JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

DESPEYROUS

Mémoire sur les équations de degré premier résolubles algébriquement

Journal de mathématiques pures et appliquées 2^e série, tome 11 (1866), p. 9-38.
<http://www.numdam.org/item?id=JMPA_1866_2_11__9_0>

gallica NUMDAM

Article numérisé dans le cadre du programme Gallica de la Bibliothèque nationale de France
http://gallica.bnf.fr/

et catalogué par Mathdoc dans le cadre du pôle associé BnF/Mathdoc
http://www.numdam.org/journals/JMPA

MÉMOIRE

SUR LES

ÉQUATIONS DE DEGRÉ PREMIER RÉSOLUBLES ALGÉBRIQUEMENT;

PAR M. DESPEYROUS.

La solution de cette question générale, *trouver toutes les équations, de degré premier, résolubles algébriquement,* fait l'objet de ce Mémoire. Nous croyons que notre solution est exacte et complète, et nous avons l'espoir qu'elle sera jugée telle par les géomètres.

Les remarquables travaux auxquels la question dont nous venons de parler a donné lieu et les noms de leurs auteurs nous ont fait hésiter longtemps à nous en occuper; mais nos recherches [*] sur la *théorie de l'ordre* et sur l'application que nous en avons faite à la classification des permutations qu'offrent m lettres en groupes de permutations *inséparables* pour tous les échanges de ces lettres, contiennent implicitement une méthode pour la solution du problème énoncé; et c'est le résultat des applications de cette méthode que nous publions aujourd'hui [**].

Nous cherchons d'abord quelles sont les quantités qui doivent entrer dans la composition de la valeur d'une quelconque des racines d'une équation algébrique, irréductible et de degré premier n que l'on suppose résoluble algébriquement. Et nous démontrons par des

[*] *Journal de Mathématiques* publié par M. Liouville, 2e série, t. VI, p. 417; t. X, p. 55 et 177.

[**] Nous devons rappeler que la méthode s'applique aussi avec succès à la solution de cette question plus générale : *trouver toutes les équations de degré composé résolubles algébriquement;* et que nous avons communiqué cette solution à la réunion des Sociétés savantes (*Revue des Sociétés savantes,* t. V, p. 346).

considérations entièrement fondées sur la théorie de l'ordre, que cette valeur doit contenir $n-1$ radicaux d'un même indice, et que chacun d'eux est équivalent à une fonction rationnelle des racines de l'équation proposée.

Puis nous établissons ce théorème :

« Pour résoudre une équation algébrique, irréductible et de degré » premier n, il est nécessaire et suffisant de résoudre deux équations, » l'une de degré $n-1$, l'autre de degré $1.2.3...(n-2)$. Les racines » de cette dernière équation sont des fonctions rationnelles de celles » de la proposée; et elle est appelée équation *résolvante* ou *réduite*. »

Ce théorème est une conséquence *nécessaire* de la théorie générale des équations; vérité aperçue par Lagrange, comme le prouve la dernière phrase de la note XIII du traité de ce grand géomètre sur la *résolution des équations numériques*. Parmi les conséquences de ce théorème, se trouve ce résultat connu : *Toute équation du troisième degré est résoluble algébriquement.*

Puisque la résolution d'une équation algébrique, irréductible et de degré premier n supérieur à 3, dépend nécessairement de la résolution de son équation résolvante du degré $1.2.3...(n-2)$, nombre supérieur au degré n de cette équation, il fallait déterminer les caractères auxquels on reconnaissait que cette équation résolvante était résoluble, ou du moins décomposable en équations de degrés moindres. Ces caractères sont actuellement connus, puisque nous avons démontré que la résolvante n'est décomposable en équations de degrés moindres, qu'autant que les groupes de permutations des racines de l'équation proposée, relatifs à celle de cette résolvante, peuvent être partagés en nouveaux groupes de permutations *inséparables* pour tous les échanges possibles de ces racines.

De là et de notre théorie sur la classification des permutations de m lettres en groupes de permutations *inséparables* pour tous les échanges de ces lettres, nous déduisons ce théorème général :

Pour qu'une équation algébrique et de degré premier n supérieur à 3 *soit résoluble algébriquement, il faut et il suffit :* 1° *qu'elle soit abélienne;* 2° *ou qu'entre trois quelconques de ses racines, il y ait la relation*

$$x_{a+p\rho} = \theta(x_{a+p}, x_a),$$

dans laquelle les indices de x sont pris suivant le module n; ϑ désignant une fonction rationnelle, ρ une des racines primitives du degré n, a un des nombres 0, 1, 2,..., $n-1$ *et p un des nombres* 1, 2, 3,..., $n-1$.

Définitions. — Soient

$$x_0,\ x_1,\ x_2,\ldots,\ x_{m-1}$$

m quantités et V une fonction de ces quantités. V sera une fonction *algébrique* de ces quantités, si elle est formée avec elles à l'aide des six opérations fondamentales des mathématiques ou de quelques-unes d'entre elles, répétées un nombre fini de fois; dont trois directes, addition, multiplication, formation des puissances, et trois respectivement inverses, soustraction, division, extraction des racines.

Si dans la formation de la fonction V, il n'y entre que des signes des quatre premières opérations ou de quelques-unes d'entre elles, V est dite fonction *entière* de $x_0, x_1, \ldots, x_{m-1}$; et si dans V ces quantités sont liées par les signes des cinq premières opérations ou de quelques-unes d'entre elles, V est une fonction *rationnelle* de ces m quantités. Mais nous donnerons une plus grande extension à ces mots *entier* et *rationnel*, et nous dirons qu'une fonction est entière ou rationnelle de ces quantités $x_0, x_1,\ldots, x_{m-1}$, quand bien même son expression contiendrait, dans la première ou dans la seconde formation, des *racines de l'unité* d'un degré quelconque k égal ou différent de m.

Une équation algébrique

$$(1) \qquad F(x) = x^m + A_1 x^{m-1} + A_2 x^{m-2} + \ldots + A_m = 0$$

est *réductible* ou *irréductible* selon que son premier membre se décompose ou ne se décompose pas en facteurs de degrés moindres en x, tels que les coefficients des divers termes de ces facteurs sont des fonctions rationnelles de $A_1, A_2,\ldots, A_m$, *indépendantes* des racines

de l'unité d'un degré quelconque. Nous verrons qu'une équation irréductible peut cesser de l'être, quand on adjoint aux coefficients A_1, A_2,..., A_m de cette équation des racines de certaines équations que nous appellerons *résolvantes*.

Résoudre algébriquement l'équation (1), c'est déterminer une fonction algébrique de ces coefficients qui, substituée à l'inconnue x, satisfasse identiquement à cette équation.

THÉORÈME I. — *Si une équation algébrique, irréductible et de degré premier n est résoluble algébriquement, la valeur d'une quelconque de ses racines contient $n-1$ radicaux d'un même indice, et chacun d'eux est équivalent à une fonction rationnelle des ces mêmes racines, ces $n-1$ radicaux pouvant se réduire à un seul.*

Soient

$$F(x) = 0 \tag{1}$$

l'équation proposée, et x_0, x_1,..., x_{n-1} ses n racines; nous supposerons qu'elle est résoluble algébriquement.

Cette équation étant, par hypothèse, irréductible et résoluble algébriquement, chacune de ses racines est égale à une fonction rationnelle faite avec ses coefficients et avec des radicaux. Et dans aucun cas, ces radicaux ne peuvent disparaître d'une quelconque de ces fonctions; car s'il en était ainsi pour l'une d'elles, le premier membre de cette équation (1) aurait un facteur rationnel, et par suite cette équation ne serait pas irréductible.

Considérons l'un des radicaux, $\sqrt[k]{z_1}$, qui entre dans la composition de l'une x de ses racines, la quantité z_1 pouvant dépendre de radicaux d'indices différents de k. Ce radical, $\sqrt[k]{z_1}$, deviendra une fonction des racines de l'équation (1) quand on y remplacera les coefficients de cette équation par les fonctions symétriques de ces racines qu'ils représentent. On a donc

$$\sqrt[k]{z_1} = f_1(x_0, x_1, \ldots, x_{n-1}). \tag{2}$$

Cela posé, considérons l'une des permutations qui font acquérir à f_1

une même valeur, $x_0 x_1 x_2 \ldots x_{n-1}$ par exemple, et joignons à cette permutation toutes celles qui sont relatives aux polygones étoilés de Poinsot, c'est-à-dire toutes celles que l'on déduit de cette première permutation en prenant successivement ces racines, à partir de la première x_0, de p_1 en p_1, de p_2 en p_2,..., de p_ν en p_ν; ces lettres désignant les ν nombres inférieurs et premiers à n; ν étant égal à $n-1$ puisque n est premier. Or nous avons démontré [*] que ces $n-1$ permutations constituaient un *seul et même ordre,* qu'elles coexistaient toutes dans une quelconque d'entre elles, comme les racines d'une même équation; donc l'expression de cette racine x de l'équation (1) et qui contient $\sqrt[k]{z_1}$, doit nécessairement contenir $\sqrt[k]{z_2}$, $\sqrt[k]{z_3}$,..., $\sqrt[k]{z_{n-1}}$ qui se déduisent de la fonction (2) f_1 en changeant la permutation $x_0 x_1 x_2 \ldots x_{n-1}$ en celles de l'ordre dont elle fait partie : à moins que f_1 ne reste encore invariable pour ces nouvelles permutations. Donc encore ces $n-1$ radicaux doivent entrer dans l'expression de cette racine x d'une manière symétrique, puisque, en changeant l'un dans l'autre ces radicaux, l'expression de cette racine ne saurait être altérée, d'après leur signification. Ainsi l'expression de cette racine x contient $n-1$ radicaux d'un même indice, à moins qu'ils ne se réduisent à un seul.

Il y a plus : si dans cette même expression de x on remplace les coefficients de l'équation proposée par les fonctions symétriques de ses racines qu'ils représentent, cette expression doit nécessairement se réduire à cette racine x. Mais elle contient d'une manière symétrique $n-1$ radicaux ou un seul d'entre eux, qui dans aucun cas ne peuvent s'annuler; donc cette réduction exige que chacun d'eux soit équivalent à une fonction rationnelle des racines de l'équation proposée, en donnant à ce mot *rationnel* l'extension dont nous avons parlé dans les définitions : ainsi f_1 est une fonction rationnelle.

Il est donc démontré que l'expression d'une quelconque x des racines de l'équation (1), supposée irréductible et de degré premier n, contient $n-1$ radicaux de même indice, et que chacun d'eux est

---

[*] *Journal de Mathématiques* publié par M. Liouville, 2e série, t. X, p. 194.

équivalent à une fonction rationnelle des racines de cette équation, ces $n-1$ radicaux se réduisant quelquefois à un seul [*].

THÉORÈME II. — *Pour résoudre une équation algébrique, irréductible et de degré premier n, il est nécessaire et suffisant de résoudre deux équations, l'une de degré* $n-1$, *l'autre de degré* $1.2.3\ldots(n-2)$.

Rappelons auparavant que, n étant un nombre premier, les résidus à n des termes de la suite

$$a,\ a+p,\ a+2p,\ldots,\ a+(n-1)p$$

sont les nombres 0, 1, 2,..., $n-1$ dans un ordre déterminé, p désignant un nombre entier quelconque inférieur à n et a un de ces mêmes nombres ou zéro. De même, ρ étant une des racines *primitives* de n, les résidus à n des termes de la suite

$$a,\ a+p\rho,\ a+p\rho^2,\ldots,\ a+p\rho^{n-2}$$

sont encore les mêmes nombres 0, 1, 2,..., $n-1$, dans tel ou tel ordre selon les valeurs de p et de ρ. Mais les résidus à n des termes de la suite

$$p,\ p\rho,\ p\rho^2,\ldots,\ p\rho^{n-2}$$

sont seulement les termes naturels 1, 2, 3,..., $n-1$. En sorte que les racines $x_0, x_1,\ldots, x_{n-1}$ de l'équation (1) peuvent être représentées par l'une des deux suites

$$x_a,\ x_{a+p},\ x_{a+2p},\ldots,\ x_{a+(n-1)p},$$
$$x_a,\ x_{a+p\rho},\ x_{a+p\rho^2},\ldots,\ x_{a+p\rho^{n-2}}.$$

Enfin, si r et α désignent deux quelconques des racines imaginaires de l'équation binôme $x^n-1=0$, on sait que les racines de cette

---

[*] On verra, dans le théorème suivant, à quoi tient la possibilité de réduire ces $n-1$ radicaux à un seul d'entre eux.

équation sont représentées par l'une des trois suites

$$1,\ \alpha,\ \alpha^2,\ldots,\ \alpha^{n-1},$$
$$1,\ \alpha^q,\ \alpha^{2q},\ldots,\ \alpha^{(n-1)q},$$
$$r,\ r\alpha^q,\ r\alpha^{2q},\ldots,\ r\alpha^{(n-1)q},$$

q désignant un des nombres entiers inférieurs à n.

Cela posé, nous allons d'abord démontrer que les conditions de l'énoncé sont nécessaires; et pour cela nous admettrons que l'équation proposée (1) soit résoluble algébriquement.

Divisons en effet en n parties égales la circonférence du cercle dont le rayon est égal à l'unité; plaçons sur cette circonférence et en ces points de division les racines

$$x_a,\ x_{a+p},\ x_{a+2p},\ldots,\ x_{a+(n-1)p},$$

de la proposée dans tel ordre que l'on voudra, par exemple dans l'ordre où elles sont écrites et qui est relatif à $\sqrt[k]{z_1}$, et joignons ces points de division, d'abord un à un, puis au centre : ces rayons représentent les racines de l'équation binôme $x^n - 1 = 0$.

Or, qu'on lise dans le même sens le polygone régulier obtenu, soit du sommet où se trouve la racine x_a, soit de tout autre sommet, du second par exemple où se trouve la racine x_{a+p}, c'est toujours le *même* polygone; donc $\sqrt[k]{z_1}$, qui est une fonction rationnelle des racines de l'équation proposée et qui est relative, par hypothèse, à la permutation précédente, doit rester invariable quand on y change à la fois les deux permutations

$$\begin{matrix} x_a & x_{a+p} & x_{a+2p}\cdots & x_{a+(n-1)p}, \\ 1 & \alpha^q & \alpha^{2q}\ldots & \alpha^{(n-1)q}, \end{matrix}$$

respectivement en leurs permutations circulaires

$$(3) \qquad \left\{ \begin{matrix} x_{a+p} & x_{a+2p}\cdots & x_a, \\ \alpha^q & \alpha^{2q}\ldots & 1. \end{matrix} \right.$$

De même, si on lit dans le même sens ce même polygone à partir

du troisième sommet où se trouve la racine x_{a+2p}, on obtient toujours ce polygone; donc encore $\sqrt[k]{z_1}$ doit rester invariable quand on change à la fois les permutations (3) respectivement en leurs permutations circulaires, et ainsi de suite pour tous les autres sommets. Donc la fonction rationnelle des racines de la proposée, $\sqrt[k]{z_1}$ doit rester invariable quand on y fait simultanément ces changements circulaires, et il est évident que la fonction la *plus simple* qui jouit de cette propriété est le polynôme

$$x_a + \alpha^q x_{a+p} + \alpha^{2q} x_{a+2p} + \ldots + \alpha^{(n-1)q} x_{a+(n-1)p}.$$

Mais ce polynôme, considéré comme fonction des racines de l'équation (1) à résoudre, est relatif à l'un des polygones étoilés de Poinsot, à celui dont on vient de parler; et ce polygone ne peut être lu que de l'un de ses n sommets. Donc $\sqrt[k]{z_1}$ est égal au polynôme précédent ou à une fonction *semblable* de ces mêmes racines et par suite égal à une fonction rationnelle de ce polynôme, d'après la théorie de Lagrange sur les fonctions semblables. En sorte que, pour déterminer les racines de l'équation proposée par les calculs les plus simples, on doit poser

$$\sqrt[k]{z_1} = x_a + \alpha^q x_{a+p} + \alpha^{2q} x_{a+2p} + \ldots + \alpha^{(n-1)q} x_{a+(n-1)p}.$$

Or $\sqrt[k]{z_1}$ a k valeurs que l'on obtient en multipliant l'une d'elles par chacune des racines de l'équation binôme $x^k - 1 = 0$, et il résulte de ce qui précède que chacune de ces valeurs jouit de la même propriété. Donc r étant l'une des racines imaginaires de cette équation binôme, le produit

$$r_1 x_a + r_1 \alpha^q x_{a+p} + r_1 \alpha^{2q} x_{a+2p} + \ldots + r_1 \alpha^{(n-1)q} x_{a+(n-1)p}$$

doit rester invariable quand on y fait les changements simultanés et circulaires dont nous venons de parler. Et ce résultat ne peut être atteint qu'autant que $r_1 = r$; puisque r_1, $r_1\alpha^q$, $r_1\alpha^{2q}, \ldots, r_1\alpha^{(n-1)q}$ doivent être les racines de l'équation binôme $x^n - 1 = 0$. D'ailleurs, ce n'est que pour ces dernières racines que le polynôme précédent doit rester invariable par suite de ces mêmes changements; donc l'équation $x^k - 1 = 0$ doit coïncider avec $x^n - 1 = 0$; ce qui exige que k

soit égal à n. Donc enfin, l'on a

$$(4) \qquad \sqrt[n]{z_1} = x_a + \alpha^q x_{a+p} + \alpha^{2q} x_{a+2p} + \ldots + \alpha^{(n-1)q} x_{a+(n-1)p}.$$

Le radical, $\sqrt[n]{z_1}$, étant actuellement connu en fonction des racines à trouver, on déduira de sa valeur celles des $n-2$ autres, $\sqrt[n]{z_2}$, $\sqrt[n]{z_3}, \ldots,$ $\sqrt[n]{z_{n-1}}$, par les permutations déjà indiquées de ces racines. Et il résulte évidemment des expressions de ces $n-1$ radicaux que si l'on parvenait à connaître leurs valeurs en fonction des coefficients de l'équation (1), on aurait $n-1$ équations, qui, réunies à l'équation connue

$$x_a + x_{a+p} + x_{a+2p} + \ldots + x_{a+(n-1)p} = -A_1$$

formeraient un système de n équations linéaires par rapport aux racines de l'équation (1) à résoudre, desquelles on déduirait chacune d'elles. Donc, pour trouver ces racines, il faut connaître

$$z_1, z_2, z_3, \ldots, z_{n-1}.$$

Or, quelles que soient leurs expressions, ces $n-1$ fonctions des n racines de l'équation proposée sont semblables. Car les $n-1$ radicaux, $\sqrt[n]{z_1}$, $\sqrt[n]{z_2}, \ldots,$ $\sqrt[n]{z_{n-1}}$, fonctions de ces racines, sont relatifs aux $n-1$ permutations de ces mêmes racines qui forment un *seul et même ordre;* donc ils jouissent tous des mêmes propriétés. De là il suit que si un changement de ces n racines fait conserver une même valeur à l'un de ces radicaux, ce même changement n'altérera pas non plus les $n-2$ autres; et que si un changement de ces mêmes racines transforme l'un de ces radicaux en un autre, ce même changement de racines transformera les $n-2$ autres les uns dans les autres. Donc ces $n-1$ radicaux sont semblables [*], et par suite leurs puissances $n^{ièmes}$, c'est-à-dire $z_1, z_2, \ldots, z_{n-1}$, seront aussi semblables.

---

[*] Ces $n-1$ radicaux étant semblables et étant équivalents à des fonctions rationnelles des racines de la proposée, l'un d'eux étant donné, chacun des $n-2$ autres est égal à une fonction rationnelle de celui-là. C'est pourquoi nous avons dit, théorème I, que la racine pouvait ne contenir qu'un seul de ces radicaux.

Ces $n-1$ fonctions étant semblables, leurs expressions, quelles qu'elles soient, et par conséquent celles qui se déduisent de la formule (4), sont racines d'une même équation, de degré $n-1$, dont les coefficients sont également semblables et ne dépendent par suite que d'un seul, de celui par exemple qui est égal à la somme de ces $n-1$ fonctions,

$$y = z_1 + z_2 + z_3 + \ldots + z_{n-1}. \tag{5}$$

En sorte que l'équation dont les racines sont ces $n-1$ quantités, est

$$Z^{n-1} - yZ^{n-2} + B_2 Z^{n-3} + \ldots + B_{n-1} = 0; \tag{6}$$

dans laquelle les coefficients $B_2, B_3, \ldots, B_{n-1}$ peuvent être exprimés en fonction rationnelle de y. Et cette dernière quantité dépend elle-même d'une autre équation,

$$\varphi(y) = 0, \tag{7}$$

dont les coefficients ne dépendent que de ceux de l'équation donnée (1). Permutons en effet les n racines de cette dernière équation dont se compose la forme connue (5) de la fonction y, et désignons par y_1, $y_2, \ldots, y_s$ les s valeurs distinctes que prend cette fonction. La somme de ces valeurs, $y_1 + y_2 + \ldots + y_s$, les sommes de leurs produits deux à deux, trois à trois,... sont évidemment des fonctions symétriques des n racines de l'équation (1); elles peuvent donc être exprimées en fonctions rationnelles de ses coefficients, fonctions qui seront les coefficients de l'équation (7).

Le degré de cette dernière est d'ailleurs facile à déterminer. En effet, chacun des termes de y est invariable pour les n permutations circulaires que produit celle des n racines de l'équation à résoudre relative à ce terme, puisque l'on a

$$\begin{aligned}&(x_{a+p} + \alpha^q x_{a+2p} + \ldots + \alpha^{(n-1)q} x_a)^n \\ &\quad = \alpha^{(n-1)qn} (x_a + \alpha^q x_{a+p} + \ldots + \alpha^{(n-1)q} x_{a+(n-1)p})^n = z_1^n,\end{aligned}$$

et que la démonstration serait la même pour chacune des $n-1$ autres

permutations circulaires, ainsi que pour chacun des autres termes de y. De plus, y est symétrique par rapport aux $n-1$ termes $z_1, z_2, \ldots, z_{n-1}$ relatifs aux $n-1$ permutations d'un même ordre. Donc y acquiert des valeurs égales pour les $n(n-1)$ permutations d'un quelconque des groupes de notre troisième classification [*]; et par suite le nombre s de ses valeurs distinctes, c'est-à-dire le degré de l'équation (7), est donné par la formule

$$s = \frac{1.2.3\ldots n}{(n-1).n} = 1.2.3\ldots(n-2);$$

et ce degré s serait le même si, au lieu de prendre pour $z_1, z_2, \ldots, z_{n-1}$ les valeurs qui se déduisent de (4), on prenait d'autres fonctions, puisque ces dernières seraient respectivement semblables aux premières.

Ainsi, pour déterminer les racines de l'équation (1), il faut avoir les valeurs de $z_1, z_2, \ldots, z_{n-1}$; il faut donc résoudre l'équation (6) du degré $n-1$, résolution qui exige celle de l'équation (7) du degré $1.2.3\ldots(n-2)$. Les conditions du théorème à démontrer sont donc nécessaires.

Démontrons actuellement qu'elles sont suffisantes. Nous remarquerons d'abord que l'une des $n-1$ valeurs $z_1, z_2, \ldots, z_{n-1}$, par exemple z_1, les reproduit toutes en y remplaçant p successivement par $p, p\rho, p\rho^2, \ldots, p\rho^{n-2}$; car ces $n-1$ valeurs étant relatives aux $n-1$ permutations d'un même ordre, celle qui est relative à z_1, et qui est faite avec les n racines de l'équation proposée, reproduira toutes ces permutations en lisant ces racines, à partir de la première, successivement de 1 à 1, de 2 à 2, ..., de $n-1$ à $n-1$; tandis que les résidus à n de $p, p\rho, p\rho^2, \ldots, p\rho^{n-2}$ sont précisément ces mêmes nombres $1, 2, 3, \ldots, n-1$ dans un ordre déterminé. Et puis, si l'on suppose en effet les équations (7) et (6) résolues, et si l'on extrait la racine $n^{ième}$ de la valeur de chacune des $n-1$ racines de cette dernière; on aura, en observant que la somme des racines de la proposée est connue et

[*] *Journal de Mathématiques* publié par M. Liouville, t. X, 2e série, p. 183.

égale à $-A_1$, les n équations

$$(8)\quad \begin{cases} x_a + x_{a+p} + x_{a+2p} + \ldots + x_{a+(n-1)p} = -A_1, \\ x_a + \alpha^q x_{a+p} + \alpha^{2q} x_{a+2p} + \ldots + \alpha^{(n-1)q} x_{a+(n-1)p} = \sqrt[n]{z_1}, \\ x_a + \alpha^q x_{a+p\rho} + \alpha^{2q} x_{a+2p\rho} + \ldots + \alpha^{(n-1)q} x_{a+(n-1)p\rho} = \sqrt[n]{z_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_a + \alpha^q x_{a+p\rho^{n-2}} + \alpha^{2q} x_{a+2p\rho^{n-2}} + \ldots + \alpha^{(n-1)q} x_{a+(n-1)p\rho^{n-2}} = \sqrt[n]{z_{n-1}}, \end{cases}$$

linéaires par rapport aux n racines à trouver.

Pour résoudre ces n équations, il suffit d'observer que, dans chacune d'elles, les racines qui sont multipliées par les diverses puissances de α sont différentes, et que dans chaque colonne verticale les racines qui sont multipliées par une même puissance de α sont également différentes. Car le nombre de ces équations étant n, et toutes les racines étant dans chaque équation, une quelconque de ces racines, x_a exceptée, aura successivement pour coefficients dans ces n équations, 1, α^q, α^{2q},..., $\alpha^{(n-1)q}$ qui sont les racines de $x^n - 1 = 0$. De là il suit que si l'on veut obtenir l'une des racines de (1), par exemple x_{a+p}, il suffira de multiplier convenablement les deux membres de chacune des équations (8) par 1, α^{-q}, α^{-2q},..., $\alpha^{-(n-1)q}$ qui sont ces mêmes racines de $x^n - 1 = 0$, et de faire la somme des produits; car, d'après les propriétés connues des racines des équations binômes, l'on aura la formule

$$(9)\qquad x_{a+p} = \frac{1}{n}\left(-A_1 + \alpha^{-q}\sqrt[n]{z_1} + \beta\sqrt[n]{z_2} + \ldots + \lambda\sqrt[n]{z_{n-1}}\right),$$

dans laquelle α^{-q}, β,..., λ désignent les racines imaginaires de cette même équation binôme.

Et il est clair que cette formule (9) donnera toutes les autres racines de (1) en remplaçant successivement les radicaux qu'elle contient par leurs diverses valeurs.

A la vérité, les valeurs du second membre de cette formule sont au nombre de n^{n-1}; mais on peut faire disparaître l'ambiguïté qui en résulte, en observant que les $n-1$ radicaux des seconds membres des équations (8) sont des fonctions rationnelles et semblables de la pro-

posee; et que par suite, l'un d'eux étant donné, on peut exprimer chacun des autres en fonction rationnelle de celui-là. Donc la formule (9) ne contiendra, réduction faite, qu'un seul radical d'indice n, et n'aura dès lors que n valeurs qui seront les n racines cherchées.

Ainsi, ces conditions sont suffisantes; elles sont d'ailleurs nécessaires. Il est donc nécessaire et suffisant, pour résoudre une équation irréductible et de degré premier n, de résoudre deux équations, l'une de degré $n-1$, l'autre de degré $1.2.3...(n-2)$; et ce résultat a été obtenu sans faire aucune hypothèse sur les racines de l'équation proposée.

Corollaire. — Si dans le calcul précédent on fait $n=3$, c'est-à-dire si l'équation à résoudre est du troisième degré, l'équation en y se réduit au premier degré, et celle en Z au deuxième. Donc, la fonction $y=z_1+z_2$ est une fonction rationnelle des coefficients de l'équation proposée, et les valeurs z_1, z_2 et, par suite, les racines x_0, x_1, x_2 de cette équation peuvent être déterminées en fonctions de ses coefficients. Les expressions de ces racines renfermeront deux radicaux cubiques et un radical carré.

On a donc ce théorème : *Toute équation du troisième degré est soluble par radicaux.*

Remarque. — Nous appellerons y la fonction *résolvante* de l'équation proposée (1), et $\varphi(y)=0$ son équation résolvante.

THÉORÈME III. — *Quelle que soit la composition de la fonction résolvante y de l'équation irréductible* $F(x)=0$, *et quel que soit le nombre s de ses valeurs distinctes; si les s groupes de permutations en $x_0, x_1, \ldots, x_{n-1}$, relatifs à ces s valeurs peuvent être partagés en ν groupes de permutations inséparables; l'équation résolvante $\varphi(y)=0$ se décompose en ν équations, chacune de degré r, $s=\nu r$, à l'aide des racines d'une équation algébrique de degré ν, dont les coefficients sont des fonctions rationnelles de ceux de la proposée.*

Puisque, par hypothèse, la fonction résolvante y a s valeurs, et qu'elle est fonction des racines de la proposée $x_0, x_1, x_2, \ldots, x_{n-1}$, il a été démontré [*] que si l'on permute dans y ces n lettres de toutes les

[*] *Journal de Mathématiques* publié par M. Liouville, t. X, 2e série, p. 59.

manières possibles, le nombre total μ des permutations de ces lettres peut être partagé en s groupes composés chacun de q permutations, $\mu = sq$, associés de telle manière que, malgré tous les échanges de ces lettres, les permutations d'un même groupe ne peuvent jamais se séparer. Supposons que ce partage soit effectué, et désignons par (A) le tableau de permutations qui en résulte.

Or, nous supposons en outre que ces s groupes se partagent en ν groupes de permutations *inséparables*, composés chacun de r groupes du tableau (A) : soit (A') le nouveau tableau de permutations que l'on obtient. Mais, si γ est une fonction symétrique quelconque des r valeurs de y relatives à l'un de ces ν groupes, la somme par exemple; et si l'on désigne par $\gamma_1, \gamma_2, \ldots, \gamma_\nu$ les valeurs qu'elle prend pour chacun de ces ν groupes; toute fonction symétrique de $\gamma_1, \gamma_2, \ldots, \gamma_\nu$ est invariable par rapport aux n racines de l'équation (1); car les groupes du tableau (A') étant inséparables pour tous les échanges des n racines, tout changement de ces racines qui ne fera que déplacer les permutations d'un de ces groupes, rendra invariable la valeur de γ relative à ce groupe, et tout changement de ces mêmes racines qui substituera les permutations d'un de ces groupes à celles d'un autre, transformera les valeurs de γ relatives à ces deux groupes l'une dans l'autre, et rendra par conséquent invariable la fonction symétrique des valeurs de γ. Donc toute fonction symétrique de ces ν valeurs est invariable par rapport aux n racines de l'équation (1), et dès lors exprimable en fonction rationnelle des coefficients de cette équation. Il est donc possible d'exprimer en fonction rationnelle de ces coefficients : 1° la somme de ces valeurs $\gamma_1, \gamma_2, \ldots, \gamma_\nu$; 2° les sommes de leurs produits deux à deux, trois à trois, et ainsi de suite; et par conséquent de former l'équation

$$\Gamma^\nu + C_1\Gamma^{\nu-1} + C_2\Gamma^{\nu-2} + \ldots + C_\nu = 0, \tag{10}$$

dont les racines sont $\gamma_1, \gamma_2, \ldots, \gamma_\nu$.

Admettons que cette dernière équation soit résolue, et soit γ_1 l'une de ses racines. Cette racine γ_1 étant la somme des r valeurs $y_1, y_2, \ldots, y_r$ de la fonction résolvante y relatives à l'un des groupes du tableau (A'), du premier par exemple, toute fonction symétrique de ces r valeurs est semblable à γ_1, et par conséquent exprimable en fonc-

tion rationnelle de γ_1 et des coefficients de l'équation (10), qui sont eux-mêmes des fonctions rationnelles des coefficients de l'équation proposée. Donc, on peut exprimer en fonction rationnelle de γ_1 et des données de la question, 1° la somme des produits deux à deux de ces valeurs $y_1, y_2, \ldots, y_r$; 2° les sommes de leurs produits trois à trois, et ainsi de suite; d'où la formation de l'équation

$$y^r - \gamma_1 y^{r-1} + P_2 y^{r-2} + \ldots + P_r = 0,$$

dont les racines sont $y_1, y_2, \ldots, y_r$.

De la même manière l'on démontrerait que $\gamma_2, \gamma_3, \ldots, \gamma_s$ étant les autres racines de l'équation (10), on peut, avec les coefficients de l'équation donnée, exprimer en fonction rationnelle, 1° de γ_2, les coefficients de l'équation dont les racines sont les valeurs de y relatives au deuxième groupe du tableau (A'); 2° de γ_3, les coefficients de l'équation dont les racines sont les valeurs de y relatives au troisième groupe du même tableau, et ainsi de suite pour les équations dont les racines correspondent aux autres groupes de (A'), ce qui produit les équations

$$\begin{aligned} &y^r - \gamma_2 y^{r-1} + Q_2 y^{r-2} + \ldots + Q_r = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ &y^r - \gamma_s y^{r-1} + U_2 y^{r-2} + \ldots + U_r = 0. \end{aligned}$$

Ainsi, sans qu'on soit obligé de former l'équation résolvante $\varphi(y) = 0$ de degré s, on peut former l'équation (10), et, à l'aide de ses racines, les équations en y dont les racines sont celles de la résolvante; ce qui démontre le théorème énoncé.

Remarque. — Si l'on forme préalablement l'équation résolvante $\varphi(y) = 0$, il est possible de trouver d'une autre manière les coefficients $P_2, P_3, \ldots, P_r$. Car l'équation $\varphi(y) = 0$ contenant toutes les racines de cette première équation en y du degré r, $\varphi(y)$ est exactement divisible par le polynome $y_1 - \gamma_1 y^{r-1} + P_2 y^{r-2} + \ldots + P_r$. Le reste de cette division, de degré $r - 1$, sera donc nul; et, en égalant à zéro chacun de ses coefficients, on aura r équations entre $\gamma_1, P_2, \ldots, P_r$; $r - 1$ de ces équations détermineront les $r - 1$ inconnues $P_2, \ldots, P_r$ en fonction rationnelle de γ_1, puisque ce sont des fonctions semblables,

et l'équation restante sera satisfaite identiquement quand on y remplacera ces coefficients par leurs valeurs.

Les coefficients des autres équations en y pourront être déterminés de la même manière.

THÉORÈME IV. — *Réciproquement, si l'équation résolvante* $\varphi(y) = 0$ *d'une équation irréductible* $F(x) = 0$ *est décomposable en* ν *facteurs de degrés moindres, à l'aide des* ν *valeurs que prend une fonction* γ *des* n *racines de cette équation en* x *par les permutations de ces racines, les groupes de permutations faites avec les racines de cette même équation en* x *relatifs aux racines de l'équation en* y, *peuvent être partagés en* ν *groupes de permutations inséparables, et ces équations de degrés moindres sont toutes d'un même degré.*

Admettons en effet que l'on ait

$$\varphi(y) = \varphi_1(y, \gamma_1) \cdot \varphi_2(y, \gamma_2) \cdots \varphi_\nu(y, \gamma_\nu), \tag{11}$$

$\gamma_1, \gamma_2, \ldots, \gamma_\nu$ désignant les ν valeurs que prend la fonction γ des n racines $x_0, x_1, \ldots, x_{n-1}$ de $F(x) = 0$, par suite de toutes les permutations de ces racines. L'équation $\varphi(y) = 0$ étant la résolvante de cette équation en x, ses racines y sont des fonctions rationnelles, théorème II, des racines de $F(x) = 0$; et si son degré est égal à s, les permutations des n racines en x peuvent être partagées, nous l'avons déjà dit, en s groupes de permutations inséparables pour tous les échanges de ces mêmes racines en x, celles d'un même groupe faisant acquérir une même valeur à y. Supposons que ce partage soit effectué, et désignons par (A) le tableau de permutations que l'on obtient.

De même, γ étant une fonction des mêmes racines en x, et ayant ν valeurs par les permutations de ces racines, ces permutations peuvent être partagées en ν groupes de permutations inséparables pour tous les échanges de ces racines, celles d'un même groupe faisant acquérir une même valeur à γ. Supposons également ce partage effectué, et soit (A') le tableau des permutations qui en résulte.

Cela posé, je remarque que les valeurs de y qui annulent les facteurs $\varphi_1, \varphi_2, \ldots, \varphi_\nu$ sont respectivement fonctions de $\gamma_1, \gamma_2, \ldots, \gamma_\nu$. De là il suit que si l'on considère d'abord toutes les permutations du groupe

du tableau (A) relatif à l'une quelconque des valeurs $y_1, y_2, \ldots, y_r$ qui annulent l'un de ces facteurs, φ_1 par exemple, r désignant son degré, tous les échanges des n lettres $x_0, x_1, \ldots, x_{n-1}$ qui n'altèrent pas cette valeur y_1, c'est-à-dire qui convertissent les unes dans les autres les permutations de ce groupe, ne doivent pas altérer non plus γ_1; car, si par suite de quelques-uns de ces échanges, γ_1 prenait une valeur différente, cette autre valeur ne pourrait être que l'une des autres valeurs de γ, par exemple γ_h; dès lors, ces mêmes échanges transformeraient les racines $y_1, y_2, \ldots, y_r$ du facteur φ_1 en celles du facteur φ_h; ce qui est contre l'hypothèse. Donc, toutes les permutations de ce groupe du tableau (A) doivent se trouver dans celui du tableau (A′) relatif à γ_1, ce dernier groupe étant effectivement le seul qui fasse acquérir à γ cette valeur γ_1. Par une même raison, si l'on considère ensuite toutes les permutations des groupes du tableau (A) relatifs à ces r valeurs de y, tous les échanges des n lettres x qui convertissent ces groupes les uns dans les autres n'altéreront pas non plus cette même valeur γ_1. Donc encore, ces r groupes du tableau (A) se trouvent dans celui du tableau (A′) qui correspond à γ_1; ce dernier groupe étant effectivement le seul qui fasse acquérir à γ cette valeur γ_1.

Ainsi, le groupe du tableau (A′) qui est relatif à γ_1 se compose de toutes les permutations qui correspondent aux r groupes du tableau (A) produisant les racines $y_1, y_2, \ldots, y_r$ de l'équation $\varphi_1 = 0$. La même démonstration s'applique évidemment aux autres groupes de (A′) relatifs aux autres valeurs $\gamma_2, \gamma_3, \ldots, \gamma_\nu$ de la fonction γ; chacun d'eux se compose des permutations des groupes de (A) qui correspondent respectivement aux racines y des équations $\varphi_2 = 0, \varphi_3 = 0, \ldots, \varphi_\nu = 0$.

De là, il suit d'abord que les s groupes du tableau (A) se décomposent en ν groupes formant le tableau (A′). Et puis, comme les permutations des groupes de ce dernier sont inséparables, le nombre de permutations, et par suite le nombre de groupes de (A) qui forment ceux de (A′), est le même pour tous ces derniers groupes, et par conséquent les facteurs du second membre de l'équation (11) sont tous du même degré r en y.

En sorte que les s groupes du tableau (A) peuvent être partagés en ν groupes de permutations inséparables, et les facteurs du second membre de l'équation (11) sont tous d'un même degré r tel que $s = \nu r$.

Remarque. — On peut évidemment considérer $\gamma_1, \gamma_2, \ldots, \gamma_\nu$ comme les racines d'une équation du degré ν dont les coefficients seraient faciles à former, comme il a déjà été dit, si la fonction γ était connue.

THÉORÈME V. — *Pour que l'équation résolvante* $\varphi(y) = 0$ *de degré* s *d'une équation irréductible* $F(x) = 0$ *soit décomposable en* ν *équations d'un même degré* r *tel que* $s = \nu r$, *à l'aide des racines d'une équation de degré* ν; *il faut et il suffit que les* s *groupes de permutations faites avec les racines de* $F(x) = 0$ *relatifs aux* s *racines de cette équation en* y *puissent être partagés en* ν *groupes de permutations inséparables.*

Ce théorème est en effet une conséquence des deux qui précèdent.

THÉORÈME VI. — *Si deux racines d'une équation algébrique irréductible et de degré composé* m *sont tellement liées, que l'une d'elles soit égale à une fonction rationnelle de l'autre, toutes les racines de cette équation peuvent être partagées en un ou plusieurs groupes composés d'un même nombre de termes, et tels, que dans chacun d'eux chaque racine soit égale à la même fonction rationnelle de la précédente.*

En effet, si x désigne une des racines de l'équation proposée

$$F(x) = 0,$$

$\theta(x)$ sera une autre racine de cette équation, θ désignant une fonction rationnelle de x et de quantités connues. On aura donc

$$F(\theta x) = 0,$$

et je dis que cette dernière équation est encore satisfaite quand on y remplace x par une racine quelconque de la proposée. Car, si l'on effectue les calculs indiqués par les signes θ et F, on obtiendra

$$F(\theta x) = \frac{\varphi(x)}{\psi(x)},$$

$\varphi(x)$ et $\psi(x)$ désignant des fonctions entières par rapport à x que l'on peut toujours supposer premières entre elles. Mais l'équation $F(\theta x) = 0$ entraîne l'équation $\varphi(x) = 0$; et comme l'on a $F(x) = 0$,

les fonctions entières $\varphi(x)$ et $F(x)$ doivent avoir un plus grand commun diviseur algébrique, et puisque $F(x) = 0$ est une équation irréductible, on doit avoir $\varphi(x) = F(x).\varphi_1(x)$, et par suite

$$F(\theta x) = \frac{\varphi_1(x)}{\psi(x)} \cdot F(x); \tag{12}$$

et j'ajoute que $\psi(x) = 0$ et $F(x) = 0$ ne sauraient avoir lieu en même temps; car on aurait alors $\psi(x) = F(x).\psi_1(x)$, et par suite $\varphi(x)$ et $\psi(x)$ ne seraient pas premières entre elles.

Cette équation (12) prouve que toute racine de l'équation proposée $F(x) = 0$, est racine de $F(\theta x) = 0$; mais θx est racine de la proposée, donc $\theta\theta x$, ou simplement $\theta^2 x$, est racine de la même équation : de même $\theta^2(x)$ étant racine de la proposée, $\theta\theta^2(x)$, ou simplement $\theta^3 x$, est encore racine de la même équation, et ainsi de suite à l'infini. Donc chacun des termes de la suite prolongée indéfiniment,

$$x,\ \theta x,\ \theta^2 x,\ldots,\ \theta^{n-1} x,\ \theta^n x\ldots,$$

est racine de la proposée; et comme cette équation est de degré fini m, cette suite ne doit contenir au plus que m termes distincts.

Soit

$$\theta^{n+p} = \theta^p x;$$

l'équation $\theta^n x - x = 0$ a donc pour racine $\theta^p x$ qui est aussi une racine de $F(x) = 0$; d'où il suit que, d'après ce qui précède, toute racine de $F(x) = 0$ est aussi racine de $\theta^n x - x = 0$, et que par conséquent on a $\theta^{n+1} x = \theta x$, $\theta^{n+2} x = \theta^2 x$, et ainsi de suite. Ainsi, les seuls termes distincts de la suite indéfinie qui précède, sont

$$x,\ \theta x,\ \theta^2 x,\ldots,\ \theta^{n-1} x : \tag{13}$$

et si $m = n$, cette suite démontre le théorème.

Supposons actuellement $m > n$, et soit x_1 une des racines de $F(x) = 0$ non comprise dans la suite (13). On démontrera de la même manière que chaque terme de la suite indéfiniment prolongée

$$x_1,\ \theta x_1,\ \theta^2 x_1,\ldots,$$

est racine de l'équation proposée, et que les seuls termes distincts de cette suite sont les n termes

$$x_1,\ \theta x_1,\ \theta^2 x_1,\ldots,\ \theta^{n-1} x_1.$$

Je dis de plus que ces termes sont différents de ceux de la suite (13). Car, si l'on pouvait avoir $\theta^h x_1 = \theta^k x$, l'on aurait

$$\theta^{n-k}\theta^h x_1 = \theta^{n-k}\theta^k x = \theta^n x = x,$$

d'où il suit que, dans cette dernière suite continuée indéfiniment, la racine x s'y trouverait, et que par conséquent elle contiendrait tous les termes de la suite (13), c'est-à-dire, en d'autres termes, que ces deux suites coïncideraient; ce qui est contre l'hypothèse, puisque x_1 diffère de chacun des termes de la suite (13).

Ainsi, ces deux suites contiennent $2n$ racines distinctes de l'équation proposée; donc si $m = 2n$, le théorème est démontré. Mais si $m > 2n$ et si x_2 désigne une racine de $F(x) = 0$ qui ne fasse partie ni de la suite (13) ni de la suivante en x_1, on démontrerait de la même manière qu'avec x_2, on formerait un troisième groupe de n racines différentes

$$x_2,\ \theta x_2,\ \theta^2 x_2,\ldots,\ \theta^{n-1} x_2,$$

et distinctes de celles des deux premiers groupes, et ainsi de suite.

En sorte que les m racines de l'équation proposée peuvent être partagées en groupes composés chacun d'un même nombre de racines,

$$\text{(B)}\qquad \left\{\begin{array}{l} x,\ \theta x,\ \theta^2 x,\ldots,\ \theta^{n-1} x,\\ x_1,\ \theta x_1,\ \theta^2 x_1,\ldots,\ \theta^{n-1} x_1,\\ x_2,\ \theta x_2,\ \theta^2 x_2,\ldots,\ \theta^{n-1} x_2,\\ \ldots\ldots\ldots\ldots\ldots; \end{array}\right.$$

et tels que, dans chacun d'eux, chaque racine est égale à la *même* fonction rationnelle de la précédente.

Corollaire. — Si le degré m de l'équation proposée est un nombre premier, les groupes du tableau (B) se réduisent en un seul. Car dans la suite (13) on a $\theta^n x = x$, et si n était inférieur à m, il y aurait au

moins $2n$ racines distinctes dans cette équation; ce qui est impossible, puisque n est premier. Donc $m = n$, et par conséquent tous les groupes (B) se réduisent au premier.

Remarque. — Une équation dont les m racines peuvent être représentées par la suite

$$x,\ \theta x,\ \theta^2 x,\ldots,\ \theta^{m-1} x,$$

θ désignant une fonction rationnelle telle que $\theta^m x = x$, est dite *abélienne*.

De cette définition et du corollaire précédent, résulte donc ce théorème : *Si deux racines d'une équation irréductible et de degré premier sont tellement liées, que l'une d'elles soit égale à une fonction rationnelle de l'autre, cette équation est abélienne.*

THÉORÈME VII. — *Pour qu'une équation algébrique, irréductible et de degré premier n, supérieur à* 3, *soit résoluble algébriquement, il faut et il suffit :* 1° *qu'elle soit abélienne;* 2° *ou qu'entre trois quelconques de ses racines il y ait la relation*

$$x_{a+p\rho} = \theta(x_{a+p},\ x_a), \tag{14}$$

dans laquelle les indices de x sont pris suivant le module n; θ désignant une fonction rationnelle, ρ une des racines primitives du degré n, a un des nombres 0, 1, 2,..., $n-1$, *et p un des nombres* 1, 2, 3,..., $n-1$.

Soient

$$\mathrm{F}(x) = 0 \tag{1}$$

l'équation que l'on considère et n son degré. Cette équation étant par hypothèse irréductible et de degré premier, sa résolution dépend nécessairement, théorème II, de celle de deux autres, l'une (6) de degré $n-1$, l'autre (7) de degré $1.2.3\ldots(n-2)$. Donc pour résoudre l'équation proposée (1), il faut résoudre ces deux équations, et d'abord la dernière dont une des racines sert effectivement à former les coefficients de la première. Mais cette dernière (7) a pour racines les $1.2.3\ldots(n-2)$ valeurs de la fonction y définie par la formule (5), valeurs qui correspondent aux groupes de notre troisième classification

déjà citée des permutations de n lettres : et n étant supérieur à 3, les groupes de cette classification ne peuvent être partagés [*] en nouveaux groupes de permutations inséparables; donc, théorème V, cette équation résolvante (7), $\varphi(y) = 0$, est indécomposable en équations de degrés moindres. Donc pour que l'équation proposée soit résoluble algébriquement, il faut que toutes les racines de cette équation résolvante soient égales entre elles; puisque toute autre hypothèse la rendrait décomposable en équations de degrés moindres.

Or, tous les coefficients de cette résolvante, $\varphi(y) = 0$, sont des fonctions symétriques des racines de l'équation proposée (1); donc la somme $y_1 + y_2 + \ldots$ des racines de cette première équation est une fonction invariable des racines de la seconde; et, puisque toutes les racines $y_1, y_2, \ldots$ sont égales, la valeur de y donnée par la formule (5), *telle qu'elle est faite*, doit être une fonction invariable des racines de l'équation (1). Mais cette fonction est rationnelle par rapport aux n racines de (1) et invariable pour les $n(n-1)$ permutations faites avec ces racines, relatives à un même ordre vu successivement de chacune d'elles; et $n(n-1)$ est égal au nombre de combinaisons deux à deux que l'on peut faire avec n lettres. Donc cette fonction résolvante y doit se réduire, d'une manière rationnelle, à ne contenir que deux des n racines de l'équation proposée (1), à moins qu'elle ne se réduise à ne contenir qu'une seule de ces mêmes racines. De là deux cas *seulement* à distinguer.

1° Si la fonction y se réduit à une fonction rationnelle d'une seule des racines de l'équation proposée, la forme de cette fonction exige que, une des racines de la proposée étant donnée, chacune des $n-1$ autres soit égale à une fonction rationnelle de celle-là; donc, corollaire du théorème VI, l'équation proposée est *abélienne*. Ainsi, dans ce premier cas, pour que l'équation (1) soit résoluble algébriquement, il faut que la première des conditions du théorème énoncé soit satisfaite.

2° Si la fonction y se réduit à une fonction rationnelle de deux des racines de l'équation proposée, cette réduction exige que, deux racines

---

[*] *Voir* la Note placée à la fin de ce Mémoire.

quelconques de cette équation étant données, par exemple x_a et x_{a+p}, on puisse exprimer par des fonctions rationnelles chacune des $n-2$ autres. Donc la fonction z_1, qui contient ces n racines, se réduira à une fonction rationnelle de x_a et x_{a+p}, par exemple à

$$z_1 = \psi(x_{a+p}, x_a), \tag{15}$$

ψ désignant une fonction rationnelle : il en sera de même des fonctions $z_2, z_3, \ldots, z_{n-1}$. Mais ces dernières fonctions se déduisent de z_1 en changeant p successivement en $p\rho, p\rho^2, \ldots, p\rho^{n-2}$, on doit donc avoir les relations

$$\left\{\begin{array}{l} z_2 = \psi(x_{a+p\rho}, x_a), \\ z_3 = \psi(x_{a+p\rho^2}, x_a), \\ \cdots\cdots\cdots, \\ z_{n-1} = \psi(x_{a+p\rho^{n-2}}, x_a); \end{array}\right. \tag{16}$$

et comme z_1 peut être écrite ainsi

$$z_1 = (x_a + \alpha^q x_{a+p} + \alpha^{2q} x_{a+p\rho} + \ldots + \alpha^{(n-1)q} x_{a+p\rho^{n-2}})^n,$$

ces relations exigent l'existence de la relation (14). Ainsi dans ce second cas, pour que l'équation proposée soit résoluble, il faut que la seconde condition du théorème énoncé soit satisfaite.

Donc l'une ou l'autre des conditions énoncées sont nécessaires.

Pour démontrer qu'elles sont suffisantes, nous devons évidemment aussi distinguer deux cas.

1° Si l'équation proposée est abélienne, c'est-à-dire si ses racines sont représentées par la suite

$$x_a, \theta x_a, \theta^2 x_a, \ldots, \theta^{n-1} x_a, \tag{17}$$

telle que $\theta^n x_a = x_a$; chacune des racines de l'équation (6), d'où dépend nécessairement la résolution de l'équation proposée, peut être trouvée immédiatement, d'où l'on déduira la valeur de la somme de ces racines qui est précisément la racine unique de l'équation résolvante (7); car l'une de ces $n-1$ racines, z_1 par exemple, est invariable

pour les n permutations circulaires relatives aux n racines de la proposée; et d'après l'hypothèse faite sur ces dernières, en changeant dans z_1, par exemple x_a en θx_a, θx_a se change en $\theta^2 x_a$, $\theta^2 x_a$ en $\theta^3 x_a$, et ainsi de suite. En sorte que ce seul changement de x_a en θx_a suffit pour amener une permutation circulaire. Donc ce changement rend z_1 invariable; et comme il peut s'appliquer à toute autre racine que x_a, il s'ensuit que le changement d'une des racines de la proposée en toute autre entraîne celui de toutes les autres, amène une permutation circulaire de la première considérée, et par suite rend z_1 invariable. Donc la fonction z_1 est invariable pour tous les changements possibles des n racines de l'équation proposée. Elle peut donc être exprimée en fonction rationnelle des coefficients de cette équation. Et pour avoir la valeur v_1 de z_1, il suffit d'exprimer, à l'aide de la fonction rationnelle θ, z_1 en fonction de l'une des racines, x_a par exemple,

$$z_1 = \psi(x_a);$$

et de remarquer que le raisonnement qui précède produisant la suite d'égalités

$$\psi(x_a) = \psi(\theta x_a) = \psi(\theta^2 x_a) = \ldots = \psi(\theta^{n-1} x_a),$$

l'on aura l'équation

$$n\psi(x_a) = \psi(x_a) + \psi(\theta x_a) + \psi(\theta^2 x_a) + \ldots + \psi(\theta^{n-1} x_a),$$

dont le second membre est une fonction symétrique des racines de l'équation proposée.

Or, si l'on considère toute autre racine de l'équation (6), z_2 par exemple, qui se déduit de z_1

$$z_1 = (x_a + \alpha\theta x_a + \alpha^2\theta^2 x_a + \ldots + \alpha^{n-1}\theta^{n-1} x_a)^n,$$

en prenant les racines x de deux en deux à partir de la première, on aura

$$z_2 = (x_a + \alpha\theta^2 x_a + \alpha^2\theta^4 x_a + \alpha^3\theta^6 x_a + \ldots)^n,$$

expression qui revient à celle de la première en y remplaçant α par α^2 qui est une racine de $x^n - 1 = 0$ différente de α. Il en est de même

de z_3, z_4,..., z_{n-1}; donc les racines z_2, z_3,..., z_{n-1} de l'équation (6) ne sont autre chose que les valeurs de z_1 quand on y remplace α successivement par l'une des $n-2$ autres racines imaginaires de $x^n-1=0$. On obtiendra donc, comme pour z_1, chacune de ces racines en fonction rationnelle des coefficients de l'équation proposée : soient $v_2, v_3,\ldots,$ v_{n-1} leurs valeurs respectives.

En extrayant la racine $n^{ième}$ de chacune de ces $n-1$ racines v_1, $v_2,\ldots, v_{n-1}$, et en réunissant aux $n-1$ équations qu'on en déduit celle qui donne la somme des racines de l'équation proposée (1), on aura les n équations suivantes, en désignant par $\alpha_1, \alpha_2,\ldots, \alpha_{n-1}$ les $n-1$ racines imaginaires de $x^n-1=0$,

$$(18)\quad \left\{\begin{array}{l} x_a+\theta x_a+\theta^2 x_a+\ldots+\theta^{n-1}x_a=-A_1,\\ x_a+\alpha_1\theta x_a+\alpha_1^2\theta^2 x_a+\ldots+\alpha_1^{n-1}\theta^{n-1}x_a=\sqrt[n]{v_1},\\ x_a+\alpha_2\theta x_a+\alpha_2^2\theta^2 x_a+\ldots+\alpha_2^{n-1}\theta^{n-1}x_a=\sqrt[n]{v_2},\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\ x_a+\alpha_{n-1}\theta x_a+\alpha_{n-1}^2\theta^2 x_a+\ldots+\alpha_{n-1}^{n-1}\theta^{n-1}x_a=\sqrt[n]{v_{n-1}}; \end{array}\right.$$

équations qui, étant linéaires par rapport aux n racines à trouver, suffiront pour déterminer facilement ces racines. Pour avoir l'une d'elles, $\theta^i x_a$ par exemple, il suffit de multiplier respectivement les deux membres de chacune de ces équations par 1, α_1^{-i}, $\alpha_2^{-i},\ldots, \alpha_{n-1}^{-i}$, et d'ajouter les produits; car cette somme donne, en ayant égard aux propriétés des racines des équations binômes, la formule

$$\theta^i x_a=\frac{1}{n}\left(-A_1+\alpha_1^{-i}\sqrt[n]{v_1}+\alpha_2^{-i}\sqrt[n]{v_2}+\ldots+\alpha_{n-1}^{-i}\sqrt[n]{v_{n-1}}\right),$$

de laquelle on déduira évidemment les n racines de la proposée en remplaçant successivement i par $0, 1, 2,\ldots, n-1$.

A la vérité, un radical d'indice n ayant n valeurs, on pourrait croire que l'expression précédente donnât n^{n-1} valeurs distinctes. Il n'en est rien, car les fonctions des racines équivalentes respectivement à $\sqrt[n]{v_1}$, $\sqrt[n]{v_2},\ldots, \sqrt[n]{v_{n-1}}$ étant des fonctions semblables, l'une d'elles étant donnée, chacune des autres peut être exprimée par une fonction ra-

tionnelle de celle-là, comme le prouve la théorie bien connue des fonctions semblables; le calcul pouvant être abrégé par des considérations dues à Abel et qu'il est inutile de rapporter ici. Cette réduction faite, l'expression précédente n'aura alors que n valeurs distinctes qui sont les n racines de la proposée.

Ainsi la condition relative au premier cas, qui déjà est nécessaire, est de plus suffisante.

Remarque. — Il est utile de remarquer que, quoique le degré n de l'équation proposée (1) ne fût pas un nombre premier, si cependant ses racines étaient représentées par la suite (17); cette équation, appelée encore abélienne, serait résoluble algébriquement, puisque rien ne suppose, dans la résolution qui précède, que n soit un nombre premier.

2° Si la condition relative au second cas est satisfaite, c'est-à-dire si la relation (14) est vraie, je dis que cette condition, qui est nécessaire, est de plus suffisante.

Cette relation montre en effet comment, deux racines quelconques x_a et x_{a+p} étant données, on peut exprimer de proche en proche les $n-2$ autres; et comment elles naissent les unes des autres. Car cette relation étant vraie, par hypothèse, quand on y remplace p successivement par $p\rho, p\rho^2, \ldots, p\rho^{n-2}$, l'on a

$$\begin{aligned} x_{a+p\rho^2} &= \theta(x_{a+p\rho}, x_a), \\ x_{a+p\rho^3} &= \theta(x_{a+p\rho^2}, x_a), \\ &\cdots\cdots\cdots, \\ x_{a+p\rho^{n-2}} &= \theta(x_{a+p\rho^{n-3}}, x_a). \end{aligned}$$

Donc, toute fonction rationnelle connue des n racines de l'équation proposée peut se réduire, à l'aide de la fonction θ, à une fonction rationnelle de deux quelconques de ses racines, x_a et x_{a+p}.

Cela posé : je dis que l'équation (6), d'où dépend nécessairement la résolution de l'équation proposée, est abélienne et que, par suite, elle est résoluble algébriquement. Car ses racines sont, dans le cas présent, les valeurs de $z_1, z_2, \ldots, z_{n-1}$ données par les formules (15) et (16).

Or, si l'on considère, avec M. Hermite, la fonction

$$u = [\psi(x_{a+p}, x_a) + \lambda\psi(x_{a+p\rho}, x_a) + \ldots + \lambda^{n-2}\psi(x_{a+p\rho^{n-2}}, x_a)]^{n-1},$$

dans laquelle λ désigne une des racines imaginaires de l'équation binôme $x^{n-1} - 1 = 0$; et si l'on y change successivement p en $p\rho, p\rho^2, \ldots, p\rho^{n-2}$, ou, ce qui est la même chose, si l'on donne à p les valeurs $1, 2, \ldots, n-1$, les divers termes du polynôme soumis à l'exposant $n-1$ ne font que se déplacer circulairement. Donc cette fonction u est invariable pour toutes ces $n-1$ valeurs de p. D'ailleurs chacun des termes de ce même polynôme, et par suite u, est encore invariable pour les n permutations circulaires que produit la permutation relative à ce terme; et, d'après la signification de chacun d'eux, l'on obtient évidemment ces n permutations en donnant à a successivement les n valeurs $0, 1, 2, \ldots, n-1$. De là il suit que si l'on réduit la fonction u à ne contenir que les deux racines x_a, x_{a+p},

$$u = \chi(x_{a+p}, x_a),$$

cette fonction rationnelle χ conservera la même valeur, quels que soient les indices de a et de p, et que par suite l'on aura

$$n(n-1)u = \sum_{0}^{n-1}\sum_{1}^{n-1}\chi(x_{a+p}, x_a),$$

relation dont le second membre est une fonction symétrique des racines de l'équation proposée $F(x) = 0$. On peut donc exprimer u en fonction rationnelle des coefficients de cette équation. Il en serait de même, si dans u on remplaçait λ par toute autre racine imaginaire de la même équation $x^{n-1} - 1 = 0$, $\lambda_2, \lambda_3, \ldots, \lambda_{n-2}$. Mais on démontrerait de la même manière que la somme

$$\psi(x_{a+p}, x_a) + \psi(x_{a+p\rho}, x_a) + \ldots + \psi(x_{a+p\rho^{n-2}}, x_a),$$

c'est-à-dire la racine unique y de l'équation résolvante (7), réduite à ne contenir que les deux mêmes racines x_a et x_{a+p}, est symétrique des racines de l'équation proposée; et dès lors qu'elle est exprimable en fonction rationnelle de ses coefficients. Donc, on aura les $n-1$ équa-

tions dont les seconds membres sont connus,

$$\psi(x_{a+p}, x_a) + \psi(x_{a+p\rho}, x_a) + \ldots + \psi(x_{a+p\rho^{n-2}}, x_a) = -\mathrm{D},$$
$$\psi(x_{a+p}, x_a) + \lambda_1 \psi(x_{a+p\rho}, x_a) + \ldots + \lambda_1^{n-2} \psi(x_{a+p\rho^{n-2}}, x_a) = \sqrt[n-1]{u_1},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$
$$\psi(x_{a+p}, x_a) + \lambda_{n-2} \psi(x_{a+p\rho}, x_a) + \ldots + \lambda_{n-2}^{n-2} \psi(x_{a+p\rho^{n-2}}, x_a) = \sqrt[n-1]{u_{n-2}}.$$

Ces $n-1$ équations, en tout semblables aux équations (18), prouvent effectivement que l'équation (6) est abélienne. De ces $n-1$ équations, on déduira donc les $n-1$ termes, $z_1, z_2, \ldots, z_{n-1}$ qui entrent dans u.

Or, ces $n-1$ termes étant connus, on aura, en ayant égard à leurs expressions (4) en fonction des racines de la proposée, $n-1$ équations, qui, réunies à l'équation connue

$$x_a + x_{a+p} + x_{a+2p} + \ldots + x_{a+(n-1)p} = -\mathrm{A}_1,$$

feront connaître les n racines cherchées, puisque ces n équations simultanées ne sont autres que les équations (8). Ainsi cette relation (14), qui déjà est nécessaire, est de plus suffisante.

Il résulte donc de tout ce qui précède que, *les seules équations algébriques, irréductibles et de degré premier supérieur à* 3 *qui soient résolubles algébriquement, sont celles qui sont abéliennes ou celles dont les racines satisfont à l'équation* (14).

Corollaire I. — Si l'on divise le premier membre $\mathrm{F}(x)$ de toute équation irréductible, de degré premier, non abélienne et résoluble algébriquement, par un de ses facteurs linéaires, le quotient égalé à zéro est une équation abélienne.

Car, l'équation $\mathrm{F}(x) = 0$ étant résoluble algébriquement, de degré premier, irréductible et non abélienne, la relation (14) est satisfaite; le quotient de $\mathrm{F}(x)$ par $x - x_a$ égalé à zéro, a pour racines x_{a+p}, $x_{a+p\rho}, \ldots, x_{a+p\rho^{n-2}}$: et l'on déduit de cette relation les équations

$$x_{a+p\rho} = \theta(x_{a+p}, x_a) = \theta x_{a+p},$$
$$x_{a+p\rho^2} = \theta x_{a+p\rho} = \theta^2 x_{a+p},$$
$$\cdots\cdots\cdots\cdots,$$
$$x_{a+p\rho^{n-2}} = \theta x_{a+p\rho^{n-3}} = \theta^{n-2} x_{a+p},$$
$$x_{a+p\rho^{n-1}} = x_{a+p} = \theta x_{a+p\rho^{n-2}} = \theta^{n-1} x_{a+p},$$

qui prouvent qu'effectivement ce quotient égalé à zéro est une équation abélienne.

Ce théorème, qui se présente ici comme corollaire, est dû à M. Hermite.

Corollaire II. — De l'une quelconque des relations précédentes, par exemple de

$$x_{a+p\rho^2} = \theta(x_{a+p\rho}, x_a),$$

on peut déduire l'une quelconque des trois racines qui y entrent en fonction rationnelle des deux autres; puisque l'équation (14) exige que, deux quelconques des racines de $F(x) = 0$ étant données, on puisse déterminer les $n - 2$ autres en fonction rationnelle de ces deux là.

Corollaire III. — Si les coefficients d'une équation algébrique n'ont entre eux aucune relation, sont indéterminés, cette équation est nécessairement irréductible. Le théorème qui vient d'être démontré produit donc cet autre théorème : *Il est impossible de résoudre algébriquement les équations générales de degré premier supérieur au troisième.*

NOTE.

Les permutations, en effet, d'un quelconque des groupes de cette troisième classification sont relatives à un seul et même ordre ou à un seul et même polygone vu successivement de chacun de ses sommets, en sorte que tous ses groupes ne sont autre chose que *tous* les polygones distincts que l'on peut former avec m lettres. Ces polygones se déduisent les uns des autres par un changement de deux lettres quelconques; leur déduction est donc arbitraire.

Donc, si on les assemble de deux en deux ou de trois en trois,..., pour former de nouveaux groupes composés de permutations *inséparables;* il n'y a pas de raison pour que, dans ces nouveaux groupes, l'on y mette plutôt tels de ces polygones que tels autres. Il faut donc, ou les laisser séparés comme dans cette troisième classification, ou les

réunir tous en un seul groupe, auquel cas il n'y a pas à proprement parler de classification, puisque ce groupe unique contient la totalité des permutations de ces m lettres.

Donc les groupes de cette troisième classification ne peuvent pas être partagés en nouveaux groupes de permutations inséparables pour tous les échanges des lettres qui les forment.

Remarque. — Si le nombre de lettres est égal à 3, le nombre de groupes de cette classification est égal à l'unité : pour tout autre nombre de lettres, le nombre de groupes est supérieur à l'unité, et même à ce nombre de lettres.