectifs de substitutions, quand on considère une même permutation initiale. Ici Galois évoque le fait suivant : si l'on rapporte cette fois les 3 colonnes du tableau 1 (c'est-à-dire les trois "groupes" dont parle Galois) à leurs premières lignes respectives, il vient :

Tableau 4 :

$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$	$\begin{pmatrix} a & c & d & b \\ a & c & d & b \end{pmatrix}$	$\begin{pmatrix} a & d & b & c \\ a & d & b & c \end{pmatrix}$
$\begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$	$\begin{pmatrix} a & c & d & b \\ c & a & b & d \end{pmatrix}$	$\begin{pmatrix} a & d & b & c \\ d & a & c & b \end{pmatrix}$
$\begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}$	$\begin{pmatrix} a & c & d & b \\ d & b & a & c \end{pmatrix}$	$\begin{pmatrix} a & d & b & c \\ b & c & a & d \end{pmatrix}$
$\begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}$	$\begin{pmatrix} a & c & d & b \\ b & d & c & a \end{pmatrix}$	$\begin{pmatrix} a & d & b & c \\ c & b & d & a \end{pmatrix}$

c'est-à-dire :

(a)(b)(c)(d)	(a)(c)(d)(b)	(a)(d)(b)(c)
(a, b) (c, d)	(a, c) (b, d)	(a, d) (b, c)
(a, c) (b, d)	(a, d) (b, c)	(a, b) (c, d)
(a, d) (b, d)	(a, b) (c, d)	(a, c) (b, d)

et les trois groupes de substitutions formés sont bien identiques à H . On comprend dans ce cas la formulation de Galois : *"les trois groupes ont les mêmes substitutions"*.

Cette propriété traduit la normalité du sous-groupe H dans $G = A_4$. En effet, puisque la substitution

$$\phi = \begin{pmatrix} a & b & c & d \\ a & c & d & b \end{pmatrix} = (a)\,(b, c, d)$$

applique chaque permutation à la première colonne du tableau 1 de Galois, sur la permutation de même ligne de la deuxième colonne, alors une substitution de la deuxième colonne du tableau 4, par exemple celle de la 2e ligne, pourra s'écrire

$$\begin{pmatrix} a & c & d & b \\ c & a & b & d \end{pmatrix} = \begin{pmatrix} \phi(a & b & c & d) \\ \phi(b & a & d & c) \end{pmatrix}$$

Or si nous appelons ψ la substitution $\begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$ l'opération qui consiste à remplacer chaque ligne A_i de ψ , par $\phi(A_i)$ revient à calculer

$$\phi^{-1}\,\psi\,\phi$$

Quand ψ parcourt le groupe H , $\phi^{-1}\psi\phi$ parcourt la 2e colonne du tableau 4, donc un sous-groupe conjugué de H . Dans ce cas, H étant normal, $\phi^{-1}\psi\phi$ appartient à H . De la même façon, chaque substitution de la 3e colonne du tableau 4, par exemple celle de la 2e ligne peut s'écrire :

$$\begin{pmatrix} a & d & b & c \\ d & a & c & b \end{pmatrix} = \begin{pmatrix} \phi^2(a & b & c & d) \\ \phi^2(b & a & d & c) \end{pmatrix} = (\phi^2)^{-1}\,\psi\,\phi^2$$

qui appartient ici aussi à H .

L'apparition des notions de sous-groupes conjugués et de sous-groupe normal est donc absolument indissociable de la problématique de la résolubilité des équations par radicaux ; par exemple n'est pas imaginée de façon autonome l'idée d'un sous-groupe H invariant dans G (c'est-à-dire tel que $xHx^{-1} = H$ pour tout $x \in G$) mais sans que soit vérifiée la propriété pour G/H d'être cyclique, tout simplement parce que cette idée n'a pas de signification dans la situation de la résolubilité des équations.

Notons ici que le mémoire suivant : *"Des équations primitives qui sont solubles par radicaux"* qui ne connut que la publication posthume de 1846, laisse apparaître un degré de sophistication dans la théorie des groupes beaucoup plus important : groupes *"irréductibles"*, groupes primitifs, développement de l'idée de représentation linéaire, considération des groupes linéaire et projectif linéaire d'un espace de dimension 2 sur un corps fini, etc. (*).

Ce degré de sophistication est d'ailleurs difficile à évaluer complètement car ce mémoire semble bien ne constituer qu'un fragment dont les parties en amont et en aval auraient disparu. Dans l'esprit de Galois, il constituait plutôt une application particulière à une classe d'équations qu'un développement de sa théorie, dont les principes de fond se trouvent dans le Premier Mémoire.

Pour justifier le détour par cette partie donnons quelques éléments historiques sur la compréhension ultérieure de cet aspect du mémoire de Galois.

Ainsi Enrico Betti, un des premiers lecteurs et commentateurs de Galois, aura beaucoup de difficultés à séparer et exprimer clairement la notion statique d'arrangement et celle de groupe de substitutions. En 1852, dans un mémoire intitulé *Sulla di Resoluzione delle equazioni algebriche*, Betti parle de groupe des arrangements mais en indiquant que ce sont les substitutions *"sur"* ce groupe, ou *"associées"* à ce groupe, qui importent dans la théorie. Il définit l'égalité de deux groupes si les ensembles de leurs substitutions associées sont identiques, même si les ensembles des arrangements sont différents et appelle *"semblables"* (*simili*) deux groupes contenant le même nombre d'arrangements et tels que les ensembles de leurs substitutions associées bien que différents contiennent le même nombre de substitutions de même ordre.

Betti avait inventé le terme *"dérivative"* d'une substitution θ par une autre ψ , comme étant $\psi^{-1}\theta\psi$, opération notée :

$$D_\psi\,\theta = \psi^{-1}\theta\psi$$

et qu'il étend aux groupes $(\psi^{-1}G\psi)$.

Betti remarque que si une substitution ψ applique un arrangement d'un groupe G sur un arrangement d'un autre groupe dérivé K , alors ψ appliquera n'importe quel arrangement de G , en un autre de K . En terminologie moderne, on peut dire que des groupes semblables d'arrangements induisent des groupes conjugués de substitutions et que des groupes égaux d'arrangements induisent un sous-groupe normal. Mais évidemment, cette notion de sous-groupe normal appelle un groupe référentiel plus grand, notion totalement absente chez Betti, ce qui rend les raisonnements très confus.

En fait, le premier qui ait parfaitement clarifié l'idée de groupe de substitutions, est le mathématicien A.L. Cauchy. Dans les années 1844-46, il reprend brusquement des travaux sur le sujet des substitutions et publie en quelques mois un grand *Mémoire sur les Arrangements que l'on peut former avec n lettres*, et vingt-sept Notes aux Comptes Rendus de l'Académie. (Il semble qu'en 1852, Betti ne les connaissait pas). Cauchy adopte une double écriture pour les substitutions : soit en deux lignes, soit en produit de cycles et définit les *"systèmes de substitutions conjuguées"* comme étant des ensembles de substitutions fermés pour la loi du produit. Cette terminologie restera en vigueur jusque dans les premiers travaux de Camille Jordan. Elle ne sera définitivement abandonnée au profit du mot groupe, que dans le Traité des Substitutions paru en 1870.

(*) Le résultat principal de ce mémoire — c'est-à-dire la caractérisation des équations primitives résolubles comme étant d'un degré égal à la puissance d'un nombre premier — est démontré de façon complète dans l'annexe de la thèse de 1860 de Camille Jordan.

Le Grand Mémoire de Cauchy constitue, en fait, une étude exhaustive, structurée du groupe symétrique S_n, et de ses sous-groupes d'indice le plus bas possible. Lui aussi définit des substitutions *"semblables"* comme des substitutions ayant la même décomposition en produit de cycles disjoints ; il démontre que si deux substitutions P et Q sont semblables, alors il en existe une troisième, R, telle que $P = RQR^{-1}$. En langage moderne, P et Q sont conjuguées dans le plus petit groupe symétrique les contenant toutes deux. Mais Cauchy restreint sa définition aux substitutions prises individuellement, sans l'étendre à des groupes, passant ainsi à côté de la notion de sous-groupes conjugués. De même, étudiant les conditions de permutabilité pour les substitutions, au moyen de manipulations subtiles sur les ensembles de lettres sur lesquels opèrent ces substitutions, Cauchy approche la notion de sous-groupe normal mais sans le cerner exactement.

Il n'est pas question de détailler davantage ici l'analyse de ces travaux de Cauchy que nous avons effectuée par ailleurs (*) ; indiquons seulement que Cauchy y fonde un véritable CALCUL DES SUBSTITUTIONS, qui s'inscrit dans la prise de conscience historique du rôle des opérations qui marque cette époque : il développe tous azimuts sur des objets nouveaux que rien n'assimile à des nombres, toutes les ressources de différentes techniques opératoires, sans qu'aucune limite ne soit a priori fixée, sinon l'épuisement parfois dans de trop grandes complications de calculs que l'émergence d'une méthode générale ou d'analogies profondes ne compense pas toujours. Pour lui, un "système de substitutions conjuguées" restera en définitive une entité indécomposable assez rigide, dont il explore les propriétés mais sans mettre profondément en évidence les concepts de sous-groupe, ou de sous-groupe distingué.

Bien qu'il obtienne des résultats fins sur ce que nous appelons aujourd'hui les groupes transitifs, les groupes transitifs primitifs, etc., dont bien des éléments seront utiles à Jordan dans la reconstruction de démonstrations lacunaires de Galois, relatives en particulier au Deuxième Mémoire (**), le Calcul des Substitutions de Cauchy élaboré sans finalité vraiment définie, aura besoin justement du choc de la théorie des équations pour témoigner de sa fécondité.

Au contraire, la démarche de Galois vise à la résolution d'un problème précis : la résolubilité des équations par radicaux. L'idée de *"décomposer"* un groupe est inscrite alors au cœur de sa théorie et confère à cette notion de groupe, exhibée au cours de la démarche, une souplesse, un pouvoir d'articulation et d'analyse qui resteront absolument étrangers au point de vue de Cauchy.

Et cette idée de *relativité*, invention propre de Galois, va se répercuter plus tard dans toutes les théories mathématiques et physiques nées de la théorie des groupes; F. Klein étant le premier à la mettre en œuvre magistralement dans son programme d'Erlangen.

BIBLIOGRAPHIE

N.H. Abel. *Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré.* Oeuvres. Ed. Sylow-Lie, tome I, p. 66-87.

A.M. Brasselet. *Résolution des équations algébriques - Premier mémoire de Galois.* Publication de l'IREM de Lille, Juin 1979.

A. Dahan. *Les recherches algébriques de Cauchy.* Thèse, Paris 1979.
Les travaux de Cauchy sur les substitutions. Etude de son approche du concept de groupe. Archive for History of Exact Sciences, vol. 23, 1980.

A. Dahan - Dalmedico & J. Peiffer. *Routes et dédales, Histoire des mathématiques.* Editions Etudes Vivantes, Paris 1982.

J. Dieudonné. *Abrégé d'histoire des mathématiques.* Ouvrage collectif. Hermann, Paris 1978.

C.F. Gauss. *Recherches Arithmétiques* traduites par A.C.M. Poulet-Delisle. Ed. Blanchard, Paris 1953.

E. Galois. *Ecrits et mémoires mathématiques.* Edition R. Bourgne et J.P. Azra, Paris 1962, Gauthier-Villars.

C. Jordan. *Mémoire sur le nombre des valeurs des fonctions* (Thèse). Oeuvre, tome I.
Traité des substitutions et des équations algébriques. Ed. Blanchard, Paris 1957.

B.M. Kiernan. *The development of Galois Theory from Lagrange to Artin.* Archive for History of Exact Sciences, vol. 8, 1971.

J.L. Lagrange. *Réflexions sur la résolution algébrique des équations.* Nouveaux mémoires de l'Académie Royale des Sciences et Belles Lettres de Berlin, années 1770-71. Oeuvres, tome III, p. 205-421.

A.T. Vandermonde. *Mémoire sur la résolution des équations.* Histoire de l'Académie Royale des Sciences, année 1771, Paris 1774, p. 365-416.

G. Verriest. *E. Galois et la théorie des équations algébriques.* Notice publiée en 1897. Rééd. Gauthier-Villars, Paris 1951.

J. Vuillemin. *La philosophie de l'Algèbre.* PUF, Paris 1962.

(*) cf. bibliographie.

(**) Edition Bourgne-Azra, p. 129. "Des équations primitives qui sont solubles par radicaux".