N° D'ORDRE
492

# THÈSES

PRÉSENTÉES

## A LA FACULTÉ DES SCIENCES DE PARIS

POUR OBTENIR

LE DOCTORAT ÈS SCIENCES MATHÉMATIQUES,

PAR M. LÉON AUTONNE,

Élève-Ingénieur des Ponts et Chaussées.



1re THÈSE. — RECHERCHES SUR LES INTÉGRALES ALGÉBRIQUES DES ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES A COEFFICIENTS RATIONNELS.

2e THÈSE. — PROPOSITIONS DONNÉES PAR LA FACULTÉ.

**Soutenues le 28 juillet 1882, devant la Commission d'Examen.**



MM. HERMITE, *Président*.
BOUQUET, } *Examinateurs*.
PICARD, }

PARIS,

GAUTHIER-VILLARS, IMPRIMEUR-LIBRAIRE

DE L'ÉCOLE POLYTECHNIQUE, DU BUREAU DES LONGITUDES,

SUCCESSEUR DE MALLET-BACHELIER,

Quai des Augustins, 55.

—

1882

# ACADÉMIE DE PARIS.

## FACULTÉ DES SCIENCES DE PARIS.

| | MM. | |
|---|---|---|
| **DOYEN** | MILNE EDWARDS, Professeur. | Zoologie, Anatomie, Physiologie comparée. |
| **PROFESSEURS HONORAIRES** | DUMAS. | |
| | PASTEUR. | |
| **PROFESSEURS** | P. DESAINS | Physique. |
| | LIOUVILLE | Mécanique rationnelle. |
| | PUISEUX | Astronomie. |
| | HÉBERT | Géologie. |
| | DUCHARTRE | Botanique. |
| | JAMIN | Physique. |
| | SERRET | Calcul différentiel et intégral. |
| | DE LACAZE-DUTHIERS | Zoologie, Anatomie, Physiologie comparée. |
| | BERT | Physiologie. |
| | HERMITE | Algèbre supérieure. |
| | BRIOT | Calcul des probabilités, Physique mathématique. |
| | BOUQUET | Mécanique physique et expérimentale. |
| | TROOST | Chimie. |
| | WURTZ | Chimie organique. |
| | FRIEDEL | Minéralogie. |
| | O. BONNET | Astronomie. |
| | DARBOUX | Géométrie supérieure. |
| | DEBRAY | Chimie. |
| **AGRÉGÉS** | BERTRAND | Sciences mathématiques. |
| | J. VIEILLE | Sciences mathématiques. |
| | PELIGOT | Sciences physiques. |
| **SECRÉTAIRE** | PHILIPPON. | |

PARIS. — IMPRIMERIE DE GAUTHIER-VILLARS, SUCCESSEUR DE MALLET-BACHELIER,
Quai des Augustins, 55.
7913

# PREMIÈRE THÈSE.

## RECHERCHES

SUR

# LES INTÉGRALES ALGÉBRIQUES

DES

## ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES A COEFFICIENTS RATIONNELS.

### INTRODUCTION.

Le problème de l'intégration des équations différentielles linéaires est, comme on sait, intimement lié à la théorie des substitutions linéaires. En particulier, la recherche des intégrales algébriques de ces équations se ramène, si l'ordre de l'équation est $p$, à la détermination des groupes de substitutions d'ordre fini, contenus dans le groupe linéaire à $p$ variables. Ce travail, commencé par M. Fuchs (*Journal de Crelle*, t. 81) et MM. Klein et Gordan (*Mathematische Annalen*, t. IX et XII), a été mené à bonne fin par M. Jordan. Dans deux très remarquables Mémoires, dont le premier a été inséré dans le tome 84 du *Journal de Crelle*, et le second présenté à l'Académie de Naples et couronné par cette Académie, M. Jordan a posé les règles générales qui doivent guider dans la recherche des groupes d'ordre fini contenus dans le groupe linéaire à $p$ variables : il a démontré que ces groupes pouvaient toujours se ramener à un nombre limité de types et il a complètement énuméré ces types dans le cas où $p = 2$ et 3.

Pour ce qui est de la recherche des intégrales algébriques des équations différentielles linéaires, M. Jordan a, comme résultat final de son travail, énoncé le théorème suivant, déjà donné avant lui par M. Fuchs pour le second ordre :

Théorème. — *Si une équation différentielle linéaire d'ordre $p$ a toutes ses intégrales algébriques, ces intégrales s'expriment linéairement par les racines d'équations binômes, dont les seconds membres sont des fonctions monodromes de la variable et des racines d'une équation auxiliaire* $X = 0$ ; *le degré de* $X = 0$ *est inférieur à une limite fixe, qui ne dépend que de la valeur numérique de* $p$.

Les remarquables résultats obtenus par M. Jordan m'ont paru propres à une application qu'on ne trouvera peut-être pas complètement dépourvue d'intérêt. Voici le problème que je me propose de résoudre : une équation différentielle linéaire Y, d'ordre $p$ et à coefficients rationnels, admet un système fondamental d'intégrales dont tous les termes sont des racines d'une équation algébrique irréductible H de degré $m = p + n$ et à coefficients rationnels. Puisque toutes les $m$ racines de H sont des intégrales de Y et que Y ne peut avoir plus de $p$ intégrales linéairement indépendantes, il existe entre les $m$ racines $n$ équations linéaires, homogènes, à coefficients constants. Je me propose d'étudier les conséquences qu'entraîne, tant pour la forme de l'équation algébrique H que pour la nature des intégrales de Y, l'existence de ce système de $n$ équations linéaires, homogènes, à coefficients constants.

Ce travail est divisé en quatre Parties.

Dans la première, j'examine le cas où $n = 1$. Si le degré $m$ est un nombre premier et si le coefficient du terme de degré $m - 1$ dans l'équation H n'est pas nul, l'équation H est abélienne et toutes les racines s'expriment rationnellement en fonction de la variable et de l'une quelconque d'entre elles. L'équation différentielle Y possède un système fondamental d'intégrales dont l'une est rationnelle et les $p - 1 = m - 2$ autres des racines $m^{\text{ièmes}}$ de fonctions rationnelles.

On voit que, dans ce cas, l'équation auxiliaire $X = 0$ de M. Jordan est du premier degré, et que les diverses équations binômes considérées sont toutes du degré $m$.

Dans la deuxième Partie, j'étudie le cas $n = 2$. Si $m$ est un nombre premier et si le terme de degré $m - 1$ ne manque pas dans l'équation H, H peut encore être une équation abélienne, et l'équation différentielle admet un système fondamental pareil à celui qui a été défini dans la première Partie. Mais, de plus, H peut être telle que toutes les racines s'expriment rationnellement en fonction de la variable et de deux quelconques d'entre elles. L'équation différentielle admet alors un système fondamental, dont une intégrale est rationnelle et dont les $p - 1 = m - 3$ autres sont de la forme $\sqrt[m]{\psi(u)}$, où $\psi$ désigne une fonction rationnelle de la variable et d'une racine $u$ d'une équation du second degré à coefficients rationnels.

L'équation auxiliaire $X = 0$ de M. Jordan est du second degré et les diverses équations binômes sont toutes du degré $m$.

La troisième Partie traite du cas $n = 3$. Le degré $m$ est encore un nombre premier et le terme de degré $m - 1$ existe dans l'équation H. Après avoir donné un certain nombre de propositions générales, je suis forcé, pour traiter complètement la question, de me restreindre aux degrés premiers inférieurs à 20. J'énonce dans ce dernier cas deux théorèmes :

1° *Si $p - 1 = m - 4$ est un multiple de 3, l'équation* H *est telle que toutes les racines s'expriment rationnellement en fonction de la variable et de deux quelconques d'entre elles. L'équation différentielle possède un système fondamental dont une intégrale est rationnelle et les $p - 1 = m - 4$ autres sont de la forme $\sqrt[m]{\psi(u, x)}$, où $\psi$ désigne une fonction rationnelle, $x$ la variable, $u$ une racine d'une équation abélienne du troisième degré à coefficients rationnels.*

L'équation auxiliaire de M. Jordan est une équation abélienne du troisième degré.

2° *Si $p - 1 = m - 4$ n'est pas un multiple de 3, les résultats ne diffèrent en rien de ceux de la première Partie.*

Dans la quatrième Partie, qui est fort courte, je me borne à indiquer la marche à suivre, si l'on voulait réellement appliquer la méthode à l'intégration d'une équation différentielle donnée.

# PREMIÈRE PARTIE.

## I.

**1.** Considérons une équation différentielle linéaire d'ordre $p$ et à coefficients rationnels :

$$(\mathrm{Y}) \qquad \frac{d^p y}{dx^p} + \mathrm{B}_1 \frac{d^{p-1} y}{dx^{p-1}} + \mathrm{B}_2 \frac{d^{p-2} y}{dx^{p-2}} + \ldots + \mathrm{B}_{p-1} \frac{dy}{dx} + \mathrm{B}_p y = 0.$$

Prenons maintenant une équation algébrique irréductible à coefficients rationnels

$$(\mathrm{H}) \qquad \eta^m + \mathrm{A}_1 \eta^{m-1} + \mathrm{A}_2 \eta^{m-2} + \ldots + \mathrm{A}_{m-1} \eta + \mathrm{A}_m = 0,$$

dont le degré $m$ soit un nombre premier $m = p + n$ et dont la somme des racines ne soit pas nulle ($\mathrm{A}_1 \gtrless 0$). Je suppose que Y possède un système fondamental d'intégrales dont tous les termes sont des racines $\eta_0, \eta_1, \eta_2, \ldots$ de l'équation algébrique H. Il existera dans ce cas, entre les $m$ racines de H $\eta_0, \eta_1, \eta_2, \ldots, \eta_{m-1}$, $n$ et seulement $n$ équations linéaires, homogènes, à coefficients constants.

Avant d'aller plus loin, je vais rappeler quelques propositions bien connues de la théorie générale des équations algébriques.

**2.** On appelle *groupe d'une équation* un groupe de substitutions entre les racines, tel que toute fonction des racines, dont les substitutions de ce groupe n'altèrent pas la valeur, soit exprimable rationnellement en fonction des coefficients, et réciproquement (JORDAN, *Traité des substitutions*, p. 257).

On sait, de plus, que le groupe d'une équation algébrique irréductible est transitif, c'est-à-dire qu'il est possible, en opérant successivement diverses substitutions au groupe, d'amener telle racine qu'on veut à la place de l'une quelconque des autres (JORDAN, *Traité des substitutions*, p. 259).

3. Cela posé, considérons le système formé par les $n$ équations linéaires, homogènes, à coefficients constants,

$$(1)\qquad X_1 = 0, \quad X_2 = 0, \quad X_3 = 0, \quad \ldots, \quad X_n = 0,$$

qui existent entre les $m$ racines de H.

Les fonctions $X_1, \ldots, X_n$ des racines sont nulles, c'est-à-dire exprimables rationnellement en fonction des coefficients : la valeur numérique de ces fonctions, qui est zéro, ne saurait, par définition, être altérée par aucune substitution S du groupe G de l'équation H.

Appelons $X'_1 \ldots X'_n$ ce que deviennent les fonctions $X_1, \ldots, X_n$ par l'effet d'une substitution S du groupe G. Les fonctions $X'_1, \ldots, X'_n$ seront encore des fonctions linéaires et homogènes des racines à coefficients constants, et l'on aura le nouveau système d'équations

$$(1')\qquad X'_1 = 0, \quad \ldots, \quad X'_n = 0.$$

Mais, par hypothèse, il ne saurait exister entre les $m$ racines de H plus de $n$ équations linéaires, homogènes, à coefficients constants, distinctes, car, si cela était, l'équation différentielle Y ne pourrait avoir un système fondamental formé exclusivement de racines de l'équation algébrique H. Donc le système (1′) n'est pas distinct du système (1), et l'on a

$$\begin{aligned}
X'_1 &= \lambda_{11} X_1 + \lambda_{12} X_2 + \ldots + \lambda_{1n} X_n,\\
X' &= \lambda_{21} X_1 + \lambda_{22} X_2 + \ldots + \lambda_{2n} X_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
X'_n &= \lambda_{n1} X_1 + \lambda_{n2} X_2 + \ldots + \lambda_{nn} X_n,
\end{aligned}$$

les $\lambda$ désignant des constantes dont le déterminant

$$\Delta = \begin{vmatrix} \lambda_{11} & \cdots & \lambda_{1n} \\ \lambda_{21} & \cdots & \lambda_{2n} \\ \cdots & \cdots & \cdots \\ \lambda_{n1} & \cdots & \lambda_{nn} \end{vmatrix}$$

est différent de o.

On voit que, en opérant entre les racines de H une substitution S du groupe G de cette équation, on opère du même coup entre les $n$ premiers membres des équations $X_1 = 0, \ldots, X_n = 0$ une substitution linéaire $\Sigma$ de déterminant $\Delta \gtrless 0$.

Les diverses substitutions linéaires $\Sigma$, $\Sigma_1$, $\Sigma_2$, ... entre les $n$ fonctions X, qui correspondent aux diverses substitutions S, $S_1$, $S_2$, ... du groupe G entre les $m$ racines de H, forment évidemment un groupe $\Gamma$. Au produit de deux substitutions du groupe G correspond dans $\Gamma$ le produit de leurs correspondantes. A une substitution S de G correspond une substitution $\Sigma$ de $\Gamma$; à une substitution $\Sigma$ de $\Gamma$ correspondent une ou plusieurs substitutions de G. Les groupes G et $\Gamma$ sont donc isomorphes.

*Nota.* — Dans la suite du discours, lorsque l'ambiguïté ne sera pas possible, je désignerai fréquemment par la même lettre une substitution de $\Gamma$ et l'une quelconque de ses correspondantes dans le groupe G.

**4.** Reprenons le système

$$(1) \quad \begin{cases} X_1 = 0, \\ X_2 = 0, \\ \ldots\ldots, \\ X_n = 0, \end{cases}$$

qu'une substitution S de G transforme en

$$(2) \quad \begin{cases} X'_1 = \lambda_{11} X_1 + \lambda_{12} X_2 + \ldots + \lambda_{1n} X_n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ X'_n = \lambda_{n1} X_1 + \lambda_{n2} X_2 + \ldots + \lambda_{nn} X_n, \end{cases}$$

$$\Delta = \begin{vmatrix} \lambda_{11} & \cdots & \lambda_{1n} \\ \cdots & \cdots & \cdots \\ \lambda_{n1} & \cdots & \lambda_{nn} \end{vmatrix} \gtrless 0,$$

et considérons une fonction

$$U = \mu_1 X_1 + \mu_2 X_2 + \ldots + \mu_n X_n,$$

les $\mu$ désignant des constantes.

La substitution S transforme U en

$$\begin{aligned} U' = \mu_1 X'_1 + \ldots + \mu_n X'_n = X_1(\mu_1\lambda_{11} + \mu_2\lambda_{21} + \ldots + \mu_n\lambda_{n1}) \\ + X_2(\mu_1\lambda_{12} + \mu_2\lambda_{22} + \mu_3\lambda_{32} + \ldots + \mu_n\lambda_{n2}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ + X_n(\mu_1\lambda_{1n} + \mu_2\lambda_{2n} + \ldots + \mu_n\lambda_{nn}). \end{aligned}$$

Déterminons maintenant les constantes $\mu$, par la condition

$$U' = KU,$$

K désignant une constante; il viendra, pour la détermination des $\mu$, le système

$$(3) \qquad \begin{cases} \mu_1(\lambda_{11} - K) + \mu_2\lambda_{21} + \ldots + \mu_n\lambda_{n1} = 0, \\ \mu_1\lambda_{12} + \mu_2(\lambda_{22} - K) + \ldots + \mu_n\lambda_{n2} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \mu_1\lambda_{1n} + \mu_2\lambda_{2n} + \ldots + \mu_n(\lambda_{nn} - K) = 0. \end{cases}$$

Ces équations sont compatibles et fournissent, pour les rapports $\frac{\mu_2}{\mu_1}$, $\frac{\mu_3}{\mu_1}$, ..., des solutions finies et déterminées si le déterminant

$$D = \begin{vmatrix} \lambda_{11} - K & \lambda_{21} & \lambda_{n1} \\ \lambda_{12} & \lambda_{22} - K & \lambda_{n2} \\ \ldots & \ldots & \ldots \\ \lambda_{1n} & \lambda_{2n} & \lambda_{nn} - K \end{vmatrix} = 0.$$

Cette équation en K est appelée l'*équation caractéristique* de la substitution S. Soient $K_0, K_1, K_2, \ldots$ les diverses racines de $D = 0$; ces quantités portées dans le système (3) détermineront chacune un système de quantités $\mu$ et, par suite, une fonction U.

Supposons d'abord les $n$ racines de l'équation caractéristique toutes distinctes. J'aurai un système de fonctions $U_1, U_2, \ldots, U_n$ que la substitution S multipliera par des facteurs constants $K_1, \ldots, K_n$. Les fonctions $U_1, \ldots, U_n$ sont appelées la *forme canonique* de la substitution S.

Si l'équation caractéristique possède une racine $K_1$ d'ordre $\alpha$ de multiplicité, à cette racine correspondra un système de fonctions U jouissant des propriétés suivantes :

$$(4)\quad \begin{cases} U'_1 = K_1 U_1, \\ U'_2 = K_{21} U_1 + K_1 U_2, \\ U'_3 = K_{31} U_1 + K_{32} U_2 + K_1 U_3, \\ \ldots\ldots\ldots\ldots\ldots\ldots, \\ U'_\alpha = K_{\alpha 1} U_1 + K_{\alpha 2} U_2 + \ldots + K_1 U_\alpha. \end{cases}$$

(*Voir*, pour la démonstration, par exemple, le travail de M. J. Tannery, *Annales scientifiques de l'École Normale,* année 1875, p. 138).

5. Le groupe G de substitutions entre les $m$ racines de l'équation H est d'ordre fini; lorsqu'on a effectué une substitution S de ce groupe un certain nombre de fois, on ramène chaque lettre à sa place, et, par conséquent, les fonctions X du système (1) du n° 4 redeviennent les mêmes. Donc la substitution linéaire $\Sigma$, qui, dans le groupe $\Gamma$, correspond à S, sera elle-même d'ordre fini. Ce que je viens de dire d'une substitution S de G et d'une substitution correspondante $\Sigma$ de $\Gamma$ s'applique aussi au produit SS′ de deux substitutions et au produit de leurs correspondantes dans le groupe $\Gamma$. Donc le groupe $\Gamma$ sera un groupe d'ordre fini contenu dans le groupe linéaire à $n$ variables.

Ce groupe $\Gamma$ sera donc l'un de ceux que M. Jordan a fait connaître et a appris à déterminer. Dans le cas où $n = 1, 2, 3$, la détermination des systèmes de coefficients $\lambda$ tels que la substitution linéaire (2) du n° 4 puisse faire partie d'un groupe d'ordre fini a été faite complètement par M. Jordan. Je transporterai donc intégralement dans ces recherches les résultats obtenus par cet éminent géomètre.

Les racines de l'équation fondamentale relative à une substitution linéaire, qui fait partie d'un groupe d'ordre fini, sont évidemment des racines entières de l'unité. Il est évident aussi que, dans ce cas, le système (4) du n° 4 se réduit à

$$(4') \quad \begin{cases} U'_1 = K_1 U_1, \\ U'_2 = K_1 U_2, \\ \dots\dots\dots, \\ U'_n = K_1 U_n. \end{cases}$$

En effet, supposons, par exemple, que $K_{21} \gtrless 0$; dans ce cas, S transforme $U_2$ en $K_{21} U_1 + K_1 U_2$, $S^2$ le transforme en $2 K_1 K_{21} U_1 + K_1^2 U_2$ ou, en posant $K_{21} = \omega K_1$, en $K_1^2 (U_2 + 2\omega U_1)$.

De même $S^3$ transforme $U_2$ en $K_1^3 (U_2 + 3\omega U_1)$ et $S^\mu$ en $K_1^\mu (U_2 + \mu\omega U_1)$. On voit que pour aucune valeur de l'entier $\mu$, $S^\mu$ ne saurait transformer $U_2$ en $U_2$, tant que $\omega$, c'est-à-dire $K_{21}$, est différent de 0. On raisonnera de la même façon sur les coefficients $K_{31}$, $K_{32}$, ..., $K_{\alpha 1}$, ..., et l'on verra sans peine que ces coefficients sont tous nuls. Donc le système (4) du n° 4 a bien la forme (4′) du n° 5, et mon assertion se trouve justifiée.

**6.** Théorème. — *Considérons les n équations*

$$X_1 = \alpha_{01} \eta_0 + \alpha_{11} \eta_1 + \alpha_{21} \eta_2 + \ldots + \alpha_{m-1.1} \eta_{m-1},$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots,$$
$$X_n = \alpha_{0n} \eta_0 + \alpha_{1n} \eta_1 + \alpha_{2n} \eta_2 + \ldots + \alpha_{m-1.n} \eta_{m-1},$$

*qui existent entre les m racines de* H. *Je dis qu'une racine quelconque figurera avec un coefficient différent de* 0, *dans l'une au moins des équations* $X_1 = 0$, $X_2 = 0$, ..., $X_n = 0$.

Considérons, en effet, par exemple, l'équation $X_1 = 0$; soient $\eta_i$ une racine qui y figure, $\eta_j$ une racine qui n'y figure pas. Puisque le groupe G de l'équation algébrique H est transitif, il existera dans G au moins une substitution S, qui amène $\eta_j$ à la place de $\eta_i$. Si donc je désigne par $X'_1$ la transformée de $X_1$ par la substitution S, la racine $\eta_j$ figurera certainement dans $X'_1$, puisqu'elle y possédera le coefficient de $\eta_i$, lequel n'est pas nul. Mais on a identiquement

$$X'_1 = \lambda_1 X_1 + \lambda_2 X_2 + \ldots + \lambda_n X_n,$$

et cette identité ne sera possible que si $n_j$ figure avec un coefficient différent de o dans l'une au moins des équations $X_2 = 0$, $X_3 = 0$, ..., $X_n = 0$.

C. Q. F. D.

A ce théorème se rattachent trois corollaires évidents, dont je ferai grand usage dans la suite, dans les cas où $n = 1, 2, 3$.

*Corollaire I.* — Si $n = 1$, l'équation linéaire, homogène à coefficients constants, entre les racines de H, savoir $X = 0$, contiendra toutes les $m$ racines.

*Corollaire II.* — Si $n = 2$, appelons $X = 0$, $Y = 0$ les deux équations entre les racines ; s'il y a $n_0$ racines communes à $X = 0$ et à $Y = 0$, $n_1$ racines qui figurent dans X seul, $n_2$ racines qui figurent dans Y seul, on aura

$$n_0 + n_1 + n_2 = m.$$

*Corollaire III.* — Si $n = 3$, appelons encore $X = 0$, $Y = 0$, $Z = 0$ les trois équations entre les racines ; s'il existe

$n_0$ racines communes à X, Y, Z,
$n_{12}$ » » X, Y,
$n_{13}$ » » X, Z,
$n_{23}$ » » Y, Z;

s'il existe

$n_1$ racines qui figurent dans X seul,
$n_2$ » » Y
$n_3$ » » Z,

on aura

$$n_0 + n_{12} + n_{13} + n_{23} + n_1 + n_2 + n_3 = m.$$

Après avoir exposé les principes de la méthode, je vais passer à l'examen du cas où $n = 1$. Ce sera l'objet du second paragraphe de la première Partie.

## II.

$n = 1.$

**7.** Théorème I. — *Si une substitution* S *entre les $l$ lettres $\eta_1, \eta_2, \ldots, \eta_l$ multiplie par un facteur constant* K *la fonction*

$$u = \alpha_1\eta_1 + \alpha_2\eta_2 + \ldots + \alpha_l\eta_l,$$

*on a* $K^d = 1$, *en désignant par $d$ le plus grand commun diviseur des degrés $i, i', i'', \ldots$ des différents cycles de* S.

Soient, en effet, $\eta_1, \eta_2, \ldots, \eta_i$ les différentes lettres d'un cycle de S. La substitution S transformera

$$u = \alpha_1\eta_1 + \alpha_2\eta_2 + \ldots + \alpha_i\eta_i + \ldots$$

en

$$u' = \alpha_1\eta_2 + \alpha_2\eta_3 + \ldots + \alpha_i\eta_1 + \ldots;$$

d'où, par suite,

$$\frac{\alpha_2}{\alpha_1} = \frac{\alpha_3}{\alpha_2} = \frac{\alpha_{\lambda+1}}{\alpha_\lambda} = \ldots = \frac{\alpha_i}{\alpha_{i-1}} = \frac{1}{K} \quad (\lambda \text{ quelconque}).$$

La substitution $S^i$ ramènera dans le cycle chaque lettre à sa place : $\eta_1$ par exemple figurera dans $u^{(i)}$ et dans $u$ avec le même coefficient ; donc $S^i$ multiplie $u$ par 1 et $K^i = 1$. De même on verra que $K^{i'} = 1$, $K^{i''} = 1$, etc. Donc K sera une racine de l'équation $K^d = 1$, en désignant par $d$ le plus grand commun diviseur de $i, i', i'', \ldots$.

*Remarque.* — On voit de plus que l'on a

$$u = \alpha_1(\eta_1 + K^{d-1}\eta_2 + K^{d-2}\eta_3 + \ldots + K\eta_i) + \ldots$$

Théorème II. — *Réciproquement, si la substitution* S *entre les $l$ lettres $\eta_1, \eta_2, \ldots, \eta_l$ multiplie la fonction*

$$u = \alpha_1\eta_1 + \alpha_2\eta_2 + \ldots + \alpha_l\eta_l$$

*par* K, K *étant une racine primitive $\delta^{\text{ième}}$ de l'unité, $\delta$ divise les degrés $i, i', i'', \ldots$ de tous les cycles de* S.

Soit, en effet, $i$ le degré de l'un quelconque des cycles de S; supposons que l'on ait $i = q\delta + r$. La substitution $S^{q\delta}$ multiplie $u$ par 1; la substitution $S^i$ multiplie aussi $u$ par 1; donc on aurait $K^r = 1$, ce qui est absurde, puisque $r < \delta$. Il faut donc que l'on ait $r = 0$, d'où $i = q\delta$.

C. Q. F. D.

*Corollaire.* — $\delta$ divise $l$, puisque $l = i + i' + i'' + \ldots$, et que $\delta$ divise chacune des parties de cette somme.

**8.** Revenons maintenant à l'équation

$$X = \alpha_0 \eta_0 + \alpha_1 \eta_1 + \ldots + \alpha_{m-1} \eta_{m-1} = 0,$$

qui existe entre les $m$ racines de l'équation algébrique irréductible H, de degré premier $m$. Nous savons, en vertu du corollaire I du n° **6**, qu'aucun des $m$ coefficients $\alpha$ n'est nul, et, en vertu des considérations exposées au n° **3**, que les diverses substitutions S du groupe G de l'équation H ne peuvent que multiplier X par des facteurs constants racines de l'unité. Soit K l'un de ces facteurs; supposons qu'il soit une racine primitive $\delta^{\text{ième}}$ de l'unité, en vertu du corollaire du théorème du n° **7**, $\delta$ divise $m$ : donc $\delta = 1$ ou $\delta = m$. Dans ce dernier cas, les $m$ racines $\eta_0, \eta_1, \ldots, \eta_{m-1}$ ne forment qu'un cycle : la substitution S est circulaire; elle remplace la racine $\eta_i$ par la racine $\eta_{i+1}$; nous la désignerons par la notation

$$S = |\, i \quad i+1 \,|$$

ou encore

$$S = (\eta_0 \eta_1 \ldots \eta_{m-1}).$$

Théorème. — *Le groupe G est formé par les puissances d'une seule substitution circulaire entre les m racines.*

1° En effet, je dis en premier lieu que G contient au moins une substitution S, qui multiplie X par une racine $m^{\text{ième}}$ $\theta$ de l'unité. Supposons, en effet, que toutes les substitutions de G multiplient X par l'unité. Considérons deux racines quelconques $\eta_i$ et $\eta_j$, dont la première a dans X le coefficient $\alpha_i$ et la seconde le coefficient $\alpha_j$. Puisque le groupe G est transitif, il existera une substitution S′, qui amène $\eta_j$ à la place de $\eta_i$, et, en vertu de l'hypothèse, cette substitution S′ multiplie X par 1; donc on a

$$\alpha_i = \alpha_j.$$

Raisonnant de même sur les diverses racines, on voit sans peine que les coefficients de toutes les racines seraient égaux : cela est contraire à l'hypothèse faite au n° 1, qui spécifie que la somme des racines n'est pas nulle.

Donc G contient au moins une substitution, qui multiplie X par une racine $m^{\text{ième}}$ $\theta$ de l'unité, c'est-à-dire une substitution circulaire entre les $m$ racines. De plus, en vertu de la remarque du théorème I du n° 7, on a

$$X = \eta_0 + \theta^{-1}\eta_1 + \theta^{-2}\eta_2 + \ldots + \theta^{-(m-1)}\eta_{m-1}.$$

Tous les coefficients sont des racines $m^{\text{ièmes}}$ de l'unité et sont tous inégaux.

2° Le groupe G ne peut contenir aucune substitution qui multiplie X par 1; en effet, une pareille substitution ne déplacerait que les lettres affectées dans X de coefficients égaux; or tous les coefficients des diverses racines sont inégaux dans X; donc la substitution se réduit à la substitution 1, qui laisse chaque racine à sa place.

3° Le groupe G ne peut contenir deux substitutions circulaires distinctes. Supposons, en effet, qu'il en existe deux, S et S′. Les puissances successives $1, S, S^2, S^3, S^4, \ldots, S^{m-1}$ multiplient X par $1, \theta, \theta^2, \ldots, \theta^{m-1}$.

Cela posé, reprenons la substitution circulaire S′; elle multiplie X par une racine $m^{\text{ième}}$ de l'unité, c'est-à-dire par un terme $\theta^a$ de la série $1, \theta, \theta^2, \ldots, \theta^{m-1}$. Donc S′ et $S^a$ multiplient X par un même facteur, donc $S'^{-1}S^a$ multiplie X par 1, et, en vertu du raisonnement que nous venons de faire, la substitution $S'^{-1}S^a$ se réduit à la substitution 1, qui laisse chaque lettre à sa place. Donc S′ est précisément la substitution $S^a$, c'est-à-dire une puissance de S.

Ainsi donc le groupe G ne peut contenir que les puissances de la substitution circulaire S. C. Q. F. D.

**9.** Reprenons le groupe G d'une équation algébrique quelconque.

Fixons, *a priori*, certaines quantités $z_1$, $z_2$, $z_3$, ..., que j'appellerai *adjointes* à l'équation. Il existera toujours un groupe G' de substitutions entre les racines, tel que toute fonction des racines dont les substitutions de ce groupe ne changent pas la valeur soit exprimable rationnellement en fonction des coefficients de l'équation et des quantités adjointes, et réciproquement (*voir* Jordan, *Traité des substitutions*, pages 253 et 257).

Le groupe G' sera d'ailleurs contenu dans le groupe G, et l'on dira que l'adjonction des quantités $z_1$, $z_2$, $z_3$, ... a réduit le groupe G au groupe G'.

On a, à cet égard, le théorème suivant, pour la démonstration duquel je renvoie au *Traité des substitutions*, p. 261 :

Théorème. — *Soient* G *le groupe d'une expression algébrique,* $\varphi_1$ *une fonction rationnelle quelconque des racines : 1° celles des substitutions de* G *qui n'altèrent pas* $\varphi_1$ *forment un groupe* G'*; 2° l'adjonction de* $\varphi_1$ *réduira le groupe* G *de l'équation précisément à* G'.

On sait, de plus, qu'on appelle équation *abélienne* une équation irréductible dont deux racines sont liées par une relation rationnelle

$$\varkappa_2 = \Psi(\varkappa_1).$$

Après avoir reproduit ces définitions, je vais passer à l'étude de l'équation algébrique irréductible H, dont le groupe est formé par les puissances d'une seule substitution circulaire

$$S = | i \quad i+1 |.$$

Théorème I. — *L'équation* H *est abélienne et toutes les m racines peuvent s'exprimer rationnellement en fonction de l'une quelconque d'entre elles.*

En effet, adjoignons à l'équation la racine $\varkappa_0$ par exemple. L'adjonction de cette racine réduit le groupe G au groupe formé par les substitutions qui ne déplacent pas $\varkappa_0$. Mais toutes les substitutions du groupe G (excepté la substitution 1) déplacent toutes les racines. Donc, par l'adjonction de la racine $\varkappa_0$, le groupe G se réduit à la seule substitution 1, et toutes les racines s'expriment rationnellement en fonction de $\varkappa_0$ et des coefficients de H.

THÉORÈME II. — *L'équation* H *est résoluble algébriquement.*

En effet, formons le système des $m-1$ fonctions

$$
(1)\quad \left\{
\begin{array}{l}
U_1 = x_0 + \theta x_1 + \theta^2 x_2 + \ldots + \theta^{m-1} x_{m-1} \qquad (\theta^m = 1), \\
U_2 = x_0 + \theta^2 x_1 + \theta^4 x_2 + \ldots + \theta^{2(m-1)} x_{m-1}; \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
U_l = x_0 + \theta^l x_1 + \theta^{2l} x_2 + \ldots + \theta^{l(m-1)} x_{m-1}, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
U_{m-1} = x_0 + \theta^{m-1} x_1 + \theta^{2(m-1)} x_2 + \ldots + \theta^{(m-1)(m-1)} x_{m-1};
\end{array}
\right.
$$

parmi ces $m-1$ fonctions, il y en aura une qui sera précisément X et qui sera nulle, mais les $m-2$ autres ne seront pas nulles. Les diverses substitutions de G, c'est-à-dire les puissances successives de la substitution circulaire S, multiplient les fonctions $U_1$, $U_2$, ... par des racines $m^{\text{ièmes}}$ de l'unité ; donc ces substitutions n'altèrent pas la valeur de $U_1^m$, $U_2^m$, ... ; les fonctions $U_1^m$, $U_2^m$, ... étant invariables par toutes les substitutions du groupe G, s'exprimeront rationnellement en fonction des coefficients de H.

Voici d'ailleurs comment pourrait s'effectuer le calcul explicite de la fonction

$$U_l^m = (x_0 + \theta^l x_1 + \theta^{2l} x_2 + \ldots + \theta^{l(m-1)} x_{m-1})^m.$$

Les $m-1$ racines $x_1, x_2, x_3, \ldots, x_{m-1}$ s'expriment rationnellement en fonction de $x_0$ et, en portant ces valeurs dans

$$(x_0 + \theta^l x_1 + \theta^{2l} x_2 + \ldots + x^{l(m-1)} \theta_{m-1})^m,$$

j'aurai

$$U_l^m = \Psi(x_0, \theta^l),$$

$\Psi$ désignant une fonction rationnelle.

La fonction $U_l^m$ est invariable par la substitution $S = (x_0 x_1 \ldots x_{m-1})$ ; donc on aura aussi

$$
\begin{aligned}
U_l^m &= \Psi(x_0, \theta^l) = \Psi(x_1, \theta^l) = \Psi(x_2, \theta^l) = \ldots \\
&= \frac{\Psi(x_0, \theta^l) + \Psi(x_1, \theta^l) + \ldots + \Psi(x_{m-1}, \theta^l)}{m} = u_l.
\end{aligned}
$$

La quantité $u_l$ sera une fonction symétrique des $m$ racines, c'est-à-dire une fonction rationnelle des coefficients de H.

On calculera de même toutes les quantités U, et l'on formera le système suivant d'équations linéaires et à coefficients constants :

$$(2)\quad \begin{cases} n_0 + \theta n_1 + \theta^2 n_2 + \ldots + \theta^{m-1} n_{m-1} = u_1^{\frac{1}{m}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ n_0 + \theta^l n_1 + \theta^{2l} n_2 + \ldots + \theta^{l(m-1)} n_{m-1} = u_l^{\frac{1}{m}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ n_0 + \theta^{m-1} n_1 + \theta^{2(m-1)} + \ldots + \theta^{(m-1)(m-1)} n_{m-1} = u_{m-1}^{\frac{1}{m}} \end{cases}$$

L'une des quantités $u$ sera d'ailleurs nulle. Si au système (2) j'ajoute encore l'équation

$$n_0 + n_1 + n_2 + \ldots + n_{m-1} = -A_1,$$

j'aurai un système de $m$ équations linéaires à $m$ inconnues. Ce système fournira toujours pour les inconnues $n_0, n_1, n_2, \ldots, n_{m-1}$ des valeurs finies et déterminées, car toutes les équations linéaires du système sont distinctes. Si, en effet, il n'en était pas ainsi, on aurait

$$D = \begin{vmatrix} 1 & \theta & \theta^2 & \ldots & \theta^{m-1} \\ 1 & \theta^2 & \theta^4 & \ldots & \theta^{2(m-1)} \\ \cdot & \cdot\cdot & \cdot\cdot & \ldots & \ldots \\ 1 & \theta^l & \theta^{2l} & \ldots & \theta^{l(m-1)} \\ \cdot & \cdot\cdot & \cdot\cdot & \ldots & \ldots \\ 1 & \theta^{m-1} & \theta^{2(m-1)} & \ldots & \theta^{(m-1)^2} \\ 1 & 1 & 1 & \ldots & 1 \end{vmatrix} = 0.$$

Or on sait qu'un pareil déterminant ne saurait être nul.

Une conséquence remarquable de ce qui précède est la suivante : l'équation différentielle Y possède par hypothèse un système fondamental formé exclusivement de racines de l'équation algébrique H; on voit donc que toutes les intégrales de ce système sont des fonctions rationnelles de la variable et de l'une quelconque d'entre elles.

**10.** THÉORÈME. — *L'équation différentielle* Y *possède un système fondamental d'intégrales, formé d'une fonction rationnelle de la variable et de* $m-2$ *racines* $m^{\text{ièmes}}$ *de fonctions rationnelles de la variable. La fonction rationnelle sera la fonction* $A_1$, *et les* $m-2$ *autres intégrales du système seront les* $m-2$ *fonctions* $u_l^{\frac{1}{m}}$, *qui ne sont pas nulles.*

En effet, on voit immédiatement que ces fonctions sont des intégrales de Y; il reste à prouver que ce sont là des intégrales linéairement indépendantes.

Supposons, en effet, qu'il n'en soit pas ainsi et reprenons l'équation

$$u_1^{\frac{1}{m}} = X = n_0 + \theta n_1 + \theta^2 n_2 + \ldots + \theta^{m-1} n_{m-1} = 0.$$

Puisque les intégrales $A_1$, $u_2^{\frac{1}{m}}$, $u_3^{\frac{1}{m}}$, $u_4^{\frac{1}{m}}$, ..., $u_{m-1}^{\frac{1}{m}}$ ne sont pas linéairement indépendantes, on pourra déterminer un système de $m-1$ constantes $\lambda_2, \lambda_3, \ldots, \lambda_m$, qui ne seront pas toutes nulles, et telles que l'on ait identiquement

$$\lambda_2, u_2^{\frac{1}{m}} + \lambda_3 u_3^{\frac{1}{m}} + \ldots + \lambda_{m-1} u_{m-1}^{\frac{1}{m}} + \lambda_m A_1 = 0,$$

c'est-à-dire

$$\begin{aligned}
&n_0[\lambda_2 + \lambda_3 + \ldots + \lambda_{m-1} + \lambda_m] \\
&+ n_1[\theta^2\lambda_2 + \theta^3\lambda_3 + \ldots + \theta^{m-1}\lambda_{m-1} + \lambda_m] \\
&+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&+ n_l[\theta^{2l}\lambda_2 + \theta^{3l}\lambda_3 + \ldots + \theta^{(m-1)l}\lambda_{m-1} + \lambda_m] \\
&+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&+ n_{m-1}[\theta^{2(m-1)}\lambda_2 + \theta^{3(m-1)}\lambda_3 + \ldots + \theta^{(m-1)2}\lambda_{m-1} + \lambda_m] = 0.
\end{aligned}$$

Voilà une équation linéaire, homogène et à coefficients constants, qui existe entre les racines; cette équation ne saurait donc être distincte de X, et l'on peut l'identifier avec $-\lambda_1 X$ par exemple, $\lambda_1$ désignant une constante. Identifiant, nous obtenons le système

$$\begin{gathered}
\lambda_1 + \lambda_2 + \lambda_3 + \ldots + \lambda_m = 0,\\
\theta\lambda_1 + \theta^2\lambda_2 + \theta^3\lambda_3 + \ldots + \theta^{(m-1)}\lambda_{m-1} + \lambda_m = 0,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\theta^l\lambda_1 + \theta^{2l}\lambda_2 + \theta^{3l}\lambda_3 + \ldots + \theta^{(m-1)l}\lambda_{m-1} + \lambda_m = 0,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\theta^{(m-1)}\lambda_1 + \theta^{2(m-1)}\lambda_2 + \ldots + \theta^{(m-1)(m-1)}\lambda_{m-1} + \lambda_m = 0.
\end{gathered}$$

Ce système ne peut donner pour l'un quelconque des coefficients $\lambda$ de valeur différente de zéro que si le déterminant

$$D = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & \theta & \ldots & \theta^{m-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & \theta^{m-1} & \ldots & \theta^{(m-1)2} \end{vmatrix} = 0;$$

mais nous avons déjà vu qu'un tel déterminant ne saurait être nul, et le théorème est démontré.

**11.** Toute la discussion précédente peut se résumer dans la proposition qui suit :

Théorème. — *Soit* Y *une équation différentielle linéaire à coefficients rationnels, d'ordre p, qui possède :* 1° *une intégrale rationnelle* $A_1$ ; 2° *un système fondamental exclusivement formé de racines d'une équation algébrique irréductible dont le degré est un nombre premier* $m = p + 1$ ; *l'équation différentielle possède un système fondamental exclusivement formé de* $m - 1$ *racines* $m^{\text{ièmes}}$ *de fonctions rationnelles de la variable, jointes à l'intégrale rationnelle* $A_1$.

Si l'on se reporte au théorème de M. Jordan, cité dans l'introduction du présent travail, on voit que l'équation auxiliaire $X = 0$ est, dans le cas que je considère, du premier degré, et que le degré de diverses équations binômes est toujours $m$.

Il est d'ailleurs facile de vérifier qu'une équation différentielle linéaire qui admet un système fondamental d'intégrales, défini comme au théorème précédent, a bien tous ses coefficients rationnels.

On sait, en effet, qu'une équation différentielle linéaire d'ordre $p$ qui admettrait un système fondamental formé par les $p$ fonctions de $x$,

$$y_1, y_2, \ldots, y_p,$$

peut se mettre sous la forme d'un déterminant et s'écrire

$$Y = \begin{vmatrix} \dfrac{d^p y}{dx^p} & \dfrac{d^p y_1}{dx^p} & \cdots & \dfrac{d^p y_p}{dx^p} \\ \cdots & \cdots & \cdots & \cdots \\ \dfrac{d^l l}{dx^l} & \cdots & \cdots & \dfrac{d^l y_p}{dx^l} \\ \dfrac{dy}{dx} & \cdots & \cdots & \dfrac{dy_p}{dx} \\ y & y_1 & \cdots & y_p \end{vmatrix} = 0.$$

Or posons

$$y_1 = A_1, \quad y_p^m = u_{m-1}, \quad y_2^m = u_2, \quad y_l^m = u_l, \quad l = (2, 3, \ldots, m-1).$$

Il viendra, en différentiant ($i$ = entier quelconque),

$$\frac{d^i y^l}{dx^i} = y_l \varphi_i(x),$$

$\varphi_i$ désignant une fonction rationnelle. Substituant dans le déterminant les valeurs successives des diverses dérivées, et supprimant le facteur $y_l$ commun à tous les éléments d'une colonne, nous obtenons un déterminant dont tous les éléments sont rationnels. C. Q. F. D.

*Application.* — Supposons $m = 3$ et prenons l'équation

$$(1) \qquad n^3 + 3A_1 n^2 + A_2 n + A_3 = 0.$$

Les équations

$$X = \alpha_0 n_0 + \alpha_1 n_1 + \alpha_2 n_2 = 0, \qquad -3A_1 = n_0 + n_1 + n_2,$$

nous fournissent, pour $n_1$ par exemple,

$$n_1 = an_0 + bA_1.$$

Substituons dans (1) cette valeur, il vient

$$(2)\qquad \left\{ \begin{array}{c|c|c|c} a^3 & n^3 + 3a^2bA_1 & n^2 + 3ab^2A_1^2 & + b^3A_1^3 \\ & + 3a^2A_1 & + 6abA_1^2 & + 3b^2A_1^3 \\ & & + aA_2 & + bA_1A_2 \\ & & & + A_3 \end{array} \right| = 0.$$

Identifions (2) avec (1), puisque (1) est irréductible par hypothèse, il vient

$$3a^2bA_1 + 3a^2A_1 = 3A_1a^3,$$
$$3ab^2A_1^2 + 6abA_1^2 + aA_2 = A_2a^3,$$
$$b^3A_1^3 + 3b^2A_1^3 + bA_1A_2 + A_3 = A_3a^3.$$

Je puis toujours supposer $a \gtrless 0$, car si $a = 0$, une racine serait rationnelle, ce qui est absurde; je divise donc par $a$ et il vient, puisque $A_1 \gtrless 0$;

$$(3)\qquad \left\{ \begin{array}{l} b + 1 = a, \\ (3b^2 + 6b)A_1^2 = (a^2 - 1)A_2, \\ (b^3 + 3b^2)A_1^3 + bA_1A_2 = A_3(a^3 - 1). \end{array} \right.$$

On ne peut avoir $a = 1$, car alors $b = 0$ et il y aurait deux racines égales. On ne peut avoir $a = -1$, car alors $b = -2$ et les trois racines seraient $n_0$, $-n_0 - 2A_1$, $-A_1$, ce qui est absurde. Supposons maintenant $a^3 - 1 \gtrless 0$, les équations (3) donnent sans peine $A_2 = 3A_1^2$, $A_3 = A_1^3$; d'où

$$H = n^3 + 3A_1n^2 + 3A_1^2n + A_1^3 = (n + A_1)^3 = 0:$$

l'équation ne serait plus irréductible.

Supposons donc $a^3 = 1$, la seconde des équations (3) fournit $A_2 = 3A_1^2$

et la troisième devient une identité : donc H prend la forme

$$n^3 + 3A_1 n^2 + 3A_1^2 n + A_3 = 0, \quad (n + A_1)^3 + A_3 - A_1^3 = 0,$$

c'est-à-dire

$$(n + u)^3 + v = 0,$$

$u$ et $v$ désignant des fonctions rationnelles, et il vient pour les trois racines

$$-u - v^{\frac{1}{3}}, \quad -u - jv^{\frac{1}{3}}, \quad -u - j^2 v^{\frac{1}{3}}, \quad (j^3 = 1).$$

On voit que l'équation différentielle Y d'ordre $p = 2$ admet le système fondamental $u$ et $\sqrt[3]{v}$, qui a bien la forme indiquée.

---

# DEUXIÈME PARTIE.

## $n = 2$.

---

**12.** Supposons maintenant que l'ordre $p$ de l'équation différentielle Y soit inférieur de deux unités au degré $m$ de l'équation algébrique, irréductible et à coefficients rationnels, H, dont $m - 2$ racines forment un système fondamental de Y. Soient

$$X = \alpha_0 n_0 + \alpha_1 n_1 + \ldots + \alpha_{m-1} n_{m-1} = 0$$

et

$$Y = \beta_0 n_0 + \beta_1 n_1 + \ldots + \beta_{m-1} n_{m-1} = 0 \quad (^1)$$

les deux équations linéaires et homogènes, distinctes, à coefficients constants, qui existent entre les $m$ racines de H.

Considérons le groupe $\Gamma$ (5) de substitutions linéaires entre les deux variables X et Y, qui est isomorphe au groupe G de l'équation H. Ce groupe $\Gamma$ est un groupe d'ordre fini, contenu dans le groupe linéaire à

(1) L'ambiguïté entre les deux notations Y n'est pas possible.

deux variables; donc Γ appartiendra à l'un des cinq types de groupes dont l'énumération a été faite par M. Jordan (tome 84 du *Journal de Crelle*, page 111). Voici cette énumération :

*Premier type.* — Ses substitutions sont toutes de la forme

$$|\,XY \quad aX \quad bY\,|,$$

$a$ et $b$ désignant des racines de l'unité.

*Deuxième type.* — Il s'obtient en ajoutant aux substitutions précédentes une substitution de la forme

$$|\,XY \quad cY \quad dX\,|.$$

*Troisième type* (*tétraédrique*). — Il est dérivé de substitutions de la forme

$$a = |\,X\;\;Y \quad aX \quad aY\,|,$$

jointes aux substitutions

$$A = |\,XY \quad iX \quad -iY\,| \quad (i^4 = 1),$$

$$B = |\,XY \quad Y \quad -X\,|,$$

$$\lambda C = \begin{vmatrix} X & \lambda\frac{1-i}{2}(X-Y) \\ Y & \lambda\frac{1+i}{2}(X+Y) \end{vmatrix},$$

$\lambda$ étant une racine de l'unité.

*Quatrième type* (*octaédrique*). — Il résulte des substitutions $a$, A, B, C, jointes à une substitution de la forme

$$\mu D = |\,XY \quad \mu jX \quad \mu j^{-1}Y\,| \quad (j^8 = 1),$$

$\mu$ désignant une racine de l'unité.

*Cinquième type* (*icosaédrique*). — Il est dérivé de substitutions de la forme

$$a = |\,XY \quad aX \quad aY\,|,$$

jointes aux substitutions

$$B = | XY \quad Y \quad -X |,$$

$$E = | XY \quad \omega X \quad \omega^{-1} Y | \quad (\omega^{10} = 1),$$

$$F = \left| \begin{matrix} X & \lambda X + \mu Y \\ Y & \mu X - \lambda Y \end{matrix} \right| \left| \begin{matrix} \lambda = \dfrac{1}{\omega^2 - \omega^{-2}} \\ \lambda^2 + \mu^2 + 1 = 0 \end{matrix} \right|.$$

Je vais maintenant démontrer deux lemmes qui me permettront d'écarter immédiatement le troisième, le quatrième et le cinquième type.

**13.** Convenons d'abord des notations suivantes :

$N_0$ désigne le système des $n_0$ racines qui entrent dans X et Y,
$N_1$ » $n_1$ » X seul,
$N_2$ » $n_2$ » Y seul.

En vertu du corollaire II du n° **6**, on a

$$n_0 + n_1 + n_2 = m.$$

*Lemme I.* — S'il existe une substitution de la forme

$$S = | XY \quad aX \quad bY |,$$

dans le groupe $\Gamma$ ($a$ étant une racine primitive $\alpha^{\text{ième}}$, $b$ une racine primitive $\beta^{\text{ième}}$ de l'unité), le plus grand commun diviseur $\delta$ des nombres $\alpha$ et $\beta$ ne peut être que l'unité.

Reprenons, en effet, les trois systèmes $N_0$, $N_1$, $N_2$ formés respectivement par $n_0$, $n_1$, $n_2$ racines ; je dis, en premier lieu, que la substitution S (¹) ne saurait échanger entre elles deux racines, qui appartiennent à deux systèmes différents. Soit $X' = aX$ et $Y' = bY$ ce que deviennent X et Y par l'effet de la substitution S; supposons un instant que S fasse entrer une racine $\nu_l$ du système $N_1$ dans le système $N_0$. La racine $\nu_l$ figurera à la fois dans $X'$ et dans $Y'$; or cela est impossible,

(¹) Voir *Nota* (3).

puisque l'on a identiquement $Y' = bY$ : $\eta_l$ figurerait dans le premier membre de cette identité sans figurer dans le second, ce qui est absurde. On démontrerait de même que S ne saurait faire entrer une racine de $N_2$ dans le système $N_0$ ni dans le système $N_1$ ; donc S permute entre elles les diverses racines d'un même système $N_0$, $N_1$ ou $N_2$.

Puisqu'il en est ainsi, chacun des systèmes $N_0$, $N_1$, $N_2$ comprend un nombre entier de cycles de S, et, en vertu du théorème II du n° 7,

$$\alpha \text{ divise } n_0 \text{ et } n_1,$$
$$\beta \text{ divise } n_0 \text{ et } n_2,$$

et $\delta$, qui divise $\alpha$ et $\beta$, divise aussi $n_0 + n_1 + n_2$, c'est-à-dire $m$. Cela n'est possible que si $\delta = 1$ ou $\delta = m$. Dans ce dernier cas, $n_1 = n_2 = 0$, $n_0 = m$, et la substitution S est circulaire entre les $m$ racines. Si nous écartons cette hypothèse, on voit que $\delta$ est toujours égal à l'unité, et les nombres $\alpha$ et $\beta$ sont premiers entre eux.

*Corollaire*. — S'il existe dans le groupe $\Gamma$ une substitution de la forme

$$|\ XY \quad \lambda X \quad \lambda Y\ |,$$

on a forcément $\lambda = 1$.

Supposons, en effet, que $\lambda$ soit une racine primitive $\delta^{\text{ième}}$ de l'unité; en vertu du lemme précédent, $\delta$ divise $m$ : donc, si $\lambda$ n'est pas égal à l'unité, $\lambda = \theta$, $(\theta^m = 1)$. Mais, dans ce dernier cas, la substitution est circulaire, et, en vertu de la remarque du théorème I du n° 7, il vient pour X et Y la forme suivante

$$X = \eta_0 + \theta^{-1}\eta_1 + \theta^{-2}\eta_2 + \ldots + \theta^{-(m-1)}\eta_{m-1},$$
$$Y = \eta_0 + \theta^{-1}\eta_1 + \theta^{-2}\eta_2 + \ldots + \theta^{-(m-1)}\eta_{m-1};$$

les équations $X = 0$, $Y = 0$ ne sont plus distinctes, ce qui est absurde.

Ainsi donc $\lambda = 1$.

*Lemme II*. — Si le groupe $\Gamma$ contient une substitution T de la forme

$$T = |\ XY \quad aY \quad bX\ |,$$

on a $n_1 = n_2$.

Je dis en premier lieu que T déplace toutes les racines du système $N_1$, par exemple, et les fait toutes entrer dans le système $N_2$. Supposons, en effet, qu'il n'en soit point ainsi, et soit $n_j$ une racine de $N_1$ que T laisse immobile; appelons X′ et Y′ les transformées de X et de Y par la substitution T; $n_j$ figurerait encore dans X′; or cela est absurde, car on a identiquement

$$X' = aY,$$

et $n_j$ figurerait dans le premier membre de cette identité, sans figurer dans le second. On démontrera de même que T déplace toutes les racines du système $N_2$.

Supposons maintenant que la substitution T fasse entrer une lettre $n_j$ de $N_1$ dans le système $N_0$; $n_j$ figurerait à la fois dans X′ et dans Y′; or cela est absurde, car on a identiquement

$$X' = aY,$$

et $n_j$ figurerait dans le premier membre de cette identité sans figurer dans le second. On démontrera de même que T ne peut faire entrer une racine de $N_2$ dans le système $N_0$.

En résumé, puisque T fait entrer toutes les $n_1$ racines de $N_1$ dans le système $N_2$, et toutes les $n_2$ racines de $N_2$ dans le système $N_1$, on a forcément

$$n_1 = n_2 = \nu$$

et, par suite,

$$n_0 + 2\nu = m.$$

**14.** Théorème. — *Le groupe tétraédrique dérivé des substitutions*

$$a = | \, XY \quad aX \quad aY \, |,$$

$$A = | \, XY \quad iX \quad -iY \, | \qquad (i^4 = 1),$$

$$B = | \, XY \quad Y \quad -X \, |,$$

$$\lambda C = \begin{vmatrix} X & \lambda \frac{1-i}{2}(X - Y) \\ Y & \lambda \frac{1+i}{2}(X + Y) \end{vmatrix}$$

*ne peut fournir aucun type d'équations algébriques irréductibles* H *de degré premier m.*

En effet, il est aisé de voir tout d'abord que la substitution A est impossible, en vertu du lemme I du n° **15**, puisque $i$ et $-i$ sont des racines primitives $4^{\text{ièmes}}$ de l'unité et que 4 ne divise pas $m$, en vertu du corollaire du même lemme $a = 1$.

En second lieu, la substitution B est impossible; en effet, son équation caractéristique (*voir* n° **4**) est

$$\begin{vmatrix} -K & 1 \\ -1 & -K \end{vmatrix} = 0,$$

$$K^2 + 1 = 0.$$

Les deux racines $i$ et $-i$ sont des racines primitives $4^{\text{ièmes}}$ de l'unité ; soit donc X' et Y' la forme canonique de la substitution B, on aura

$$B = |\ X'Y' \quad iX' \quad -iY'\ |,$$

et l'on démontrera que cette substitution est impossible, comme on vient de le faire pour la substitution A.

Le groupe se réduit donc à la seule substitution $\lambda$C. Soit

$$|\ X''Y'' \quad a''X'' \quad b''Y''\ |$$

la forme canonique de la substitution C ; le groupe se réduit au premier type de l'énumération de M. Jordan et n'est plus tétraédrique.

C. Q. F. D.

**15.** Théorème. — *Le groupe octaédrique dérivé des substitutions a,* A, B, C *et*

$$D = |\ XY \quad njX \quad nj^{-1}Y\ | \quad (j^8 = 1)$$

*ne peut fournir aucun type d'équation* H.

En effet, on démontrera, comme dans le cas précédent, que $a = 1$, que

A et B sont impossibles. Je dis que, de plus, C est aussi impossible. En effet, l'équation caractéristique de C est

$$\begin{vmatrix} \frac{1-i}{2} - K & -\frac{1-i}{2} \\ \frac{1+i}{2} & \frac{1+i}{2} - K \end{vmatrix} = 0,$$

c'est-à-dire

$$K^2 - K + 1 = 0.$$

Les deux racines sont $-\alpha$ et $-\alpha^2$ $(\alpha^3 = 1)$ et sont des racines primitives $6^{\text{ièmes}}$ de l'unité. Soit donc $X''$ et $Y''$ la forme canonique de C, il viendra

$$C = |\; X''Y'' \quad -\alpha X'' \quad -\alpha^2 Y'' \;|;$$

or, en vertu du lemme I du n° **13**, une telle substitution est impossible, puisque 6 ne divise pas $m$.

Donc le groupe se réduit à la seule substitution D, c'est-à-dire au premier des cinq types de M. Jordan.

**16.** Théorème. — *Le groupe icosaédrique dérivé des substitutions*

$$a = |\; XY \quad aX \quad aY \;|,$$
$$B = |\; XY \quad Y \quad -X \;|,$$
$$E = |\; XY \quad \omega X \quad \omega^{-1} Y \;| \quad (\omega^{10} = 1),$$
$$E = \begin{vmatrix} X & \lambda X + \mu Y \\ Y & \mu X - \lambda Y \end{vmatrix} \quad \begin{vmatrix} \left(\lambda = \dfrac{1}{\omega^2 - \omega^{-2}}\right) \\ (\lambda^2 + \mu^2 + 1 = 0) \end{vmatrix}$$

*ne peut fournir aucun type d'équations* H.

En vertu du lemme I du n° **13**, la substitution E est impossible; en vertu du corollaire du même lemme $a = 1$; on démontrera, comme dans le n° **14**, que la substitution B est impossible. Le groupe se réduit donc à la seule substitution E. Cette substitution E elle-même est impossible;

son équation caractéristique est, en effet,

$$\begin{vmatrix} \lambda - K & \mu \\ \mu & -\lambda - K \end{vmatrix} = 0,$$

c'est-à-dire

$$K^2 = \lambda^2 + \mu^2 = -1, \quad \text{puisque} \quad \lambda^2 + \mu^2 + 1 = 0;$$

les deux valeurs de K sont des racines $4^{\text{ièmes}}$ de l'unité ; si donc $X''$ et $Y''$ sont la forme canonique de E, on a

$$E = |\, X''Y'' \quad iX'' \quad -iY'' \,|,$$

ce qui est impossible (n° **13**, lemme I).

Après avoir ainsi écarté les trois derniers types de l'énumération de M. Jordan, je vais passer à la discussion des deux premiers, qui donnent chacun un type distinct d'équations H.

**17.** Je suppose que le groupe $\Gamma$ se ramène au premier des cinq types de M. Jordan, c'est-à-dire qu'il ne contienne que des substitutions de la forme

$$|\, XY \quad aX \quad bY \,|.$$

Je dis que dans ce cas X et Y contiennent chacune toutes les $m$ racines. En effet, reprenons les notations $N_0$, $N_1$, $N_2$, $n_0$, $n_1$, $n_2$ (n° **13**). Une quelconque des substitutions du groupe G permute entre elles diverses racines d'un même système (**13**, lemme I) et il n'existe pas de substitution capable d'échanger entre elles deux racines appartenant à deux systèmes différents $N_0$, $N_1$, $N_2$. Donc, puisque le groupe G est transitif, il faut nécessairement que les systèmes $N_1$ et $N_2$ n'existent pas, d'où

$$n_1 = n_2 = 0, \quad n_0 = m.$$

On voit que nous sommes ramené à un cas qui est complètement identique au cas $n = 1$, traité dans la première Partie ; l'on démontrera par des raisonnements identiques les propositions suivantes :

THÉORÈME I. — *L'équation* H *est abélienne et résoluble algébriquement* ($n^{os}$ **8** et **9**), *puisqu'elle a son groupe exclusivement formé par les puissances d'une seule substitution circulaire entre les* $m$ *racines.*

THÉORÈME II. — *L'équation différentielle linéaire* Y *admettra un système fondamental d'intégrales, formé d'une fonction rationnelle* $A_1$ *de* $x$, *et de* $m-3$ *intégrales* $\sqrt[m]{u_i}$, *en désignant par* $u_i$ *une fonction rationnelle de la variable* $x$.

Rien, en effet, n'est changé aux raisonnements faits plus haut ($n^o$ **10**), si ce n'est qu'il y a deux fonctions $u$, qui sont nulles.

**18.** Je vais actuellement rechercher la nature du groupe G de l'équation H, quand son isomorphe $\Gamma$, défini de la façon qu'on sait, appartient au second des cinq types de l'énumération de M. Jordan. Dans ce cas $\Gamma$ ne contient que des substitutions de la forme

$$S = |\, XY \quad aX \quad bY \,|,$$

jointes à une substitution

$$T = |\, XY \quad a'Y \quad b'X \,|.$$

*Lemme.* — Chacune des équations $X = 0$ et $Y = 0$ contient toutes les $m$ racines.

Reprenons, en effet, les notations connues $N_0$, $N_1$, $N_2$, $n_0$, $n_1$, $n_2$ (**13**). Les substitutions telles que S permutent entre elles des racines d'un même système $N_0$, $N_1$ ou $N_2$ (**13**, lemme I); la substitution T permute entre elles des racines du système $N_0$, et fait entrer toutes les racines de $N_1$ dans le système $N_2$, et réciproquement (**13**, lemme II). Aucune substitution du groupe G ne peut faire passer, par conséquent, une racine de $N_0$ dans $N_1$ ou $N_2$, et réciproquement. Le groupe G est transitif : donc ou le système $N_0$ manque, ou bien les deux systèmes $N_1$ et $N_2$. Mais on a (**13**, lemme II) $n_1 = n_2 = \nu$, $n_0 + 2\nu = m$, et il est absurde de supposer l'absence de $N_0$, car, si $n_0 = 0$, il reste

$$2\nu = m,$$

ce qui est impossible. Donc $n_0 = n_1 = \nu = 0$, et le lemme est démontré.

Puisque X et Y contiennent chacune toutes les $m$ racines, on démontrera sans aucune peine, et par des raisonnements identiques à ceux du n° **8**, que toutes les substitutions de la forme

$$|\, XY \quad aX \quad bY \,|$$

sont des puissances d'une seule substitution circulaire entre les $m$ racines; $a$ et $b$ sont des racines $m^{\text{ièmes}}$ de l'unité, X et Y sont de la forme

$$X = \eta_0 + \theta^{\alpha}\eta_1 + \theta^{2\alpha}\eta_2 + \ldots + \theta^{(m-1)\alpha}\eta_{m-1} \quad (\theta^m = 1),$$
$$Y = \eta_0 + \theta^{\beta}\eta_1 + \theta^{2\beta}\eta_2 + \ldots + \theta^{(m-1)\beta}\eta_{m-1}.$$

On remarque qu'il n'existe pas de coefficients égaux dans X et dans Y.

Passons maintenant à la discussion de la substitution T.

**19.** *Lemme I.* — La substitution $T^2$ laisse à sa place chacune des $m$ racines.

En effet, puisque

$$T = |\, XY \quad a'Y \quad b'X \,|,$$
$$T^2 = |\, XY \quad a'b'X \quad a'b'Y \,|.$$

Or $a'b' = 1$ (**13**, corollaire du lemme I) : donc $T^2$ ne déplace que les racines qui ont des coefficients égaux dans X et dans Y; mais nous venons de voir que les coefficients de X sont tous inégaux; il en est de même des coefficients de Y donc $T^2$ ne déplace aucune racine. C. Q. F. D.

*Lemme II.* — Les coefficients $a'$ et $b'$ sont des racines $m^{\text{ièmes}}$ de l'unité.

En effet, $a'$ et $b'$ sont des rapports de racines $m^{\text{ièmes}}$ de l'unité et $a' = \theta^{\mu}$. De plus, $a'b' = 1$, d'où $b' = \theta^{-\mu}$.

Cela posé, reprenons les $m$ racines $\eta_0, \eta_1, \ldots, \eta_i, \ldots, \eta_j, \ldots, \eta_{m-1}$. T remplace l'indice $i$ par l'indice $j$; cherchons à exprimer $j$ en fonction de $i$.

**20.** THÉORÈME. — *La substitution* T *est égale au produit* $S^{\mu'\mu}$ *t des deux* *substitutions* $S^{\mu,\mu'}$ *et* $t$, *dont l'une*

$$S^{\mu'\mu} = | \, i \quad i + \mu'\mu \, | \quad (\bmod m)$$

*est une substitution circulaire entre les* $\mu$ *racines, et dont l'autre*

$$t = | \, i \quad -i \, | \quad (\bmod m)$$

*ne déplace pas l'indice zéro, mais déplace tous les* $m - 1$ *autres indices.*

En effet, X et Y sont de la forme

$$\begin{aligned} X &= \eta_0 + \theta^{\alpha}\eta_1 + \ldots + \theta^{i\alpha}\eta_i + \ldots + \theta^{(m-1)\alpha}\eta_{m-1}, \\ Y &= \eta_0 + \theta^{\beta}\eta_1 + \ldots + \theta^{i\beta}\eta_j + \ldots + \theta^{(m-1)\beta}\eta_{m-1}, \\ X &= \ldots + \theta^{\alpha i}\eta_i + \ldots + \theta^{\alpha j}\eta_j + \ldots, \\ Y &= \ldots + \theta^{\beta i}\eta_i + \ldots + \theta^{\beta j}\eta_j + \ldots; \end{aligned}$$

opérant la substitution

$$T = | \, i \quad j \, | \quad (\bmod m)$$

il vient

$$\begin{aligned} X' &= \ldots + \theta^{\alpha i}\eta_j + \ldots, \\ Y' &= \ldots + \theta^{\beta i}\eta_j + \ldots. \end{aligned}$$

D'ailleurs

$$\begin{aligned} a'Y &= \theta^{-\mu}Y = \ldots + \theta^{\beta j-\mu}\eta_j + \ldots, \\ b'X &= \theta^{\mu}X = \ldots + \theta^{\alpha j+\mu}\eta_j + \ldots. \end{aligned}$$

Donc $i$ et $j$ sont liés par la relation suivante obtenue en identifiant X′ avec $a'$Y et Y′ avec $b'$X,

$$\begin{aligned} &\theta^{\alpha j+\mu} = \theta^{\beta i}, \quad \theta^{\beta j-\mu} = \theta^{\alpha i}, \\ &\beta j - \mu \equiv \alpha i, \\ &\alpha j + \mu \equiv \beta i \quad (\bmod m). \end{aligned}$$

Donc T peut se mettre sous l'une des deux formes

$$T = \left| \, i \quad \frac{\alpha i + \mu}{\beta} \, \right| \quad (\bmod m)$$

ou

$$T = \left| \, i \quad \frac{\beta i - \mu}{\alpha} \, \right| \quad (\bmod m),$$

ce qui exige

$$\frac{\alpha}{\beta} \equiv \frac{\beta}{\alpha}, \quad \frac{\mu}{\beta} \equiv -\frac{\mu}{\alpha} \quad (\bmod m).$$

D'ailleurs

$$T^2 = \left| i \quad \frac{\alpha^2}{\beta^2} i + \frac{\mu(\alpha+\beta)}{\beta^2} \right| \quad (\bmod m),$$

et, comme $T^2$ laisse chaque indice à sa place,

$$\frac{\alpha^2}{\beta^2} \equiv 1, \quad \alpha + \beta \equiv 0 \quad (\bmod m),$$

donc $\beta \equiv -\alpha$, et l'on a

$$T = \left| i \quad -i - \frac{\mu}{\alpha} \right| \quad (\bmod m).$$

Multipliant les deux termes de $\frac{\mu}{\alpha}$ par l'entier $\mu'$ tel que $\alpha\mu' \equiv 1 \ (\bmod m)$, il vient

$$T = | i \quad -i - \mu\mu' | = S^{\mu\mu'} t \qquad \text{C. Q. F. D.}$$

*Exemple.* — Prenons $m = 5$, $\mu = 3$, $\alpha = 2$, il viendra alors

$$\mu' = 3 \quad \text{et} \quad T = | i \quad -i + 1 | \quad (\bmod 5).$$

Les équations X et Y seront

$$X = n_0 + \theta^2 n_1 + \theta^4 n_2 + \theta n_3 + \theta^3 n_4,$$
$$Y = n_0 + \theta^3 n_1 + \theta n_2 + \theta^4 n_3 + \theta^2 n_4.$$

Effectuons la substitution

$$T = | i \quad -i + 1 | = (01)(3)(24),$$

il vient

$$X' = n_1 + \theta^2 n_0 + \theta^4 n_4 + \theta n_3 + \theta^3 n_2$$
$$= \theta^2 (n_0 + \theta^3 n_1 + \theta n_2 + \theta^4 n_3 + \theta^2 n_4) = \theta^2 Y = \theta^{-\mu} Y,$$
$$Y' = n_1 + \theta^3 n_0 + \theta n_4 + \theta^4 n_3 + \theta^2 n_2$$
$$= \theta^3 (n_0 + \theta^2 n_1 + \theta^4 n_2 + \theta n_3 + \theta^3 n_4) = \theta^{\mu} X.$$

On voit, par conséquent, que le groupe G est dérivé uniquement des deux substitutions

$$S = | i \quad i+1 | \quad (\text{mod}\, m),$$

substitution circulaire entre les $m$ racines, et

$$t = | i \quad -i | \quad (\text{mod}\, m),$$

substitution qui déplace tous les indices, sauf l'indice zéro.

**21.** Théorème. — *Toutes les racines de l'équation algébrique* H, *dont le groupe est constitué comme nous venons de le voir, peuvent s'exprimer rationnellement en fonction des coefficients et de deux quelconques d'entre ces racines.*

En effet, adjoignons à l'équation deux quelconques des racines, $v_0$ et $v_1$ par exemple; par l'adjonction de ces deux racines le groupe G se réduira à celles de ses substitutions qui ne déplacent ni $v_0$ ni $v_1$; mais nous venons de voir que la substitution 1, qui laisse toutes les racines immobiles, est aussi la seule qui laisse immobile plus d'une racine. Ainsi, par l'adjonction de $v_0$ et de $v_1$, le groupe G se réduit à la seule substitution 1 : donc les $m-2$ racines $v_3, v_4, \ldots, v_{m-1}$ s'expriment rationnellement en fonction de $v_0$, de $v_1$ et des coefficients de l'équation H.

C. Q. F. D.

*Corollaire.* — L'équation différentielle linéaire Y admettra un système fondamental dont toutes les intégrales seront des fonctions rationnelles de la variable et de deux quelconques d'entre ces intégrales.

En effet, l'équation différentielle linéaire admet un système fondamental exclusivement formé de racines de l'équation algébrique H.

**22.** Théorème. — *L'équation algébrique irréductible* H, *de degré premier m, dont le groupe est constitué de la façon que nous venons de voir, est résoluble algébriquement.*

En effet, considérons les $m - 1$ fonctions

$$
(1)\quad \left\{
\begin{array}{l}
u_0 = [r_0 + \theta^{\alpha_0} r_1 + \theta^{2\alpha_0} r_2 + \ldots + \theta^{(m-1)\alpha_0} r_{m-1}]^m, \\
v_0 = [r_0 + \theta^{-\alpha_0} r_1 + \theta^{-2\alpha_0} r_2 + \ldots + \theta^{-(m-1)\alpha_0} r_{m-1}]^m, \\
\qquad\qquad \theta^m = 1, \quad \theta \gtrless 1, \\
u_1 = [r_0 + \theta^{\alpha_1} r_1 + \theta^{2\alpha_1} r_2 + \ldots + \theta^{(m-1)\alpha_1} r_{m-1}]^m, \\
v_1 = [r_0 + \theta^{-\alpha_1} r_1 + \theta^{-2\alpha_1} r_2 + \ldots + \theta^{-(m-1)\alpha_1} r_{m-1}]^m, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
u_i = [r_0 + \theta^{2\alpha_i} r_1 + \theta^{2\alpha_i} r_2 + \ldots + \theta^{(m-1)\alpha_i} r_{m-1}]^m, \\
v_i = [r_0 + \theta^{-\alpha_i} r_1 + \theta^{-2\alpha_i} r_2 + \ldots + \theta^{-(m-1)\alpha_i} r_{m-1}]^m, \\
\text{et enfin} \\
u_l = [r_0 + \theta^{\alpha_l} r_1 + \theta^{2\alpha_l} r_2 + \ldots + \theta^{(m-1)\alpha_l} r_{m-1}]^m, \\
v_l = [r_0 + \theta^{-\alpha_l} r_1 + \theta^{-2\alpha_l} r_2 + \ldots + \theta^{-(m-1)\alpha_l} r_{m-1}]^m,
\end{array}
\right.
$$

en posant

$$m - 1 = 2(l + 1).$$

Deux de ces $m - 1$ fonctions ($u_0$ et $v_0$ par exemple), toutes distinctes, se confondront avec X et Y et seront, par conséquent, nulles; mais les $2l$ autres $u_1, u_2, \ldots, u_l$ et $v_1, v_2, \ldots, v_l$ seront différentes de zéro.

Prenons $u_i$ et $v_i$; la substitution S du groupe G ne les altère pas; la substitution $t$ les permute; toute fonction symétrique de $u_i$ et de $v_i$ sera invariable par toutes les substitutions du groupe G et s'exprimera rationnellement en fonction des coefficients de H, c'est-à-dire de la variable $x$. Donc $u_i$ et $v_i$ seront racines d'une équation $W_i = 0$ du second degré, dont tous les coefficients seront des fonctions rationnelles de $x$.

Si je forme successivement les $l$ équations auxiliaires du second degré

$$W_1 = 0, \quad W_2 = 0, \quad \ldots, \quad W_l = 0,$$

j'en tirerai $u_1, u_2, \ldots, u_l, v_1, v_2, \ldots, v_l$; alors le système (1) me fournira les $m-1$ équations linéaires entre les racines

$$(1')\quad\left\{\begin{array}{l}
n_0+\theta^{\alpha_1}n_1+\ldots+\theta^{(m-1)\alpha_1}n_{m-1}=\sqrt[m]{u_1},\\
n_0+\theta^{-\alpha_1}n_1+\ldots+\theta^{-(m-1)\alpha_1}n_{m-1}=\sqrt[m]{v_1},\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
n_0+\theta^{\alpha_l}n_1+\ldots+\theta^{(m-1)\alpha_l}n_{m-1}=\sqrt[m]{u_l},\\
n_0+\theta^{-\alpha_l}n_1+\ldots+\theta^{-(m-1)\alpha_l}n_{m-1}=\sqrt[m]{v_l},\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
n_0+\theta^{\alpha_0}n_1+\ldots+\theta^{(m-1)\alpha_0}n_{m-1}=0,\\
n_0+\theta^{-\alpha_0}n_1+\ldots+\theta^{-(m-1)\alpha_0}n_{m-1}=0;
\end{array}\right.$$

ces $m-1$ équations linéaires, jointes à

$$n_0+n_1+n_2+\ldots+n_{m-1}=-A_1,$$

déterminent sans ambiguïté les $m$ racines, car le déterminant D du système ne peut être nul (n° **9**).

**23.** Théorème. — *L'équation différentielle linéaire* Y *admet un système fondamental, dont une intégrale est une fonction rationnelle* $A_1$ *de la variable* $x$, *et les* $m-3$ *autres intégrales sont deux à deux de la forme*

$$\sqrt[m]{u_i}\quad\text{et}\quad\sqrt[m]{v_i},$$

*en désignant par* $u_i$ *et* $v_i$ *les deux racines d'une équation algébrique auxiliaire* $W_i$, *du second degré et à coefficients rationnels en* $x$.

En effet, les fonctions $A_1, \sqrt[m]{u_1}, \sqrt[m]{v_1}, \ldots, \sqrt[m]{u_l}, \sqrt[m]{v_l}$ sont évidemment des intégrales de Y; il suffit de démontrer que ce sont des intégrales linéairement indépendantes. Cela est aisé à voir, car on aurait, dans le cas contraire,

$$0=\lambda_3\sqrt[m]{u_1}+\lambda_4\sqrt[m]{v_1}+\ldots+\lambda_{m-2}\sqrt[m]{u_l}+\lambda_{m-1}\sqrt[m]{v_l}+\lambda_m A_1,$$

en désignant par $\lambda_3, \ldots, \lambda_m$ des constantes, qui ne sont pas toutes nulles. Remplaçant dans cette équation $A_1, u_1, v_1, \ldots, u_l, v_l$ par les valeurs qui leur correspondent dans le système (1) (n° **22**), j'obtiens une équation linéaire, homogène, à coefficients constants entre les $m$ racines de H. Cette équation doit pouvoir s'identifier avec

$$-\lambda_1 X - \lambda_2 Y,$$

en désignant par $\lambda_1$ et $\lambda_2$ deux constantes qui ne sont pas nulles toutes les deux. La démonstration s'achève comme au n° **10**.

**24.** Toute la discussion du cas $n = 2$ peut se résumer dans la proposition suivante :

Théorème. — *Soit* Y *une équation différentielle linéaire d'ordre $p$ à coefficients rationnels en $x$, qui :* 1° *possède une intégrale rationnelle* $A_1$ ; 2° *admet un système fondamental exclusivement formé de racines d'une équation algébrique irréductible* H, *à coefficients rationnels en $x$, dont le degré est un nombre premier $m = p + 2$ ;*

1° *Il existe un système fondamental d'intégrales qui contient, outre l'intégrale rationnelle* $A_1$, $m - 3 = p - 1$ *intégrales de la forme* $\sqrt[m]{u_i}$, *en désignant par $u_i$ une fonction rationnelle de la variable ; ou bien*

2° *Il existe un système fondamental qui contient, outre la fonction rationnelle* $A_1$, $p - 1 = m - 3$ *intégrales de la forme* $\sqrt[m]{u_i}$, *en désignant par* $u_1, u_2, \ldots, u_{m-3}$, $m - 3$ *fonctions, qui sont deux à deux racines d'une même équation du second degré à coefficients rationnels.*

**25.** Il est aisé de vérifier qu'une équation différentielle linéaire, qui possède un système fondamental d'intégrales, défini comme au n° **24**, a tous ses coefficients rationnels.

Si, en effet, le système fondamental est celui du 1° (n° **24**), le calcul ne diffère en rien de celui qui termine la première Partie (n° **11**).

Si le système fondamental est celui du 2° (n° **24**), voici la vérification : on peut écrire

$$Y = \begin{vmatrix} \dfrac{d^p y}{dx^p} & \cdots & \dfrac{d^p y_i}{dx^p} & \dfrac{d^p y_{i+1}}{dx^p} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \dfrac{dy}{dx} & \cdots & \dfrac{dy_i}{dx} & \dfrac{dy_{i+1}}{dx} & \cdots \\ y & \cdots & y_i & y_{i+1} & \cdots \end{vmatrix} = 0,$$

en posant

$$(1)\qquad y_i^m = u_i, \quad y_{i+1}^m = v_i,$$

$u_i$ et $v_i$ étant les deux racines de l'équation

$$(2)\qquad W_i = w_i^2 + L_i w_i + M_i = 0.$$

Différentiant les équations (1), on a ($l$ étant un entier quelconque)

$$\frac{d^l y_i}{dx^l} = y_i \psi_l\left(x, u_i, \frac{du_i}{dx}, \cdots\right),$$

$$\frac{d^l y_{i+1}}{dx^l} = y_{i+1} \psi_l\left(x, v_i, \frac{dv_i}{dx}, \cdots\right);$$

différentiant (2) et remplaçant par leurs valeurs obtenues ainsi les dérivées successives $\frac{du_i}{dx}, \frac{d^2 u_i}{dx^2}, \cdots, \frac{dv_i}{dx}, \frac{d^2 v_i}{dx^2}, \cdots$, on a

$$(3)\qquad \frac{d_l y_i}{dx^l} = y_i \varphi_l(u_i), \qquad \frac{d_l y_{i+1}}{dx^l} = y_{i+1} \varphi_l(v_i),$$

où $\varphi_l$ désigne une fonction rationnelle et $l$ un entier quelconque.

Si je porte dans le déterminant les valeurs (3) des dérivées successives, j'obtiens, après la suppression de facteurs tels que $y_i$, communs à tous les éléments d'une colonne, un déterminant, où chaque élément dans une colonne est une fonction rationnelle de $u_i$, et l'élément correspondant de la colonne suivante est la même fonction rationnelle de $v_i$. Permutant les deux colonnes considérées, ce qui revient à permuter $u_i$ et $v_i$, on change le signe du premier membre de l'équation différentielle $Y = 0$ : donc tous les coefficients de cette équation sont des fonctions alternées de $u_i$ et de $v_i$, c'est-à-dire des fonctions de la forme

$$B_\lambda = (u_i - v_i)\,\omega(u_i, v_i),$$

$\omega$ désignant une fonction symétrique et rationnelle. Mais, en vertu de l'équation (2) et de la symétrie de la fonction $\omega$, on peut faire disparaître de $\omega$

les quantités $u_i$ et $v_i$ pour faire entrer dans $\omega$ les quantités rationnelles $L_i$ et $M_i$, coefficients de

$$(2) \qquad W_i = w_i^2 + L_i w_i + M_i = 0.$$

Raisonnant sur $u_{i'}$ et $v_{i'}$ racines de

$$W_{i'} = w_{i'}^2 + L_{i'} w_{i'} + M_{i'} = 0,$$

comme je viens de le faire sur $u_i$ et $v_i$, je ferai disparaître de $\omega$, $u_{i'}$ et $v_{i'}$, pour y faire entrer $L_{i'}$ et $M_{i'}$. Procédant ainsi de proche en proche, j'exprimerai la fonction $\omega$ rationnellement à l'aide de $L_i$, $M_i$, $L_{i'}$, $L_{i''}$, $M_{i'}$, $M_{i''}$, ..., c'est-à-dire rationnellement à l'aide de la variable $x$. Si enfin je supprime le facteur

$$(u_i - v_i)(u_{i'} - v_{i'}), \ldots,$$

commun à tous les coefficients de l'équation différentielle, ces coefficients se trouveront complètement expurgés d'irrationnelles, et la vérification se trouvera faite.

*Remarque*. — Reprenons les $2l$ fonctions

$$u_1, u_2, \ldots, u_l, \quad v_1, v_2, \ldots, v_l$$

du système (1) (n° **22**); ces fonctions sont invariables par les mêmes substitutions du groupe G : donc elles s'expriment rationnellement à l'aide de l'une quelconque d'entre elles et de fonctions symétriques des racines (JORDAN, *Traité des substitutions,* p. 50), c'est-à-dire rationnellement à l'aide de la variable $x$ et de l'une quelconque d'entre ces fonctions $u$ ou $v$. En nous reportant au théorème de M. Jordan, cité dans l'Introduction, nous voyons que l'équation auxiliaire $X = 0$ de ce théorème est du second degré, tandis que les diverses équations binômes sont toutes du degré $m$.

*Application au cas* $m = 5$. — Nous allons donner successivement un exemple des deux circonstances différentes qui peuvent se présenter.

Supposons d'abord que l'on ait, par exemple,

$$(1)\quad \left\{\begin{aligned} X &= n_0 + \theta\, n_1 + \theta^2 n_2 + \theta^3 n_3 + \theta^4 n_4 = 0, \\ Y &= n_0 + \theta^2 n_1 + \theta^4 n_2 + \theta\, n_3 + \theta^3 n_4 = 0 \qquad (\theta^5 = 1), \\ 5u &= n_0 + \theta^3 n_1 + \theta\, n_2 + \theta^4 n_3 + \theta^2 n_4, \\ 5v &= n_0 + \theta^4 n_1 + \theta^3 n_2 + \theta^2 n_3 + \theta\, n_4, \\ 5P &= n_0 + n_1 + n_2 + n_3 + n_4, \end{aligned}\right.$$

l'équation H étant

$$n^5 - 5Pn^4 + A_2 n^3 + A_3 n^2 + A_4 n + A_5 = 0.$$

Le système (1) nous fournit aisément pour les valeurs des cinq racines $n_0, n_1, n_2, n_3, n_4$ :

$$\begin{aligned} n_0 &= u + v + P, \\ n_1 &= \theta^4 u + \theta^3 v + P, \\ n_2 &= \theta^3 u + \theta\, v + P, \\ n_3 &= \theta^2 u + \theta^4 v + P, \\ n_4 &= \theta\, u + \theta^2 v + P. \end{aligned}$$

Nous n'avons rien spécifié jusqu'à présent sur la nature des quantités $u$ et $v$; nous allons vérifier directement que ces quantités sont des racines cinquièmes de fonctions rationnelles de $x$, que nous formerons.

Posons $n - P = \zeta$; $\zeta$ satisfait à l'équation à coefficients rationnels

$$Z = \zeta^5 + B_2 \zeta^3 + B_3 \zeta^2 + B_4 \zeta + B_5 = 0,$$

équation que nous formons sans peine, en remplaçant dans H, $n$ par $\zeta + P$.

Il vient ensuite

$$\begin{aligned} \zeta_0 &= u + v, \\ \zeta_1 &= \theta^4 u + \theta^3 v, \\ \zeta_2 &= \theta^3 u + \theta v, \\ \zeta_3 &= \theta^2 u + \theta^4 v, \\ \zeta_4 &= \theta\, u + \theta^2 v. \end{aligned}$$

Mais on a

$$Z = (\zeta - \zeta_0)(\zeta - \zeta_1)(\zeta - \zeta_2)(\zeta - \zeta_3)(\zeta - \zeta_4) = 0.$$

Développant ce produit, il vient finalement, tout calcul fait,

$$\zeta^5 + 5uv^2\zeta^2 - 5u^3v\zeta - (u^5 + v^5) = 0;$$

d'où, en identifiant les deux expressions de $Z = 0$,

$$B_2 = 0, \quad B_3 = 5uv^2, \quad B_4 = -5u^3v, \quad B_5 = -(u^5 + v^5),$$

d'où

$$uv^2 = \lambda, \quad u^3v = \mu,$$

en désignant par $\lambda$ et $\mu$ des quantités rationnelles; on a donc

$$u^3v^6 = \lambda^3,$$

d'où

$$v^5 = \frac{\lambda^3}{\mu}.$$

De même,

$$u^6v^2 = \mu^2,$$

d'où

$$u^5 = \frac{\mu^2}{\lambda}.$$

La vérification se trouve donc faite par un procédé purement élémentaire.

Supposons maintenant que l'on ait

$$X = n_0 + \theta n_1 + \theta^2 n_2 + \theta^3 n_3 + \theta^4 n_4 = 0,$$
$$Y = n_0 + \theta^4 n_1 + \theta^3 n_2 + \theta^2 n_3 + \theta n_4 = 0.$$

Posons

$$5u = n_0 + \theta^2 n_1 + \theta^4 n_2 + \theta n_3 + \theta^3 n_4,$$
$$5v = n_0 + \theta^3 n_1 + \theta n_2 + \theta^4 n_3 + \theta^2 n_4,$$
$$5P = n_3 + n_1 + n_2 + n_3 + n_4,$$

l'équation H étant

$$n^5 - 5Pn^4 + A_2 n^3 + A_3 n^2 + A_4 n + A_5 = 0.$$

Posant encore $n - P = \zeta$, il viendra pour $\zeta_0, \zeta_1, \zeta_2, \zeta_3, \zeta_4$ les valeurs

$$\zeta_0 = u + v, \quad \zeta_1 = \theta^4 u + \theta v, \quad \zeta_2 = \theta^3 u + \theta^2 v,$$
$$\zeta_3 = \theta^2 u + \theta^3 v, \quad \zeta_4 = \theta u + \theta^4 v.$$

Formons l'équation Z, qui sera à la fois [si $H = f(n) = 0$]

$$f(\zeta + P) = 0 = \zeta^5 + B_2 \zeta^3 + B_3 \zeta^2 + B^4 \zeta + B_5$$

et

$$(\zeta - \zeta_0)(\zeta - \zeta_1)(\zeta - \zeta_2)(\zeta - \zeta_3)(\zeta - \zeta_4) = 0,$$

c'est-à-dire, en développant, tout calcul fait,

$$\zeta^5 - 5uv\zeta^3 - 5u^2v^2\zeta - (u^5 + v^5) = 0.$$

Identifiant les deux formes de Z, on a

$$B_2 = -5uv, \quad B_3 = 0, \quad B_4 = -5u^2v^2, \quad B_5 = -(u^5 + v^5).$$

Ces relations prouvent : 1° que $u$ et $v$ s'expriment rationnellement en fonction l'un de l'autre, puisque leur produit est rationnel ; 2° que $u^5$ et $v^5$ sont les deux racines de l'équation du second degré à coefficients rationnels

$$W = w^2 + B_5 w - (\tfrac{1}{5})^5 B_2^5 = 0,$$

J'ai donc effectivement formé l'équation W à l'aide des coefficients de l'équation proposée H.

---

# TROISIÈME PARTIE.

## $n=3$.

---

### I.

**25.** L'énumération complète des groupes d'ordre fini contenus dans le groupe linéaire à trois variables a été faite par M. Jordan à la page 92 du tome 84 du *Journal de Crelle;* un groupe primitivement omis (le huitième) a été construit et discuté dans le Mémoire présenté à l'Académie de Naples (p. 21, 22 et 23). Voici cette énumération :

*Premier type.* — Toutes les substitutions sont de la forme

$$|\,XYZ \quad \alpha X+\beta Y \quad \alpha' X+\beta' Y \quad \gamma' Z\,|,$$

les coefficients $\gamma$ étant des racines de l'unité, et les coefficients $\alpha$, $\beta$, $\alpha'$, $\beta'$ tels, que les substitutions à deux variables

$$|\,XY \quad \alpha X+\beta Y \quad \alpha' X+\beta' Y\,|$$

forment un groupe $\Gamma'$ d'ordre fini. On obtiendra ainsi cinq sortes de groupes différents, suivant le type auquel appartient $\Gamma'$.

*Deuxième type.* — Le groupe est dérivé de substitutions de la forme

$$S=|\,XYZ \quad aX \quad bY \quad cZ\,|,$$

jointes à la substitution

$$T=|\,XYZ \quad a'Y \quad b'Z \quad c'X\,|$$

(les coefficients $a$, $b$, $c$, $a'$, $b'$, $c'$ sont des racines de l'unité).

*Troisième type.* — Il s'obtient en adjoignant au groupe précédent une substitution de la forme

$$T' = | \,XYZ \quad a''Y \quad b''X \quad c''Z\, |$$

(où $a''$, $b''$, $c''$ sont des racines de l'unité).

*Quatrième type.* — Le groupe est dérivé de la combinaison des substitutions

$$\lambda = | \,XYZ \quad \lambda X \quad \lambda Y \quad \lambda Z\, |,$$
$$A = | \,XYZ \quad \tau X \quad \tau^{-1} Y \quad Z\, |,$$
$$B = | \,XYZ \quad Y \quad X \quad -Z\, |,$$
$$C = \left| \begin{array}{ll} X & aX + (1-a)Y + 2a(1-a)Z \\ Y & (1-a)X + aY - 2a(1-a)Z \\ Z & X - Y + (1-2a)Z \end{array} \right|,$$

où

$$\tau^5 = 1, \quad 1 + a(\tau + \tau^{-1} - 2) = 0.$$

*Nota.* — Les formes ci-dessus de la substitution C et de l'équation qui définit $a$ sont différentes de celles qui se trouvent à la page 92 du tome 84 du *Journal de Crelle*. Cela tient à une faute d'impression, qui a défiguré le texte. La forme de C et l'équation qui définit $a$ m'ont été communiquées par M. Jordan lui-même.

*Cinquième type.* — Le groupe est dérivé de la combinaison des substitutions

$$\lambda = | \,XYZ \quad \lambda X \quad \lambda Y \quad \lambda Z\, |,$$
$$A = | \,XYZ \quad X \quad \theta Y \quad \theta^2 Z\, |,$$
$$B = | \,XYZ \quad Y \quad Z \quad X\, |,$$
$$rD = | \,XYZ \quad rjX \quad rj\theta^2 Y \quad rjZ\, |,$$
$$r^2 E = \left| \begin{array}{ll} X & r^2 a(X + Y + \theta Z) \\ Y & r^2 a(X + \theta Y + Z) \\ Z & r^2 a(X + \theta^2 Y + \theta^2 Z) \end{array} \right|,$$

où l'on a

$$\theta^3 = 1, \quad j^3 = \theta, \quad a^3 = \frac{1}{3(1-\theta^2)},$$

$\lambda^{3\rho} = 1$, $r^3 = \lambda^{\mu}$ ($\rho$ quelconque, mais entier), $\mu = 0, 1, 2$.

*Sixième type.* — Le groupe est dérivé des substitutions $\lambda$, A, B, $s$DE, où $s^4 = 1$, $\lambda$, $\lambda^2$ ou $\lambda^3$, le reste défini comme au type précédent.

*Septième type.* — Le groupe est dérivé des substitutions $\lambda$, A, B, $s$DE, $t$ED, où $t^2 = s^2$ ou $\lambda s^2$, le reste défini comme au type précédent.

*Huitième type.* — Le groupe est dérivé de la combinaison des substitutions

$$\lambda = | \, XYZ \quad \lambda X \quad \lambda Y \quad \lambda Z \, |,$$

$$A = | \, XYZ \quad \tau X \quad \tau^2 Y \quad \tau^4 Z \, |,$$

$$B = | \, XYZ \quad Y \quad Z \quad X \, |,$$

$$C = \left| \begin{array}{ll} X & aX + cY + bZ \\ Y & cX + bY + aZ \\ Z & bX + aY + cZ \end{array} \right|,$$

où $\tau^7 = 1$, et $a$, $b$, $c$ sont définis par le système linéaire

$$\begin{aligned} a \quad + b \quad + c \quad &= -1, \\ a\tau + b\tau^2 + c\tau^4 &= 0, \\ a\tau^6 + b\tau^5 + c\tau^3 &= 0. \end{aligned}$$

**26.** Convenons d'abord des notations suivantes : soient $X = 0$, $Y = 0$, $Z = 0$ les trois équations linéaires, homogènes, à coefficients constants, qui existent entre les $m$ racines de H ; je désigne par

| | | | | |
|---|---|---|---|---|
| $N_0$ | le système des | $n_0$ | racines communes à | X, Y et Z; |
| $N_{12}$ | » | $n_{12}$ | » | X, Y; |
| $N_{13}$ | » | $n_{13}$ | » | X, Z; |
| $N_{23}$ | » | $n_{23}$ | » | Y, Z. |

De même, je désigne par

| | | | | | |
|---|---|---|---|---|---|
| $N_1$ | le système des | $n_1$ | racines qui figurent dans | | X seul; |
| $N_2$ | » | $n_2$ | » | » | Y seul; |
| $N_3$ | » | $n_3$ | » | » | Z seul; |

on aura (**6**, corollaire III),

$$n_0 + n_{12} + n_{13} + n_{23} + n_1 + n_2 + n_3 = m.$$

Cela posé, je vais établir trois lemmes, qui me permettront d'éliminer immédiatement tous les types de M. Jordan, excepté le premier, le second, le quatrième.

*Lemme I.* — Si le groupe Γ contient une substitution S de la forme

$$S = |\ XYZ \quad aX \quad bY \quad cZ\ |,$$

où

$a$ est une racine primitive $\alpha^{\text{ième}}$ de l'unité;
$b$ » » $\beta^{\text{ième}}$ » ;
$c$ » » $\gamma^{\text{ième}}$ » ;

le plus grand commun diviseur $\delta$ de $\alpha$, $\beta$ et $\gamma$ doit diviser $m$, c'est-à-dire $\delta = 1$ ou $\delta = m$.

En effet, chacun des systèmes $N_0$, $N_{12}$, $N_{13}$, $N_{23}$, $N_1$, $N_2$, $N_3$ contient un nombre entier de cycles de S et cette substitution permute entre elles des racines d'un même système.

Car, supposons qu'il n'en soit point ainsi, et que S fasse entrer une racine $n_i$ de $N_{12}$ dans le système $N_0$ par exemple. Soient X', Y', Z' ce que deviennent X, Y, Z par l'effet de la substitution S, $n_i$ figurerait dans X', Y', Z'; mais on a identiquement

$$Z' = cZ,$$

et $n_i$ figurerait dans le premier membre de cette identité, sans figurer dans le second, ce qui est absurde. On démontrera par un raisonnement tout pareil que chacun des sept systèmes $N_0$, $N_{12}$, $N_{13}$, $N_{23}$, $N_1$, $N_2$, $N_3$ contient un nombre entier de cycles de S.

Cela posé, en vertu du théorème II du n° **7**,

$\alpha$ divise $n_0$, $n_{12}$, $n_{13}$, $n_1$;
$\beta$ » $n_0$, $n_{12}$, $n_{23}$, $n_2$;
$\gamma$ » $n_0$, $n_{13}$, $n_{23}$, $n_3$;

et leur plus grand commun diviseur $\delta$ divise

$$n_0 + n_{12} + n_{13} + n_{23} + n_1 + n_2 + n_3,$$

c'est-à-dire $m$. Donc $\delta = 1$ ou $\delta = m$ ; dans ce dernier cas, on a évidemment

$$n_{12} = n_{13} = n_{23} = n_1 = n_2 = n_3 = 0, \quad n_0 = m.$$

S est une substitution circulaire entre les $m$ racines.

*Corollaire.* — Si le groupe $\Gamma$ contient une substitution S de la forme

$$S | \, XYZ \quad \lambda X \quad \lambda Y \quad \lambda Z \, |,$$

on a $\lambda = 1$.

En effet, si $\lambda \gtrless 1$, $\lambda^m = 1$ en vertu du lemme précédent et la substitution S est une substitution circulaire entre les $m$ racines. Mais, dans ce cas, on a (7, théorème I[er], Remarque),

$$\begin{aligned} X &= \mathfrak{n}_0 + \lambda^{m-1}\mathfrak{n}_1 + \lambda^{m-2}\mathfrak{n}_2 + \ldots + \lambda\mathfrak{n}_{m-1}, \\ Y &= \mathfrak{n}_0 + \lambda^{m-1}\mathfrak{n}_1 + \ldots + \lambda\mathfrak{n}_{m-1}, \\ Z &= \mathfrak{n}_0 + \lambda^{m-1}\mathfrak{n}_1 + \ldots + \lambda\mathfrak{n}_{m-1}, \end{aligned}$$

et les trois équations $X = 0$, $Y = 0$, $Z = 0$ ne sont plus distinctes, ce qui est absurde.

Donc

$$\lambda = 1. \qquad \text{C. Q. F. D.}$$

*Lemme II.* — Si le groupe $\Gamma$ contient une substitution T de la forme

$$T = | \, XYZ \quad a'Y \quad b'Z \quad c'X \, |,$$

on a

$$n_{12} = n_{23} = n_{13} = \mu, \quad n_1 = n_2 = n_3 = \nu.$$

Considérons d'abord le système $N_1$ par exemple; je dis que T déplace toutes les $n_1$ racines de $N_1$ ; supposons, en effet, que T laisse immobile une racine $\mathfrak{n}_i$ de $N_1$ ; soit X', Y', Z' ce que deviennent X, Y et Z par l'effet de la substitution T; $\mathfrak{n}_i$ figurerait encore dans X', mais on a identiquement

$$X' = a'Y,$$

et $n_i$ figurerait dans le premier membre de cette identité sans figurer dans le second, ce qui est absurde.

Je dis, en second lieu, que T ne saurait faire entrer une racine $n_i$ de $N_1$, ni dans $N_0$, ni dans aucun des trois systèmes $N_{12}$, $N_{23}$, $N_{13}$. Si, en effet, $n_i$ prend la place d'une racine de $N_0$, $n_i$ figurera dans $X'$, $Y'$ et $Z'$, mais on a identiquement

$$Y' = b'Z, \quad X' = a'Y,$$

et l'on voit que l'hypothèse est absurde, puisque le premier membre de ces identités contiendrait $n_i$ sans que le second la contienne.

De même, aucune racine de $N_1$ ne peut entrer dans $N_{12}$ ou $N_{13}$ ou $N_{23}$, et ce que je viens de dire de $N_1$ s'applique à $N_2$ et à $N_3$.

Les raisonnements sont identiques pour démontrer : 1° que T déplace toutes les racines de $N_{12}$, de $N_{13}$, de $N_{23}$; 2° ne fait entrer aucune de ces racines dans $N_0$, $N_1$, $N_2$ ou $N_3$; 3° permute entre elles des racines de $N_0$.

En second lieu, je dis que toutes les $n_1$ racines de $N_1$ entrent dans $N_3$. En effet, si une racine $n_i$ de $N_1$ entre dans le système $N_2$, $n_i$ figurera dans $Y'$, mais

$$Y' = b'Z,$$

et $n_i$ figurerait dans le premier membre de cette identité sans figurer dans le second, ce qui est absurde. On verra ensuite que, par l'effet de la substitution T,

les $n_2$ racines de $N_2$ entrent dans $N_1$;
» $n_3$ » $N_3$ » $N_2$;

d'où

$$n_1 \leq n_3, \quad n_2 \leq n_1, \quad n_3 \leq n_2,$$

c'est-à-dire, forcément,

$$n_1 = n_2 = n_3.$$

On démontrera par un procédé identique que : 1° la substitution T fait entrer

les $n_{12}$ racines de $N_{12}$ dans $N_{13}$;
» $n_{13}$ » $N_{13}$ » $N_{23}$;
» $n_{23}$ » $N_{23}$ » $N_{12}$;

2° Que l'on a forcément

$$n_{12} = n_{13} = n_{23}. \qquad \text{C. Q. F. D.}$$

La substitution T peut donc se mettre sous la forme symbolique suivante :

$$T = (N_0)(N_{12}N_{23}N_{13})(N_1N_2N_3).$$

Faisant usage de la même notation symbolique, il viendrait pour la substitution S,

$$S = | XYZ \quad aX \quad bY \quad cZ |,$$

l'expression

$$S = (N_0)(N_{12})(N_{13})(N_{23})(N_1)(N_2)(N_3).$$

*Remarque.* — Raisonnant sur la substitution T',

$$T' = | XYZ \quad a''Y \quad b''X \quad c''Z |,$$

comme on vient de le faire sur la substitution T, on démontrera par un procédé identique que : 1° l'on a

$$n_1 = n_2 \quad \text{et} \quad n_{13} = n_{23};$$

2° T' peut se mettre sous la forme symbolique

$$T' = (N_0)(N_{12})(N_3)(N_1N_2)(N_{13}N_{23}).$$

*Lemme III.* — S'il existe une fonction linéaire et homogène U de X, Y et Z, que *toutes* les substitutions du groupe Γ multiplient par des facteurs constants, le groupe G se réduira aux puissances d'une seule substitution circulaire entre les $m$ racines.

Je dis, en premier lieu, que U contient toutes les $m$ racines; supposons, en effet, qu'il n'en soit point ainsi : soit $n_i$ une racine qui figure dans U, $n_j$ une racine qui n'y figure pas. Le groupe G, étant transitif, contient au moins une substitution S, qui remplace $n_i$ par $n_j$; mais, en vertu de l'hypothèse, S transforme U en $U' = KU$; or $U'$ contient $n_j$ et KU ne contient pas $n_j$ : donc l'identité

$$U' = KU$$

est impossible, ce qui est contre l'hypothèse.

Puisque nous avons démontré que U contient toutes les racines, nous rentrons dans le cas traité précédemment dans la première Partie (**8**), et l'on démontrera par un raisonnement identique : 1° que le groupe G est formé par les puissances d'une seule substitution circulaire entre les $m$ racines; 2° que les facteurs, tels que K, sont ou bien égaux à l'unité, ou bien des racines $m^{\text{ièmes}}$ de l'unité.

Le lemme est donc démontré.

**27.** Théorème. — *Le groupe* $\Gamma$, *dérivé de substitutions* S *de la forme*

$$S = |\, XYZ \quad aX \quad bY \quad cZ \,|,$$

*jointes aux deux substitutions*

$$T = |\, XYZ \quad a'Y \quad b'Z \quad c'X \,|$$

*et*

$$T' = |\, XYZ \quad a''Y \quad b''X \quad c''Z \,|,$$

*ne peut fournir aucun type d'équations algébriques irréductibles* H *de degré premier* $m$.

La démonstration de ce théorème repose sur deux lemmes, que je vais successivement établir.

*Lemme I.* — Chacune des fonctions X, Y, Z contient toutes les $m$ racines.

En effet, faisant usage de la notation symbolique adoptée à la fin du lemme II du n° **26**, je vois que l'on a

$$\begin{aligned} S &= (N_0)(N_1)(N_2)(N_3)(N_{12})(N_{13})(N_{23}),\\ T' &= (N_0)(N_{12})(N_3)(N_1N_2)(N_{13}N_{23}),\\ T &= (N_0)(N_{12}N_{23}N_{13})(N_1N_2N_3); \end{aligned}$$

on voit donc que, si je répartis les sept systèmes de racines $N_0$, $N_{12}$, $N_{13}$, $N_{23}$, $N_1$, $N_2$, $N_3$ en trois groupes

(1) $N_0$,

(2) $N_{12}$ $N_{13}$ $N_{23}$,

(3) $N_1$ $N_2$ $N_3$,

il n'existera pas dans le groupe G de substitution capable de faire passer une racine d'un quelconque des groupes (1), (2) ou (3) dans l'un quelconque des deux autres. Or le groupe G est transitif : donc l'un des trois groupes (1), (2) ou (3) subsiste seul et les deux autres doivent ne pas exister.

D'ailleurs, on a (**26**, lemme II), puisque la substitution T entre dans le groupe Γ,

$$n_1 = n_2 = n_3 = \mu, \quad n_{12} + n_{13} + n_{23} = \nu$$

et (**6**, corollaire III)

$$n_0 + 3\mu + 3\nu = m.$$

Si donc je suppose que le groupe (1), c'est-à-dire le système $N_0$, disparaît, il faut supposer $n_0 = 0$, et il reste

$$3(\mu + \nu) = m,$$

ce qui est absurde, puisque $m$ est premier.

Donc ce sont les groupes (2) et (3) qui disparaissent; le groupe (1) subsiste seul; par conséquent,

$$n_1 = n_2 = n_3 = n_{12} = n_{13} = n_{23} = 0 \quad \text{et} \quad n_0 = m,$$

et le lemme est démontré.

*Lemme II.* — On a

$$a'' = a', \quad b'' = \frac{1}{a'}, \quad c'' = 1,$$

et, par conséquent, la substitution T' a la forme

$$T' = \left| XYZ \quad a'Y \quad \frac{1}{a'}X \quad Z \right|,$$

la substitution T étant

$$T = | XYZ \quad a'Y \quad b'Z \quad c'X |.$$

Pour démontrer ce lemme, considérons la substitution

$$T' = | XYZ \quad a''Y \quad b''Y \quad c''Z |;$$

puisque Z contient toutes les $m$ racines (lemme I), on a $c'' = 1$ ou bien $c''^m = 1$ (**7**, corollaire).

Supposons d'abord $c''^m = 1$ ou $c'' = \theta$, en désignant, suivant l'habitude, par $\theta$ une racine $m^{\text{ième}}$ de l'unité; dans ce cas, T' est une substitution circulaire entre les $m$ racines

$$T' = (n_0 n_1 \ldots n_{m-1}),$$

ou encore

$$T' = | i \quad i+1 | \quad (\text{mod}\, m).$$

Cela posé, soient

$$X = \ldots + \alpha_i n_i + \alpha_{i+1} n_{i+1} + \ldots,$$
$$Y = \ldots + \beta_i n_i + \beta_{i+1} n_{i+1} + \ldots;$$

aucun des $m$ coefficients $\alpha$ ou des $m$ coefficients $\beta$ ne sera nul. Si je désigne par X' et Y' ce que deviennent X et Y par l'effet de la substitution T', il viendra

$$X' = \ldots + \alpha_i n_{i+1} + \alpha_{i+1} n_{i+2} + \ldots,$$
$$Y' = \ldots + \beta_i n_{i+1} + \beta_{i+1} n_{i+2} + \ldots.$$

D'ailleurs,

$$a''Y = \ldots + a''\beta_i n_i + a''\beta_{i+1} n_{i+1} + \ldots,$$
$$b''X = \ldots + b''\alpha_i n_i + b''\alpha_{i+1} n_{i+1} + \ldots.$$

Mais on a identiquement

$$X' = a''Y, \quad Y' = b''X.$$

Donc il vient ($i = 0, 1, 2, \ldots, m-1$), en identifiant,

$$\alpha_i = a''\beta_{i+1}, \quad \beta_i = b''\alpha_{i+1},$$

et de même

$$\alpha_{i+1} = a''\beta_{i+2}, \quad \beta_{i+1} = b''\alpha_{i+2},$$

c'est-à-dire

$$\alpha_i = a''b''\alpha_{i+2}, \quad \beta_i = a''b''\beta_{i+2},$$

d'où, en posant $a''b''u = 1$,

$$\alpha_{i+2} = u\alpha_i, \quad \beta_{i+2} = u\alpha_i.$$

Il vient pour X et Y la forme suivante :

$$X = \eta_0 + u^{\frac{m+1}{2}}\eta_1 + u\eta_2 + u^{\frac{m+3}{2}}\eta_3 + \ldots + u^{\frac{m-1}{2}}\eta_{m-1},$$

$$Y = \eta_0 + u^{\frac{m+1}{2}}\eta_1 + u\eta_2 + \ldots + u^{\frac{m-1}{2}}\eta_{m-1},$$

et les deux équations $X = 0$, $Y = 0$ ne seraient plus distinctes, ce qui est absurde.

Il faut donc supposer forcément $c'' = 1$. Mais alors reprenons la substitution

$$T'^2 = |\, XYZ \quad a''b''X \quad a''b''Y \quad Z \,|;$$

puisque X et Y contiennent chacune toutes les $m$ racines, on a

$$a''b'' = 1 \quad \text{ou} \quad a''b'' = \theta^l \quad (\theta^m = 1)$$

(n° **6**, lemme I et n° **7**).

Si $a''b'' = \theta^l$, il vient pour X et Y la forme

$$X = \eta_0 + \theta^{-l}\eta_1 + \theta^{-2l}\eta_1 + \ldots + \theta^{-(m-1)l}\eta_{m-1},$$

$$Y = \eta_0 + \theta^{-l}r_1 + \theta^{-2l}\eta + \ldots + \theta^{-(m-1)l}\eta_{m-1};$$

les deux équations $X = 0$ et $Y = 0$ ne seraient encore pas distinctes, ce qui est absurde.

Donc

$$a'' b'' = 1 \qquad \text{C. Q. F. D.}$$

et T′ est de la forme

$$T' = | \; XYZ \quad a''Y \quad a''^{-1}Z \quad Z \; |.$$

Cela posé, reprenons la substitution

$$T = | \; XYZ \quad a'Y \quad b'Z \quad c'X \; |$$

et

$$T^3 = | \; XYZ \quad a'b'c'X \quad a'b'c'Y \quad a'b'c'Z \; |;$$

on a $a'b'c' = 1$ (**26**, lemme I, corollaire).

Raisonnant maintenant sur la substitution

$$TT' = \left| \; XYZ \quad a''b'Z \quad \frac{a'}{a''}Y \quad c'Z \; \right|,$$

comme je viens de le faire sur T′, j'obtiens

$$\frac{a'}{a''} = 1 \quad \text{d'où} \quad a' = a'', \quad a''b'c' = 1,$$

c'est-à-dire $a'' = a'$ encore, puisque $a'b'c' = 1$. En résumé, on a bien

$$c'' = 1, \quad a'' = a', \quad b'' = \frac{1}{a},$$

et le lemme est démontré

*Remarque.* — Considérons la fonction

$$U = X + a'Y + a'b'Z.$$

T transforme U en

$$a'Y + a'b'Z + a'b'c'X,$$

c'est-à-dire en U, puisque $a'b'c' = 1$. La substitution T′ transforme U en

$$a'Y + X + a'b'Z,$$

c'est-à-dire encore en U. Cette remarque nous sera fort utile pour la démonstration du théorème.

Après avoir établi les deux lemmes dont nous avons besoin, reprenons les substitutions

$$S = | \; XYZ \quad aX \quad bY \quad cZ \; |,$$

où chacun des coefficients $a, b, c$ est 1 ou une racine primitive $\theta$ de l'unité.

Supposons d'abord qu'aucun des trois coefficients $a, b, c$ n'est 1, et posons

$$a = \theta^{\alpha}, \quad b = \theta^{\beta}, \quad c = \theta^{\gamma} \quad (\theta^{m} = 1).$$

Il viendra pour les fonctions X, Y, Z les formes suivantes (**8**) :

$$X = \eta_0 + \theta^{-\alpha}\eta_1 + \theta^{-2\alpha}\eta_2 + \ldots + \theta^{-(m-1)\alpha}\eta_{m-1},$$
$$Y = \eta_0 + \theta^{-\beta}\eta_1 + \ldots + \theta^{-(m-1)\beta}\eta_{m-1}$$

et

$$Z = \eta_0 + \theta^{-\gamma}\eta_1 + \ldots + \theta^{-(m-1)\gamma}\eta_{m-1};$$

on voit que dans X, dans Y et dans Z les coefficients des racines sont tous inégaux.

Cela posé, reprenons la substitution

$$T' = \left| \; XYZ \quad a'Y \quad \frac{1}{a'}X \quad Z \; \right|;$$

suivant une remarque déjà faite dans la démonstration du lemme II, T′, qui multiplie Z par 1, ne déplace que les racines affectées dans Z de coefficients égaux ; mais nous venons de voir que les coefficients des racines dans Z sont tous inégaux ; donc T′ se réduit à la substitution 1 et laisse toutes les racines immobiles, ce qui est absurde.

Si maintenant je suppose $\gamma = 0$, $c = 1$, la substitution S est encore circulaire et il me viendra pour Z

$$Z = \eta_0 + \eta_1 + \ldots + \eta_{m-1},$$

ce qui est absurde, puisque la somme des racines de l'équation algébrique H n'est pas nulle.

Il faut donc supposer simultanément $\alpha = \beta = \gamma = 0$ et $a = b = c = 1$. Mais, dans ce dernier cas, reprenons la fonction

$$U = X + a'Y + a'b'Z.$$

T, T′ et S multiplient U par 1 : donc (**26**, lemme III)

$$U = n_0 + n_1 + \ldots + n_{m-1},$$

ce qui est impossible.

En admettant donc dans le groupe Γ l'existence simultanée des substitutions T et T′, on arrive dans tous les cas à des absurdités : par suite, T et T′ sont incompatibles. Si je supprime T du groupe Γ, je retombe sur le premier type de M. Jordan ; supprimant, au contraire, T′, je ramène Γ au second type.

Le théorème est donc démontré.

**28**. Théorème. — *Le groupe* Γ (*cinquième type*), *dérivé des substitutions*

$$\lambda = |\,XYZ \quad \lambda X \quad \lambda Y \quad \lambda Z\,|,$$

$$A = |\,XYZ \quad X \quad \theta Y \quad \theta^2 Z\,|,$$

$$B = |\,XYZ \quad Y \quad Z \quad X\,|,$$

$$rD = |\,XYZ \quad rjX \quad rj\theta^2 Y \quad rjZ\,|,$$

$$r^2 E = \left|\begin{array}{ll} X & r^2 a(X + Y + \theta Z) \\ Y & r^2 a(X + \theta Y + Z) \\ Z & r^2 a(X + \theta^2 Y + \theta^2 Z) \end{array}\right|,$$

*où l'on a*

$$\theta^3 = 1, \quad j^3 = \theta, \quad a^3 = \frac{1}{3(1-\theta^2)},$$

$\lambda^{3\rho} = 1$, $r^3 = \lambda^\mu$ ($\rho$ *entier quelconque*, $\mu = 0, 1, 2$), *ne peut fournir aucun type d'équation algébrique irréductible de degré premier* $m$.

En premier lieu, on a (**26**, lemme I, corollaire)

$$\lambda = 1, \quad \text{d'où} \quad \rho = 0, \quad r^3 = 1.$$

En second lieu, la substitution $rD$ est impossible ; en effet, si Γ contient la substitution

$$rD = | \, XYZ \quad rjX \quad rj\theta^2 Y \quad rjZ \, |,$$

$\Gamma$ contiendra également la substitution

$$(rD)^3 = | \, XYZ \quad r^3 j^3 X \quad r^3 j^3 \theta^6 Y \quad r^3 j^3 Z \, |,$$

c'est-à-dire, puisque $r^3 = 1$, $j^3 = \theta$, $\theta^3 = 1$,

$$(rD)^3 = | \, XYZ \quad \theta X \quad \theta Y \quad \theta Z \, |.$$

Or cela est contraire au corollaire du lemme I du n° **26** : donc la substitution $rD$ est impossible.

Le groupe $\Gamma$ se réduit, par conséquent, aux substitutions A, B et $r^2$E; mais je vais démontrer que les substitutions A et B sont incompatibles. Si B existe dans le groupe $\Gamma$, on a (**26**, lemme II)

$$n_1 = n_2 = n_3 = \mu, \quad n_{12} = n_{13} = n_{23} = \nu, \quad n_0 + 3\mu + 3\nu = m;$$

mais si A existe, comme $\theta$ est une racine cubique de l'unité, 3 divise $n_0$, $n_{12}$, c'est-à-dire $\nu$ et $n_2$, c'est-à-dire $\mu$ (**26**, lemme I) : donc 3 divise

$$n_0 + 3\mu + 3\nu \quad \text{ou} \quad m,$$

ce qui est absurde.

Je ne puis donc, pour former le groupe $\Gamma$, combiner $r^2$E qu'à la substitution A seule, ou à la substitution B seule. Cela posé, je vais démontrer le lemme suivant :

*Lemme.* — On a entre les substitutions A, B, E les relations

$$AE = EB, \quad BE = EA^2B^2.$$

Cela est aisé à vérifier, car

$$AE = \left| \begin{array}{ll} X & a(X + \theta Y + Z) \\ Y & a(X + \theta^2 Y + \theta^2 Z) \\ Z & a(X + Y + \theta Z) \end{array} \right|,$$

et de même la substitution EB a la forme

$$EB = \begin{vmatrix} X & a(X + \theta X + Z) \\ Y & a(X + \theta^2 Y + \theta^2 Z) \\ Z & a(X + Y + \theta Z) \end{vmatrix}.$$

Pareillement

$$BE = \begin{vmatrix} X & a(\theta X + Y + Z) \\ Y & a(X + Y + \theta Z) \\ Z & a(\theta^2 X + Y + \theta^2 Z) \end{vmatrix},$$

et

$$EA^2 B^2 = \begin{vmatrix} X & a\theta(X + \theta^2 Y + \theta^2 Z) \\ Y & a(X + Y + \theta Z) \\ Z & a\theta^2(X + \theta Y + Z) \end{vmatrix};$$

donc

$$AE = EB, \quad BE = EA^2 B^2, \qquad \text{C. Q. F. D.}$$

Cela posé : 1° combinons $r^2 E$ avec A ; le groupe Γ contiendra la substitution

$$(r^2 E)^{-1} A (r^2 E),$$

c'est-à-dire B, ce qui est impossible ; 2° combinons $r^2 E$ avec B : le groupe Γ contiendra la substitution

$$(r^2 E)^{-1} B (r^2 E) B^{-2},$$

c'est-à-dire $A^2$, ce qui est impossible.

En résumé, le groupe Γ se réduit, dans tous les cas, à une seule des trois substitutions A, B et $r^2 E$. Soit

$$| X_1 Y_1 Z_1 \quad a_1 X_1 \quad b_1 Y_1 \quad c_1 Z_1 |$$

la forme canonique de cette substitution ; je retombe sur le premier des huit types de M. Jordan, et le théorème est démontré.

**29.** Théorème. — *Le groupe* $\Gamma$ (*sixième type*), *dérivé des substitutions*

$$\lambda,\quad A,\quad B,\quad s\,DE$$

(*où* $s^4 = 1, \lambda, \lambda^2, \lambda^3$, *le reste défini comme au type précédent*), *ne peut fournir aucun type d'équation algébrique irréductible de degré premier m.*

On démontrera, comme au cas précédent : 1° que $\lambda = 1$, d'où $s^4 = 1$ ; 2° que les substitutions A et B sont incompatibles.

Cela posé, considérons la substitution DE, qui sera de la forme

$$DE = \left| \begin{array}{ll} X & aj(X + \theta^2 Y + \theta Z) \\ Y & aj(X + Y + Z) \\ Z & aj(X + \theta Y + \theta^2 Z) \end{array} \right|.$$

Je dis qu'on a les relations

$$ADE = DEB, \qquad BDE = \theta DEA^2.$$

En effet,

$$ADE = \left| \begin{array}{ll} X & aj(X + Y + Z) \\ Y & aj(X + \theta Y + \theta^2 Z) \\ Z & aj(X + \theta^2 Y + \theta Z) \end{array} \right|,$$

et

$$DEB = \left| \begin{array}{ll} X & aj(X + Y + Z) \\ Y & aj(X + \theta Y + \theta^2 Z) \\ Z & aj(X + \theta^2 Y + \theta Z) \end{array} \right|.$$

Pareillement

$$BDE = \left| \begin{array}{ll} X & aj(\theta X + Y + \theta^2 Z) \\ Y & aj(X + Y + Z) \\ Z & aj(\theta^2 X + Y + \theta Z) \end{array} \right|,$$

et

$$\theta DEA^2 = \left| \begin{array}{ll} X & aj\theta(X + \theta^2 Y + \theta Z) \\ Y & aj(X + Y + Z) \\ Z & aj\theta^2(X + \theta Y + \theta^2 Z) \end{array} \right|.$$

Par conséquent : 1° si nous combinons $s$DE avec A, le groupe $\Gamma$ contiendra la substitution

$$(s\mathrm{DE})^{-1}\mathrm{A}(s\mathrm{DE}) = \mathrm{B},$$

ce qui est impossible, puisque A et B sont incompatibles; 2° si nous combinons $s$DE avec B, le groupe $\Gamma$ contiendra la substitution

$$(s\mathrm{DE})^{-1}\mathrm{B}(s\mathrm{DE}) = \theta\mathrm{A}^2,$$

ce qui est encore impossible.

En résumé, le groupe $\Gamma$ se réduit à l'une des trois substitutions

$$\mathrm{A},\ \mathrm{B},\ s\mathrm{DE},$$

et le raisonnement s'achève comme dans le cas précédent.

**30.** Théorème. — *Le groupe* $\Gamma$ (*septième type*), *dérivé des substitutions*

$$\lambda,\ \mathrm{A},\ \mathrm{B},\ s\mathrm{DE},\ t\mathrm{ED}$$

(*où* $t^2 = s^2$ *ou* $\lambda s^2$, *le reste défini comme au type précédent*), *ne peut fournir aucun type d'équations algébriques irréductibles* H *de degré premier* $m$.

On verra, comme dans le cas précédent, que $\lambda = 1$; d'où $t^4 = s^4 = 1$. Je dis ensuite que la substitution $t$ED est impossible. Si cela est, le groupe $\Gamma$ se ramène au type qui vient d'être traité.

Pour démontrer que la substitution $t$ED ne peut exister dans $\Gamma$, je considère cette substitution

$$\mathrm{ED} = \begin{vmatrix} \mathrm{X} & aj(\mathrm{X} + \mathrm{Y} + \theta\mathrm{Z}) \\ \mathrm{Y} & aj(\theta^2\mathrm{X} + \mathrm{Y} + \theta^2\mathrm{Z}) \\ \mathrm{Z} & aj(\mathrm{X} + \theta^2\mathrm{Y} + \theta^2\mathrm{Z}) \end{vmatrix};$$

l'équation caractéristique en K (4) relative à ED est, en posant $\mathrm{K} = aj\mathrm{K}'$,

$$\begin{vmatrix} 1-\mathrm{K}' & 1 & \theta \\ \theta^2 & 1-\mathrm{K}' & \theta^2 \\ 1 & \theta^2 & \theta^2-\mathrm{K}' \end{vmatrix} = 0,$$

c'est-à-dire

$$(K' + \theta - 1)(K'^2 - 3\theta) = 0.$$

Les trois valeurs de K, savoir $K_1$, $K_2$, $K_3$, satisfont donc aux relations

$$K_1 = aj(1 - \theta); \quad K_2^2 = 3\theta a^2 j^2, \quad K_3^2 = 3\theta a^2 j^2.$$

Élevant au cube, il vient

$$K_1^3 = a^3 j^3 (1 - \theta)^3 = a^3\theta(1 - 3\theta + 3\theta^2 - 1) = \frac{\theta^2(\theta - 1)}{1 - \theta^2} = -\frac{\theta^2}{1 + \theta} = 1,$$

$$K_2^6 = 27 a^6 \theta^2 = \frac{27\theta^2}{9(1 - 2\theta^2 + \theta)} = -\frac{27\theta^2}{27\theta^2} = -1,$$

et pareillement

$$K_3^6 = -1.$$

Donc

$$K_1 = \theta^\alpha, \quad K_2^2 = -\theta^\beta, \quad K_3^2 = -\theta^\beta,$$

aucun des exposants $\alpha$ et $\beta$ n'étant nul. On voit que $K_1$ est une racine cubique, $K_2$ et $K_3$ des racines sixièmes de l'unité.

Cela posé, considérons la forme canonique de la substitution $t$ED,

$$t\mathrm{ED} = |\, X_1 Y_1 Z_1 \quad tK_1 X_1 \quad tK_2 Y_1 \quad tK_3 Z_1 \,|.$$

La substitution $(t\mathrm{ED})^4 = (\mathrm{ED})^4$, puisque $t^4 = 1$, et sera de la forme

$$(t\mathrm{ED})^4 = |\, X_1 Y_1 Z_1 \quad K_1^4 X_1 \quad K_2^4 Y_1 \quad K_3^4 Z_1 \,|;$$

or, d'après ce que nous venons de dire, $K_1^4$, $K_2^4$ et $K_3^4$ sont des racines cubiques de l'unité : donc (**26**, lemme I) 3 diviserait $m$, ce qui est absurde.

Le groupe $\Gamma$ est ainsi ramené au cas traité précédemment (**29**), et le raisonnement s'achève comme plus haut.

**31**. Théorème. — *Le groupe* $\Gamma$ (*huitième type*), *dérivé des substitutions*

$$\lambda = |\, XYZ \quad \lambda X \quad \lambda Y \quad \lambda Z \,|,$$
$$A = |\, XYZ \quad \tau X \quad \tau^2 Y \quad \tau^4 Z \,|,$$
$$B = |\, XYZ \quad Y \quad Z \quad X \,|,$$
$$C = \left|\begin{matrix} X & aX + cY + bZ \\ Y & cX + bY + aZ \\ Z & bX + aY + cZ \end{matrix}\right|,$$

*ne peut fournir aucun type d'équations algébriques irréductibles* H *de degré premier m.*

On a d'ailleurs $\tau^7 = 1$; les coefficients $a$, $b$ et $c$ sont définis par le système linéaire

$$\begin{aligned} a + b + c &= -1, \\ a\tau + b\tau^2 + c\tau^4 &= 0, \\ a\tau^6 + b\tau^5 + c\tau^3 &= 0. \end{aligned}$$

La substitution A est impossible (**26**, lemme I), puisque 7 ne divise pas $m$. (J'examinerai tout à l'heure le cas $m = 7$.) Γ se réduit, par conséquent, aux deux substitutions B et C. Or considérons la fonction U

$$U = X + Y + Z;$$

B multiplie U par 1 et C multiplie U par $-1$.

Puisque toutes les substitutions du groupe Γ multiplient U par des constantes, on retombe sur un cas précédemment traité (**26**, lemme III). Les constantes par lesquelles les substitutions de Γ multiplient U ne peuvent être égales qu'à l'unité ou à des racines $m^{\text{ièmes}}$ de l'unité. Mais C multiplie U par la constante $-1$ : donc la substitution C est impossible, puisque $-1$ est une racine carrée de l'unité.

Le groupe Γ se réduit, par suite à la seule substitution B; si l'on ramène B à sa forme canonique, on retombe sur le premier des huit types énumérés par M. Jordan, ce qui est contre l'hypothèse.

Le théorème se trouve donc démontré.

**32.** Pour achever la discussion du huitième type de M. Jordan, il nous faut supposer $m = 7$, et dans ce cas la substitution A est possible.

Je dis que les substitutions A, B et C existent nécessairement toutes les trois dans le groupe Γ. En effet, je ne puis supprimer A sans rentrer dans le cas que je viens de traiter; je ne puis supprimer C sans rentrer dans le second des huit types de M. Jordan. Il me suffira de démontrer qu'il est impossible de supprimer B du groupe Γ.

On sait (*Mémoires couronnés par l'Académie de Naples*, t. LX, p. 23) que l'on a

$$CA^{\rho}C = A^{\mu}CB^{\nu}A^{\varpi},$$

où $\rho$, $\mu$, $\varpi$ désignent des entiers convenablement choisis entre 1 et 7, $\nu$ un entier convenablement choisi entre 1 et 3.

Si donc le groupe $\Gamma$ contient les substitutions A et C, il contiendra la substitution

$$(A^{\mu}C)^{-1}.CA^{\rho}C.A^{-\varpi},$$

c'est-à-dire $B^{\nu}$.

Donc A, B et C coexistent nécessairement dans $\Gamma$.

Cela posé, la substitution A permute circulairement les six indices

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,$$

et l'on a

$$A = |\, i \quad i+1 \,| \quad (\bmod 7).$$

Il vient, par conséquent, pour X, Y et Z la forme

$$\begin{aligned} X &= \quad n_0 + \tau^{-1} n_1 + \tau^{-2} n_2 + \tau^{-3} n_3 + \tau^{-4} n_4 + \tau^{-5} n_5 + \tau^{-6} n_6, \\ Y &= b(n_0 + \tau^{-2} n_1 + \tau^{-4} n_2 + \tau^{-6} n_3 + \tau^{-1} n_4 + \tau^{-3} n_5 + \tau^{-5} n_6), \\ Z &= c(n_0 + \tau^{-4} n_1 + \tau^{-1} n_2 + \tau^{-5} n_3 + \tau^{-2} n_4 + \tau^{-6} n_5 + \tau^{-3} n_6). \end{aligned}$$

Pour que la substitution B soit possible, il faut que les coefficients des racines soient les mêmes à l'ordre près dans X, dans Y et dans Z; cela exige que l'on ait

$$b = \tau^{\beta}, \quad c = \tau^{\gamma},$$

$\beta$ et $\gamma$ désignant des entiers convenablement choisis entre zéro et 6.

Cela posé, formons la fonction U.

$$U = X + Y + Z.$$

Il faut, pour que C puisse multiplier U par $-1$ (7, théorème II), que U contienne un nombre pair de racines : donc les coefficients d'au moins une racine doivent se réduire quand on fait la somme $X + Y + Z$; soient $\tau^{\alpha}$, $\tau^{\beta}$,

$\tau^\gamma$ ces coefficients, on aurait

$$\tau^\alpha + \tau^\beta + \tau^\gamma = 0,$$

mais cela est impossible, car l'équation

$$\tau^6 + \tau^5 + \tau^4 + \tau^3 + \tau^2 + \tau + 1 = 0,$$

à laquelle satisfait $\tau$, est irréductible.

La substitution C ne peut donc pas exister dans $\Gamma$, lorsque $m = 7$, et $\Gamma$ se réduit au second des huit types de M. Jordan.

## II.

**33.** Nous allons maintenant passer à la discussion du quatrième type de l'énumération de M. Jordan. Le groupe $\Gamma$ résulte de la combinaison des substitutions

$$\begin{aligned} \lambda &= | \, XYZ \quad \lambda X \quad \lambda Y \quad \lambda Z \, |, \\ A &= | \, XYZ \quad \tau X \quad \tau^{-1} Y \quad \lambda Z \, |, \\ B &= | \, XYZ \quad Y \quad X \quad -Z \, | \end{aligned}$$

et

$$C = \begin{vmatrix} X & aX + (1-a)Y + 2a(1-a)Z \\ Y & (1-a)X + aY - 2a(1-a)Z \\ Z & X - Y + (1-2a)Z \end{vmatrix},$$

$$\tau^5 = 1, \qquad 1 + a(\tau + \tau^{-1} - 2) = 0.$$

Un pareil groupe a résisté à toutes mes tentatives; il est, en effet, aisé de voir qu'aucune de ses substitutions ne tombe sous le coup de l'un des trois lemmes du n° **26**. Je me bornerai à démontrer la proposition suivante :

Théorème. — *Le groupe* $\Gamma$ *dérivé des substitutions* A, B, C ($\lambda = 1$ forcément, en vertu du corollaire du lemme I du n° **26**) *ne peut fournir aucun type d'équation algébrique irréductible* H, *dont le degré* $m$ *soit un nombre premier inférieur à* 20.

La démonstration de ce théorème repose sur deux lemmes que je vais successivement démontrer.

*Lemme I.* — On a

$$n_{13} = n_{23} = n_1 = n_2 = 0$$

et, par suite,

$$n_0 + n_{12} + n_3 = m.$$

Pour démontrer ce lemme, je remarque que les substitutions A et B peuvent se mettre sous une forme symbolique (**26**, lemme II), qui est

$$A = (N_0)(N_1)(N_2)(N_3)(N_{12})(N_{13})(N_{23})$$

et

$$B = (N_0)(N_{12})(N_3)(N_1 N_2)(N_{13} N_{23}).$$

Cela posé, il est aisé de voir que C multiplie par 1 la fonction

$$U = X + Y;$$

C permute donc les racines qui figurent dans U entre elles, et les racines qui ne figurent pas dans U entre elles. Or les $n_3$ racines du système $N_3$ ne figurent pas dans U, tandis que les $n_1$ racines de $N_1$, les $n_2$ racines de $N_2$, les $n_{23}$ racines de $N_{23}$, les $n_{13}$ racines de $N_{13}$ figurent dans U : en effet, ces diverses racines ont un coefficient nul dans l'une des deux fonctions X et Y et ne peuvent disparaître dans la somme $X + Y = U$.

Ce que nous venons de dire de la substitution C, joint à ce que nous savons déjà des substitutions A et B, nous permet de voir qu'aucune substitution du groupe C ne peut faire prendre à une racine $n_i$ de $N_3$ la place de l'une quelconque des racines de $N_1$, ou $N_2$, ou $N_{13}$, ou $N_{23}$. Mais le groupe C est transitif : donc l'un des deux systèmes

(1) $$N_3,$$

(2) $$N_1 + N_2 + N_{13} + N_{23}$$

n'existe pas. Il est absurde de supposer que le système (1) est absent, car alors $n_3$ serait nul. Or, puisque la substitution A existe, en vertu du lemme I du n° **26**,

$$5 \text{ divise } n_0 \quad n_{12} \quad n_{13} \quad n_1,$$

$$5 \quad \text{»} \quad n_0 \quad n_{12} \quad n_{23} \quad n_2;$$

mais, si $n_3 = 0$,

$$n_0 + n_{12} + n_{13} + n_{23} + n_1 + n_2 = m,$$

et 5 diviserait $m$.

C'est donc le système (2) qui manque : donc

$$n_1 = n_2 = n_{13} = n_{23} = 0. \qquad \text{C. Q. F. D.}$$

*Remarque.* — Pour qu'une racine $n_i$ de $N_3$ puisse entrer dans le système $N_0$, il faut évidemment qu'il y ait au moins une racine de $N_0$ qui disparaisse dans la somme $U = X + Y$. Comme le groupe C est transitif, il existera dans $N_0$ au moins une racine affectée, dans X et dans Y, de coefficients égaux et de signe contraire.

Ce qui vient d'être dit du système $N_0$ s'applique évidemment de même au système $N_{12}$.

*Lemme II.* — On a toujours l'inégalité $6n_3 < m$.

En effet, puisque la substitution A existe, en vertu de la remarque du théorème I du n° 7, X et Y sont de la forme

$$\begin{aligned}X = {} & \alpha_0(n_0 + \tau^{-1}n_1 + \tau^{-2}n_2 + \tau^{-3}n_3 + \tau^{-4}n_4) \\ & + \alpha_1(n_5 + \tau^{-1}n_6 + \ldots + \tau^{-4}n_9) + \ldots + \alpha_i(n_{5i} + \ldots + \tau^{-4}n_{5i+4}) + \ldots \\ & + \alpha_{k-1}\left[n_{5(k-1)} + \ldots + \tau^{-4}n_{5(k-1)+4}\right].\end{aligned}$$

et de même, changeant $\tau$ en $\tau^{-1}$ et $\alpha$ en $\beta$,

$$\begin{aligned}Y = {} & \beta_0(n_0 + \ldots + \tau^4 n_4) + \ldots + \beta_i(n_{5i} + \ldots + \tau^4 n_{5i+4}) + \ldots \\ & + \beta_{k-1}\left[n_{5(k-1)} + \tau n_{5(k-1)+1} + \ldots + \tau^4 n_{5(k-1)+4}\right],\end{aligned}$$

où $5k = n_0 + n_{12} = m - n_3$.

En vertu de la remarque du lemme précédent, on doit avoir, en faisant la somme $U = X + Y$, des réductions entre les coefficients. Je dis qu'il ne saurait y avoir plus d'une réduction par groupe de cinq lettres, tel que

$$\alpha_i(\eta_{5i}+\tau^{-1}\eta_{5i+1}+\ldots+\tau^{-4}\eta_{5i+4})$$

et

$$\beta_i(\eta_{5i}+\tau\eta_{5i+1}+\ldots+\tau^{4}\eta_{5i+4}).$$

Supposons, en effet, qu'il y ait deux réductions, c'est-à-dire à la fois deux équations

$$\alpha_i\tau^{-a}+\beta_i\tau^{a}=0$$

et

$$\alpha_i\tau^{-b}+\beta_i\tau^{b}=0.$$

Il faut donc qu'on ait alors

$$\begin{vmatrix}\tau^{a} & \tau^{-a}\\ \tau^{b} & \tau^{-b}\end{vmatrix}=0,$$

c'est-à-dire

$$\tau^{2(a-b)}=1,$$
$$\tau^{a}=\pm\tau^{b};$$

cette dernière égalité est absurde, quel que soit le signe que l'on adopte. Donc il ne peut y avoir plus d'une réduction par cinq racines, c'est-à-dire plus de $k$ réductions en tout entre les $5k=n_0+n_{12}=m-n_3$ racines de $N_0$ et de $N_{12}$.

Cela posé, je suppose qu'on ait $n_3>k$ (on ne peut supposer $n_3=k$, car alors $5n_3=m-n_3$, $6n_3=m$, ce qui est absurde), c'est-à-dire $n_3=k+\rho$.

La substitution C ne pourra faire entrer, par conséquent, dans les systèmes $N_0$ et $N_{12}$, que $k$ au plus des $n_3=k+\rho$ racines du système $N_3$. Considérons maintenant la transformée X' de X par C, on a identiquement

$$X'=aX+(1-a)Y+2a(1-a)Z.$$

Dans le second membre de cette identité figurent les $n_3=k+\rho$ racines de $N_3$ ; dans le premier membre il ne figure au plus que $k$ des $n_3$ racines de $N_3$. L'identité est donc impossible tant que $\rho > 0$; on a, par conséquent, forcément l'inégalité

$$n_3 < k,$$

et, comme $k = \frac{m - n_3}{5}$,

$$6n_3 < m. \qquad \text{C. Q. F. D.}$$

Nous allons discuter degré par degré la possibilité de l'existence de l'équation algébrique H. Je remarque tout d'abord qu'aucune des trois substitutions A, B et C ne peut manquer dans le groupe, puisque chacune d'entre elles peut dériver de la combinaison des deux autres (*voir* le Mémoire de M. Jordan).

Ainsi donc, puisque B figure forcément dans le groupe, les coefficients des racines sont les mêmes à l'ordre près dans X et dans Y. En second lieu, puisque A multiplie X par $\tau$ et Y par $\tau^{-1}$ ($\tau^5 = 1$), et puisque B multiplie Z par $-1$, racine carrée de l'unité, on a (**26**, lemme I) :

les nombres $n_0$ et $n_{12}$ divisibles par 5,
» $n_0$ » $n_3$ » 2,

Donc $n_0$ est un multiple de 10, $n_3$ un nombre pair, $n_{12}$ un multiple impair de 5.

Cela posé, je vais discuter une à une les diverses hypothèses $m = 5$, 7, 11, 13, 17, 19 :

1° $m = 5$. Dans ce cas $n_3 = 2$ au moins, mais alors $n_0 = n_{12} = 0$. Le groupe $\Gamma$ est donc impossible.

2° $m = 7$, $n_3 = 2$ au moins. $n_0 = 0$, $n_{12} = 5$. Mais $6.2 > 7$; donc le groupe est impossible.

3° $m = 11$. $n_3 = 2$ au moins, et comme $6.2 > 11$, le groupe est encore impossible.

4° $m = 13$. La seule hypothèse possible pour $n_3$ est $n_3 = 2$, car si $n_3 \geqq 4$, $6n_3 > m$. Or, $13 - 2 = 11$, qui n'est pas un multiple de 5. Donc, le groupe $\Gamma$ ne peut exister.

5° $m = 17$. La seule hypothèse possible pour $n_3$ est $n_3 = 2$. Je ne puis d'ailleurs supposer $n_0 = 0$, car alors l'équation $Z = 0$ serait de la forme

$$\alpha_i n_i + \alpha_j n_j = 0,$$

c'est-à-dire

$$n_j = \theta n_i,$$

en désignant par $\theta$ une constante, ce qui est contre l'hypothèse. Il faut donc supposer que $n_0 = 10$ et $n_{12} = 5$. Considérons maintenant les cinq racines $n_0, n_1, n_2, n_3, n_4$ de $N_{12}$; X et Y sont de la forme

$$X = n_0 + \tau^{-1} n_1 + \tau^{-2} n_2 + \tau^{-3} n_3 + \tau^{-4} n_4 + \ldots$$

et

$$Y = \beta(n_0 + \tau n_1 + \tau^2 n_2 + \tau^3 n_3 + \tau^4 n_4) + \ldots.$$

Il faut, pour que la substitution B existe, que les coefficients de ces cinq lettres de $N_{12}$ soient les mêmes à l'ordre près dans X et dans Y; donc $\beta = \tau^{\gamma}$. Mais, avec cette hypothèse, aucune réduction entre les coefficients des cinq racines n'est possible dans la somme $U = X + Y$, car on aurait

$$\tau^{\lambda} + \tau^{\mu} = 0,$$

ce qui est absurde. Le groupe $\Gamma$ est donc impossible quand le degré $m = 17$.

6° $m = 19$. Comme $n_3 = 4$, au moins, et qu'alors $6n_3 > m$, le groupe $\Gamma$ est impossible.

On voit, par conséquent, que si le degré de l'équation irréductible H est l'un des nombres premiers inférieurs à 20,

$$5,\ 7,\ 11,\ 13,\ 17,\ 19,$$

le groupe $\Gamma$ dérivé des substitutions A, B, C ne saurait exister. Le théorème est donc démontré.

On voit que la discussion précédente ne laisse subsister, parmi les huit types de M. Jordan, que le premier et le second. Chacun de ces types fournit une classe spéciale d'équations H.

## III.

**34.** Théorème. — *Si le groupe* Γ *appartient au premier type de M. Jordan, c'est-à-dire s'il est formé exclusivement de substitutions de la forme*

$$S = | XYZ \quad \alpha X + \beta Y \quad \alpha' X + \beta' Y \quad \gamma Z |,$$

*le groupe* G *est formé exclusivement par les puissances d'une seule substitution circulaire entre les m racines.*

En effet, puisque toutes les substitutions de Γ multiplient Z par des constantes, on retombe sur le lemme III (**26**), et le théorème est démontré.

*Corollaire I.* — L'équation H est abélienne et résoluble algébriquement (**9**, théorèmes I et II).

*Corollaire II.* — L'équation différentielle linéaire Y admet un système fondamental d'intégrales formé de la fonction rationnelle $A_1$ de $x$ et de $m-1$ fonctions de la forme $\sqrt[m]{u_i}$, où $u_i$ désigne une fonction rationnelle de $x$ (**10** et **11**).

**35.** Je vais actuellement rechercher la nature du groupe G de l'équation H, lorsque Γ appartient au second type de M. Jordan, c'est-à-dire lorsque Γ résulte de la combinaison des substitutions

$$S = | XYZ \quad aX \quad bY \quad cZ |$$

et

$$T = | XYZ \quad a'Y \quad b'Z \quad c'X |.$$

*Lemme.* — X, Y et Z contiennent chacune toutes les $m$ racines.

En effet (**26**, lemmes I et II), les substitutions S et T peuvent se mettre sous la forme symbolique

$$S = (N_0)(N_{12})(N_{13})(N_{23})(N_1)(N_2)(N_3)$$

et

$$T = (N_0)(N_{12} N_{23} N_{13})(N_1 N_2 N_3).$$

On voit que, si l'on considère les trois groupes de systèmes de racines

(1) $N_0$,

(2) $N_{12}$ $N_{13}$ $N_{23}$,

(3) $N_1$ $N_2$ $N_3$,

aucune substitution de G ne peut faire passer une racine quelconque $n_i$ de (1), par exemple, ni dans (2), ni dans (3). Donc deux de ces groupes de systèmes manquent, puisque le groupe G est transitif.

Mais on a (**26**, lemme II)

$$n_{12} = n_{13} = n_{23} = \mu, \quad n_1 = n_2 = n_3 = \nu,$$
$$n_0 + 3\mu + 3\nu = m.$$

Donc, si l'on suppose que $N_0$ manque, ce qui revient à faire $n_0 = 0$, il viendrait

$$3(\mu + \nu) = m,$$

résultat absurde. Donc

$$\mu = 0, \quad \nu = 0, \quad n_0 = m. \qquad \text{C. Q. F. D.}$$

*Lemme II.* — Le faisceau des substitutions

$$S = |\, XYZ \quad aX \quad bY \quad cZ \,|$$

est formé par les puissances d'une seule substitution circulaire entre les $m$ racines.

En effet, puisque X, Y et Z contiennent chacune toutes les $m$ racines, les coefficients $a$, $b$, $c$ sont égaux à l'unité, ou sont des racines $m^{\text{ièmes}}$ de l'unité.

Supposons d'abord $a = b = c = 1$, alors le groupe Γ se réduit à la seule substitution T; soit $X_1$, $Y_1$, $Z_1$ la forme canonique de la substitution T, toutes les substitutions de G multiplieraient $X_1$, $Y_1$, $Z_1$ par des constantes et on retomberait sur le cas traité plus haut (**34**), ce qui est contre l'hypothèse.

Supposons l'un des coefficients, $a$ par exemple, différent de l'unité, alors $a = \theta^{-\alpha} (\theta^m = 1)$, la substitution S est circulaire entre les $m$ racines, et le lemme est démontré (**8**). D'ailleurs $b$ et $c$ ne peuvent être égaux à l'unité, car, si $b = 1$, par exemple, on aurait

$$Y = g(\eta_0 + \eta_1 + \ldots + \eta_{m-1}),$$

résultat inadmissible; par conséquent,

$$a = \theta^{-\alpha}, \quad b = \theta^{-\beta}, \quad c = \theta^{-\gamma} \quad (\theta^m = 1)$$

et

$$\begin{aligned} X &= \eta_0 + \theta^{\alpha} \eta_1 + \ldots + \theta^{(m-1)\alpha} \eta_{m-1}, \\ Y &= \eta_0 + \theta^{\beta} \eta_1 + \ldots + \theta^{(m-1)\beta} \eta_{m-1}, \\ Z &= \eta_0 + \theta^{\gamma} \eta_1 + \ldots + \theta^{(m-1)\gamma} \eta_{m-1}. \end{aligned}$$

*Remarque.* — On voit qu'il n'existe pas de coefficients égaux ni dans X, ni dans Y, ni dans Z.

Ces préliminaires vont nous permettre d'aborder l'étude de la substitution T.

**36.** *Lemme I.* — La substitution $T^3$ ne déplace aucune des $m$ racines.

En effet, puisque

$$T = | \, XYZ \quad a'Y \quad b'Z \quad c'X \, |,$$

on a

$$T^3 = | \, XYZ \quad a'b'c'X \quad a'b'c'Y \quad a'b'c'Z \, |;$$

mais $a'b'c' = 1$ (**26**, corollaire du lemme I) : donc $T^3$ ne déplace que les racines affectées de coefficients égaux; mais tous les coefficients de X, Y et Z sont inégaux, suivant la remarque ci-dessus : donc $T^3$ laisse chaque racine à sa place, et le lemme est démontré.

*Lemme II.* — Les coefficients $a'$, $b'$ et $c'$ sont des racines $m^{\text{ièmes}}$ de l'unité.

En effet, pour que la substitution T soit possible, il faut que les coefficients soient les mêmes à l'ordre près, dans X, Y et Z, et le lemme devient évident.

Théorème. — *La substitution* T *est égale au produit* $S^{-l^2\alpha'\mu'}t$ *de deux substitutions, dont l'une* S *est de la forme*

$$S = | i \quad i+1 | \pmod{m},$$

*c'est-à-dire circulaire entre les* $m$ *racines, et l'autre* $t$ *est de la forme*

$$t = | i \quad l^2 i | \pmod{m},$$

*et ne déplace pas l'indice* 0, *en permutant entre eux les* $m-1$ *autres indices. D'ailleurs, on a*

$$a = \theta^{-\alpha}, \quad l^3 \equiv 1 \pmod{m} \quad a' = \theta^{\alpha'}, \qquad \alpha\mu' \equiv 1 \pmod{m}.$$

En effet, on a (*voir* plus haut)

$$\begin{aligned} X &= \eta_0 + \theta^{\alpha}\eta_1 + \ldots + \theta^{(m-1)\alpha}\eta_{m-1}, \\ Y &= \eta_0 + \theta^{\beta}\eta_1 + \ldots + \theta^{(m-1)\beta}\eta_{m-1}, \\ Z &= \eta_0 + \theta^{\gamma}\eta_1 + \ldots + \theta^{(m-1)\gamma}\eta_{m-1}; \end{aligned}$$

puisque $a'$, $b'$, $c'$ sont des racines $m^{\text{ièmes}}$ de l'unité (lemme II), on peut poser

$$a' = \theta^{\alpha'}, \quad b' = \theta^{\beta'}, \quad c' = \theta^{\gamma'}.$$

Cela posé, désignons par $j$ l'indice que T met à la place de $i$,

$$T = | i \quad j | \pmod{m},$$

et cherchons à déterminer $j$ en fonction de $i$.

Il vient, comme on sait, pour X, Y, Z, la forme

$$\begin{aligned} X &= \ldots + \theta^{\alpha i}\eta_i + \ldots + \theta^{\alpha j}\eta_j + \ldots, \\ Y &= \ldots + \theta^{\beta i}\eta_i + \ldots + \theta^{\beta j}\eta_j + \ldots, \\ Z &= \ldots + \theta^{\gamma i}\eta_i + \ldots + \theta^{\gamma j}\eta_j + \ldots \end{aligned}$$

Faisant maintenant la substitution T, il vient

$$\begin{aligned} X' &= \ldots + \theta^{\alpha i}\eta_j + \ldots, \\ Y' &= \ldots + \theta^{\beta i}\eta_j + \ldots, \\ Z' &= \ldots + \theta^{\gamma i}\eta_j + \ldots \end{aligned}$$

D'autre part,

$$a'Y = \theta^{\alpha'}Y = \ldots + \theta^{\beta j+\alpha'}\eta_j + \ldots,$$
$$b'Z = \theta^{\beta'}Z = \ldots + \theta^{\gamma j+\beta'}\eta_j + \ldots,$$
$$c'X = \theta^{\gamma'}X = \ldots + \theta^{\alpha j+\gamma'}\eta_j + \ldots;$$

identifiant X' avec $a'$Y, Y' avec $b'$Z, Z' avec $c'$X, il vient

$$\theta^{\alpha i} = \theta^{\beta j+\alpha'}, \quad \theta^{\beta i} = \theta^{\gamma j+\beta'}, \quad \theta^{\gamma i} = \theta^{\alpha j+\gamma'};$$

d'où les relations linéaires suivantes entre $i$ et $j$ :

$$\left.\begin{aligned} \alpha i &\equiv \beta j + \alpha' \\ \beta i &\equiv \gamma j + \beta' \\ \gamma i &\equiv \alpha j + \gamma' \end{aligned}\right\} \pmod{m},$$

et, par suite, on peut mettre T sous l'une des trois formes

$$\left.\begin{aligned} T &= \left| i \quad \frac{\gamma i - \gamma'}{\alpha} \right| \\ T &= \left| i \quad \frac{\beta i - \beta'}{\gamma} \right| \\ T &= \left| i \quad \frac{\alpha i - \alpha'}{\beta} \right| \end{aligned}\right\} \pmod{m}.$$

Or ces trois formes doivent indiquer la même substitution ; donc il vient

$$\frac{\alpha}{\beta} \equiv \frac{\beta}{\gamma} \equiv \frac{\gamma}{\alpha} \pmod{m}, \qquad \frac{\alpha'}{\beta} \equiv \frac{\beta'}{\gamma} \equiv \frac{\gamma'}{\alpha} \pmod{m}.$$

Ce n'est pas tout : puisque T laisse chaque racine à sa place et que $T^3$ a l'une des trois formes suivantes :

$$T^3 = \left| i \quad \frac{\alpha^3}{\beta^3} i - \frac{\alpha'(\alpha^2 + \alpha\beta + \beta^2)}{\beta^3} \right|,$$
$$T^3 = \left| i \quad \frac{\beta^3}{\gamma^3} i - \frac{\beta'(\beta^2 + \beta\gamma + \gamma^2)}{\gamma^3} \right|,$$
$$T^3 = \left| i \quad \frac{\gamma^3}{\alpha^3} i - \frac{\gamma'(\gamma^2 + \alpha\gamma + \alpha^2)}{\alpha^3} \right|,$$

il faut évidemment que l'on ait

$$\frac{\alpha^3}{\beta^3} \equiv \frac{\beta^3}{\gamma^2} \equiv \frac{\gamma^3}{\alpha^3} \equiv 1 \pmod{m},$$

$$\alpha'(\alpha^2 + \alpha\beta + \beta^3) \equiv \beta'(\beta^2 + \beta\gamma + \gamma^2) \equiv \gamma'(\alpha^2 + \alpha\gamma + \gamma^2) \equiv 0.$$

Par conséquent, il faut avoir

$$\frac{\alpha}{\beta} \equiv \frac{\beta}{\gamma} \equiv \frac{\gamma}{\alpha} \equiv \frac{1}{l} \pmod{m},$$

en désignant par $l$ une racine primitive de la congruence binôme

$$l^3 \equiv 1 \pmod{m}.$$

Cette congruence n'admettra des racines réelles différentes de l'unité que lorsque $m - 1$ sera divisible par 3. Il faut donc que le degré $m$ de l'équation algébrique irréductible H soit un nombre premier de la forme $6k + 1$.

Supposons cette condition remplie, il viendra

$$\beta \equiv l\alpha, \quad \gamma \equiv l^2\alpha \pmod{m}$$

et, par suite,

$$\beta' \equiv l\alpha', \quad \gamma' = l^2\alpha' \pmod{m}.$$

Donc la substitution T pourra se représenter par la notation

$$T = \left| i \quad \frac{1}{l} i - \frac{\alpha'}{l\alpha} \right|,$$

c'est-à-dire

$$T = \left| i \quad l^2 i - l^2 \frac{\alpha'}{\alpha} \right|,$$

et, multipliant les deux termes de la fraction $\frac{\alpha'}{\alpha}$ par l'entier $\mu'$, tel que

$$\alpha\mu' \equiv 1 \pmod{m},$$

il vient

$$T = | \, i \quad l^2 i - l^2 \mu' \alpha' \, | = S^{-l^2\mu'\alpha'} t.$$

*Exemple.* — Prenons $m=7$, $\alpha=3$, $\alpha'=4$, $l=2$; il viendra $\beta=6$, $\gamma=5$, $\beta'=1$, $\gamma'=2$; d'ailleurs $\mu'=5$.

Avec ces hypothèses, il vient

$$T = |\, i \quad 4i - 4.5.4 \,|,$$
$$T = |\, i \quad 4i + 4 \,|,$$
$$T = (046)(1)(253).$$

Cela posé, on a

$$X = \eta_0 + \theta^3\eta_1 + \theta^6\eta_2 + \theta^2\eta_3 + \theta^5\eta_4 + \theta\ \eta_5 + \theta^4\eta_6,$$
$$Y = \eta_0 + \theta^6\eta_1 + \theta^5\eta_2 + \theta^4\eta_3 + \theta^3\eta_4 + \theta^2\eta_5 + \theta\ \eta_6,$$
$$Z = \eta_0 + \theta^5\eta_1 + \theta^3\eta_2 + \theta\ \eta_3 + \theta^6\eta_4 + \theta^4\eta_5 + \theta^2\eta_6,$$

et

$$X' = \eta_4 + \theta^3\eta_1 + \theta^6\eta_5 + \theta^2\eta_2 + \theta^5\eta_6 + \theta\ \eta_3 + \theta^4\eta_0,$$
$$Y' = \eta_4 + \theta^6\eta_1 + \theta^5\eta_5 + \theta^4\eta_2 + \theta^3\eta_6 + \theta^2\eta_3 + \theta\ \eta_0,$$
$$Z' = \eta_4 + \theta^5\eta_1 + \theta^3\eta_5 + \theta\ \eta_2 + \theta^6\eta_6 + \theta^4\eta_3 + \theta^2\eta_0,$$

c'est-à-dire

$$X' = \theta^4(\eta_0 + \theta^6\eta_1 + \theta^5\eta_2 + \ldots) = \theta^4 Y = a'Y,$$
$$Y' = \theta\ (\eta_0 + \theta^5\eta_1 + \theta^3\eta_2 + \ldots) = \ \theta Z\ = b'Z,$$
$$Z' = \theta^2(\eta_0 + \theta^3\eta_1 + \theta^6\eta_2 + \ldots) = \theta^2 X = c'X.$$

En résumé, on voit que le groupe G de l'équation algébrique irréductible H sera formé de la combinaison des deux substitutions

$$S = |\, i \quad i+1 \,|$$

et

$$t = |\, i \quad li \,| \quad l^3 \equiv 1 \ (\text{mod}\, m).$$

La substitution S permute circulairement toutes les $m$ racines; $t$ déplace toutes les racines sauf $\eta_0$.

**37.** Théorème. — *Toutes les racines de l'équation algébrique* H *peuvent s'exprimer rationnellement en fonction de deux quelconques d'entre elles et des coefficients de l'équation.*

Cette démonstration ne diffère en rien de la démonstration analogue de la deuxième Partie (**21**).

**38. Théorème.** — *L'équation algébrique* H *est résoluble algébriquement.*

En effet, considérons les $m-1$ quantités

$$
(1)\quad \left\{
\begin{aligned}
u_0 &= \left[\eta_0 + \theta^{\alpha_0}\eta_1 + \theta^{2\alpha_0}\eta_2 + \theta^{3\alpha_0}\eta_3 + \ldots + \theta^{(m-1)\alpha_0}\eta_{m-1}\right]^m,\\
v_0 &= \left[\eta_0 + \theta^{l\alpha_0}\eta_1 + \ldots\ldots\ldots\ldots + \theta^{(m-1)l\alpha_0}\eta_{m-1}\right]^m,\\
w_0 &= \left[\eta_0 + \theta^{l^2\alpha_0}\eta_1 + \ldots\ldots\ldots\ldots + \theta^{(m-1)l^2\alpha_0}\eta_{m-1}\right]^m,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
u_i &= \left[\eta_0 + \theta^{\alpha_i}\eta_1 + \ldots\ldots\ldots\ldots + \theta^{(m-1)\alpha_i}\eta_{m-1}\right]^m,\\
v_i &= \left[\eta_0 + \theta^{l\alpha_i}\eta_1 + \ldots\ldots\ldots\ldots + \theta^{(m-1)l\alpha_i}\eta_{m-1}\right]^m,\\
w_i &= \left[\eta_0 + \theta^{l^2\alpha_i}\eta_1 + \ldots\ldots\ldots\ldots + \theta^{(m-1)l^2\alpha_i}\eta_{m-1}\right]^m,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
u_k &= \left[\eta_0 + \theta^{\alpha_k}\eta_1 + \ldots\ldots\ldots\ldots + \theta^{(m-1)\alpha_k}\eta_{m-1}\right]^m,\\
v_k &= \left[\eta_0 + \theta^{l\alpha_k}\eta_1 + \ldots\ldots\ldots\ldots + \theta^{(m-)l\alpha_k}\eta_{m-1}\right]^m,\\
w_k &= \left[\eta_0 + \theta^{l^2\alpha_k}\eta_1 + \ldots\ldots\ldots\ldots + \theta^{(m-1)l^2\alpha_k}\eta_{m-1}\right]^m,
\end{aligned}
\right.
$$

où $l$ désigne une racine primitive de la congruence binôme $l^3 \equiv 1 \pmod{m}$. On a d'ailleurs posé $3(k+1) = m-1$. Il va sans dire que $m$ est un nombre premier de la forme $6\lambda + 1$, sans quoi $l$ serait imaginaire.

Parmi les $3(k+1)$ fonctions $u_i$, $v_i$, $w_i$, il y en a trois ($u_0$, $v_0$ et $w_0$ par exemple) qui sont précisément X, Y, Z et qui, par conséquent, sont nulles, mais les $3k$ autres fonctions ne sont pas nulles.

Considérons maintenant les deux substitutions S et $t$ du groupe G de l'équation H. La substitution S ne change pas la valeur des fonctions $u_i$, $v_i$, $w_i$; $t$ permute ces fonctions circulairement. Par conséquent, toute fonction symétrique de $u_i$, $v_i$, $w_i$ sera invariable par toutes les substitutions du groupe G, c'est-à-dire sera une fonction rationnelle des coefficients de H, c'est-à-dire encore une fonction rationnelle de la variable $x$: donc $u_i$, $v_i$, $w_i$ sont les trois racines de l'équation du troisième degré à coefficients rationnels

$$\Phi_i = \varphi_i^3 + L_{i1}\varphi_i^2 + L_{i2}\varphi_i + L_{i3} = 0.$$

D'ailleurs on vient de voir que les trois racines $u_i$, $v_i$, $w_i$ de $\Phi_i$ se permutent circulairement : donc l'équation $\Phi_i = 0$ est abélienne et deux quelconques de ses racines s'expriment rationnellement en fonction de la troisième.

Je n'aurai besoin d'ailleurs, pour avoir toutes les fonctions $u_i$, $v_i$, $w_i$, que de former et de résoudre une seule des $k$ équations $\Phi_i = 0$. En effet, les diverses fonctions $u_i$, $v_i$, $w_i$ sont invariables par les mêmes substitutions entre les $m$ racines de H : donc (JORDAN, *Traité des substitutions*, p. 50, et aussi **25**) toutes les fonctions $w_i$, $v_i$, $u_i$, s'exprimeront rationnellement en fonction d'une seule d'entre elles, $u_i$ par exemple, et de la variable $x$.

Ayant obtenu les $m - 1$ quantités $u_0, \ldots, w_k$, j'aurai un système de $m - 1$ équations linéaires entre les $m$ racines de H, et si au système (1) j'ajoute l'équation

$$\eta_0 + \eta_1 + \ldots + \eta_{m-1} = - A_1,$$

les $m$ équations linéaires obtenues de la sorte détermineront les $m$ racines de H sans ambiguïté aucune, car le déterminant D des inconnues (**9**) ne saurait être nul.

**39.** THÉORÈME. — *L'équation différentielle linéaire* $Y = 0$ *admet un système fondamental d'intégrales, dont un terme est une fonction rationnelle de* $x$ *et les* $m - 4$ *autres des fonctions de la forme* $\sqrt[m]{\omega_i}$, *les* $\omega_i$ *désignant une fonction rationnelle de la variable* $x$ *et d'une même racine d'une équation algébrique du troisième degré à coefficients rationnels en* $x$.

Ces $m - 4$ intégrales $\sqrt[m]{\omega_i}$ sont évidemment les $3k$ fonctions $\sqrt[m]{u_i}$, $\sqrt[m]{v_i}$, $\sqrt[m]{w_i}$, qui ne sont pas nulles. On démontrera, comme dans la première partie (**10**), que les $m - 3$ intégrales $A_1$ et $\sqrt[m]{\omega_i}$ forment un système fondamental de l'équation différentielle linéaire Y.

On peut donner au théorème précédent un énoncé légèrement différent, qui revient à l'énoncé donné, et qui est plus commode pour la vérification que je vais faire. On peut dire que les quantités $\omega_i$ sont trois à trois les racines d'une même équation algébrique du troisième degré à coefficients rationnels.

*Vérification.* — Il est aisé de vérifier que l'équation différentielle linéaire Y, qui admet le système fondamental d'intégrales définies plus haut, a tous ses coefficients rationnels.

La démonstration est toute pareille à celle de la vérification analogue de la deuxième Partie (**24**). En effet, soient

$$y_1, \quad y_2, \quad \ldots, \quad y_p$$

les $p = m - 3$ intégrales, où

$$y_1 = A_1, \quad y_\lambda^m = u_i, \quad y_\mu^m = v_i, \quad y_\nu^m = w_i,$$

$u_i$, $v_i$, $w_i$ désignant les trois racines de l'équation du troisième degré

$$\Phi_i = \varphi_i^3 + L_{i1}\varphi_i^2 + L_{i2}\varphi_i + L_{i3},$$

à coefficients rationnels en $x$.

L'équation différentielle Y peut s'écrire

$$Y = 0 = \begin{vmatrix} \dfrac{d^p y}{dx^p} & \cdots & \dfrac{d^p y_\lambda}{dx^p} & \dfrac{d^p y_\mu}{dx^p} & \dfrac{d^p y_\nu}{dx^p} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ y & \cdots & y_\lambda & y_\mu & y_\nu & \cdots \end{vmatrix}.$$

D'ailleurs (**11**) on a ($l =$ entier quelconque)

$$\frac{d^l y_\lambda}{dx^l} = y_\lambda \varphi_l(u_i), \quad \frac{d^l y_\mu}{dx^l} = y_\mu \varphi_l(v_i), \quad \frac{d^l y_\nu}{dx^l} = y_\nu \varphi_l(w_i),$$

en désignant par $\varphi_l$ une fonction rationnelle.

Je porte dans le déterminant ces valeurs des dérivées successives et je supprime les facteurs $y_\lambda$, $y_\mu$, $y_\nu$, ... communs à tous les éléments d'une colonne; j'obtiens un déterminant où chaque élément dans une colonne est une fonction rationnelle de $u_i$; l'élément correspondant de la colonne suivante est la même fonction rationnelle de $v_i$; de même, dans la colonne suivante, l'élément correspondant est encore la même fonction rationnelle de $w_i$.

Cela posé, intervertissons les deux colonnes du déterminant qui contiennent $u_i$ et $v_i$; le premier membre de l'équation différentielle $Y = 0$ change de signe; or intervertir les deux colonnes, cela revient à permuter $u_i$ et $v_i$; puisque le premier membre de l'équation différentielle Y change de signe, quand on transpose deux des trois quantités $u_i$, $v_i$, $w_i$, l'un quelconque des coefficients de l'équation différentielle sera de la forme

$$(u_i - v_i)(v_i - w_i)(w_i - u_i)\psi(u_i, v_i, w_i),$$

$\psi$ désignant une fonction rationnelle et symétrique de $u_i$, $v_i$ et $w_i$. Le raisonnement s'achèvera comme à la fin de la deuxième Partie (**24**).

La discussion complète du cas $n = 3$, qui constitue la troisième Partie du présent Travail, peut se résumer dans deux théorèmes, que je vais successivement énoncer.

**40.** Théorème I. — *Soit* Y *une équation différentielle linéaire à coefficients rationnels par rapport à la variable $x$, qui admet une intégrale rationnelle* $A_1$, *et dont l'ordre est un des trois nombres* 4, 10 *et* 16; *si* Y *possède un système fondamental dont tous les termes sont des racines d'une équation algébrique irréductible* H, *laquelle a tous ses coefficients rationnels et pour degré l'un des nombres premiers* 7, 13 *et* 19, Y *admettra un système fondamental formé de l'une des deux manières suivantes* :

1° *L'un des termes sera l'intégrale rationnelle* $A_1$, *et les* $p - 1$ *autres termes du système seront des intégrales de la forme* $\sqrt[m]{\omega}$, $\omega$ *désignant une fonction rationnelle de la variable $x$, et $m$ le degré de* H.

2° *Les* $p - 1$ *termes du système fondamental autres que* $A_1$ *seront de la forme* $\sqrt[m]{\omega}$, $\omega$ *désignant une fonction rationnelle de la variable et d'une même racine d'une équation algébrique, abélienne, du troisième degré, à coefficients rationnels.*

Si l'on se reporte au théorème de M. Jordan, cité dans l'Introduction, on voit que les diverses équations binômes que considère M. Jordan sont, dans le cas actuel, toutes du degré $m$ de l'équation H; l'équation auxiliaire $X = 0$ est une équation abélienne du troisième degré, ou une équation du premier degré.

Théorème II. — *Si l'ordre de l'équation différentielle est l'un des nombres* 2, 8, 14 *et le degré de l'équation algébrique l'un des nombres* 5, 11, 17, *toutes les autres conventions étant les mêmes qu'au théorème précédent, l'équation différentielle possédera un système fondamental formé de la façon suivante :*

*Les $p - 1$ intégrales autres que l'intégrale rationnelle $A_1$ seront des racines $m^{\text{ièmes}}$ de fonctions rationnelles de la variable.*

*L'équation auxiliaire du théorème de M. Jordan se réduit au premier degré.*

---

## QUATRIÈME PARTIE.

---

**41.** Si l'on voulait, par la méthode qui vient d'être exposée, chercher à intégrer une équation différentielle donnée, on serait conduit, comme dans la plupart des questions relatives à la théorie générale des équations algébriques, à des calculs très laborieux.

Je me bornerai donc, en ce qui concerne l'application de la méthode, à des indications tout à fait sommaires. En effet, l'intérêt des présentes recherches ne me semble point être tant dans l'essai d'un nouveau procédé d'intégration que dans la réduction, opérée dans un cas assez général, de fonctions algébriques implicites à des fonctions algébriques explicites très simples.

Considérons donc une équation différentielle linéaire et à coefficients rationnels

$$(Y) = \frac{d^p y}{dx^p} + B_1 \frac{d^{p-1} y}{dx^{p-1}} + B_2 \frac{d^{p-2} y}{dx^{p-2}} + \ldots + B_{p-1} \frac{dx}{dy} = B_p y = 0\,;$$

supposons que l'on se soit assuré qu'on est bien dans les conditions de notre problème, c'est-à-dire qu'un système fondamental de Y est exclusivement formé de racines d'une équation algébrique irréductible H, de degré $p+n(n=1, 2, 3$ et si $n=3, p+n<20)$, $p+n$ étant premier. De plus, l'équation Y a, par hypothèse, une intégrale rationnelle P.

Il sera, en général, assez malaisé de constater l'existence du système fondamental qui vient d'être défini. Voici quelques remarques qui pourront, de prime abord, faire écarter un grand nombre d'équations différentielles linéaires données.

L'équation Y, ayant toutes ses intégrales algébriques, les aura toutes régulières, c'est-à-dire que les infinis de ces intégrales seront d'ordre fini, et même d'ordre commensurable et réel. Si donc $a_1, a_2, a_3, \ldots, a_\rho$ désignent les divers points critiques des coefficients de Y, cette équation doit pouvoir, dans le domaine du point $a_i$, par exemple, se mettre sous la forme

$$0=\frac{dy^p}{dx^p}+\frac{\varphi_1(x)}{x-a_i}\frac{d^{p-1}y}{dx^{p-1}}+\ldots+\frac{\varphi_l(x)}{(x-a_i)^l}\frac{d^{p-l}y}{dx^{p-l}}+\ldots+\frac{\varphi_p(x)}{(x-a_i)^p}y,$$

avec la condition que les quantités

$$\varphi_1(a_i), \varphi_2(a_i), \ldots, \varphi_l(a_i), \ldots, \varphi_p(a_i)$$

soient toutes finies.

De plus, l'équation fondamentale déterminante relative au point

$$a_i(i=1, 2, 3, \ldots, \rho),$$

c'est-à-dire l'équation

$$k(k-1)\ldots(k-p+1)+\varphi_1(a_i)k(k-1)\ldots(k-p+2)+\ldots$$
$$+\varphi_l k(k-1)\ldots(k-p+l+1)+\ldots+\varphi_p(a_i)=0,$$

ne doit avoir que des racines réelles et commensurables. Enfin, dans l'expression générale d'une intégrale quelconque dans le domaine du point $a_i$

$$(x-a_i)^k\{\psi_0+\psi_1\log(x-a_i)+\psi_2[\log(x-a_i)]^2+\ldots\},$$

les coefficients des puissances de $\log(x-a_i)$ doivent être tous nuls.

Si toutes ces conditions sont remplies pour tous les points critiques $a_1$, $a_2, a_3, \ldots, a_\rho$ et pour le point $x^{-1}=0$, on pourra procéder à la recherche de l'intégrale rationnelle P.

La fonction P ne pouvant avoir d'autres infinis que les points critiques $a_1, a_2, \ldots, a_\rho$ et le point $x = \infty$, on posera

$$P = (x - a_1)^{\alpha_1}(x - a_2)^{\alpha_2} \ldots (x - a_\rho)^{\alpha_\rho} g(x),$$

les $\alpha$ désignant des entiers négatifs à déterminer et $g(x)$ un polynôme en $x$.

La limite inférieure des exposants $\alpha_1, \ldots, \alpha_\rho$ sera évidemment donnée par la plus petite racine négative de l'équation fondamentale déterminante relative à chaque point critique. On choisira dans les limites convenables un système de valeurs $\alpha_1, \ldots, \alpha_\rho$ et l'on en déduira immédiatement le degré maximum de $g(x)$. En effet, si dans $Y = 0$ je fais $x^{-1} = t$, formant l'équation différentielle linéaire T en $t$ et résolvant l'équation fondamentale déterminante relative au point $t = 0$, on aura pour limite supérieure du degré de $g(x)$ le nombre $k - (\alpha_1 + \alpha_2 + \ldots + \alpha_\rho)$, si l'on désigne par $-k$ la plus petite racine réelle et négative de l'équation fondamentale déterminante.

Posons donc $\mu + \alpha_1 + \ldots + \alpha_\rho = k$, il viendra

$$P = (x - a_1)^{\alpha_1}(x - a_2)^{\alpha_2} \ldots (x - a_\rho)^{\alpha_\rho}(c_0 x^\mu + c_1 x^{\mu-1} + \ldots + c_\mu),$$

les $c$ étant des constantes.

Je forme les dérivées successives $\frac{dP}{dx}, \frac{d^2P}{dx^2}, \ldots, \frac{d^pP}{dx^p}$, que je porte dans Y, je supprime le facteur

$$(x - a_1)^{\alpha_1 - p}(x - a_2)^{\alpha_2 - p} \ldots (x - a_\rho)^{\alpha_\rho - p},$$

commun à tous les termes, et j'obtiens un polynôme en $x$, qui doit être identiquement nul. Les coefficients de ce polynôme sont des fonctions linéaires des quantités $c$; on égale ces fonctions à zéro et l'on cherche par tâtonnements à déterminer les exposants $\alpha_1, \ldots, \alpha_\rho$ et les coefficients $c_0, \ldots, c_\mu$, de manière à satisfaire à ce système d'équations. Les essais pourront être multipliés, mais ils seront toujours en nombre fini, et, après avoir essayé tous les entiers négatifs compris entre les limites données pour les $\alpha$, on pourra décider si l'intégrale rationnelle P existe et former du même coup cette intégrale.

Supposons donc cette intégrale P formée, il nous reste, pour achever la solution du problème, à rechercher s'il existe des intégrales de la forme $\sqrt[m]{u}$ et à former ces intégrales si elles existent. D'après ce que nous avons vu, $u$ ne peut être qu'une quantité rationnelle, qu'une racine d'une équation du second degré à coefficients rationnels, qu'une racine d'une équation du troisième degré à coefficients rationnels.

1° $u$ est une quantité rationnelle en $x$. Dans ce cas, une intégrale quelconque $y$ de Y est de la forme suivante (en désignant encore par $a_1, \ldots, a_\rho$ les $\rho$ points critiques de Y) :

$$y = (x - a_1)^{\alpha_1} \ldots (x - a_\rho)^{\alpha_\rho}(c_0 x^\mu + c_1 x^{\mu-1} + \ldots + c_{\mu-1} x + c_\mu),$$

où le degré $\mu$ est déterminé comme plus haut pour l'intégrale rationnelle P. Les $c$ sont des constantes et les exposants $\alpha$ sont des nombres de la forme $\frac{k}{m}$ ($k$ entier quelconque). La recherche des quantités $\alpha$ et $c$ se fait par un procédé identique à celui qui vient d'être exposé.

2° $u$ satisfait à une équation du second degré. Dans ce cas, on pose, comme au n° **25**,

$$\mathrm{Y} = \begin{vmatrix} \frac{d^p y}{dx^p} & \cdots & \frac{d^p y_p}{dx^p} \\ \cdots & \cdots & \cdots \\ \frac{dy}{dx} & \cdots & \frac{dy_p}{dx} \\ y & \cdots & y_p \end{vmatrix} = 0,$$

$$y_i^m = u, \quad y_j^m = v,$$

$u$ et $v$ étant les deux racines de

$$\mathrm{W} = w^2 + \mathrm{L}w + \mathrm{M}.$$

On se donnera comme quantités à déterminer les $\frac{p-3}{2}$ fonctions rationnelles L et les $\frac{p-3}{2}$ fonctions rationnelles M. On exprimera rationnellement (**25**) tous les éléments du déterminant à l'aide des $p-3$ fonctions L et M et de leurs dérivées successives ; on développera le déterminant et l'on cherchera par tâtonnements à déterminer les $p - 3$ fonctions L et M de façon à identifier le déterminant développé avec l'équation différentielle linéaire proposée Y.

2° Si $u$ satisfait à une équation abélienne du troisième degré, on procédera comme pour la vérification faite au n° 40 et l'on opérera sur les équations

$$(\Phi) \qquad \varphi^3 + L_1\varphi_2^2 + L_2\varphi + L_3 = 0,$$

comme on vient d'opérer sur les équations W.

VU ET APPROUVÉ :

Paris, le 8 mai 1882.

*Le Doyen de la Faculté des Sciences,*

MILNE EDWARDS.

VU ET PERMIS D'IMPRIMER :

Paris, le 8 mai 1882.

*Le Vice-Recteur de l'Académie de Paris,*

GRÉARD.

# SECONDE THÈSE.

## PROPOSITIONS DONNÉES PAR LA FACULTÉ.

Des figures ellipsoïdales d'équilibre d'un fluide animé d'un mouvement de rotation uniforme et soumis seulement à l'attraction mutuelle de ses parties.

VU ET APPROUVÉ :

Paris, le 8 mai 1882.

*Le Doyen de la Faculté des Sciences,*

MILNE EDWARDS.

VU ET PERMIS D'IMPRIMER :

Paris, le 8 mai 1882.

*Le Vice-Recteur de l'Académie de Paris,*

GRÉARD.



7913 PARIS. — IMPRIMERIE DE GAUTHIER-VILLARS, QUAI DES AUGUSTINS, 55.