Mémoire
Sur les conditions de résolubilité des équations par radicaux.
Évariste Galois

Le Mémoire ci-joint[1] est extrait d'un ouvrage que j'ai eu l'honneur de présenter à l'Académie il y a un an. Cet ouvrage n'ayant pas été compris, les propositions qu'il renferme ayant été révoquées en doute, j'ai dû me contenter de donner, sous forme synthétique, les principes généraux, et une *seule* application de ma théorie. Je supplie mes juges de lire du moins avec attention ce peu de pages.

On trouvera ici une *condition générale* à laquelle *satisfait toute équation soluble par radicaux*, et qui réciproquement assure leur résolubilité. On en fait l'application seulement aux équations dont le degré est un nombre premier. Voici le théorème donné par notre analyse :

"Pour qu'une équation de degré premier, qui n'a pas de diviseurs commensurables, soit soluble par radicaux, il *faut* et il *suffit* que toutes les racines soient des fonctions rationnelles de deux quelconques d'entre elles."

Les autres applications de la théorie sont elles-mêmes autant de théories particulières. Elles nécessitent d'ailleurs l'emploi de la théorie des nombres, et d'un algorithme particulier : nous les réservons pour une autre occasion. Elles sont en partie relatives aux équations modulaires de la théorie des fonctions elliptiques, que nous démontrons ne pouvoir se résoudre par radicaux.

Ce 16 janvier 1831.

E. Galois.

Principes.

Je commencerai par établir quelques définitions et une suite de lemmes qui sont tous connus.

Définitions. Une équation est dite réductible quand elle admet des diviseurs rationnels ; irréductible dans le cas contraire.

Il faut ici expliquer ce qu'on doit entendre par le mot *rationnel*, car il se représentera souvent.

Quand l'équation a *tous* ses coefficients numériques et rationnels, cela veut dire simplement que l'équation peut se décomposer en facteurs qui aient leurs coefficients numériques et rationnels.

Mais quand les coefficients d'une équation ne seront pas *tous* numériques et rationnels, alors il faudra entendre par diviseur rationnel un diviseur dont les coefficients s'exprimeraient en fonction rationnelle des coefficients de la proposée, en général par quantité rationnelle, une quantité qui

http://www.bibnum.education.fr/sites/default/files/galois_memoire_sur_la_resolubiblite.pdf.

[1] J'ai jugé convenable de placer en tête de ce Mémoire la préface qu'on va lire, bien que je l'aie trouvée biffée dans le manuscrit.

A. Ch.

s'exprime en fonction rationnelle des coefficients de la proposée.

Il y a plus : on pourra convenir de regarder comme rationnelle toute fonction rationnelle d'un certain nombre de quantités déterminées, supposées connues a 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.

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.

Ainsi, quand on adjoint à l'équation

$$\frac{x^n - 1}{x - 1} = 0, \qquad \text{où } n \text{ est premier,}$$

une racine d'une des équations auxiliaires de M. Gauss, cette équation se décompose en facteurs, et devient par conséquent réductible.

Les substitutions sont le passage d'une permutation à l'autre.

La permutation d'où l'on part pour indiquer les substitutions est toute arbitraire, quand il s'agit de fonctions ; car il n'y a aucune raison pour que, dans une fonction de plusieurs lettres, une lettre occupe un rang plutôt qu'un autre.

Cependant, comme on ne peut guère se former l'idée d'une substitution sans se former celle d'une permutation, nous ferons dans le langage un emploi fréquent des permutations, et nous ne considèrerons les substitutions que comme le passage d'une permutation à une autre.

Quand nous voudrons grouper des substitutions, nous les ferons toutes provenir d'une même permutation.

Comme il s'agit toujours de questions où la disposition primitive des lettres n'influe en rien dans les groupes que nous considèrerons, on devra avoir les mêmes substitutions, quelle que soit la permutation d'où l'on sera parti. Donc, si dans un pareil groupe on a les substitutions S et T, on est

sûr d'avoir la substitution ST.

Telles sont les définitions que nous avons cru devoir rappeler.

Lemme I. "Une équation irréductible ne peut avoir aucune racine commune avec une équation rationnelle, sans la diviser."

Car le plus grand commun diviseur entre l'équation irréductible et l'autre équation, sera encore rationnel ; donc, etc.

Lemme II. "Étant donnée une équation quelconque, qui n'a pas de racines égales, dont les racines sont $a, b, c, ...$, on peut toujours former une fonction V des racines, telle qu'aucune des valeurs que l'on obtient en permutant dans cette fonction les racines de toutes manières, ne soient égales."
Par exemple, on peut prendre

$$V = Aa + Bb + Cc + ..$$

A, B, C étant des nombres entiers convenablement choisis.

Lemme III. "La fonction V étant choisie comme il est indiqué dans l'article précédent, elle jouira de cette propriété, que toutes les racines de l'équation proposée s'exprimeront rationnellement en fonction de V."

En effet, soit

$$V = \varphi(a, b, c, d, ...),$$

ou bien

$$V - \varphi(a, b, c, d, ...) = 0.$$

Multiplions entre elles toutes les équations semblables, que l'on obtient en permutant dans celles-ci toutes les lettres, la première seulement restant fixe ; il viendra une expression suivante :

$$[V - \varphi(a, b, c, d, ...)][V - \varphi(a, c, b, d, ...)][V - \varphi(a, b, d, c, ...]...,$$

symétrique en $b, c, d, ...$, laquelle pourra par conséquent s'écrire en fonction de a. Nous aurons donc une équation de la forme

$$F(V, a) = 0.$$

Or je dis que de là on peut tirer la valeur de a. Il suffit pour cela de chercher la solution commune à cette équation et à la proposée. Cette solution est la seule commune, car on ne peut avoir, par exemple,

$$F(V, b) = 0,$$

cette équation ayant un facteur commun avec l'équation semblable, sans quoi l'une des fonctions $\varphi(a, ...)$ serait égale à l'une des fonctions $\varphi(b, ...)$; ce qui est contre l'hypothèse.

Il suit de là que a s'exprime en fonction rationnelle de V, et il en est de même des autres racines.

Cette proposition[2] est citée sans démonstration par Abel, dans le Mémoire posthume sur les fonctions elliptiques.

Lemme IV. "Supposons que l'on ait formé l'équation en V, et que l'on ait pris l'un de ses facteurs irréductibles, en sorte que V soit racine d'une équation irréductible. Soient $V, V', V'', ...$ les racines de cette équation irréductible. Si $a = f(V)$ est une des racines de la proposée, $f(V')$ de même sera une racine de la proposée."

En effet, en multipliant entre eux tous les facteurs de la forme $V - \varphi(a, b, c, ..., d)$, où l'on aura opéré sur les lettres toutes les permutations possibles, on aura une équation rationnelle en V, laquelle se trouvera nécessairement divisible par l'équation en question ; donc V' doit s'obtenir par l'échange des lettres dans la fonction V. Soit $F(V, a) = 0$ l'équation qu'on obtient en permutant dans V toutes les lettres, hors la première. On aura donc $F(V', b) = 0$, b pouvant être égal à a, mais étant certainement l'une des racines de l'équation proposée ; par conséquent, de même que de la proposée et de $F(V, a) = 0$ est résulté $a = f(V)$, de même il résultera de la proposée et de $F(V', b) = 0$ combinées, la suivante $b = f(V')$.

Proposition i.

Théorème. "Soit une équation donnée, dont $a, b, c, ...$ sont les m racines. Il y aura toujours un groupe de permutations des lettres $a, b, c,...$ qui jouira de la propriété suivante :

1°. Que toute fonction des racines, invariable[3] par les substitutions de ce groupe, soit rationnellement connue ;

2°. Réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par les substitutions."

(Dans le cas des équations algébriques, ce groupe n'est autre chose que l'ensemble des 1.2.3....m permutations possibles sur les m lettres, puisque, dans ce cas, les fonctions symétriques sont seules déterminables rationnellement.)

(Dans le cas de l'équation $\dfrac{x^n - 1}{x - 1} = 0$, si l'on suppose $a = r, b = r^g, c = r^{g^2}, ..., g$ étant une racine

[2]Il est remarquable, que de cette proposition on peut conclure que toute équation dépend d'une équation auxiliaire telle que toutes les racines de cette nouvelle équation soient des fonctions rationnelles les unes des autres ; car l'équation auxiliaire en V est dans ce cas.
Au surplus, cette remarque est purement curieuse. En effet, une équation qui a cette propriété n'est pas, en général, plus facile à résoudre qu'une autre.

[3]Nous appelons ici invariable non-seulement une fonction dont la forme est invariable par les substitutions des racines entre elles, mais encore celle dont la valeur numérique ne varierait pas par ces substitutions. Par exemple, si $Fx = 0$ est une équation, Fa est une fonction des racines qui ne varie par aucune permutation.
Quand nous disons qu'une fonction est rationnellement connue, nous voulons dire que sa valeur numérique est exprimable en fonction rationnelle des coefficients de l'équation et des quantités adjointes.

primitive, le groupe de permutations sera simplement celui-ci :

$$\begin{array}{l} abcd\ldots k \\ bcd\ldots ka \\ cd\ldots kab \\ \ldots \\ kabc\ldots i\ ; \end{array}$$

dans ce cas particulier, le nombre des permutations est égal au degré de l'équation, et la même chose aurait lieu dans les équations dont toutes les racines seraient des fonctions rationnelles les unes des autres.)

Démonstration. Quelle que soit l'équation donnée, on pourra trouver une fonction rationnelle V des racines, telle que toutes les racines soient fonctions rationnelles de V. Cela posé, considérons l'équation irréductible dont V est racine (lemmes III et IV). Soient $V, V', V'', ..., V^{n-1}$ les racines de cette équation.

Soient $\varphi V, \varphi_1 V, \varphi_2 V \ldots., \varphi_{m-1} V$ les racines de la proposée.

Écrivons les n permutations suivantes des racines

$$\begin{array}{l|llll} (V) & \varphi V, & \varphi_1 V, & \varphi_2 V, & \ldots\ \varphi_{m-1} V, \\ (V') & \varphi V', & \varphi_1 V', & \varphi_2 V', & \ldots\ \varphi_{m-1} V', \\ (V'') & \varphi V'', & \varphi_1 V'', & \varphi_2 V'', & \ldots\ \varphi_{m-1} V'', \\ \ldots & & & & \\ (V^{(n-1)}) & \varphi V^{(n-1)}, & \varphi_1 V^{(n-1)}, & \varphi_2 V^{(n-1)}, & \ldots\ \varphi_{m-1} V^{(n-1)}\ : \end{array}$$

je dis que ce groupe de permutations jouit de la propriété énoncée.

En effet,

1°. toute fonction F des racines, invariable par les substitutions de ce groupe, pourra être écrite ainsi : $F = \psi V$, et l'on aura

$$\psi V = \psi V' = \psi V'' = \ldots = \psi V^{(n-1)}.$$

La valeur de F pourra donc se déterminer rationnellement.

2°. *Réciproquement.* Si une fonction F est déterminable rationnellement, et que l'on pose $F = \psi V$, on devra avoir

$$\psi V = \psi V' = \psi V'' = \ldots = \psi V^{(n-1)},$$

puisque l'équation en V n'a pas de diviseur commensurable et que V satisfait à l'équation $F = \psi V$, F étant une quantité rationnelle. Donc la fonction F sera nécessairement invariable par les substitutions du groupe écrit ci-dessus.

Ainsi, ce groupe jouit de la double propriété dont il s'agit dans le théorème proposé. Le théorème est donc démontré.

Nous appellerons groupe de l'équation le groupe en question.

Scolie 1. Il est évident que dans le groupe de permutations dont il s'agit ici, la disposition des lettres n'est point à considérer, mais seulement les substitutions de lettres par lesquelles on passe d'une permutation à l'autre.

Ainsi l'on peut se donner arbitrairement une première permutation, pourvu que les autres permutations s'en déduisent toujours par les mêmes substitutions de lettres. Le nouveau groupe ainsi formé jouira évidemment des mêmes propriétés que le premier, puisque dans le théorème précédent, il ne s'agit que des substitutions que l'on peut faire dans les fonctions.

Scolie 2. Les substitutions sont indépendantes même du nombre des racines.

Proposition ii.

Théorème[4]. "Si l'on adjoint à une équation donnée la racine r d'une équation auxiliaire irréductible,

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 respectivement quand on lui adjoint 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."

1°. Si, après l'adjonction de r, l'équation en V, dont il est question plus haut, reste irréductible, il est clair que le groupe de l'équation ne sera pas changé. Si, au contraire, elle se réduit, alors l'équation en V se décomposera en p facteurs, tous de même degré et de la forme

$$f(V, r) \times f(V, r') \times f(V, r''),$$

$r, r', r'', \ldots$ étant d'autres valeurs de r. Ainsi le groupe de l'équation proposée se décomposera aussi en groupes chacun d'un même nombre de permutations, puisqu'à chaque valeur de V correspond une permutation. Ces groupes seront respectivement ceux de l'équation proposée, quand on lui adjoindra successivement $r, r', r'', \ldots$.

2°. Nous avons vu plus haut que toutes les valeurs de V étaient des fonctions rationnelles les unes des autres. D'après cela, supposons que V étant une racine de $f(V, r) = 0, F(V)$ en soit une autre

[4]Dans l'énoncé du théorème, après ces mots : "la racine r d'une équation auxiliaire irréductible," Galois avait mis d'abord ceux-ci : "de degré p premier," qu'il a effacés plus tard. De même, dans la démonstration, au lieu de "$r, r', r'', \ldots$ étant d'autres valeurs de r", la rédaction primitive portait : "$r, r', r'', \ldots$ étant les diverses valeurs de r." Enfin on trouve à la marge du manuscrit la note suivante de l'auteur :
"Il y a quelque chose à compléter dans cette démonstration. Je n'ai pas le temps."
Cette ligne a été jetée avec une grande rapidité sur le papier ; circonstance qui, jointe aux mots : "Je n'ai pas le temps.", me fait penser que Galois a relu son Mémoire pour le corriger avant d'aller sur le terrain.
A. CH.

; il est clair que de même si V' est une racine de $f(V,r')=0, F(V')$ en sera une autre ; car l'on aura

$$f[F(V),r] = \text{ une fonction divisible par} f(V,r).$$

Donc (*lemme 1*)

$$[F(V'),r'] = \text{ une fonction divisible par } f(V',r').$$

Cela posé, je dis que l'on obtient le groupe relatif à r' en opérant partout dans le groupe relatif à r une même substitution de lettres.

En effet, si l'on a, par exemple,

$$\varphi_\mu F(V) = \varphi_\nu(V),$$

on aura encore (*lemme 1*)

$$\varphi_\mu F(V') = \varphi_\nu(V').$$

Donc, pour passer de la permutation $[F(V)]$ à la permutation $[F(V')]$, il faut faire la même substitution que pour passer de la permutation (V) à la permutation $f(V')$.

Le théorème est donc démontré.

Proposition III.

Théorème. "Si l'on adjoint à une équation *toutes* les racines d'une équation auxiliaire, les groupes dont il est question dans le théorème II jouiront de plus de cette propriété, que les substitutions sont les mêmes dans chaque groupe."

On trouvera la démonstration[5].

Proposition IV.

Théorème. "Si l'on adjoint à une équation la valeur *numérique* d'une certaine fonction de ses racines, le groupe de l'équation s'abaissera de manière à n'avoir plus d'autres permutations que celles par lesquelles cette fonction est invariable."

En effet, d'après la proposition I, toute fonction connue doit être invariable par les permutations du groupe de l'équation.

[5]Dans le manuscrit, l'énoncé du théorème qu'on vient de lire se trouve en marge et en remplace un autre que Galois avait écrit avec sa démonstration sous le même titre : Proposition III. Voici le texte primitif :
Théorème. "Si l'équation en r est de la forme $r^p = A$, et que les racines $p^{\text{ièmes}}$ de l'unité se trouvent au nombre des quantités précédemment adjointes, les p groupes dont il est question dans le théorème II jouiront de plus de cette propriété, que les substitutions de lettres par lesquelles on passe d'une permutation à une autre dans chaque groupe soient les mêmes pour tous les groupes".
En effet, dans ce cas, il revient au même d'adjoindre à l'équation telle ou telle valeur de r. Par conséquent, ses propriétés doivent être les mêmes après l'adjonction de telle ou telle valeur. Ainsi son groupe doit être le même quant aux substitutions (Proposition I, scolie). Donc, etc.
Tout cela est effacé avec soin ; le nouvel énoncé porte la date 1832, et montre, par la manière dont il est écrit, que l'auteur était extrêmement pressé, ce qui confirme l'assertion que j'ai avancée dans la note précédente.
A. Ch.

Proposition v.

Problème. "Dans quels cas une équation est-elle soluble par de simples radicaux ?"

J'observerai d'abord que, pour résoudre une équation, il faut successivement abaisser son groupe jusqu'à ne contenir plus qu'une seule permutation. Car, quand une équation est résolue, une fonction quelconque de ses racines est connue, même quand elle n'est invariable par aucune permutation.

Cela posé, cherchons à quelle condition doit satisfaire le groupe d'une équation, pour qu'il puisse s'abaisser ainsi par l'adjonction de quantités radicales.

Suivons la marche des opérations possibles dans cette solution, en considérant comme opérations distinctes l'extraction de chaque racine de degré premier.

Adjoignons à l'équation le premier radical extrait dans la solution. Il pourra arriver deux cas : ou bien, par l'adjonction de ce radical, le groupe des permutations de l'équation sera diminué ; ou bien, cette extraction de racine n'étant qu'une simple préparation, le groupe restera le même.

Toujours sera-t-il qu'après un certain nombre *fini* d'extractions de racines, le groupe devra se trouver diminué, sans quoi l'équation ne serait pas soluble.

Si, arrivé à ce point, il y avait plusieurs manières de diminuer le groupe de l'équation proposée par une simple extraction de racine, il faudrait, pour ce que nous allons dire, considérer seulement un radical du degré le moins haut possible parmi tous les simples radicaux, qui sont tels que la connaissance de chacun d'eux diminue le groupe de l'équation.

Soit donc p le nombre premier qui représente ce degré minimum, en sorte que par une extraction de racine de degré p, on diminue le groupe de l'équation.

Nous pouvons toujours supposer, du moins pour ce qui est relatif au groupe de l'équation, que parmi les quantités adjointes précédemment à l'équation se trouve une racine $p^{\text{ième}}$ de l'unité, α. Car, comme cette expression s'obtient par des extractions de racines de degré inférieur à p, sa connaissance n'altèrera en rien le groupe de l'équation.

Par conséquent, d'après les théorèmes II et III, 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.

Je dis réciproquement, que si le groupe de l'équation peut se partager en p groupes qui jouissent de cette double propriété, on pourra, par une simple extraction de racine $p^{\text{ième}}$, et par l'adjonction de cette racine $p^{\text{ième}}$, réduire le groupe de l'équation à l'un de ces groupes partiels.

Prenons, en effet, une fonction des racines qui soit invariable pour toutes les substitutions de l'un des groupes partiels, et varie pour toute autre substitution. (Il suffit, pour cela, de choisir une fonction symétrique des diverses valeurs que prend, par toutes les permutations de l'un des groupes

partiels, une fonction qui n'est invariable pour aucune substitution.)

Soit θ cette fonction des racines.

Opérons sur la fonction θ une des substitutions du groupe total qui ne lui sont pas communes avec les groupes partiels. Soit θ_1 le résultat. Opérons sur la fonction θ_1 la même substitution, et soit θ_2 le résultat, et ainsi de suite.

Comme p est un nombre premier, cette suite ne pourra s'arrêter qu'au terme θ_{p-1}, ensuite l'on aura $\theta_p = \theta_1, \theta_{p+1} = \theta_1$, et ainsi de suite.

Cela posé, il est clair que la fonction

$$(\theta + \alpha\theta_1 + \alpha^2\theta_2 + \ldots + \alpha^{p-1}\theta_{p-1})^p$$

sera invariable par toutes les permutations du groupe total, et, par conséquent, sera actuellement connue.

Si l'on extrait la racine $p^{\text{ième}}$ de cette fonction, et qu'on l'adjoigne à l'équation, alors, par la proposition IV, le groupe de l'équation ne contiendra plus d'autres substitutions que celles des groupes partiels.

Ainsi, pour que le groupe d'une équation puisse s'abaisser par une simple extraction de racine, la condition ci-dessus est nécessaire et suffisante.

Adjoignons à l'équation le radical en question ; nous pourrons raisonner maintenant sur le nouveau groupe comme sur le précédent, et il faudra qu'il se décompose lui-même de la manière indiquée, et ainsi de suite, jusqu'à un certain groupe qui ne contiendra plus qu'une seule permutation.

Scolie. Il est aisé d'observer cette marche dans la résolution connue des équations générales du quatrième degré. En effet, ces équations se résolvent au moyen d'une équation du troisième degré, qui exige elle-même l'extraction d'une racine carrée. Dans la suite naturelle des idées, c'est donc par cette racine carrée qu'il faut commencer. Or, en adjoignant à l'équation du quatrième degré cette racine carrée, le groupe de l'équation, qui contenait en tout vingt-quatre 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 :

$$\begin{array}{lll} abcd, & acdb, & adbc, \\ badc, & cabd, & dacb, \\ cdab, & dbac, & bcad, \\ dcba, & bdca, & cbda. \end{array}$$

Maintenant ce groupe se partage lui-même en trois groupes, comme il est indiqué aux théorèmes II et III. Ainsi, par l'extraction d'un seul radical du troisième degré, il reste simplement le groupe

$$\begin{array}{l} abcd, \\ badc, \\ cdab, \\ dcba\ ; \end{array}$$

ce groupe se partage de nouveau en deux groupes :

$$\begin{array}{ll} abcd, & cdab, \\ badc, & dcba. \end{array}$$

Ainsi, après une simple extraction de racine carrée, il restera

$$\begin{array}{l} abcd\ , \\ badc\ ; \end{array}$$

ce qui se résoudra enfin par une simple extraction de racine carrée. On obtient ainsi, soit la solution de Descartes, soit celle d'Euler ; car, bien qu'après la résolution de l'équation auxiliaire du troisième degré, ce dernier extraye trois racines carrées, on sait qu'il suffit de deux, puisque la troisième s'en déduit rationnellement. Nous allons maintenant appliquer cette condition aux équations irréductibles dont le degré est premier.

Application aux équations irréductibles de degré premier.

PROPOSITION VI.

LEMME. "Une équation irréductible de degré premier ne peut devenir réductible par l'adjonction d'un radical dont l'indice serait autre que le degré même de l'équation."

Car si $r, r', r'', \ldots$ sont les diverses valeurs du radical, et $Fx = 0$ l'équation proposée, il faudrait que Fx se partageât en facteurs

$$f(x,r) \times f(x,r') \times \ldots,$$

tous de même degré, ce qui ne se peut, à moins que $f(x,r)$ ne soit du premier degré en x. Ainsi une équation irréductible de degré premier ne peut devenir réductible, à moins que son groupe ne se réduise à une seule permutation.

PROPOSITION VII.

PROBLÈME. "Quel est le groupe d'une équation irréductible d'un degré premier n, soluble par radicaux ?"

D'après la proposition précédente, le plus petit groupe possible avant celui qui n'a qu'une seule permutation, contiendra n permutations. Or 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 circulaire de l'ordre n. (Voir le Mémoire de M. Cauchy, *Journal de l'Ecole Polytechnique*, XVII^{e} cahier.) Ainsi l'avant-dernier groupe sera

$$\left\{\begin{array}{llllllll} x_0, & x_1, & x_2, & x_3, & \ldots, & x_{n-3}, & x_{n-2}, & x_{n-1}, \\ x_1, & x_2, & x_3, & x_4, & \ldots, & x_{n-2}, & x_{n-1}, & x_0 \\ x_2, & x_3, & \ldots, & \ldots & \ldots & x_{n-1}, & x_0, & x_1, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_{n-1}, & x_0, & x_1, & \ldots, & \ldots & x_{n-4}, & x_{n-3}, & x_{n-2}, \end{array}\right.$$

Maintenant, le groupe qui précédera immédiatement celui-ci dans l'ordre des décompositions devra se composer d'un certain nombre de groupes ayant tous les mêmes substitutions que celui-ci. Or j'observe que ces substitutions peuvent s'exprimer ainsi : (Faisons en général $x_n = x_0, x_{n+1} = x_1, ...$, il est clair que chacune des substitutions du groupe (G) s'obtient en mettant partout à la place de x_k, x_{k+c}, c étant une constante.)

Considérons l'un quelconque des groupes semblables au groupe (G). D'après le théorème II, il devra s'obtenir en opérant partout dans ce groupe une même substitution ; par exemple, en mettant partout dans le groupe (G), à la place de $x_k, x_{f(k)}$, f étant une certaine fonction.

Les substitutions de ces nouveaux groupes devant être les mêmes que celles du groupe (G), on devra avoir

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

C étant indépendant de k.

Donc

$$\begin{aligned} &f(k+2c) = f(k) + 2C, \\ &\dots \\ &f(k+mc) = f(k) + mC. \end{aligned}$$

Si $c = 1, k = 0$, on trouvera

$$f(m) = am + b,$$

ou bien

$$f(k) = ak + b,$$

a et b étant des constantes.

Donc le groupe qui précède immédiatement le groupe (G) ne devra contenir que des substitutions telles que

$$x_k, \quad x_{ak+b},$$

et ne contiendra pas, par conséquent, d'autre substitution circulaire que celle du groupe (G).

On raisonnera sur ce groupe comme sur le précédent, et il s'ensuivra que le premier groupe dans l'ordre des décompositions, c'est- à-dire le groupe *actuel* de l'équation, ne peut contenir que des substitutions de la forme

$$x_k, \quad x_{ak+b}.$$

Donc, "si une équation irréductible de degré premier est soluble par radicaux, le groupe de cette équation ne saurait contenir que des substitutions de la forme

$$x_k, \quad x_{ak+b},$$

a et b étant des constantes."

Réciproquement, si cette condition a lieu, je dis que l'équation sera soluble par radicaux. Considérons, en effet, les fonctions

$$\begin{aligned}
&(x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{n-1} x_{n-1})^n && = X_1,\\
&(x_0 + \alpha x_a + \alpha^2 x_{2a} + \ldots + \alpha^{n-1} x_{(n-1)a})^n && = X_a,\\
&(x_0 + \alpha x_{a^2} + \alpha^2 x_{2a^2} + \ldots + \alpha^{n-1} x_{(n-1)a^2})^n && = X_{a^2},\\
&\ldots
\end{aligned}$$

α étant une racine $n^{\text{ième}}$ de l'unité, a une racine primitive de n.

Il est clair que toute fonction invariable par les substitutions circulaires des quantités $X_1, X_a, X_{a^2}, ...$ sera, dans ce cas, immédiatement connue. Donc on pourra trouver $X_1, X_a, X_{a^2}, ...$, par la méthode de M. Gauss pour les équations binômes. Donc, etc.

Ainsi, pour qu'une équation irréductible de degré premier soit soluble par radicaux, il *faut* et il *suffit* que toute fonction invariable par les substitutions

$$x_k, \quad x_{ak+b}$$

soit rationnellement connue.

Ainsi la fonction

$$(X_1 - X)(X_a - X)X_{a^2} - X)...$$

devra, quel que soit X, être connue.

Il *faut* donc et il *suffit* que l'équation qui donne cette fonction des racines admette, quel que soit X, une valeur rationnelle.

Si l'équation proposée a tous ses coefficients rationnels, l'équation auxiliaire qui donne cette fonction les aura tous aussi, et il suffira de reconnaître si cette équation auxiliaire du degré $1.2.3...(n-2)$ a ou non une racine rationnelle, ce que l'on sait faire.

C'est là le moyen qu'il faudrait employer dans la pratique. Mais nous allons présenter le théorème sous une autre forme.

Proposition viii.

Théorème. "Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il *faut* et il *suffit* que deux quelconques des racines étant connues, les autres s'en déduisent rationnellement."

Premièrement, il le faut, car la substitution

$$x_k, \quad x_{ak+b}$$

ne laissant jamais deux lettres à la même place, il est clair qu'en adjoignant deux racines à l'équation, par la proposition iv, son groupe devra se réduire à une seule permutation.

En second lieu, cela suffit ; car, dans ce cas, aucune substitution du groupe ne laissera deux lettres aux mêmes places. Par conséquent, le groupe contiendra tout au plus $n(n-1)$ permutations. Donc il ne contiendra qu'une seule substitution circulaire (sans quoi il y aurait au moins n^2 permutations). Donc toute substitution du groupe, x_k, x_{fk} devra satisfaire à la condition

$$f(k+c) = fk + C,$$

Donc, etc.

Le théorème est donc démontré.

Exemple du théorème VII.

Soit $n = 5$; le groupe sera le suivant :

abcde
bcdea
cdeab
deabc
eabcd

---

acebd
cebda
ebdac
bdace
daceb

---

aedcb
edcba
dcbae
cbaed
baedc

---

adbec
dbeca
becad
ecadb
cadbe.
