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

ÉMILE MATHIEU

Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables

Journal de mathématiques pures et appliquées 2^e série, tome 6 (1861), p. 241-323.
<http://www.numdam.org/item?id=JMPA_1861_2_6__241_0>

MÉMOIRE

SUR

L'ÉTUDE DES FONCTIONS DE PLUSIEURS QUANTITÉS,

SUR

LA MANIÈRE DE LES FORMER

ET SUR

LES SUBSTITUTIONS QUI LES LAISSENT INVARIABLES;

PAR M. ÉMILE MATHIEU.

Quand je me suis occupé de la question qui est traitée dans ce Mémoire, on ne connaissait alors de fonctions remarquables que la fonction deux fois transitive (ou résolvante) de Lagrange et une fonction trois fois transitive de 6 lettres ayant 6 valeurs donnée par M. Hermite; ajoutons à cela les deux fonctions deux fois transitives qui ont été rencontrées durant le cours de mes recherches par M. Kronecker, l'une de 7 lettres ayant 30 valeurs, l'autre de 11 lettres ayant 6048o valeurs, et l'on aura toutes les fonctions qui ont été données avant mes publications. Je rappellerai encore que, malgré le petit nombre de résultats acquis à cette doctrine, Cauchy avait publié pendant le cours de l'année 1845, dans les *Comptes rendus des séances de l'Académie*, une longue série de Mémoires entièrement relatifs à cette théorie, mais il ne fit la découverte d'aucune fonction.

A ces Mémoires de Cauchy j'ai toutefois emprunté une idée, et une seule : c'est celle de distinguer les fonctions en fonctions transitives et en fonctions intransitives. En effet, dans cette théorie, ce sont les fonctions transitives, et surtout celles qui le sont plusieurs fois, qui sont seules vraiment remarquables.

J'ai donné dans ce journal (année 1860) des notions générales sur les

fonctions transitives, et j'ai démontré l'existence de fonctions trois fois transitives de $p+1$ et de p^r+1 quantités, lorsque p est un nombre premier.

Dans le Mémoire actuel je supposerai connus ces résultats et je n'y reviendrai pas; mais j'exposerai la découverte de plusieurs autres familles de fonctions plusieurs fois transitives dont le nombre des quantités est une puissance d'un nombre premier ou un tel nombre augmenté d'une unité, et je donnerai des méthodes très-simples pour les former. Et l'on comprendra toute l'importance de mes théorèmes, sachant qu'ayant cherché directement toutes les fonctions qui n'ont pas plus de 12 quantités, j'ai pu reconnaître que les 22 fonctions de moins de 11 quantités qui sont plusieurs fois transitives sont renfermées dans les familles que j'ai découvertes. Ce résultat fait voir clairement que l'on n'a pas de fonctions de n quantités plusieurs fois transitives, lorsqu'on laisse le nombre n complétement indéterminé, et ensuite que mes théorèmes donnent toutes les fonctions plusieurs fois transitives dont le nombre des variables est un nombre premier, une puissance d'un nombre premier, ou de tels nombres augmentés d'une unité, lorsqu'on ne particularise pas davantage le nombre des variables. Enfin, j'ai pu m'apercevoir qu'en particularisant convenablement ces mêmes nombres, on trouverait de certaines fonctions qui seraient invariables d'abord par les substitutions qui ne changent pas mes fonctions plusieurs fois transitives, et ensuite par un nombre plus ou moins grand d'autres substitutions. Je ne saurais mieux faire que de donner ici pour exemple l'étonnante fonction 5 fois transitive de 12 quantités que l'on trouvera dans ce Mémoire; cette fonction est due : 1° à ce que 12 est un nombre premier 11, augmenté d'une unité; 2° à ce que le nombre 11 est le double d'un nombre premier, plus 1; 3° à ce que 11 est une puissance paire d'un nombre premier, plus 2.

Ainsi je dois dire que, bien que les familles de fonctions que j'ai trouvées donnent les fonctions plusieurs fois transitives qui se présentent le plus ordinairement, je ne doute pas que par suite du concours de circonstances plus ou moins extraordinaires, il y ait non-seulement d'autres fonctions, mais encore qu'il y ait un nombre très-considérable de classes de fonctions plusieurs fois transitives, en ne rangeant dans une même classe que des fonctions dues à des circonstances identiques.

Ce Mémoire contient aussi une méthode qui permet de découvrir des fonctions plusieurs fois transitives, et des théorèmes généraux sur les fonctions transitives d'un nombre premier de quantités.

CHAPITRE I.

DE LA FORMATION DES FONCTIONS. — MÉTHODE POUR DÉCOUVRIR ET FORMER DES FONCTIONS PLUSIEURS FOIS TRANSITIVES.

De la formation des fonctions.

Considérons une fonction de n quantités, que nous représenterons par la seule lettre x affectée de n indices différents; soit $\varphi(z)$ une fonction de z telle, qu'en remplaçant z par ces n indices les résultats soient ces mêmes indices pris seulement dans un ordre différent; $\varphi(z)$ pourra caractériser une substitution que nous désignerons par $(x_z\, x_{\varphi z})$, ou même souvent par $(z, \varphi z)$.

D'après cela, soit

$$(1) \qquad (x_z\, x_z),\ (x_z\, x_{\varphi_1 z}),\ (x_z\, x_{\varphi_2 z}),\ \ldots,\ (x_z\, x_{\varphi_{r-1} z})$$

un système de substitutions *conjuguées*, c'est-à-dire telles, qu'en faisant une quelconque de ces substitutions, puis cette même substitution ou une autre des substitutions (1), on fasse en définitive une des substitutions (1), on aura

$$\varphi_\alpha \varphi_\beta z = \varphi_\gamma z.$$

THÉORÈME. — *Il y a toujours une fonction invariable par un système de substitutions conjuguées donné, et invariable par ces seules substitutions.*

Proposons-nous de former une fonction invariable par le système de substitutions conjuguées (1), et supposons que les indices des n variables soient $0, 1, 2, \ldots, n-1$. Soit

$$\psi(x_0, x_1, x_2, \ldots, x_{n-1})$$

une fonction qui a $1.2.3\ldots n$ valeurs, et qui est par conséquent changée par toute substitution. Sur cette fonction faisons successivement toutes les substitutions (1), nous aurons les r fonctions différentes :

$$(2)\qquad \begin{cases} \psi(x_0, & x_1, & x_2, \ldots, & x_{n-1}), \\ \psi\left(x_{\varphi_1 0}, & x_{\varphi_1 1}, & x_{\varphi_1 2}, \ldots, & x_{\varphi_1(n-1)}\right), \\ \psi\left(x_{\varphi_2 0}, & x_{\varphi_2 1}, & x_{\varphi_2 2}, \ldots, & x_{\varphi_2(n-1)}\right), \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \psi\left(x_{\varphi_{r-1} 0}, & x_{\varphi_{r-1} 1}, & x_{\varphi_{r-1} 2}, \ldots, & x_{\varphi_{r-1}(n-1)}\right). \end{cases}$$

Prenons une fonction symétrique de ces r fonctions, et nous aurons une fonction Ψ qui est invariable par les substitutions (1).

En effet, faisons sur les fonctions (2) la substitution $(z, \varphi_e z)$, elles deviendront

$$(3)\qquad \begin{cases} \psi\left(x_{\varphi_e 0}, & x_{\varphi_e 1}, & x_{\varphi_e 2}, \ldots, & x_{\varphi_e(n-1)}\right), \\ \psi\left(x_{\varphi_e\varphi_1 0}, & x_{\varphi_e\varphi_1 1}, & x_{\varphi_e\varphi_1 2}, \ldots, & x_{\varphi_e\varphi_1(n-1)}\right), \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \psi\left(x_{\varphi_e\varphi_{r-1} 0}, & x_{\varphi_e\varphi_{r-1} 1}, & x_{\varphi_e\varphi_{r-1} 2}, \ldots, & x_{\varphi_e\varphi_{r-1}(n-1)}\right). \end{cases}$$

Or on a $\varphi_e\varphi_g z = \varphi_v z$; d'ailleurs les fonctions (2) étant différentes, les fonctions (3) le sont aussi ; donc les fonctions (3) sont les fonctions (2) prises dans un autre ordre; donc Ψ est invariable par les substitutions (1). Il est évident qu'en général la fonction Ψ est changée par toute autre substitution, et que le nombre de ses valeurs distinctes est $\frac{1.2.3\ldots n}{r}$.

Si, $\psi(x_0, x_1, x_2, \ldots, x_{n-1})$ étant une fonction quelconque, le nombre des valeurs de la fonction Ψ n'était pas $\frac{1.2\ldots n}{r}$, il serait, comme il est aisé de le démontrer, un diviseur de ce nombre.

Supposons actuellement que $\psi(x_0, x_1, x_2, \ldots, x_{n-1})$ soit invariable par un système de substitutions conjuguées

$$(4)\qquad (z, z),\ (z, \theta_1 z),\ (z, \theta_2 z), \ldots,\ (z, \theta_{u-1} z).$$

Écrivons les substitutions

$$(\mathrm{A})\quad\left\{\begin{array}{lllll}(z, z), & (z, \theta_1 z), & (z, \theta_2 z), \ldots, & (z, \theta_{u-1} z), \\ (z, \varphi_1 z), & (z, \varphi_1 \theta_1 z), & (z, \varphi_1 \theta_2 z), \ldots & (z, \varphi_1 \theta_{u-1} z), \\ (z, \varphi_2 z), & (z, \varphi_2 \theta_1 z), & (z, \varphi_2 \theta_2 z), \ldots, & (z, \varphi_2 \theta_{u-1} z), \\ \ldots & \ldots & \ldots & \ldots \\ (z, \varphi_{r-1} z), & (z, \varphi_{r-1} \theta_1 z), & (z, \varphi_{r-1} \theta_2 z), \ldots, & (z, \varphi_{r-1} \theta_{u-1} z).\end{array}\right.$$

Si la réunion de ces substitutions forme un système de substitutions conjuguées, je dis que la fonction Ψ, formée comme il a été dit ci-dessus, est invariable par ce système de substitutions.

La fonction Ψ est encore invariable par les substitutions (1); il reste donc à démontrer qu'elle n'est pas changée non plus par les substitutions (4). Sur la fonction Ψ faisons la substitution $(z, \theta_e z)$, les fonctions (2) qui la composent deviendront

$$(6)\quad\left\{\begin{array}{l}\psi\left(x_{\theta_e 0}, \quad x_{\theta_e 1}, \quad x_{\theta_e 2}, \ldots, \quad x_{\theta_e (n-1)}\right), \\ \psi\left(x_{\theta_e \varphi_1 0}, \ x_{\theta_e \varphi_1 1}, \ x_{\theta_e \varphi_1 2}, \ldots, \ x_{\theta_e \varphi_1 (n-1)}\right), \\ \psi\left(x_{\theta_e \varphi_2 0}, \ x_{\theta_e \varphi_2 1}, \ x_{\theta_e \varphi_2 2}, \ldots, \ x_{\theta_e \varphi_2 (n-1)}\right), \\ \ldots\ldots\ldots\ldots\ldots\ldots\end{array}\right.$$

La substitution $(z, \theta_e \varphi_s z)$ fait partie du système de substitutions conjuguées (A), puisqu'on l'obtient en faisant $(z, \varphi_s z)$, puis $(z, \theta_e z)$; donc on a

$$\theta_e \varphi_s z = \varphi_\alpha \theta_\beta z.$$

Ainsi les fonctions (6) peuvent s'écrire

$$(7)\quad\left\{\begin{array}{l}\psi\left(x_{\theta_e 0}, \qquad x_{\theta_e 1}, \qquad x_{\theta_e 2}, \ldots, \qquad x_{\theta_e (n-1)}\right), \\ \psi\left(x_{\varphi_{\alpha_1} \theta_{\beta_1} 0}, \quad x_{\varphi_{\alpha_1} \theta_{\beta_1} 1}, \quad x_{\varphi_{\alpha_1} \theta_{\beta_1} 2}, \ldots, \quad x_{\varphi_{\alpha_2} \theta_{\beta_1} (n-1)}\right), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \psi\left(x_{\varphi_{\alpha_{r-1}} \theta_{\beta_{r-1}} 0}, \ x_{\varphi_{\alpha_{r-1}} \theta_{\beta_{r-1}} 1}, \ldots, \ x_{\varphi_{\alpha_{r-1}} \theta_{\beta_{r-1}} (n-1)}\right).\end{array}\right.$$

La première des fonctions (2) est invariable par la substitution $(z, \theta_e z)$; donc elle est égale à la première des fonctions (7). On voit aussi, par la même raison, que la seconde des fonctions (7) est égale à

$$\psi\left(x_{\varphi_{\alpha_1} 0}, x_{\varphi_{\alpha_1} 1}, x_{\varphi_{\alpha_1} 2}, \ldots, x_{\varphi_{\alpha_1}(n-1)}\right),$$

que la troisième des fonctions (7) est égale à

$$\psi\left(x_{\varphi_{\alpha_2} 0}, x_{\varphi_{\alpha_2} 1}, x_{\varphi_{\alpha_2} 2}, \ldots, x_{\varphi_{\alpha_2}(n-1)}\right),$$

et ainsi des autres. Donc les fonctions (7) sont les fonctions (2) prises dans un autre ordre; car il est clair qu'elles sont différentes entre elles et la fonction Ψ est invariable par le système des substitutions (4); donc enfin Ψ est invariable par le système des substitutions conjuguées (A).

Le système des substitutions conjuguées (A) peut aussi s'écrire :

$$\begin{cases} (z, z), & (z, \varphi_1 z); & (z, \varphi_2 z), \ldots & (z, \varphi_{r-1} z), \\ (z, \theta_1 z), & (z, \theta_1 \varphi_1 z), & (z, \theta_1 \varphi_2 z), \ldots, & (z, \theta_1 \varphi_{r-1} z), \\ \ldots & \ldots & \ldots & \ldots \\ (z, \theta_{u-1} z), & (z, \theta_{u-1} \varphi_1 z), & (z, \theta_{u-1} \varphi_2 z), \ldots, & (z, \theta_{u-1} \varphi_{r-1} z); \end{cases}$$

car toutes ces substitutions sont différentes. Supposons en effet que l'on ait

$$\theta_s \varphi_r z = \theta_v \varphi_t z;$$

désignons par $\theta'_s z$ et $\varphi'_t z$ les fonctions inverses de $\theta_s z$ et de $\varphi_t z$, nous aurons

$$\varphi_r z = \theta'_s \theta_v \varphi_t z \quad \text{et} \quad \varphi_r \varphi'_t z = \theta'_s \theta_v z,$$

et l'une des substitutions (1) serait identique à une des substitutions (4), ce qui ne doit pas avoir lieu.

D'après cela, on peut encore former une fonction invariable par le système des substitutions conjuguées (A) de la manière suivante. On formera d'abord la fonction

$$\chi(x_0, x_1, x_2, \ldots, x_{n-1}),$$

qui soit invariable par le système de substitutions conjuguées (1); puis sur cette fonction on fera toutes les substitutions (4); enfin on prendra une fonction symétrique X des fonctions ainsi obtenues.

Il est évident que les fonctions (2) sont invariables respectivement par les systèmes suivants de substitutions conjuguées :

$$\begin{array}{llll}(z,z), & (z,\theta_1 z), & (z,\theta_2 z)\ldots, & (z,\theta_{u-1}z);\\ (\varphi_1 z,\varphi_1 z), & (\varphi_1 z,\varphi_1\theta_1 z) & (\varphi_1 z,\varphi_1\theta_2 z),\ldots, & (\varphi_1 z,\varphi_1\theta_{u-1}z);\\ \cdots & \cdots & \cdots & \cdots\\ (\varphi_{r-1}z,\varphi_{r-1}z), & (\varphi_{r-1}z,\varphi_{r-1}\theta_1 z), & (\varphi_{r-1}z;\varphi_{r-1}\theta_2 z),\ldots, & (\varphi_{r-1}z,\varphi_{r-1}\theta_{u-1}z),\end{array}$$

et si on désigne en général par $\varphi'_e z$ la fonction inverse de $\varphi_e z$, ces systèmes de substitutions peuvent s'écrire

$$\begin{array}{llll}(z,z), & (z,\theta_1 z), & (z,\theta_2 z),\ldots, & (z,\theta_{u-1}z),\\ (z,z), & (z,\varphi_1\theta_1\varphi'_1 z) & (z,\varphi_1\theta_2\varphi'_1 z),\ldots, & (z,\varphi_1\theta_{u-1}\varphi'_1 z),\\ \cdots & \cdots & \cdots & \cdots\\ (z,z), & (z,\varphi_{r-1}\theta_1\varphi'_{r-1}z), & (z,\varphi_{r-1}\theta_2\varphi'_{r-1}z),\ldots, & (z,\varphi_{r-1}\theta_{u-1}\varphi'_{r-1}z).\end{array}$$

Méthode pour former des fonctions plusieurs fois transitives.

Soit une fonction transitive F de n quantités $x_0, x_1, x_2,\ldots, x_{n-1}$, qui, considérée comme fonction des $n-1$ quantités $x_1, x_2,\ldots, x_{n-1}$, est invariable par le système des substitutions conjuguées

$$(1)\qquad (x_z x_z),\quad \left(x_z x_{\theta_1 z}\right),\quad \left(x_z x_{\theta_2 z}\right),\ldots,\quad \left(x_z x_{\theta_{r-1}z}\right),$$

et qui n'est pas changée non plus par les $n-1$ substitutions

$$(2)\qquad \left(x_z x_{\varphi_1 z}\right),\quad \left(x_z x_{\varphi_2 z}\right),\ldots,\quad \left(x_z x_{\varphi_{n-1}z}\right),$$

qui s'effectuent sur toutes les n variables, et qui jointes à $(x_z x_z)$ constituent un système de substitutions conjuguées qui caractérise une fonction transitive. Nous nous proposons de former, si elle existe, une fonction deux fois transitive Φ des $n+1$ variables $x_0, x_1, x_2,\ldots,$

x_{n-1}, x'_0, qui, considérée comme fonction des n premières variables, soit semblable à F.

Considérée comme fonction des $n-1$ variables $x_1, x_2, \ldots, x_{n-1}$, la fonction Φ n'est pas changée par les substitutions (1). Si donc on désigne dans un ordre convenable les variables $x_1, x_2, \ldots, x_{n-1}$ par $x'_1, x'_2, \ldots, x'_{n-1}$, par la raison que Φ n'est pas changée par les substitutions (1) et (2), Φ considérée comme fonction des variables $x'_0, x'_1, x'_2, \ldots, x'_{n-1}$ n'est pas changée par les substitutions

$$(3) \qquad (x'_z x'_z), \quad \left(x'_z x'_{\theta_1 z}\right), \quad \left(x'_z x'_{\theta_2 z}\right), \ldots, \quad \left(x'_z x'_{\theta_{r-1} z}\right),$$

$$(4) \qquad \left(x'_z x'_{\varphi_1 z}\right), \quad \left(x'_z x'_{\varphi_2 z}\right), \ldots, \qquad\qquad \left(x'_z x'_{\varphi_{n-1} z}\right).$$

Or les substitutions (1) et les substitutions (3) s'effectuent sur les mêmes variables $x_1, x_2, \ldots, x_{n-1}$; donc elles sont identiques. Quant aux substitutions (4), elles contiennent les n variables x'_0, x_1, $x_2, \ldots, x_{n-1}$, et si la valeur de chaque x' était connue, une quelconque des substitutions (4), jointe aux substitutions (1) et (2), suffirait pour que l'on pût former le système de toutes les substitutions conjuguées qui laissent Φ invariable. Or, les substitutions (3) étant identiques aux substitutions (1), une quelconque des substitutions (3) $\left(x'_z x'_{\theta_\beta z}\right)$ est identique à une certaine substitution (1) $\left(x_z x_{\theta_\alpha z}\right)$ qui lui est semblable. Supposons qu'en identifiant ces deux substitutions on trouve $x'_z = x_{\chi z}$; on aura les substitutions (4) en remplaçant les x' par leurs valeurs.

D'après cela, pour obtenir des substitutions qui laissent invariable la fonction Φ et qui contiennent x'_0, on choisira parmi les substitutions (1) celle qui renferme le moins de cycles, une substitution circulaire, s'il y en a une. Soit $\left(x_z x_{\theta_\alpha z}\right)$ cette substitution; on identifiera cette substitution de toutes les manières possibles avec chacune des substitutions (3) qui lui seront semblables. Restera ensuite à reconnaître celles de ces identifications qui sont bonnes, et pour cela on cherchera si, parmi les substitutions dérivées des substitutions (1), (2) et (4), il y en a qui s'effectuent sur les n variables $x_0, x_1, x_2, \ldots, x_{n-1}$, et qui ne coïncident pas avec les substitutions (1) et (2); dans quel cas l'identification est à rejeter. Mais si l'identification est reconnue bonne,

on pourra former le système de substitutions conjuguées qui laissent Φ invariable, et par suite former Φ.

Si dans les substitutions (1) toutes les variables entrent de la même manière, ce qui aura lieu en particulier si la fonction F est deux fois transitive, et par suite la fonction Φ trois fois transitive, on pourra poser $x'_1 = x_1$; ce qui facilitera beaucoup l'identification de la substitution $\left(x_z x_{\theta_\alpha z}\right)$ avec chacune des substitutions (3) qui lui sont semblables; ainsi, par exemple, si $\left(x_z x_{\theta_\alpha z}\right)$ est une substitution circulaire de $n-1$ variables, il n'y aura qu'une seule manière de l'identifier avec une substitution (3) qui lui est semblable, au lieu qu'il y en ait n.

Si la fonction Φ était quatre fois transitive, on pourrait non-seulement faire $x'_1 = x_1$, mais on pourrait poser $x'_e = x_f$. Si la fonction Φ était cinq fois transitive, on pourrait faire

$$x'_1 = x_1, \quad x'_e = x_f, \quad x'_g = x_h.$$

Nous allons maintenant nous proposer de former la fonction Φ.

La fonction

$$F = F(x_0, x_1, x_2, \ldots, x_{n-1})$$

est invariable par le système de substitutions conjuguées :

$$(A) \quad \left\{ \begin{array}{c} (x_z x_z),\ \left(x_z x_{\theta_1 z}\right), \ldots, \left(x_z x_{\theta_{r-1} z}\right),\ \left(x_z x_{\varphi_1 z}\right),\ \left(x_z x_{\varphi_1 \theta_1 z}\right), \ldots, \\ \left(x_z x_{\varphi_{n-1} \theta_{r-1} z}\right). \end{array} \right.$$

Remarquons ensuite que, puisque l'on a $x'_z = x_{\chi z}$, une quelconque des substitutions (4) $\left(x'_z x'_{\varphi_r z}\right)$ peut s'écrire $\left(x_{\chi z} x_{\chi\varphi_r z}\right)$ ou $\left(x_z x_{\chi\varphi_r \chi' z}\right)$, en désignant par $\chi' z$ la fonction inverse de χz, ou enfin $\left(x_z x_{\varphi'_r z}\right)$ en posant

$$\chi\varphi_r\chi' z = \varphi'_r z.$$

La fonction Φ est donc évidemment invariable par les rn^2 substitu-

tions suivantes :

$$(B)\quad \left\{\begin{array}{l} \left[\begin{array}{llll} (x_z x_z), & (x_z x_{\theta_1 z}), \ldots, & (x_z x_{\theta_{r-1} z}), \\ (x_z x_{\varphi_1 z}), & (x_z x_{\varphi_1 \theta_1 z}), \ldots, & (x_z x_{\varphi_{n-1}\theta_{r-1} z}), \end{array}\right] \\ \left[\begin{array}{llll} (x_z x_{\varphi'_1 z}), & (x_z x_{\varphi'_1 \theta_1 z}), \ldots, & (x_z x_{\varphi'_1 \theta_{r-1} z}), \\ (x_z x_{\varphi'_1 \varphi_1 z}), & (x_z x_{\varphi'_1 \varphi_1 \theta_1 z}), \ldots, & (x_z x_{\varphi'_1 \varphi_{n-1}\theta_{r-1} z}), \end{array}\right] \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \left[\begin{array}{llll} (x_z x_{\varphi'_{n-1} z}), & (x_z x_{\varphi'_{n-1}\theta_1 z}), \ldots, & (x_z x_{\varphi'_{n-1}\theta_{r-1} z}), \\ (x_z x_{\varphi'_{n-1}\varphi_1 z}), & (x_z x_{\varphi'_{n-1}\varphi_1\theta_1 z}), \ldots, & (x_z x_{\varphi'_{n-1}\varphi_{n-1}\theta_{r-1} z}). \end{array}\right] \end{array}\right.$$

Toutes ces substitutions sont différentes ; car si, en désignant les fonctions $\varphi\theta z$ par ψz, on avait

$$\varphi'_r \psi_s z = \varphi_\alpha \psi_\beta z,$$

on aurait, en désignant par φ'_{α_1} l'inverse de φ'_α,

$$\varphi'_{\alpha_1}\varphi'_r \psi_s z = \psi_\beta z,$$

et en changeant z en $\psi_{s_1} z$, inverse de $\psi_s z$,

$$\varphi'_{\alpha_1}\varphi'_r z = \psi_\beta \psi_{s_1} z,$$

égalité impossible puisque $\left(x_z x_{\varphi'_{\alpha_1}\varphi'_r z}\right)$ permute nécessairement x', et que $\left(x_z x_{\psi_\beta \psi_{s_1} z}\right)$ ne le permute pas.

Ainsi il reste rn substitutions à ajouter aux substitutions (B) pour compléter le système des $rn(n+1)$ substitutions conjuguées qui laissent Φ invariable. Désignons par $(x_z x_{\lambda z})$ une quelconque de ces rn substitutions, ces rn substitutions seront

$$(C)\qquad \left[\begin{array}{llll} (x_z x_{\lambda z}), & (x_z x_{\lambda\theta_1 z}), \ldots, & (x_z x_{\lambda\theta_{r-1} z}), \\ (x_z x_{\lambda\varphi_1 z}), & (x_z x_{\lambda\varphi_1\theta_1 z}), \ldots, & (x_z x_{\lambda\varphi_{n-1}\theta_{r-1} z}), \end{array}\right]$$

car elles sont distinctes entre elles et elles sont distinctes des substitutions (B), comme on le voit aisément.

Aucune des substitutions (B) ne change x'_0 en x_0; donc les rn substitutions (C) changent x'_0 en x_0. Supposons que $(x_z x_{\varphi_1 z})$ change x_0 en x_1; représentons l'inverse de $\varphi_1 z$ par $\varphi_{-1} z$; supposons aussi que l'on ait $x'_1 = x_1$ et alors $(x_z x_{\varphi'_1 z})$ change x'_0 en x_1 et $(x_z x_{\varphi_{-1} z})$ change x_1 en x_0; donc la substitution

$$\left(x_z x_{\varphi_{-1}\varphi'_1 z}\right)$$

change $x_0{}'$ en x_0, et peut être prise pour la substitution $(x_z x_{\lambda z})$.

Cela posé, formons les fonctions

$$(\mathrm{D})\qquad \left\{\begin{array}{l} \mathrm{F}\,(x_0,\quad x_1,\quad x_2,\ldots,\quad x_{(n-1)}),\\ \mathrm{F}\left(x_{\varphi'_1 0},\quad x_{\varphi'_1 1},\quad x_{\varphi'_1 2},\ldots,\quad x_{\varphi'_1 (n-1)}\right),\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ \mathrm{F}\left(x_{\varphi'_{n-1} 0},\ x_{\varphi'_{n-1} 1},\ x_{\varphi'_{n-1} 2},\ldots,\ x_{\varphi'_{n-1} (n-1)}\right),\\ \mathrm{F}\,(x_{\lambda 0},\quad x_{\lambda 1},\quad x_{\lambda 2},\ldots,\quad x_{\lambda (n-1)}), \end{array}\right.$$

que l'on obtient en faisant sur la première les substitutions (4), puis $(x_z x_{\lambda z})$. Prenons une fonction Θ symétrique des $n+1$ fonctions (D), et nous allons démontrer que la fonction Θ est invariable par les substitutions (B) et (C), et par conséquent n'est autre que la fonction Φ.

En effet, soit $(x_z x_{\psi z})$ une quelconque des substitutions (B) et (C), et démontrons que Θ n'est pas changée par cette substitution.

Considérons une quelconque des fonctions (D)

$$(\mathrm{K})\qquad \mathrm{F}\left(x_{\varphi'_\alpha 0},\ x_{\varphi'_\alpha 1},\ x_{\varphi'_\alpha 2},\ldots,\ x_{\varphi'_\alpha (n-1)}\right);$$

la substitution $(x_z x_{\psi z})$ changera cette fonction en la suivante

$$(\mathrm{E})\qquad \mathrm{F}\left(x_{\psi\varphi'_\alpha 0},\ x_{\psi\varphi'_\alpha 1},\ x_{\psi\varphi'_\alpha 2},\ldots,\ x_{\psi\varphi'_\alpha (n-1)}\right).$$

La substitution $\left(x_z x_{\psi\varphi'_\alpha z}\right)$ fait nécessairement partie des substitutions (B) et (C); on a donc

$$\psi\varphi'_\alpha z = \varphi'_a \varphi_c \theta_b z \quad \text{ou} \quad \psi\varphi'_\alpha z = \lambda\varphi_c\theta_b z.$$

Dans le premier de ces deux cas, la fonction (E) peut s'écrire

$$F\left(x_{\varphi'_a\varphi_c\theta_b 0},\ x_{\varphi'_a\varphi_c\theta_b 1},\ldots,\ x_{\varphi'_a\varphi_c\theta_b(n-1)}\right);$$

or la fonction $F(x_0, x_1, \ldots, x_{n-1})$ est invariable par la substitution $(x_z\, x_{\varphi_c\theta_b z})$; donc la fonction (E) peut encore s'écrire

$$F\left(x_{\varphi'_a 0},\ x_{\varphi'_a 1},\ldots,\ x_{\varphi'_a(n-1)}\right),$$

et c'est une des fonctions (D). Dans le deuxième cas, la fonction (E) peut s'écrire

$$F\left(x_{\lambda\varphi_c\theta_b 0},\ x_{\lambda\varphi_c\theta_b 1},\ldots,\ x_{\lambda\varphi_c\theta_b(n-1)}\right),$$

ou encore

$$F(x_{\lambda 0}, x_{\lambda 1}, \ldots, x_{\lambda(n-1)}).$$

Donc la substitution $(x_z\, x_{\psi z})$ change la fonction (K) en une autre fonction (D). Ce que nous venons de dire de la fonction (K) est applicable à une quelconque des fonctions (D), y compris la dernière.

D'ailleurs les fonctions (D) étant toutes différentes le sont encore après que l'on a fait sur elles la substitution $(x_z\, x_{\psi z})$; donc cette dernière ne fait que permuter les fonctions (D).

Application. — Considérons une fonction F de sept quantités $x_0, x_1, \ldots, x_6$ qui soit invariable par les seules substitutions $(x_z\, x_{a^2z+b})$; regardée comme fonction des six variables $x_1, x_2, \ldots, x_6$ seulement, cette fonction n'est invariable que par les substitutions $(x_z\, x_{a^2z})$, c'est-à-dire par

$$(e) \qquad (x_1 x_2 x_4)(x_3 x_6 x_5) \quad \text{et} \quad (x_1 x_4 x_2)(x_3 x_5 x_6),$$

et les substitutions de sept variables qui ne la changent pas, sont les puissances de $(x_z\, x_{z+1})$ ou de

$$(d) \qquad (x_0 x_1 x_2 x_3 x_4 x_5 x_6).$$

Le nombre des valeurs de cette fonction transitive est

$$\frac{1.2.3.4.5.6}{3} = 240.$$

Cela posé, cherchons s'il existe une fonction deux fois transitive des huit quantités $x_0, x_1, \ldots, x_6 x'_0$, et qui, considérée comme fonction des sept premières, soit semblable à F.

En désignant les quantités $x_1, x_2, \ldots, x_6$ dans un ordre convenable par $x'_1, x'_2, \ldots, x'_6$, cette fonction deux fois transitive sera invariable par les substitutions

$$(e') \qquad (x'_1\, x'_2\, x'_4)(x'_3\, x'_6\, x'_5) \quad \text{et} \quad (x'_1\, x'_4\, x'_2)(x'_3\, x'_6\, x'_5),$$

et par les puissances de la substitution

$$(d') \qquad (x'_0\, x'_1\, x'_2\, x'_3\, x'_4\, x'_5\, x'_6).$$

Les substitutions (e) sont identiques aux substitutions (e'). Faisons

$$x'_1 = x_1.$$

En identifiant la première des substitutions (e) avec la première des substitutions (e'), on aura les deux résultats suivants :

$$1^0 \quad x'_1 = x_1, \quad x'_2 = x_2, \quad x'_4 = x_4, \quad x'_3 = x_6, \quad x'_6 = x_5, \quad x'_5 = x_3;$$
$$2^0 \quad x'_1 = x_1, \quad x'_2 = x_2, \quad x'_4 = x_4, \quad x'_3 = x_5, \quad x'_6 = x_3, \quad x'_5 = x_6.$$

On pourra ensuite identifier la première des substitutions (e) avec la seconde des substitutions (e') d'une des trois manières suivantes :

$$3^0 \quad x'_1 = x_1, \quad x'_4 = x_2, \quad x'_2 = x_4, \quad x'_3 = x_3, \quad x'_5 = x_6, \quad x'_6 = x_5;$$
$$4^0 \quad x'_1 = x_1, \quad x'_4 = x_2, \quad x'_2 = x_4, \quad x'_3 = x_6, \quad x'_5 = x_5, \quad x'_6 = x_3;$$
$$5^0 \quad x'_1 = x_1, \quad x'_4 = x_2, \quad x'_2 = x_4, \quad x'_3 = x_5, \quad x'_5 = x_3, \quad x'_6 = x_6.$$

D'après cela, la substitution (d') sera l'une des cinq suivantes :

$$(1) \qquad (x'_0 x_1 x_2 x_6 x_4 x_3 x_5),$$
$$(2) \qquad (x'_0 x_1 x_2 x_5 x_4 x_6 x_3),$$
$$(3) \qquad (x'_0 x_1 x_4 x_3 x_2 x_6 x_5),$$
$$(4) \qquad (x'_0 x_1 x_4 x_6 x_2 x_5 x_3),$$
$$(5) \qquad (x'_0 x_1 x_4 x_5 x_2 x_3 x_6).$$

La substitution (3) ne peut convenir; en effet faisons la substitution (d), puis la substitution (3), opération représentée par le tableau

$$\begin{array}{cccccccc} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x'_0 \\ x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_0 & x'_0 \\ x_4 & x_6 & x_2 & x_3 & x'_0 & x_5 & x_0 & x_1 \end{array}$$

et nous aurons la substitution $(x_0\, x_4\, x'_0\, x_1\, x_6)$ qui ne peut laisser invariable la fonction cherchée, puisqu'elle n'est semblable ni aux substitutions (e), ni à la substitution (d).

La quatrième identification ne peut convenir non plus; en effet faisons la substitution (4), puis deux fois la substitution (d), ce qui est indiqué par le tableau

$$\begin{array}{cccccccc} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x'_0 \\ x_0 & x_4 & x_5 & x'_0 & x_6 & x_3 & x_2 & x_1 \\ x_2 & x_6 & x_0 & x'_0 & x_1 & x_5 & x_4 & x_3 \end{array}$$

et nous aurons la substitution $(x_0\, x_2)\ (x_1\, x_6\, x_4)\ (x_3\, x'_0)$, qui ne peut laisser invariable la fonction cherchée.

Reste donc à examiner s'il existe des fonctions transitives de huit quantités ayant 240 valeurs, invariables par l'un des trois systèmes de substitutions suivants

1^0 $(x_1\, x_2\, x_4)\,(x_3\, x_6\, x_5)$, $(x_0\, x_1\, x_2\, x_3\, x_4\, x_5\, x_6)$, $(x'_0\, x_1\, x_2\, x_6\, x_4\, x_3\, x_5)$;

2^0 $(x_1\, x_2\, x_4)\,(x_3\, x_6\, x_5)$, $(x_0\, x_1\, x_2\, x_3\, x_4\, x_5\, x_6)$, $(x'_0\, x_1\, x_2\, x_5\, x_4\, x_6\, x_3)$;

3^0 $(x_1\, x_2\, x_4)\,(x_3\, x_6\, x_5)$, $(x_0\, x_1\, x_2\, x_3\, x_4\, x_5\, x_6)$, $(x'_0\, x_1\, x_4\, x_5\, x_2\, x_3\, x_6)$.

Si sur le premier système, on fait la substitution $(x_1\, x_6)$, $(x_2\, x_5)$, $(x_3\, x_4)$, il devient

$$(x_6\, x_5\, x_3)\,(x_4\, x_1\, x_2),\ (x_0\, x_6\, x_5\, x_4\, x_3\, x_2\, x_1),\ (x'_0\, x_6\, x_5\, x_1\, x_3\, x_4\, x_2);$$

les deux dernières de ces substitutions sont des puissances des deux dernières du système 2^0; donc le système 2^0 ne diffère du système 1^0 que par la manière de désigner les variables.

Enfin si l'on cherche des substitutions dérivées du système 1° ou du système 3°, on ne trouve pas de substitutions de moins de huit quantités qui ne soient pas de la forme des substitutions (e) et (d). Il nous serait très-facile de former ici ces deux fonctions d'après ce qui a été dit ci-dessus; mais comme nous n'avons donné cette application que pour mieux faire comprendre notre méthode, nous ne nous arrêterons pas davantage sur ces deux fonctions [*].

Actuellement, conservant les notations employées ci-dessus, supposons qu'il y ait une fonction Φ au mois deux fois transitive de $n+1$ variables $x_0, x_1, x_2, \ldots, x_{n-1}, x'_0$ qui, considérée comme fonction des $n-1$ quantités $x_1, x_2, \ldots, x_{n-1}$ soit invariable par le système de substitutions conjuguées

$$(1) \qquad (x_z\, x_z),\ \left(x_z\, x_{\theta_1 z}\right),\ \left(x_z\, x_{\theta_2 z}\right), \ldots,\ \left(x_z\, x_{\theta_{r-1} z}\right),$$

et qui ne soit pas changée non plus par les $n-1$ substitutions

$$(2) \qquad \left(x_z\, x_{\varphi_1 z}\right),\ \left(x_z\, x_{\varphi_2 z}\right),\ \left(x_z\, x_{\varphi_3 z}\right), \ldots,\ \left(x_z\, x_{\varphi_{n-1} z}\right),$$

qui s'effectuent sur les n variables, et au moyen desquelles on peut amener une quelconque des variables à la place d'une autre. Enfin la fonction Φ est invariable par les substitutions

$$(3) \qquad (x'_z\, x'_z),\quad \left(x'_z\, x'_{\theta_1 z}\right),\ \left(x'_z\, x'_{\theta_2 z}\right), \ldots,\ \left(x'_z\, x'_{\theta_{r-1} z}\right),$$

$$(4) \qquad \left(x'_z\, x'_{\varphi_1 z}\right),\ \left(x'_z\, x'_{\varphi_2 z}\right),\ \ldots\ldots\ldots,\ \left(x'_z\, x'_{\varphi_{n-1} z}\right),$$

les substitutions (3) étant identiques aux substitutions (1) dans un certain ordre. Supposons que l'identification des substitutions (3) avec les substitutions (1) ait donné $x'_z = x_{\chi z}$, nous aurons

$$\chi\theta_s\chi' z = \theta_v z, \quad \chi\varphi_r\chi' z = \varphi'_r z, \quad \chi\varphi_r\theta_s\chi' z = \varphi'_r\theta_v z,$$

---

[*] Nous reverrons ces deux fonctions dans le chapitre III à propos de la fonction de huit quantités qui a trente valeurs.

et la fonction Φ est invariable par les $m(n+1)$ substitutions

$$(B)\quad \left\{\begin{array}{l}
\left[\begin{array}{llll}(x_z x_z), & (x_z x_{\theta_1 z}), & (x_z x_{\theta_2 z}), & (x_z x_{\theta_{r-1} z}),\\ & (x_z x_{\varphi_1 z}), & (x_z x_{\varphi_1\theta_1 z}),\ldots, & (x_z x_{\varphi_{n-1}\theta_{r-1} z}),\end{array}\right]\\
\left[\begin{array}{llll}(x_z x_{\varphi'_1 z}), & (x_z x_{\varphi'_1\theta_1 z}), & (x_z x_{\varphi'_1\theta_2 z}),\ldots, & (x_z x_{\varphi'_1\theta_{r-1} z}),\\ & (x_z x_{\varphi'_1\varphi_1 z}), & (x_z x_{\varphi'_1\varphi_1\theta_1 z}),\ldots, & (x_z x_{\varphi'_1\varphi_{n-1}\theta_{r-1} z}),\end{array}\right]\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\left[\begin{array}{llll}(x_z x_{\varphi'_{n-1} z}), & (x_z x_{\varphi'_{n-1}\theta_1 z}), & (x_z x_{\varphi'_{n-1}\theta_2 z}),\ldots, & (x_z x_{\varphi'_{n-1}\theta_{r-1} z}),\\ & (x_z x_{\varphi'_{n-1}\varphi_1 z}), & (x_z x_{\varphi'_{n-1}\varphi_1\theta_1 z}),\ldots, & (x_z x_{\varphi'_{n-1}\varphi_{n-1}\theta_{r-1} z}),\end{array}\right]
\end{array}\right.$$

$$(C)\quad \left[\begin{array}{llll}(x_z x_{\varphi_{-1}\varphi'_1 z}), & (x_z x_{\varphi_{-1}\varphi'_1\theta_1 z}), & (x_z x_{\varphi_{-1}\varphi'_1\theta_2 z}),\ldots, & (x_z x_{\varphi_{-1}\varphi'_1\theta_{r-1} z}),\\ & & (x_z x_{\varphi_{-1}\varphi'_1\varphi_1 z}),\ldots, & (x_z x_{\varphi_{-1}\varphi'_1\varphi'_{n-1}\theta_{r-1} z}),\end{array}\right]$$

$\varphi_{-1} z$ étant la fonction inverse de $\varphi_1 z$.

Supposons ensuite qu'il y ait une seconde identification des substitutions (3) avec les substitutions (1) qui donne une fonction semblable à la fonction Φ, en faisant abstraction de la manière de désigner les variables. Au lieu des substitutions (3) et (4), nous aurons les substitutions

$$(3')\qquad (x''_z x''_z),\quad (x''_z x''_{\theta_1 z}),\ (x''_z x''_{\theta_2 z}),\ldots,\ (x''_z x''_{\theta_{r-1} z}),$$

$$(4')\qquad (x''_z x''_{\varphi_1 z}),\ (x'_z x''_{\varphi_2 z}),\ \ldots\ldots\ldots,\ (x''_z x''_{\varphi_{n-1} z});$$

les substitutions (3') sont, dans un certain ordre, les substitutions (1), et on a $x''_z = x_{\mu z}$; posons

$$\mu\theta_s\mu' z = \theta_u z,$$

$$\mu\varphi_r\mu' z = \varphi''_r z,$$

par suite

$$\mu\varphi_r\theta_s\mu' z = \varphi''_r\theta_u z,$$

$\mu' z$ étant la fonction inverse de μz. Nous aurons donc le système de

substitutions conjuguées

$$
(\mathrm{B}')\left\{\begin{array}{l}
\left[\begin{array}{llll}
(x_z x_z), & (x_z x_{\theta_1 z}), & (x_z x_{\theta_2 z}),\ldots, & (x_z x_{\theta_{r-1} z}), \\
 & (x_z x_{\varphi_1 z}), & (x_z x_{\varphi_1 \theta_1 z}),\ldots, & (x_z x_{\varphi_{n-1} \theta_{r-1} z}),
\end{array}\right] \\
\left[\begin{array}{llll}
(x_z x_{\varphi''_1 z}), & (x_z x_{\varphi''_1 \theta_1 z}), & (x_z x_{\varphi''_1 \theta_2 z}),\ldots, & (x_z x_{\varphi''_1 \theta_{r-1} z}), \\
 & (x_z x_{\varphi''_1 \varphi_1 z}), & (x_z x_{\varphi''_1 \varphi_1 \theta_1 z}),\ldots, & (x_z x_{\varphi''_1 \varphi_{n-1} \theta_{r-1} z}),
\end{array}\right] \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\left[\begin{array}{llll}
(x_z x_{\varphi''_{n-1} z}), & (x_z x_{\varphi''_{n-1} \theta_1 z}), & (x_z x_{\varphi''_{n-1} \theta_2 z}),\ldots, & (x_z x_{\varphi''_{n-1} \theta_{r-1} z}), \\
 & & (x_z x_{\varphi''_{n-1} \varphi_1 z}),\ldots, & (x_z x_{\varphi''_{n-1} \varphi_{n-1} \theta_{r-1} z}),
\end{array}\right]
\end{array}\right.
$$

$$
(\mathrm{C}')\quad\left[\begin{array}{lll}
(x_z x_{\varphi_{-1} \varphi''_1 z}), & (x_z x_{\varphi_{-1} \varphi''_1 \theta_1 z}),\ldots, & (x_z x_{\varphi_{-1} \varphi''_1 \theta_{r-1} z}), \\
 & (x_z x_{\varphi_{-1} \varphi''_1 \varphi_1 z})\ldots, & (x_z x_{\varphi_{-1} \varphi''_1 \varphi_{n-1} \theta_{r-1} z}),
\end{array}\right]
$$

et, d'après l'hypothèse, le système (B′), (C′) ne diffère du système (B), (C) que par la manière de désigner les variables.

Supposons alors que l'on ait, $\tau' z$ étant l'inverse de τz,

$$\tau\theta_s \tau' z = \theta_e z, \quad \tau\varphi_\nu \tau' z = \varphi_f z, \quad \tau\varphi'_\alpha \tau' z = \varphi''_\beta z;$$

nous aurons

$$\tau\varphi'_\alpha \varphi_\nu \theta_s \tau' z = \varphi''_\beta \varphi_f \theta_e z;$$

on passera donc des substitutions (B) aux substitutions (B′) par la substitution $(x_z x_{\tau z})$; par suite la substitution $(x_z x_{\tau\varphi_{-1}\varphi'_1 \tau' z})$ est une des substitutions (C′) et on peut poser

$$\tau\varphi_{-1} \varphi'_1 \tau' z = \varphi_{-1} \varphi''_1 \theta_e z$$

et

$$\tau\varphi_{-1} \varphi'_1 \theta_\nu \tau' z = \varphi_{-1} \varphi''_1 \theta_\alpha z.$$

Voyons maintenant s'il pourra exister une fonction M des $n+2$ quantités $x_0, x_1, x_2, \ldots, x_{n-1}, x'_0, x''_0$, qui, considérée comme fonction des $n+1$ premières de ces quantités, soit semblable à Φ et soit invariable par les substitutions (B) et (C) et aussi par les substitutions (B′)

et (C'); de sorte que cette nouvelle fonction soit transitive une fois de plus que Φ.

Si la fonction M existe, les substitutions

$$(B'')\quad \left\{\begin{array}{l}
\left[\begin{array}{lll}(x_z\,x_z), & (x_z\,x_{\theta_1 z}), & (x_z\,x_{\theta_{r-1}z}),\\ (x_z\,x_{\varphi'_1 z}), & (x_z\,x_{\varphi'_1\theta_1 z}), & (x_z\,x_{\varphi'_{n-1}\theta_{r-1}z}),\end{array}\right]\\
\left[\begin{array}{lll}(x_z\,x_{\varphi''_1 z}), & (x_z\,x_{\varphi''_1\theta_1 z}),\dots, & (x_z\,x_{\varphi''_1\theta_{r-1}z}),\\ (x_z\,x_{\varphi''_1\varphi'_1 z}), & (x_z\,x_{\varphi''_1\varphi'_1\theta_1 z}),\dots, & (x_z\,x_{\varphi''_1\varphi'_{n-1}\theta_{r-1}z}),\end{array}\right]\\
\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
\left[\begin{array}{lll}(x_z\,x_{\varphi''_{n-1}z}), & (x_z\,x_{\varphi''_{n-1}\theta_1 z}),\dots, & (x_z\,x_{\varphi''_{n-1}\theta_{r-1}z}),\\ (x_z\,x_{\varphi''_{n-1}\varphi'_1 z}), & (x_z\,x_{\varphi''_{n-1}\varphi'_1\theta_1 z}),\dots, & (x_z\,x_{\varphi''_{n-1}\varphi'_{n-1}\theta_{r-1}z}),\end{array}\right]
\end{array}\right.$$

$$(C'')\quad \left[\begin{array}{lll}(x_z\,x_{\varphi'_{-1}\varphi''_1 z}), & (x_z\,x_{\varphi'_{-1}\varphi''_1\theta_1 z}),\dots, & (x_z\,x_{\varphi'_{-1}\varphi''_1\theta_{r-1}z}),\\ (x_z\,x_{\varphi'_{-1}\varphi''_1\varphi'_1 z}), & (x_z\,x_{\varphi'_{-1}\varphi''_1\varphi'_1\theta_1 z}),\dots, & (x_z\,x_{\varphi'_{-1}\varphi''_1\varphi'_{n-1}\theta_{r-1}z}),\end{array}\right]$$

sont conjuguées entre elles; ce sont les seules qui effectuées sur x_1, $x_2,\dots, x_{n-1}$, x'_0, x''_0, laissent invariable la fonction M, et l'on passe des substitutions (B), (C) aux substitutions (B''), (C'') par une même substitution.

Après cela, nous reconnaissons que cette fonction M est invariable par les $rn(n+1)(n+2)$ substitutions

(a) $\quad \left(x_z\,x_{\varphi''_u\varphi'_s\varphi_t\theta_v z}\right),$

(b) $\quad \left(x_z\,x_{\varphi''_u\varphi_{-1}\varphi'_1\varphi_t\theta_v z}\right),$

(c) $\quad \left(x_z\,x_{\varphi_{-1}\varphi''_1\varphi'_s\varphi_t\theta_v z}\right),$

(d) $\quad \left(x_z\,x_{\varphi_{-1}\varphi''_1\varphi_{-1}\varphi'_1\varphi_t\theta_v z}\right),$

(e) $\quad \left(x_z\,x_{\varphi'_{-1}\varphi''_1\varphi'_s\varphi_t\theta_v z}\right),$

(f) $\quad \left(x_z\,x_{\varphi'_{-1}\varphi''_1\varphi_{-1}\varphi'_1\varphi_t\theta_v z}\right).$

Les substitutions (e) et (f) sont évidemment différentes entre elles, et elles sont évidemment différentes des substitutions (a), (b), (c),

(d), puisque seules elles changent x''_0 en x'_0. Les substitutions (c) et (d) sont évidemment différentes entre elles, et elles sont différentes des substitutions (a) et (b), puisqu'elles changent x''_0 en x_0 et qu'aucune des substitutions (a) et (b) ne change x''_0 en x_0. Enfin les substitutions (a) et (b) sont évidemment différentes. Donc les substitutions (a), (b), (c), (d), (e), (f) étant toutes différentes, sont les seules qui laissent invariables la fonction M.

Actuellement je dis que, pour que la fonction M existe, il suffit que l'on puisse passer des substitutions (B), (C) aux substitutions (B″), (C″) par une même substitution.

Remarquons d'abord que les substitutions (B) et (C) peuvent être représentées par les deux expressions

$$\left(x_z\, x_{\varphi'_s \varphi_t \theta_\nu z}\right),\ \left(x_z\, x_{\varphi_{-1}\varphi'_1 \varphi_t \theta_\nu z}\right);$$

elles sont pareillement données par les deux expressions

$$\left(x_z\, x_{\varphi_t \varphi'_s \theta_\nu z}\right),\ \left(x_z\, x_{\varphi'_{-1}\varphi_1 \varphi'_t \theta_\nu z}\right).$$

Donc on a, quels que soient s et t,

$$(g)\quad \begin{cases} \varphi'_s \varphi_t \theta_\nu z = \varphi_{t_1} \varphi'_{s_1} \theta_{\nu_1} z & \varphi_t \varphi'_s \theta_\nu z = \varphi'_{s_1} \varphi_{t_1} \theta_{\nu_1} z \\ \quad \text{ou } = \varphi'_{-1} \varphi_1 \varphi'_{t_1} \theta_{\nu_1} z, & \quad \text{ou } = \varphi_{-1} \varphi'_1 \varphi_{t_1} \theta_{\nu_1} z. \end{cases}$$

Pareillement on a

$$(h)\quad \begin{cases} \varphi''_s \varphi_t \theta_\nu z = \varphi_{t_1} \varphi''_{s_1} \theta_{\nu_1} z & \varphi_t \varphi''_s \theta_\nu z = \varphi''_{s_1} \varphi_{t_1} \theta_{\nu_1} z \\ \quad \text{ou } = \varphi''_{-1} \varphi_1 \varphi''_t \theta_u z, & \quad \text{ou } = \varphi_{-1} \varphi''_1 \varphi_{t_1} \theta_{\nu_1} z. \end{cases}$$

Enfin puisqu'on admet que l'on passe des substitutions (B), (C) aux substitutions (B″), (C″) par une même substitution, celles-ci sont conjuguées entre elles, et on a encore

$$(i)\quad \begin{cases} \varphi''_s \varphi'_t \theta_\nu z = \varphi'_{t_1} \varphi''_{s_1} \theta_{\nu_1} z & \varphi'_t \varphi''_s \theta_\nu z = \varphi''_{s_1} \varphi_{t_1} \theta_{\nu_1} z \\ \quad \text{ou } = \varphi''_{-1} \varphi'_1 \varphi''_{i_1} \theta_{\nu_1} z, & \quad \text{ou } = \varphi'_{-1} \varphi''_1 \varphi'_{t_1} \theta_{\nu_1} z. \end{cases}$$

Observons enfin qu'on a les égalités

$$(k) \qquad \theta_\nu \varphi_s z = \varphi_t \theta_u z, \quad \theta_\nu \varphi'_s z = \varphi'_t \theta_u z, \quad \theta_\nu \varphi''_s z = \varphi''_t \theta_\nu z.$$

Soient $\varphi^{(\alpha)}$ et $\varphi^{(\beta)}$ deux des fonctions φ, φ', φ''; au lieu d'écrire les égalités (g), (h), (i), nous pouvons dire qu'une fonction composée seulement des $\varphi^{(\alpha)}$, $\varphi^{(\beta)}$ et des θ peut s'écrire

$$\varphi_u^{(\alpha)} \varphi_s^{(\beta)} \theta_\nu z \quad \text{ou} \quad \varphi_{-1}^{(\beta)} \varphi_1^{(\alpha)} \varphi_s^{(\beta)} \theta_\nu z.$$

Ceci établi, nous voyons aisément qu'en intervertissant l'ordre des fonctions φ, φ', φ'', on pourra toujours ramener une substitution dérivée des substitutions (B), (C), (B'), (C') à une des formes (a), (b), (c), (d), (e), (f). Donc la fonction M existe.

Remarque. — S'il arrive que la substitution $(x_z\, x_{\chi z})$ ne fait que permuter les substitutions $(x_z\, x_{\varphi'' z})$, on passe des substitutions (B), (C) aux substitutions (B''), (C'') par la substitution $(x_z\, x_{\chi\tau z})$, et par conséquent la fonction M existe. En effet, on a dans ce cas

$$\chi\tau\varphi'_\alpha \varphi_\beta \theta_\gamma \tau' \chi' z = \chi\tau\varphi'_\alpha \tau' \chi' \chi\tau\varphi_\beta \theta_\gamma \tau' \chi' z = \chi\varphi''_\alpha \chi' \chi\varphi_\nu \theta_\epsilon \chi' z.$$

Or on a par hypothèse

$$\chi\varphi''_\alpha \chi' z = \varphi''_{\overline{\beta}_1} z,$$

et on a d'ailleurs

$$\chi\varphi_\nu \theta_\epsilon \chi' z = \varphi'_s \theta_t z;$$

donc

$$\chi\tau\varphi'_\alpha \varphi_\beta \theta_\gamma \tau' \chi' z = \varphi''_{\beta_1} \varphi'_s \theta_t z.$$

Application. — Nous avons dit précédemment qu'il y a une fonction deux fois transitive de huit variables qui a 240 valeurs et qui est invariable par les substitutions

$$(m)\ (x_1 x_2 x_4)\,(x_3 x_6 x_5),\ (x_0 x_1 x_2 x_3 x_4 x_5 x_6),\ (x'_0 x_1 x_2 x_6 x_4 x_3 x_5),$$

ou par les substitutions

$$(m')\ (x_1 x_2 x_4)\,(x_3 x_6 x_5),\ (x_0 x_1 x_2 x_3 x_4 x_5 x_6)\,(x''_0 x_1 x_2 x_5 x_4 x_6 x_3),$$

et que l'on passe des substitutions (m) aux substitutions (m') par la substitution

$$(x_s x_{\tau s}) = (x_1 x_6)(x_2 x_5)(x_3 x_4).$$

La substitution $(x_s x_{\chi s})$ est ici $(x_3 x_6 x_5)$, et l'on passe des substitutions (m) aux substitutions

$$(m'') \quad (x_6 x_5 x_2)(x_1 x_2 x_4), (x'_0 x_6 x_5 x_1 x_3 x_4 x_2), (x''_0 x_6 x_5 x_2 x_3 x_1 x_4)$$

par la substitution

$$(x_s x_{\tau\chi s}) = (x_1 x_6 x_2 x_5 x_4 x_3).$$

Donc il existe une fonction trois fois transitive de 9 quantités qui a 240 valeurs, invariable par les substitutions (m) et (m') (*).

Nous donnerons à la fin du chapitre suivant une application bien plus remarquable de cette théorie.

CHAPITRE II.

FONCTIONS DE p^ν QUANTITÉS INVARIABLES PAR DES SUBSTITUTIONS $(x_s x_{as p^\alpha + b})$ ET FONCTIONS DE $p^\nu + 1$ QUANTITÉS INVARIABLES PAR DES SUBSTITUTIONS $\begin{pmatrix} x_s & x_{\frac{A_{sp^\alpha}+B}{C_{sp^\alpha}+D}} \end{pmatrix}$.

Soit p un nombre premier; en mettant comme indices à la lettre x les p^ν quantités qui satisfont à la congruence $z^{p^\nu} \equiv z \pmod{p}$, nous avous étendu dans le *Journal* de M. Liouville (1860, p. 38), aux

---

(*) Cette fonction est donnée par ce théorème qui se trouve dans le Chapitre II : Si p est un nombre premier, il y a une fonction trois fois transitive de $p^\nu + 1$ variables qui a $\frac{1.2.3\ldots(p^\nu - 2)}{\nu}$ valeurs.

fonctions de p^ν et de $p^\nu + 1$ quantités des théorèmes que nous avions d'abord démontrés pour les fonctions de p et de $p + 1$ variables; nous allons maintenant donner ici pour les premières fonctions des théorèmes qui leur sont propres, en adoptant les mêmes indices.

Soit τ un diviseur de ν, et u un diviseur de $p^\nu - 1$, il y a une fonction transitive de p^ν quantités invariable pour toutes les substitutions

$$(z, \quad a^u z^{p^{\tau\alpha}} + b) \tag{10}$$

et qui a $\frac{1.2...(p^\nu - 2)\times\tau}{\nu} \times u$ valeurs.

Soit ψ une fonction invariable par la substitution (z, z^{p^τ}), on formera une fonction invariable par toutes les substitutions (10) au moyen de ψ, comme on forme une fonction invariable par les substitutions $(z, a^u z + b)$ au moyen d'une fonction qui est changée par toute substitution.

Si nous supposons $u = 1$, nous aurons une fonction deux fois transitive de p^ν quantités invariable par les substitutions

$$(z, az^{p^{\tau\alpha}} + b) \tag{11}$$

et qui a $\frac{1.2...(p^\nu - 2)\times\tau}{\nu}$ valeurs.

Soit τ un diviseur de ν, il existe une fonction trois fois transitive de $p^\nu + 1$ quantités qui a $\frac{1.2...(p^\nu - 2)\times\tau}{\nu}$ valeurs, et qui est invariable par toutes les substitutions

$$\left(z, \frac{Az^{p^{\tau\alpha}} + B}{Cz^{p^{\tau\alpha}} + D}\right). \tag{12}$$

Soit F une fonction deux fois transitive invariable par toutes les substitutions (11); on construira une fonction invariable par toutes les substitutions (12) au moyen de F, de la même manière que l'on forme une fonction invariable par toutes les substitutions $\left(z, \frac{Az+B}{Cz+D}\right)$ au moyen d'une fonction invariable par les substitutions $(z, az + b)$.

Soit τ un diviseur de ν, et p différent de 2, il existe une fonction A deux fois transitive de $p^\nu + 1$ variables qui a $\frac{1.2\ldots(p^\nu-2)}{\nu} \times 2\tau$ valeurs, et qui est invariable par les substitutions (12) pour lesquelles AD — BC est un résidu quadratique.

Nous formerons la fonction A au moyen de la fonction λ invariable par les substitutions $(z, a^2 z^{p^{\tau\alpha}} + b)$ de la même manière que l'on peut former la fonction invariable par les substitutions $\left(z, \frac{Az+B}{Cz+D}\right)$ pour lesquelles AD — BC est résidu quadratique au moyen de la fonction invariable par les substitutions $(z, a^2 z + b)$. Ainsi faisons sur λ toutes les substitutions $\left(\frac{1}{z}, \frac{1}{z+n}\right)$, nous obtiendrons ainsi les $p^\nu - 1$ fonctions $\lambda_1, \lambda_2, \ldots, \lambda_{p^\nu-1}$; faisons encore sur λ la substitution $\left(z, \frac{(-1)^{\frac{p^\nu-1}{2}}}{z}\right)$ ce qui donnera λ'; enfin formons une fonction symétrique de $\lambda, \lambda_1, \ldots, \lambda_{p^\nu-1}, \lambda'$, et nous aurons A.

La substitution (z, z^{p^τ}) peut changer ou laisser invariable la fonction qui a deux valeurs; dans le premier cas, en multipliant A par la fonction qui a deux valeurs, on obtient une fonction qui a un nombre de valeurs double; dans le second cas, on obtient une autre fonction semblable à A.

Supposons ν pair et p différent de 2, et soit 2τ un diviseur de ν; il existe une fonction deux fois transitive de p^ν quantités qui a $\frac{1.2\ldots(p^\nu-2)}{\nu} \times 2\tau$ valeurs, et qui est invariable par toutes les substitutions renfermées dans les deux expressions

$$(13) \qquad \left(z, \omega^{2r} z^{p^{2\alpha\tau}} + m\right), \quad \left(z, \omega^{2s+1} z^{p^{(2\alpha+1)\tau}} + n\right),$$

ω étant une racine primitive de $z^{p^\nu-1} \equiv 1 \pmod{p}$.

Pour construire cette fonction deux fois transitive, nous formerons une fonction φ invariable par les substitutions

$$\left(z, \omega^{2r} z^{p^{2\alpha\tau}}\right), \quad \left(z, \omega^{2s+1} z^{p^{(2\alpha+1)\tau}}\right);$$

nous ferons sur cette fonction toutes les substitutions $(z, z+m)$, nous obtiendrons les fonctions $\varphi, \varphi_1, \varphi_2, \ldots, \varphi_{p^\nu-1}$ et nous prendrons une fonction symétrique Ψ de ces p^ν fonctions.

On voit encore que, u étant un diviseur impair de $p^\nu - 1$, il y a une fonction transitive de p^ν quantités qui a $\frac{1.2\ldots(p^\nu-2)}{\nu} \times 2\tau \times u$ valeurs, et qui est invariable par les substitutions (13), dans lesquelles ω est remplacé par ω^u.

Supposons ν pair, p différent de 2, et 2τ un diviseur de ν ; il existe une fonction trois fois transitive de $p^\nu + 1$ quantités, qui a $\frac{1.2\ldots(p^\nu-2)}{\nu} \times 2\tau$ valeurs, et qui est invariable par les substitutions

$$(14) \qquad \left(z, \frac{Az^{p^{2\alpha\tau}}+B}{Cz^{p^{2\alpha\tau}}+D}\right), \quad \left(z, \frac{A_1 z^{p^{(2\alpha+1)\tau}}+B_1}{C_1 z^{p^{(2\alpha+1)\tau}}+D_1}\right),$$

$AD - BC$ étant résidu quadratique, et $A_1 D_1 - B_1 C_1$ non résidu.

On construit cette fonction trois fois transitive au moyen de la fonction Ψ invariable par les substitutions (13) de la même manière que l'on forme la fonction invariable par les substitutions $\left(z, \frac{Az+B}{Cz+D}\right)$, pour lesquelles $AB - BC$ est résidu quadratique au moyen de la fonction invariable par les substitutions $(z, a^2 z + b)$.

Remarque. — Ces différents théorèmes donnent des fonctions qui ont le même nombre de valeurs, sans être semblables. Ainsi dans le cas où $\frac{\nu}{\tau}$ est pair, il y a deux fonctions trois fois transitives et une fonction deux fois transitive de $p^\nu + 1$ quantités qui ont $\frac{1.2\ldots(p^\nu-2)\times 2\tau}{\nu}$ valeurs. L'une de ces fonctions trois fois transitive est celle qui n'est pas changée par les substitutions (14); l'autre fonction trois fois transitive est celle qui est invariable par toutes les substitutions

$$\left(z, \frac{Az^{p^{2\alpha\tau}}+B}{Cz^{p^{2\alpha\tau}}+D}\right);$$

enfin la fonction deux fois transitive est celle qui est invariable par toutes les substitutions

$$\left(z, \frac{Az^{p^{\alpha\tau}}+B}{Cz^{p^{\alpha\tau}}+D}\right),$$

pour lesquelles AD — BC est résidu quadratique.

Étude des substitutions $\left(z, \frac{Az^{p^{\alpha}}+B}{Cz^{p^{\alpha}}+D}\right)$.

Parmi ces substitutions considérons d'abord la substitution (z, z^p) et ses puissances $\left(z, z^{p^{\alpha}}\right)$.

Les racines de la congruence $z^p \equiv z \pmod{p}$ sont $0, 1, 2, \ldots, p-1$; donc la substitution (z, z^p) laisse immobiles les variables $x_0, x_1, x_2, \ldots, x_{p-1}$ et permute les $p^\nu - p$ autres variables.

Si ν est un nombre premier, la substitution (z, z^p) est une substitution régulière composée de $\frac{p^\nu - p}{\nu}$ cycles de ν quantités. Car $x_k, x_{kp}, x_{kp^2}, \ldots, x_{kp^{\nu-1}}$ sont des variables différentes. La substitution $\left(z, z^{p^r}\right)$ est semblable à (z, z^p).

Si ν est un nombre composé, les racines de $z^{p^{\alpha}} \equiv z$ qui appartiennent à $z^{p^{\nu}} \equiv z$ sont celles de la congruence $z^{p^{\tau}} \equiv z$, τ étant le plus grand commun diviseur de ν et de α; par conséquent la substitution $\left(z, z^{p^{\alpha}}\right)$ s'effectue alors seulement sur $p^\nu - p^\tau$ variables.

Considérons en second lieu les substitutions

$$(a) \qquad \left(z, az^{p^{\alpha}}\right)$$

et soit τ le plus grand commun diviseur de α et de ν. D'après ce qui a été dit au commencement du chapitre I, il résulte du mode même de formation des fonctions qni sont invariables par les substitutions (a), que les substitutions qui ont moins de $p^\nu - 1$ variables sont de la

forme $\left(kz,\ kz^{p^\alpha}\right)$ ou de la forme

$$(b) \qquad \left(z,\ l^{p^\alpha-1}z^{p^\alpha}\right);$$

ce sont donc les substitutions (a) pour lesquelles a est résidu de puissance $(p^\tau - 1)^{ième}$; par conséquent aussi les substitutions (a) pour lesquelles a n'est pas résidu de puissance $(p^\tau - 1)^{ième}$ s'effectuent sur $p^\nu - 1$ quantités.

Occupons-nous ensuite des substitutions

$$(c) \qquad \left(z,\ az^{p^\alpha} + b\right).$$

Reportons-nous à la manière de former une fonction invariable par les substitutions (c) au moyen d'une fonction invariable par les substitutions (a), et nous reconnaissons que toutes les substitutions (c) qui ont moins de p^ν variables sont de la forme

$$(d) \qquad \left(z + m,\ az^{p^\alpha} + m\right),$$

et sont semblables aux substitutions (a); les substitutions (d) peuvent encore s'écrire

$$\left(z,\ az^{p^\alpha} - am^{p^\alpha} + m\right).$$

D'après cela, pour que la substitution (c) s'effectue sur moins de p^ν quantités, il faut que l'on puisse trouver une valeur de m satisfaisant à la congruence

$$-am^{p^\alpha} + m \equiv b$$

ou

$$am^{p^\alpha} - m + b \equiv 0;$$

si au contraire b est tel qu'il n'y ait aucun diviseur commun au premier membre de cette congruence et à $m^{p^\nu-1} - 1$, la substitution (c) s'effectue sur p^ν variables.

Nous avons examiné ces différents cas particuliers de la substitution

$$(e) \qquad \left(z,\ \frac{Az^{p^\alpha}+B}{Cz^{p^\alpha}+D}\right),$$

parce que toutes les substitutions (e) qui s'effectuent sur moins de $p^\nu+1$ variables sont semblables aux substitutions que nous venons de considérer; nous allons maintenant passer au cas général.

Pour étudier les substitutions (e), nous allons procéder comme nous l'avons fait pour les substitutions $\left(z, \frac{Az+B}{Cz+D}\right)$. (*Journal de M. Liouville*, année 1860.)

ω étant une racine primitive de $z^{p^\nu-1}\equiv 1$, soit

$$(f) \qquad \varphi\left[(x_0),\ x_1,\ x_\omega,\ x_{\omega^2},\ldots,\ x_{\omega p^\nu-2}\right]$$

une fonction qui est invariable par toutes les substitutions $\left(z,\ az^{p^\alpha}\right)$; faisons sur cette fonction toutes les substitutions $(z, z+m)$ et formons une fonction symétrique F de ces p^ν fonctions; sur la fonction F faisons la substitution $\left(z, \frac{1}{z}\right)$, nous aurons la fonction F'; enfin sur la fonction F' faisons les substitutions $\left(\frac{1}{z}, \frac{1}{z+k}\right)$, ce qui donnera les fonctions $F', F'_1,\ldots, F'_{p^\nu-1}$; soit Θ une fonction symétrique des $p^\nu+1$ fonctions $F, F', F'_1,\ldots, F'_{p^\nu-1}$; Θ est une fonction invariable par les substitutions (e), et les substitutions qui ne changent pas ces fonctions F sont les substitutions (e) qui s'effectuent sur moins de $p^\nu+1$ quantités.

La fonction F'_u contient la fonction

$$\varphi\left[\left(x_{\frac{1}{r}+u}\right),\ x_{\frac{1}{r+1}+u},\ x_{\frac{1}{r+\omega}+u},\ x_{\frac{1}{r+\omega^2}+u},\ldots,\ x_{\frac{1}{r+\omega^{p^\nu-2}}+u}\right],$$

qui est invariable par les substitutions

$$(g) \qquad \left(\frac{1}{r+z}+u,\ \frac{1}{r+az^{p^\alpha}}+u\right),$$

puisque la fonction (f) est invariable par les substitutions $\left(z, az^{p^\alpha}\right)$; donc F'_u est aussi invariable par les substitutions (g).

On met facilement les substitutions (g) sous cette forme

$$(h) \qquad \left\{ z, \frac{\left(\frac{1}{r - ar^{p^\alpha}} + u\right) z^{p^\alpha} - u^{p^\alpha + 1} + \frac{au - u^{p^\alpha}}{r - ar^{p^\alpha}}}{z^{p^\alpha} + \frac{a}{r - ar^{p^\alpha}} - u^{p^\alpha}} \right\}.$$

En donnant à r et u les p^ν valeurs dont ils sont susceptibles, on aura toutes les substitutions qui ont moins de $p^\nu + 1$ variables, et qui ne changent pas les fonctions F', F'_1, F'_2,..., $F'_{p^\nu - 1}$; il n'y a pas lieu d'ajouter aux substitutions (h) les substitutions $\left(z, mz^{p^\alpha} + n\right)$ qui laissent F invariable; car ces dernières substitutions se déduisent de l'expression (h) en y faisant

$$r \equiv 0.$$

Les substitutions (h) ou (g) qui s'effectuent sur moins de $p^\nu - 1$ variables sont celles pour lesquelles a est résidu de puissance $(p^\tau - 1)^{ième}$, τ étant le plus grand commun diviseur de α et de ν.

Les deux variables x_u et $x_{\frac{1}{r} + u}$ sont laissées immobiles par les substitutions (h); si cette substitution s'effectue sur moins de $p^\nu - 1$ quantités, les autres quantités qui resteront immobiles seront celles dont les indices sont racines de la congruence $z^{p^\alpha - 1} \equiv \frac{1}{a}$.

La puissance $s^{ième}$ de la substitution (g) ou (h) s'obtient en y changeant a en $a^{\frac{p^{s\alpha} - 1}{p - 1}}$ et z^{p^α} en $z^{p^{\alpha s}}$.

Les substitutions de p^ν quantités qui laissent F invariable sont les substitutions $\left(z, az^{p^\alpha} + n\right)$, dans lesquelles n est tel que $am^{p^\alpha} - m + n$ n'a aucun diviseur commun avec $m^{p^\nu - 1} - 1$; n étant pris de la même manière, toutes les substitutions de p^ν variables qui ne changent pas F'_u

sont données par l'expression

$$(k) \qquad \left(z,\ \frac{\left(\frac{1}{n}+u\right)z^{p^\alpha} - u^{p^\alpha+1} + \frac{au-u^{p^\alpha}}{n}}{z^{p^\alpha} + \frac{a}{n} - u^{p^\alpha}} \right);$$

nous avons donc toutes les substitutions (e) qui s'effectuent sur p^ν quantités.

On voit d'après cela que, excepté la substitution $(z, az^{p^\alpha}+n)$ de p^ν variables, toutes les substitutions (e) qui s'effectuent sur moins de $p^\nu+1$ quantités sont représentées par l'expression (k), n étant alors quelconque.

Si la substitution (e) s'effectue sur les $p^\nu+1$ quantités, elle peut encore être représentée par l'expression (k), mais à la condition que a, u, n ne soient plus de la forme $\alpha_0+\alpha_1 i+\ldots+\alpha_{\nu-1} i^{\nu-1}$, α_0, α_1, etc., étant entiers et i racine d'une congruence irréductible du degré ν; il faudra d'ailleurs que l'on ait

$$(m) \qquad \frac{1}{n}+u \equiv \frac{A}{C}, \quad -u^{p^\alpha+1} + \frac{au-u^{p^\alpha}}{n} \equiv \frac{B}{C}, \quad \frac{a}{n} - u^{p^\alpha} \equiv \frac{D}{C},$$

A, B, C, D étant de la forme $\alpha_0+\alpha_1 i+\ldots+\alpha_{\nu-1} i^{\nu-1}$.

Des congruences (m) on tire les deux suivantes :

$$\frac{A^{p^\alpha} + DC^{p^\alpha-1}}{C^{p^\alpha}} \equiv \frac{1+an^{p^\alpha-1}}{n^{p^\alpha}}, \quad \frac{AD-BC}{C^2} \equiv \frac{a}{n^2},$$

et en les joignant à la première congruence (m), on en tirera facilement ces trois autres équations qui donnent n, a et u :

$$(q) \qquad \frac{AD-BC}{C^2} n^{p^\alpha+1} - \frac{A^{p^\alpha} + DC^{p^\alpha-1}}{C^{p^\alpha}} n^{p^\alpha} + 1 \equiv 0,$$

$$a \equiv n^2 \frac{AD-BC}{C^2}, \quad u \equiv \frac{1}{n} - \frac{A}{C}.$$

Donc s'il y a une valeur de n de la forme $\alpha_0 + \alpha_1 i + \ldots + \alpha_{\nu-1} i^{\nu-1}$ satisfaisant à (q), les valeurs de a et de u sont de la même forme; donc aussi, pour que la substitution (e) s'effectue sur $p^\nu + 1$ quantités, la condition nécessaire et suffisante est que le premier membre de la congruence (q) n'ait aucun diviseur commun avec $n^{p^\nu - 1} - 1$.

D'après cela, supposons que λ et μ soient pris de telle sorte que la congruence

$$n^{p^\alpha + 1} - \lambda n^{p^\alpha} + \mu \equiv 0$$

soit irréductible, c'est-à-dire que son premier membre n'ait aucun facteur commun avec $n^{p^\nu - 1} - 1$. Posons

$$\frac{A^{p^\alpha} + DC^{p^\alpha - 1}}{C^{p^\alpha - 2}(AD - BC)} \equiv \lambda, \quad \frac{C^2}{AD - BC} \equiv \mu;$$

nous en tirerons

$$\frac{D}{C} \equiv \frac{\lambda}{\mu} - \frac{A^{p^\alpha}}{C^{p^\alpha}}, \quad \frac{B}{C} \equiv \frac{A\lambda}{C\mu} - \frac{A^{p^\alpha + 1}}{C^{p^\alpha + 1}} - \frac{1}{\mu}.$$

On voit d'après cela que pour chaque système de valeurs de λ et de μ, nous aurons p^ν systèmes de valeurs pour $\frac{A}{C}$, $\frac{B}{C}$, $\frac{D}{C}$, et les substitutions de $p^\nu + 1$ variables peuvent s'écrire

$$\left(z, \frac{A}{C} - \frac{1}{\mu z^{p^\alpha} + \lambda - \mu \dfrac{A^{p^\alpha}}{C^{p^\alpha}}} \right).$$

Fonction cinq fois transitive de douze quantités ayant $1.2.3.4.5.6.7 = 5040$ *valeurs.*

En nous appuyant sur ce qui a été dit dans ce chapitre et surtout sur ce qui a été exposé à la fin du chapitre I[er], nous pouvons facilement

démontrer l'existence d'une fonction cinq fois transitive de douze quantités.

Soit ω une racine de la congruence irréductible

$$\omega^2 + 2\omega + 2 \equiv 0 \pmod 3,$$

et considérons la fonction deux fois transitive des neuf quantités x_0, x_1, x_2, x_ω, $x_{1+\omega}$, $x_{2+\omega}$, $x_{2\omega}$, $x_{1+2\omega}$, $x_{2+2\omega}$, qui est invariable par toutes les substitutions comprises dans les deux expressions

$$(l) \qquad (x_z x_{\omega^{2r} z+m}),\ (x_z x_{\omega^{2r+1} z^3+m});$$

celles de ces substitutions qui ne s'effectueront que sur x_1, x_2, x_ω, $x_{1+\omega}$, $x_{2\omega}$, $x_{1+2\omega}$, $x_{2+\omega}$, $x_{2+2\omega}$, sont les suivantes :

$$(m) \qquad (x_z x_{\omega^2 z}) = (x_1\, x_{1+\omega}\, x_2\, x_{2+2\omega})(x_\omega\, x_{1+2\omega}\, x_{2\omega}\, x_{2+\omega}),$$

$$(n) \qquad (x_z x_{\omega^3 z^3}) = (x_1\, x_{1+2\omega}\, x_2\, x_{2+\omega})(x_{2+2\omega}\, x_{2\omega}\, x_{1+\omega}\, x_\omega),$$

$$(p) \qquad (x_z x_{\omega^5 z^3}) = (x_1\, x_{2\omega}\, x_2\, x_\omega)(x_{2+\omega}\, x_{1+\omega}\, x_{1+2\omega}\, x_{2+2\omega}),$$

$$(x_z x_{\omega^4 z}) = (x_1\, x_2)(x_{1+\omega}\, x_{2+2\omega})(x_\omega\, x_{2\omega})(x_{1+2\omega}\, x_{2+\omega}),$$

et leurs inverses; de plus toutes les substitutions (l) sont des dérivées de celles-là et de

$$(q) \qquad (x_0\, x_1\, x_2)(x_\omega\, x_{1+\omega}\, x_{2+\omega})(x_{2\omega}\, x_{1+2\omega}\, x_{2+2\omega}).$$

Identifions la substitution

$$(x_1\, x_{1+\omega}\, x_2\, x_{2+2\omega})(x_\omega\, x_{1+2\omega}\, x_{2\omega}\, x_{2+\omega})$$

avec

$$(x'_1\, x'_{2+2\omega}\, x'_2\, x'_{1+\omega})(x'_{2+\omega}\, x'_{2\omega}\, x'_{1+2\omega}\, x'_\omega);$$

nous pouvons faire $x'_1 = x_1$, et nous avons pour les quatre identifications :

$$x'_1 = x_1, \quad x'_{2+2\omega} = x_{1+\omega}, \quad x'_2 = x_2, \quad x'_{1+\omega} = x_{2+2\omega},$$

avec

$$1^\circ \quad x'_{2+\omega} = x_\omega, \quad x'_{2\omega} = x_{1+2\omega}, \; x'_{1+2\omega} = x_{2\omega}, \quad x'_\omega = x_{2+\omega};$$

$$2^\circ \quad x'_{2\omega} = x_\omega, \; x'_{1+2\omega} = x_{1+2\omega}, \quad x'_\omega = x_{2\omega}, \; x'_{2+\omega} = x^{2+\omega};$$

$$3^\circ \quad x'_{1+2\omega} = x_\omega, \quad x'_\omega = x_{1+2\omega}, \quad x'_{2+\omega} = x_{2\omega}, \quad x'_{2\omega} = x_{2+\omega};$$

$$4^\circ \quad x'_\omega = x_\omega, \; x'_{2+\omega} = x_{1+2\omega}, \quad x'_{2\omega} = x_{2\omega}, \quad x'_\omega = x_{2+\omega}.$$

Pour chacune de ces identifications la substitution

$$(x'_0\, x'_1\, x'_2)\,(x'_\omega\, x'_{1+\omega}\, x'_{2+\omega})\,(x'_{2\omega}\, x'_{1+2\omega}\, x'_{2+2\omega})$$

devient respectivement

$$1^\circ \quad (x'_1\, x_1\, x_2)\,(x_{2+\omega}\, x_{2+2\omega}\, x_\omega)\,(x_{1+2\omega}\, x_{2\omega}\, x_{1+\omega}),$$

$$2^\circ \quad (x'_0\, x_1\, x_2)\,(x_{2\omega}\, x_{2+2\omega}\, x_{2+\omega})\,(x_\omega\, x_{1+2\omega}\, x_{1+\omega}),$$

$$3^\circ \quad (x'_0\, x_1\, x_2)\,(x_{1+2\omega}\, x_{2+2\omega}\, x_{2\omega})(x_{2+\omega}\, x_\omega\, x_{1+\omega}),$$

$$4^\circ \quad (x'_0\, x_1\, x_2)\,(x_\omega\, x_{2+2\omega}\, x_{1+2\omega})\,(x_{2\omega}\, x_{2+\omega}\, x_{1+\omega}).$$

En cherchant quelques dérivées de la substitution 3° et des substitutions (m), (n), (q), on reconnaît immédiatement que la substitution 3° ne saurait donner une fonction trois fois transitive de dix variables.

Prenons les substitutions (m), (n), (p), (q) avec la substitution 1°, nous aurons un système que nous appellerons A; prenons les substitutions (m), (n), (p), (q), avec la substitution 2°, nous aurons un système B; enfin, prenons encore (m), (n), (p), (q) avec 4°, nous aurons le système C.

On voit facilement que pour la première identification on a $x'_z = x_{\chi z} = x_{\frac{1}{z}}$, et par suite qu'il existe une fonction invariable par le système A, et qu'elle est invariable par toutes les substitutions comprises dans les deux expressions

$$\left(x_z\, x_{\frac{Az+B}{Cz+D}}\right), \quad \left(x_z\, x_{\frac{A_1 z^1+B_1}{C_1 z^1+D_1}}\right),$$

AD — BC étant résidu quadratique et $A_1 D_1 - B_1 C_1$ non résidu.

On reconnaît ensuite que l'on passe du système A au système B par la substitution

$$(x_{1+\omega} x_{1+2\omega})(x_\omega x_{2\omega})(x_{2+2\omega} x_{2+\omega});$$

on passe aussi du système A au système C par la substitution

$$(x_{1+\omega} x_{2\omega})(x_{2+2\omega} x_\omega)(x_{1+2\omega} x_{2+\omega}).$$

Pour la première identification on a $x'_z = x_{\chi z} = x_{\frac{1}{z}}$, et la substitution $(x_z x_{\chi z}) = \left(x_z x_{\frac{1}{z}}\right)$ ne change pas les substitutions 2° et 4°.

Il résulte donc de la théorie exposée à la fin du chapitre I et en particulier de la dernière remarque que nous y avons faite, que l'on passe par une même substitution du système dérivé de

$$(m), (n), (p), (q), \quad 1°,$$

non-seulement au système dérivé de

$$(m), (n), (p), (q), \quad 2°,$$

mais encore au système dérivé de

$$(m), (n), (p), (q), \quad 3°.$$

Et pareillement on passe par une même substitution du système des substitutions dérivées de

$$(m), (n), (p), (q) \quad 1°$$

au système des substitutions dérivées de

$$(m), (n), (p), (q), \quad 4°$$

et au système des substitutions dérivées de

$$(m), (n), (p), \quad 1° \text{ et } 4°.$$

Nous avons donc bien une fonction cinq fois transitive des douze variables $x_1, x_2, x_\omega, x_{1+\omega}, x_{2\omega}, x_{1+2\omega}, x_{2+\omega}, x_{2+2\omega}, x_0, x'_0, x''_0, x'''_0$, et on caractérise cette fonction en disant qu'elle est invariable par les substitutions (l) et par les substitutions

$$(x'_0\, x_1\, x_2)\,(x_{2+\omega}\, x_{2+2\omega}\, x_\omega)\,(x_{1+2\omega}\, x_{2\omega}\, x_{1+\omega}),$$
$$(x''_0\, x_1\, x_2)(x_{2\omega}\, x_{2+2\omega}\, x_{2+\omega})(x_\omega\, x_{1+2\omega}\, x_{\omega+1}),$$
$$(x'''_0\, x_1\, x_2)(x_\omega\, x_{2+2\omega}\, x_{1+2\omega})(x_{2\omega}\, x_{2+\omega}\, x_{1+\omega}).$$

Enfin j'énoncerai encore sur cette fonction la remarque suivante que je ne démontrerai pas : Si on remplace les variables

$$x''_0, x'_0, x_\omega, x_{1+\omega}, x_{2+2\omega}, x_{1+2\omega}, x_2, x_1, x_0, x_{2+\omega}, x_{2\omega}, x'''_0$$

par

$$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_\infty,$$

respectivement, cette fonction de douze quantités est invariable par toutes les substitutions

$$\left(z, \frac{Az+B}{Cz+D}\right) \quad (\text{mod. } 11).$$

AD — BC étant résidu quadratique.

Je possède une fonction cinq fois transitive de 24 quantités qui a $\frac{1.2.3.4\ldots18.19}{16\times 3}$ valeurs, et qui est due à des circonstances différentes de celles qui donnent la fonction cinq fois transitive de douze quantités dont nous venons de parler [*].

[*] En joignant cette fonction cinq fois transitive aux fonctions de moins de trente-quatre quantités qui sont données par nos théorèmes généraux, on voit que l'on a des fonctions plusieurs fois transitives de n quantités, tant que n est < 34; ce fait tient simplement à ce que tous les nombres < 34, excepté 21 et 22, sont des nombres premiers, des puissances de nombres premiers, ou de tels nombres augmentés d'une unité, ou enfin des puissances de 2 diminuées d'une unité.

CHAPITRE III.

FONCTIONS PLUSIEURS FOIS TRANSITIVES DE p^ν VARIABLES (p NOMBRE PREMIER), QUI ONT $\frac{1.2.3\ldots(p^\nu-1)}{(p^\nu-1)(p^\nu-p)\ldots(p^\nu-p^{\nu-1})}$ VALEURS.

De la formation de ces fonctions.

Considérons un système de p^ν variables, et comme dans le chapitre précédent désignons-les par la lettre x affectée de p^ν indices qui soient les racines de la congruence

$$z^{p^\nu} - z \equiv 0 \pmod{p}; \tag{1}$$

nous allons maintenant nous occuper des fonctions de ces p^ν variables qui ne sont pas changées par toutes les substitutions

$$(z,\ Az^{p^\nu-1} + Bz^{p^\nu-2} + Cz^{p^\nu-3} + \ldots + Hz + L). \tag{2}$$

Il faut immédiatement remarquer que dans l'expression (2), A, B, C, ..., L ne sont pas des racines de la congruence (1) prises arbitrairement; pour que l'expression (2) représente une substitution, il faut en effet que le polynôme $Az^{p^\nu-1} + Bz^{p^\nu-2} + \ldots + Hz$ n'ait aucun facteur commun avec $z^{p^\nu} - z$, afin que, z_1 et z_2 étant deux racines de la congruence (1), on ne puisse avoir

$$Az_1^{p^\nu-1} + Bz_1^{p^\nu-2} + \ldots + Hz_1 \equiv Az_2^{p^\nu-1} + Bz_2^{p^\nu-2} + \ldots + Hz_2$$

ou

$$A(z_1 - z_2)^{p^\nu-1} + B(z_1 - z_2)^{p^\nu-2} + \ldots + H(z_1 - z_2) \equiv 0.$$

Cela posé, on a identiquement

$$\left\{\begin{aligned} &h\left(z^{p^\nu} - z\right) \equiv \left(h^{p^\nu-1}z^{p^\nu-1} + h^{p^\nu-2}z^{p^\nu-2} + \ldots + h^p z^p + hz\right) \\ &\times\left(h^{p^\nu-1}z^{p^\nu-1} + \ldots + hz + 1\right)\left(h^{p^\nu-1}z^{p^\nu-1} + \ldots + hz + 2\right)\cdots \\ &\times\left(h^{p^\nu-1}z^{p^\nu-1} + \ldots + hz + p - 1\right). \end{aligned}\right. \tag{3}$$

Soient $\alpha^{1,1}$, $\alpha^{1,2}$, $\alpha^{1,3}$, ..., $\alpha^{1,p^\nu-1}$ les racines de $z^{p^\nu} \equiv z$ dues au premier facteur, $\alpha^{2,1}$, $\alpha^{2,2}$, ..., $\alpha^{2,p^\nu-1}$ les racines dues au second, $\alpha^{3,1}$, $\alpha^{3,2}$, ..., $\alpha^{3,p^\nu-1}$ celles qui sont dues au troisième, et ainsi de suite. Prenons la fonction

$$(4)\quad \left\{ \begin{array}{c} x_{\alpha^{1,1}} x_{\alpha^{1,2}} x_{\alpha^{1,3}} \dots x_{\alpha^{1,p^\nu-1}} + x_{\alpha^{2,1}} x_{\alpha^{2,2}} \dots x_{\alpha^{2,p^\nu-1}} + \dots \\ + x_{\alpha^{p,1}} x_{\alpha^{p,2}} \dots x_{\alpha^{p,p^\nu-1}}; \end{array} \right.$$

nous pouvons donner à h dans l'expression (3) $p^\nu - 1$ valeurs; mais si e est une racine de $z^{p-1} \equiv 1$, $h = h_1$ et $h = h_1 e$ donnent les mêmes facteurs; de sorte que pour décomposer $z^{p^\nu} - z$ de toutes les manières possibles en facteurs comme dans l'identité (3), il suffit de donner à h $\frac{p^\nu - 1}{p-1}$ valeurs; à chaque décomposition de $z^{p^\nu} - z$ correspond une fonction telle que (4); prenons une fonction symétrique Φ de ces $\frac{p^\nu - 1}{p-1}$ fonctions, et nous aurons une fonction qui est invariable par toutes les substitutions (2). Il est clair d'après cela que l'on obtiendra la fonction Φ en faisant sur la fonction (4) les substitutions

$$(z, z),\quad (z, \omega z),\quad (z, \omega^2 z), \dots,\quad \left(z, \omega^{\frac{p^\nu - p}{p-1}} z\right),$$

ω étant une racine primitive de $z^{p^\nu - 1} \equiv 1$, et en formant une fonction symétrique des $\frac{p^\nu - 1}{p-1}$ fonctions ainsi obtenues.

Pour démontrer que la fonction Φ est invariable par toutes les substitutions (2), il suffit évidemment de prouver qu'une telle substitution change les indices qui satisfont à l'une des congruences

$$(5)\quad \left\{ \begin{array}{l} h^{p^\nu-1} z^{p^\nu-1} + h^{p^\nu-2} z^{p^\nu-2} + \dots + h^p z^p + hz \equiv 0, \\ h^{p^\nu-1} z^{p^\nu-1} + \dots + hz + 1 \equiv 0, \dots, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ h^{p^\nu-1} z^{p^\nu-1} + \dots + hz + p - 1 \equiv 0, \end{array} \right.$$

en les indices qui satisfont à l'une de celles-ci :

$$(6)\quad \begin{cases} h'^{p^{\nu-1}} z^{p^{\nu-1}} + h'^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + h'^{p} z^{p} + h' z \equiv 0, \\ h'^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h' z + 1 \equiv 0, \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ h'^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h' z + p - 1 \equiv 0. \end{cases}$$

Par la substitution (2) la racine z d'une des congruences (5) sera hangée en

$$u \equiv \mathrm{A} z^{p^{\nu-1}} + \mathrm{B} z^{p^{\nu-2}} + \ldots + \mathrm{H} z + \mathrm{L},$$

et de cette congruence on tirera

$$(7)\qquad z \equiv a u^{p^{\nu-1}} + b u^{p^{\nu-2}} + \ldots + l u^{p} + m u + n,$$

en désignant par

$$\left(z,\ a z^{p^{\nu-1}} + b z^{p^{\nu-2}} + \ldots + m u + n\right)$$

la substitution inverse de la substitution (2). Si donc nous remplaçons z par l'expression (7) dans les congruences (5), chacune des congruences qui en résulteront, donnera les indices en lesquels seront changés les indices qui satisfont à chaque congruence (5).

Substituons donc l'expression (7) dans

$$h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + h z + \nu \equiv 0,$$

et nous aurons

$$\begin{cases} h^{p^{\nu-1}} \left(a u^{p^{\nu-1}} + b u^{p^{\nu-2}} + \ldots + l u^{p} + m u + n\right)^{p^{\nu-1}} \\ + h^{p^{\nu-2}} \left(a u^{p^{\nu-1}} + b u^{p^{\nu-2}} + \ldots + m u + n\right)^{p^{\nu-2}} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ + h \left(a u^{p^{\nu-1}} + b u^{p^{\nu-2}} + \ldots + l u^{p} + m u + n\right) + \nu \equiv 0. \end{cases}$$

Posons

$$h m + h^{p^{\nu-1}} l^{p^{\nu-1}} + \ldots + h^{p} a^{p} \equiv h',$$
$$h^{p^{\nu-1}} n^{p^{\nu-1}} + h^{p^{\nu-2}} n^{p^{\nu-2}} + \ldots + h n \equiv \beta,$$

β étant une racine de $z^p \equiv z$, et la congruence précédente deviendra

$$h'^{p^{\nu-1}} u^{p^{\nu-1}} + h'^{p^{\nu-2}} u^{p^{\nu-2}} + \ldots + h'u + \beta + \nu \equiv 0,$$

h' et β étant indépendants de ν. Donc la fonction Φ est invariable par toutes les substitutions (2).

La fonction Φ est d'ailleurs changée par toute autre substitution, ainsi que nous allons le démontrer.

Donnons-nous une substitution quelconque $(z, \varphi z)$ et prenons la substitution inverse

$$\left(u,\ f_{p^{\nu-1}} u^{p^{\nu-1}} + f_{p^{\nu-2}} u^{p^{\nu-2}} + \ldots + f_l u^l + \ldots\right).$$

Pour que la substitution $(z, \varphi z)$ ne change pas la fonction Φ, il faut qu'en substituant

$$z \equiv f_{p^{\nu-1}} u^{p^{\nu-1}} + f_{p^{\nu-2}} u^{p^{\nu-2}} + \ldots + f_l u^l + \ldots \tag{8}$$

dans les congruences (5), on ait des congruences telles que (6), et cela quel que soit h; c'est la condition nécessaire et suffisante.

Substituons l'expression (8) dans

$$h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + hz + \nu \equiv 0$$

et nous aurons la congruence suivante

$$\left\{\begin{aligned}
&h^{p^{\nu-1}}\left[f_{p^{\nu-1}}^{p^{\nu-1}} u^{(p^{\nu}-1)p^{\nu-1}} + f_{p^{\nu-2}}^{p^{\nu-1}} u^{(p^{\nu}-2)p^{\nu-1}} + \ldots + f_l^{p^{\nu-1}} u^{lp^{\nu-1}} + \ldots\right]\\
&+ h^{p^{\nu-2}}\left[f_{p^{\nu-1}}^{p^{\nu-2}} u^{(p^{\nu}-1)p^{\nu-2}} + \ldots + f_l^{p^{\nu-2}} u^{lp^{\nu-2}} + \ldots\right] + \ldots\\
&+ h^{p^{\nu-r}}\left[f_{p^{\nu-1}}^{p^{\nu-r}} u^{(p^{\nu}-1)p^{\nu-r}} + \ldots + f_l^{p^{\nu-r}} u^{lp^{\nu-r}} + \ldots\right] + \ldots\\
&+ h\left[f_{p^{\nu-1}} u^{p^{\nu-1}} + f_{p^{\nu-2}} u^{p^{\nu-2}} + \ldots + f_l u^l + \ldots\right] + \nu \equiv 0.
\end{aligned}\right. \tag{9}$$

Parmi les termes de cette congruence, il y a les ν suivants :

$$\left\{\begin{array}{l}
\left[h^{p^\nu-1}f_l^{p^\nu-1}+h^{p^\nu-2}f_{lp}^{p^\nu-2}+h^{p^\nu-3}f_{lp^2}^{p^\nu-3}+\ldots\right.\\
\qquad\qquad\left.+h^{p^\nu-r}f_{lp^r}^{p^\nu-r}+\ldots+hf_{lp^{\nu-1}}\right]u^{lp^\nu-1}\\
+\left[h^{p^\nu-2}f_l^{p^\nu-2}+h^{p^\nu-3}f_{lp}^{p^\nu-3}+h^{p^\nu-4}f_{lp^2}^{p^\nu-4}+\ldots\right.\\
\qquad\qquad\left.+h^{p^\nu-r-1}f_{lp^r}^{p^\nu-r-1}+\ldots+h^{p^\nu-1}f_{lp^{\nu-1}}^{p^\nu-1}\right]u^{lp^\nu-2}\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
+\left[h^{p^\nu-s}f_l^{p^\nu-s}+h^{p^\nu-s-1}f_{lp}^{p^\nu-s-1}+h^{p^\nu-s-2}f_{lp^2}^{p^\nu-s-2}+\ldots\right.\\
\qquad\left.+h^{p^\nu-s-r}f_{lp^r}^{p^\nu-s-r}+\ldots+h^{p^\nu-s+1}f_{lp^{\nu-1}}^{p^\nu-s+1}\right]u^{lp^\nu-s}.\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}\right.$$

Nous voyons que les coefficients de ces puissances de u sont tous des puissances du premier. Supposons que l ne soit pas une puissance de p; pour que la congruence (9) ait la forme des congruences (6), il faut que les coefficients de ces puissances de u soient nuls : ce qu'on exprimera en égalant simplement le premier à zéro et il viendra :

$$(10)\quad h^{p^\nu-1}f_l^{p^\nu-1}+h^{p^\nu-2}f_{lp}^{p^\nu-2}+\ldots+h^{p^\nu-r}f_{lp^r}^{p^\nu-r}+\ldots+hf_{lp^{\nu-1}}\equiv 0;$$

remarquons que f_l, f_{lp}, f_{lp^2}, $f_{lp^{\nu-1}}$ ne figurent pas dans les autres coefficients des puissances de u; mais la congruence (10) devant avoir lieu quel que soit h, on a

$$f_l\equiv 0,\quad f_{lp}\equiv 0,\quad f_{lp^2}\equiv 0,\ldots,\quad f_{lp^{\nu-1}}\equiv 0.$$

Si au contraire l est une puissance de p, les coefficients de $u^{lp^\nu-1}$, $u^{lp^\nu-2}$, etc., ne devront pas être égalés à zéro et l'on n'aura plus à poser la congruence (10). Donc dans l'expression (8), des différents coefficients f il ne reste que ceux dont les indices sont des puissances de u; ce qu'il fallait démontrer.

On peut encore former d'une autre manière élégante une fonction invariable par toutes les substitutions (2).

Soient o, b_1, b_2,..., $b_{p^\nu-1-1}$ les racines de la congruence

$$z^{p^\nu-1}+z^{p^\nu-2}+z^{p^\nu-3}+\ldots+z^p+z\equiv 0,$$

on a la congruence identique

$$(11)\quad\begin{cases}\lambda\left(z^{p^\nu}-z\right)\equiv(\lambda^p z^p-\lambda z)(\lambda^p z^p-\lambda z-b_1)(\lambda^p z^p-\lambda z-b_2)\ldots\\ \ldots\ldots\ldots\ldots\ldots\ldots(\lambda^p z^p-\lambda z-b_{p^\nu-1-1}).\end{cases}$$

Désignons par $\alpha_1,\alpha_2,\ldots,\alpha_p$ les racines de la congruence $\lambda^p z^p-\lambda z\equiv 0$, par α_1+m, $\alpha_2+m,\ldots,\alpha_p+m$ les racines de $\lambda^p z^p\equiv\lambda z+b_1$, par α_1+m', $\alpha_2+m',\ldots\alpha_p+m'$ les racines de $\lambda^p z^p\equiv\lambda z+b_2$, et ainsi de suite. Prenons la fonction

$$(12)\quad\begin{cases}x_{\alpha_1}x_{\alpha_2}x_{\alpha_3}\ldots x_{\alpha_p}+x_{\alpha_1+m}x_{\alpha_2+m}\ldots x_{\alpha_p+m}\\ \qquad\qquad+x_{\alpha_1+m'}x_{\alpha_2+m'}\ldots+x_{\alpha_p+m'}+\ldots;\end{cases}$$

on peut, dans la congruence identique (11), donner $p^\nu-1$ valeurs à λ; mais si e est racine de $z^{p-1}\equiv 1$, $\lambda\equiv\lambda_1$ et $\lambda=\lambda_1 e$ donnent la même décomposition en facteurs; il y a donc $\frac{p^\nu-1}{p-1}$ de ces décompositions, et à chacune de ces décompositions correspond une fonction telle que (12). Pour obtenir ces $\frac{p^\nu-1}{p-1}$ fonctions, il suffit de faire sur la fonction (12) les substitutions

$$(z,\ z),\quad(z,\ \omega z),\quad(z,\ \omega^2 z),\ldots,\quad\left(z,\ \omega^{\frac{p^\nu-p}{p-1}}z\right),$$

ω étant une racine primitive de $z^{p^\nu-1}\equiv 1$; formons une fonction symétrique Ψ de ces fonctions et nous aurons une fonction invariable par toutes les substitutions (2).

Remarquons d'abord que l'une des fonctions qui composent Ψ est la fonction (12), et que toutes les autres sont représentées par

$$x_{a\alpha_1}x_{a\alpha_2}\ldots x_{a\alpha_p}+x_{a(\alpha_1+m)}x_{a(\alpha_2+m)}\ldots x_{a(\alpha_p+m)}$$
$$+x_{a(\alpha_1+m')}x_{a(\alpha_2+m')}\ldots x_{a(\alpha_p+m')}+\ldots$$

Faisons la substitution (2); les indices α_1, α_2,..., α_p seront changés en

$$(13)\qquad \begin{cases} A\alpha_1^{p^\nu-1} + B\alpha_1^{p^\nu-2} + \ldots + H\alpha_1 + L, \\ A\alpha_2^{p^\nu-1} + B\alpha_2^{p^\nu-2} + \ldots + H\alpha_2 + L, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{cases}$$

et puisque chacune de ces quantités α satisfait à $\lambda^p\alpha^p - \lambda\alpha \equiv 0$ ou $\alpha^p \equiv \frac{1}{\lambda}\alpha$, les quantités (13) peuvent se mettre sous la forme

$$R\alpha_1 + S, \quad R\alpha_2 + S, \quad R\alpha_3 + S, \ldots,$$

et les indices $\alpha_1 + m$, $\alpha_2 + m$, $\alpha_3 + m$,..., seront changés en

$$R\alpha_1 + S + M, \quad R\alpha_2 + S + M, \quad R\alpha_3 + S + M, \ldots$$

D'où il suit évidemment que les fonctions qui composent Ψ s'échangent entre elles par la substitution (2).

On pourrait encore démontrer que la fonction Ψ est changée par toute substitution qui n'est pas de la forme (2).

Comme précédemment, désignons par $\alpha^{1,1}$, $\alpha^{1,2}$,..., $\alpha^{1,p^\nu-1}$ les racines de $z^{p^\nu} \equiv z$ dues au premier facteur du second membre de (3), par $\alpha^{2,1}$, $\alpha^{2,2}$,..., $\alpha^{2,p^\nu-1}$ les racines dues au second, et ainsi de suite. On obtiendra une des fonctions qui composent Φ en formant une fonction symétrique des produits des variables dont les indices sont donnés par les lignes horizontales de ce tableau :

$$(a)\qquad \begin{cases} \alpha^{1,1}, & \alpha^{1,2}, & \alpha^{1,3}, \ldots, & \alpha^{1,p^\nu-1}, \\ \alpha^{2,1}, & \alpha^{2,2}, & \alpha^{2,3}, \ldots, & \alpha^{2,p^\nu-1}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha^{p,1}, & \alpha^{p,2}, & \alpha^{p,3}, \ldots, & \alpha^{p,p^\nu-1}. \end{cases}$$

Multiplions les indices du tableau (a) par m', nous aurons cet autre

tableau

$$(a') \qquad \begin{cases} m'\alpha^{1,1}, & m'\alpha^{1,2}, & m'\alpha^{1,3},\ldots, & m'\alpha^{1,p^\nu-1}, \\ m'\alpha^{2,1}, & m'\alpha^{2,2}, & m'\alpha^{2,3},\ldots, & m'\alpha^{2,p^\nu-1}, \\ \ldots & \ldots & \ldots & \ldots \\ m'\alpha^{p,1}, & m'\alpha^{p,2}, & m'\alpha^{p,3},\ldots, & m'\alpha^{p,p^\nu-1}. \end{cases}$$

On obtiendra encore une des fonctions qui composent Φ en prenant la même fonction symétrique des produits des variables dont les indices sont donnés par les lignes horizontales du tableau (a').

Remarquons ensuite qu'il y a une et une seule racine de la congruence $z^p \equiv z + b_\nu$ qui appartient à la congruence

$$h^{p^\nu-1} z^{p^\nu-1} + h^{p^\nu-2} z^{p^\nu-2} + \ldots + hz + a \equiv 0.$$

D'après cela, si dans le tableau (a) on a disposé convenablement les termes dans chaque ligne horizontale, les lignes verticales représenteront les racines de $z^p - z - b_\nu \equiv 0$. Alors en prenant une fonction symétrique des produits des variables données par les lignes verticales du tableau (a), on aura une fonction qui compose Ψ; on aura de même les autres fonctions qui composent Ψ en agissant semblablement sur les tableaux tels que (a').

Nota. — Soient Ψ et Ψ' deux fonctions invariables par les substitutions (2) et soit χ la fonction des mêmes variables qui a deux valeurs. Si p est différent de 2, la fonction $\Psi + \Psi'\chi$ a un nombre de valeurs double de celui de Ψ.

Étude des substitutions $\left(z,\ \lambda_{\nu-1} z^{p^{\nu-1}} + \lambda_{\nu-2} z^{p^{\nu-2}} + \ldots + \lambda_1 z^p + \lambda_0 z\right)$.

Si on laisse immobile la variable x_0, les seules substitutions qui laissent invariables les fonctions que nous venons de considérer sont données par l'expression

$$(14) \qquad \left(z,\ \lambda_{\nu-1} z^{p^{\nu-1}} + \lambda_{\nu-2} z^{p^{\nu-2}} + \ldots + \lambda_1 z^p + \lambda_0 z\right),$$

et nous allons étudier ces substitutions.

Désignons par ω une racine d'une congruence irréductible du degré ν; toutes les racines de la congruence $z^{p^\nu} \equiv z$ sont données par l'expression $a_0 + a_1\omega + a_2\omega^2 + \ldots + a_{\nu-1}\omega^{\nu-1}$, a_0, $a_1, \ldots$, $a_{\nu-1}$ étant des entiers réels pris par rapport au module p. Désignons ensuite par u_0, u_1, $u_2, \ldots$, $u_{\nu-1}$ les valeurs en lesquelles les indices 1, ω, $\omega^2, \ldots$, $\omega^{\nu-1}$ sont changés par la substitution (14), nous aurons les congruences :

$$(15)\quad \begin{cases} \lambda_{\nu-1} + \lambda_{\nu-2} + \lambda_{\nu-3} + \ldots + \lambda_1 + \lambda_0 \equiv u_0, \\ \omega^{p^\nu-1}\lambda_{\nu-1} + \omega^{p^\nu-2}\lambda_{\nu-2} + \omega^{p^\nu-3}\lambda_{\nu-3} + \ldots + \omega^p\lambda_1 + \omega\lambda_0 \equiv u_1, \\ \omega^{2p^\nu-1}\lambda_{\nu-1} + \omega^{2p^\nu-2}\lambda_{\nu-2} + \omega^{2p^\nu-3}\lambda_{\nu-3} + \ldots + \omega^{2p}\lambda_1 + \omega^2\lambda_0 \equiv u_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \omega^{(\nu-1)p^\nu-1}\lambda_{\nu-1} + \omega^{(\nu-1)p^\nu-2}\lambda_{\nu-2} + \omega^{(\nu-1)p^\nu-3}\lambda_{\nu-3} + \ldots + \omega^{\nu-1}\lambda_0 \equiv u_{\nu-1}, \end{cases}$$

Au moyen de ces congruences, on pourra tirer les valeurs de $\lambda_{\nu-1}$, $\lambda_{\nu-2}, \ldots$, λ_0, et il s'agit de prendre les quantités u_0, u_1, $u_2, \ldots$, $u_{\nu-1}$ de telle façon que l'expression (14) soit bien une substitution.

Multiplions les congruences (15) respectivement par les entiers a_0, $a_1, \ldots$, $a_{\nu-1}$ et ajoutons, nous aurons

$$\begin{cases} \left(a_0 + a_1\omega + a_2\omega^2 + \ldots + a_{\nu-1}\omega^{\nu-1}\right)^{p^\nu-1}\lambda_{\nu-1} \\ + \left(a_0 + a_1\omega + \ldots + a_{\nu-1}\omega^{\nu-1}\right)^{p^\nu-2}\lambda_{\nu-2} + \ldots\ldots \\ + \left(a_0 + a_1\omega + \ldots + a_{\nu-1}\omega^{\nu-1}\right)^p\lambda_1 \\ + \left(a_0 + a_1\omega + \ldots + a_{\nu-1}\omega^{\nu-1}\right)\lambda_0 \\ \equiv a_0u_0 + a_1u_1 + \ldots + a_{\nu-1}u_{\nu-1}. \end{cases}$$

D'après cela, pour que l'expression (14) représente une substitution, il faut qu'en donnant aux quantités a_0, $a_1, \ldots$, $a_{\nu-1}$ toutes les valeurs dont elles sont susceptibles, l'expression $a_0u_0 + a_1u_1 + \ldots + a_{\nu-1}u_{\nu-1}$ prenne p^ν valeurs différentes; à cet effet nous prendrons u_0, $u_1, \ldots$, $u_{\nu-1}$ de la manière suivante.

Nous prendrons d'abord pour u_0 une quelconque des racines de la

congruence $z^{p^\nu-1} \equiv 1$. Formons la congruence

$$z(z-u_0)(z-2u_0)(z-3u_0)\dots(z-\overline{p-1}\,u_0)\equiv 0,$$

ou

$$z^p - u_0^{p-1} z \equiv 0;$$

nous prendrons pour u_1 une quelconque des valeurs qui ne satisfont pas à cette congruence, c'est-à-dire qui ne sont pas de la forme $\alpha_0 u_0$, α_0 étant un nombre entier.

Formons la congruence

$$\begin{aligned}(z^p - u_0^{p-1}z)\left[z^p - u_0^{p-1}z - (u_1^p - u_0^{p-1}u_1)\right]\\ \times \left[z^p - u_0^{p-1}z - 2(u_1^p - u_0^{p-1}u_1)\right]\dots\\ \times \left[z^p - u_0^{p-1}z - \overline{p-1}(u_1^p - u_0^{p-1}u_1)\right]\equiv 0\end{aligned}$$

qui peut se mettre sous la forme

$$z^{p^2} + \mathrm{M}z^p + \mathrm{N}\equiv 0;$$

nous prendrons pour u_2 une quelconque des $p^\nu - p^2$ quantités qui ne satisfont pas à cette dernière congruence; u_2 sera donc assujetti à ne pas être de la forme $\alpha_0 u_0 + \alpha_1 u_1$, α_0 et α_1 étant deux entiers.

Ayant ainsi fixé les valeurs de u_0, $u_1,\dots,$ $u_{\nu-1}$, l'expression $a_0u_0 + a_1u_1 + \dots + a_{\nu-1}u_{\nu-1}$ renferme évidemment p^ν quantités différentes; car a_0u_0 est susceptible de p valeurs; u_1 n'est pas de la forme $\alpha_0 u_0$; donc $a_0u_0 + a_1u_1$ est susceptible de p^2 valeurs, et ainsi de suite.

D'ailleurs si $u_0, u_1,\dots, u_{\nu-1}$ sont pris d'autre sorte et que l'on ait par exemple $u_k = \alpha_0u_0 + \alpha_1u_1 + \dots + \alpha_{k-1}u_{k-1}$, il est clair que l'on n'a plus p^ν valeurs distinctes pour l'expression $a_0u_0 + a_1u_1 + \dots + a_{\nu-1}u_{\nu-1}$, et par conséquent l'expression (14) ne représente plus une substitution. Donc $u_0, u_1,\dots, u_{\nu-1}$ doivent être déterminés comme nous l'avons fait.

Nous avons vu que l'on peut donner $p^\nu - 1$ valeurs à u_0, que la va-

leur de u_0 étant fixée, on peut choisir pour u_1 entre $p^\nu - p$ valeurs, puis pour u_2 on peut choisir entre $p^\nu - p^2$ valeurs, etc, et enfin pour $u_{\nu-1}$ on peut choisir entre $p^\nu - p^{\nu-1}$ valeurs; donc le nombre des substitutions (14) est

$$(p^\nu - 1)(p^\nu - p)(p^\nu - p^2)\dots(p^\nu - p^{\nu-1});$$

donc aussi le nombre des valeurs de la fonction de p^ν quantités invariable par toutes les substitutions

$$(z,\ Az^{p^\nu-1} + Bz^{p^\nu-2} + \dots + Hz + L)$$

est

$$\frac{1.2.3\dots(p^\nu-1)}{(p^\nu-p^{\nu-1})(p^\nu-p^{\nu-2})\dots(p^\nu-p)(p^\nu-1)}.$$

Soient $\omega_0,\ \omega_1,\ \omega_2,\dots,\ \omega_{\nu-1}$, ν quantités obtenues comme $u_0,\ u_1,\dots,\ u_{\nu-1}$; toutes les racines de $z^{p^\nu} \equiv z$ sont renfermées dans la formule $a_0\omega_0 + a_1\omega_1 + \dots + a_{\nu-1}\omega_{\nu-1}$. Si donc, au lieu de poser les congruences (15), on pose les congruences

$$(16)\quad \begin{cases} \omega_0^{p^\nu-1}\lambda_{\nu-1} + \omega_0^{p^\nu-2}\lambda_{\nu-2} + \dots + \omega_0^p\lambda_1 + \omega_0\lambda_0 \equiv u_0, \\ \omega_1^{p^\nu-1}\lambda_{\nu-1} + \omega_1^{p^\nu-2}\lambda_{\nu-2} + \dots + \omega_1^p\lambda_1 + \omega_1\lambda_0 \equiv u_1, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \omega_{\nu-1}^{p^\nu-1}\lambda_{\nu-1} + \omega_{\nu-1}^{p^\nu-2}\lambda_{\nu-2} + \dots + \omega_{\nu-1}^p\lambda_1 + \omega_{\nu-1}\lambda_0 \equiv u_{\nu-1}, \end{cases}$$

on en tirera

$$(b)\quad \begin{cases} (a_0\omega_0 + a_1\omega_1 + \dots + a_{\nu-1}\omega_{\nu-1})^{p^\nu-1}\lambda_{\nu-1} \\ + (a_0\omega_0 + a_1\omega_1 + \dots + a_{\nu-1}\omega_{\nu-1})^{p^\nu-2}\lambda_{\nu-2} + \dots\dots \\ + (a_0\omega_0 + \dots + a_{\nu-1}\omega_{\nu-1})\lambda_0 \equiv a_0u_0 + a_1u_1 + \dots + a_{\nu-1}u_{\nu-1}, \end{cases}$$

et les valeurs de $u_0,\ u_1,\dots,\ u_{\nu-1}$ devront encore être prises comme nous l'avons fait ci-dessus.

Considérons les substitutions (14) qui laissent immobiles les p^k va-

riables dont les indices sont représentés par l'expression

$$(17) \qquad a_0\omega_0 + a_1\omega_1 + \ldots + a_{k-1}\omega_{k-1}.$$

Je dis que la fonction qui est invariable par les substitutions (14) est transitive par rapport aux $p^\nu - p^k$ variables qui ne sont pas comprises dans la forme (17).

En effet, dans les congruences (16), faisons $u_0 \equiv \omega_0$, $u_1 \equiv \omega_1, \ldots$ $u_{k-1} \equiv \omega_{k-1}$, la substitution (14) laissera alors immobiles les p_k variablés (17), puisque la congruence (b) deviendra

$$\left\{\begin{array}{l} (a_0\omega_0 + a_1\omega_1 + \ldots + a_{\nu-1}\omega_{\nu-1})^{p^\nu-1}\lambda_{\nu-1} \\ + (a_0\omega_0 + a_1\omega_1 + \ldots + a_{\nu-1}\omega_{\nu-1})^{p^\nu-2}\lambda_{\nu-2} + \ldots \\ + (a_0\omega_0 + \ldots + a_{\nu-1}\omega_{\nu-1})\lambda_0 \\ \equiv a_0\omega_0 + \ldots a_{k-1}\omega_{k-1} + a_k u_k + \ldots + a_{\nu-1}u_{\nu-1}. \end{array}\right.$$

Pour que la fonction considérée soit transitive par rapport aux $p^\nu - p^k$ variables autres que les variables (17), il suffit que l'on puisse changer une de ces variables en une quelconque des $p^\nu - p^k - 1$ autres; or on changera l'indice déterminé

$$a_0\omega_0 + a_1\omega_1 + \ldots + a_{k-1}\omega_{k-1} + a_k\omega_k,$$

dans lequel a_k est incongru à zéro, en l'indice

$$a'_0\omega_0 + a'_1\omega_1 + \ldots + a'_{k-1}\omega_{k-1} + \ldots + a'_{\nu-1}\omega_{\nu-1},$$

en satisfaisant à la congruence

$$(18) \quad a_0\omega_0 + \ldots + a_{k-1}\omega_{k-1} + a_k u_k \equiv a'_0\omega_0 + a'_1\omega_1 + \ldots + a'_{\nu-1}\omega_{\nu-1};$$

a_k est différent de zéro, et parmi les quantités $a'_k, a'_{k+1}, \ldots, a'_{\nu-1}$, il y en a au moins une qui est différente de zéro; donc la valeur de u_k donnée par la congruence (18) est convenable, puisque l'on peut prendre pour u_k toute expression qui n'est pas de la forme (17). On voit donc que l'on peut changer une des $p^\nu - p^k$ variables qui ne sont

pas de la forme (17) en une quelconque des $p^\nu - p^k - 1$ autres de ces variables; donc la fonction considérée est transitive par rapport à ces $p^\nu - p^k$ variables.

D'après cela, soient $\omega_0, \omega_1, \ldots, \omega_{\nu-1}, \nu$ racines de la congruence $z^{p^\nu} \equiv z$, telles que l'on n'ait pas $\omega_k \equiv \alpha_0\omega_0 + \alpha_1\omega_1 + \ldots + \alpha_{k-1}\omega_{k-1}$, $\alpha_0, \alpha_1, \ldots, \alpha_{k-1}$ étant des entiers, la fonction de p^ν variables qui n'est pas changée par toutes les substitutions

$$(19) \qquad \left(z, \quad \lambda_{\nu-1} z^{p^{\nu-1}} + \lambda_{\nu-2} z^{p^{\nu-2}} + \ldots + \lambda_0 z + m\right),$$

est transitive par rapport à ses p^ν variables, puis transitive par rapport aux $p^\nu - 1$ variables autres que x_0, puis transitive par rapport aux $p^\nu - p$ variables dont les indices ne sont pas de la forme $\alpha_0\omega_0$, puis transitive par rapport aux $p^\nu - p^2$ variables dont les indices ne sont pas de la forme $\alpha_0\omega_0 + \alpha_1\omega_1$, etc., et enfin transitive par rapport aux $p^\nu - p^{\nu-1}$ variables dont les indices ne sont pas de la forme

$$\alpha_0\omega_0 + \alpha_1\omega_1 + \ldots + \alpha_{\nu-2}\omega_{\nu-2}.$$

La fonction invariable par toutes les substitutions (19) est donc en général deux fois transitive; dans le cas de $p = 2$, cette fonction est trois fois transitive.

Désignons par D le déterminant

$$\begin{vmatrix} \omega_0^{p^{\nu-1}}, & \omega_0^{p^{\nu-2}}, \ldots, & \omega_0^{p}, & \omega_0 \\ \omega_1^{p^{\nu-1}}, & \omega_1^{p^{\nu-2}}, \ldots, & \omega_1^{p}, & \omega_1 \\ \cdots & \cdots & \cdots & \cdots \\ \omega_{\nu-1}^{p^{\nu-1}}, & \omega_{\nu-1}^{p^{\nu-2}}, \ldots, & \omega_{\nu-1}^{p}, & \omega_{\nu-1} \end{vmatrix}.$$

Les congruences (16) nous donneront

$$\lambda_\varepsilon \equiv \frac{1}{\mathrm{D}}\left(u_0 \frac{d\mathrm{D}}{d\omega_0^{p^\varepsilon}} + u_1 \frac{d\mathrm{D}}{d\omega_1^{p^\varepsilon}} + \ldots + u_{\nu-1} \frac{d\mathrm{D}}{d\omega_{\nu-1}^{p^\varepsilon}}\right),$$

et par conséquent nous aurons, en posant

$$\frac{d\mathrm{D}}{d\omega_r} = h_r$$

et par suite

$$\frac{d\mathrm{D}}{d\omega_r^{p^\varepsilon}} \equiv \left(\frac{d\mathrm{D}}{d\omega_r}\right)^{p^\varepsilon} = h_r^{p^\varepsilon}$$

la congruence

$$(20)\quad \begin{cases} \lambda_{\nu-1} z^{p^{\nu-1}} + \lambda_{\nu-2} z^{p^{\nu-2}} + \ldots + \lambda_1 z^p + \lambda_0 z \\ \equiv \dfrac{u_0}{\mathrm{D}} \left(h_0^{p^{\nu-1}} z^{p^{\nu-1}} + h_0^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + h_0 z\right) \\ + \dfrac{u_1}{\mathrm{D}} \left(h_1^{p^{\nu-1}} z^{p^{\nu-1}} + h_1^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + h_1 z\right) + \ldots \\ + \dfrac{u_{\nu-1}}{\mathrm{D}} \left(h_{\nu-1}^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h_{\nu-1} z\right). \end{cases}$$

Si la substitution (14) ne permute aucune des p^k variables

$$x_{a_0\omega_0 + a_1\omega_1 + \ldots + a_{k-1}\omega_{k-1}}$$

on voit facilement que l'on a

$$\begin{cases} \lambda_{\nu-1} z^{p^{\nu-1}} + \ldots + \lambda_1 z^p + \lambda_0 z \\ \equiv z + \dfrac{u_k - \omega_k}{\mathrm{D}} \left(h_k^{p^{\nu-1}} z^{p^{\nu-1}} + h_k^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + h_k z\right) \\ + \dfrac{u_{k+1} - \omega_{k+1}}{\mathrm{D}} \left(h_{k+1}^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h_{k+1} z\right) + \ldots \\ + \dfrac{u_{\nu-1} - \omega_{\nu-1}}{\mathrm{D}} \left(h_{\nu-1}^{p^{\nu-1}} z^{p^{\nu-1}} + h_{\nu-1}^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + h_{\nu-1} z\right). \end{cases}$$

En particulier, si on fait $k = \nu - 1$, on aura

$$\begin{aligned} &\lambda_{\nu-1} z^{p^{\nu-1}} + \ldots + \lambda_1 z^p + \lambda_0 z \\ &\equiv z + a\left(h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + hz\right), \end{aligned}$$

et par conséquent les substitutions qui s'effectuent sur $p^\nu - p^{\nu-1}$ variables sont données par l'expression

$$\left[z,\ z + a\left(h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + hz\right)\right].$$

Si on élève D à la puissance p^{ieme}, il est aisé de voir que D reste le même ou change de signe seulement; on a donc $D^p \pm D \equiv 0 \pmod{p}$; ainsi dans le cas de $p = 2$, on a $D \equiv 1 \pmod{2}$.

Application à la fonction deux fois transitive de neuf quantités qui a 840 valeurs.

Proposons-nous de déterminer la fonction deux fois transitive de neuf quantités qui a $\frac{1.2.3.4.5.6.7.8}{(3^2-1)(3^2-3)} = 840$ valeurs, et qui est invariable par toutes les substitutions

$$(a) \qquad (z, \lambda_1 z^3 + \lambda_0 z + m).$$

Désignons par ω une racine de la congruence irréductible

$$\omega^2 + 2\omega + 2 \equiv 0 \pmod{3},$$

nous aurons

$$z^{3^2} - z \equiv (z^3 + z)(z^3 + z + 1)(z^3 + z + 2),$$

et les racines de $z^{3^2} - z \equiv 0$ dues à ces trois facteurs sont

$$1^o \quad 0, 1+\omega, 2+2\omega; \quad 2^o \quad 1, 2+\omega, 2\omega; \quad 3^o \quad 2, \omega, 1+2\omega.$$

Nous aurons donc la fonction cherchée en formant une fonction symétrique de ces quatre fonctions :

$$\begin{cases} x_0 x_{1+\omega} x_{2+2\omega} + x_1 x_{2+\omega} x_{2\omega} + x_2 x_\omega x_{1+2\omega}, \\ x_0 x_{1+2\omega} x_{2+\omega} + x_\omega x_1 x_{2+2\omega} + x_{2\omega} x_{1+\omega} x_2, \\ x_0 x_2 x_1 + x_{1+\omega} x_\omega x_{2+\omega} + x_{2+2\omega} x_{1+2\omega} x_{2\omega}, \\ x_0 x_{2\omega} x_\omega + x_{1+2\omega} x_{1+\omega} x_1 + x_{2+\omega} x_2 x_{2+2\omega}. \end{cases}$$

Nous déterminerons λ_1 et λ_0 par les congruences

$$\left.\begin{aligned} \lambda_1 + \lambda_0 &\equiv u_0, \\ \omega^3 \lambda_1 + \omega \lambda_0 &\equiv u_1, \end{aligned}\right\} \pmod{3},$$

et les substitutions (a) sont données par l'expression

$$[z, (\omega^3 u_0 + \omega^6 u_1) z^3 + (\omega u_0 + \omega^2 u_1) z + m],$$

u_0 étant un nombre quelconque différent de zéro, et u_1 étant un nombre quelconque autre que 0, u_0, 2 u_0.

Application à la fonction trois fois transitive de huit quantités qui a 30 *valeurs.*

Formons ensuite la fonction trois fois transitive de huit quantités, qui a $\frac{1.2.3.4.5.6\ 7}{(2^3-1)(2^3-2)(2^3-2^2)} = 30$ valeurs, et qui est invariable par toutes les substitutions

$$(b) \qquad (z, \lambda_2 z^4 + \lambda_1 z^2 + \lambda_0 z + m).$$

Soit ω une racine de la congruence irréductible

$$\omega^3 + \omega + 1 \equiv 0 \pmod 2,$$

ω est racine primitive de $z^7 \equiv 1$. On a la congruence

$$z^{2^3} - z \equiv (z^4 + z^2 + z)(z^4 + z^2 + z + 1),$$

et les racines de $z^{2^3} - z \equiv 0$ dues à ces deux facteurs sont

$$0, \quad \omega, \quad \omega^2, \quad \omega + \omega^2,$$

et

$$1, \quad 1 + \omega, \quad 1 + \omega^2, \quad 1 + \omega + \omega^2.$$

On a d'autre part

$$z^{2^3} - z \equiv (z^2 + z)(z^2 + z + \omega)(z^2 + z + \omega^2)(z^2 + z + \omega + \omega^2),$$

et les racines dues à ces facteurs sont

1° $0, 1$; 2° $\omega, 1+\omega$; 3° $\omega^2, 1+\omega^2$; 4° $\omega+\omega^2, 1+\omega+\omega^2$.

D'après cela, faisons sur la fonction

$$x_0 x_\omega x_{\omega^2} x_{\omega+\omega^2} + x_1 x_{1+\omega} x_{1+\omega^2} x_{1+\omega+\omega^2}$$

la substitution $(z, \omega z)$ ou

$$(x_1 x_\omega x_{\omega^2} x_{1+\omega} x_{\omega+\omega^2} x_{1+\omega+\omega^2} x_{1+\omega^2}),$$

et ses puissances, nous aurons les sept fonctions :

$$\begin{cases} x_0 x_\omega x_{\omega^2} x_{\omega+\omega^2} + x_1 x_{1+\omega} x_{1+\omega^2} x_{1+\omega+\omega^2}, \\ x_0 x_{\omega^2} x_{1+\omega} x_{1+\omega+\omega^2} + x_\omega x_{\omega+\omega^2} x_1 x_{1+\omega^2}, \\ x_0 x_{1+\omega} x_{\omega+\omega^2} x_{1+\omega^2} + x_{\omega^2} x_{1+\omega-\omega^2} x_\omega x_1, \\ x_0 x_{\omega+\omega^2} x_{1+\omega+\omega^2} x_1 + x_{1+\omega} x_{1+\omega^2} x_{\omega^2} x_\omega, \\ x_0 x_{1+\omega+\omega^2} x_{1+\omega^2} x_\omega + x_{\omega+\omega^2} x_1 x_{1+\omega} x_{\omega^2}, \\ x_0 x_{1+\omega^2} x_1 x_{\omega^2} + x_{1+\omega+\omega^2} x_\omega x_{\omega+\omega^2} x_{1+\omega}, \\ x_0 x_1 x_\omega x_{1+\omega} + x_{1+\omega^2} x_{\omega^2} x_{1+\omega+\omega^2} x_{\omega+\omega^2}, \end{cases}$$

et toute fonction symétrique de ces fonctions est invariable par les substitutions (b).

En second lieu considérons la fonction

$$x_0 x_1 + x_\omega x_{1+\omega} + x_{\omega^2} x_{1+\omega^2} + x_{\omega+\omega^2} x_{1+\omega+\omega^2},$$

et faisons sur cette fonction la substitution circulaire $(z, \omega z)$ et ses puissances, nous aurons les sept fonctions suivantes :

$$\begin{cases} x_0 x_1 + x_\omega x_{1+\omega} + x_{\omega^2} x_{1+\omega^2} + x_{\omega+\omega^2} x_{1+\omega+\omega^2}, \\ x_0 x_\omega + x_{\omega^2} x_{\omega+\omega^2} + x_{1+\omega} x_1 + x_{1+\omega+\omega^2} x_{1+\omega^2}, \\ x_0 x_{\omega^2} + x_{1+\omega} x_{1+\omega+\omega^2} + x_{\omega+\omega^2} x_\omega + x_{1+\omega^2} x_1, \\ x_0 x_{1+\omega} + x_{\omega+\omega^2} x_{1+\omega^2} + x_{1+\omega+\omega^2} x_{\omega^2} + x_1 x_\omega, \\ x_0 x_{\omega+\omega^2} + x_{1+\omega+\omega^2} x_1 + x_{1+\omega^2} x_{1+\omega} + x_\omega x_{\omega^2}, \\ x_0 x_{1+\omega+\omega^2} + x_{1+\omega^2} x_\omega + x_1 x_{\omega+\omega^2} + x_{\omega^2} x_{1+\omega}, \\ x_0 x_{1+\omega^2} + x_1 x_{\omega^2} + x_\omega x_{1+\omega+\omega^2} + x_{1+\omega} x_{\omega+\omega^2}; \end{cases}$$

formons une fonction symétrique de ces fonctions, et nous aurons encore une fonction invariable par toutes les substitutions (b).

Actuellement déterminons dans l'expression (b) les coefficients λ_2, λ_1, λ_0; pour cela nous poserons les congruences

$$\left.\begin{aligned} \lambda_2 + \lambda_1 + \lambda_0 &\equiv u_0, \\ \omega^4\lambda_2 + \omega^2\lambda_1 + \omega\lambda_0 &\equiv u_1, \\ \omega\lambda_2 + \omega^4\lambda_1 + \omega^2\lambda_0 &\equiv u_2, \end{aligned}\right\} \quad (\text{mod. } 2).$$

et nous en tirerons

$$\left.\begin{aligned} \lambda_2 &\equiv u_0 + \omega u_1 + (\omega + \omega^2)\, u_2, \\ \lambda_1 &\equiv u_0 + (\omega + \omega^2) u_1 + \omega^2 u_2, \\ \lambda_0 &\equiv u_0 + \omega^2 u_1 + \omega u_2, \end{aligned}\right\} \quad (\text{mod. } 2).$$

Par conséquent les substitutions (b) sont données par l'expression

$$(c) \qquad \left\{\begin{aligned} &\Big[z, (u_0 + \omega u_1 + \omega^4 u_2)\, z^4 + (u_0 + \omega^4 u_1 + \omega^2 u_2)\, z^2 \\ &\qquad + (u_0 + \omega^2 u_1 + \omega u_2)\, z + m\Big], \end{aligned}\right.$$

u_0, u_1, u_2 étant trois quantités différentes entre elles et différentes de zéro et u_2 étant de plus assujetti à n'être pas $\equiv u_0 + u_1$.

Il y a deux fonctions deux fois transitives distinctes de huit quantités qui ont 240 valeurs, et il est remarquable que la fonction de huit quantités qui a 30 valeurs est invariable par les substitutions qui ne changent pas ces deux fonctions.

L'une de ces fonctions deux fois transitives est invariable par les substitutions $\left(z, az^{2^\alpha} + b\right)$, α étant quelconque, et ces substitutions font évidemment partie des substitutions (c).

La seconde de ces fonctions est invariable par les substitutions

$$\left(z, \frac{Az + B}{Cz + D}\right) \quad (\text{mod. } 7),$$

AD — BC étant résidu quadratique et les huit variables étant désignées par x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_∞. D'après un théorème facile à dé-

montrer, toutes ces substitutions sont des dérivées des deux substitutions

$$(e) \qquad (z,\ z+1),$$

$$(f) \qquad \left(z,\ \frac{z}{z+1}\right).$$

Remplaçons donc les variables

$$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_\infty$$

respectivement par

$$x_1, x_\omega, x_{\omega^2}, x_{\omega^3}, x_{\omega^4}, x_{\omega^5}, x_{\omega^6}, x_0,$$

ω étant une racine de $z^7 \equiv 1$, de sorte que nous reprenons nos notations précédentes pour représenter les huit quantités.

La substitution $(z, z+1)$ est remplacée par

$$(\omega^z,\ \omega^{z+1}) \quad \text{ou} \quad (z,\ \omega z);$$

la substitution (f) devient par le même changement de notation, en prenant les exposants suivant le module 7,

$$(x_0\, x_\omega\, x_{\omega^{\frac{1}{2}}}\, x_{\omega^{\frac{1}{3}}}\, x_{\omega^{\frac{1}{4}}}\, x_{\omega^{\frac{1}{5}}}\, x_{\omega^{\frac{1}{6}}})$$

ou

$$(g) \qquad [z,\ (\omega+\omega^2)z^4 + (\omega^2+\omega^4)z^2 + (\omega^4+1)z + \omega\,];$$

donc elle fait partie des substitutions (c) et l'on voit que la fonction qui a 30 valeurs est invariable par toutes les substitutions qui ne changent pas la fonction deux fois transitive considérée.

Quand on a eu le soin d'écrire la substitution (g) tout à fait comme nous venons de le faire, les puissances 2^e, 3^e, ..., 6^e s'obtiennent en remplaçant ω respectivement par $\omega^{\frac{1}{2}} = \omega^4$, $\omega^{\frac{1}{3}} = \omega^5$, $\omega^{\frac{1}{4}} = \omega^2$, $\omega^{\frac{1}{5}} = \omega^3$, $\omega^{\frac{1}{6}} = \omega^6$; de sorte que les puissances de cette substitution sont ren-

fermées dans l'expression

$$[z, (a + a^2) z^4 + (a^2 + a^4) z^2 + (a^4 + 1) z + a]$$

a étant quelconque, excepté zéro.

Etude des substitutions $\left[z, z + a\left(h^{p^{\nu}-1} z^{p^{\nu}-1} + h^{p^{\nu}-2} z^{p^{\nu}-2} + \ldots + hz\right)\right]$.

D'après ce que nous avons reconnu ci-dessus, toutes les substitutions de la forme $\left(z, \lambda_{\nu-1} z^{p^{\nu}-1} + \ldots + \lambda_0 z\right)$ qui s'effectuent sur $p^{\nu} - p^{\nu-1}$ quantités, sont renfermées dans l'expression

$$(a) \qquad \left[z, z + a\left(h^{p^{\nu}-1} z^{p^{\nu}-1} + h^{p^{\nu}-2} z^{p^{\nu}-2} + \ldots + hz\right)\right].$$

Or on peut, au moyen de ces seules substitutions, déterminer le nombre des valeurs de la fonction de $p^{\nu} - 1$ quantités qui est invariable pour toutes les subtitutions

$$(b) \qquad \left(z, \lambda_{\nu-1} z^{p^{\nu}-1} + \lambda_{\nu-2} z^{p^{\nu}-2} + \ldots + \lambda_0 z\right)$$

et par conséquent toutes les substitutions (b) sont des dérivées des substitutions (a); c'est ce que nous allons expliquer. Mais, avant tout, disons comment les substitutions (a) se décomposent en cycles.

Comme nous l'avons déjà dit, on a

$$\begin{aligned} h\left(z^{p^{\nu}} - z\right) \equiv & \left(h^{p^{\nu}-1} z^{p^{\nu}-1} + \ldots + h^p z^p + hz\right) \\ & \times \left(h^{p^{\nu}-1} z^{p^{\nu}-1} + \ldots + hz + 1\right) \\ & \times \left(h^{p^{\nu}-1} z^{p^{\nu}-1} + \ldots + hz + 2\right) \ldots \\ & \times \left(h^{p^{\nu}-1} z^{p^{\nu}-1} + \ldots + hz + p - 1\right), \end{aligned}$$

et par suite toute racine de $z^{p^{\nu}} \equiv z$ satisfait à la congruence

$$h^{p^{\nu}-1} z^{p^{\nu}-1} + h^{p^{\nu}-2} z^{p^{\nu}-2} + \ldots + hz \equiv m \pmod{p},$$

m étant un nombre entier convenablement choisi.

La substitution (a) laisse immobiles les $p^{\nu-1}$ quantités dont les indices satisfont à

$$h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + hz \equiv 0.$$

Posons

$$h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + hz \equiv \psi z,$$

et l'on trouve facilement que la puissance $k^{ième}$ de la substitution (a) est

$$\left(z, z + \frac{[(1+\psi(a)^k - 1]a}{\psi(a)} \psi z\right).$$

Si $\psi(a)$ est $\equiv 0$, la puissance $k^{ième}$ de la substitution (a) se réduit à $(z, z + k\psi z)$, et l'on voit par là que (a) est une substitution régulière de $p^\nu - p^{\nu-1}$ quantités composée de $p^{\nu-1} - p^{\nu-2}$ cycles de p quantités.

Supposons $\psi(a) \equiv m$, m étant un nombre entier qui n'est pas nul, et soit ε le plus petit nombre pour lequel on a

$$[1 + \psi(a)]^\varepsilon \equiv 1;$$

cette congruence pourra toujours être satisfaite si $\psi(a)$ n'est pas $\equiv -1$, et on en conclut que l'expression (a) n'est pas une substitution dans le cas où $\psi(a)$ est $\equiv p-1$, et que si on a $\psi(a) \equiv m$, m étant différent de zéro et de $p-1$, l'expression (a) représente une substitution régulière de $p^\nu - p^{\nu-1}$ variables composée de $\frac{p^\nu - p^{\nu-1}}{\varepsilon}$ cycles de ε variables.

Actuellement soient p^k variables dont les indices satisfont à la congruence

$$(c) \qquad z^{p^k} + l_{k-1} z^{p^{k-1}} + l_{k-2} z^{p^{k-2}} + \ldots + l_0 z \equiv \zeta(z) \equiv 0,$$

et soient x_{z_i} et x_α deux quelconques des $p^\nu - p^k$ variables dont les indices ne satisfont pas à (c), et parmi les substitutions (a) ne considérons que celles qui s'effectuent sur ces $p^\nu - p^k$ variables; nous allons faire voir qu'au moyen de ces substitutions, on peut toujours changer x_{z_i} en x_α.

Toutes les racines de (c) sont racines de $z^{p^\nu} \equiv z$, et par suite si on ajoute aux racines de la congruence (c) une racine d de $z^{p^\nu} \equiv z$, qui n'appartienne pas à (c), la congruence qui en résulte est

$$(g) \qquad \zeta(z) - \zeta(d) \equiv 0,$$

et son premier membre est un diviseur de $z^{p^\nu} - z$; de même si e est une racine de $z^{p^\nu} \equiv z$ qui n'appartient ni à (c), ni à (g),

$$\zeta(z) - \zeta(e)$$

est un diviseur de $z^{p^\nu} - z$. Comme on peut former ainsi successivement des diviseurs de $z^{p^\nu} - z$, on voit que l'on peut poser

$$z^{p^\nu} - z \equiv \zeta(z).[\zeta(z) + m'][\zeta(z) + m'']\dots\left[\zeta(z) + m^{(p^\nu - k - 1)}\right].$$

Alors il arrivera de deux choses l'une : z_1 et α satisferont à deux congruences différentes

$$(h) \qquad \zeta(z) + m' \equiv 0, \quad \zeta(z) + m'' \equiv 0,$$

ou bien z_1 et α satisferont à une seule de ces deux congruences.

Supposons d'abord que z_1 et α satisfassent tous deux à la première congruence (h). Formons les deux congruences

$$(\alpha) \qquad \zeta(z) \equiv 0,$$

$$(\beta) \qquad [\zeta(z) + m'][\zeta(z) + 2m'][\zeta(z) + 3m']\dots[\zeta(z) + (p-1)m'] \equiv 0.$$

Soit β_1 une racine de $z^{p^\nu} - z \equiv 0$, qui n'appartient ni à (α), ni à (β), et formons une congruence qui ait pour racines les racines de (α) augmentées successivement de $0, \beta_1, 2\beta_1, \dots, (p-1)\beta_1$; nous l'écrirons :

$$(\alpha') \qquad \zeta(z)[\zeta(z) + r][\zeta(z) + 2r]\dots[\zeta(z) + (p-1)r] \equiv \theta z \equiv 0.$$

Formons de même une congruence qui ait pour racines les racines

de (β) augmentées successivement de $0, \beta_1, 2\beta_1, \ldots (p-1)\beta_1$; elle sera

$$(\beta') \quad [\theta(z)+s][\theta(z)+2s][\theta(z)+3s]\ldots[\theta(z)+(p-1)s] \equiv 0.$$

Soit β_2 une racine de $z^{p^\nu} \equiv z$ qui n'appartient ni à (α'), ni à (β'), nous formerons de même une congruence (α'') qui ait pour racines les racines de (α') augmentées successivement de $0, \beta_2, 2\beta_2, \ldots, (p-1)\beta_2$,

$$(\alpha'') \qquad z^{p^{k+2}} + q_{k+1} z^{p^{k+1}} + q_k z^{p^k} + \ldots + q_0 z \equiv \lambda(z) \equiv 0,$$

et nous formerons une congruence (β'') qui ait les racines de (β') augmentées de ces mêmes quantités :

$$(\beta'') \qquad [\lambda(z)+t][\lambda(z)+2t]\ldots[\lambda(z)+(p-1)t] \equiv 0.$$

Et en continuant d'agir ainsi, on finira par former les deux congruences

$$(A) \qquad h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + hz \equiv 0,$$

$$(B) \qquad \begin{cases} \left(h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h^p z^p + hz + 1\right) \\ \times \left(h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + hz + 2\right)\ldots \\ \times \left(h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + hz + p - 1\right) \equiv 0, \end{cases}$$

qui seront telles que les indices des p^k variables qui satisfont à la congruence (c) satisferont à (A) et que z_1 et α satisferont à (B).

Supposons ensuite que z_1 et α satisfassent respectivement à la première et à la seconde congruence (h). Dans le cas où m'' est $\equiv rm'$, r étant un entier, nous voyons que les deux congruences (h) sont renfermées dans la congruence (β), et par conséquent la méthode que nous venons d'exposer nous conduira encore aux deux congruences (A) et (B) qui jouiront des mêmes propriétés.

Supposons donc que l'on n'ait pas $m'' \equiv rm'$; formons la congruence :

$$(\alpha_1) \qquad \begin{cases} \zeta(z)[\zeta(z)+m''-m'][\zeta(z)+2(m''-m')]\ldots \\ \times [\zeta(z)+(p-1)(m''-m')] \equiv \theta_1(z) \equiv 0, \end{cases}$$

et ensuite prenons la congruence

$$(\beta_1)\quad \left\{\begin{array}{l} \Pi[\zeta(z)+bm'+c(m''-m')]\equiv[\theta_1(z)+s_1][\theta_1(z)+2s_1]\ldots \\ \times[\theta_1(z)+(p-1)s_1]\equiv 0, \end{array}\right.$$

Π représentant le produit des différents facteurs que l'on obtient en remplaçant b et c par $1, 2, 3, \ldots, p-1$.

Nous pouvons opérer sur les congruences (α_1) et (β_1) comme nous avons opéré précédemment sur les congruences (α') et (β') et nous arriverons encore aux congruences (A) et (B) qui satisferont aux mêmes conditions.

Ainsi, quels que soient z_1 et α, on peut former les congruences (A) et (B) qui sont telles que les p^k racines de (c) satisfont à (A) et que z_1 et α satisfont à (B); par conséquent la substitution

$$(\gamma)\qquad \left[z, z+a\left(h^{p^{\nu-1}}z^{p^{\nu-1}}+h^{p^{\nu-2}}z^{p^{\nu-2}}+\ldots+hz\right)\right]$$

ne permute pas les p^k variables dont les indices satisfont à (c).

Reste à déterminer a de manière que cette subtitution change x_{z_1} en x_α; or il faudra pour cela que l'on ait

$$(k)\qquad z_1+a\left(h^{p^{\nu-1}}z_1^{p^{\nu-1}}+\ldots+h^p z_1^p+hz_1\right)\equiv\alpha.$$

D'ailleurs z_1 et α satisfaisant à la congruence (B), on a

$$h^{p^{\nu-1}}z_1^{p^{\nu-1}}+\ldots+h^p z_1^p+hz_1\equiv r,\quad h^{p^{\nu-1}}\alpha^{p^{\nu-1}}+\ldots+h^p\alpha^p+h\alpha\equiv s,$$

r et s étant des nombres entiers égaux ou inégaux, mais différents de zéro; la congruence (k) donnera donc

$$a\equiv\frac{\alpha-z_1}{r}.$$

Il faut toutefois s'assurer qu'en prenant cette valeur pour a, l'expression (γ) représente bien une substitution, et qu'ainsi l'on n'a pas

$$k^{p^{\nu-1}}a^{p^{\nu-1}}+\ldots+k^p a^p+ka\equiv -1;$$

or, on a

$$h^{p^{\nu-1}} a^{p^{\nu-1}} + \ldots + h^p a^p + ha$$

$$\equiv \frac{h^{p^{\nu-1}}\left(\alpha^{p^{\nu-1}} - z_1^{p^{\nu-1}}\right) + \ldots + h^p\left(\alpha^p - z_1^p\right) + h(\alpha - z_1)}{r} \equiv \frac{s}{r} - 1,$$

quantité différente de -1, puisque s est différent de zéro.

Il est donc démontré que la fraction Ψ, qui est invariable par toutes les substitutions (γ), est transitive par rapport aux $p^\nu - p^k$ variables dont les indices ne satisfont pas à la congruence (c).

Toute substitution dérivée des substitutions (γ) est de la forme

$$(l) \qquad \left(z, z + \mu_{\nu-1} z^{p^{\nu-1}} + \mu_{\nu-2} z^{p^{\nu-2}} + \ldots + \mu z\right);$$

et le plus grand commun diviseur de $\mu_{\nu-1} z^{p^{\nu-1}} + \ldots + \mu z$ et de $z^{p^\nu} - z$ est de la même forme que le premier de ces deux polynômes; donc toute substitution dérivée des substitutions (γ) s'effectue sur $p^\nu - p^\varepsilon$ variables.

Cela posé, formons les congruences :

$$[0] \qquad z \equiv 0,$$

$$[1] \qquad z(z+a)(z+2a)\ldots(z+\overline{p-1}\,a) \equiv z^p - a^{p-1} z \equiv 0,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$z^{p^{\nu-3}} + \ldots + \rho_1 z^p + \rho_0 z \equiv 0,$$

$$[\nu-2] \quad \left\{ \begin{array}{l} \left(z^{p^{\nu-3}} + \ldots + \rho_1 z^p + \rho_0 z\right)\left(z^{p^{\nu-3}} + \ldots + \rho_0 z + l\right)\ldots \\ \times \left(z^{p^{\nu-3}} + \ldots + (p-1)\,l\right) \equiv z^{p^{\nu-2}} + \sigma_{\nu-3} z^{p^{\nu-3}} + \ldots + \sigma z \equiv 0, \end{array} \right.$$

$$[\nu-1] \quad \left\{ \begin{array}{l} \left(z^{p^{\nu-2}} + \ldots + \sigma_1 z^p + \sigma_0 z\right)\left(z^{p^{\nu-2}} + \ldots + \sigma_0 z + m\right)\ldots \\ \times \left(z^{p^{\nu-2}} + \ldots + \sigma_0 z + (p-1)m\right) \\ \equiv z^{p^{\nu-1}} + \tau_{\nu-2} z^{p^{\nu-2}} + \ldots + \tau_0 z \equiv 0, \end{array} \right.$$

dont les premiers membres sont des diviseurs de $z^{p^\nu} - z$, et qui sont telles que chacune contient les racines de la précédente.

Nous voyons que la fonction Ψ est transitive par rapport aux $p^\nu - p^{\nu-1}$ variables dont les indices ne satisfont pas à la congruence $[\nu - 1]$, puis transitive par rapport aux $p^\nu - p^{\nu-2}$ variables dont les indices ne satisfont pas à la congruence $[\nu - 2]$, etc., enfin transitive par rapport aux $p^\nu - 1$ variables autres que x_0; d'où l'on déduit facilement que le nombre des valeurs de Ψ est

$$\frac{1.2.3\ldots(p^\nu-1)}{(p^\nu-p^{\nu-1})(p^\nu-p^{\nu-2})\ldots(p^\nu-p)(p^\nu-1)},$$

et par suite toutes les subtitutions

$$\left(z, \lambda_{\nu-1} z^{p^{\nu-1}} + \lambda_{\nu-2} z^{p^{\nu-2}} + \ldots \lambda_0 z\right)$$

sont des dérivées des substitutions

$$(\gamma) \qquad \left[z,\ z + a\left(h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h^p z^p + hz\right)\right].$$

Si dans l'expression (γ) on change h en he, e étant un nombre entier, le polynôme $h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + hz$ est seulement multiplié par e; donc si on donne une valeur η à h, on pourra se dispenser de donner à h les valeurs 2η, $3\eta, \ldots, (p-1)\eta$. D'après cela, pour avoir toutes les substitutions (γ), on donnera à h $\frac{p^\nu-1}{p-1}$ valeurs, puis on donnera à la lettre a toutes les valeurs autres que zéro et que celles qui satisfont à

$$h^{p^{\nu-1}} a^{p^{\nu-1}} + h^{p^{\nu-2}} a^{p^{\nu-2}} + \ldots + ha \equiv -1;$$

donc pour chaque valeur de h, on a $p^\nu - p^{\nu-1} - 1$ valeurs de a, et le nombre des substitutions (γ) est $\frac{(p^\nu-1)(p^\nu-p^{\nu-1}-1)}{p-1}$.

Enfin nous terminerons cet article en faisant remarquer que la substitution

$$\left(z,\ z + a\left(h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h^p z^p + hz\right) + b\right)$$

est semblable aux substitutions (γ), si $\frac{b}{a}$ est racine de $z^p \equiv z$, et que, dans le cas contraire, la substitution s'effectue sur toutes les variables.

Des fonctions de $p^{\eta\tau}$ variables qui ne sont pas changées par les substitutions $\left(z, \mathrm{A}z^{p^{\eta(\tau-1)}} + \mathrm{B}z^{p^{\eta(\tau-2}} + \ldots + \mathrm{H}z + \mathrm{L}\right)$.

Tout ce que nous avons établi pour les fonctions de p^ν quantités qui ne sont pas changées par les substitutions

$$\left(z, \mathrm{A}z^{p^{\nu-1}} + \mathrm{B}z^{p^{\nu-2}} + \ldots + \mathrm{H}z + \mathrm{L}\right),$$

peut être étendu par des raisonnements tout semblables, aux fonctions de $p^{\eta\tau}$ quantités qui sont invariables par les substitutions

$$(\eta) \qquad \left(z, \mathrm{A}z^{p^{\eta(\tau-1)}} + \mathrm{B}z^{p^{\eta(\tau-2)}} + \ldots + \mathrm{I}z^{p^\eta} + \mathrm{H}z + \mathrm{L}\right).$$

Désignons par $0, a_1, a_2, \ldots, a_{p^\eta-1}$ les racines de la congruence

$$z^{p^\eta} - z \equiv 0,$$

dont le premier membre est un diviseur de $z^{p^{\eta\tau}} - z$, nous aurons la congruence

$$\begin{aligned} h\left(z^{p^{\eta\tau}} - z\right) \equiv & \left(h^{p^{\eta(\tau-1)}} z^{p^{\eta(\tau-1)}} + h^{p^{\eta(\tau-2)}} z^{p^{\eta(\tau-2)}} + \ldots + h^{p^\eta} z^{p^\eta} + hz\right) \\ & \times \left(h^{p^{\eta(\tau-1)}} z^{p^{\eta(\tau-1)}} + \ldots + h^{p^\eta} z^{p^\eta} + hz + a_1\right) \\ & \times \left(h^{p^{\eta(\tau-1)}} z^{p^{\eta(\tau-1)}} + \ldots + hz + a_2\right) \ldots \\ & \times \left(h^{p^{\eta(\tau-1)}} z^{p^{\eta(\tau-1)}} + \ldots + hz + a_{p^\eta-1}\right). \end{aligned}$$

Soient $\alpha^{1,1}, \alpha^{1,2}, \alpha^{1,3}, \ldots, \alpha^{1,p^{\eta(\tau-1)}}$ les racines de $z^{p^{\eta\tau}} \equiv z$ dues au premier facteur; $\alpha^{2,1}, \alpha^{2,2}, \alpha^{2,3}, \ldots, \alpha^{2,p^{\eta(\tau-1)}}$ les racines de $z^{p^{\eta\tau}} \equiv z$ dues au second; $\alpha^{3,1}, \alpha^{3,2}, \ldots, \alpha^{3,p^{\eta(\tau-1)}}$ celles qui sont dues au troi-

sième, et ainsi de suite. Prenons la fonction

$$x_{\alpha^1,1}\,x_{\alpha^1,2}\cdots x_{\alpha^1,p^{\eta(\tau-1)}} + x_{\alpha^2,1}\,x_{\alpha^2,2}\cdots x_{\alpha^2,p^{\eta(\tau-1)}} + x_{\alpha^3,1}\,x_{\alpha^3,2}\cdots x_{\alpha^3,p^{\eta(\tau-1)}} + \ldots;$$

soit ω une racine primitive de $z^{p^{\eta\tau}} \equiv z$; faisons sur cette fonction les $\frac{p^{\eta\tau}-p^{\eta}}{p^{\eta}-1}$ premières puissances de $(z, \omega z)$, et formons une fonction symétrique des $\frac{p^{\eta\tau}-1}{p^{\eta}-1}$ fonctions ainsi obtenues; nous aurons ainsi une fonction invariable par les substitutions (η).

Désignons par $0, b_1, b_2, \ldots b_{p^{\eta(\tau-1)}}$ les racines de la congruence

$$z^{p^{\eta(\tau-1)}} + z^{p^{\eta(\tau-2)}} + \ldots + z^{p^{\eta}} + z \equiv 0,$$

nous aurons la congruence identique

$$\lambda\left(z^{p^{\eta\tau}} - z\right) \equiv \left(\lambda^{p^{\eta}} z^{p^{\eta}} - \lambda z\right)\left(\lambda^{p^{\eta}} z^{p^{\eta}} - \lambda z - b_1\right)\left(\lambda^{p^{\eta}} z^{p^{\eta}} - \lambda z - b_2\right)\ldots \times \left(\lambda^{p^{\eta}} z^{p^{\eta}} - \lambda z - b_{p^{\eta(\tau-1)}-1}\right).$$

Soient $\alpha_1, \alpha_2, \ldots, \alpha_{p^{\eta}}$ les racines de $z^{p^{\eta\tau}} \equiv z$ dues au premier facteur, soient $\beta_1, \beta_2, \ldots, \beta_{p^{\eta}}$ les racines qui sont dues au second, $\gamma_1, \gamma_2, \ldots, \gamma_{p^{\eta}}$ celles qui sont dues au troisième et ainsi de suite. Faisons sur la fonction

$$\varphi = x_{\alpha_1}\,x_{\alpha_2}\cdots x_{\alpha_{p^{\eta}}} + x_{\beta_1}\,x_{\beta_2}\cdots x_{\beta_{p^{\eta}}} + x_{\gamma_1}\,x_{\gamma_2}\cdots x_{\gamma_{p^{\eta}}} + \ldots$$

les $\frac{p^{\eta\tau}-p^{\eta}}{p^{\eta}-1}$ premières puissances de $(z, \omega z)$, ω étant racine primitive de $z^{p^{\nu}} \equiv z$, nous aurons ainsi $\frac{p^{\eta\tau}-p^{\eta}}{p^{\eta}-1}$ fonctions; ajoutons-y la fonction φ; enfin formons une fonction symétrique de ces fonctions, et nous aurons encore une fonction invariable par les substitutions (η).

Le nombre des substitutions (η) est égal à

$$p^{\eta\tau}\left(p^{\eta\tau}-1\right)\left(p^{\eta\tau}-p^{\eta}\right)\left(p^{\eta\tau}-p^{2\eta}\right)\cdots\left(p^{\eta\tau}-p^{\eta(\tau-1)}\right),$$

et par conséquent le nombre des valeurs de la fonction de $p^{n\tau}$ quantités qui n'est pas changée par ces substitutions est

$$\frac{1.2.3\ldots(p^{n\tau}-1)}{(p^{n\tau}-p^{n(\tau-1)})(p^{n\tau}-p^{n(\tau-2)})\ldots(p^{n\tau}-p^{n})(p^{n\tau}-1)}.$$

Si on désigne par Ω une racine d'une congruence du degré τ, dont les coefficients sont racines de $z^{p^n}\equiv z$, et dont le premier membre n'a aucun facteur commun avec $z^{p^n}-z$, toutes les racines de $z^{p^{n\tau}}\equiv z$, lesquelles sont les indices de nos $p^{n\tau}$ variables, sont renfermées dans l'expression

$$(\mu)\qquad A_0+A_1\Omega+A_2\Omega^2+\ldots+A_{\tau-1}\Omega^{\tau-1},$$

$A_0, A_1, A_2,\ldots, A_{\tau-1}$ étant racines de la congruence $z^{p^n}\equiv z$.

Si on désigne ensuite par $\nu_0, \nu_1,\ldots, \nu_{\tau-1}$ les valeurs en lesquelles les indices $1, \Omega, \Omega^2,\ldots, \Omega^{\tau-1}$ sont changés par la substitution

$$(m)\qquad \left(z, \lambda_{\tau-1}z^{p^{n(\tau-1)}}+\lambda_{\tau-2}z^{p^{n(\tau-2)}}+\ldots\lambda_1 z^{p^n}+\lambda_0 z\right),$$

nous aurons les congruences

$$\lambda_{\tau-1}+\lambda_{\tau-2}+\lambda_{\tau-3}+\ldots+\lambda_1+\lambda_0\equiv\nu_0,$$
$$\Omega^{p^{n(\tau-1)}}\lambda_{\tau-1}+\Omega^{p^{n(\tau-2}}\lambda_{\tau-2}+\Omega^{p^{n(\tau-3)}}\lambda_{\tau-3}+\ldots+\Omega^{p^n}\lambda_1+\Omega\lambda_0\equiv\nu_1,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\Omega^{(\tau-1)p^{n(\tau-1)}}\lambda_{\tau-1}+\Omega^{(\tau-1)p^{n(\tau-2)}}\lambda_{\tau-2}+\ldots+\Omega^{\tau-1}\lambda_0\equiv\nu_{\tau-1},$$

et l'indice en lequel sera changé l'indice (μ) sera donné par l'expression

$$A_0\nu_0+A_1\nu_1+\ldots+A_{\tau-1}\nu_{\tau-1}.$$

Ainsi pour que l'expression (m) représente une substitution, il faut que $\nu_0, \nu_1,\ldots, \nu_{\tau-1}$ soient tels, que l'on n'ait pas

$$\nu_k=\alpha_0\nu_0+\alpha_1\nu_1+\ldots+\alpha_{k-1}\nu_{k-1},$$

$\alpha_0, \alpha_1,\ldots, \alpha_{k-1}$ étant des racines de la congruence $z^{p^n}\equiv z$.

Soient $\Omega_0, \Omega_1, \ldots, \Omega_{\tau-1}$ τ racines de la congruence $z^{p^{\eta\tau}} \equiv z$ telles, que l'on n'ait pas $\Omega_k \equiv \alpha_0\Omega_0 + \alpha_1\Omega_1 + \ldots + \alpha_{k-1}\Omega_{k-1}$, $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}$ étant racines de $z^{p^\eta} \equiv z$; la fonction de $p^{\eta\tau}$ variables qui n'est pas changée par toutes les substitutions (η) est transitive par rapport aux $p^{\eta\tau} - 1$ variables autres que x_0, puis transitive par rapport aux $p^{\eta\tau} - p^\eta$ variables qui ne sont pas de la forme $x_{\alpha_0\Omega_0}$, puis transitive par rapport aux $p^{\eta\tau} - p^{2\eta}$ variables qui ne sont pas de la forme $x_{\alpha_0\Omega_0+\alpha_1\Omega_1}$, et ainsi de suite.

Toutes les substitutions (η) sont des dérivées des substitutions

$$\left[z,\ z + a\left(h^{p^{\eta(\tau-1)}} z^{p^{\eta(\tau-1)}} + h^{p^{\eta(\tau-2)}} z^{p^{\eta(\tau-2)}} + \ldots + h^{p^\eta} z^{p^\eta} + hz\right)\right]$$

qui s'effectuent sur $p^{\eta\tau} - p^{\eta(\tau-1)}$ variables.

CHAPITRE IV.

DES FONCTIONS TRANSITIVES D'UN NOMBRE PREMIER DE QUANTITÉS.

Nous commencerons l'étude de ces fonctions par un théorème qui est fondamental, et que nous avons reconnu aussitôt que nous nous sommes occupé du sujet de ce Mémoire, mais dont la démonstration, quoique assez simple, nous a longtemps échappé. Cette proposition est celle-ci :

THÉORÈME. — *Une fonction transitive d'un nombre premier de quantités est nécessairement invariable par une certaine substitution circulaire effectuée sur toutes les quantités.*

Pour démontrer ce théorème, nous établirons d'abord ce lemme :

Soient $a, b, c, \ldots, k, l$, les p quantités, et supposons que K soit le nombre des substitutions effectuées sur $p - r$ lettres qui laissent l immobile, et qui laissent la fonction F considérée invariable; F est invariable par $\frac{Kp}{r}$ substitutions effectuées sur $p - r$ lettres.

En effet, considérons $p - 1$ lettres quelconques de la fonction tran-

sitive F; il y a sur ces $p-1$ lettres K substitutions de $p-r$ lettres, qui laissent F invariable. Faisons la somme des substitutions de $p-r$ lettres que l'on a pour chaque arrangement de $p-1$ lettres, nous aurons ainsi Kp substitutions de $p-r$ lettres; mais il est aisé de voir que chaque substitution se trouve répétée r fois, de sorte qu'il n'y a que $\frac{Kp}{r}$ substitutions de $p-r$ lettres qui ne changent pas la fonction transitive F. En effet, si en considérant les $p-1$ lettres $a, b, \ldots, e, f, \ldots, i, k$, on a une substitution faite sur les $p-r$ lettres $a, b, \ldots, e$, on a pareillement cette substitution de $p-r$ lettres en considérant les $p-1$ lettres $a, b, \ldots, e, f, \ldots, i, l$, et en général on a cette substitution dans tous les groupes de $p-1$ lettres, que l'on obtient en prenant les $p-r$ lettres $a, b, \ldots, e$ avec $r-1$ des lettres restantes. Donc dans les Kp substitutions ci-dessus obtenues, la substitution que nous venons de considérer sur les $p-r$ lettres $a, b, \ldots, e$ se trouve répétée autant de fois que l'on peut combiner r quantités $r-1$ à $r-1$, c'est-à-dire r fois, et notre lemme est démontré.

Démontrons ensuite cet autre principe : S'il existe une substitution S de p lettres non circulaire qui laisse invariable la fonction F, le nombre des substitutions semblables à S et qui laissent F invariable, est divisible par p.

Soit β le nombre des lettres d'un certain cycle de S; prenons la puissance $\beta^{ième}$ de cette substitution, nous aurons pour cette puissance une certaine substitution A.

A étant ainsi défini, soit g une des lettres qui ne se trouvent pas dans A, et désignons par

$$(\alpha) \qquad A, A', A'', \ldots, A^{(\nu-1)},$$

les ν substitutions semblables à A, et qui ne contiennent pas g.

Considérons $p-1$ lettres de la fonction F, qui ne comprennent pas la lettre h autre que g; il y aura sur ces $p-1$ lettres ν substitutions

$$(\beta) \qquad A_1, A'_1, A''_1, \ldots, A_1^{(\nu-1)}$$

semblables à A, et qui ne différeront des substitutions (α) que par la

manière de désigner les variables; ainsi on passera des substitutions (α) aux substitutions (β) en faisant sur les variables une même substitution.

Considérons de même les $p-1$ lettres autres que i, i étant différent de g et de h, et ainsi de suite. Nous aurons en définitive les νp substitutions

$$(\gamma)\quad \begin{cases} A, & A', & A'', \ldots, & A^{(\nu-1)}, \\ A_1, & A'_1, & A''_1, \ldots, & A_1^{(\nu-1)}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ A_{p-1}, & A'_{p-1}, & A''_{p-1}, \ldots, & A_{p-1}^{(\nu-1)}, \end{cases}$$

parmi lesquelles il n'y en a que $\frac{\nu}{r}p$ qui soient distinctes, $p-r$ étant le nombre des lettres permutées par A. On passera des substitutions d'une ligne horizontale du groupe (γ) à celles d'une autre ligne en faisant une même substitution sur les variables des substitutions de la première de ces deux lignes.

Supposons maintenant que S, $S^{(1)}$, $S^{(2)}, \ldots, S^{(i-1)}$ soient toutes les substitutions semblables à S qui ont A pour puissance $\beta^{ième}$, et qui laissent F invariable. Désignons ensuite par $R^{(0)}$, $R^{(1)}, \ldots, R^{(s-1)}$ toutes les substitutions semblables à S qui ont A′ pour puissance $\beta^{ième}$, etc., enfin par $L^{(0)}$, $L^{(1)}, \ldots, L^{(t-1)}$ toutes les substitutions semblables à S qui ont $A^{(\nu-1)}$ pour puissance $\beta^{ième}$. Nous aurons ainsi les μ substitutions

$$(\delta)\quad S, S^{(1)}, S^{(2)}, \ldots, S^{(i-1)}, R^{(0)}, R^{(1)}, \ldots, R^{(s-1)}, \ldots, L^{(0)}, L^{(1)}, \ldots, L^{(t-1)},$$

qui sont toutes différentes; par exemple les substitutions $R^{(0)}$, $R^{(1)}, \ldots,$ $R^{(s-1)}$ sont différentes entre elles, et elles sont différentes de S, $S^{(1)}, \ldots,$ $S^{(i-1)}$, puisqu'elles ont une puissance $\beta^{ième}$ différente.

Nous observons alors que tout ce qui a lieu pour les substitutions

$$A, A', A'', \ldots, A^{(\nu-1)},$$

a lieu identiquement, et pour les substitutions

$$A_1, A'_1, A''_1, \ldots, A_1^{(\nu-1)},$$

et pour les substitutions

$$A_2,\ A'_2,\ A''_2,\ \ldots,\ A_2^{(\nu-1)},$$

etc. Ainsi il y a μ substitutions

$$(\varepsilon)\quad S_1^{(0)},\ S_1^{(1)},\ S_1^{(2)},\ \ldots,\ S_1^{(i-1)},\ R_1^{(0)},\ R_1^{(1)},\ \ldots,\ R_1^{(s-1)},\ \ldots,\ L_1^{(0)},\ L_1^{(1)},\ \ldots,\ L_1^{(t-1)},$$

différentes entre elles, et qui ont pour puissance $\beta^{ième}$ les i premières A_1,, les s suivantes A'_1, etc., les t dernières $A_1^{(\nu-1)}$. Il y a μ substitutions

$$(\zeta)\quad S_2^{(0)},\ S_2^{(1)},\ S_2^{(2)},\ \ldots,\ S_2^{(i-1)},\ R_2^{(0)},\ R_2^{(1)},\ \ldots,\ R_2^{(s-1)},\ \ldots,\ L_2^{(0)},\ L_2^{(1)},\ \ldots,\ L_2^{(t-1)},$$

différentes entre elles, et qui ont pour puissance $\beta^{ième}$ les i premières A_2, les s suivantes A'_2, etc., les t dernières $A_2^{(\nu-1)}$. Et ainsi de suite.

On passe des substitutions (δ) aux substitutions (ε), puis aux substitutions (ζ), etc., en faisant sur les variables les substitutions au moyen desquelles on passe de la première ligne horizontale des substitutions (γ) à la seconde, puis à la troisième, etc.

Actuellement les substitutions (γ) étant identiques r à r, les μp substitutions (δ), (ε), (ζ), etc., sont aussi identiques r à r; le nombre de ces substitutions qui sont distinctes est donc $\frac{\mu p}{r}$, et puisque r est $< p$, ce nombre est divisible par p.

D'ailleurs il n'y a pas d'autres substitutions que les substitutions (δ), (ε), (ζ), etc., qui soient semblables à S et qui laissent F invariable. Notre principe est donc démontré.

Cela posé, considérons toutes les substitutions qui ne comprennent pas une certaine lettre g, et qui laissent F invariable, et soient K_1 le nombre de celles qui s'effectuent sur $p - r_1$ lettres, K_2 le nombre de celles qui s'effectuent sur $p - r_2$ lettres, etc. Désignons enfin par rp le nombre des substitutions qui laissent F invariable; le nombre des substitutions qui s'effectuent sur toutes les lettres, est

$$rp - p\left(\frac{K_1}{r_1} + \frac{K_2}{r_2} + \ldots + \frac{K_i}{r_i}\right) - 1;$$

c'est donc un nombre non divisible par p; car $\frac{K_1}{r_1}, \frac{K_2}{r_2}$, etc., sont des nombres entiers. Il est donc nécessaire que quelques-unes de ces substitutions soient circulaires.

COROLLAIRE. — *Le nombre des substitutions circulaires distinctes de p lettres qui laissent invariable une fonction transitive de p lettres est de la forme* $\alpha p + 1$.

En effet, si l'on désigne par x le nombre des substitutions circulaires distinctes de p lettres, et par py le nombre de toutes les substitutions non circulaires de p lettres, on a

$$(p-1)x + py = rp - p\left(\frac{K_1}{r_1} + \frac{K_2}{r_2} + \ldots + \frac{K_i}{r_i}\right) - 1,$$

d'où

$$x = \alpha p + 1.$$

Le raisonnement précédent conduit également à ce théorème :

Une fonction transitive dont le nombre des lettres est une puissance d'un nombre premier, est invariable par quelque substitution régulière effectuée sur toutes ses lettres.

D'après cela, étant donnée une fonction transitive d'un nombre premier p de quantités, nous désignerons ces p quantités par x_0, x_1, $x_2, \ldots, x_{p-1}$, et supposerons que cette fonction est invariable par la substitution

$$(x_0 x_1 x_2 \ldots x_{p-1})$$

ou $(z, z+1)$ en convenant que $x_a = x_e$, si l'on a $a \equiv e \pmod{p}$.

Il est facile de démontrer que *si une fonction transitive de p quantités n'est invariable que par des substitutions effectuées sur p et sur* $p-1$ *quantités, toutes ces substitutions sont données par l'expression*

$$(\alpha) \qquad (z, a^u z + b),$$

u étant un diviseur de $p-1$.

On voit d'abord que si l'on désigne par αp le nombre total des

substitutions, le nombre des substitutions de p quantités est $\alpha p - 1 - p(\alpha - 1) = p - 1$, de sorte qu'elles sont toutes comprises dans l'expression $(z, z + m)$.

Soit $(z, \theta_r z)$ une quelconque des substitutions effectuées sur x_1, $x_2, \ldots, x_{p-1}$; $[\theta_r z, \theta_r(z + m)]$ est une substitution semblable à $(z, z + m)$, puisqu'on l'obtient en faisant sur les variables de $(z, z + m)$ la substitution $(z, \theta_r z)$; désignons par $\theta'_r z$ la fonction inverse de $\theta_r z$, cette substitution pourra s'écrire $[z, \theta_r(\theta'_r z + m)]$; or cette substitution laisse la fonction considérée invariable, elle est donc identique à une des substitutions $(z, z + n)$ et on aura

$$\theta_r(\theta'_r z + m) \equiv z + n \pmod{p},$$

d'où

$$\theta'_r(z + n) \equiv \theta'_r z + m.$$

De cette congruence, on tire

$$\theta'_r(z + 2n) \equiv \theta'_r(z + n) + m \equiv \theta'_r z + 2m,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\theta'_r(z + kn) \equiv \theta'_r z + km.$$

Faisons $z = 0$, nous aurons, k étant quelconque,

$$\theta'_r(kn) \equiv \theta'_r 0 + km;$$

$\theta'_r 0$ est nul; on a donc, en remplaçant kn par z,

$$\theta'_r z \equiv \frac{m}{n} z,$$

et par conséquent toutes les substitutions qui laissent la fonction considérée invariable, sont comprises dans la formule (α).

On voit aussi par cette démonstration que si une fonction transitive de p quantités n'est invariable que par une seule substitution circulaire de p quantités, toutes les substitutions qui la laissent invariable sont les substitutions (α).

Or le nombre des substitutions circulaires qui laissent une fonction transitive de p lettres invariable est de la forme $\alpha p + 1$; donc si une fonction transitive de p quantités est invariable par d'autres substitutions que les substitutions (α), elle est invariable par au moins $p + 1$ substitutions circulaires.

THÉORÈME. — *Une fonction transitive F de p quantités est invariable par toutes les substitutions* $(z, a^u z + b)$, *a et b étant quelconques et u un certain diviseur de* $p - 1$ *plus petit que* $p - 1$, *et même plus petit que* $\frac{p-1}{2}$ *si p est de la forme* $4n - 1$. *Le nombre des substitutions circulaires de p quantités qui laissent cette fonction invariable est au moins égal à* $\frac{ru}{p-1}$, *r étant le nombre des substitutions qui, effectuées sur* $x_1, x_2, \ldots, x_{p-1}$, *laissent cette fonction invariable.*

La fonction F est supposée invariable par la substitution $(z, z + 1)$ et soient ensuite

$$(1) \qquad (z, z), \quad (z, \theta_1 z), (z, \theta_2 z), \ldots, \quad (z, \theta_{r-1} z)$$

les substitutions qui ne permutent que $x_1, x_2, \ldots, x_{p-1}$ et qui laissent la fonction F invariable.

Les substitutions $[\theta_s z, \theta_s(z + m)]$ ou $[z, \theta_s(\theta'_s z + m)]$ sont des substitutions circulaires, qui sont les puissances de $[z, \theta_s(\theta'_s z + 1)]$. Or, le nombre total des substitutions qui laissent F invariable est rp ; donc, en faisant dans l'expression $[z, \theta_s(\theta'_s z + m)]$ $s = 0, 1, 2, \ldots, r - 1$, on n'obtiendra pas toutes des substitutions circulaires différentes, puisque, si elles étaient toutes différentes, on aurait $r(p - 1)$ substitutions circulaires de p variables, et par conséquent le nombre de toutes les substitutions qui ont moins de p variables serait au plus égal à r, ce qui est absurde ; donc il y aura nécessairement deux substitutions telles que $[z, \theta_s(\theta'_s z + m)]$ et $[z, \theta_\nu(\theta'_\nu z + n)]$ qui seront identiques : ce qui donnera

$$\theta_s(\theta'_s z + m) \equiv \theta_\nu(\theta'_\nu z + n) \pmod{p}.$$

Changeons z en $\theta_\nu z$, et nous aurons

$$\theta_s(\theta'_s\theta_\nu z + m) \equiv \theta_\nu(z+n),$$

$$\theta'_s\theta_\nu z + m \equiv \theta'_s\theta_\nu(z+n).$$

Posons

$$\theta'_s\theta_\nu z \equiv \theta_t z, \tag{2}$$

et nous obtiendrons

$$\theta_t(z+n) \equiv \theta_t z + m,$$

ce qui donne

$$\theta_t z \equiv cz, \tag{3}$$

et il est prouvé que les substitutions (1) contiennent toutes les substitutions $(z, a^u z)$, u étant un diviseur de $p-1$.

Démontrons ensuite que si p est de la forme $4n-1$, u est plus petit que $\frac{p-1}{2}$, si la fonction est invariable par d'autres substitutions que les substitutions $\left[z, (\pm 1)^{\frac{p-1}{2}} z + b\right]$.

En effet, supposons cette fonction de p quantités invariable par les substitutions $(z, \pm z + b)$, et par d'autres qui ne soient pas de la forme $(z, az+b)$. Multiplions cette fonction par la fonction des mêmes quantités qui a deux valeurs, laquelle est changée par la substitution $(z, -z)$, et nous obtiendrons une fonction transitive de p quantités qui ne serait invariable par aucune des substitutions (z, az), ce qui est impossible.

On voit en particulier que si $\frac{p-1}{2}$ *est un nombre premier, une fonction transitive de p quantités qui n'est pas la fonction invariable par les seules substitutions* $(z, \pm z + b)$, *est invariable par toutes les substitutions* $(z, a^2 z + b)$.

Pour achever la démonstration de notre théorème, supposons qu'il y ait e des expressions $\theta(\theta' z + m)$, qui puissent servir à représenter une

même substitution circulaire, de sorte que l'on ait

$$(4)\qquad \begin{cases} \theta_s(\theta'_s z+n)\equiv\theta_{s_1}(\theta'_{s_1}z+n_1)\equiv\theta_{s_2}(\theta'_{s_2}z+n_2)\equiv\dots \\ \qquad\qquad \equiv\theta_{s_{e-1}}\left(\theta'_{s_{e-1}}z+n_{e-1}\right); \end{cases}$$

de la première de ces congruences on tire, en changeant z en $\theta'_k z$ inverse de $\theta_k z$,

$$\theta_s(\theta'_s\,\theta'_k z+n)\equiv\theta_{s_1}(\theta'_{s_1}\theta'_k z+n_1),$$

et

$$\theta_k\theta_s(\theta'_s\,\theta'_k z+n)\equiv\theta_k\theta_{s_1}(\theta'_{s_1}\theta'_k z+n_1);$$

donc on aura

$$\theta_k\theta_s(\theta'_s\,\theta'_k z+n)\equiv\theta_k\theta_{s_1}(\theta'_{s_1}\theta'_k z+n_1)\equiv\dots\equiv\theta_k\theta_{s_{e-1}}\left(\theta'_{s_{e-1}}\theta'_k z+n_{e-1}\right);$$

$\theta'_s\,\theta'_k z$ est l'inverse de $\theta_k\theta_s z$; donc toutes les expressions $\theta(\theta' z+m)$ sont égales e à e. D'après les congruences (2) et (3), on aura

$$\theta'_s\,\theta_{s_1}z\equiv c_1 z,\quad \theta'_s\,\theta_{s_2}z\equiv c_2 z,\dots,\quad \theta'_s\,\theta_{s_{e-1}}z\equiv c_{e-1}z,$$

et par conséquent il y a e substitutions de la forme (z, cz), qui laissent la fonction invariable, et il n'y en a pas davantage; car s'il y en avait plus, on pourrait poser $\theta'_s\theta_g z\equiv dz$, θ_g étant différent de θ_{s_1}, θ_{s_2},…, $\theta_{s_{e-1}}$, et on aurait à ajouter aux e termes (4) congrus entre eux le terme $\theta_g(\theta'_g z+q)$; donc ces e substitutions ne sont pas autres que les substitutions $(z, a^u z)$, et on a $e=\frac{p-1}{u}$.

Les r expressions $\theta_s(\theta'_s z+1)$ peuvent donc être groupées e à e, de manière à être identiques ou puissances l'une de l'autre; donc le nombre des substitutions circulaires distinctes renfermées dans l'expression $[z, \theta(\theta' z+1)]$ est $\frac{r}{e}$ ou $\frac{ru}{p-1}$. Comme toutefois nous n'avons pas démontré que toutes les substitutions circulaires qui laissent la fonction invariable sont de la forme $[z, \theta(\theta' z+m)]$, il faudrait bien se

garder de croire que le nombre de ces substitutions circulaires est égal à $\frac{ru}{p-1}$, mais seulement qu'il est au moins égal à $\frac{ru}{p-1}$.

D'après ce que nous venons de voir, les substitutions (1) qui s'effectuent sur $x_1, x_2, \ldots, x_{p-1}$ peuvent s'écrire

$$(\varepsilon) \qquad (z, a^u z), \quad (z, a^u \theta_1 z), \quad (z, a^u \theta_2 z), \ldots, \quad (z, a^u \theta_{r'-1} z).$$

Si u est impair, en multipliant la fonction invariable par les substitutions (ε) par la fonction qui a deux valeurs, on aura une fonction qui ne sera invariable que par les substitutions $(z, a^u z)$ pour lesquelles a est résidu quadratique, et comme le nombre des substitutions qui la laissent invariable doit devenir deux fois moindre, ce sont

$$(z, a^{2u} z), \quad (z, a^{2u} \theta_1 z), \quad (z, a^{2u} \theta_2 z), \ldots, \quad (z, a^{2u} \theta_{r'-1} z);$$

on voit donc aussi que les substitutions

$$(z, \theta_1 z), \quad (z, \theta_2 z), \ldots, \quad (z, \theta_{r'-1} z)$$

laissent invariable la fonction qui a deux valeurs.

Supposons une fonction de $p+1$ variables qui ne soit pas changée par toutes les substitutions $\left(z, \frac{Az+B}{Cz+D}\right)$ pour lesquelles $(AD-BC)$ est résidu quadratique, ni par les substitutions (1); $(z, a^2 z)$ figure donc parmi ces dernières substitutions. La substitution $\left\{ z, \frac{(-1)^{\frac{p-1}{2}}}{\theta_r\left[\frac{(-1)^{\frac{p-1}{2}}}{z}\right]} \right\}$ laisse cette fonction invariable et ne permute ni x_0, ni x_∞; c'est donc une des substitutions (1), et on a

$$\frac{(-1)^{\frac{p-1}{2}}}{\theta_r\left[\frac{(-1)^{\frac{p-1}{2}}}{z}\right]} = \theta_u z,$$

d'où

$$(g) \qquad \theta_u z\,\theta_v\left[\frac{(-1)^{\frac{p-1}{2}}}{z}\right]\equiv(-1)^{\frac{p-1}{2}}.$$

Il est ensuite aisé de démontrer que si l'on a $\theta_t(z+m)\equiv\theta_g z+n$, quel que soit t, et que si toutes les substitutions (1) sont assujetties à la congruence (g), il existe une fonction deux fois transitive de $p+1$ quantités invariable par les substitutions (1) et par les substitutions $\left(z, \frac{Az+B}{Cz+D}\right)$ pour lesquelles AD — BC est résidu quadratique, et si l'on écrit les substitutions (1)

$$(z, a^2 z), \quad (z, a^2\theta_1 z), \quad (z, a^2\theta_2 z),\ldots, \quad (z, a^2\theta_{\varepsilon-1} z),$$

ε étant égal à $\frac{2r}{p-1}$, toutes les substitutions qui laissent cette fonction invariable sont données par l'expression

$$\left(z, \frac{A\theta_s z+B}{C\theta_s z+D}\right),$$

AD — BC étant résidu quadratique (et $s<\varepsilon$).

THÉORÈME. — *Soit une fonction transitive d'un nombre premier p de lettres, dont toutes les substitutions s'effectuant sur p lettres sont circulaires; si elle est invariable par des substitutions qui changent la fonction qui a deux valeurs, toutes ces substitutions s'effectuent sur* $p-1$ *lettres.*

Supposons en effet une fonction F de p lettres, dont toutes les substitutions de p lettres soient circulaires, et qui soit invariable par des substitutions qui changent la fonction des mêmes lettres, qui a deux valeurs.

Considérons les substitutions qui ne contiennent pas x_0 et qui laissent F invariable. Soient K_1 le nombre de ces substitutions effectuées sur $p-r_1$ lettres, K_2 le nombre de ces substitutions effectuées sur $p-r_2$ lettres, etc. Le nombre des substitutions de moins de p lettres

qui laissent F invariable est

$$\frac{K_1 p}{r_1} + \frac{K_2 p}{r_2} + \ldots + \frac{K_i p}{r_i} + 1,$$

et l'on a, en désignant par rp le nombre des substitutions qui laissent F invariable,

$$(\alpha) \qquad r = K_1 + K_2 + \ldots + K_i + 1;$$

donc le nombre des substitutions de p lettres qui, par hypothèse, sont toutes circulaires, est

$$rp - \left(\frac{K_1 p}{r_1} + \frac{K_2 p}{r_2} + \ldots + \frac{K_i p}{r_i} + 1\right).$$

Multiplions la fonction F par la fonction des mêmes lettres qui a deux valeurs, nous aurons une fonction transitive F′ dont le nombre des valeurs égales est $\frac{r}{2} p$. Considérons encore les substitutions qui ne contiennent pas x_0, et qui laissent F′ invariable. Soient K'_1 le nombre de ces substitutions effectuées sur $p - r_1$ lettres, K'_2 le nombre de ces substitutions effectuées sur $p - r_2$ lettres, etc. Le nombre des substitutions de moins de p lettres, qui laissent F′ invariable, est

$$\frac{K'_1 p}{r_1} + \frac{K'_2 p}{r_2} + \ldots + \frac{K'_i p}{r_i} + 1,$$

et on a

$$(\beta) \qquad \frac{r}{2} = K'_1 + K'_2 + \ldots + K'_i + 1;$$

quant au nombre des substitutions circulaires de p lettres qui laissent F′ invariable, il est

$$\frac{rp}{2} - \left(\frac{K'_1 p}{r_1} + \frac{K'_2 p}{r_2} + \ldots + \frac{K'_i p}{r_i} + 1\right).$$

Or le nombre des substitutions circulaires de p lettres qui laissent les

deux fonctions F et F′ invariables est le même ; on a donc

$$rp - p\left(\frac{K_1}{r_1} + \frac{K_2}{r_2} + \ldots + \frac{K_i}{r_i} + \frac{1}{p}\right) = \frac{rp}{2} - p\left(\frac{K'_1}{r_1} + \frac{K'_2}{r_2} + \ldots + \frac{1}{p}\right),$$

d'où

$$\frac{r}{2} = \frac{K_1 - K'_1}{r_1} + \frac{K_2 - K'_2}{r_2} + \ldots + \frac{K_i - K'_i}{r_i}.$$

En retranchant (β) de (α), on a d'autre part

$$\frac{r}{2} = (K_1 - K'_1) + (K_2 - K'_2) + \ldots + (K_i - K'_i),$$

et en comparant ces deux dernières égalités, on a

$$r_1 = 1, \quad K_2 = K'_2, \quad K_3 = K'_3 \ldots.$$

Nous ferons remarquer à propos de ce théorème ce fait digne d'attention, que nous ne connaissons aucune fonction transitive d'un nombre premier de quantités invariable par d'autres substitutions que $(z, az + b)$ et qui ne soit pas changée par des substitutions qui changent la fonction qui a deux valeurs.

Enfin nous pouvons certifier ce théorème, quoique nous n'en connaissions pas de démonstration rigoureuse : *Une fonction transitive d'un nombre premier de quantités ne peut être invariable par des substitutions qui s'effectuent sur moins de* $\frac{p+1}{2}$ *de ces quantités.*

Soit $(z, \theta z)$ une substitution des $p - 1$ variables $x_1, x_2, \ldots, x_{p-1}$ pour laquelle on a $\theta(a^u z) \equiv \alpha^u \theta z$, u étant un diviseur de $p - 1$; cette substitution est de la forme

$$(1) \qquad \left[\begin{array}{c} z,\ Az^{\lambda+(u-1)\frac{p-1}{u}} + Bz^{\lambda+(u-2)\frac{p-1}{u}} + \ldots + Iz^{\lambda+2\frac{p-1}{u}} \\ + Kz^{\lambda+\frac{p-1}{u}} + Lz^{\lambda} \end{array}\right].$$

D'ailleurs les dérivées des substitutions de cette forme sont encore de la même forme ; car si l'on a

$$\theta(a^u z) \equiv \alpha^u \theta z, \quad \mu(a^u z) \equiv \beta^u \mu z,$$

on aura

$$\theta\mu(a^u z) \equiv \theta(\beta^u \mu z) \quad \text{et} \quad \theta\mu(a^u z) \equiv \gamma^u \theta\mu z.$$

On voit donc que, λ étant un nombre variable, les substitutions de la forme (1) jointes aux substitutions (z, az) forment un système de substitutions conjuguées, et la fonction de $p-1$ quantités invariable par ces substitutions est transitive, puisqu'elle est invariable par toutes les substitutions (z, az).

Actuellement considérons une fonction transitive de p quantités, invariable par toutes les substitutions $(z, a^u z + b)$, et soient

$$(2) \qquad (z, z), \quad (z, \theta_1 z), \quad (z, \theta_2 z), \ldots, \quad (z, \theta_{r-1} z)$$

les substitutions qui ne contiennent pas x_0; désignons par $\theta'_s z$ la fonction inverse de $\theta_s z$, la substitution $(z, \theta_s a^u \theta'_s z)$ est semblable à $(z, a^u z)$ et laisse la fonction invariable; ce sera une substitution différente de $(z, a^u z)$, à moins que l'on n'ait

$$\theta_s a^u \theta'_s z \equiv \alpha^u z, \quad \text{d'où} \quad \theta_s (a^u z) \equiv \alpha^u \theta_s z,$$

et alors $(z, \theta_s z)$ est de la forme (1).

Parmi les substitutions (2), il y en a qui s'effectuent sur moins de $p-1$ variables; soit $(z, \theta_\rho z)$ une telle substitution, et supposons qu'elle ne permute pas x_α; si la substitution $(z, \theta_\rho z)$ est de la forme (1), la substitution $[z, \theta_\rho(z+\alpha) - \alpha]$ ne contient pas x_0 et n'est pas de la forme (1). Donc il existe au moins une substitution $(z, \theta_s a^u \theta'_s z)$ semblable à $(z, a^u z)$, et qui ne lui est pas identique.

Occupons-nous maintenant du cas particulier où la fonction transitive de p quantités est invariable par toutes les substitutions $(z, a^2 z)$, ce qui arrive toutes les fois que $\frac{p-1}{2}$ est un nombre premier.

Soient

$$(z, z), \quad (z, \theta_1 z), \quad (z, \theta_2 z), \ldots \quad (z, \theta_{\varepsilon-1} z)$$

les substitutions qui ne permutent que $x_2, x_3, \ldots, x_{p-1}$. Les substitutions $(z, \theta_s a^2 \theta'_s z)$ sont des substitutions semblables à $(z, a^2 z)$.

Supposons d'abord que le nombre des substitutions qui ne contiennent pas x_0 et qui laissent la fonction invariable, soit $\frac{\varepsilon(p-1)}{2}$. Faisons dans l'expression $(z, \theta_s a^2 \theta'_s z)$ $a = 2, 3, \ldots, \frac{p-1}{2}$, et $s = 0, 1, 2, \ldots, \varepsilon - 1$, nous aurons $\frac{\varepsilon(p-3)}{2}$ substitutions de $p-1$ quantités semblables à $(z, a^2 z)$. Donc, comme le nombre total des substitutions faites sur $x_1, x_2, \ldots, x_{p-1}$ est $\frac{\varepsilon(p-1)}{2}$, et que le nombre de ces substitutions qui ont moins de $p-1$ variables est $> \varepsilon$, toutes les substitutions $(z, \theta_s a^2 \theta'_s z)$ ne sont pas distinctes, et on a

$$\theta_s a^2 \theta'_s z \equiv \theta_t b^2 \theta'_t z,$$

ou

$$\theta'_t \theta_s (a^2 z) \equiv b^2 \theta'_t \theta_s z;$$

d'où

$$\theta'_t \theta_s z \equiv A z^{\frac{p-1}{2}+\lambda} + B z^{\lambda};$$

ainsi la fonction est invariable par au moins une substitution de la forme

$$\left(z, A z^{\frac{p-1}{2}+\lambda} + B z^{\lambda}\right).$$

En second lieu, supposons que le nombre des substitutions qui ne contiennent pas x_0 et qui laissent la fonction invariable soit $\varepsilon(p-1)$, auquel cas la fonction est deux fois transitive.

Soit $(z, \tau z)$ une substitution du second ordre qui contient x_1, et qui ne contient pas x_0; τz n'étant pas une des fonctions

$$a^2 z, \quad a^2 \theta_1 z, \quad a^2 \theta_2 z, \ldots, \quad a^2 \theta_{\varepsilon-1} z,$$

et supposons que toutes les substitutions du second ordre qui ne contiennent pas x_0, soient données par les fonctions

$$a^2 z, \quad a^2 \theta_1 z, \quad a^2 \theta_2 z, \ldots, \quad a^2 \theta_{\varepsilon-1} z,$$
$$a^2 z, \quad \tau a^2 \theta_1 z, \quad \tau a^2 \theta_2 z, \ldots, \quad \tau a^2 \theta_{\varepsilon-1} z.$$

Si toutes les substitutions $(z, \theta_s a^2 \theta'_s z)$ et $(z, \theta_s \tau a^2 \tau' \theta'_s z)$ étaient différentes entre elles, elles seraient en nombre égal à $\varepsilon(p-3)$, puisque a est susceptible des valeurs $2, 3, \ldots, \frac{p-1}{2}$, et s des valeurs $0, 1, 2, \ldots, \varepsilon - 1$, et par conséquent on n'aurait que 2ε substitutions de moins de $p-1$ lettres; ce qui est impossible, puisqu'il n'y a pas de substitutions de moins de $\frac{p+1}{2}$ variables.

1° Supposons que l'on ait $\theta_s a^2 \theta'_s z \equiv \theta_t b^2 \theta'_t z$, on aura

$$\theta'_t \theta_s (a^2 z) \equiv b^2 \theta'_t \theta_s z;$$

2° Soit $\theta_s \tau a^2 \tau' \theta'_s z \equiv \theta_v b^2 \theta'_v z$, on aura

$$\theta'_v \theta_s \tau a^2 \tau' z \equiv b^2 \theta'_v \theta_s z,$$

$$\theta'_v \theta_s \tau (a^2 z) \equiv b^2 \theta'_v \theta_s \tau z.$$

3° Soit $\theta_s \tau a^2 \tau' \theta'_s z \equiv \theta_v \tau \alpha^2 \tau' \theta'_v z$, on aura

$$\theta'_v \theta_s \tau a^2 \tau' z \equiv \tau \alpha^2 \tau' \theta'_v \theta_s z,$$

$$\tau' \theta'_v \theta_s \tau a^2 \tau' z \equiv \alpha^2 \tau' \theta'_v \theta_s z,$$

$$\tau' \theta'_v \theta_s \tau (a^2 z) \equiv \alpha^2 \tau' \theta'_v \theta_s \tau z.$$

Donc parmi les substitutions qui ne contiennent pas x_0, il y en a au moins une $(z, \mu z)$ pour laquelle on a

$$\mu (a^2 z) \equiv \alpha^2 \mu z \quad \text{ou} \quad \mu z \equiv A z^{\frac{p-1}{2}+\lambda} + B z^{\lambda}.$$

En terminant cette étude des fonctions d'un nombre premier de quantités, nous ferons remarquer que l'on ne doit pas croire à l'existence d'un très-grand nombre de théorèmes généraux relatifs à *toutes* ces fonctions; car il existe des fonctions transitives d'un nombre premier de variables, qui ne proviennent nullement de ce que le nombre de leurs variables est premier, et qui devraient satisfaire à ces théorèmes. Je citerai pour exemple la fonction trois fois transitive de 17 va-

riables qui a 1.2.3... 14 valeurs, et qui doit son existence non à ce que 17 est un nombre premier, mais à ce que 17 est une puissance de nombre premier, plus 1.

CHAPITRE V.

DES FONCTIONS TRANSITIVES DE n QUANTITÉS, n ÉTANT QUELCONQUE.

Nous allons donner dans ce chapitre plusieurs classes de fonctions transitives d'un nombre quelconque de quantités. Mais comme le sujet que nous allons traiter ici est bien loin d'avoir le même intérêt que celui qui a fait l'objet des chapitres précédents, nous n'y donnerons pas tout ce que nous avons pu trouver, et nous nous contenterons d'énoncer quelques propositions qui sont toutes très-faciles à démontrer.

Les classes de fonctions que nous allons donner, renferment presque toutes les fonctions une seule fois transitives qui ont moins de douze lettres.

Des fonctions cycliques.

On appelle fonction cyclique une fonction qui reste invariable par une certaine substitution circulaire contenant toutes ses variables.

Désignons par x_0, x_1, x_2,..., x_{n-1} les n variables de la fonction. Si cette fonction n'est invariable par aucune substitution circulaire de toutes ses variables qui ne soit puissance de (x_z, x_{z+1}), cette fonction n'est invariable que par des substitutions de la forme (x_z, x_{az+b}); mais la réciproque n'est pas vraie, une fonction invariable seulement par les substitutions (x_z, x_{az+b}), n'est pas nécessairement une seule fois cyclique.

Soient a, b,..., c, des nombres différents par rapport au module n et premiers à n, il y a une fonction cyclique de n quantités invariable par les substitutions comprises dans la formule

$$(z, a^\alpha b^\beta \ldots c^\gamma z + m);$$

en particulier, on a une fonction cyclique de n quantités invariable

par toutes les substitutions

$$(z,\ az+b),$$

a étant premier à n, et qui a $\frac{1.2\ldots(n-1)}{\varphi(n)}$ valeurs, $\varphi(n)$ désignant combien il y a de nombres inférieurs et premiers à n.

Si n est un nombre pair, l'expression $[z,\ z+(-1)^z]$ est une substitution régulière de n variables qui peut s'écrire

$$(x_0x_1)(x_2x_3)(x_4x_5)\ldots(x_{n-2}x_{n-1});$$

mais si n est impair, cette expression n'est plus une substitution, car elle changerait x_1 et x_{n-1} en x_0.

On voit d'après cela que si n est un nombre pair, il existe une fonction cyclique de n quantités ayant $\frac{1.2\ldots(n-1)}{n}$ valeurs, et invariable par toutes les substitutions

$$[z,\ z+m+l(-1)^z],$$

et qu'il y a aussi une fonction cyclique de ces quantités invariable par les substitutions

$$\left[z,\ a^\alpha b^\beta\ldots c^\gamma z+m+l(-1)^z\right].$$

Si n est pair, il n'y a pas de fonctions cycliques invariables seulement par des substitutions de n et de $n-1$ quantités. Si n est impair, il existe au moins une de ces fonctions, savoir la fonction invariable par les substitutions $(z,\ \pm z+b)$.

Des fonctions invariables par les substitutions

$$\left(x_{y,z,\ldots,u}\,x_{y+\alpha,\,z+\beta,\ldots,\,u+\gamma}\right).$$

Soit $n=pqr\ldots t$; considérons l'expression $x_{a,b,c,\ldots,e}$ et convenons que l'on aura

$$x_{a,b,c,\ldots,e}=x_{a',b',c',\ldots,e'}$$

si l'on a

$$a' \equiv a \pmod{p}, \qquad b' \equiv b \pmod{q}, \quad \ldots, \qquad e' \equiv e \pmod{t}.$$

L'expression $x_{a,b,c,\ldots,e}$ pourra représenter les n variables. Désignons par

$$(\alpha) \qquad (x_{\gamma,\varepsilon,\ldots,\iota}\, x_{\gamma+\alpha,\varepsilon+\beta,\ldots,\iota+\gamma})$$

une substitution qui augmente tous les premiers indices de α, tous les seconds indices de β, etc. En donnant à $\alpha, \beta, \ldots, \gamma$ toutes les valeurs dont ils sont susceptibles, on obtient des substitutions conjuguées entre elles, et qui laissent invariable une fonction transitive F qui a $1.2.3\ldots(n-1)$ valeurs.

Si $p, q, r, \ldots, t$ sont des nombres qui sont tous premiers entre eux, les substitutions (α) sont toutes les puissances d'une même substitution circulaire, de sorte que les substitutions peuvent s'écrire sous cette forme beaucoup plus simple $(x_\varepsilon\, x_{\varepsilon+m})$, les indices étant pris par rapport au module n.

En général, si l'on veut avoir toutes les fonctions d'un nombre donné n de variables, telles que F, et si l'on veut que le nombre des indices soit le plus petit possible, on adoptera la règle suivante : On cherchera de combien de manières le nombre n peut être décomposé en facteurs $p, q, r, \ldots, t$ tels, que q soit un diviseur de p, r un diviseur de q, et ainsi de suite. Autant il y aura de manières de décomposer ainsi le nombre n, autant il y aura de fonctions transitives différentes telles que F. On prendra un nombre d'indices égal au nombre des facteurs $p, q, r, \ldots, t$ et l'on prendra ces indices respectivement suivant ces nombres considérés comme modules.

Soit $n = mp$; il y a une fonction transitive de n quantités qui a $\frac{1.2.3\ldots(n-1)}{m^{p-2}}$ valeurs, et qui est invariable par les substitutions que l'on obtient en prenant le premier des cycles

$$(A) \qquad \begin{cases} (x_0^0\, x_1^0\, x_2^0\, x_3^0 \ldots x_{m-1}^0), \; (x_0^1\, x_1^1\, x_2^1 \ldots x_{m-1}^1), \\ (x_0^2\, x_1^2 \ldots x_{m-1}^2), \ldots, (x_0^{p-1}\, x_1^{p-1} \ldots x_{m-1}^{p-1}), \end{cases}$$

avec l'inverse de l'un quelconque des suivants, ni par la substitution

$$\text{(B)} \qquad \begin{cases} (x_0^0\, x_0^1\, x_0^2 \dots x_0^{p-1})\ (x_1^0\, x_1^1\, x_1^2 \dots x_1^{p-1}) \\ (x_2^0\, x_2^1\, x_2^2 \dots x_2^{p-1}) \dots (x_{m-1}^0\, x_{m-1}^1 \dots x_{m-1}^{p-1}). \end{cases}$$

Il y a une seconde fonction transitive de n quantités qui a $\frac{1.2.3\dots(n-1)}{m^{p-2}}$ valeurs et qui n'est changée ni par les substitutions que l'on obtient en prenant le premier des cycles (A) avec l'un quelconque des cycles (A) de rang pair ou avec l'inverse d'un quelconque des cycles (A) de rang impair, ni par la substitution (B).

Soit $n = mn_1$; s'il existe une fonction transitive de m quantités ayant p valeurs, il existe aussi une fonction transitive de n quantités qui a $\frac{1.2\dots(n-1)}{1.2\dots(m-1)}\, p$ valeurs.

Considérons la fonction transitive de m quantités qui a p valeurs; désignons ses m quantités par x_0, x_1, x_2,..., x_{m-1} et supposons que toutes les substitutions qui ne changent pas cette fonction soient

$$(x_z x_z),\ (x_z x_{\varphi_1 z}),\ (x_z x_{\varphi_2 z}), \dots, (x_z x_{\varphi_{r-1} z}).$$

Désignons par

$$x_0^0, x_1^0, x_2^0, \dots, x_{m-1}^0, x_0^1, x_1^1, x_2^1, \dots, x_{m-1}^1, \dots, x_0^{n_1-1}, x_1^{n_1-1}, \dots, x_{m-1}^{n_1-1},$$

n quantités, et imaginons une fonction de ces quantités invariable par la substitution

$$(x_z^\gamma\, x_z^{\gamma+1})$$

et par les substitutions

$$(x_z^\gamma\, x_z^\gamma),\ (x_z^\gamma\, x_{\varphi_1 z}^\gamma),\ (x_z^\gamma\, x_{\varphi_2 z}^\gamma), \dots, (x_z^\gamma\, x_{\varphi_{r-1} z}^\gamma),$$

et nous aurons la fonction dont il s'agit.