Title: Mémoire sur les équations résolubles algébriquement

Author: M. Despeyrous

Release Date: July 24, 2008 [EBook #26118]

Language: French

Character set encoding: ISO-8859-1

MÉMOIRE

SUR

LES ÉQUATIONS

RÉSOLUBLES ALGÉBRIQUEMENT

PAR

M. DESPEYROUS

Ancien professeur à la Faculté des sciences de Toulouse.

Paris, 1887

Transcriber's notes

This e-text was created from scans of the book published at Paris in 1887 by A. Hermann as part of the *Librairie Scientifique* series. The book was printed by G. Gounouilhou of Bordeaux.

The author's footnotes are labelled numerically([1]) and are in French; footnotes showing where corrections to the text have been made are labelled using printer's marks* and are in English.

The author uses a vinculum $\overline{n-1}p$ where modern usage would be to use parentheses $(n-1)p$.

Details of minor typographical corrections are documented in the LaTeX source.

This document is designed for two-sided printing. It can be recompiled for on-screen viewing: see comments in source LaTeX code.

MÉMOIRE SUR LES ÉQUATIONS RÉSOLUBLES ALGÉBRIQUEMENT

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.

La résolution des équations des quatre premiers degrés était connue depuis longtemps, lorsque Vandermonde et Lagrange lurent presque en même temps, l'un à l'Académie des Sciences de Paris(1), l'autre à l'Académie des Sciences de Berlin(2), leurs savantes recherches sur la résolution générale des équations. Par des méthodes différentes, ces deux grands géomètres arrivèrent à des résultats identiques ; et, en particulier à celui-ci : «*La résolution de l'équation générale du cinquième degré dépend en dernière analyse d'une équation du sixième degré* ; et la résolution de celle-ci d'une équation du quinzième ou du dixième degré.» Mais est-ce là le dernier degré de réduction auquel on puisse parvenir ?

On en était là lorsque le célèbre Gauss publia en 1801 ses *Disquisitiones arithmeticae*, qui contiennent dans la septième section la résolution algébrique des équations binômes.

Vingt-cinq ans plus tard l'illustre Abel s'occupa à son tour de la résolution algébrique des équations, comme le prouve la lettre qu'il écrivait, trois ans avant sa mort, à M. Holmboe : «Depuis mon arrivée à Berlin, je me suis occupé de la solution du problème général suivant : *trouver toutes les équations qui sont résolubles algébriquement* ; ma solution n'est pas encore complète, mais autant que j'en puis juger, elle aboutira. Tant que le degré de l'équation est un nombre premier, la difficulté n'est pas très grande, mais lorsque ce nombre est composé, le diable s'en mêle(3).»

Nous devons ajouter qu'il ne réussit même pas lorsque le degré est premier, mais qu'il trouva, en généralisant les résultats de Gauss sur les équations binômes, une classe d'équations résolubles algébriquement, appelées aujourd'hui *abéliennes*, et qu'il démontra l'impossibilité de résoudre algébriquement des équations générales de degré supérieur au quatrième(4).

(1) *Mémoires de l'Académie des Sciences de Paris*, année 1771.
(2) *Mémoires de l'Académie des Sciences de Berlin*, années 1770–71.
(3) *Oeuvres complètes d'Abel*, 2e vol., p. 265.
(4) *Id.*, p. 5 et 114 du premier volume.

Enfin M. Liouville a publié en 1846, dans son journal, les oeuvres mathématiques de Gallois, dont la mort prématurée a été une véritable perte pour la science. Dans ces oeuvres, se trouve la démonstration de ce beau théorème : «Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il faut et il suffit que toutes les racines soient des fonctions rationnelles de deux quelconques d'entre elles.» Mais la démonstration laisse beaucoup à désirer, elle a des lacunes, et il a fallu toute l'autorité de M. Liouville pour faire admettre l'existence du théorème. Nous avons encore de Gallois un *fragment* sur les conditions de résolubilité des équations de degré composé ; mais il est inintelligible, à l'exception des trois premières pages.

Les remarquables travaux dont nous venons de parler nous ont fait hésiter longtemps à nous occuper de la question générale ci-dessus énoncée, mais nos recherches([1]) 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 quels que soient les échanges de ces lettres, fournissent une méthode pour la solution de cette question générale, et c'est le résultat des applications de cette méthode que nous soumettons au jugement des géomètres.

Notre travail est divisé en deux sections : dans la première, après avoir rappelé l'indispensable théorie de Lagrange sur les fonctions semblables et dissemblables, nous exposons les principes de notre théorie sur les équations résolubles par radicaux. Ces principes se composent de six théorèmes dont un seul, le cinquième, était connu et appartient à Gallois.

Le but de ces principes est d'établir : 1° que la résolution de toute équation algébrique, irréductible et soluble par radicaux dépend *nécessairement* de la résolution d'une équation auxiliaire appelée *résolvante*, dont les racines sont des fonctions rationnelles de celles de la proposée ; 2° que cette équation résolvante n'est décomposable en facteurs de degrés moindres, qu'autant que les groupes de permutations des racines de l'équation proposée, relatifs à celles de l'équation résolvante, peuvent être partagés en nouveaux groupes de permutations *inséparables*.

Ces deux théorèmes contiennent en germe la méthode qu'on doit suivre pour la détermination des conditions nécessaires et suffisantes pour qu'une équation algébrique et irréductible soit soluble par radicaux.

Dans la deuxième section, nous développons cette méthode, et nous démontrons que les deux théorèmes de Lagrange, sur la théorie générale des équations, sont des conséquences nécessaires de la théorie des équations, vérité([2]) aperçue par ce grand géomètre, et que nous mettons, ce nous semble, hors de doute.

Ainsi nous démontrons : 1° que pour résoudre une équation algébrique irréductible et de degré premier n, il est nécessaire et suffisant de résoudre deux équations, l'une de degré $n-1$ et l'autre de degré $1\cdot 2\cdot 3\cdots(n-2)$; 2° que pour résoudre une équation algébrique irréductible et de degré composé $m = nq$ (n étant premier) il est nécessaire et suffisant de résoudre n équations de degré q et deux autres équations, l'une de degré $n-1$ et l'autre de degré γ donné par la formule

$$\gamma = \frac{1\cdot 2\cdot 3\cdots m}{(1\cdot 2\cdot 3\cdots q)^n\cdot n(n-1)}\,.$$

([1]) *Journal de Mathématiques pures et appliquées*, deuxième série, t. VI, p. 417 ; t. X, p. 55 et 177.
([2]) *Traité de la résolution des équations numériques*, 2e éd., p. 274.

De là, et de notre théorème de la classification des permutations(1) nous déduisons d'une manière *directe, qu'il est impossible de résoudre algébriquement les équations générales de degré supérieur au quatrième.* Ce théorème, dû à Abel, comme nous l'avons déjà dit, a été démontré par ce géomètre par la réduction à l'absurde ; plus tard, Wantzel en a donné une démonstration plus simple, mais ayant le même caractère. Notre démonstration est directe et elle est déduite de la nature même des choses, aussi est-elle simple et facile.

Puisqu'il est impossible de résoudre algébriquement les équations générales de degré supérieur au quatrième, on doit chercher les conditions nécessaires et suffisantes pour qu'une équation irréductible, de degré supérieur à quatre, soit résoluble algébriquement, c'est-à-dire soluble par radicaux.

Notre théorie de la classification des permutations nous fait d'abord retrouver une classe d'équations résolubles algébriquement, c'est celle des équations dites *abéliennes*, et la décomposition de ces équations en d'autres, de degrés moindres, selon la loi de Gauss. Puis nous distinguons dans cette recherche deux cas, celui où le degré est un nombre premier, et celui où il est composé. Dans le premier cas nous démontrons ce théorème : *Pour qu'une équation irréductible et de degré premier soit soluble par radicaux, il faut et il suffit que, deux racines étant données, les autres s'en déduisent rationnellement suivant une loi que nous faisons connaître.*

Ce théorème, tel que Gallois l'avait énoncé, ne faisait pas connaître cette loi de dérivation des racines ; c'est peut-être pour cette raison que la démonstration de ce géomètre laissait beaucoup à désirer : nous espérons que la nôtre sera à l'abri de ce reproche.

Ensuite, nous donnons, théorème XIV, les conditions nécessaires et suffisantes pour qu'une équation algébrique irréductible et dont le degré ne contient aucun des facteurs premiers deux et trois soit résoluble algébriquement.

Enfin nous examinons les cas particuliers qui ne sont pas compris dans ce dernier théorème, et pour chacun d'eux nous donnons les conditions nécessaires et suffisantes pour qu'une équation irréductible soit soluble par radicaux. C'est ainsi que nous complétons la solution de ce problème général : *trouver toutes les équations résolubles algébriquement.*

---

(1) *Journal de Mathématiques*, 2e série, t. VI, p. 417.

I

PRINCIPES

Définitions.—Soient $x_0, x_1, x_2, \dots, x_{m-1}$, m quantités, et V une fonction de ces quantités, cette fonction étant 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 de puissances, et trois inverses, soustraction, division, extraction de racines.

Si, dans la formation de la fonction V, il n'y a que des signes des quatre premières opérations ou de quelques-unes d'entre elles, V est dite fonction entière de $x_0, x_1, x_2, \dots, x_{m-1}$; 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 $x_0, x_1, x_2, \dots, x_{m-1}$, 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

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

est *réductible* ou *irréductible*, selon que le 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 $A_1, A_2, \dots, A_m$ *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 $A_1, A_2, \dots, A_m$ de cette équation des racines de certaines équations que nous appellerons *résolvantes.*

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

Fonctions semblables(¹)

Considérons une fonction rationnelle V des m racines de l'équation (1) de forme déterminée et connue, et admettons qu'elle prenne s valeurs quand on y permute de toutes les manières possibles ces m racines que son expression renferme.

Nous avons démontré ailleurs(²), qu'on peut partager les $1 \cdot 2 \cdot 3 \cdots m = \mu$ permutations, produites par les m racines 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. Admettons que ce partage soit effectué, et soit

$$\text{(A)} \qquad \begin{cases} \alpha_1, & \beta_1, & \ldots, & \omega_1 \\ \alpha_2, & \beta_2, & \ldots, & \omega_2 \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_s, & \beta_s, & \ldots, & \omega_s \end{cases}$$

le tableau des permutations qui en résulte, le nombre des lettres $\alpha, \beta, \ldots, \omega$ étant égal à q.

Soient V_1 la valeur que prend la fonction donnée V pour toutes les permutations $\alpha_1, \beta_1, \ldots, \omega_1$ du premier groupe et $V_2, V_3, \ldots, V_s$ les valeurs qu'elle prend respectivement pour les permutations des 2ᵉ, 3ᵉ, …, sᵉ groupes.

Cela rappelé, considérons une autre fonction rationnelle y de ces mêmes racines ; cette fonction y est *semblable* à V si elle est invariable pour toutes les permutations d'un quelconque des groupes du tableau (A), et si elle change de valeur en passant d'un groupe à un autre : en sorte que V et y ont un même nombre s de valeurs distinctes. Pour toute autre hypothèse V et y sont des fonctions *dissemblables*.

La question à résoudre est celle-ci : connaissant V et les coefficients de l'équation (1), trouver l'inconnue y. Nous devons distinguer deux cas dans la solution de ce problème, celui où les fonctions V et y sont semblables, et celui où elles sont dissemblables.

Premier Cas.—Les fonctions V et y sont semblables. Puisque la forme de la fonction rationnelle V est connue, nous connaissons les valeurs analytiques $V_1, V_2, \ldots, V_s$. Considérons actuellement une fonction rationnelle quelconque et symétrique de ces s valeurs,

$$\theta(V_1, V_2, \ldots, V_s)\,.$$

Tout changement opéré sur les m racines $x_0, x_1, \ldots, x_{m-1}$ laissera une quelconque de ces s valeurs, V_i par exemple invariable, ou il la transformera en une autre de ces m valeurs. Dans l'une ou l'autre de ces deux hypothèses, ce même changement produira les mêmes effets, sur les autres valeurs de V, d'après les propriétés connues du tableau A. Mais la fonction θ est symétrique par rapport à ces s valeurs, donc elle est symétrique par rapport aux racines de l'équation (1), et par conséquent elle est exprimable en fonction rationnelle des coefficients de cette équation. On doit donc

(¹) Voir les *Mémoires de Berlin* pour l'année 1771, p. 192, et aussi *l'Algèbre supérieure* de Serret, 2ᵉ éd., p. 149.
(²) *Journal de Mathématiques de Liouville*, février 1865.

considérer comme connues : 1° la somme des valeurs $V_1, V_2, \dots, V_s$; 2° la somme de leurs produits deux à deux ; 3° la somme de leurs produits trois à trois ; et ainsi de suite, et par conséquent l'équation :

$$\varphi(V) = V^s + P_1 V^{s-1} + P_2 V^{s-2} + \dots + P_s = 0\,, \tag{2}$$

dont les racines sont ces s valeurs $V_1, V_2, \dots, V_s$. Considérons actuellement la fonction rationnelle yV^k, k désignant un nombre entier quelconque ; et désignons par $y_1, y_2, \dots, y_s$ les valeurs que prend respectivement y pour une quelconque des permutations des s groupes du tableau (A). Il résulte de ce qui précède que toute fonction symétrique des s valeurs $y_1V_1^k, y_2V_2^k, \dots, y_sV_s^k$ est invariable par rapport aux m racines de l'équation (1), et par conséquent exprimable en fonction rationnelle de ses coefficients. On doit donc considérer comme connue la fonction définie par l'équation

$$y_1V_1^k + y_2V_2^k + \dots + y_sV_s^k = t^k$$

quelle que soit la valeur entière attribuée à k ; et par conséquent les fonctions $t_0, t_1, \dots, t_{s-1}$ définies par les équations

$$\begin{array}{ccccccc}
y_1 & + & y_2 & + \dots + & y_s & = t_0\,, \\
y_1V_1 & + & y_2V_2 & + \dots + & y_sV_s & = t_1\,, \\
\multicolumn{6}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\
\multicolumn{6}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\
y_1V_1^{s-1} & + & y_2V_2^{s-1} & + \dots + & y_sV_s^{s-1} & = t_{s-1}\,,
\end{array}$$

qui se déduisent de la première en donnant successivement à k les valeurs $0, 1, 2, \dots, s-1$; ces équations serviront à déterminer $y_1, y_2, \dots, y_s$. Pour déterminer l'une des inconnues, y_i par exemple, nous suivrons la méthode des multiplicateurs ; nous multiplierons donc respectivement les deux membres de chacune de ces s équations par $h_0, h_1, \dots, h_{s-2}, 1$; nous ferons la somme des produits membre à membre, et nous aurons, en faisant pour abréger

$$h_0 + h_1V + h_2V^2 + \dots + h_{s-2}V^{s-2} + V^{s-1} = \psi(V)\,,$$
$$y_1\psi(V_1) + \dots + y_i\psi(V_i) + \dots + y_s\psi(V_s) = h_0t_0 + h_1t_1 + \dots + h_{s-2}t_{s-2} + t_{s-1}\,.^*$$

Pour déduire de cette dernière équation la valeur de y_i, il faut déterminer les $s-1$ coefficients indéterminés $h_0, h_1, \dots, h_{s-2}$, par les $s-1$ équations :

$$\psi(V_1) = 0, \quad \psi(V_2) = 0, \quad \dots, \quad \psi(V_0) = 0\,; \tag{3}$$

et ces indéterminées étant connues par ces équations, on aura

$$y_i = \frac{h_0t_0 + h_1t_1 + \dots + h_{s-2}t_{s-2} + t_{s-1}}{\psi(V_i)}\,. \tag{4}$$

Pour déterminer ces $s-1$ indéterminées et par suite y_i, il suffit de résoudre les équations (3) ; mais on peut opérer plus simplement, car ces équations (3) prouvent

* Original has t_{s-i} as the final term

que les $s-1$ racines de l'équation $\psi(V)=0$ sont $V_1, V_2, \dots, V_s$, c'est-à-dire toutes celles de l'équation (2), la racine V_i exceptée ; donc

$$\psi(V)\ ^{*} = \frac{\varphi(V)}{V-V_i} = V^{s-1} + \begin{array}{l|l|l} V_i & V^{s-2} + V_i^2 & V^{s-3} \dots + V_i^{s-1}, \\ + P_1\ ^{\dagger} & \quad + P_1 V_i & \qquad + P_1 V_i^{s-2}, \\ & \quad + P_2 & \qquad + P_2 V^{s-3}, \\ & & \qquad \dots\dots \\ & & \qquad + P_{s-1}; \end{array}$$

et puisque ce quotient doit être identique au polynôme $\psi(V)$, on doit avoir

$$h_{s-2} = V_i + P_1, \quad h_{s-3} = V_i^2 + P_1 V_i + P_2, \quad \dots,$$
$$h_0 = V_i^{s-1} + P_1 V_i^{s-2} + \dots + P_{s-1}.$$

Ces valeurs font connaître celle de y_i ; mais le numérateur de son expression (4) peut être simplifié par le calcul suivant dû à Lagrange. Posons en effet

$$\begin{aligned} T_0 &= t_0, \\ T_1 &= t_1 + t_0 P_1, \\ T_2 &= t_2 + t_1 P_1 + t_0 P_2, \\ &\dots\dots\dots\dots \\ T_{s-1} &= t_{s-1} + t_{s-2} P_1 + t_{s-3} P_2 + \dots + t_0 P_{s-1}, \end{aligned}$$

et multiplions les deux membres de chacune de ces s équations respectivement par $V_i^{s-1}, V_i^{s-2}, \dots, V_i, 1$; nous aurons, en faisant la somme des produits membre à membre, et en ayant égard aux valeurs de $h_0, h_1, \dots, h_{s-2}$,

$$\begin{aligned} &T_0 V_i^{s-1} + T_1 V_i^{s-2} + \dots + T_{s-2} V_i + T_{s-1} \\ &\qquad = h_0 t_0 + h_1 t_1 + \dots + h_{s-2} t_{s-2} + t_{s-1} = \Theta(V_i); \end{aligned}$$

et, par suite, la formule (4) deviendra

$$y_i = \frac{\Theta(V_i)}{\psi(V_i)},$$

les coefficients des diverses puissances de V_i, dans le numérateur, étant des fonctions rationnelles des coefficients de l'équation (1). Or, l'équation $\psi(V) = \dfrac{\varphi(V)}{V-V_i}$ donne $\psi(V_i) = \varphi'(V_i)$, donc enfin

$$y_i = \frac{\Theta(V_i)}{\varphi'(V_i)}, \tag{5}$$

formule qui donnera les valeurs $y_1, y_2, \dots, y_s$ en remplaçant i par les nombres $1, 2, 3, \dots, s$.

* Original lacks ψ

† Original has P_i

Ainsi ces valeurs s'expriment en fonction rationnelle de $V_1, V_2, \ldots, V_s$.

Sous le point de vue analytique, les valeurs $V_1, V_2, \ldots, V_s$ sont inégales ; mais pour des valeurs particulières des racines $x_0, x_1, \ldots, x_{m-1}$ et pour des formes particulières de la fonction V, quelques-unes de ces valeurs peuvent être égales entre elles, $V_1 = V_2$ par exemple ; auquel cas $\varphi'(V_1) = 0$. Cette hypothèse rend illusoire la formule (5) pour les valeurs y_1 et y_2 relatives à V_1 et à V_2 ; mais on peut, en suivant une méthode connue, déterminer la somme $y_1 + y_2$.

Modifions, en effet, les coefficients de l'équation (2) de telle manière que les racines V_1 et V_2 aient une différence ε et que les autres conservent les mêmes valeurs ; nous avons

$$\begin{gathered} V_2 = V_1 + \varepsilon\,, \\ \varphi(V) = (V - V_1)(V - V_2)(V - V_3)\cdots(V - V_s)\,. \end{gathered}$$

De cette dernière équation nous déduisons

$$\begin{aligned} \varphi'(V_1) &= (V_1 - V_2)(V_1 - V_3)\cdots(V_1 - V_s)\,, \\ \varphi'(V_2) &= (V_2 - V_1)(V_2 - V_3)\cdots(V_2 - V_s)\,; \end{aligned}$$

et si on pose

$$\frac{\Theta(V)}{(V - V_3)\cdots(V - V_s)} = F_1(V)\,,$$

on aura successivement, à la limite $\varepsilon = 0$, c'est-à-dire en rétablissant les valeurs des coefficients de l'équation (2),

$$\begin{aligned} y_1 &= \lim \frac{F_1(V_1)}{V_1 - V_2} = -\lim \frac{F_1(V_1)}{\varepsilon}\,, \\ y_2 &= \lim \frac{F_1(V_2)}{(V_2 - V_1)} = \lim \frac{F_1(V_1 + \varepsilon)}{\varepsilon}\,, \\ y_1 + y_2 &= \lim \frac{F_1(V_1 + \varepsilon) - F_1(V_1)}{\varepsilon} = F_1'(V_1)\,. \end{aligned}$$

On connaît donc la somme $y_1 + y_2$; mais, si on prend pour inconnue y^2, on obtiendrait par un calcul analogue $y_1^2 + y_2^2$. De ces deux sommes, on déduira l'équation du second degré dont les racines sont y_1 et y_2.

Si $V_1 = V_2 = V_3$, la formule (5) devient illusoire pour y_1, y_2, y_3 ; mais elle peut faire connaître la somme $y_1 + y_2 + y_3$ par la même méthode. Modifions, en effet, les coefficients de l'équation (2) de telle manière que V_1 soit racine double, que $V_3 = V_1 + \varepsilon$ et que les autres restent les mêmes ; et posons

$$\frac{\Theta(V)}{(V - V_4)(V - V_5)\cdots(V - V_s)} = F_2(V)\,.$$

Nous aurons

$$\begin{aligned} \varphi'(V_3) &= (V_3 - V_1)^2(V_3 - V_4)\cdots(V_3 - V_s)\,, \\ F_1(V) &= \frac{F_2(V)}{V - V_3}\,, \\ F_1'(V) &= \frac{(V - V_3)F_2'(V) - F_2(V)}{(V - V_3)^2}\,; \end{aligned}$$

et à la limite, c'est-à-dire en rétablissant les valeurs des coefficients de l'équation (2), nous obtiendrons

$$y_3 = \lim \frac{F_2(V_1+\varepsilon)}{\varepsilon^2},$$
$$y_1+y_2+y_3 = \lim \frac{-\varepsilon F_2'(V_1) - F_2(V_1) + F_2(V_1+\varepsilon)}{\varepsilon^2} = \frac{1}{1\cdot 2} F_2''(V_1).$$

En prenant pour inconnue d'abord y^2, puis y^3, on trouverait par un calcul analogue $y_1^2+y_2^2+y_3^2$ et $y_1^3+y_2^3+y_3^3$; et, par suite, l'équation du 3e degré dont les racines seraient y_1, y_2, y_3.

Généralement, si V_1 était une racine multiple du degré i de multiplicité, on poserait

$$\frac{\Theta(V)}{(V-V_{i+1})\cdots(V-V_s)} = F_{i-1}(V),$$

et on trouverait la formule

$$y_1+y_2+\cdots+y_i = \frac{1}{1\cdot 2\cdot 3\cdots(i-1)} F_{i-1}^{i-1}(V),$$

qu'on démontrerait être vraie par la voie bien connue de la démonstration de proche en proche. Et en prenant successivement pour inconnues $y^2, y^3, \ldots, y^i$, on connaîtrait $y_1^2+y_2^2+\cdots+y_i^2, \ldots, y_1^i+y_2^i+\cdots+y_i^i$, et par suite l'équation dont les racines seraient $y_1, y_2, \ldots, y_i$. Cette généralité n'étant pas nécessaire à notre objet, nous en supprimons la démonstration.

Ce résultat pouvait d'ailleurs être prévu ; car, à une même valeur V_1 de V correspondent par hypothèse i valeurs de y, donc chacune d'elles doit dépendre de la même manière de V_i. Ces i valeurs doivent donc être racines d'une même équation de degré i.

Ainsi, les fonctions V et y des racines de l'équation (1) étant rationnelles et semblables, on peut généralement avoir la valeur de y par une expression rationnelle de V et des coefficients de cette équation. Dans le cas où la fonction connue V est racine multiple du degré i de multiplicité de l'équation (2), y dépend d'une équation de ce degré dont les coefficients sont des fonctions rationnelles de V et des coefficients de l'équation (1).

Deuxième Cas.—Les fonctions V et y sont *dissemblables*. Nous continuerons de désigner les s valeurs distinctes de V par $V_1, V_2, \ldots, V_s$, et nous désignerons celles de y par $y_1, y_2, \ldots, y_l$, l étant différent de s.

Si s est égal au nombre total μ de permutations que produisent les m racines dont V et y sont fonctions, quelle que soit la valeur l, qui du reste ne peut être qu'un diviseur de μ, la méthode précédente s'applique sans modification à la détermination de chaque valeur de y. En sorte que, dans cette hypothèse, la formule générale (5) donnera les diverses valeurs de y, chacune d'elles répétée un même nombre de fois k, si $\mu = lk$.

Si s diffère de μ, s sera aussi un diviseur de μ ; et dans cette deuxième hypothèse, soient $y_1, y_2, \ldots, y_q$ les valeurs de y relatives aux q permutations du premier groupe du tableau (A), qui font acquérir à V une même valeur V_1 ; $y_{1+q}, y_{2+q}, \ldots, y_{2q}$ celles qui sont relatives aux permutations du second groupe et qui donnent une même valeur V_2 à V ; et ainsi de suite, chaque valeur de y étant répétée un certain nombre de fois k.

Il est clair que si on prend une fonction z rationnelle et symétrique de $y_1, y_2, \ldots, y_q$, les fonctions V et z seront semblables, ou du moins telles qu'on pourra appliquer à z la formule (5). On pourra donc généralement exprimer respectivement $z_1, z_2, \ldots, z_s$ en fonction rationnelle de $V_1, V_2, \ldots, V_s$ et des coefficients de l'équation (1), par cette formule générale (5). Et en prenant successivement pour z la somme des produits deux à deux de ces valeurs $y_1, y_2, \ldots, y_q$; la somme des produits trois à trois de ces mêmes valeurs, et ainsi de suite ; on déterminera, de la même manière, chacune de ces sommes relatives à $V_1, V_2, \ldots, V_s$; et, avec les valeurs de ces sommes, on aura l'équation en y du degré q dont les racines seront $y_1, y_2, \ldots, y_q$. Par un calcul analogue on aurait les équations dont les racines seraient $y_{1+q}, y_{2+q}, \ldots, y_{2q}$, ainsi que les équations relatives aux autres groupes.

Corollaire I.—Il résulte de ce qui précède que, si la fonction connue V prenait μ valeurs distinctes, chacune des racines de l'équation (1) pourrait être exprimée en fonction rationnelle d'une de ces valeurs de V et des coefficients de cette équation, car il suffirait de prendre x pour y.

Corollaire II.—Si la fonction rationnelle V avait une même valeur pour toutes les permutations d'une même *classe*, V aurait m valeurs distinctes, et dès lors V et x seraient semblables, et par suite chacune des racines de l'équation (1) s'exprimerait en fonction rationnelle d'une de ces valeurs et des coefficients de cette équation.

Remarque I.—Dans un cas particulier, le degré q de chacune de ces équations, au nombre de s, peut être abaissé. Soit en effet q' le nombre de valeurs distinctes de la fonction y pour les q permutations du premier groupe du tableau (A) ; les permutations de chacun des $s-1$ autres groupes de ce tableau étant assujetties à la même loi de formation que celles du premier, cette fonction y prendra q' valeurs distinctes pour les q permutations de chacun d'eux. Mais il peut arriver que les valeurs de y relatives à quelques-uns de ces s groupes soient égales entre elles ou soient différentes. Dans ce dernier cas, le nombre l de valeurs distinctes de y sera égal à sq' ; et comme $\mu = qs = lk$, on aura $qs = sq'k$, et par suite $q = kq'$. Ainsi, dans le cas particulier que nous examinons, chacune des s équations, de degré q, a q' racines égales du degré de multiplicité k. Donc le premier membre de chacune de ces s équations est une puissance parfaite de l'indice k ; en sorte qu'en extrayant la racine d'indice k de leurs premiers membres, le degré q de chacune d'elles sera abaissé au degré q' ; et la détermination de y sera ramenée à la résolution de ces dernières.

Remarque II.—Il peut arriver, et il y a de nombreux exemples, que l soit égal à s sans que y prenne une même valeur pour les q permutations qui font acquérir à V une même valeur. Dans ce cas nous dirons que V et y sont des fonctions dissemblables : le raisonnement du deuxième cas peut en effet être appliqué à cette hypothèse.

On doit observer toutefois que, si pour les q permutations de chacun des s groupes du tableau (A), y a q' valeurs distinctes, $\frac{s}{q'}$ de ces groupes seulement feront acquérir à cette fonction y des valeurs différentes ; et que par conséquent la remarque précédente ne peut être appliquée à ce cas.

THÉORÈME I.—*La résolution de toute équation algébrique et irréductible dépend de la résolution d'une équation dont les racines sont des fonctions rationnelles de celles de la proposée.*

Soient m le degré de l'équation proposée

$$f(x) = 0 \tag{1*}$$

et $x_0, x_1, \ldots, x_{m-1}{}^{\dagger}$ ses m racines ; supposons d'abord qu'elle soit résoluble algébriquement. Cette équation étant irréductible, chacune de ses racines est assujettie à la même loi de détermination, celle de satisfaire identiquement à cette équation ; tout ce qu'on peut dire de l'une d'elles, *appartient nécessairement* à toute autre. Et comme ces racines sont connues par hypothèse, et exprimées par des fonctions rationnelles faites avec des radicaux et avec les coefficients de l'équation (1), la fonction de ces radicaux qui donne l'une des racines doit donner toutes les autres en prenant successivement toutes les déterminations de ces radicaux. Cette fonction, réduite à sa plus simple expression, doit donc se réduire successivement à $x_0, x_1, \ldots, x_{m-1}$, lorsqu'on y remplace les coefficients de l'équation proposée par les fonctions symétriques des racines qu'ils expriment. Or, il ne peut en être ainsi que parce que chaque radical de cette expression est équivalent à une fonction rationnelle de ces mêmes racines, en donnant à ce mot *rationnel* l'extension dont nous avons parlé dans les définitions.

Ainsi, chaque radical qui entre dans l'expression d'une quelconque des racines est équivalent à une fonction rationnelle de ces racines ; et les valeurs algébriques de ces fonctions sont parfaitement déterminées, puisqu'elles sont équivalentes à ces radicaux connus par hypothèse.

Donc, si on conçoit l'une quelconque de ces fonctions

$$y = F(x_0, x_1, \ldots, x_{m-1}),$$

et l'équation $\varphi(y) = 0$ de degré s dont elle est racine, équation dont on obtient les coefficients en fonction rationnelle de ceux de l'équation (1) par le procédé connu([1]), les racines de cette équation $\varphi(y) = 0$ seront connues.

Ainsi, quand une équation irréductible est soluble par radicaux, la fonction y et l'équation $\varphi(y) = 0$ dont elle dépend existent, et les racines de cette dernière sont parfaitement déterminées. *Réciproquement* : soient

$$y = F(x_0, x_1, \ldots, x_{m-1})$$

([1]) Ce procédé consiste à permuter les m lettres $x_0, x_1, \ldots, x_{m-1}$ dont se compose cette fonction, à former les valeurs distinctes $y_1, y_2, \ldots, y_s$ qu'elle prend pour toutes ces permutations, et à déterminer 1° la somme de ces valeurs ; 2° la somme de leurs produits deux à deux ; 3° la somme de leurs produits trois à trois, et ainsi de suite. Car chacune de ces sommes, étant évidemment symétrique par rapport aux m racines de la proposée (1), peut être exprimée en fonction rationnelle des coefficients de cette équation.

* A new sequence of equation numbers begins here

† Original has $x_1, x_2, \ldots, x_{m-1}$

une fonction rationnelle des racines de l'équation (1), et

$$\varphi(y) = 0 \tag{2}$$

l'équation dont cette fonction dépend, équation dont les coefficients sont des fonctions rationnelles de ceux de l'équation proposée (1) ; et admettons : 1° que cette équation soit résoluble ou décomposable en d'autres équations de degrés moindres ; qu'elles-mêmes soient décomposables en d'autres équations de degrés moindres, et ainsi de suite, les dernières équations auxquelles on parvient étant résolubles ; 2° et que des diverses valeurs de cette fonction y, on puisse déduire les valeurs des racines cherchées. Le problème de la détermination des racines de l'équation donnée (1) sera complètement résolu.

Plus généralement, soient $z_1, z_2, \dots, z_h$ des fonctions rationnelles contenant toutes les racines de l'équation (1), ou contenant, la première, un groupe de ces racines, la deuxième, un autre groupe de ces mêmes racines, et ainsi de suite ; et soient

$$y = F(z_1, z_2, \dots, z_h)$$

une fonction rationnelle de ces quantités, et

$$\varphi(y) = 0$$

l'équation dont y dépend, équation qu'on peut former avec les coefficients de l'équation (1). Admettons : 1° que cette équation $\varphi(y) = 0$ soit telle qu'elle soit résoluble directement ou par sa décomposition en d'autres de degrés moindres ; 2° que des diverses valeurs de y on puisse déduire les valeurs des expressions $z_1, z_2, \dots, z_h$; 3° que de ces dernières on puisse déduire directement les racines de l'équation (1), ou les équations dont les racines sont respectivement celles qui entrent dans chacune de ces expressions ; 4° enfin que ces dernières équations soient résolubles. Le problème de la détermination des racines de l'équation proposée (1) sera complètement résolu.

Ainsi le théorème est démontré.

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

Remarque.—Ce théorème détermine la méthode à suivre pour résoudre les équations. La résolution de l'équation (1) dépend de celle de l'équation (2), pourvu que des diverses valeurs de y on puisse déduire les racines de la proposée.

Théorème II.—*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 $x_0, x_1 x_2, \dots, x_{n-1}$ relatifs à ces s valeurs peuvent être partagés en v groupes de permutations inséparables, l'équation $\varphi(y) = 0$ d'où dépend cette fonction y se décompose en v équations, chacune du degré r, $s = vz$, à l'aide des racines d'une équation algébrique, de degré v, dont les coefficients sont des fonctions rationnelles de ceux de la proposée.*

Quel que soit, en effet, le nombre s des valeurs distinctes de la fonction résolvante y, et quelle que soit sa composition, les permutations, nous l'avons déjà rappelé, produites par les m racines de l'équation proposée dont cette fonction se compose se partagent en s groupes formés chacun de q permutations associées de telle manière que, malgré tous les échanges de ces lettres, les permutations d'un même groupe ne peuvent jamais se séparer. Admettons que ce partage soit effectué, et soit (A) le tableau qui en résulte.

Or, nous supposons que ces s groupes se partagent en v groupes de permutations *inséparables*, composés chacun de r groupes du tableau (A). Donc, si z est une fonction symétrique quelconque des r valeurs de y relatives à l'un de ces v groupes, la somme par exemple ; et si on désigne par $z_1, z_2, \dots, z_v$ les valeurs qu'elle prend pour chacun de ces v groupes ; toute fonction symétrique de $z_1, z_2, \dots, z_v$, nous l'avons démontré, est invariable par rapport aux m racines de l'équation donnée (1), et elle est par conséquent 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 $\gamma_1, \gamma_2, \dots, \gamma_v$; 2° la somme de leurs produits deux à deux ; 3° la somme de leurs produits trois à trois, et ainsi de suite, et par conséquent de former l'équation

$$\Gamma^v + C_1\Gamma^{v-1} + \cdots + C_v = 0 \tag{3}$$

dont les racines sont $\gamma_1, \gamma_2, \dots, \gamma_v$.

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 $y_1, y_2, \dots, y_r$ de la fonction résolvante y relatives à l'un des groupes du tableau (A), au premier par exemple, toute fonction symétrique de ces r valeurs est semblable à cette racine γ_1 et par conséquent exprimable en fonction rationnelle de γ_1 et des coefficients de l'équation (3), 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 $y_1, y_2, \dots, y_r$; 2° la somme de leurs produits trois à trois, et ainsi de suite : d'où la formation de l'équation

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

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

De la même manière, l'on démontrerait que $\gamma_2, \gamma_3, \dots, \gamma_v$ étant les autres racines de l'équation (3), on peut, avec les coefficients de l'équation proposée, 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 autres racines des autres groupes ; ce qui produit les équations

$$\begin{gathered} y^r - \gamma_2 y^{r-1} + Q_2 y^{r-2} + \cdots + Q_r = 0\,, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ y^r - \gamma_v y^{r-1} + U_2 y^{r-2} + \cdots + U_r = 0\,.^* \end{gathered}$$

* Original has γ_2

Ainsi, sans qu'on soit obligé de former l'équation résolvante $\varphi(y) = 0$ de degré s, on peut former l'équation (3) 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 on forme préalablement l'équation résolvante $\varphi(y) = 0$, on peut 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 de degré r, $\varphi(y)$ est exactement divisible par le polynôme $y^r - \gamma_1 y^{r-1} + P_2 y^{r-2} + \cdots + P_r$. 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 $P_2, P_3, \ldots, P_r$ 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 III.—*Réciproquement : si l'équation résolvante $\varphi(y) = 0$ d'une équation irréductible quelconque, $F(x) = 0$, est décomposable en facteurs de degrés moindres, à l'aide des racines d'une équation Γ, de degré v, dont les racines sont des fonctions rationnelles de celles de cette équation en x ; 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 v groupes de permutations inséparables : et ces équations de degrés moindres sont toutes d'un même degré.*

Admettons, en effet, que l'on ait

$$\varphi(y) = \psi_1(y, \gamma_1)\psi_2(y, \gamma_2) \cdots \psi_v(y, \gamma_v)\,, \tag{4}$$

$\gamma_1, \gamma_2, \ldots, \gamma_v$ désignant les racines de l'équation en Γ de degré v. L'équation $\varphi(y) = 0$ étant la résolvante de $F(x) = 0$, ses racines y sont des fonctions rationnelles (théorème III) de celles $x_0, x_1, \ldots, x_{n-1}$ de cette équation en x ; et son degré étant égal à s, les permutations des n racines x peuvent être partagées, nous l'avons déjà dit, en s groupes de permutations inséparables pour tous les échanges de ces racines, celles d'un même groupe faisant acquérir une même valeur à y : supposons ce partage effectué, et soit (A) le tableau qui en résulte.

Par les mêmes raisons, les mêmes permutations des n racines x peuvent être partagées en v groupes de permutations inséparables pour tous les échanges de ces racines, celles d'un même groupe faisant acquérir une même valeur à γ : supposons ce nouveau partage effectué et soit (A′) le tableau, analogue à (A), qui en résulte.

Cela étant : je remarque que les valeurs de y qui annulent les facteurs $\psi_1, \psi_2, \ldots, \psi_v$ sont respectivement fonction de $z_1, z_2, \ldots, z_v$. De là, il suit que si 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, le premier par exemple, r désignant son degré ; tous les échanges des lettres $x_0, x_1, \ldots, x_{m-1}$, 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 z_1. Car si quelques-uns de ces échanges transformaient cette valeur z_1 ; ils ne pourraient, les groupes de (A′) étant inséparables, que transformer z_1 en une autre racine de l'équation auxiliaire, en z_h par exemple ; et dès lors ces mêmes échanges transformeraient les racines $y_1, y_2, \ldots, y_r$ du facteur ψ_1 en celles du facteur ψ_h ; ce qui est contre l'hypothèse. Donc toutes les permutations de ce groupe doivent se trouver dans celui du tableau (A′) qui est relatif à z_1. Si ensuite l'on considère toutes les permutations des groupes de (A) relatifs à ces r valeurs de y, tous les échanges des mêmes lettres qui convertissent ces groupes les uns dans les autres, n'altèreront pas non plus cette même racine z_1 par une raison entièrement semblable. Donc encore, ces r groupes de (A) se trouvent dans celui de (A′) qui correspond à z_1.

Ainsi, ce groupe de (A′) se compose de toutes les permutations qui sont relatives aux r groupes de (A) qui correspondent aux r racines de $\psi_1 = 0$. Il en est de même des autres groupes de (A′) relatifs aux autres racines $z_2, z_3, \ldots, z_v$ de l'équation auxiliaire ; chacun d'eux se compose des permutations des autres groupes de (A) qui correspondent respectivement aux racines y des équations $\psi_2 = 0, \psi_3 = 0, \ldots, \psi_v = 0$. Mais les racines y des v facteurs sont distinctes, donc les s groupes de (A) sont d'abord partagés en v groupes formant le tableau (A′) ; et puis, comme les permutations des groupes de ce dernier tableau sont inséparables, le nombre de permutations, et par conséquent le nombre de groupes de (A) qui forment ceux de (A′) est le même pour tous ces derniers. En sorte que les s groupes du tableau (A) peuvent être partagés en v groupes de permutations inséparables ; et de plus les v facteurs dans lesquels se décompose $\varphi(y)$ sont d'un même degré r tel que $s = vr$.

Théorème IV.—*Pour que l'équation résolvante $\varphi(y) = 0$, de degré déterminé s, d'une équation irréductible $F(x) = 0$, soit décomposable en v équations, d'un même degré r tel que $s = vr$, à l'aide des racines d'une équation de degré v ; il faut et 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 v groupes de permutations inséparables.*

Ce théorème résulte en effet des deux précédents.

Théorème V.—*Si une équation algébrique, irréductible et de degré premier est soluble par radicaux, l'indice le plus élevé de ces radicaux est égal au degré même de cette équation.*

Soit n le degré premier de l'équation irréductible à résoudre $f(x) = 0$: puisque cette équation est irréductible et résoluble algébriquement, c'est-à-dire soluble par radicaux, il faut qu'à l'aide d'un radical r d'un certain indice i, son premier membre soit décomposable en facteurs.

Or, si la valeur r_1 de ce radical produit le facteur $f_1(x, r_1)$ de degré p, chacune des autres valeurs de ce même radical $r_2, r_3, \ldots r_i$ produira un facteur analogue et du même degré p. On aura donc

$$f(x) = f_1(x, r_1) \cdot f_2(x, r_2) \cdots f_i(x, r_i)\,, \tag{5}$$

et $ip = n$: mais n est un nombre premier, i est au moins égal à 2, et p est inférieur à n ; donc $i = n$, et par suite $p = 1$.

Ce théorème appartient à Gallois.

Remarque.—L'expression radicale r dépendra en général de radicaux d'indices inférieurs à n, comme nous le verrons bientôt.

Théorème VI.—*Si une équation algébrique et irréductible est soluble par radicaux, et si son degré m est un nombre composé, $m = nq$ (n étant premier) les racines de cette équation contiennent le radical d'indice n.*

Puisque cette équation algébrique, $f(x) = 0$, est irréductible et soluble par radicaux, son premier membre est décomposable en facteurs de degrés moindres, à l'aide d'un radical r d'un certain indice i. Or, si la valeur r_1 de ce radical produit le facteur $f_1(x, r_1)$ de degré p, chacune des autres valeurs de ce même radical, $r_2, r_3, \ldots, r_i$ produira un facteur analogue de même degré p. On aura donc

$$f(x) = f_1(x, r_1) \cdot f_2(x, r_2) \cdots f_i(x, r_i)\,, \tag{6}$$

$m = ip$, et par suite $ip = nq$.

Cela posé : examinons d'abord le cas où le degré m de l'équation est égal au produit de deux facteurs premiers, $m = nn_1$. Dans ce cas l'équation précédente devient $ip = nn_1$; et comme n divise le second membre, il doit diviser le premier ; mais, n étant premier, ce nombre doit diviser ou i ou p, on a donc soit $i = hn$, soit $p = kn$.

L'hypothèse $p = kn$ est inadmissible ; car, si elle était vraie, on aurait $ik = n_1$, ce qui est impossible puisque n_1 est premier. Par la même raison on ne peut avoir $i = hn$, car cette hypothèse entraînerait l'équation $ph = n_1$. On doit donc avoir ou $p = n$, ou $i = n$: l'hypothèse $i = n$ convient au théorème énoncé, et celle de $p = n$ donne $i = n_1$, qui est également un nombre premier.

Ainsi, dans le cas de $m = nn_1$, le théorème est démontré.

Supposons actuellement que m soit égal au produit de trois facteurs premiers, $m = nn_1n_2$. Dans ce nouveau cas, l'équation $ip = nq$ devient $ip = nn_1n_2$; et comme dans le premier cas on devrait avoir soit $i = hn$, soit $p = kn$. Cette dernière hypothèse entraîne l'équation $ik = n_1n_2$, qui exige elle-même, d'après ce qui vient d'être dit, que $i = n_1$ ou $k = n_1$: mais $k = n_1$ donne $i = n_2$, donc i est encore égal à un des facteurs premiers de m. Et la première hypothèse $i = hn$ entraîne l'équation $ph = n_1n_2$ qui exige elle-même que $p = n_1$ ou $p = n_2$, c'est-à-dire que p soit un nombre premier, $p = n_2$ par exemple. Ainsi chacun des facteurs du second membre de l'équation (6) est d'un même degré premier n_2. Donc chacun d'eux est (théorème V) décomposable en facteurs du premier degré, à l'aide des valeurs d'un radical dont l'indice est égal à ce nombre premier n_2. Or, la décomposition de $f(x)$ en ces facteurs du premier degré produira, par la multiplication, une nouvelle décomposition de $f(x)$ en n_2 facteurs, de degré nn_1, à l'aide de ce radical d'indice premier n_2. Donc le théorème est encore vrai dans le cas où $m = nn_1n_2$.

Cette démonstration peut évidemment être généralisée, et être étendue au cas où m est égal au produit d'un nombre quelconque de facteurs premiers égaux ou inégaux.

Ainsi, l'équation (6) existe dans tous les cas ; i étant égal à n, et le degré p, commun aux n facteurs de son second membre, étant égal à q.

II

DES ÉQUATIONS RÉSOLUBLES ALGÉBRIQUEMENT

THÉORÈME VII.—*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* $1 \cdot 2 \cdot 3 \cdots (n-2)$.

Rappelons auparavant que le degré n de l'équation proposée $f(x) = 0$ étant premier, tout nombre entier p inférieur à n jouit de cette propriété que les résidus à n de la suite

$$p, \quad 2p, \quad 3p, \quad \ldots, \quad \overline{n-1}p$$

sont les nombres naturels $1, 2, 3, \ldots, n-1$ dans un ordre déterminé. De même, ρ étant une des racines *primitives* de n, les résidus à n de l'une et de l'autre suites

$$\begin{gathered} p, \quad p\rho, \quad p\rho^2, \quad \ldots, \quad p\rho^{n-2}, \\ p\rho^h, \quad 2p\rho^h, \quad 3p\rho^h, \quad \ldots, \quad \overline{n-1}p\rho^h, \end{gathered}$$

sont encore les nombres naturels $1, 2, 3, \ldots, n-1$, dans un ordre déterminé; h désignant un nombre entier quelconque inférieur à $n-2$, ou au plus égal à ce nombre.

On peut donc représenter les racines de l'équation proposée, $f(x) = 0$, par l'une des suites

$$\begin{array}{lllll} x_a, & x_{a+p}, & x_{a+2p}, & \ldots, & x_{a+\overline{n-1}p}, \\ x_a, & x_{a+p}, & x_{a+p\rho}, & \ldots, & x_{a+p\rho^{n-2}}, \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ x_a, & x_{a+p\rho^h}, & x_{a+2p\rho^h}, & \ldots, & x_{a+\overline{n-1}p\rho^h}, \end{array}$$

a désignant l'un des nombres entiers $0, 1, 2, \ldots, n-1$.

Enfin r et α désignant deux racines imaginaires différentes de l'équation binôme $x^{n-1} = 0$, ces racines sont $r, r\alpha, r\alpha^2, \ldots, r\alpha^{n-1}$; ou bien $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. Donc elles pourront être représentées par l'une des suites

$$\begin{array}{lllll} r, & r\alpha^p, & r\alpha^{2p}, & \ldots, & r\alpha^{\overline{n-1}p}, \\ 1, & \alpha^p, & \alpha^{p\rho}, & \ldots, & \alpha^{p\rho^{n-2}}, \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1, & \alpha^{p\rho^h}, & \alpha^{2p\rho^h}, & \ldots, & \alpha^{\overline{n-1}p\rho^h}. \end{array}$$

Cela posé : nous allons d'abord démontrer que les conditions de l'énoncé sont nécessaires ; et pour cela nous admettrons que l'équation proposée est résoluble algébriquement.

L'équation proposée étant en effet résoluble par hypothèse, l'équation (5) existe, et elle deviendra, d'après ce qui précède,

$$(7) \qquad f(x) = f_1(x_a, r) \cdot f_2(x_{a+p}, r\alpha^p) \cdots f_n(x_{a+\overline{n-1}p}, r\alpha^{\overline{n-1}p}),$$

chacun des n facteurs du second membre étant du premier degré par rapport à x.

Or, toutes les racines d'une équation irréductible ont un même caractère qui sert à les déterminer, celui de satisfaire identiquement à cette équation ; on peut donc, dans l'équation (7), changer la racine r en la racine $r\alpha^p$; auquel cas $r\alpha^p, r\alpha^{2p}$, $\ldots, r\alpha^{\overline{n-1}p}$ se changent respectivement en $r\alpha^{2p}, r\alpha^{3p}, \ldots, r$: et cet échange de racines, [équation (7)], transforme celles de l'équation proposée $f(x) = 0$, x_a, x_{a+p}, $\ldots, x_{a+\overline{n-1}p}$, respectivement en $x_{a+p}, x_{a+2p}, \ldots, x_a$; c'est-à-dire la permutation $x_a, x_{a+p}, \ldots, x_{a+\overline{n-1}p}$ en la permutation *circulaire* $x_{a+p}, x_{a+2p}, \ldots, x_a$.

Mais ce changement n'en amène aucun dans le second membre de l'équation (7) ; donc, quelle que soit la fonction *résolvante* y de l'équation proposée qui ait produit sa décomposition, cette fonction y est inaltérable par la permutation circulaire précédente, et par suite par les n permutations circulaires de cette première x_a, x_{a+p}, $\ldots, x_{a+\overline{n-1}p}$.

De plus, on peut également changer p qui est arbitraire en $p\rho^h$ qui est tout aussi arbitraire ; et ce changement transforme la suite des $n-1$ racines imaginaires

$$\alpha^p, \quad \alpha^{2p}, \quad \ldots, \quad \alpha^{\overline{n-1}p},$$

en la suite

$$\alpha^{p\rho^h}, \quad \alpha^{2p\rho^h}, \quad \ldots, \quad \alpha^{\overline{n-1}p\rho^h};$$

et ce même changement transforme les racines de $f(x) = 0$, équation (7), x_a, x_{a+p}, $\ldots, x_{a+\overline{n-1}p}$ respectivement en les racines $x_a, x_{a+p\rho^h}, x_{a+2p\rho^h}, \ldots, x_{a+\overline{n-1}p\rho^h}$; c'est-à-dire la permutation

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

en la permutation

$$x_a, x_{a+p\rho^h}, x_{a+2p\rho^h}, \ldots, x_{a+\overline{n-1}p\rho^h}$$

qui correspond, théorème IV d'un autre Mémoire([1]), à l'un quelconque des polygones étoilés de Poinsot.

Or, ce changement n'en amène aucun dans le second membre de l'équation (7), et cela quelle que soit la valeur de p ; donc la fonction résolvante y jouit encore de la propriété d'être inaltérable par les $n-1$ permutations relatives aux $n-1$ polygones étoilés de Poinsot qui constituent un *seul et même* ordre.

Or, ces deux changements sont les seuls qui n'altèrent pas la décomposition de $f(x)$, équation (7), donc cette fonction résolvante n'est inaltérable que par les n permutations circulaires et par les $n-1$ permutations d'un même ordre que produit

([1]) Voir le 6e volume, 2e série, du journal publié par M. Liouville, p. 425.

une permutation quelconque des n racines de l'équation proposée ; et par conséquent le nombre s de ses valeurs distinctes est donné par la formule

$$s = \frac{1 \cdot 2 \cdot 3 \cdots n}{n(n-1)} = 1 \cdot 2 \cdot 3 \cdots (n-2)\,.$$

Cette fonction dépend donc d'une équation de ce degré qu'il serait toujours possible de former avec les coefficients de l'équation proposée, si la forme de cette fonction était connue ; équation dont les racines sont relatives aux $1, 2, 3, \ldots, (n-2)$ groupes de la deuxième classification du même Mémoire.

Quelle est la forme de cette fonction résolvante y ? Je remarque à cet effet que si cette fonction était composée de r termes distincts et relatifs aux $n(n-1)$ permutations pour lesquelles elle doit conserver une même valeur, les équations auxiliaires, analogues à celles en y du théorème II, seraient du degré r. Il est donc indispensable de rendre r le plus petit possible.

Or, la théorie de l'ordre étant indépendante de la notion de grandeur et n'étant relative qu'à la notion de situation, nous pouvons placer les n racines de l'équation proposée sur une circonférence de cercle de rayon arbitraire, à égales distances les unes des autres, et dans l'ordre de la permutation, d'ailleurs quelconque, $x_a, x_{a+p}, x_{a+2p}, \ldots, x_{a+\overline{n-1}p}$; la racine x_a étant placée à l'origine des arcs. Et si nous joignons le centre à ces n points de division, ces n rayons représenteront les n racines n^{e} de l'unité $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$; α étant l'une d'elles, mais différente de l'unité.

Or, pour amener la permutation circulaire $x_{a+p}, x_{a+2p}, \ldots, x_a$ dans la position de la première, il faut multiplier chacune des racines n^{e} de l'unité par α^{n-1} ; et puisque la fonction résolvante y doit être invariable pour toute permutation circulaire, chaque terme de cette fonction doit donc être de la forme

$$z_1 = \left(x_a + \alpha x_{a+p} + \alpha^2 x_{a+2p} + \cdots + \alpha^{n-1} x_{a+\overline{n-1}p}\right)^n \;; \tag{8}$$

expression qui est telle en effet qu'en multipliant le polynôme soumis à l'exposant n par α^{n-1}, on obtient le polynôme

$$x_{a+p} + \alpha x_{a+2p} + \cdots + \alpha^{n-2} x_{a+\overline{n-1}p} + \alpha^{n-1} x_a\,,$$

offrant la permutation circulaire de la disposition du premier, et qui cependant conserve sa valeur z_1 puisque

$$\alpha^{(n-1)n} = (\alpha^n)^{n-1} = 1\,.(^1)$$

Cette fonction (8), étant invariable pour une permutation circulaire, est invariable pour les n permutations circulaires déduites de la première ; d'autant qu'il suffirait de multiplier successivement z_1 par $(\alpha^{n-2})^n = 1$, $(\alpha^{n-3})^n = 1 \ldots$ Mais cette même fonction prend $n-1$ valeurs distinctes $z_1, z_2, \ldots, z_{n_1}$, pour les $n-1$ autres permutations pour lesquelles y doit conserver une même valeur, celles qui se rapportent aux $n-1$ polygones étoilés de Poinsot ; donc les équations, analogues

(1) C'est ainsi qu'on retrouve la fonction z_1 de Lagrange appelée *résolvante* par cet illustre géomètre.

à celles en y du théorème II, sont du degré $n-1$; et la fonction résolvante y sera définie d'après ce théorème, par l'expression

$$y = z_1 + z_2 + z_3 + \cdots + z_{n-1} \tag{9}$$

qui est la fonction symétrique la plus simple de ces $n-1$ valeurs. Il est utile de remarquer que ces $n-1$ valeurs peuvent être déduites de z_1, en y remplaçant successivement p par $p\rho, p\rho^2, \ldots, p\rho^{n-2}$.

D'après ce qui a été démontré dans ce même théorème II, on peut, avec cette fonction (9) et avec les coefficients de l'équation proposée former l'équation en y du degré $1 \cdot 2 \cdot 3 \cdots (n-2)$ et avec l'une de ses racines, former celle en z du degré $n-1$: et pour résoudre l'équation donnée résoudre cette dernière équation qui a pour racines $z_1, z_2, \ldots, z_{n-1}$.

Corollaire.—Si dans le calcul précédent on fait $n=3$, c'est-à-dire si l'équation donnée est du 3e 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 fonction de ses coefficients. Les expressions de ces racines contiendront deux radicaux cubiques et un radical carré.

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

Théorème VIII.—*Pour résoudre une équation algébrique irréductible et de degré composé $m = nq$, n étant premier, il est nécessaire et suffisant de résoudre n équations de degré q ; et deux autres équations, l'une de degré $n-1$ et l'autre de degré s donnée par la formule*

$$s = \frac{1 \cdot 2 \cdot 3 \cdots m}{(1 \cdot 2 \cdot 3 \cdots q)^n \cdot n(n-1)}$$

En conservant les notations du théorème précédent, et en admettant que l'équation proposée, $f(x) = 0$, soit soluble ; l'équation (6) sera vraie et elle deviendra

$$f(x) = f_1(x, r) \cdot f_2(x, r\alpha^p) \cdot f_3(x, r\alpha^{2p}) \cdots f_n(x, r\alpha^{\overline{n-1}p}), \tag{10}$$

analogue à l'équation (7), avec cette différence qu'ici les facteurs sont d'un même degré q différent de l'unité. Or, en permutant les q racines d'un des facteurs du second membre, ce facteur est invariable. Donc ces permutations n'altèrent pas la décomposition (10) de $f(x)$; et par suite la fonction résolvante y de l'équation proposée, qui produit cette décomposition, doit être invariable par les permutations des q racines d'un quelconque de ces facteurs. Mais le nombre de permutations de q lettres est égal à $1 \cdot 2 \cdot 3 \cdots q$, et il y a n facteurs, donc y doit être invariable pour un nombre de permutations égal à $(1 \cdot 2 \cdot 3 \cdots q)^n$.

De plus, si on considère une fonction symétrique quelconque des q racines d'un des facteurs de l'équation (10), par exemple la somme, et si on désigne par X_a, X_{a+p}, $\ldots, X_{a+\overline{n-1}p}$ les sommes respectives des q racines du 1er, du 2e, …, du ne facteur, il est clair que ces sommes jouissent des mêmes propriétés que les racines x_a, x_{a+p},

$\ldots, x_{a+\overline{n-1}p}$ du théorème précédent. Donc la fonction résolvante y de $f(x) = 0$ jouit encore de cette propriété, d'être invariable et par les n permutations circulaires et par les $n-1$ permutations d'un *même ordre*, relatif à une permutation quelconque des n lettres $X_a, X_{a+p}, \ldots, X_{a+\overline{n-1}p}$.

Or ces 3 changements sont les seuls qui n'altèrent pas la décomposition (10) de l'équation proposée $f(x) = 0$; donc cette fonction résolvante n'est invariable que par le nombre de permutations déterminé par la formule

$$(1 \cdot 2 \cdot 3 \cdots q)^n \cdot n(n-1)\,,$$

dès lors le nombre des valeurs distinctes est donné par la formule

$$s = \frac{1 \cdot 2 \cdot 3 \cdots m}{(1 \cdot 2 \cdot 3 \cdots q)^n \cdot n(n-1)}\,.$$

Cette fonction dépend donc d'une équation algébrique de degré s qu'il est possible, dans tous les cas, de former avec les coefficients de l'équation donnée, si la forme de cette fonction est connue. Et cette fonction résolvante y est déterminée par la formule

$$y = Z_1 + Z_2 + \cdots + Z_{n-1}\,, \tag{11}$$

dans laquelle Z_1 désigne la fonction

$$Z_1 = (X_a + \alpha X_{a+p} + \alpha^2 X_{a+2p} + \cdots + \alpha^{n-1} X_{a+\overline{n-1}p})^n\,,$$

et $Z_2, Z_3, \ldots, Z_{n-1}$ les valeurs qu'on déduit de Z_1 en remplaçant successivement p par $p\rho, p\rho^2, \ldots, p\rho^{n-2}$: car il résulte de ce qui précède que $X_a, X_{a+p}, \ldots, X_{a+\overline{n-1}p}$ jouissent, dans ce théorème, des mêmes propriétés que $x_a, x_{a+p}, \ldots, x_{a+\overline{n-1}p}$ dans le théorème précédent.

Or, ce dernier théorème prouve qu'on peut former, avec la fonction (11), l'équation résolvante en y ; et, avec l'une de ses racines, l'équation en Z du degré $n-1$ dont les racines sont $Z_1, Z_2, \ldots, Z_{n-1}$. Il prouve de plus que cette dernière équation doit être résolue, et qu'on aura par suite, par des équations en tout semblables aux équations (10), les valeurs de $X_a, X_{a+p}, \ldots, X_{a+\overline{n-1}p}$. Mais, connaissant la somme X_a de q racines de l'équation proposée, on peut déterminer en fonction rationnelle de X_a toute fonction symétrique des mêmes racines, et par conséquent former l'équation

$$x^q - X_a x^{q-1} + C_2 x^{q-2} + \cdots + C_q = 0\,,$$

dont les racines sont ces q racines.

Car, ces q racines étant dans l'équation proposée $f(x) = 0$, le premier membre $f(x)$ est divisible par le premier membre de l'équation à former. On devra donc égaler à zéro les q coefficients du reste de cette division ; et $q-1$ de ces équations détermineront les $q-1$ coefficients inconnus $C_2, C_3, \ldots, C_q$ en fonction *rationnelle* de X_a, puisque ces coefficients sont semblables à X_a. Et en remplaçant successivement dans les expressions de ces coefficients X_a par $X_{a+p}, X_{a+2p}, \ldots, X_{a+\overline{n-1}p}$, on aura les équations dont les racines sont celles qui ont pour somme respectivement $X_{a+p}, X_{a+2p}, \ldots, X_{a+\overline{n-1}p}$. Il faudra donc résoudre ces n équations, de degré q, pour avoir les racines de l'équation proposée.

Donc les conditions énoncées du théorème à démontrer sont nécessaires.

Elles sont de plus suffisantes : car, si on résout l'équation en y de degré s, ainsi que celle en Z de degré $n-1$, on peut obtenir les n équations en x, d'un même degré q, dont la résolution entraîne celle de l'équation proposée.

Corollaire.—Si dans le calcul précédent on fait $m = 2 \cdot 2 = 4$, c'est-à-dire si l'équation à résoudre est du quatrième degré, l'équation en y est du troisième degré et l'équation en Z du premier. Or toute équation du troisième degré est résoluble algébriquement, donc il est possible d'avoir ses trois racines en y ; et par suite de former, avec l'une d'elles et avec les coefficients de l'équation proposée, les deux équations du second degré dont les racines sont les quatre de la proposée.

Ainsi, la résolution de toute équation du quatrième degré se ramène à celle d'une équation du troisième degré et à celles de deux équations du second. D'où ce théorème : *toute équation du quatrième degré est soluble par radicaux.*

Théorème IX.—*Il est impossible de résoudre algébriquement les équations générales de degré supérieur au quatrième.*

En premier lieu : les équations des quatre premiers degrés sont résolubles algébriquement ; car toute équation du premier degré est résoluble et sa racine est rationnelle par rapport aux coefficients ; et les équations des 2e, 3e et 4e degrés sont également résolubles algébriquement par une même méthode, celle de l'équation résolvante, comme cela résulte de la théorie bien connue des équations du second degré[1] et des corollaires des théorèmes VII et VIII. Les racines des équations du second degré contiennent un radical carré ; et celles des équations des troisième et quatrième degrés, des radicaux carrés et cubiques.

En second lieu il résulte : 1° du théorème VII, que pour résoudre une équation de degré premier n, il faut nécessairement résoudre d'abord une équation de degré $1 \cdot 2 \cdot 3 \cdots (n-2)$, produit supérieur à n, puisque pour la plus petite valeur 5 de n, $1 \cdot 2 \cdot 3 \cdots (n-2) = 6$ qui est supérieur à 5 et que, pour des nombres supérieurs à 5, *a fortiori* on a $1 \cdot 2 \cdot 3 \cdots (n-2) > n$.

Or, les racines de cette équation sont les valeurs de y (9) relatives aux groupes de la deuxième classification de notre Mémoire déjà cité en nombre $1 \cdot 2 \cdot 3 \cdots (n-2)$: chacun d'eux étant un seul et même ordre vu successivement de chacune des n racines de l'équation proposée. Mais ces groupes ou ordres ne peuvent pas être partagés en nouveaux groupes de permutations inséparables[2] ; donc, théorème III, cette équation, dont le degré est supérieur à 4, ne peut être décomposée en d'autres de degrés moindres. 2° Il résulte du théorème VIII que pour résoudre une équation de degré composé $m = nq$, n étant premier, il faut d'abord résoudre nécessairement une équation du degré

$$\frac{1 \cdot 2 \cdot 3 \cdots m}{(1 \cdot 2 \cdot 3 \cdots q)^n \cdot n(n-1)},$$

[1] La résolution de toute équation du second degré, $x^2 + A_1 x + A_2 = 0$, n'échappe pas à cette méthode : et ici la fonction résolvante devient $y = (x_1 - x_2)^2$ qui, étant symétrique par rapport aux racines, s'exprime en fonction rationnelle des coefficients A_1, A_2, de l'équation proposée. On a, en effet, $y = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = A_1^2 - 4A_2$, et comme $x_1 + x_2 = -A_1$, on a deux équations desquelles on déduit les deux racines.

[2] Voir la note placée à la fin de ce mémoire.

nombre supérieur à n pour la plus petite valeur 6 de m et qui *a fortiori* est encore supérieur à m pour tous les nombres plus grands que 6.

Or, les racines de cette équation sont les valeurs (11) de y relatives à tous les ordres formés avec les n quantités $X_a, X_{a+p}, \ldots, X_{a+\overline{n-1}p}$ *, *considérées comme des lettres*, dans lesquelles on échange les racines de l'équation proposée $f(x) = 0$, que ces quantités contiennent ; mais, d'après la même note, les ordres ne peuvent être partagés en groupes de permutations inséparables : donc, même théorème III, cette équation en y est indécomposable en d'autres de degrés moindres.

Donc, quel que soit le degré m de l'équation proposée, que ce degré m soit premier ou composé, s'il est supérieur à 4, la résolution de cette équation dépend essentiellement de la résolution d'une autre équation non résoluble et d'un degré supérieur à celui de la proposée : il est donc impossible de résoudre les équations générales de degré supérieur au quatrième.

Recherche d'une classe d'équations résolubles algébriquement.

Puisqu'il est impossible de résoudre algébriquement les équations générales de degré supérieur au quatrième, on doit chercher les conditions nécessaires et suffisantes qui doivent exister entre les racines d'une équation irréductible, de degré supérieur à 4, pour que cette équation soit résoluble algébriquement. Et d'abord, nous allons déterminer, à l'aide de nos principes, une classe d'équations, solubles par radicaux, qui jouent un rôle important dans la recherche de toutes les équations résolubles algébriquement.

Il résulte, en effet, 1° du théorème I que la résolution de toute équation algébrique et irréductible, $f(x) = 0$, dépend de la résolution de son équation résolvante $\varphi(y) = 0$; 2° du théorème IV que cette équation $\varphi(y) = 0$ n'est décomposable en facteurs de degrés moindres, à l'aide de racines d'une équation auxiliaire de degré v, qu'autant que les s groupes de permutations où $x_0, x_1, \ldots, x_{m-1}$, relatifs aux s racines de cette résolvante, peuvent être partagés en v groupes de permutations inséparables. On aura donc des équations solubles par radicaux, en cherchant les conditions nécessaires et suffisantes qui doivent exister entre les racines de l'équation proposée pour que le degré commun r aux équations en y du théorème II soit égal à l'unité et pour que le degré v de l'équation auxiliaire (3) en z soit aussi égal à l'unité ; auquel cas le degré s de l'équation résolvante est aussi égal à l'unité, puisque $s = vr$. De là il suit que si (A) est le tableau des groupes de permutations relatifs à l'équation $\varphi(y) = 0$, la fonction résolvante y doit être invariable pour tous ces s groupes.

Distinguons actuellement deux cas : celui où le degré de l'équation proposée $f(x) = 0$ est un nombre premier n, et celui où ce degré est un nombre composé.

Dans le premier cas, $m = n$, la fonction résolvante est définie par la formule (9) dans laquelle z_1 désigne la fonction (8), théorème VII ; il résulte donc de ce qui précède, que cette expression y ne doit avoir qu'une valeur et être égale par conséquent à une fonction rationnelle et symétrique des racines de l'équation proposée ; et ce résultat sera atteint si z_1 est dans le même cas que y. Or, comme cette expression z_1 n'est invariable que par les n permutations circulaires d'une permutation

* Original has $X_{a+\overline{m-1}p}$

quelconque des n racines de la proposée, ou ce qui est la même chose, quand on y remplace a successivement par les valeurs $a+p, a+2p, \ldots, a+\overline{n-1}p$. Donc cette exposition z_1 doit pouvoir se réduire à ne contenir qu'une seule de ces racines ; ce qui exige que $n-1$ d'entre elles soient des fonctions rationnelles de l'une d'elles : et de plus, quelle que soit la fonction rationnelle de x_a qui soit égale à x_{a+p}, la racine x_{a+2p} doit dépendre de x_{a+p} comme celle-ci dépend de x_a, la racine x_{a+3p} doit dépendre de x_{a+2p} de la même manière, et ainsi de suite, et enfin x_a sera liée à $x_{a+\overline{n-1}p}$ par la même relation.

Ainsi, si $x_{a+p} = \theta(x_a)$, on doit avoir

$$x_{a+2p} = \theta(x_{a+p}), \quad x_{a+3p} = \theta(x_{a+2p}), \quad \ldots, \quad x_a = \theta(x_{a+\overline{n-1}p})\,;$$

en d'autres termes les racines de l'équation proposée doivent être représentées par la suite

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

θ désignant une fonction rationnelle telle que $\theta^n x_a = x_a$, et $\theta^2, \theta^3, \ldots$ désignant des indices d'opérations à répéter.

Effectivement l'expression

$$r_1 = (x_a + \alpha\theta x_a + \alpha^2\theta^2 x_a + \cdots + \alpha^{n-1}\theta^{n-1} x_a)^n = \psi(x_a)\,,$$

peut être exprimée en fonction rationnelle des coefficients de $f(x)$ et de θ. Car cette expression étant invariable pour les n permutations circulaires des n racines, elle conservera la même valeur en y remplaçant successivement x_a par $\theta x_a, \theta^2 x_a, \ldots, \theta^{n-1} x_a$. On a donc

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

et par conséquent

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

relation dont le second membre est une fonction symétrique des racines de l'équation proposée $f(x) = 0$.

Dans le second cas, $m = nq$, la fonction résolvante est définie par l'équation (11) ; et, si on applique à Z_1 le même raisonnement qu'à z_1, on aura ce résultat, en observant que $X_a, X_{a+p}, \ldots, X_{a+\overline{n-1}p}$ dont se compose Z_1 sont des sommes d'un même nombre de racines de l'équation proposée ; pour que l'équation auxiliaire en z soit du premier degré et pour que l'équation en y soit aussi du premier degré, il est nécessaire que les racines de l'équation proposée soient représentées par la suite

$$x_a, \quad \theta x_a, \quad \theta^2 x_a, \quad \ldots, \quad \theta^{m-1} x_a\,, \tag{12}$$

θ désignant une fonction rationnelle telle que $\theta^m x_a = x_a$.

Ajoutons qu'on démontrerait absolument de la même manière que l'expression analogue à z_1,

$$y = (x_a + \alpha\theta x_a + \alpha^2\theta^2 x_a + \cdots + \alpha^{m-1}\theta^{m-1} x_a)^m, \tag{13}$$

invariable par les m permutations circulaires des m racines est une fonction symétrique de ces racines, α désignant une des racines imaginaires de $x^m - 1 = 0$: puisque le raisonnement appliqué à z_1 est indépendant de cette considération que l'exposant n est premier.

On obtient donc ce résultat : l'équation résolvante et, par suite, l'équation auxiliaire d'une équation algébrique quelconque irréductible sont du premier degré, si les racines de celle-ci sont représentées par la suite (12).

Nous pouvons actuellement démontrer le théorème suivant qui est, en quelque sorte, la réciproque de ce dernier résultat.

Théorème X.—*Si les m racines d'une équation algébrique quelconque peuvent être représentées par la suite*

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

θx_a désignant une fonction rationnelle telle que $\theta^m x_a = x_a$ l'équation est toujours soluble par radicaux.

En effet, l'hypothèse faite sur les racines de l'équation proposée permet d'exprimer, en fonction rationnelle des coefficients de cette équation et de ceux de la fonction θ, la fonction y définie par l'expression (13). Soit donc v la valeur connue de cette fonction, on aura, en désignant par $1, \alpha_1, \alpha_2, \ldots, \alpha_{m-1}$, les m racines de l'équation $x^m - 1 = 0$, les m équations

$$\begin{array}{rcrcrcrcl}
x_a & + & \theta x_a & + & \theta^2 x_a & + \cdots + & \theta^{m-1} x_a & = & -A_1\,,\\
x_a & + & \alpha_1 \theta x_a & + & \alpha_1^2 \theta^2 x_a & + \cdots + & \alpha_1^{m-1} \theta^{m-1} x_a & = & \sqrt[m]{v_1}\,,\\
x_a & + & \alpha_2 \theta x_a & + & \alpha_2^2 \theta^2 x_a & + \cdots + & \alpha_2^{m-1} \theta^{m-1} x_a & = & \sqrt[m]{v_2}\,,\\
\multicolumn{9}{c}{\dotfill}\\
x_a & + & \alpha_{m-1} \theta x_a & + & \alpha_{m-1}^2 \theta^2 x_a & + \cdots + & \alpha_{m-1}^{m-1} \theta^{m-1} x_a & = & \sqrt[m]{v_{m-1}}\,,
\end{array}$$

dont les seconds membres sont connus.

De ces équations linéaires par rapport aux m racines à trouver, on peut déduire facilement chacune d'elles. Car, pour avoir $\theta^i x_a$ par exemple, il suffit de multiplier les deux membres de chacune de ces équations respectivement par $1, \alpha_1^{-i}, \alpha_2^{-i}, \ldots, \alpha_{m-1}^{-i}$ et d'ajouter les produits : cette somme en effet donne, en ayant égard aux propriétés des racines des équations binômes, la formule

$$\theta^i x_a = \frac{1}{m}\left\{-A_1 + \alpha_1^{-i}\sqrt[m]{v_1} + \alpha_2^{-i}\sqrt[m]{v_2} + \cdots + \alpha_{m-1}^{-i}\sqrt[m]{v_{m-1}}\right\}$$

de laquelle on déduira les m racines de la proposée en faisant successivement $i = 0, 1, 2, 3, \ldots, m-1$.

Mais comme un radical d'indice m a m valeurs, on pourrait croire que l'expression précédente a m^{m-1} valeurs. Or, il est facile d'exprimer chacun des radicaux qu'elle renferme en fonction d'un seul, auquel cas elle n'aura que m valeurs.

Soit en effet ρ une des racines *primitives* de l'équation $x^m - 1 = 0$, et faisons dans le calcul précédent :

$$\alpha_1 = \rho, \quad \alpha_2 = \rho^2, \quad \alpha_3 = \rho^3, \quad \ldots, \quad \alpha_n = \rho^n, \quad \ldots, \quad \alpha_{m-1} = \rho^{m-1}\,,$$

ce qui est permis, puisque $\rho, \rho^2, \rho^3, \ldots, \rho^{m-1}$ sont les m racines de l'équation $x^m - 1 = 0$. On aura

$$\begin{aligned} \sqrt[m]{v_1} &= x_a + \rho\theta x_a + \rho^2\theta^2 x_a + \cdots + \rho^{m-1}\theta^{m-1}x_a \,, \\ \sqrt[m]{v_n} &= x_a + \rho^n\theta x_a + \rho^{2n}\theta^2 x_a + \cdots + \rho^{(m-1)n}\theta^{m-1}x_a \,. \end{aligned}$$

Mais si dans la valeur de $\sqrt[m]{v_1}$ on change x_a en $\theta^k\alpha_a$, cette valeur est multipliée par ρ^{m-k} ; et ce même changement multiplie le second membre de la seconde égalité par $\rho^{n(m-k)}$; donc ce changement multiplie le produit $\left(\sqrt[m]{v_1}\right)^{m-n} \cdot \sqrt[m]{v_n}$ par $\rho^{n(m-k)} \cdot \rho^{(m-n)(m-k)} = \rho^{(m-k)m} = 1$.

Ce produit étant donc inaltérable en changeant x_a en $\theta^k x_a$, quelle que soit la valeur de k, on aura, en posant

$$\begin{gathered} \left(\sqrt[m]{v_1}\right)^{m-n} \sqrt[m]{v_n} = \chi(x_a) \,, \\ \chi(x_a) = \chi(\theta x_a) = \chi(\theta^2 x_a) = \cdots = \chi(\theta^{m-1}x_a) \end{gathered}$$

et par conséquent

$$\chi(x_a) = \frac{1}{m}\left\{\chi(x_a) + \chi(\theta x_a) + \chi(\theta^2 x_a) + \cdots + \chi(\theta^{m-1}x_a)\right\} \,,$$

relation dont le second membre est une fonction symétrique des racines de l'équation proposée $f(x) = 0$. Donc $\chi(x_a)$ peut être exprimé en fonction rationnelle des coefficients de $f(x)$ et de ceux de la fonction connue θ. Soit u_n sa valeur, on aura donc

$$\left(\sqrt[m]{v_1}\right)^{m-n} \sqrt[m]{v_n} = u_n \,,$$

d'où on déduit

$$\sqrt[m]{v_n} = \frac{u_n}{v_1}\left(\sqrt[m]{v_1}\right)^n \,,$$

et, par suite, cette expression équivalente de $\theta^i x_a$

$$\theta^i x_a = \frac{1}{m}\left\{-A_1 + \rho^{-i}\sqrt[m]{v_1} + \frac{u_2}{v_1}\left(\rho^{-i}\sqrt[m]{v_1}\right)^2 + \cdots + \frac{u_{m-1}}{v_1}\left(\rho^{-i}\sqrt[m]{v_1}\right)^{m-1}\right\} \,;$$

mais si dans cette formule on fait $i = 0$, auquel cas elle devient

$$\frac{x}{a} = \frac{1}{m}\left\{-A_1 + \sqrt[m]{v_1} + \frac{u_2}{v_1}\left(\sqrt[m]{v_1}\right)^2 + \cdots + \frac{u_{m-1}}{v_1}\left(\sqrt[m]{v_1}\right)^{m-1}\right\} \,,$$

et, si on donne successivement au seul radical qu'elle contient ses m valeurs, on aura exactement les mêmes valeurs que celles qui seraient produites par la formule précédente en y faisant successivement $i = 0, 1, 2, \ldots, m-1$; c'est-à-dire les m racines de l'équation proposée.

Remarque.—Ce théorème a été trouvé par Abel en généralisant les travaux de Gauss sur les équations binômes. Les équations algébriques dont les racines jouissent des propriétés énoncées par ce théorème sont dites *abéliennes*. Notre théorie fait donc retrouver, d'une manière simple, cette classe d'équations résolubles algébriquement.

Théorème XI.—*Si le degré m d'une équation abélienne est*

$$m = n_1^{k_1} \cdot n_2^{k_2} \cdots n_\omega^{k_\omega} ,$$

$n_1, n_2, \dots, n_\omega$ étant des nombres premiers, la résolution de cette équation se ramène à celle de k_1 équations de degré n_1, de k_2 équations de degré $n_2, \dots$, et de k_ω équations de degré n_ω ; ces équations étant toutes abéliennes comme la proposée.

Le théorème précédent est vrai, quelle que soit la valeur du degré m ; mais lorsque ce degré est composé, on peut simplifier la solution. En effet, l'équation proposée étant abélienne, ses racines sont

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

x désignant l'une d'elles, et θ une fonction rationnelle telle que $\theta^m x = x$. Or, si nous posons

$$m = m_1 n$$

n étant premier, on peut partager ces m racines en n groupes

$$\text{(B)} \qquad \left\{ \begin{array}{lllll} x, & \theta^n x, & \theta^{2n} x, & \dots, & \theta^{\overline{m_1-1}n} x , \\ \theta x, & \theta^{1+n} x, & \theta^{1+2n} x, & \dots, & \theta^{1+\overline{m_1-1}n} x , \\ \multicolumn{5}{c}{\dotfill} \\ \theta^{n-1} x, & \theta^{n-1+n} x, & \theta^{n-1+2n} x, & \dots, & \theta^{n-1+\overline{m_1-1}n} x , \end{array} \right.$$

composés chacun de m_1 racines telles que l'équation dont les racines seraient celles de l'un quelconque d'entre eux serait également abélienne, puisque $\theta^m x = \theta^{m_1 n} x = x$.

Ces n groupes sont de plus *inséparables*(1) ; donc si nous prenons une fonction quelconque, $F(x)$, symétrique des racines du premier groupe, la somme par exemple ; auquel cas les sommes des racines des groupes suivants sont $F(\theta x), F(\theta^2 x)$, $\dots, F(\theta^{n-1} x)$; toute fonction symétrique des n quantités

$$F(x), F(\theta x), \dots, F(\theta^{n-1} x) ,$$

sera symétrique par rapport aux m racines de la proposée, et par conséquent elle pourra être exprimée en fonction rationnelle de ses coefficients. Il est donc possible de former l'équation

$$X^n + C_1 X^{n-1} + C_2 X^{n-2} + \dots + C_n = 0 \tag{14}$$

dont les racines sont ces n quantités. Et cette équation est encore abélienne : car $F(x)$ et $F(\theta x)$ sont évidemment des fonctions semblables ; on aura donc $F(\theta x) = \varphi \cdot (F x)$, φ désignant une fonction rationnelle, et par suite $F(\theta^2 x) = \varphi \cdot (F \theta x) = \varphi^2 \cdot (F x), \dots$ et $F(\theta^n x) = F(x)$.

Or (théorème II), l'équation proposée, est décomposable, à l'aide des racines de cette équation auxiliaire (14) en n équations d'un même degré m_1 dont les racines

(1) Voir le 8e théorème de notre Mémoire déjà cité ; t. VI du journal de M. Liouville, 2e série, p. 435.

sont respectivement celles de chacun des n groupes du tableau (B) ; et ces équations sont évidemment toutes abéliennes ; on peut donc les résoudre.

Mais si le nombre m_1 est lui-même composé et égal à $m_2 p$, p étant premier, on peut faire la même décomposition sur chacune de ces n équations de degré m_1. Car l'une quelconque d'entre elles, la première par exemple, étant abélienne, on peut faire sur elle ce qu'on a fait sur l'équation proposée ; et par conséquent cette équation peut être décomposée en p équations abéliennes d'un même degré m_2, à l'aide d'une nouvelle équation abélienne, de degré p, et analogue à (14), qu'il est possible de former avec les coefficients de l'équation de degré m_1, et par suite aussi avec les coefficients de l'équation proposée.

Si m_2 était lui-même un nombre composé, on pourrait, sur l'une des p équations de degré m_2, opérer la même décomposition ; et ainsi de suite. En sorte que la résolution de l'équation abélienne proposée de degré m dépend de celles d'équations abéliennes analogues à (14) dont les degrés sont les facteurs premiers de m. Ce qui démontre le théorème énoncé.

Avant de déterminer les conditions nécessaires et suffisantes pour qu'une équation irréductible soit résoluble algébriquement, nous démontrerons encore le théorème suivant, parce qu'il nous sera utile dans cette recherche.

Théorème XII.—*Si deux racines d'une équation algébrique irréductible et de degré composé m, sont tellement liées entre elles que l'une puisse s'exprimer rationnellement par l'autre, cette équation est ou abélienne ou composée d'équations abéliennes de degrés moindres ; et réciproquement.*

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 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 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 $\varphi(x) = F(x) \cdot \varphi_1(x)$, et par suite

$$F(\theta x) = \frac{\varphi_1(x)}{\psi(x)} F(x)\,. \tag{15}$$

Et j'ajoute qu'on ne saurait avoir en même temps $\psi(x) = 0$ et $F(x) = 0$, car on aurait alors $\psi(x) = F(x) \cdot \psi_1(x)$, et par conséquent les fonctions $\varphi(x)$ et $\psi(x)$ ne seraient pas des fonctions premières entre elles.

Cette équation (15) prouve que toute racine de l'équation proposée $F(x) = 0$ est racine de $F(\theta x) = 0$: mais $\theta(x)$ étant racine de $F(x) = 0$, $\theta\theta x$ ou $\theta^2 x$ est racine de la même équation : de même $\theta^2(x)$ étant racine de la proposée, $\theta\theta^2$ ou $\theta^3 x$ est encore racine de la même équation ; et ainsi de suite à l'infini. Donc chacun des termes de la suite, prolongée indéfiniment,

$$x, \quad \theta x, \quad \theta^2 x, \quad \theta^3 x, \quad \ldots, \quad \theta^{n-1} x, \quad \theta^n x, \ldots$$

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

Soit

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

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 précédente sont

$$x, \quad \theta x, \quad \theta^2 x, \quad \ldots, \quad \theta^{n-1} x\,; \tag{16}$$

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

Supposons actuellement $m > n$, et soit x_1 une des racines de l'équation $F(x) = 0$, non comprise dans la suite (16). On démontrera, de la même manière, que chaque terme de la suite prolongée indéfiniment

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

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

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

Je dis de plus que ces termes sont différents de ceux de la suite (16). Car si on pouvait avoir $\theta^h x_1 = \theta^k x$, 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 se trouverait, et que par conséquent elle contiendrait tous les termes de la suite (16) ; 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 (16).

Ainsi, ces deux suites contiennent $2n$ racines distinctes de l'équation proposée ; donc si $m = 2n$, cette équation est formée de deux équations, d'un même degré n, donnant l'une les racines de la suite (16), et l'autre celles de la dernière suite, chacune d'elles étant évidemment abéliennes.

Si $m > 2n$, et si x_2 désigne une racine de $F(x) = 0$ qui ne fasse partie ni de la suite (16) ni de la suivante composée d'un même nombre n de termes, on démontrera de la même manière qu'avec x_2 on formera un troisième groupe n de racines différentes

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

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, de n racines

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

ces groupes étant tels que, dans chacun, chaque racine est égale à la *même* fonction rationnelle θ de la précédente.

Corollaire.—Si le degré m de l'équation proposée $F(x) = 0$ est un nombre premier, les groupes du tableau (B) se réduisent en un seul. Car dans la suite (16), on a $\theta^n(x) = x$, et si $n < m$ il y aurait au moins $2n$ racines distinctes dans cette équation, ce qui est impossible, puisque m est premier. Donc $m = n$ et par conséquent tous ces groupes (B) se réduisent au premier.

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

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

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 algébrique, 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 XIII.—*Pour qu'une équation algébrique, non abélienne, irréductible et de degré premier n supérieur à trois soit résoluble algébriquement, il faut et il suffit qu'entre trois quelconques de ses racines il y ait la relation*

$$x_{a+p\rho} = \theta(x_{a+p}, \quad x_a)\,, \tag{17}$$

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

Cette relation montre comment, deux racines x_a et x_{a+p} étant données, on peut exprimer de proche en proche les $n-2$ autres racines en fonction de ces deux-là ; et comment ces racines naissent les unes des autres. Car cette relation étant vraie quand on remplace successivement p par $1, 2, 3, \ldots, n-1$, dans tel ordre qu'on voudra, et les résidus à n de la suite $p\rho, p\rho^2, \ldots, p\rho^{n-1}$ étant ces mêmes nombres dans un ordre déterminé, on peut remplacer dans cette formule (17) p successivement par $p\rho, p\rho^2, \ldots, p\rho^{n-2}$: et nous aurons les $n-1$ autres racines de l'équation à résoudre

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

* The duplication of the tag (B) appears to be intentional : *cf* page 29

Cela posé : si l'équation proposée est abélienne, elle est résoluble algébriquement, théorème X ; mais par hypothèse, cette équation n'étant pas abélienne, étant irréductible et de degré premier n, sa résolution dépend essentiellement, théorème VII, de celle de deux équations, l'une de degré $n-1$, l'autre de degré $1 \cdot 2 \cdot 3 \cdots (n-2)$.*

Mais, n étant premier et supérieur à trois, cette dernière équation, qui est l'équation résolvante dont l'expression générale y de ses racines est donnée par la formule (9), est indécomposable en équations de degrés moindres, son degré étant supérieur à 4, comme nous l'avons démontré au théorème IX. Donc, l'équation proposée devant être soluble par radicaux, cette équation résolvante doit avoir toutes ses racines égales ; puisque toute autre hypothèse la rendrait décomposable en équations de degrés moindres.

Or, cette fonction rationnelle (9) des racines $x_a, x_{a+p}, \ldots, x_{a+\overline{n-1}p}$ de l'équation proposée jouit de cette propriété, *telle qu'elle est faite*, d'être invariable pour les $n(n-1)$ permutations qui constituent un seul et même ordre de ces n racines vu successivement de chacune d'elles ; et comme elle doit être encore invariable pour les $1 \cdot 2 \cdot 3 \cdot \cdots (n-2)$ groupes de la troisième classification déjà citée de notre mémoire, cette fonction (9) doit être symétrique par rapport aux n racines de la proposée. Mais $n(n-1)$ est précisément égal au nombre d'arrangements de n lettres prises deux à deux ; donc cette expression (9) doit se réduire, d'une manière rationnelle, à ne contenir que deux de ces racines. Cette réduction exige donc que, deux racines quelconques de l'équation proposée étant données, x_a et x_{a+p} par exemple, on puisse exprimer par des fonctions rationnelles les $n-2$ autres. Par suite 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

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

ψ désignant une fonction rationnelle.

Mais $z_2, z_3, \ldots, z_{n-1}$ se déduisent de z_1 en changeant successivement p en $p\rho, p\rho^2, \ldots, p\rho^{n-2}$, et ces changements n'altèrent pas y, on doit donc avoir

$$\begin{aligned} z_2 &= \psi(x_{a+p\rho}, \quad x_a), \\ z_3 &= \psi(x_{a+p\rho^2}, \quad x_a), \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ z_{n-1} &= \psi(x_{a+p\rho^{n-2}}, x_a); \end{aligned}$$

équations qui exigent que l'on ait l'équation (17), puisque la valeur de z_1 aurait pu être écrite de la manière suivante :

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

Cette équation (17) étant nécessaire, démontrons maintenant qu'elle est suffisante. Considérons à cet effet la fonction de Lagrange :

$$u = \left\{\psi(x_{a+p}, x_a) + \lambda\psi(x_{a+p\rho}, x_a) + \cdots + \lambda^{n-2}\psi(x_{a+p\rho^{n-2}}, x_a)\right\}^{n-1} ,$$

* Original has $1, 2, 3, \ldots, (n-2)$

dans laquelle λ désigne une des racines de l'équation binôme $x^{n-1} = 1$. En y changeant successivement p en $p\rho, p\rho^2, \dots, p\rho^{n-2}$, ses divers termes ne font que se déplacer circulairement ; elle est donc invariable quelle que soit la valeur de p : d'ailleurs ses divers termes sont aussi invariables quelle que soit la valeur de a, donc cette fonction conserve la même valeur quelles que soient les n valeurs de a et les $n-1$ valeurs de p. De là il suit que si on réduit la fonction u à ne contenir que les deux racines x_a, x_{a+p} à l'aide de la formule (17),

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

cette fonction, ainsi réduite, conservera la même valeur quels que soient les indices a et p, et 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 $f(x)$ et de la fonction connue θ ; et par suite, en remplaçant successivement λ par les $n-1$ racines $1, \lambda, \lambda_2, \dots, \lambda_{n-2}$ de l'équation $x^{n-1} = 1$, on aura les $n-1$ équations

$$\text{(18)}\qquad \begin{cases} \psi(x_{a+p}, x_a) + \psi(x_{a+p\rho}, x_a) + \dots + \psi(x_{a+p\rho^{n-2}}, x_a) = \sqrt[n-1]{u_1}\,, \\ \psi(x_{a+p}, x_a) + \lambda_1\psi(x_{a+p\rho}, x_a) + \dots + \lambda_1^{n-2}\psi(x_{a+p\rho^{n-2}}, x_a) = \sqrt[n-1]{u_2}\,, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \psi(x_{a+p}, x_a) + \lambda_{n-2}\psi(x_{a+p\rho}, x_a) + \dots + \lambda_{n-2}^{n-2}\psi(x_{a+p\rho^{n-2}}, x_a) = \sqrt[n-1]{u_{n-1}}\,; \end{cases}$$

$u_1, u_2, \dots, u_{n-1}$ désignant des fonctions rationnelles et connues des coefficients de $f(x)$ et de θ : de ces $n-1$ équations nous déduirons les $n-1$ termes dont se compose la fonction u.

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

$$x_a + x_{a+p} + x_{a+2p} + \dots + x_{a+\overline{n-1}p} = -A_1\,,$$

feront connaître les n racines cherchées ; puisque ces n équations simultanées ne sont autres que les équations (18).

Ainsi, cette relation (17) est suffisante ; de là la démonstration du théorème énoncé.

Remarque.—Il est utile d'observer que les $n-1$ valeurs $z_1, z_2, \dots, z_{n-1}$ sont les racines d'une équation abélienne résoluble par l'extraction d'un seul radical d'indice $n-1$. Donc les racines de toute équation, de degré premier n, et soluble par radicaux, ne contiennent que le radical d'indice n et ceux dont les radicaux sont les facteurs premiers de $n-1$.

Corollaire I.—Si on divise le premier membre $f(x)$ de toute équation irréductible, de degré premier, non abélienne et soluble par radicaux, par un de ses facteurs linéaires, le quotient égalé à zéro est une équation abélienne.

Car l'équation $f(x) = 0$ étant soluble par radicaux, irréductible, de degré premier n, est abélienne, la relation (17) est satisfaite ; et le quotient de $f(x)$ 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 on déduit de cette relation les équations

$$\begin{aligned}
x_{a+p\rho} &= \theta(x_{a+p}, x_a) = \theta x_{a+p}\,,\\
x_{a+p\rho^2} &= \theta x_{a+p\rho} = \theta^2 x_{a+p}\,,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
x_{a+p\rho^{n-2}} &= \theta x_{a+p\rho^{n-3}} = \theta^{n-2} x_{a+p}\,,\\
x_{a+p\rho^{n-1}} &= x_{a+p} = \theta x_{a+p\rho^{n-2}} = \theta^{n-1} x_{a+p}\,,
\end{aligned}$$

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.—Il résulte du théorème X et de celui que nous venons de démontrer, ce résultat : *les seules équations algébriques, irréductibles et de degré premier supérieur à trois qui soient solubles par radicaux, sont celles qui sont abéliennes ou celles dont les racines satisfont à l'équation* (17).

Et il est utile de rappeler le résultat du corollaire du théorème XII : pour qu'une équation irréductible et de degré premier soit abélienne, il faut et il suffit que deux quelconques de ses racines soient tellement liées entre elles que l'une puisse être exprimée rationnellement par l'autre.

Théorème XIV.—*Pour qu'une équation algébrique, irréductible et dont le degré composé ne contient aucun des facteurs premiers deux et trois soit résoluble algébriquement, il faut et il suffit : 1º ou que deux quelconques de ces racines soient tellement liées entre elles que l'une puisse s'exprimer rationnellement par l'autre ; et que si θx et $\theta_1 x$ désignent deux de ces racines distinctes exprimées l'une et l'autre en fonction rationnelle d'une troisième x, on ait $\theta\theta_1 x = \theta_1\theta x$; 2º ou que le degré de l'équation soit de la forme n^v, n étant premier, et que trois de ses racines quelconques soient liées par la relation*

$$x_{a+\alpha p\rho,\ b+\beta q\rho,\ \ldots,\ l+\lambda t\rho} = \theta(x_{a+\alpha p,\ b+\beta q,\ \ldots,\ l+\lambda t}, \qquad x_{a,b,\ldots,l})\,, \tag{18a*}$$

dans laquelle les indices de x sont pris suivant le module n ; θ désignant une fonction rationnelle ; ρ une des racines primitives de n ; $a, b, \ldots, l$, v indices indépendants et prenant chacun les n valeurs $0, 1, 2, \ldots, n-1$; $p, q, \ldots, t$, v nouveaux indices indépendants et prenant chacun les $n-1$ valeurs $1, 2, 3, \ldots, n-1$; et enfin $\alpha, \beta, \ldots, \lambda$ les nombres 0 *ou* 1.

Si l'équation proposée $f(x) = 0$ est abélienne, elle est résoluble algébriquement, théorème X. Si elle ne l'est pas, nous distinguerons plusieurs cas pour la recherche des conditions nécessaires et suffisantes de sa résolution : celui où son degré n est égal au produit de deux facteurs premiers, celui où ce degré est égal au produit de trois facteurs premiers, et ainsi de suite ; chacun de ces facteurs premiers étant supérieur à trois.

* Duplicate tag (18)—see page 34

Premier cas général : $m = nn_1$.

L'équation proposée $f(x) = 0$ étant irréductible, sa résolution dépend nécessairement, théorème VIII, de la résolution de n équations, d'un même degré n_1 dont les nn_1 racines sont celles de la proposée, équations qu'on peut former avec les coefficients de l'équation donnée et avec les racines de deux autres équations, l'une de degré $n-1$, l'autre d'un degré déterminé s. Cette dernière peut être formée directement avec les seuls coefficients de $f(x) = 0$, et celle de degré $n-1$ avec ces mêmes coefficients et avec l'une des racines de cette équation de degré s. Mais n_1 est un nombre premier supérieur à trois, donc la résolution d'une quelconque des n équations de ce degré n_1 exige, théorème VII, ou que cette équation soit abélienne, ou que les n_1 racines soient liées par une relation analogue à l'équation (17) ; de là deux hypothèses :

Première hypothèse.—Si l'une quelconque de ces équations de degré n_1 est abélienne, une quelconque de ses racines est une fonction rationnelle d'une autre de ces mêmes racines ; mais toutes ces racines appartiennent à l'équation proposée $F(x) = 0$, donc, théorème VI, les nn_1 racines de cette dernière se partagent en n groupes composés chacun de n_1 racines, comme on le fait au tableau (B) dans lequel n doit être remplacé par n_1 ; et par conséquent $\theta^{n_1}x = x$. Or, il résulte de ce même théorème, que les n groupes de ce tableau doivent se réduire à un seul ou qu'ils doivent être distincts. Dans le premier cas n_1 doit être remplacé par m dans cette dernière équation. Dans le second cas, l'équation proposée $F(x) = 0$ est *abélienne*, le même théorème VI prouve que $x_1 = \theta_1 x$, $\theta_1(x)$ désignant une fonction de x telle que $\theta_1^n(x) = x$ puisque n est premier ; elle doit être différente de θ puisque cette équation n'a pas de racines égales ; et qu'enfin $x_2 = \theta_1^2(x)$, $x_3 = \theta_1^3(x)$, $x_4 = \theta_1^4(x)$, …, $x_{n-1} = \theta_1^{n-1}(x)$. Avec ces résultats, le tableau (B) devient

$$
\text{(C)} \qquad \left\{
\begin{array}{lllll}
x, & \theta x, & \theta^2 x, & \ldots, & \theta^{n_1-1}x\,, \\
\theta_1 x, & \theta\theta_1 x, & \theta^2\theta_1 x, & \ldots, & \theta^{n_1-1}\theta_1 x\,, \\
\theta_1^2 x, & \theta\theta_1^2 x, & \theta^2\theta_1^2 x, & \ldots, & \theta^{n_1-1}\theta_1^2 x\,, \\
\multicolumn{5}{c}{\dotfill} \\
\theta_1^{n-1}x, & \theta\theta_1^{n-1}x, & \theta^2\theta_1^{n-1}x, & \ldots, & \theta^{n_1-1}\theta_1^{n-1}x\,.
\end{array}
\right.
$$

Or, chaque racine de l'équation résolvante $\varphi(y) = 0$ décompose, à l'aide d'une équation auxiliaire de degré $n-1$, théorème VIII, l'équation proposée en n équations abéliennes d'un même degré n_1. Il y a donc autant de valeurs de y qu'il y a de manières de décomposer cette équation en n équations abéliennes. Mais avec les fonctions θ et θ_1 il n'y a évidemment qu'une seule manière d'opérer cette décomposition, chacun des nombres n et n_1 étant premier ; donc l'équation résolvante $\varphi(y) = 0$ est du premier degré ; et, par suite, la fonction y (13) qui peut être exprimée, tableau (C), rationnellement en x avec les fonctions θ et θ_1, doit être une fonction symétrique, théorème II, des racines de l'équation proposée. De plus, les divers termes de y, exprimés en x, se réduisent évidemment à un seul Z_1, en sorte que l'on aura

$$y = Z_1 = \psi(x)\,,$$

$\psi(x)$ étant une fonction symétrique des racines de $f(x) = 0$. Ainsi, cette fonction doit conserver une même valeur quand on y remplace x par une quelconque des racines de cette équation.

Or, d'après l'expression de Z_1, et la signification des n quantités $X_a, X_{a+p}, \ldots, X_{a+\overline{n-1}p}$ qui désignent respectivement la somme des racines contenues dans chacun des n groupes du tableau (C), cette expression Z_1 ou $\psi(x)$ n'est invariable qu'en échangeant toutes les racines contenues dans chacune de ces quantités, les unes dans les autres, et que par les permutations circulaires de ces mêmes quantités, en nombre n. Mais toutes les racines du tableau (C) dépendent d'une seule x, il faut donc qu'en échangeant x en une quelconque des racines d'un des groupes, du premier par exemple, changement qui laisse invariable X_a, cet échange laisse aussi invariable chacune des autres quantités $X_{a+p}, \ldots, X_{a+\overline{n-1}p}$. Et il faut de plus qu'en changeant x en une quelconque des racines d'un autre groupe, du second par exemple, les quantités $X_a, X_{a+p}, \ldots, X_{a+\overline{n-1}p}$, se changent respectivement en $X_{a+p}, X_{a+2p}, \ldots, X_a$, changement qui laisse en effet invariable $\psi(x)$. En d'autres termes, il faut nécessairement que les n groupes du tableau (C) soient *inséparables.*

Or, en changeant par exemple x en θx, les divers termes du premier groupe ne font que se déplacer, et ceux du deuxième deviennent

$$\theta_1\theta x, \quad \theta\theta_1\theta x, \quad \theta^2\theta_1\theta x, \quad \ldots, \quad \theta^{n_1-1}\theta_1\theta x\,;$$

et comme ces derniers termes ne doivent aussi que se déplacer, on doit avoir $\theta_1\theta x = \theta\theta_1 x$.

Ainsi, si $m = nn_1$, les conditions énoncées dans le premier cas sont nécessaires.

Démontrons actuellement qu'elles sont suffisantes. En effet, si elles sont satisfaites, on a $\theta_1\theta x = \theta\theta_1 x$, et par conséquent $\theta^2\theta_1 x = \theta\theta_1\theta x = \theta_1\theta^2 x$, $\theta^2\theta_1\theta x = \theta\theta\theta_1\theta x = \theta\theta_1\theta^2 x = \theta_1\theta^3 x$, et ainsi de suite ; en sorte que le tableau (C) devient

$$(\mathrm{D}_1) \qquad \left\{ \begin{array}{lllll} x, & \theta x, & \theta^2 x, & \ldots, & \theta^{n_1-1}x\,, \\ \theta_1 x, & \theta_1\theta x, & \theta_1\theta^2 x, & \ldots, & \theta_1\theta^{n_1-1}x\,, \\ \multicolumn{5}{c}{\dotfill} \\ \theta_1^{n-1}x, & \theta_1^{n-1}\theta x, & \theta_1^{n-1}\theta^2 x, & \ldots, & \theta_1^{n-1}\theta^{n_1-1}x\,. \end{array} \right.$$

Et il est évidemment tel que ces n groupes sont inséparables, et que si par exemple le premier se change en le second pour un changement, le second se changera en le troisième, le troisième en le quatrième, ..., et le dernier en le premier, par suite du même changement. De plus, si on échange entre elles deux racines quelconques d'un de ces groupes, on voit que les termes de ce groupe ne font que se déplacer. Donc, pour tout changement, ces groupes sont inséparables ou ne produisent que des permutations circulaires. Mais tous ces changements font acquérir une même valeur à y ou $\psi(x)$; donc $\psi(x)$ est invariable quand on y remplace successivement x par une quelconque des m racines de l'équation proposée, $f(x) = 0$. Admettons qu'on ait effectué ces substitutions dans cette fonction comme $\psi(x)$ et qu'on ait fait la somme, le résultat $\Sigma\psi(x)$ sera une fonction symétrique des racines de cette équation et par conséquent exprimable en fonction rationnelle de ses coefficients ; et on aura

$$y = \frac{1}{m}\sum\psi(x)\,.$$

La fonction résolvante y étant connue pour la racine α de l'équation binôme $x^n - 1 = 0$, on pourra déterminer, de la même manière, sa valeur pour chacune des $n - 1$ autres racines de cette équation binôme : et en extrayant la racine n^{e} de chacune de ces valeurs, on aura n équations linéaires par rapport aux n quantités $X_a, X_{a+p}, \ldots, X_{a+\overline{n-1}p}$, analogues aux équations (11).

De ces n équations nous déduirons ces n inconnues ; et, comme dans le théorème VIII, nous pourrons former, avec chacune d'elles, les n équations dont les racines sont respectivement celles de chacun des n groupes du tableau précédent. Mais ces équations dernières sont abéliennes ; elles sont donc solubles par radicaux, théorème X ; ce qui fera connaître les m racines de l'équation proposée.

Donc enfin, quand $m = nn_1$, les conditions énoncées en premier lieu sont nécessaires et suffisantes.

Seconde hypothèse.—Soit $m = nn_1$, et supposons que les n_1 racines de chacune des n équations, en lesquelles doit être décomposée l'équation proposée et irréductible $F(x) = 0$ à l'aide des racines de deux équations de degrés $n - 1$ et s, soient liées par une relation analogue à (17). Il suffira, à cet effet, que l'on ait l'équation

$$x_{a+p\rho,\, b} = \theta(x_{a+p,\, b}, \quad x_{a,\, b}) \tag{19}$$

quelle que soit la valeur de b, dans laquelle ρ désigne une racine primitive de n. Car le symbole $x_{a,\, b}$ peut représenter les nn_1 racines de $F(x) = 0$ d'après les hypothèses faites sur a et b, a prenant en effet les valeurs $0, 1, 2, \ldots, n_1 - 1$, et b les valeurs $0, 1, 2, \ldots, n - 1$; les indices de x étant d'ailleurs pris respectivement suivant les modules n_1 et n. Nous appellerons racines *conjuguées* les n_1 racines que produit l'équation (19), $x_{a+p,\, b}$ et $x_{a,\, b}$ comprises, en changeant successivement p en $p\rho, p\rho^2, \ldots, p\rho^{n_1-2}$, et relatives à l'une des n valeurs de b.

Cela posé, écrivons sur des lignes horizontales les racines conjuguées de ces n équations ; on aura le tableau suivant, en observant que les résidus à n des n valeurs de b sont les mêmes, à la disposition près, que ceux de $b, b + q, b + q\rho, \ldots, b + q\rho^{n-2}$ par rapport à n, b étant un nombre entier quelconque inférieur à n,

$$\text{(E)} \quad \left\{ \begin{array}{lllll} x_{a,\, b} & x_{a+p,\, b} & x_{a+p\rho,\, b} & \cdots & x_{a+p\rho^{n_1-2},\, b} \\ x_{a,\, b+q} & x_{a+p,\, b+q} & x_{a+p\rho,\, b+q} & \cdots & x_{a+p\rho^{n_1-2},\, b+q} \\ x_{a,\, b+q\rho} & x_{a+p,\, b+q\rho} & x_{a+p\rho,\, b+q\rho} & \cdots & x_{a+p\rho^{n_1-2},\, b+q\rho} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{a,\, b+q\rho^{n-2}} & x_{a+p,\, b+q\rho^{n-2}} & x_{a+p\rho,\, b+q\rho^{n-2}} & \cdots & x_{a+p\rho^{n_1-2},\, b+q\rho^{n-2}} \end{array} \right. ;$$

dans ce tableau le ρ qui a pour coefficient q désigne une des racines primitives de n.

Or, chacune des racines de l'équation $F(x) = 0$ a le même caractère, celui de satisfaire à cette équation et qui seul doit servir à les déterminer, puisqu'elle est irréductible : mais, par hypothèse, les nn_1 racines de cette équation se partagent en n groupes écrits en ligne horizontale, et composés chacun de n_1 racines conjuguées ; chacun de ces groupes étant relatifs à une même valeur de l'indice b et à des valeurs différentes de l'indice a. Donc, n étant premier comme n_1, tout ce qui est vrai pour les indices b et a doit être vrai pour les indices a et b ; et par suite dans chaque colonne verticale il doit y avoir, en intervertissant, s'il le faut, l'ordre des lignes horizontales, des racines *conjuguées* et en *même* nombre : d'où il suit que $n = n_1$ et par conséquent $m = n^2$. Et de plus on doit avoir

$$x_{a,\,b+q\rho} = \theta(x_{a,\,b+q}, \quad x_{a,\,b})\,, \tag{20}$$

relation analogue à (19) ; et toutes deux étant évidemment comprises dans (18a) en n'y prenant que deux indices a et b, et en y faisant successivement $\beta = 0, \alpha = 1$; et $\beta = 1, \alpha = 0$.

Ainsi, dans le cas où le degré m de $F(x) = 0$ est égal au produit de deux facteurs premiers supérieurs à trois, il faut que, si les conditions énoncées en premier lieu ne sont pas satisfaites, celles énoncées en deuxième lieu le soient.

Nous allons démontrer actuellement que ces dernières sont suffisantes. Cherchons d'abord le degré s de l'équation résolvante $\varphi(y) = 0$: ce degré est donné par la formule (22), quand les racines n'ont entre elles aucune relation ; mais dans le cas actuel, ce degré est moindre et égal à l'unité, et la valeur unique de y est une fonction symétrique des racines de $F(x) = 0$.

En effet, chaque racine de $\varphi(y) = 0$ décompose, à l'aide des racines d'une équation auxiliaire de degré $n-1$, théorème IX, l'équation proposée $F(x) = 0$ en n équations d'un même degré n, dont les racines, pour chacune d'elles, sont *conjuguées.* Il y aura donc autant de valeurs de y qu'il y a de manières de décomposer les n^2 racines de $F(x) = 0$ en n systèmes composés chacun de n racines conjuguées.

Pour effectuer ces décompositions, admettons que dans le tableau (E) $n_1 = n$, et que dans chacune des colonnes horizontales et verticales, les racines soient écrites dans l'ordre où elles naissent des relations (19) et (20), vraies par hypothèse. Écrivons d'abord ces n^2 racines, en les prenant de gauche à droite dans le tableau (E), sur une circonférence de cercle et à égales distances les unes des autres ; et considérons le polygone régulier qui est relatif à cette disposition, ainsi que ceux qui s'en déduisent par le procédé de l'intervalle constant, au nombre de $n(n-1)$. Nous avons démontré(1) que tous ces polygones, en ne considérant d'abord que les idées d'ordre et de disposition, n'étaient qu'un seul et même polygone, qu'un seul et même ordre ; et que les côtés de ces mêmes polygones, en faisant intervenir les idées de grandeur, étaient donnés par une *même* équation algébrique.

Il résulte donc de là que tous ces polygones jouissent des mêmes propriétés ; et que par conséquent chacun d'eux sera en général composé, comme le premier, de n systèmes de n racines conjuguées chacun. Mais, dans le cas actuel, deux racines d'un de ces systèmes suffisent, théorème XIII, pour déterminer les $n-2$ autres ; donc la valeur de l'intervalle constant, qui amènera dans les n premières racines du polygone relatif à cette valeur deux quelconques des n racines conjuguées d'une des colonnes horizontales ou verticales du tableau (E), fournira un polygone qui ne sera pas composé de n systèmes formés chacun de n racines conjuguées. Et les seuls polygones, jouissant de cette propriété, seront ceux qui sont produits par les valeurs de h qui n'amèneront dans aucun des n systèmes deux quelconques des racines d'un des systèmes conjugués de ce tableau (E).

Or, si l'on prend $h = n+1$, c'est-à-dire si l'on saute, à partir de $x_{a,\,b}$ de $n+1$ en $n+1$ dans le polygone primitif ; on passera, pour les n premières racines,

(1) *Journal de Mathématiques* publié par M. Liouville ; théorème I, février 1865.

successivement sur une racine des 2e, 3e, …, ne lignes horizontales de (E) : il en est de même pour les n racines suivantes, ainsi que pour les autres considérées de n en n. Donc l'intervalle $h = n + 1$ produit un nouveau polygone formé, comme le premier, de n nouveaux systèmes de n racines conjuguées chacun.

Si généralement l'on prend $h = kn + 1$, k étant un entier inférieur à n et si l'on observe que, n étant premier, les résidus à n de $k, 2k, \ldots, (n-1)k$ sont les nombres $1, 2, \ldots, n-1$, dans un ordre déterminé(1) ; avec cette valeur h on passera également sur chacune des n lignes horizontales de (E), et on ne prendra qu'une racine de chacune de ces lignes : il en sera de même pour les n racines suivantes, ainsi que pour les autres considérées de n en n. Donc ce nouvel intervalle produira un nouveau polygone formé, comme les deux premiers, de n nouveaux systèmes de n racines conjuguées chacun. Et comme ce résultat est vrai quelle que soit la valeur de k, il en résulte, qu'avec cette disposition première des n^2 racines de $F(x) = 0$, on obtient, le polygone primitif et correspondant à cette disposition étant compris, n systèmes différents formés chacun de n racines conjuguées.

Mais si l'on prend pour h toute autre valeur, 2 par exemple, on ne passerait pas évidemment, pour les n premières racines du polygone correspondant à cette valeur, sur une racine de chacune des lignes horizontales de (E) ; dans ces n premières racines se trouveraient nécessairement deux racines au moins d'une de ces lignes avec des racines étrangères à cette même ligne ; et dès lors ces n racines ne seraient pas conjuguées. Il en serait de même pour toute autre valeur de h. On obtient donc seulement, avec cette première disposition, n systèmes différents composés chacun de n racines conjuguées.

Écrivons actuellement les n^2 racines de (E) en allant de haut en bas et en commençant par la gauche, sur une circonférence de cercle ; et considérons le polygone qui est relatif à cette disposition nouvelle. Il est, par hypothèse, formé de n nouveaux systèmes de n racines conjuguées chacun ; et si l'on forme les $n-1$ autres polygones qui seuls, d'après ce qui précède, jouissent de la même propriété, on trouve qu'ils ne produisent rien de nouveau. Car, dans les n premières racines de ces n polygones, se trouvent nécessairement toutes les racines de $F(x) = 0$: mais ces n polygones se déduisent des n premiers que nous avons obtenus en échangeant entre eux les indices a et b, donc cette nouvelle disposition ne produit qu'*un* nouveau polygone composé, comme les n premiers, de n systèmes de n racines conjuguées chacun. Donc enfin les n^2 racines de l'équation proposée, se partagent seulement de $n+1 = (n^2-1) : (n-1)$ manières différentes en n systèmes composés chacun de n racines conjuguées.

Si l'on forme ces $n + 1$ décompositions, on obtient les $n + 1$ tableaux suivants :

$$(\mathrm{E}_1) \qquad \left\{\begin{array}{lllll}
x_{a,\,b} & x_{a+p,\,b} & x_{a+p\rho,\,b} & \cdots & x_{a+p\rho^{n-2},\,b} \\
x_{a,\,b+q} & x_{a+p,\,b+q} & x_{a+p\rho,\,b+q} & \cdots & x_{a+p\rho^{n-2},\,b+q} \\
x_{a,\,b+q\rho} & x_{a+p,\,b+q\rho} & x_{a+p\rho,\,b+q\rho} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho} \\
\multicolumn{5}{c}{\dotfill} \\
x_{a,\,b+q\rho^{n-2}} & x_{a+p,\,b+q\rho^{n-2}} & x_{a+p\rho,\,b+q\rho^{n-2}} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-2}}
\end{array}\right.$$

(1) En effet, n étant premier, et p étant inférieur à n, pk n'est pas divisible par n ; et si les résidus à n de pk et de $p'k$ étaient égaux, la différence $k(p-p')$ serait un multiple de n ; ce qui est impossible, puisque p' est aussi inférieur à n.

$$
(\mathrm{E}_2)\qquad\left\{\begin{array}{lllll}
x_{a,\,b} & x_{a+p,\,b+q} & x_{a+p\rho,\,b+q\rho} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-2}}\\
x_{a,\,b+q} & x_{a+p,\,b+q\rho} & x_{a+p\rho,\,b+q\rho^2} & \cdots & x_{a+p\rho^{n-2},\,b}\\
x_{a,\,b+q\rho} & x_{a+p,\,b+q\rho^2} & x_{a+p\rho,\,b+q\rho^3} & \cdots & x_{a+p\rho^{n-2},\,b+q}\\
\multicolumn{5}{c}{\dotfill}\\
x_{a,\,b+q\rho^{n-2}} & x_{a+p,\,b} & x_{a+p\rho,\,b+q} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-3}}
\end{array}\right.
$$

$$
(\mathrm{E}_3)\qquad\left\{\begin{array}{lllll}
x_{a,\,b} & x_{a+p,\,b+q\rho} & x_{a+p\rho,\,b+q\rho^3} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-3}}\\
x_{a,\,b+q} & x_{a+p,\,b+q\rho^2} & x_{a+p\rho,\,b+q\rho^4} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-2}}\\
\multicolumn{5}{c}{\dotfill}\\
x_{a,\,b+q\rho^{n-2}} & x_{a+p,\,b+q} & x_{a+p\rho,\,b+q\rho^2} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-4}}
\end{array}\right.
$$

. . . .

$$
(\mathrm{E}_n)\qquad\left\{\begin{array}{lllll}
x_{a,\,b} & x_{a+p,\,b+q\rho^{n-2}} & x_{a+p\rho,\,b+q\rho^{n-3}} & \cdots & x_{a+p\rho^{n-2},\,b+q}\\
x_{a,\,b+q} & x_{a+p,\,b} & x_{a+p\rho,\,b+q\rho^{n-2}} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho}\\
\multicolumn{5}{c}{\dotfill}\\
x_{a,\,b+q\rho^{n-2}} & x_{a+p,\,b+q\rho^{n-3}} & x_{a+p\rho,\,b+q\rho^{n-4}} & \cdots & x_{a+p\rho^{n-2},\,b}
\end{array}\right.
$$

$$
(\mathrm{E}_{n+1})\qquad\left\{\begin{array}{lllll}
x_{a,\,b} & x_{a,\,b+q} & x_{a,\,b+q\rho} & \cdots & x_{a,\,b+q\rho^{n-2}}\\
x_{a+p,\,b} & x_{a+p,\,b+q} & x_{a+p,\,b+q\rho} & \cdots & x_{a+p,\,b+q\rho^{n-2}}\\
x_{a+p\rho,\,b} & x_{a+p\rho,\,b+q} & x_{a+p\rho,\,b+q\rho} & \cdots & x_{a+p\rho,\,b+q\rho^{n-2}}\\
\multicolumn{5}{c}{\dotfill}\\
x_{a+p\rho^{n-2},\,b} & x_{a+p\rho^{n-2},\,b+q} & x_{a+p\rho^{n-2},\,b+q\rho} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-2}}
\end{array}\right.
$$

Il est utile de remarquer que, dans les n premiers tableaux, les racines contenues dans la première colonne verticale sont exactement les mêmes ; et que les racines contenues dans les autres colonnes verticales sont respectivement les permutations *circulaires* les unes des autres.

Cela posé : pour former la fonction résolvante y, définie par l'équation (11) et relative à chacune de ces $n+1$ décompositions, l'on doit prendre pour chacune des quantités $X_a, X_{a+p}, \ldots, X_{a+\overline{n-1}p}$ n racines quelconques de l'équation proposée $F(x) = 0$. Or, si l'on prend successivement pour X_a la somme des racines de la première colonne verticale des n premiers tableaux et la somme de celles de la première colonne horizontale du dernier, X_a conservera une même valeur pour ces $n+1$ décompositions. De même, si l'on prend successivement pour X_{a+p} la somme des racines qui forment la deuxième colonne verticale des n premiers tableaux et la somme de celles de la deuxième colonne horizontale du dernier, X_{a+p} conservera une même valeur pour ces mêmes $n+1$ décompositions ; et ainsi de suite. Enfin, si l'on prend successivement pour $X_{a+\overline{n-1}p}$ la somme des racines de la dernière colonne verticale des n premiers tableaux et la somme de celles de la dernière colonne horizontale du dernier, $X_{a+\overline{n-1}p}$ sera également invariable pour ces mêmes $n+1$ décompositions. Donc les fonctions $Z_1, Z_2, \ldots, Z_{n-1}$ et la fonction résolvante y relatives à chacune de ces $n+1$ décompositions conservent une *même* valeur puisqu'elles ne sont formées que de ces n quantités $X_a, X_{a+p}, \ldots, X_{a+\overline{n-1}p}$. Ainsi, quoiqu'il y ait $n+1$ décompositions, y n'a cependant qu'une *seule* valeur, et par conséquent l'équation résolvante $\varphi(y) = 0$ est du premier degré. Ce résultat pouvait d'ailleurs être prévu ; puisque, d'après ce qui a été démontré au 2° du théorème IX, l'équation résolvante $\varphi(y) = 0$ est indécomposable.

Démontrons enfin que cette valeur unique de y peut être exprimée en fonction rationnelle des coefficients de l'équation proposée et de la fonction connue θ ; et qu'à l'aide de cette valeur y on peut obtenir ses n^2 racines.

En effet, toutes ces racines et aussi la fonction y peuvent d'abord être exprimées en fonction rationnelle des n racines

$$x_{a,\,b}, \quad x_{a+p,\,b+q}, \quad x_{a+p,\,b+q\rho}, \quad \ldots, \quad x_{a+p,\,b+q\rho^{n-2}}$$

qui évidemment ne sont pas conjuguées. Car la première colonne horizontale des 2ᵉ, 3ᵉ, …, nᵉ tableaux donnent respectivement

$$\begin{aligned}
x_{a+p\rho,\,b+q\rho} &= \theta(x_{a+p,\,b+q}, \quad x_{a,\,b}), \quad \ldots, \\
&\qquad x_{a+p\rho^{n-2},\,b+q\rho^{n-2}} = \theta(x_{a+p\rho^{n-3},\,b+q\rho^{n-3}},\ x_{a,\,b}), \\
x_{a+p\rho,\,b+q\rho^2} &= \theta(x_{a+p,\,b+q\rho}, \quad x_{a,\,b}), \quad \ldots, \\
&\qquad x_{a+p\rho^{n-2},\,b+q\rho^{n-3}} = \theta(x_{a+p\rho^{n-3},\,b+q\rho^{n-5}},\ x_{a,\,b}), \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
x_{a+p\rho,\,b+q\rho^{n-3}} &= \theta(x_{a+p,\,b+q\rho^{n-2}},\ x_{a,\,b}), \quad \ldots, \\
&\qquad x_{a+p\rho^{n-2},\,b+q} = \theta(x_{a+p\rho^{n-3},\,b+q\rho}, \quad x_{a,\,b}).
\end{aligned}$$

Avec ces équations les n^2 racines de l'équation proposée $F(x) = 0$ peuvent être exprimées en fonction rationnelle de ces n racines non conjuguées, à l'exception des $n-1$ racines

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

et des $n-1$ autres

$$x_{a,\,b+q}, \quad x_{a,\,b+q\rho}, \quad \ldots, \quad x_{a,\,b+q\rho^{n-2}}, \quad x_{a+p,\,b};$$

mais chacune d'elles s'exprime rationnellement, en fonction de deux de celles que nous venons de déterminer, les $n-1$ premières à l'aide du tableau (E_1), les $n-1$ dernières à l'aide du tableau (E_{n+1}). Donc toute fonction rationnelle et connue de ces n^2 racines peut être exprimée en fonction rationnelle des n racines non conjuguées ; et, par suite, si l'on considère, non la fonction y (11), mais la fonction plus générale,

$$y_1 = (Z_1 + \lambda_1 Z_2 + \lambda_1^2 Z_3 + \cdots + \lambda_1^{n-2} Z_{n-1})^{n-1}$$

dans laquelle λ_1 désigne l'une des racines de l'équation binôme $x^{n-1} - 1 = 0$, fonction qui se réduit à y pour $\lambda_1 = 1$ et quand on en a extrait la racine $n-1$; on aura

$$y_1 = \pi\left(x_{a,\,b},\ x_{a+p,\,b+q},\ x_{a+p,\,b+q\rho},\ \ldots,\ x_{a+p,\,b+q\rho^{n-2}}\right).$$

Si l'on forme actuellement tous les arrangements n à n des n^2 racines de $F(x) = 0$, $n(n+1)$ de ces arrangements seront composés de n racines conjuguées, et tous les autres de n racines non conjuguées. Mais si l'on remplace successivement dans π les n racines qui s'y trouvent, d'abord par les $n(n+1)$ premiers arrangements et que l'on fasse la somme des résultats ; puis par tous les autres et que l'on fasse également la somme des résultats obtenus : on aura, en désignant par $\Sigma'\pi$ la première somme et par $\Sigma''\pi$ la seconde,

$$\sum{}' \pi + \sum{}'' \pi = w_1,$$

w_1 étant évidemment une fonction symétrique des n^2 racines de l'équation proposée $F(x) = 0$, et par suite exprimable en fonction rationnelle des coefficients de cette équation et de ceux de la fonction connue θ.

Mais, les n racines qui entrent dans chaque terme de $\Sigma'\pi$ sont conjuguées, elles peuvent donc être réduites, à l'aide de la fonction connue θ, à deux racines x_1, x_2 ; et on aura $\pi = \pi_1(x_1, x_2)$. Or les quantités $Z_1, Z_2, \ldots, Z_{n-1}$ sont invariables pour les $n(n+1)$ systèmes de racines conjuguées des $(n+1)$ tableaux : de plus, ces mêmes quantités sont encore invariables pour les n valeurs $0, 1, 2, \ldots, n-1$ de l'indice a, et elles se déduisent les unes des autres en changeant successivement p en les $n-1$ valeurs $p, p\rho, p\rho^2, \ldots, p\rho^{n-2}$, changements qui n'altèrent pas la fonction y_1. Donc $\Sigma'\pi = \Sigma'\pi_1(x_1, x_2)$ est invariable par les $n^2(n^2-1)$ arrangements deux à deux des n^2 racines de $F(x) = 0$, et par conséquent ce terme est symétrique de ces racines et exprimable, par suite, en fonction rationnelle des quantités connues.

De là, il suit que $\Sigma''\pi$ est aussi une fonction rationnelle et symétrique des racines de $F(x) = 0$, et par conséquent exprimable également en fonction rationnelle des quantités connues. Mais la fonction Y_1 n'a qu'une seule valeur ; donc l'égalité précédente donnera, k désignant le nombre de termes de $\Sigma''\pi$,

$$y_1 = \frac{1}{k}\left\{w_1 - \sum{}' \pi_1(x_1, x_2)\right\} = V_1\,,$$

V_1 étant une fonction connue.

Si dans cette dernière équation on remplace successivement λ_1 par chacune des $n-1$ racines de $x^{n-1} - 1 = 0$, on aura les $n-1$ équations

$$(21)\qquad \left\{\begin{array}{l} Z_1 + \lambda_1 Z_2 + \lambda_1^2 Z_3 + \cdots + \lambda_1^{n-2} Z_{n-1} = \sqrt[n-1]{v_1}\,, \\ Z_1 + \lambda_2 Z_2 + \lambda_2^2 Z_3 + \cdots + \lambda_2^{n-2} Z_{n-1} = \sqrt[n-1]{v_2}\,, \\ \dotfill \\ Z_1 + \lambda_{n-1} Z_2 + \lambda_{n-1}^2 Z_3 + \cdots + \lambda_{n-1}^{n-2} Z_{n-1} = \sqrt[n-1]{v_{n-1}}\,, \end{array}\right.$$

dont les seconds membres sont connus. De ces équations on déduira les $n-1$ quantités $Z_1, Z_2, \ldots, Z_{n-1}$ qui à leur tour fourniront, après avoir extrait la racine n^{e} de chacune d'elles, $n-1$ équations formant avec l'équation dont le second membre est connu,

$$X_a + X_{a+p} + \cdots + X_{a+\overline{n-1}p} = -A_1\,,$$

un système de n équations linéaires par rapport aux n quantités $X_a, X_{a+p}, \ldots, X_{a+\overline{n-1}p}$. De ces équations nous déduirons ces n quantités ; et, comme dans le théorème VIII, nous pourrons former avec chacune d'elles les n équations dont les racines sont toutes celles de la proposée $F(x) = 0$: équations résolubles algébriquement, puisque chacune d'elles rentre dans le théorème précédent.

Ces conditions sont donc suffisantes.

En réunissant ce résultat à celui de la première hypothèse, il est donc prouvé que, si le degré m de $F(x) = 0$ n'est composé que de deux facteurs premiers supérieurs à 3, les conditions énoncées du théorème à démontrer sont nécessaires et suffisantes.

Deuxième cas général : $m = nn_1n_2$.

L'équation proposée $F(x) = 0$ n'étant pas abélienne et étant irréductible, sa résolution dépend nécessairement, théorème VIII, de la résolution de n équations d'un même degré $n_1 \cdot n_2$, dont les m racines sont celles de la proposée ; équations que l'on peut former avec les coefficients de $F(x) = 0$ et avec les racines de deux autres équations, l'une de degré $n - 1$ et l'autre d'un degré déterminé s. Cette dernière peut être formée directement avec les coefficients seuls de $F(x) = 0$, et celle de degré $n - 1$ avec ces mêmes coefficients et avec les racines de l'équation de degré s. Mais le degré commun à ces n équations, $n_1 \cdot n_2$, est égal au produit de deux facteurs premiers supérieurs à 3, donc la résolution d'une quelconque de ces équations exige, 1er cas général déjà expliqué, ou qu'elle soit abélienne, ou que les conditions du 1° du théorème à démontrer soient satisfaites, ou enfin que ce soit celles du 2° du même théorème : de là deux hypothèses.

Première hypothèse.—Si chacune de ces n équations dont le degré est $n_1 \cdot n_2$ est abélienne, l'équation proposée ne l'étant pas, on démontre, d'une manière absolument semblable à celle qui est relative à la première hypothèse du 1er cas général, que les conditions énoncées du 1° sont nécessaires. Il suffit, en effet, de remplacer n_1 par $n_1 \cdot n_2$. Si chacune de ces n équations, de degré $n_1 \cdot n_2$, n'est pas abélienne, ces mêmes conditions du 1° sont nécessaires par hypothèse. Ainsi, dans l'un et l'autre cas, ces conditions sont nécessaires.

Pour démontrer qu'elles sont suffisantes ; il suffit, dans la démonstration relative au 1er cas général, de mettre dans le tableau (D_1) $n_1 \cdot n_2$ à la place de n_1, si chacune des n équations de degré $n_1 \cdot n_2$ est abélienne ; et de substituer à chacun des groupes de ce même tableau, un tableau analogue fait avec les facteurs n_1 et n_2, si les racines de l'équation proposée jouissent de la propriété énoncée au 1° du théorème à démontrer. Dans l'un et l'autre de ces deux cas, on obtient en effet les n équations, d'un même degré $n_1 \cdot n_2$; et ces dernières sont solubles par suite de nos hypothèses, à l'aide du procédé de la première hypothèse du 1er cas général.

Donc, quand $m = n \cdot n_1 \cdot n_2$ les conditions énoncées du 1° du théorème à démontrer sont nécessaires et suffisantes dans cette première hypothèse.

Seconde hypothèse.—Soit $m = n \cdot n_1 \cdot n_2$, et supposons que les $n_1 \cdot n_2$ racines de chacune des n équations, en lesquelles doit être décomposée l'équation proposée, $F(x) = 0$, soient assujetties aux conditions énoncées du 2° du théorème à démontrer. Il suffira, à cet effet, que l'on ait $n_1 = n_2$, c'est-à-dire $m = n \cdot n_1^2$, et que l'on ait la relation

$$x_{a+\alpha p,\, b+\beta q\rho,\, c} = \theta\ (x_{a+\alpha p,\, b+\beta q,\, c}, \quad x_{a,\, b,\, c}) \tag{22}$$

quelles que soient les valeurs $0, 1, 2, \ldots, n-1$ de c et les valeurs 0 et 1 de α et de β ; θ désignant une fonction rationnelle, ρ une des racines primitives de n_1, et $x_{a,\, b,\, c}$ les nn_1^2 racines de $F(x) = 0$ avec les hypothèses déjà faites sur a, b, c.

Cela posé : écrivons sur des lignes horizontales les racines de ces n équations, qui sont celles de la proposée ; on aura le tableau suivant, en observant que les résidus à n des valeurs $0, 1, 2, \ldots, n-1$ que prend c sont les mêmes, à la disposition près, que ceux de $c, c+r, c+r\rho, \ldots, c+r\rho^{n-2}$; c désignant un des nombres entiers inférieurs à n, et ρ une racine primitive de n ;

(F)
$$\left\{\begin{array}{l}
x_{a,b,c} \quad x_{a+p,b,c} \;\cdots\; x_{a+p\rho^{n_1-2},b,c} \;\; x_{a,b+q,c} \;\; x_{a+p,b+q,c} \;\cdots\; x_{a,b+q\rho^{n_1-2},c} \;\cdots \\
\hfill \cdots\; x_{a+p\rho^{n_1-2},b+q\rho^{n_1-2},c}\,, \\
x_{a,b,c+r} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\,, \\
x_{a,b,c+r\rho} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\,, \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\,, \\
x_{a,b,c+r\rho^{n-2}} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\,.
\end{array}\right.$$

Dans ce tableau, les indices de x relatifs aux deux premières lettres a, b sont les mêmes, terme à terme, dans chaque colonne verticale, et ceux de c sont respectivement $c, c+r, c+r\rho, \ldots, c+r\rho^{n-2}$; enfin chacune des lignes horizontales contient les n_1^2 racines d'une des n équations dont nous avons parlé, et elle est par conséquent composée de n_1 systèmes formés chacun de n_1 racines *conjuguées.* Mais l'équation $F(x) = 0$ proposée étant irréductible, chacune de ses racines est assujettie à la même loi de détermination, celle de satisfaire identiquement à cette même équation ; et puisque n est premier tout aussi bien que n_1, il s'ensuit que dans chaque colonne verticale il doit y avoir, en intervertissant s'il le faut l'ordre des lignes horizontales, des racines *conjuguées* et en *même* nombre. Il résulte donc de là que $n = n_1$ et que, par suite, $m = n_1^3$, et de plus on doit avoir

$$x_{a,\,b,\,c+r\rho} = \theta(x_{a,\,b,\,c+r}, \quad x_{a,\,b,\,c})\,, \tag{23}$$

relation analogue à (22), et toutes deux étant évidemment comprises dans (18a) en n'y prenant que trois indices a, b, c et en y faisant d'abord $\gamma = 0$, et puis $\alpha = \beta = 0$, $\gamma = 1$.

Ainsi, dans le cas où $m = n \cdot n_1 \cdot n_2$, si les conditions énoncées du 1° du théorème à démontrer ne sont pas satisfaites, celles du 2° du même théorème doivent l'être.

Nous allons actuellement démontrer que ces conditions dernières, d'ailleurs nécessaires, sont suffisantes. Cherchons d'abord le degré s de l'équation résolvante $\varphi(y) = 0$ de l'équation proposée $F(x) = 0$: ce degré est déterminé par la formule de l'énoncé du théorème VIII quand les racines n'ont entre elles aucune relation. Mais, dans le cas actuel, ce degré est moindre et égal à l'unité ; et la valeur unique de y est une fonction symétrique des racines de $F(x) = 0$.

En effet, chaque racine de la résolvante $\varphi(y) = 0$ décompose, à l'aide des racines d'une équation auxiliaire de degré $n - 1$, théorème VIII, l'équation proposée $F(x) = 0$ en n équations d'un même degré n^2 et dont les racines, pour chacune d'elles, constituent n systèmes de n racines conjuguées chacun. Il y aura donc autant de valeurs de y qu'il y aura de manières de décomposer les n^3 racines de $f(x) = 0$ en n systèmes composés chacun de n^2 racines qui forment n systèmes de n racines conjuguées chacun.

Pour ces décompositions, admettons que dans le tableau (F) $n_1 = n$ et que dans chaque ligne, soit horizontale, soit verticale, les racines soient écrites dans l'ordre où elles naissent des relations (22) et (23), vraies par hypothèse. Écrivons *d'abord* ces n^3 racines sur une circonférence de cercle, à égales distances les unes des autres, en les prenant dans le tableau (F) de gauche à droite et ligne par ligne ; et considérons le polygone régulier qui est relatif à cette disposition. Ce polygone est, par hypothèse, composé de n^2 systèmes de n racines conjuguées chacun ; et on démontrerait, comme dans le 1er cas général, que ce polygone produit de nouveaux polygones, jouissant de la même propriété, en prenant pour intervalles constants les nombres qui suivent et qui sont en progression arithmétique dont la raison est n :

$$\begin{array}{rrcr} 1 & n^2+1 & \dots & (n-1)n^2+1\,, \\ n+1 & n^2+n+1 & \dots & (n-1)n^2+n+1\,, \\ 2n+1 & n^2+2n+1 & \dots & (n-1)n^2+2n+1\,, \\ \dots\dots & \dots\dots & \dots & \dots\dots \\ n(n-1)+1 & n^2+(n-1)n+1 & \dots & (n-1)n^2+(n-1)n+1\,. \end{array}$$

Ainsi, avec ce polygone on en fait n^2 composés chacun de n^2 systèmes de n racines conjuguées chacun.

Puis, si l'on écrit sur une circonférence les n^2 racines du tableau (E), en allant de gauche à droite et ligne par ligne ; si l'on joint aux deux indices a, b un troisième c auquel on donnera successivement les valeurs $c, c+r, c+r\rho, \dots, c+r\rho^{n-2}$, on aura un nouveau polygone composé par hypothèse, comme les précédents, de n^2 systèmes de n racines conjuguées chacun. Or, si pour obtenir de nouveaux polygones, par le procédé de l'intervalle constant, on prend pour h des termes en progression arithmétique dont la raison est n, on ne trouve rien de nouveau : mais si la raison est n^2 on obtient n nouveaux polygones relatifs aux valeurs de h

$$1, \quad 1+n^2, \quad 1+2n^2, \quad \dots, \quad 1+(n-1)n^2\,,$$

jouissant de la même propriété ; tandis que toute autre valeur de h ne produit pas de nouveaux polygones ayant cette même propriété. On démontre ces résultats exactement de la même manière que dans le cas de deux indices.

Enfin, en lisant le tableau (F) de haut en bas, on obtient un autre polygone composé également de n^2 systèmes de n racines conjuguées chacun ; polygone qui n'en produit pas d'autres ayant la même propriété. Car, dans les n premières racines des n^2+n premiers polygones, se trouvent toutes les racines de l'équation donnée $F(x)=0$; mais les polygones qu'on formerait avec cette troisième disposition se déduisent des premiers en échangeant entre eux les indices a, b, c, donc cette nouvelle disposition ne produit rien de nouveau.

Il résulte donc de ce qui précède que les n^3 racines de $F(x)=0$ assujetties aux relations (22) et (23) se partagent en n^2 systèmes de n racines conjuguées chacun en un nombre de manières déterminé par la formule

$$n^2+n+1 = \frac{n^3-1}{n-1}\,.$$

Ces $\frac{n^3-1}{n-1}$ décompositions produisent les tableaux suivants :

$$(\mathrm{F}_1) \qquad \left\{\begin{array}{llcl} x_{a,\,b,\,c} & x_{a+p,\,b,\,c} & \cdots & x_{a+p\rho^{n-2},\,b,\,c} \\ x_{a,\,b,\,c+r} & x_{a+p,\,b,\,c+r} & \cdots & x_{a+p\rho^{n-2},\,b,\,c+r} \\ \dots\dots & \dots\dots & \dots & \dots\dots \\ x_{a,\,b+q,\,c} & x_{a+p,\,b+q,\,c} & \cdots & x_{a+p\rho^{n-2},\,b+q,\,c} \\ x_{a,\,b+q,\,c+r} & x_{a+p,\,b+q,\,c+r} & \cdots & x_{a+p\rho^{n-2},\,b+q,\,c+r} \\ \dots\dots & \dots\dots & \dots & \dots\dots \end{array}\right.$$

$$(\mathrm{F}_2)\qquad \left\{\begin{array}{llll}
x_{a,\,b,\,c} & x_{a+p,\,b+q,\,c} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-2},\,c} \\
x_{a,\,b,\,c+r} & x_{a+p,\,b+q,\,c+r} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-2},\,c+r} \\
\multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\
x_{a,\,b+q,\,c+r} & x_{a+p,\,b+q\rho,\,c+r} & \cdots & x_{a+p\rho^{n-2},\,b,\,c+r\rho} \\
x_{a,\,b+q,\,c+r\rho} & x_{a+p,\,b+q\rho,\,c+r\rho} & \cdots & x_{a+p\rho^{n-2},\,b,\,c+r\rho^2} \\
\multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots}
\end{array}\right.$$

$$(\mathrm{F}_3)\qquad \left\{\begin{array}{llll}
x_{a,\,b,\,c} & x_{a+p,\,b+q\rho,\,c} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-3},\,c+r} \\
x_{a,\,b,\,c+r} & x_{a+p,\,b+q\rho,\,c+r} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-3},\,c+r\rho^2} \\
\multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\
x_{a,\,b+q,\,c+r\rho} & x_{a+p,\,b+q\rho^2,\,c+r\rho} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-2},\,c+r\rho^2} \\
x_{a,\,b+q,\,c+r\rho^2} & x_{a+p,\,b+q\rho^2,\,c+r\rho^2} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho^{n-2},\,c+r\rho^3} \\
\multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots}
\end{array}\right.$$

. . . .

$$(\mathrm{F}_{n^2})\qquad \left\{\begin{array}{llll}
x_{a,\,b,\,c} & x_{a+p,\,b+q\rho^{n-2},\,c+r\rho^{n-2}} & \cdots & x_{a+p\rho^{n-2},\,b+q,\,c+r} \\
x_{a,\,b,\,c+r} & x_{a+p,\,b+q\rho^{n-2},\,c} & \cdots & x_{a+p\rho^{n-2},\,b+q,\,c+r\rho} \\
\multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\
x_{a,\,b+q,\,c} & x_{a+p,\,b,\,c+r\rho^{n-2}} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho,\,c+r} \\
x_{a,\,b+q,\,c+r} & x_{a+p,\,b,\,c} & \cdots & x_{a+p\rho^{n-2},\,b+q\rho,\,c+r\rho} \\
\multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots}
\end{array}\right.$$

$$(\mathrm{F}_{n^2+1})\qquad \left\{\begin{array}{llll}
x_{a,\,b,\,c} & x_{a+p,\,b,\,c} & \cdots & x_{a+p\rho^{n-2},\,b,\,c} \\
x_{a,\,b,\,c+r} & x_{a+p,\,b,\,c+r} & \cdots & x_{a+p\rho^{n-2},\,b,\,c+r} \\
\multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\
x_{a,\,b+q,\,c} & x_{a+p,\,b+q,\,c} & \cdots & x_{a+p\rho^{n-2},\,b+q,\,c} \\
x_{a,\,b+q,\,c+r} & x_{a+p,\,b+q,\,c+r} & \cdots & x_{a+p\rho^{n-2},\,b+q,\,c+r} \\
\multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots}
\end{array}\right.$$

. . . .

$$(\mathrm{F}_{n^2+n+1})\qquad \left\{\begin{array}{llll}
x_{a,\,b,\,c} & x_{a+p,\,b,\,c} & \cdots & x_{a+p\rho^{n-2},\,b,\,c} \\
x_{a,\,b,\,c+r} & x_{a+p,\,b,\,c+r} & \cdots & x_{a+p\rho^{n-2},\,b,\,c+r} \\
\multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\
x_{a,\,b+q,\,c} & x_{a+p,\,b+q,\,c} & \cdots & x_{a+p\rho^{n-2},\,b+q,\,c} \\
x_{a,\,b+q,\,c+r} & x_{a+p,\,b+q,\,c+r} & \cdots & x_{a+p\rho^{n-2},\,b+q,\,c+r} \\
\multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots}
\end{array}\right.$$

Dans ces tableaux, *ainsi écrits*, il est utile de faire les remarques suivantes : 1° dans chacun de ces n^2+n+1 tableaux, il y a dans chaque colonne verticale n^2

racines relatives à toutes les valeurs des indices b, c et à une même valeur de l'indice a ; ces valeurs de b et c se déduisent les unes des autres, pour une même colonne verticale et à partir de la 2^{e}, par des permutations circulaires relatives à n termes et à ces mêmes valeurs de b et c ; 2^{o} on passe d'une des colonnes verticales à la suivante en changeant p en $p\rho$, à partir de la deuxième, qui elle-même se déduit de la première en changeant a en $a+p$; 3^{o} les n racines de chaque ligne horizontale des n^2 premiers tableaux sont conjuguées ; 4^{o} dans chacun des n suivants, les n racines qui occupent le même rang dans les n groupes de chaque colonne verticale, sont aussi conjuguées ; 5^{o} enfin les n racines consécutives de chacun des n groupes contenus dans chaque colonne verticale du dernier tableau sont également conjuguées. En sorte que les n^3 racines de l'équation proposée $F(x) = 0$ forment $n^2(n^2 + n + 1)$ systèmes de n racines conjuguées chacun.

Cela posé, pour former la fraction résolvante y définie par l'équation (11) et relative à chacune de ces $n^2 + n + 1$ décompositions, on doit prendre pour chacune des quantités $X_a, X_{a+p}, \dots, X_{a+\overline{n-1}p}$ la somme de n^2 racines quelconques de $F(x) = 0$. Or, si l'on prend successivement pour X_a la somme des racines de la première colonne verticale de chacun de ces tableaux (F), cette quantité conservera évidemment une même valeur pour toutes ces décompositions. Et il résulte des deux premières remarques que si on prend successivement pour X_{a+p} la somme des n^2 racines de la deuxième colonne verticale de ces mêmes tableaux, cette somme conservera également une même valeur pour toutes ces décompositions ; et ainsi de suite. Enfin, si on prend successivement pour $X_{a+\overline{n-1}p}$ la somme des n^2 racines de la dernière colonne verticale de ces mêmes tableaux, cette quantité acquerra une même valeur pour ces mêmes décompositions. Donc les fractions $Z_1, Z_2, \dots, Z_{n-1}$ et la fonction résolvante y, qui ne sont formées que de ces quantités X_a, X_{a+p}, $\dots, X_{a+\overline{n-1}p}$, sont invariables pour ces $n^2 + n + 1$ décompositions. Ainsi, quoiqu'il y ait $n^2 + n + 1$ décompositions, y n'a cependant qu'une *seule* valeur. Ce résultat pouvait d'ailleurs être prévu, puisque, d'après ce qui a été démontré au 2^{o} du théorème IX, l'équation résolvante $\varphi(y) = 0$ est indécomposable.

Démontrons enfin que cette valeur unique de y peut être exprimée en fonction rationnelle des coefficients de l'équation donnée $F(x) = 0$ et de ceux de la fonction connue θ ; et qu'avec cette valeur on peut obtenir les n^3 racines de cette équation.

En effet, toutes ces racines, et par suite la fonction y, peuvent être exprimées, comme dans le premier cas général, en fonction rationnelle des n racines

$$x_{a,\,b,\,c}, \quad x_{a+p,\,b+q,\,c}, \quad x_{a+p,\,b+q\rho,\,c}, \quad \dots, \quad x_{a+p,\,b+q\rho^{n-2},\,c}$$

qui évidemment ne sont pas conjuguées. Car, il résulte d'abord de ce premier cas, que chacune des n^2-n autres racines relatives à la même valeur c du troisième indice de x peut être exprimée en fonction de ces n racines. Puis on voit que, tableaux (F_3), (F_4), ..., on peut, avec les racines relatives à c, obtenir celles qui sont relatives à $c+r$; et, par suite, ces racines étant conjuguées par groupes de n, déterminer toutes les racines relatives à $c + r\rho, c + r\rho^2, \dots, c + r\rho^{n-2}$. Donc, toute fonction connue des n^3 racines de $F(x) = 0$ peut être exprimée en fonction rationnelle des n racines non conjuguées qui précèdent. De là il suit que si l'on considère, non la fonction y, mais la fonction plus générale

$$y_1 = (Z_1 + \lambda_1 Z_2 + \lambda_1^2 Z_3 + \dots + \lambda_1^{n-2} Z_{n-1})^{n-1},$$

dans laquelle les quantités $X_a, X_{a+p}, \dots, X_{a+\overline{n-1}p}$ qui servent à former $Z_1, Z_2, \dots, Z_{n-1}$ désignent précisément celles dont nous venons de parler, et λ_1 une des racines de l'équation binôme $x^{n-1}-1=0$; fonction qui est égale à y pour $\lambda_1 = 1$ après en avoir extrait la racine $n-1^{\text{e}}$; on aura

$$y_1 = \psi\big(x_{a,\,b,\,c},\ x_{a+p,\,b+q,\,c},\ x_{a+p,\,b+q\rho,\,c},\ \dots,\ x_{a+p,\,b+q\rho^{n-2},\,c}\big)\,.$$

Si l'on forme actuellement tous les arrangements n à n des n^3 racines de $F(x)=0$, $n^2\cdot\dfrac{n^3-1}{n-1}$ de ces arrangements seront composés de n racines conjuguées, et tous les autres de n racines non conjuguées. Mais si l'on remplace successivement dans ψ les n racines qui s'y trouvent, d'abord par les premiers arrangements et que l'on fasse la somme des résultats, et puis par tous les autres, et que l'on fasse également la somme des résultats obtenus, on aura, en désignant par $\Sigma'\psi$ la première somme et par $\Sigma''\psi$ la seconde,

$$\textstyle\sum'\psi + \sum''\psi = W_1\,,$$

W_1 étant une fonction évidemment symétrique par rapport aux n^3 racines de $F(x)=0$, et par conséquent exprimable en fonction rationnelle des coefficients de cette équation.

Mais, les n racines qui entrent dans $\Sigma'\psi$ étant conjuguées, elles peuvent être réduites à deux racines x_1, x_2 ; et on aura $\psi=\psi_1(x_1,x_2)$. Or, les quantités $Z_1, Z_2, \dots, Z_{n-1}$ sont invariables pour les $n^2\cdot\dfrac{n^3-1}{n-1}$ systèmes de racines conjuguées des tableaux précédents : de plus, ces mêmes quantités sont encore invariables pour les n valeurs $0,1,2,\dots,n-1$ de a, et elles se déduisent les unes des autres en changeant p successivement en les $n-1$ valeurs $p, p\rho, p\rho^2, \dots, p\rho^{n-2}$, changements qui n'altèrent pas la fonction y_1(1). Donc $\Sigma'\psi = \Sigma'\psi_1(x_1,x_2)$ est invariable pour les $n^2\cdot\dfrac{n^3-1}{n-1}n(n-1) = n^3(n^3-1)$ arrangements deux à deux des n^3 racines de $F(x)=0$; et, par suite, ce terme est symétrique de ces racines et dès lors exprimable en fonction rationnelle des quantités connues.

De là il suit aussi que $\Sigma''\psi$ est exprimable en fonction rationnelle des quantités connues ; mais la fonction y, et évidemment aussi y_1, ne prend qu'une valeur pour tous les arrangements n à n relatifs à toutes les décompositions possibles de $F(x)=0$ en équations de degrés moindres, puisque l'équation résolvante $\varphi(y)=0$ est du premier degré ; donc l'égalité précédente donnera, k' désignant le nombre de termes de $\Sigma''\psi$,

$$y_1 = \frac{1}{k'}\left\{W_1 - \textstyle\sum'\psi_1(x_1,x_2)\right\} = V_1\,,$$

V_1 étant une fonction connue.

Si, dans cette dernière égalité, on remplace successivement λ_1 par chacune des racines de $x^{n-1}-1=0$, on aura $n-1$ équations analogues aux équations (21), dans lesquelles il suffira de remplacer v par V, et dont les seconds membres sont connus.

(1) Car les sommes $X_a, X_{a+p}, \dots, X_{a+\overline{n-1}p}$ jouent évidemment, dans cette deuxième hypothèse, le même rôle que celles qui sont désignées par les mêmes lettres dans la première.

De ces $n-1$ équations on déduira les $n-1$ quantités $Z-1, Z_2, \ldots, Z_{n-1}$, qui à leur tour fourniront, après avoir extrait la racine n^{e} de chacune d'elles, $n-1$ équations constituant avec l'équation dont le second membre est donné,

$$X_a + X_{a+p} + X_{a+2p} + \cdots + X_{a+\overline{n-1}p} = -A_1\,,$$

un système de n équations linéaires par rapport aux n quantités $X_a, X_{a+p}, \ldots, X_{a+\overline{n-1}p}$.

De ces n équations nous déduirons ces n quantités inconnues ; et, comme dans le 1^{er} cas général, nous pourrons former avec chacune d'elles les n équations, de degré n^2, dont les racines sont toutes celles de la proposée $F(x) = 0$. Enfin, ces dernières équations, rentrant dans ce premier cas général, seront toutes résolubles algébriquement par la méthode déjà indiquée : et on aura ainsi les n^3 racines de l'équation à résoudre $F(x) = 0$.

Ces conditions sont donc suffisantes.

En réunissant ce dernier résultat à celui de la première hypothèse, il est prouvé que si le degré m de $F(x) = 0$ est composé de trois facteurs premiers et supérieurs à 3, les conditions énoncées du théorème à démontrer sont encore nécessaires et suffisantes.

La méthode d'exposition qui précède peut évidemment être étendue au cas où le degré m est égal au produit d'un nombre quelconque de facteurs premiers et supérieurs à 3 ; on doit donc regarder ce théorème général XIV comme démontré.

Corollaire.—Il résulte du théorème X et de celui que nous venons de démontrer que *les seules équations algébriques, irréductibles et dont le degré composé ne contient aucun des facteurs premiers* 2 *et* 3*, qui soient solubles par radicaux, sont celles qui sont abéliennes ou celles dont les racines satisfont aux conditions du 1º ou du 2º du théorème XIV.*

Cas particuliers non compris dans le théorème XIV.

Ces cas sont évidemment au nombre de 3 seulement : celui où le degré m de l'équation à résoudre $F(x) = 0$ est égal au facteur premier 2 élevé à une puissance entière quelconque, $m = 2^\alpha$; celui où $m = 3^\beta$; et celui enfin où $m = 2^\alpha \cdot 3^\beta$, β désignant un nombre entier quelconque.

Premier cas : $m = 2^\alpha$.

Si $m = 2^2$, le corollaire du théorème VIII* démontre que $F(x) = 0$ est toujours soluble par radicaux, quelles que soient ses racines.

Si $m = 2^3$, ce théorème démontre, n étant égal à 2, que la fonction résolvante y de $F(x) = 0$ est donnée par la formule (13), que le degré de l'équation résolvante $\psi(y) = 0$ est égal à 35, et qu'avec l'une des racines de cette dernière on décompose l'équation proposée $F(x) = 0$ en deux équations d'un même degré 4. Or, ces deux dernières sont toujours résolubles algébriquement ; donc pour que l'équation $F(x) = 0$ soit elle-même résoluble, il faut et il suffit que $\psi(y) = 0$ soit également

* Original has IX

résoluble algébriquement, ou du moins décomposable en d'autres équations de degrés moindres, celles ci en d'autres de degrés moindres, et ainsi de suite jusqu'à ce qu'on parvienne à des équations résolubles.

Mais, dans le cas actuel, la formule (13) donne

$$y = Z_1 = (X_a + \alpha X_{a+p})^2\,,$$

les quantités X_a et X_{a+p} étant respectivement égales à la somme des quatre racines de chacune des deux équations en lesquelles se décompose l'équation proposée, se composent chacune de la somme de quatre racines quelconques de $F(x) = 0$; et, puisque le degré de l'équation résolvante est égal à 35, le nombre total 40320 de permutations des 2^3 racines de $F(x) = 0$ se décompose, théorème III([1]), en 35 groupes composés chacun de $(1 \cdot 2 \cdot 3 \cdot 4)^2 \cdot 2 = 1152$ permutations inséparables. Or, dans le théorème IX, les quantités désignées généralement par $X_a, X_{a+p}, \ldots, X_{a+(n-1)p}$ jouent le même rôle que les racines $x_a, x_{a+p}, \ldots, x_{a+(n-1)p}$ dans le théorème II ; donc les groupes de permutations faites avec les racines et relatifs à l'équation résolvant $\varphi(y) = 0$ étant indécomposables, note du premier mémoire ; les groupes de permutations relatifs à l'équation résolvante $\psi(y) = 0$ de l'équation à résoudre $F(x) = 0$ seront aussi *indécomposables*.

Ainsi, dans le cas présent, les 35 groupes relatifs aux racines de $\psi(y) = 0$ sont indécomposables ; donc, théorème V, cette équation résolvante est indécomposable elle-même. Mais la résolution de la proposée $F(x) = 0$ entraîne la résolution de $\varphi(y) = 0$, donc les racines de cette dernière doivent être égales entre elles ; puisque toute autre hypothèse la rendrait décomposable. Mais en échangeant entre elles, soit les racines du groupe des 4 racines qui entrent dans X_a, soit celles du groupe des 4 racines qui entrent dans X_{a+p}, soit enfin le premier groupe tout entier en le second, la fonction résolvante y ne change pas de valeur ; tandis que tout autre échange de ces 8 racines altère cette fonction. Donc, l'équation résolvante devant avoir ses racines égales entre elles, il est nécessaire que les racines, d'ailleurs quelconques, d'un de ces deux groupes dépendent les unes des autres. Or, ces racines étant au nombre de 4, il ne peut arriver que 3 cas ; l'une d'elles peut être en effet une fonction rationnelle d'une seule, ou de deux, ou des trois autres.

Dans le 1er cas, un raisonnement analogue à celui qui a été fait pour démontrer la première hypothèse du premier cas général ou la deuxième hypothèse du second cas général du théorème X, prouverait que ce 1er cas entraîne les conditions du 1° et du 2° de ce théorème : conditions qui d'ailleurs ont été démontrées suffisantes pour la résolution de l'équation proposée $F(x) = 0$.

Dans le 2e cas, on a par hypothèse, en désignant respectivement les racines des deux groupes par

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

$c = \theta(b, a)$; et, par suite, $d = \theta_1(b, a)$. En sorte que les quatre racines du 1er groupe sont *conjuguées* ; il en est de même de celles du second. On devrait donc avoir, dans chaque colonne verticale, d'après ce qui a été démontré plusieurs fois, un groupe de 4 racines conjuguées ; ce qui ne peut être, puisque l'équation proposée étant du 8e

([1]) Voir notre Mémoire inséré dans le *Journal de M. Liouville*, février 1865.

degré, il n'y a que deux racines dans chacune de ces colonnes verticales : ainsi, ce cas est inadmissible.

Par la même raison le troisième cas est également inadmissible.

Il résulte donc de ce qui précède que si $m = 2^3$, pour que l'équation proposée $F(x) = 0$ soit résoluble algébriquement, il faut et il suffit qu'elle soit abélienne ou que ses racines satisfassent aux conditions du 2° du théorème X.

Si on suppose actuellement $m = 2^4$; le théorème IX démontre que, n étant égal à 2 et l'équation proposée $F(x) = 0$ étant irréductible, cette équation doit être décomposée, pour sa résolution, en deux équations résolubles du 8ᵉ degré chacune. Mais, d'après ce qui vient d'être démontré, la résolution de chacune de ces dernières équations exige ou qu'elle soit abélienne ou que les racines de chacune d'elles satisfassent aux conditions du 2° du théorème X. Dans l'un et l'autre de ces deux cas, on démontrerait absolument de la même manière que l'équation proposée doit être abélienne ou que ses racines doivent encore satisfaire aux conditions du 2° du même théorème ; et que ces conditions nécessaires sont d'ailleurs suffisantes.

Donc, si $m = 2^4$, pour que l'équation irréductible $F(x) = 0$ soit soluble par radicaux, il faut et il suffit qu'elle soit abélienne, ou que ses racines satisfassent aux conditions du 2° du théorème X.

De même que les conditions de résolubilité pour le cas où $m = 2^3$ donnent celles du cas où $m = 2^4$; de même ces dernières donneraient celles où $m = 2^5$; et ainsi de suite. De là ce théorème :

Théorème XV.—*Pour qu'une équation algébrique irréductible et de degré 2^α, α étant supérieur à 2, soit résoluble algébriquement, il faut et il suffit qu'elle soit abélienne, ou que deux quelconques de ses racines soient tellement liées entre elles que l'une puisse s'exprimer rationnellement par l'autre ; et que si θx et $\theta_1 x$ désignent deux de ses racines distinctes, exprimées l'une et l'autre en fonction rationnelle d'une troisième x, on ait*

$$\theta\theta_1 x = \theta_1\theta x\,.$$

Deuxième cas : $m = 3^\beta$.

Soit d'abord $m = 3^2$: le théorème IX démontre, n étant égal à 3, que la fonction résolvante Y de l'équation proposée (1) à résoudre est donnée par la formule (13), que le degré de son équation résolvante $\psi(y) = 0$ est égal à 280 ; et qu'avec l'une des racines de cette dernière et celles d'une équation du second degré, on décompose l'équation proposée en trois équations d'un même degré 3. Or, ces trois dernières sont toujours résolubles algébriquement, donc pour que la proposée soit dans le même cas il faut et il suffit que $\psi(y) = 0$ soit elle-même résoluble algébriquement, ou du moins décomposable en d'autres équations de degrés moindres, celles-ci en d'autres de degrés moindres, et ainsi de suite jusqu'à ce qu'on parvienne à des équations solubles.

Or il a été démontré généralement et par conséquent pour le cas où $m = 3^2$ que l'équation $\psi(y) = 0$ est indécomposable, que ses racines doivent être égales entre elles, et que l'égalité de ces racines exige que les trois racines de la proposée, d'ailleurs quelconques, qui entrent dans chacune des trois quantités, X_a, X_{a+p}, X_{a+2p} relatives à cette hypothèse $m = 3^2$, dépendent les unes des autres. Mais, le nombre de ces racines étant ici égal à 3, il ne peut arriver que deux cas ; l'une d'elles peut être en effet une fonction d'une seule ou des deux autres.

Dans le premier cas, on démontrerait, comme dans la première hypothèse du deuxième cas général du théorème X, que cette supposition entraîne les conditions du 1° ou du 2° de ce théorème ; conditions qui d'ailleurs sont suffisantes pour la résolution de l'équation proposée $F(x) = 0$, comme cela a été prouvé.

Dans le deuxième cas, on a par hypothèse, en conservant les notations adoptées, la relation suivante entre les trois racines d'un des trois groupes dont nous avons parlé,

$$x_{a+p\rho,\,b} = \theta(x_{a+p,\,b}, \quad x_{a,\,b})\,;$$

nous dirons que ces 3 racines sont *conjuguées.* Cette équation étant vraie pour chacun des 3 groupes, c'est-à-dire pour chacune des valeurs 0, 1, 2 de b, les 9 racines de $F(x) = 0$ se décomposent en 3 systèmes composés chacun de 3 racines conjuguées. Et on prouverait, comme dans le théorème X relatif à deux indices, 1° que l'on doit avoir encore

$$x_{a,\,b+q\rho} = \theta(x_{a,\,b+q}, \quad x_{a,\,b})\,,$$

équation qui fournit 3 nouveaux systèmes composés chacun de 3 racines conjuguées ; 2° que, par suite, les 9 racines de $F(x) = 0$ se décomposent de 4 manières différentes en 3 systèmes composés chacun de 3 racines conjuguées ; 3° que la fonction résolvante y, et aussi que la fonction plus générale

$$y_1 = (Z_1 + \lambda_1 Z_2)^2$$

dans laquelle λ_1 est racine de l'équation binôme $x^2 - 1 = 0$, est une fonction symétrique des racines de $F(x) = 0$, et dès lors exprimable en fonction rationnelle des quantités connues ; 4° enfin, qu'avec les deux valeurs de y_1, relatives aux deux racines de l'équation binôme, on peut déterminer Z_1 et Z_2 ; quantités qui permettent d'obtenir les 3 équations, de degré 3, en lesquelles se décompose $F(x) = 0$. Or, ces 3 dernières équations sont résolubles algébriquement, il en est donc de même de $F(x) = 0$. De là ce théorème : si $m = 3^2$, pour que l'équation irréductible $f(x) = 0$ soit soluble par radicaux, il faut et il suffit que cette équation satisfasse une condition soit du 1°, soit du 2°, soit du 3° du théorème X(1).

Soit actuellement $m = 3^3$: dans ce cas, le théorème IX décompose l'équation proposée $F(x) = 0$ en 3 équations, de même degré 3^2. Mais chacune d'elles, devant être résoluble, doit satisfaire, nous venons de le démontrer, aux conditions du 1°, ou du 2°, ou du tertio du théorème X.

Si ces équations satisfont au 1°, c'est-à-dire si elles sont abéliennes, on prouve comme dans les cas analogues qui précèdent, que la fonction résolvante y doit être symétrique par rapport aux racines de $F(x) = 0$; ce qui exige que les racines de cette dernière satisfassent aux conditions du 1° ou du 2° du théorème X. Et ces conditions nécessaires sont d'ailleurs suffisantes pour résoudre la proposée, comme nous l'avons démontré dans ce théorème.

(1) La résolution de l'équation du 9e degré a été trouvée, dans ce deuxième cas, par M. Hesse d'une manière très différente. (Voir le 34e volume du *Journal de Crelle.*)

Si les racines de chacune de ces 3 équations, de degré 9, satisfont aux conditions du 2° du théorème X, $F(x) = 0$ est encore résoluble, d'après ce qui vient d'être dit.

Enfin, si les racines de chacune de ces mêmes équations de degré 9, satisfont aux conditions du 3° du même théorème X, un raisonnement analogue à celui qui a été fait dans le cas général où $m = n^3$ de ce théorème, démontre que $F(x) = 0$ est encore résoluble.

Donc si $m = 3^3$, pour que l'équation irréductible $f(x) = 0$ soit résoluble algébriquement, il faut et il suffit qu'elle soit abélienne ou que ses racines satisfassent aux conditions du 2° ou du 3° du théorème général X.

Ce raisonnement pouvant être généralisé sans qu'il soit nécessaire d'entrer dans d'autres détails, on a ce théorème :

Théorème XVI.—*Pour qu'une équation algébrique, irréductible et de degré* 3^β *soit résoluble algébriquement, il faut et il suffit 1° qu'elle soit abélienne ; 2° ou que deux quelconques de ses racines soient tellement liées entre elles que l'une puisse s'exprimer rationnellement par l'autre ; et que si* θx *et* $\theta_1 x$ *désignent deux de ses racines distinctes, exprimées l'une et l'autre en fonction rationnelle d'une troisième* x*, on ait* $\theta\theta_1 x = \theta_1\theta x$ *; 3° enfin ou que l'on ait entre trois de ses racines la relation* (19) *relative à 3 indices.*

Troisième cas : $m = 2^\alpha \cdot 3^\beta$.

Pour cette hypothèse nous prendrons $n = 2$ dans le théorème IX, et nous décomposerons par conséquent l'équation irréductible à résoudre $F(x) = 0$ en deux équations, d'un même degré $2^{\alpha-1} \cdot 3^\beta$, à l'aide des racines y de l'équation résolvante $\psi(y) = 0$; l'expression générale de ces racines étant fournie par la formule (13) qui se réduit ici à

$$y = Z_1 = (X_a + \alpha X_{a+p})^2 .$$

On prouverait, absolument comme dans le premier cas, que l'équation résolvante $\psi(y) = 0$ est indécomposable, que ses racines doivent être égales entre elles, et que cela exige que les racines de $F(x) = 0$ satisfassent aux conditions du 1° ou du 2° du théorème X ; conditions qui d'ailleurs sont suffisantes. De là ce théorème :

Théorème XVII.—*Pour qu'une équation algébrique, irréductible et de degré* $2^\alpha \cdot 3^\beta$ *soit résoluble algébriquement, il faut et il suffit qu'elle soit abélienne ; ou que deux quelconques de ses racines soient tellement liées entre elles que l'une puisse s'exprimer rationnellement par l'autre, et que si* θx *et* $\theta_1 x$ *désignent deux de ses racines distinctes, exprimées l'une et l'autre en fonction rationnelle d'un troisième* x*, on ait*

$$\theta\theta_1 x = \theta_1\theta x .$$

NOTE

Les permutations, en effet, d'un quelconque de groupes de cette classification sont relatives à *un seul et même ordre*, c'est-à-dire 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 des 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 des 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.

FIN.

A LA MÊME LIBRAIRIE

Acta Mathematica. — Rédacteur en chef **M. Mittag-Leffler**. — Tomes I à VIII; le vol .... 15 fr.
Tome IX en cours de publication.

American Journal of Mathematics. — Simon Newcomb and Th. Craig, editor. — Tomes II à VIII. — Le vol .... 28 fr.
Tome IX en cours de publication.

Ch. HERMITE, de l'Institut. — **Cours de la Faculté des sciences** *sur les intégrales définies, la théorie des fonctions d'une variable imaginaire et les fonctions elliptiques.* — 3e édition, revue par M. Hermite; in-4o, lith., 1886 .... 14 fr.

DESPEYROUS. — **Cours de Mécanique rationnelle**, avec des notes par M.G. Darboux, de l'Institut, professeur à la Faculté des sciences. — 2 vol. gr. in-8o, 1884–86, de près de 1,100 pages .... 22 fr.

GRUEY, professeur d'Astronomie et directeur de l'Observatoire de Besançon — **Leçons d'Astronomie rédigées conformément au programme de la licence**. — In-4o lith. 357 pages, 1885 .... 16 fr.

AMPÈRE. — **Théorie mathématique des phénomènes électrodynamiques uniquement déduite de l'expérience**. — 2e édition conforme à la première, publiée en 1826.— 2 planches gravées, 1883.
Tirage sur papier fort .... 5 fr.
Tirage sur papier de Hollande .... 7 fr.

P. DUHEM, ancien élève de l'École normale supérieure, agrégé de l'Université — **Le potentiel thermodynamique et ses applications à la Mécanique chimique et à l'étude des phénomènes électriques**. 1 vol. gr. in-8o, 1886, de près de 300 pages, imprimé en caractères compacts .... 10 fr.

E. CESARO, de l'Université de Rome, correspondant de la Société royale des sciences de Liège — **Excursions arithmétiques à l'infini**. — In-4o de 120 pages, 1886 5 fr. 50

C. RIQUIER, agrégé et docteur ès-sciences — **Extension à l'hyperespace de la méthode de M. Carl Neumann**, *pour la résolution de problèmes relatifs aux fonctions de variables réelles qui vérifient l'équation différentielle* $\Delta F = 0$. — In-4o, 112 pages compactes, 1886 .... 6 fr.

J. DESCHAMPS. — **Essai sur le postulatum d'Euclide**. — 1 vol. in-8o, 1885 1 fr. 50

H.-A. ROWLAND. — Professor at the Johns Hopkins University, Baltimore. — **Photograph of the normal Solar Spectrum**. — 1886.
The set of seven plates, unmounted .... 52 fr.
The set of seven plates, mounted on cloth .... 63 fr.

THÉVENET, docteur ès-sciences, professeur à l'École supérieure des sciences d'Alger — **Etude analytique du déplacement infiniment petit d'un corps solide**. — In-4o de 156 p., avec figures. 1886. .... 6 fr.

DESCARTES. — **Géométrie**. — Petit in-4o carré avec 32 figures gravées intercalées dans le texte. — 1886.
Tirage sur papier glacé .... 5 fr.
Tirage sur papier de Hollande .... 8 fr.

J. TANNERY, sous-directeur des études scientifiques à l'École normale supérieure — **Introduction à la théorie des fonctions d'une variable**. — 1 vol. gr. in-8o de 400 pages compactes. — 1886. .... 12 fr.