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

ÉMILE MATHIEU

Mémoire sur le nombre de valeurs que peut acquérir une fonction quand on y permute ses variables de toutes les manières possibles

Journal de mathématiques pures et appliquées 2^e série, tome 5 (1860), p. 9-42.
<http://www.numdam.org/item?id=JMPA_1860_2_5__9_0>

MÉMOIRE

SUR

LE NOMBRE DE VALEURS QUE PEUT ACQUÉRIR UNE FONCTION

QUAND ON Y PERMUTE SES VARIABLES DE TOUTES LES MANIÈRES POSSIBLES;

PAR M. ÉMILE MATHIEU [*].

Des substitutions.

Soient $abcd\ldots l$ et $efgh\ldots k$ deux permutations des mêmes lettres : on représente par la notation

$$\begin{pmatrix} a\,b\,c\,d\ldots l \\ e\,f\,g\,h\ldots k \end{pmatrix}$$

l'opération qui consiste à remplacer les lettres de la permutation supérieure par celles qui occupent le même rang dans la permutation inférieure; cette opération porte le nom de *substitution.*

Rangeons les lettres a, b, c, d,..., l sur un cercle, puis mettons chacune d'elles à la place de celle qui la précède : nous aurons ainsi fait sur ces lettres une substitution qui est dite *circulaire;* ainsi la substitution

$$\begin{pmatrix} a\,b\,c\ldots\ l \\ b\,c\,d\ldots la \end{pmatrix}$$

est circulaire; on l'écrit plus simplement

$$(a\,b\,c\,d\ldots l).$$

[*] Ce Mémoire est un extrait de plusieurs Mémoires présentés à l'Académie des Sciences. (*Voyez* les *Comptes rendus* des 31 mai, 21 juin et 2 novembre 1858, et du 25 avril 1859.)

Toute substitution, si elle n'est pas circulaire, équivaut à plusieurs substitutions circulaires effectuées simultanément sur des lettres différentes. Ainsi la substitution

$$\begin{pmatrix} a\ b\ c\ d\ e\ f\ g\ h\ i\ k\ l\ m\ n\ o\ p \\ m\ g\ a\ l\ b\ n\ d\ c\ k\ f\ e\ o\ i\ p\ h \end{pmatrix}$$

peut s'écrire

$$(amophc)\ (bgdle)\ (ikfn).$$

Les substitutions circulaires en lesquelles se décompose une substitution quelconque sont appelées les *cycles* de la substitution. Si le nombre des lettres de chacun des cycles d'une substitution est le même, la substitution est dite *régulière*.

Une substitution S que l'on obtient en faisant une autre substitution S_1 k fois de suite, se nomme la $k^{ième}$ puissance de S_1.

Soient

$$A, B, C, \ldots, G,$$

différentes substitutions effectuées sur les n lettres d'une fonction

$$F(a, b, c, \ldots, l),$$

et qui laissent cette fonction invariable; si nous faisons successivement dans un ordre quelconque quelques-unes de ces substitutions, nous obtiendrons en général d'autres substitutions, qui laisseront évidemment la fonction F invariable; les substitutions ainsi formées sont appelées les *dérivées* des substitutions A, B, ..., G. On considère

$$\begin{pmatrix} a\ b\ c \ldots\ l \\ a\ b\ c \ldots\ l \end{pmatrix}$$

comme faisant partie de ces substitutions dérivées.

Si sur la fonction

$$F(a, b, c, \ldots, l) \tag{1}$$

on fait les M substitutions qui la laissent invariable, on obtient M valeurs égales de cette fonction $F, F_1, F_2, \ldots, F_{M-1}$.

Faisons ensuite sur cette fonction la substitution

$$\begin{pmatrix} a & b & c \ldots & l \\ a' & b' & c' \ldots & l' \end{pmatrix}$$

qui change cette fonction ; $a', b', c', \ldots, l'$ étant par conséquent les lettres $a, b, c, \ldots, l$ prises dans un autre ordre; nous aurons la fonction

$$(2) \qquad F(a', b', c', \ldots, l');$$

changeons dans les M substitutions qui laissent la fonction (1) invariable les lettres $a, b, c, \ldots, l$, respectivement en $a', b', \ldots, l'$, et nous aurons M substitutions qui laissent la fonction (2) invariable, et si on les effectue sur la fonction (2), on obtient M autres valeurs égales $F', F'_1, F'_2, \ldots, F'_{M-1}$. On voit d'après cela que les $1.2.3 \ldots n$ valeurs que l'on obtient en permutant les n lettres $a, b, c, \ldots, l$ dans la fonction (1) de toutes les manières possibles sont égales M à M, et que le nombre des valeurs distinctes de la fonction (1) est égal à $\frac{1.2.3 \ldots n}{M}$, et, par conséquent, à un diviseur du produit $1.2.3 \ldots n$.

Des fonctions transitives.

Nous appellerons fonction *transitive* une fonction dans laquelle on peut faire occuper à une lettre quelconque telle place que l'on veut, sans que la fonction change de valeur, pourvu que l'on fasse occuper à toutes les autres des positions convenablement choisies.

Une fonction qui n'est pas transitive, sera dite *intransitive*.

C'est à M. Cauchy que nous empruntons l'idée de distinguer les fonctions en fonctions transitives et en fonctions intransitives.

Puisque dans une fonction symétrique on peut déplacer les lettres d'une manière quelconque, sans qu'elle change de valeur, il est clair qu'une fonction symétrique est transitive. Mais il existe bien d'autres fonctions transitives; car une fonction est transitive toutes les fois qu'elle n'est pas changée par une substitution circulaire effectuée sur toutes ses lettres.

Supposons en effet une fonction de n lettres qui ne soit pas changée

par la substitution circulaire suivante, effectuée sur ses n lettres,

$$(abcd\ldots g\ldots kl).$$

Il sera toujours possible d'amener une lettre quelconque à telle place que l'on voudra dans la fonction, sans que la valeur de cette fonction soit changée. Car si l'on veut, par exemple, amener dans la fonction la lettre g, qui occupe la $\beta^{ième}$ place dans la substitution à la place de la lettre a, il est clair qu'il suffira de faire cette substitution $\beta - 1$ fois.

Ainsi, par exemple, la fonction de trois lettres

$$ab^2c^3 + bc^2a^3 + ca^2b^3,$$

qui n'est pas changée par la substitution circulaire (abc), est une fonction transitive.

Une fonction peut d'ailleurs être transitive sans jouir de la propriété d'être invariable par une substitution circulaire effectuée sur toutes ses lettres. Par exemple, la fonction

$$(a - b)(c - d)$$

est transitive, et il est aisé de voir qu'elle est changée par toute substitution circulaire effectuée sur les quatre lettres a, b, c, d.

Il est facile de reconnaître que le nombre des valeurs distinctes d'une fonction transitive de n lettres est le même que si cette fonction était considérée comme fonction de $n - 1$ lettres, et que, par conséquent, on supposât une lettre immobile.

Considérons, en effet, une fonction transitive de n lettres

$$F(a, b, c, d, \ldots, k, l),$$

et supposons que l'on ait fait sur ses lettres toutes les substitutions possibles. Nous pourrons ensuite, dans toutes les fonctions ainsi obtenues, et dans lesquelles la lettre a ne sera pas à la première place, l'amener à cette place, pourvu que nous déplacions convenablement les autres. Toutes les valeurs se réduisant à des fonctions dans lesquelles a occupe la première place, il est clair que la fonction F acquiert toutes ses valeurs, considérée comme fonction des $n - 1$ lettres $b, c, d, \ldots, l$.

Réciproquement, si la fonction F acquiert toutes ses valeurs, considérée comme fonction des $n-1$ lettres $b, c, \ldots, l$, cette fonction est transitive par rapport à ses n lettres.

En effet, imaginons que l'on fasse sur les n lettres $a, b, \ldots, l$ les $1.2.3\ldots n$ permutations possibles, on obtiendra des valeurs dans lesquelles a occupera la première place, d'autres dans lesquelles a occupera la deuxième place, etc., d'autres enfin dans lesquelles a occupera la $n^{ième}$ place, et les valeurs distinctes se réduiront à celles dans lesquelles a occupera la première place. Il suit de là qu'on peut amener une lettre quelconque à la première place sans que la fonction change de valeur, pourvu que l'on permute convenablement toutes les lettres, et réciproquement on peut amener une lettre qui se trouve à la première place à une place quelconque. D'après cela, on pourra amener une lettre quelconque d à la place d'une lettre quelconque f, sans que la fonction change de valeur; car on pourra d'abord amener d à la place de a en permutant convenablement les lettres, puis on pourra amener d qui occupe la première place à la place de la lettre f. Donc la fonction est transitive.

On peut remarquer que si r est le nombre des substitutions qui s'effectuent sur les $n-1$ lettres $b, c, \ldots, l$, sans changer la valeur de la fonction F, le nombre des valeurs de cette fonction est $\frac{1.2.3\ldots(n-1)}{r}$, et, par conséquent, le nombre total des substitutions qui la laissent invariable est rn.

Des fonctions plusieurs fois transitives.

Imaginons une fonction transitive de n lettres; cette fonction, considérée comme fonction de $n-1$ lettres, pourra encore être transitive. S'il en est ainsi, nous dirons que la fonction est deux fois transitive.

Si cette fonction est encore transitive, considérée comme fonction de $n-2$ lettres prises parmi les $n-1$ précédentes, nous dirons qu'elle est trois fois transitive, et ainsi de suite.

Il suit de là qu'une fonction μ fois transitive acquiert toutes ses valeurs, considérée comme fonction de $n-\mu$ lettres. On voit encore qu'une fonction symétrique est une fonction $n-1$ fois transitive.

Une fonction de n lettres qui est invariable par une substitution

circulaire de ses n lettres, par une substitution circulaire de $n-1$ lettres, par une troisième substitution circulaire faite sur $n-2$ d'entre ces dernières, etc.; enfin, par une $\mu^{ième}$ substitution circulaire effectuée sur $n-\mu+1$ lettres obtenues en agissant comme précédemment, est μ fois transitive.

THÉORÈME. — *Si une fonction de n lettres est μ fois transitive, elle est transitive par rapport à $n-1$ lettres quelconques, elle est transitive par rapport à $n-2$ lettres quelconques, etc.; enfin, elle est transitive par rapport à $n-\mu+1$ lettres quelconques.*

En effet, supposons une fonction transitive par rapport à ses n lettres

$$a, b, c, d, \ldots, k, l,$$

puis par rapport aux lettres

$$b, c, d, \ldots, k, l,$$

puis par rapport aux lettres

$$c, d, \ldots, k, l,$$

et ainsi de suite. Je dis que cette fonction est transitive par rapport à $n-\mu+1$ lettres quelconques $e_1, f_1, \ldots, k_1, l_1$.

En effet, désignons par a', b'', c''', ... les $\mu-1$ lettres de la fonction qui ne font pas partie de celles-ci. La fonction étant transitive par rapport aux lettres $a, b, c, \ldots, k, l$, nous pouvons amener la lettre a' à la place de la lettre a, et les $n-1$ autres $b', c', \ldots, k', l'$ remplaceront respectivement $b, c, \ldots k, l$. Or ces $n-1$ lettres $b', c', \ldots, k', l'$ remplaçant respectivement $b, c, \ldots, k, l$, la fonction sera transitive par rapport aux lettres

$$b', c', d', \ldots, k', l',$$

puis par rapport aux lettres

$$c', d' \ldots, k', l',$$

et ainsi de suite. Parmi les $n-1$ lettres $b', c', \ldots, k', l'$, nous pouvons prendre b'' et l'amener à la place de b', pourvu que nous déplacions

convenablement les autres, et les lettres $c', d', \ldots, k', l'$ seront remplacées respectivement par $c'', d'', \ldots, k'', l''$. Les lettres $c'', d'', \ldots, k'', l''$ se trouvent dans les mêmes conditions que les lettres $c', d', \ldots, k', l'$, et par suite que les lettres $c, d, \ldots, k, l$. Et si l'on imagine que l'on continue ce raisonnement, la proposition devient évidente.

COROLLAIRE I. — *Dans une fonction μ fois transitive, on peut amener μ lettres quelconques à telles places que l'on veut.*

COROLLAIRE II. — *Réciproquement, si dans une fonction on peut amener μ lettres quelconques à telles places que l'on veut sans que la fonction change de valeur, la fonction est μ fois transitive.*

Supposons, en effet, que dans une fonction on puisse amener μ lettres quelconques à la place de μ autres lettres quelconques. Puisqu'on peut amener une lettre quelconque a' à la place d'une autre quelconque a sans que la fonction change de valeur, cette fonction est une fois transitive. Puisque, sans déranger a', on peut amener une lettre quelconque b' à la place de b, la fonction est deux fois transitive, et ainsi de suite.

THÉORÈME. — *Si une fonction de n lettres acquiert toutes ses valeurs, considérée comme fonction de $n - \mu$ lettres, elle est μ fois transitive.*

Nous avons vu que, si une fonction de n lettres $a, b, c, \ldots, l$ acquiert toutes ses valeurs considérée comme fonction de $n - 1$ lettres $b, c, \ldots, l$, elle est transitive par rapport à ses n lettres. D'après cela, supposons une fonction de n lettres $a, b, \ldots, f, g, \ldots, k, l$, qui acquière toutes ses valeurs considérée comme fonction des $n - \mu$ lettres $g, \ldots, k, l$; elle acquerra évidemment toutes ses valeurs considérée comme fonction des $n - 1$ lettres

$$b, c, \ldots, f, g, \ldots, k, l,$$

puis elle acquerra toutes ses valeurs, considérée comme fonction des $n - 2$ lettres

$$c, \ldots, f, g, \ldots, k, l,$$

et ainsi de suite; enfin elle acquerra toutes ses valeurs considérée comme fonction des $n - \mu$ lettres

$$g, \ldots, k, l.$$

et, par conséquent, la fonction sera transitive par rapport à n lettres, puis par rapport à $n-1$ de ces dernières, puis par rapport à $n-2$ lettres prises parmi les $n-1$ précédentes, et ainsi de suite. Donc enfin la fonction est μ fois transitive.

THÉORÈME. — *Si une fonction de n lettres est transitive par rapport à ses n lettres*

$$a, b, \ldots, f, g, h,$$

puis transitive par rapport à $n-1$ *lettres*

$$a', b', \ldots, f', g',$$

puis transitive par rapport à $n-2$ *lettres*

$$a'', b'', \ldots, f'',$$

et ainsi de suite, enfin transitive par rapport à $n-\mu+1$ *lettres, elle est* μ *fois transitive.*

La fonction est transitive par rapport aux lettres $a, b, \ldots, f, g, h$, et elle est aussi transitive par rapport à $n-1$ de ces lettres $a', b', \ldots, f', g'$; elle est donc deux fois transitive, et par suite elle est transitive par rapport à $n-1$ lettres quelconques; ainsi la fonction est transitive par rapport aux $n-1$ lettres

$$a'', b'', \ldots, f'', g_1;$$

on voit donc que la fonction est transitive par rapport aux n lettres

$$a'', b'', \ldots, f'', g_1, h_1,$$

puis par rapport aux $n-1$ lettres

$$a'', b'', \ldots, f'', g_1,$$

puis par rapport aux $n-2$ lettres

$$a'', b'', \ldots, f'';$$

la fonction est donc trois fois transitive, et si l'on imagine que l'on

continue ce raisonnement, il devient clair que la fonction considérée est μ fois transitive.

THÉORÈME. — *Une fonction μ fois transitive, qui n'est pas changée par une certaine substitution qui ne comprend pas plus de μ lettres, est invariable par une substitution circulaire de trois lettres quelconques, et, par suite, elle n'a au plus que deux valeurs.*

Supposons, en effet, une fonction qui soit μ fois transitive et qui ne soit pas changée par la substitution

$$(1) \qquad \begin{pmatrix} a\,b\,c\,\ldots f\ldots p \\ k\,l\,m\ldots b\,\ldots\,q \end{pmatrix}$$

qui ne renferme pas plus de μ lettres. La fonction étant μ fois transitive, à la place des lettres $a, b, c, \ldots, p$, on peut amener d'autres lettres quelconques, sans que cette fonction change de valeur; donc aux places de $a, b, c, \ldots, p$, on peut mettre respectivement les lettres $a, \alpha, c, \ldots, p$, la lettre α n'appartenant pas à la substitution (1), et, par conséquent, la fonction n'étant pas changée par la substitution (1) n'est pas changée non plus par la substitution

$$(2) \qquad \begin{pmatrix} a\,\alpha\,c\,\ldots f\ldots p \\ k\,l\,m\ldots\alpha\ldots q \end{pmatrix}.$$

Faisons la substitution (1), puis l'inverse de la substitution (2), et nous aurons fait en définitive la substitution circulaire de trois lettres $(b\alpha f)$, sans que la fonction ait changé de valeur. Si donc la fonction est au moins trois fois transitive, à la place des lettres b, α, f, on pourra mettre dans la fonction trois lettres quelconques; la fonction ne sera donc changée par aucune substitution circulaire de trois lettres, et je dis que, par suite, elle aura au plus deux valeurs.

En effet, faire une substitution circulaire $(ab\alpha)$ revient à faire la transposition (ab), puis la transposition $(a\alpha)$. La transposition (ab) changera la valeur F_1 de la fonction considérée en F_2, et la transposition $(a\alpha)$ changera la valeur F_2 en la valeur primitive F_1. Faisons ensuite la substitution circulaire (abc) sur F_1, et pour cela faisons la transposition (ab), puis la transposition (ac). La transposition (ab)

change F_1 en F_2, et la transposition (ac) faite sur F_2 doit rendre la fonction F_1. Ainsi les deux transpositions $(a\alpha)$ et (ac) qui ont une lettre commune, produisent le même changement sur la fonction; de même (ac) produira le même changement que (cd). Par conséquent, $(a\alpha)$ et (cd) produisent le même changement sur la fonction. Or toute substitution peut s'effectuer par une série de transpositions successives. Si l'on fait une première transposition sur F_1, F_1 deviendra F_2; en faisant une deuxième transposition sur F_2, on changera F_2 en F_1; une troisième transposition changera F_1 en F_2, et ainsi de suite. La fonction a donc évidemment au plus deux valeurs, car on peut avoir $F_2 = F_1$.

Ainsi le théorème est démontré toutes les fois que la fonction est au moins trois fois transitive.

Il reste à démontrer qu'une fonction deux fois transitive qui est invariable par la transposition (ab) n'a pas plus de deux valeurs. Or, comme dans une telle fonction on peut amener à la place de a et b deux lettres quelconques, on voit que cette fonction est invariable par une transposition quelconque, ou qu'elle est symétrique par rapport à toutes ses lettres.

COROLLAIRE. — *Une fonction de n lettres ne peut être plus de $\frac{n}{2}$ fois transitive, lorsqu'elle a plus de deux valeurs.*

En effet, considérons une fonction de n lettres μ fois transitive; cette fonction est changée par toute substitution qui s'effectue sur μ lettres; elle a donc au moins $1.2.3...\ \mu$ valeurs. D'ailleurs le nombre des valeurs de la fonction est un diviseur du produit $1.2.3...\ (n-\mu)$; on a donc

$$1.2.3...\ (n-\mu) \geqq 1.2.3...\ \mu,$$

et, par suite, μ est au plus égal à $\frac{n}{2}$.

On peut citer un cas où μ est précisément égal à $\frac{n}{2}$. Soit la fonction

$$(ad+bc+ef)(ab+ce+df)(ae+bd+cf)(ac+de+bf)(af+cd+be);$$

cette fonction est invariable par chacune des trois substitutions circu-

laires

$$(acbfed), \quad (abcde), \quad (abdc),$$

comme il est aisé de le vérifier.

Cette fonction est donc trois fois transitive; par suite elle a au moins $1.2.3 = 6$ valeurs; car il est aisé de voir qu'elle a plus de deux valeurs; elle n'a pas d'ailleurs plus de six valeurs, puisqu'elle doit acquérir toutes ses valeurs, considérée comme fonction de trois lettres; elle a donc six valeurs.

Fonctions de n lettres qui ont deux valeurs.

Quel que soit n, on peut former des fonctions de n lettres qui n'aient que deux valeurs

Prenons en effet les n lettres $a, b, c, \ldots, k, l$, et faisons le produit ν de toutes les différences de ces n lettres, nous aurons

$$\nu = (a-b)(a-c)\ldots(a-k)(a-l)(b-c)\ldots(k-l);$$

ν^2 est évidemment une fonction symétrique des n lettres, et ν a deux valeurs égales et de signe contraire; car ν change de signe si l'on transpose a avec b.

Soit F une fonction des n lettres $a, b, c, \ldots, l$, qui a deux valeurs; on démontre facilement que cette fonction est changée par la transposition de deux lettres quelconques. (*Voir* 19e leçon de l'*Algèbre supérieure* de M. Serret.) D'après cela, désignons par $F(a, b)$ l'une de ces deux valeurs, l'autre valeur sera $F(b, a)$. Posons

$$F(a,b) + F(b,a) = \varphi, \quad F(a,b)\nu - F(b,a)\nu = \psi,$$

φ et ψ ne sont pas changées par la transposition (ab), et comme a et b sont deux quelconques des lettres $a, b, \ldots, l$, les fonctions φ et ψ sont symétriques. De ces équations on déduit

$$F(a,b) = \frac{\varphi}{2} + \frac{\psi}{2\nu^2}\nu, \quad \text{ou} \quad F = \Phi + \Psi\nu,$$

Φ et Ψ étant deux fonctions symétriques des lettres $a, b, \ldots, l$.

THÉORÈME. — *La fonction de n lettres qui a deux valeurs, est changée*

par toute substitution circulaire effectuée sur un nombre pair de lettres, et elle n'est changée par aucune substitution circulaire faite sur un nombre impair de lettres.

Faisons en effet sur cette fonction la substitution circulaire de α lettres $(abcd\ldots g)$. Pour faire cette substitution, nous pourrons transposer a avec b, puis a avec c, puis a avec d, et ainsi de suite; et nous ferons ainsi $\alpha - 1$ transpositions. Or à chaque transposition la fonction change de valeur; donc puisque la fonction n'a que deux valeurs, si α est pair, la fonction change de valeur, et si α est impair, la fonction ne change pas. Ce qu'il fallait démontrer.

Scolie. — D'après cela, pour reconnaître si une substitution ne change pas la fonction qui a deux valeurs, on décomposera cette substitution en ses cycles. Si le nombre des cycles qui renferment un nombre pair de lettres est pair, la fonction qui a deux valeurs n'est pas changée par cette substitution; si le nombre de ces cycles est impair, la fonction est changée par cette substitution.

COROLLAIRE. — *Soit une fonction φ invariable par une substitution* A *qui renferme un nombre impair de cycles ayant un nombre pair de lettres; si l'on multiplie cette fonction φ par la fonction des mêmes lettres qui a deux valeurs, on obtient une fonction* F *qui a un nombre de valeurs double du nombre des valeurs de φ.*

En effet, soient

$$\varphi, \varphi_1, \varphi_2, \ldots, \varphi_{\mu-1}$$

les μ valeurs distinctes de la fonction φ que l'on obtient en faisant sur la première les substitutions

$$(a) \qquad S_1, S_2, \ldots, S_{\mu-1};$$

soit ν la fonction des mêmes lettres qui a deux valeurs; faisons sur $\varphi\nu$ les mêmes substitutions, nous aurons les fonctions

$$(b) \qquad \varphi\nu, \varphi_1\nu_1, \varphi_2\nu_2, \ldots, \varphi_{\mu-1}\nu_{\mu-1},$$

$\nu, \nu_1, \nu_2, \ldots, \nu_{\mu-1}$ se réduisant à deux valeurs ν et ν'. Sur les lettres de la substitution A, faisons successivement les substitutions (a), nous

aurons les substitutions semblables

$$A, A_1, A_2, \ldots, A_{\mu-1};$$

faisons chacune de ces substitutions respectivement sur les fonctions (b) de même rang, les premiers facteurs ne seront pas changés, et, d'après le scolie ci-dessus, les seconds facteurs le seront : on aura donc μ autres valeurs de $\varphi\nu$. Comme la fonction $\varphi\nu$ n'a évidemment pas plus de 2μ valeurs, elle en a effectivement 2μ.

Ainsi, par exemple, la fonction

$$(ad+bc+ef)(ab+ce+df)(ae+bd+cf)(ac+de+bf)(af+be+cd)$$

est une fonction trois fois transitive qui a six valeurs, et qui n'est pas changée par les substitutions

$$(acbfed), \quad (abcde), \quad (abdc).$$

Si nous multiplions cette fonction par la fonction des mêmes lettres qui a deux valeurs, nous aurons une fonction qui aura douze valeurs, et qui sera invariable par les substitutions

$$(abe)(cfd), \quad (abcde), \quad (ad)(bc);$$

on voit donc aussi que cette fonction est deux fois transitive.

Fonctions transitives d'un nombre premier p de lettres. — Fonction trois fois transitive de $p+1$ lettres qui a $1.2\ldots(p-2)$ valeurs, et fonction deux fois transitive de $p+1$ lettres qui a $1.2\ldots(p-2)\times 2$ valeurs.

Pour étudier les fonctions transitives d'un nombre premier de variables, nous désignerons ces p variables par $x_0, x_1, x_2, \ldots, x_{p-1}$, en convenant que l'on aura $x_a = x_e$, si l'on a

$$a \equiv e \,(\text{mod. } p).$$

Nous désignerons aussi par $(x_z x_{\theta z})$ la substitution qui changera en général x_z en $x_{\theta z}$.

Il est facile de former une fonction

$$(a) \qquad \psi(x_0, x_1, x_2, \ldots, x_{p-1})$$

qui soit invariable par la substitution circulaire

$$(b) \qquad (x_0\, x_1\, x_2 \ldots x_{p-1});$$

pour cela, il suffira de prendre une fonction $\lambda(x_0, x_1, x_2, \ldots, x_{p-1})$ qui soit changée par toutes les substitutions, et de faire sur cette fonction $p-1$ fois de suite la substitution (b); on aura ainsi les p fonctions

$$\begin{aligned}
&\lambda(x_0, x_1, x_2, \ldots, x_{p-1}),\\
&\lambda(x_1, x_2, x_3, \ldots, x_0),\\
&\lambda(x_2, x_3, x_4, \ldots, x_1),\\
&\ldots\ldots\ldots\ldots
\end{aligned}$$

et, en prenant une fonction symétrique de ces p fonctions, on aura la fonction (a). Cette fonction transitive, qui est invariable par les p substitutions $(x_z x_{z+m})$, a évidemment $1.2\ldots(p-1)$ valeurs.

Soient ω une racine primitive de p, et u un diviseur de $p-1$; faisons sur la fonction (a) la substitution régulière $(x_z\, x_{\omega^u z})$ et ses puissances $(x_z\, x_{a^u z})$, nous aurons les fonctions

$$(c) \qquad \left\{\begin{aligned}
&\psi(x_0, x_1, x_2, \ldots, x_{p-1}),\\
&\psi(x_0, x_{\omega^u}, x_{2\omega^u}, \ldots, x_{(p-1)\omega^u}),\\
&\psi(x_0, x_{\omega^{2u}}, x_{2\omega^{2u}}, \ldots, x_{(p-1)\omega^{2u}});\\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}\right.$$

formons une fonction symétrique de ces $\frac{p-1}{u}$ fonctions, et nous aurons une fonction Ψ invariable par toutes les substitutions

$$(d) \qquad (x_z\, x_{a^u z+b}).$$

On voit d'abord immédiatement que si l'on fait sur les fonctions (c) la substitution $(x_z\, x_{\omega^u z})$, on passe d'une de ces fonctions à la suivante; par conséquent, Ψ est invariable par $(x_z\, x_{\omega^u z})$ et par ses puis-

sances $(x_z\, x_{a^u z})$. Ensuite la première des fonctions (c) étant invariable par les substitutions $(x_z\, x_{z+m})$, la fonction

$$\psi(x_0, x_{\omega^{su}}, x_{2\omega^{su}}, x_{3\omega^{su}}, \ldots)$$

est invariable par les substitutions

$$(x_{\omega^{su} z}, x_{\omega^{su}_{s} z+m}),$$

ou $(x_z\, x_{z+m})$. Donc chacune des fonctions (c) est invariable par les substitutions $(x_z\, x_{z+m})$; donc Ψ est invariable par les substitutions $(x_z\, x_{a^u z})$ et $(x_z\, x_{z+m})$, et par conséquent aussi, par les substitutions (d); Ψ est donc une fonction transitive qui a $1.2\ldots(p-2)\times u$ valeurs.

Ainsi, *soient p un nombre premier, et u un diviseur de* $p-1$, *il y a toujours une fonction transitive de p variables qui a* $1.2\ldots(p-2)\times u$ *valeurs.*

On doit remarquer, en particulier, le cas où u est égal à 1; dans ce cas la fonction Ψ est une fonction deux fois transitive qui a $1.2\ldots(p-2)$ valeurs et qui est invariable par toutes les substitutions $(x_z\, x_{az+b})$; cette fonction coïncide avec la fonction résolvante de Lagrange, si l'on prend pour la fonction (a) la fonction

$$(x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{p-1} x_{p-1}),$$

α étant une racine $p^{ième}$ imaginaire de l'unité.

Nous allons donner une autre méthode pour former les fonctions invariables par les substitutions (d).

Il est aisé de former une fonction

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

qui soit invariable par la substitution régulière $(x_z\, x_{\omega^u z})$; il suffira, pour cela, de faire cette substitution et ses puissances sur une fonction quelconque μ, et de prendre une fonction symétrique des fonctions $\mu, \mu_1, \mu_2, \ldots$ ainsi obtenues.

Faisons sur la fonction (e) les p substitutions comprises dans l'expression $(x_z\, x_{z+k})$, nous aurons p fonctions renfermées dans la

formule

$$(f) \qquad \varphi\left[(x_k), x_{1+k}, x_{\omega+k}, x_{\omega^2+k}, \ldots, x_{\omega^{p-2}+k}\right] = \varphi_k,$$

k étant susceptible des valeurs 0, 1, 2,..., $p-1$. Formons une fonction symétrique Φ des fonctions (f), et nous aurons une fonction invariable par les substitutions (d).

Il est d'abord évident que la fonction Φ est invariable par les substitutions $(x_z\, x_{z+m})$; je dis ensuite que cette fonction est invariable par la substitution $(x_z\, x_{\omega^u z})$. Or, par cette substitution φ_k deviendra

$$(g) \qquad \varphi\left[(x_{k\omega^u}), x_{\omega^u+k\omega^u}, x_{\omega^{u+1}+k\omega^u}, x_{\omega^{u+2}+k\omega^u}, \ldots\right],$$

et de même que la fonction (e) est invariable par $(x_z\, x_{\omega^u z})$, la fonction (f) n'est pas changée par $(x_{z+k}\, x_{\omega^u z+k})$ et (g) n'est pas changée par

$$(x_{\omega^u z+k\omega^u}, x_{\omega^{2u} z+k\omega^u});$$

si l'on fait sur (g) l'inverse de cette dernière substitution, cette fonction devient

$$\varphi\left[(x_{k\omega^u}), x_{1+k\omega^u}, x_{\omega+k\omega^u}, x_{\omega^2+k\omega^u}, \ldots\right],$$

ou $\varphi_{k\omega^u}$; ainsi la substitution $(x_z\, x_{\omega^u z})$ change φ_k en $\varphi_{k\omega^u}$; en faisant sur les variables la substitution $(x_z\, x_{\omega^u z})$, on fait sur les fonctions φ la substitution $(\varphi_k\, \varphi_{\omega^u k})$; la fonction Φ est donc invariable par $(x_z\, x_{\omega^u z})$, et, par suite, par les substitutions (d).

Il est naturel de se demander ici s'il n'existe pas une fonction trois fois transitive de $p+1$ variables, qui ait $1.2\ldots(p-2)$ valeurs, et qui, considérée comme fonction de p lettres, soit la fonction deux fois transitive qui est invariable par toutes les substitutions $(x_z\, x_{az+b})$; or nous allons démontrer que cette fonction existe effectivement, en sorte que l'on a ce théorème :

Si p est un nombre premier, il y a une fonction trois fois transitive de $p+1$ variables, qui a $1.2\ldots(p-2)$ valeurs.

Nous allons donner la forme générale de cette fonction.

Soit $\varphi\left[(x_0), x_1, x_\omega, x_{\omega^2}, x_{\omega^3}, \ldots, x_{\omega^{p-2}}\right]$ une fonction qui est inva-

riable par la substitution circulaire $(x_z\, x_{\omega z})$; d'après ce que nous venons de voir, nous aurons une fonction deux fois transitive invariable par toutes les substitutions $(x_z\, x_{az+b})$, en formant une fonction symétrique des fonctions suivantes :

$$
(\mathrm{A}) \quad \left\{
\begin{array}{l}
\varphi\left[(x_0),\quad x_1,\quad x_\omega,\quad x_{\omega^2},\quad x_{\omega^3},\ldots,\quad x_{\omega^{p-2}}\right],\\
\varphi\left[(x_1),\quad x_2,\quad x_{1+\omega},\quad x_{1+\omega^2},\quad x_{1+\omega^3},\ldots,\quad x_{1+\omega^{p-2}}\right],\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\varphi\left[(x_r),\quad x_{r+1},\quad x_{r+\omega},\quad x_{r+\omega^2},\quad x_{r+\omega^3},\ldots,\quad x_{r+\omega^{p-2}}\right],\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\varphi\left[(x_{p-1}),\ x_0,\quad x_{p-1+\omega},\ x_{p-1+\omega^2},\ x_{p-1+\omega^3},\ldots,\ x_{p-1+\omega^{p-2}}\right].
\end{array}
\right.
$$

Désignons cette fonction par

$$(\mathrm{B}) \qquad \Phi(x_0,\, x_1,\, x_\omega,\ldots,\, x_{\omega^{p-2}});$$

soit x'_0 une $(p+1)^{ième}$ variable, qui entre d'une manière arbitraire dans la fonction (B); faisons sur cette fonction la substitution

$$(h) \qquad (x'_0\, x'_1\, x'_2 \ldots x'_{p-1})$$

et ses puissances, x'_1, x'_2, x'_3, etc., étant déterminées par les égalités

$$x'_1 = x_1,\quad x'_\omega = x_{\omega^{p-2}},\quad x'_{\omega^2} = x_{\omega^{p-3}},\ldots,\ x'_{\omega^k} = x_{\omega^{p-1-k}},\ldots;$$

nous obtiendrons ainsi p fonctions Φ. Considérons encore la fonction

$$(\mathrm{C}) \qquad \Phi(x'_0,\, x'_1,\, x_{\omega^{p-2}},\, x_{\omega^{p-3}},\ldots,\, x_\omega),$$

que nous obtenons en changeant dans la fonction (B), $x_0, x_1, x_2,\ldots, x_{p-1}, x'_0$ respectivement en $x'_0, x'_1, x'_2,\ldots, x'_{p-1}, x_0$; enfin, formons une fonction symétrique Θ de ces $p+1$ fonctions Φ; je dis que cette fonction n'est pas changée par les substitutions

$$(i) \qquad (x_1\, x_\omega\, x_{\omega^2} \ldots x_{\omega^{p-2}}),\quad (k)\ (x_0\, x_1\, x_2 \ldots x_{p-1}),$$

et par (h), et qu'ainsi elle est trois fois transitive, et a $1.2\ldots(p-2)$ valeurs.

Il est facile de reconnaître d'abord que la fonction Θ est invariable par les substitutions (h) et (i). En effet, la fonction (B) n'est pas changée par la substitution (i), et par suite elle n'est pas changée par $(x_1\, x_{\omega^{p-2}}\, x_{\omega^{p-3}}\ldots x_\omega)$ ou par

$$(i') \qquad (x'_1\, x'_\omega\, x'_{\omega^2}\ldots x'_{\omega^{p-2}});$$

donc, la fonction (B) étant invariable par la substitution (i'), si l'on fait sur la fonction (B) la substitution (h) et ses puissances, on obtiendra p fonctions, et les substitutions (h) et (i') ne feront que permuter ces p fonctions. D'ailleurs, de même que la fonction (B) n'est pas changée par les substitutions (k) et (i), la fonction (C) n'est pas changée par les substitutions (h) et (i'); donc la fonction Θ n'est pas changée par les substitutions (h) et (i'), ou par les substitutions (h) et (i).

Reste donc à démontrer que la fonction Θ est invariable par la substitution (k).

Dans la fonction Θ changeons $x_0, x_1, x_2, \ldots, x_{p-1}, x'_0$ en $x'_0, x'_1, x'_2, \ldots, x'_{p-1}, x_0$, nous aurons ainsi une fonction Θ', et puisque la fonction Θ n'est pas changée par la substitution (h), Θ' n'est pas changée par la substitution (k). Si donc nous démontrons que la fonction Θ' est égale à la fonction Θ, il sera démontré que la fonction Θ est invariable par la substitution (k) : c'est ce que nous allons faire.

Remarquons que les fonctions (B) et (C) entrent toutes deux dans Θ et Θ', et il s'agit de démontrer que les $p-1$ autres fonctions Φ qui entrent dans Θ sont les mêmes que les $p-1$ autres qui entrent dans Θ'; ce qui revient encore à démontrer que si l'on fait sur la fonction (B) t fois la substitution (h), on aura la même fonction que si l'on fait sur la fonction (C) u fois la substitution (k), en assignant à u une valeur convenablement choisie.

En général, si l'on a

$$x_a = x'_b,$$

c'est que l'on a

$$ab \equiv 1 \pmod{p}; \quad \text{ou} \quad x_a = x'_{\frac{1}{a}}.$$

D'après cela, les fonctions (A) peuvent s'écrire :

$$
(D)\left\{
\begin{array}{llllll}
\varphi\Big[(x_0), & x'_1, \quad x'_{\frac{1}{\omega}}, & x'_{\frac{1}{\omega^2}}, & x'_{\frac{1}{\omega^3}}, \ldots, & x'_{\frac{1}{\omega^{p-2}}}\Big], \\
\varphi\Big[(x'_1), & x'_{\frac{1}{2}}, \quad x'_{\frac{1}{1+\omega}}, & x'_{\frac{1}{1+\omega^2}}, & x'_{\frac{1}{1+\omega^3}}, \ldots, & x'_{\frac{1}{1+\omega^{p-2}}}\Big], \\
\cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots \\
\varphi\Big[\Big(x'_{\frac{1}{r}}\Big), & x'_{\frac{1}{r+1}}, \quad x'_{\frac{1}{r+\omega}}, & x'_{\frac{1}{r+\omega^2}}, & x'_{\frac{1}{r+\omega^3}}, \ldots, & x'_{\frac{1}{r+\omega^{p-2}}}\Big], \\
\cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots \\
\varphi\Big[\Big(x'_{\frac{1}{p-1}}\Big), & x_0, \quad x'_{\frac{1}{p-1+\omega}}, & x'_{\frac{1}{p-1+\omega^2}}, & x'_{\frac{1}{p-1+\omega^3}}, \ldots, & x'_{\frac{1}{p-1+\omega^{p-2}}}\Big],
\end{array}
\right.
$$

La fonction (B) est une fonction symétrique des fonctions (D). Faisons sur la fonction (B) t fois la substitution (h), la fonction qui résultera sera la fonction symétrique de ces fonctions :

$$
(E)\left\{
\begin{array}{llllll}
\varphi\Big[(x_0), & x'_{1+t}, & x'_{\frac{1}{\omega}+t}, & x'_{\frac{1}{\omega^2}+t}, & x'_{\frac{1}{\omega^3}+t}, \ldots, & x'_{\frac{1}{\omega^{p-2}}+t}\Big], \\
\varphi\Big[(x'_{1+t}), & x'_{\frac{1}{2}+t}, & x'_{\frac{1}{1+\omega}+t}, & x'_{\frac{1}{1+\omega^2}+t}, & x'_{\frac{1}{1+\omega^3}+t}, \ldots, & x'_{\frac{1}{1+\omega^{p-2}}+t}\Big], \\
\cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots \\
\varphi\Big[\Big(x'_{\frac{1}{r}+t}\Big), & x'_{\frac{1}{r+1}+t}, & x'_{\frac{1}{r+\omega}+t}, & x'_{\frac{1}{r+\omega^2}+t}, & x'_{\frac{1}{r+\omega^3}+t}, \ldots, & x'_{\frac{1}{r+\omega^{p-2}}+t}\Big], \\
\cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots \\
\varphi\Big[\Big(x'_{\frac{1}{p+1}+t}\Big), & x_0, & x'_{\frac{1}{p-1+\omega}+t}, & x'_{\frac{1}{p-1+\omega^2}+t}, & x'_{\frac{1}{p-1+\omega^3}+t}, \ldots, & x'_{\frac{1}{p-1+\omega^{p-2}}+t}\Big].
\end{array}
\right.
$$

De même la fonction (C) est une fonction symétrique des fonctions suivantes

$$
(F)\left\{
\begin{array}{llllll}
\varphi\Big[(x'_0), & x_1, & x_{\frac{1}{\omega}}, & x_{\frac{1}{\omega^2}}, & x_{\frac{1}{\omega^3}}, \ldots, & x_{\frac{1}{\omega^{p-2}}}\Big], \\
\varphi\Big[(x_1), & x_{\frac{1}{2}}, & x_{\frac{1}{1+\omega}}, & x_{\frac{1}{1+\omega^2}}, & x_{\frac{1}{1+\omega^3}}, \ldots, & x_{\frac{1}{1+\omega^{p-2}}}\Big], \\
\cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots \\
\varphi\Big[\Big(x_{\frac{1}{r}}\Big), & x_{\frac{1}{r+1}}, & x_{\frac{1}{r+\omega}}, & x_{\frac{1}{r+\omega^2}}, & x_{\frac{1}{r+\omega^3}}, \ldots, & x_{\frac{1}{r+\omega^{p-2}}}\Big], \\
\cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots
\end{array}
\right.
$$

et si l'on fait sur la fonction (C) u fois la substitution (k), on aura une fonction symétrique de ces fonctions

$$(G)\left\{\begin{array}{l}
\varphi\left[(x'_0),\quad x_{1+u},\quad x_{\frac{1}{\omega}+u},\quad x_{\frac{1}{\omega^2}+u},\quad x_{\frac{1}{\omega^3}+u},\ldots,\quad x_{\frac{1}{\omega^{p-2}}+u}\right],\\
\varphi\left[(x_{1+u}),\quad x_{\frac{1}{2}+u},\quad x_{\frac{1}{1+\omega}+u},\quad x_{\frac{1}{1+\omega^2}+u},\quad x_{\frac{1}{1+\omega^3}+u},\ldots,\quad x_{\frac{1}{1+\omega^{p-2}}+u}\right],\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\varphi\left[\left(x_{\frac{1}{r}+u}\right),\quad x_{\frac{1}{r+1}+u},\quad x_{\frac{1}{r+\omega}+u},\quad x_{\frac{1}{r+\omega^2}+u},\quad x_{\frac{1}{r+\omega^3}+u},\ldots,\quad x_{\frac{1}{r+\omega^{p-2}}+u}\right],\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{array}\right.$$

Nous avons à démontrer que t étant quelconque et u convenablement choisi, les fonctions (E) sont égales aux fonctions (G) prises dans un certain ordre.

Si la première des fonctions (E) est égale à la $(r+1)^{ième}$ des fonctions (G), c'est que l'on a

$$x_0 = x_{\frac{1}{r}+u},\quad x'_{1+t} = x_{\frac{1}{r+\omega^\sigma}+u},\quad x'_{\frac{1}{\omega}+t} = x_{\frac{1}{r+\omega^{\sigma+1}}+u},$$

$$x'_{\frac{1}{\omega^2}+t} = x_{\frac{1}{r+\omega^{\sigma+2}}+u},\ldots,\qquad x'_{\frac{1}{\omega^k}+t} = x_{\frac{1}{r+\omega^{\sigma+k}}+u},\ldots,$$

d'où les congruences

$$(l)\qquad\left.\begin{array}{r}
\frac{1}{r}+u\equiv 0,\\
(1+t)\left(\frac{1}{r+\omega^\sigma}+u\right)\equiv 1,\\
\left(\frac{1}{\omega}+t\right)\left(\frac{1}{r+\omega^{\sigma+1}}+u\right)\equiv 1,\\
\cdots\cdots\cdots\cdots\cdots\\
\left(\frac{1}{\omega^k}+t\right)\left(\frac{1}{r+\omega^{\sigma+k}}+u\right)\equiv 1,\\
\cdots\cdots\cdots\cdots\cdots
\end{array}\right\}\pmod{p}.$$

Au moyen des trois premières congruences, on trouve

$$(m) \qquad u \equiv \frac{1}{t}, \quad r \equiv -t, \quad \omega^{\sigma} \equiv -t^2 \pmod{p},$$

et ces valeurs satisfont effectivement à la congruence générale (l). Ainsi la première des fonctions (E) est égale à la $(r+1)^{ième}$ des fonctions (G), si u et r ont les valeurs (m).

Recherchons maintenant si, u étant $\equiv \frac{1}{t}$, toutes les fonctions (E) sont égales aux fonctions (G); voyons donc si la deuxième des fonctions (E) est égale à la $(r+1+\tau)^{ième}$ des fonctions (G), la troisième des fonctions (E) égale à la $(r+1+2\tau)^{ième}$ des fonctions (G), etc., et, en général, si la $(\rho+1)^{ième}$ des fonctions (E) est égale à la $(r+1+\rho\tau)^{ième}$ des fonctions (G).

Si la $(\rho+1)^{ième}$ des fonctions (E) est égale à la $(r+1+\rho\tau)^{ième}$ des fonctions (G), on a

$$x'_{\frac{1}{\rho}+t} = x_{\frac{1}{r+\rho\tau}+u}, \qquad x'_{\frac{1}{\rho+1}+t} = x_{\frac{1}{r+\rho\tau+\omega^{\sigma}}+u},$$

$$x'_{\frac{1}{\rho+\omega}+t} = x_{\frac{1}{r+\rho\tau+\omega^{\sigma}+1}+u}, \ldots, \qquad x'_{\frac{1}{\rho+\omega^{k}}+t} = x_{\frac{1}{r+\rho\tau+\omega^{\sigma}+k}+u}, \ldots$$

ce qui donne les congruences

$$(n) \qquad \left.\begin{aligned} \left(\frac{1}{\rho}+t\right)\left(\frac{1}{r+\rho\tau}+u\right) &\equiv 1 \\ \left(\frac{1}{\rho+\omega^{0}}+t\right)\left(\frac{1}{r+\rho\tau+\omega^{\sigma}}+u\right) &\equiv 1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ \left(\frac{1}{\rho+\omega^{k}}+t\right)\left(\frac{1}{r+\rho\tau+\omega^{\sigma+k}}+u\right) &\equiv 1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots & \end{aligned}\right\} \pmod{p}.$$

Quel que soit ρ, la congruence (n) est satisfaite pour les valeurs (m) de r, u et ω^{σ} et pour $\tau \equiv -t^2$. Il est donc enfin démontré que la fonction Θ est trois fois transitive et n'est pas changée par les substitutions (h), (i) et (k).

Remplaçons x_0' par x_∞; la fonction Θ est invariable par les trois substitutions (i), (k), (h) qui peuvent s'écrire

$$(x_z\, x_{\omega z}),\quad (x_z\, x_{z+1}),\quad \left(x_z\, x_{\frac{z}{1+z}}\right);$$

toutes les substitutions qui laissent cette fonction invariable sont donc de la forme $\left(x_z\, x_{\frac{Az+B}{Cz+D}}\right)$; cette expression a p^3 valeurs, mais en supprimant les p valeurs de cette expression qui changeraient z en une constante et qui par conséquent ne peuvent représenter des substitutions, il en reste $p^3 - p$ ou $(p-1)p(p+1)$; par conséquent toutes les substitutions $\left(x_z\, x_{\frac{Az+B}{Cz+D}}\right)$ laissent la fonction Θ invariable.

Soint P et P′ deux fonctions semblables à Θ, et soit χ la fonction des mêmes variables qui a deux valeurs. La fonction $P + P'\chi$ est une fonction qui a $1.2\ldots(p-2)\times 2$ valeurs et qui est invariable par les substitutions

$$(x_z\, x_{\omega^2 z}),\quad (x_z\, x_{z+1}),\quad \left(x_z\, x_{\frac{z}{1+z}}\right);$$

cette fonction est évidemment deux fois transitive.

La fonction $P + P'\chi$ est invariable par la puissance deuxième d'une quelconque des substitutions $\left(x_z\, x_{\frac{Az+B}{Cz+D}}\right)$; or la puissance deuxième de $\left(x_z\, x_{\frac{Az+B}{Cz+D}}\right)$ est

$$\left(x_z\, x_{\frac{(A^2+BC)z+B(A+D)}{C(A+D)z+(CB+D^2)}}\right),$$

et l'on a

$$(A^2 + BC)(CB + D^2) - BC(A + D)^2 = (AD - BC)^2;$$

donc la fonction $P + P'\chi$ est invariable par toutes les substitutions $\left(x_z\, x_{\frac{Az+B}{Cz+D}}\right)$ pour lesquelles $AD - BC$ est un résidu quadratique.

Étude des substitutions $\left(x_z\, x_{\frac{Az+B}{Cz+D}}\right)$.

Si par la substitution

$$(p) \qquad \left(x_z\, x_{\frac{Az+B}{Cz+D}}\right)$$

la variable x_k n'a pas été déplacée, on a

$$k \equiv \frac{Ak+B}{Ck+D} \pmod{p},$$

ce qui donne la congruence du second degré

$$Ck^2 - (A-D)k - B \equiv 0,$$

et

$$k \equiv \frac{A-D \pm \sqrt{(A+D)^2 - 4(AD-BC)}}{2C}.$$

D'après cela, si l'on a

$$(A+D)^2 - 4(AD-BC) \equiv 0,$$

une seule lettre restera immobile et la substitution s'effectuera sur p variables. Si $(A+D)^2 - 4(AD-BC)$ est un résidu quadratique, deux lettres resteront immobiles et la substitution s'effectuera sur $p-1$ variables. Enfin si $(A+D)^2 - 4(AD-BC)$ est un non-résidu, la substitution s'effectuera sur $p+1$ variables.

Reportons-nous au mode de formation de la fonction Θ. La fonction Θ est une fonction symétrique de $p+1$ fonctions Φ, et, sauf la fonction (B), toutes ces fonctions se déduisent de la fonction

$$(C) \qquad \Phi(x_0, x_1, x_{\omega^{p-2}}, \ldots, x_{\omega^2}, x_\omega) = \Phi'_0,$$

en faisant sur celle-ci les substitutions $(x_z x_z)$, $(x_z x_{z+1})$, $(x_z x_{z+2})$, etc.; désignons ces fonctions respectivement par Φ'_0, Φ'_1, $\Phi'_2, \ldots, \Phi'_{p-1}$ et représentons par Φ_0 la fonction (B).

De même que les substitutions qui laissent invariable la fonction Φ_0 laissent invariable la fonction Θ, toutes les substitutions qui laissent

invariables les fonctions $\Phi'_0, \Phi'_1, \Phi'_2, \ldots, \Phi'_{p-1}$ laissent aussi invariable la fonction Θ, et ce sont les seules substitutions de p et de $p-1$ variables qui ne changent pas cette fonction trois fois transitive.

Φ'_0 n'est pas changée par la substitution $\left(x_1 \, x_{\frac{1}{y+1}}\right)$; donc Φ'_u n'est pas changée par la substitution circulaire de p variables

$$(q) \qquad \left(x_{\frac{1}{y}+u} \, x_{\frac{1}{y+1}+u}\right) \quad \text{ou} \quad \left(x_z \, x_{\frac{(1+u)z-u^2}{z+1-u}}\right).$$

Nous avons p substitutions circulaires différentes en faisant

$$u = 0, 1, 2, \ldots, p-1;$$

en y ajoutant la substitution $(x_z x_{z+1})$, nous avons les $p+1$ substitutions circulaires de p lettres qui laissent la fonction Θ invariable.

Chacune de ces substitutions a $p-1$ puissances; on a donc p^2-1 substitutions de p lettres de la forme (p).

Cherchons maintenant les substitutions de $p-1$ variables. La fonction Φ'_u étant une fonction symétrique des fonctions (G) est invariable par les p substitutions circulaires de $p-1$ variables qui sont renfermées dans l'expression

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

et que l'on obtient en faisant

$$r = 0, 1, 2, \ldots, p-1.$$

En donnant aussi à u les valeurs $0, 1, 2, \ldots, p-1$ dans cette expression on obtiendra p^2 substitutions; mais il est aisé de voir que ces substitutions ne sont pas toutes distinctes, et qu'il y en a qui sont les inverses des autres.

Les deux variables qui ne se trouvent pas dans la substitution (r) sont x_u et $x_{\frac{1}{r}+u}$; pareillement les deux variables qui ne sont pas permutées par

$$(s) \qquad \left(x_{\frac{1}{r'+1}+u'} \, x_{\frac{1}{r'+\omega}+u'} \, x_{\frac{1}{r'+\omega^2}+u'} \ldots x_{\frac{1}{r'+\omega^{p-2}}+u'}\right)$$

sont $x_{u'}$ et $x_{\frac{1}{r'}+u'}$. Donc pour que ces deux substitutions s'effectuent sur les mêmes variables, il faut que l'on ait

$$x_u = x_{\frac{1}{r'}+u'}, \qquad x_{\frac{1}{r}+u} = x_{u'};$$

ce qui donne

$$u \equiv \frac{1}{r'} + u', \quad \frac{1}{r} + u \equiv u' \pmod{p}$$

ou

$$(t) \qquad r' = p - r, \quad u' \equiv \frac{1}{r} + u.$$

r' et u' ayant les valeurs ainsi déterminées, la substitution (s) est l'inverse de la substitution (r); ainsi ω^ν étant une quantité à déterminer, on a

$$x_{\frac{1}{r+1}+u} = x_{\frac{1}{r'+\omega^\nu}+u'}, \qquad x_{\frac{1}{r+\omega}+u} = x_{\frac{1}{r'+\omega^{\nu-1}}+u'},$$

$$x_{\frac{1}{r+\omega^2}+u} = x_{\frac{1}{r'+\omega^{\nu-2}}+u'}, \ldots, \qquad x_{\frac{1}{r+\omega^k}+u} = x_{\frac{1}{r'+\omega^{\nu-k}}+u'}, \ldots;$$

car cela revient aux congruences

$$\frac{1}{r+1} + u \equiv \frac{1}{r'+\omega^\nu} + u',$$

$$\frac{1}{r+\omega} + u \equiv \frac{1}{r'+\omega^{\nu-1}} + u',$$

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

$$\frac{1}{r+\omega^k} + u \equiv \frac{1}{r'+\omega^{\nu-k}} + u', \ldots,$$

et si l'on remplace r' et u' par leurs valeurs (t), ces congruences sont satisfaites pour $\omega^\nu \equiv -r^2$.

Les valeurs (t) ne sont plus admissibles dans le cas particulier où on a $r \equiv 0$, car u' serait infini; dans ce cas la substitution (r) a pour inverse la substitution $(x_{1+u}\, x_{\omega+u}\, x_{\omega^2+u} \ldots x_{\omega^{p-2}+u})$ qui ne change pas la fonction Φ_0.

D'après cela si dans la substitution (r) nous donnons à r les valeurs

0, 1, 2,..., $\frac{p-1}{2}$, et à u les valeurs 0, 1, 2,..., $p-1$, nous aurons $\frac{p(p+1)}{2}$ substitutions circulaires distinctes de $p-1$ variables.

La substitution (r) peut s'écrire $\left(x_{\frac{1}{r+y}+u}\; x_{\frac{1}{r+\omega y}+u}\right)$, ou, en faisant $\frac{1}{r+y}+u \equiv z$,

$$(u) \qquad \left[x_z\; x_{\frac{\left(\frac{1}{1-\omega}+ru\right)z-u(1+ur)}{rz-ru+\frac{\omega}{1-\omega}}}\right],$$

et en faisant dans cette expression $r = 0, 1, 2,..., \frac{p-1}{2}$ et $u = 0, 1, 2,..., p-1$, on aura les $\frac{p(p+1)}{2}$ substitutions circulaires de $p-1$ variables qui ne changent pas Θ.

En comptant les puissances de ces substitutions, on aura $\frac{p(p+1)(p-2)}{2}$ substitutions de $p-1$ variables qui ne changent pas Θ.

La puissance $\alpha^{ième}$ de la substitution (r) ou (u) est $\left(x_{\frac{1}{r+y}+u}\; x_{\frac{1}{r+\omega^\alpha y}+u}\right)$, ou

$$(u') \qquad \left[x_z\; x_{\frac{\left(\frac{1}{1-\omega^\alpha}+ru\right)z-u(1+ur)}{rz-ru+\frac{\omega^\alpha}{1-\omega^\alpha}}}\right],$$

et remarquons que la substitution (u') comme la substitution (u) ne contient pas les deux variables x_u et $x_{\frac{1}{r}+u}$.

Dans l'expression (u') la quantité $(A+D)^2 - 4(AD-BC)$ est $\equiv 1$, et par conséquent il est vérifié que c'est un résidu quadratique.

Cherchons maintenant les substitutions circulaires de $p+1$ variables. Remarquons d'abord que l'expression (u) peut donner la substitution (q) de p variables; pour cela divisons par r les deux termes de la fraction qui entre dans l'expression (u), la variable $x_{\frac{1}{r}+u}$ coïncidant

avec x_u, nous ferons $r = \infty$, et nous voyons alors que l'expression (u) donne la substitution (q), si l'on fait

$$\omega \equiv 1, \quad r(1-\omega) \equiv 1.$$

La formule (u) peut aussi évidemment représenter les substitutions circulaires de $p+1$ variables, si l'on modifie convenablement le sens des quantités qui y entrent. Ainsi x_u et $x_{\frac{1}{r}+u}$ cessent d'exister; donc u et $\frac{1}{r}+u$ sont des imaginaires. Afin que la substitution soit d'ordre $p+1$, prenons pour ω une racine primitive de la congruence $\omega^{p+1} \equiv 1$, r et u seront alors des imaginaires telles, que $\frac{1}{r(1-\omega)}+u$, $u\left(\frac{1}{r}+u\right)$, $-u+\frac{\omega}{r(1-\omega)}$ soient des nombres entiers réels. Posons d'après cela les congruences

$$(\rho) \quad \frac{1}{r(1-\omega)}+u \equiv \frac{A}{C}, \quad -u\left(\frac{1}{r}+u\right) \equiv \frac{B}{C}, \quad -u+\frac{\omega}{r(1-\omega)} \equiv \frac{D}{C},$$

A, B, C, D étant des nombres entiers réels. On tire de ces congruences

$$(w) \qquad \frac{AD-BC}{(A+D)^2} \equiv \frac{\omega}{(1+\omega)^2} \pmod{p}.$$

Posons

$$(H) \qquad \frac{AD-BC}{(A+D)^2} \equiv \frac{1}{k+2},$$

la congruence (w) deviendra

$$(I) \qquad \omega^2 - k\omega + 1 \equiv 0.$$

Cette congruence étant irréductible, ses racines peuvent être représentées par ω et par ω^p, de sorte que l'on a $\omega^{p+1} \equiv 1$.

D'après cela, on cherchera une racine primitive de la congruence $x^{p+1} \equiv 1 \pmod{p}$; cette racine sera $\omega = \alpha + \beta\sqrt{-1}$, on l'ajoutera à son inverse $\alpha - \beta\sqrt{-1}$; soit k la somme : ces deux racines primitives sont les racines de (I).

k étant déterminé, on calculera A, B, C, D de manière qu'ils satisfassent à la congruence (H); remarquons que AD — BC est un non-résidu, puisqu'une substitution circulaire de $p+1$ variables change la fonction qui a deux valeurs; donc, d'après la congruence (H), $k+2$ est aussi non-résidu, et l'on satisfera à cette congruence en posant

$$AD - BC \equiv k+2, \quad A+D \equiv k+2;$$

on en tirera

$$(K) \qquad B \equiv \frac{-A^2+(A-1)(k+2)}{C}, \quad D \equiv k+2-A.$$

Ces dernières formules ont été données par M. Serret, dans une étude de ces substitutions. (*Comptes rendus de l'Académie des Sciences*, du 17 janvier 1859.)

On aura ainsi les valeurs de B et D au moyen de celles de A et C, et la substitution circulaire de $p+1$ variables aura la forme (p), A, B, C, D étant des nombres entiers réels.

Il n'est peut-être pas inutile de démontrer ici que les substitutions que l'on obtient de la sorte sont bien des substitutions circulaires de $p+1$ variables. Les substitutions considérées peuvent s'écrire

$$(L) \qquad \left[x_z \; x^{\frac{\left(\frac{1}{r(1-\omega)}+u\right)z-u\left(\frac{1}{r}+u\right)}{z-u+\frac{\omega}{r(1-\omega)}}} \right],$$

ω étant une racine primitive de $x^{p+1} \equiv 1$, et u et r ayant les valeurs

$$(M) \qquad u \equiv \frac{(A-1)\omega-1}{C\omega}, \quad \frac{1}{r} \equiv \frac{1-\omega^2}{C\omega},$$

que l'on tire des congruences (ν). Donc, de même que la substitution (u) est identique à la substitution (r), la substitution (L) peut se mettre sous la forme

$$(N) \qquad \left(x^{\frac{1}{r+1}+u} \; x^{\frac{1}{r+\omega}+u} \; x^{\frac{1}{r+\omega^2}+u} \; \dots \; x^{\frac{1}{r+\omega^p}+u} \right),$$

ce qui est évidemment une substitution circulaire de $p+1$ variables.

Dans les expressions (K), nous pouvons donner à A les valeurs 0, 1, 2,..., $p-1$; ce qui nous donnera $p(p-1)$ substitutions de $p+1$ variables; mais elles ne sont pas toutes distinctes, car $\frac{p(p-1)}{2}$ de ces substitutions sont les inverses des $\frac{p(p-1)}{2}$ autres. En effet, la substitution

$$(\mathrm{N}') \qquad \left(x_{\frac{1}{r'+1}+u'} \; x_{\frac{1}{r'+\omega}+u'} \; x_{\frac{1}{r'+\omega^2}+u'} \; \dots \; x_{\frac{1}{r'+\omega^p}+u'} \right)$$

est l'inverse de la substitution (N), si l'on a

$$u \equiv \frac{1}{r'} + u', \quad \frac{1}{r} + u \equiv u',$$

et cela est évidemment prouvé par le raisonnement qui a servi à démontrer que la substitution (s) est l'inverse de (r), si ces deux congruences ont lieu. Représentons la substitution (N') par $\left(x_z \, x_{\frac{A'z+B'}{C'z+D'}} \right)$, et remplaçons dans les deux dernières congruences u et r par leurs valeurs (M), u' et r' par leurs valeurs analogues; ces deux congruences jointes à ces deux-ci :

$$B' \equiv \frac{-A'^2+(A'-1)(k+2)}{C'}, \quad D' \equiv k+2-A',$$

donneront

$$A' \equiv D, \quad B' \equiv -B, \quad C' \equiv -C, \quad D' \equiv A.$$

Il suit de là que si dans les congruences (K) on donne A les valeurs 0, 1, 2,..., $p-1$, et à C seulement les valeurs 1, 2,..., $\frac{p-1}{2}$, on aura les $\frac{p(p-1)}{2}$ substitutions circulaires distinctes de $p+1$ variables.

En formant les puissances de ces substitutions, nous aurons $\frac{p^2(p-1)}{2}$ substitutions régulières de $p+1$ variables.

Ajoutons à toutes les substitutions que nous avons trouvées, la substitution $(x_z \, x_z)$, et nous reconnaissons que leur nombre est

$(p-1)\,p(p+1)$; nous vérifions ainsi que nous avons considéré toutes les substitutions (p).

Fonctions transitives de p^ν variables, p étant premier. — Fonction trois fois transitive de $p^\nu+1$ variables qui a $1.2\ldots(p^\nu-2)$ valeurs et fonction deux fois transitive de $p^\nu+1$ variables, qui a $1.2\ldots(p^\nu-2)\times 2$ valeurs.

Soient p un nombre premier, et i une racine d'une congruence irréductible du degré ν, $F(x)\equiv 0\,(\text{mod. } p)$: considérons l'expression

$$(1)\qquad \alpha_0+\alpha_1 i+\alpha_2 i^2+\ldots+\alpha_{\nu-1} i^{\nu-1},$$

dans laquelle on prend les valeurs de α_0, α_1, α_2, etc., qui sont entières par rapport au module p; cette expression est susceptible de p^ν valeurs distinctes, et, sauf la valeur zéro, ces p^ν valeurs satisfont à la congruence binôme

$$(2)\qquad z^{p^\nu-1}-1\equiv 0\,(\text{mod. } p).$$

Soit β une de ces $p^\nu-1$ valeurs; posons

$$\beta^n\equiv 1\,(\text{mod. } p);$$

le plus petit nombre n pour lequel a lieu cette congruence est un diviseur de $p^\nu-1$. Si ce nombre n est égal à $p^\nu-1$, β est dite *racine primitive* de la congruence (2) [*].

Ces principes, qui sont dus à Galois, ayant été rappelés, nous voyons que nous aurons p^ν variables en mettant comme indices à la lettre x les p^ν quantités (1), et en répétant presque littéralement les raisonnements que nous venons de faire, nous pouvons étendre aux fonctions de p^ν et de $p^\nu+1$ variables, les théorèmes que nous avons démontrés pour les fonctions de p et de $p+1$ variables. Nous allons donc reprendre très-rapidement ces propositions.

Soit m une quelconque des quantités (1), la substitution $(x_z\,x_{z+m})$ est une substitution régulière composée de $p^{\nu-1}$ cycles de p lettres. Soit λ une fonction quelconque; faisons sur λ les p^ν substitutions $(x_z\,x_{z+m})$,

[*] J.-A. Serret, *Algèbre supérieure*, 25e leçon.

nous obtiendrons les p^ν fonctions $\lambda, \lambda_1, \lambda_2, \ldots, \lambda_{p^\nu-1}$; formons une fonction symétrique ψ de ces p^ν fonctions, nous aurons une fonction transitive invariable par toutes les substitutions $(x_z\, x_{z+m})$.

Soient ω une racine primitive de la congruence (2), et u un diviseur de $p^\nu - 1$, faisons sur la fonction ψ la substitution régulière $(x_z\, x_{\omega^u z})$ et ses puissances, nous aurons les $\frac{p^\nu - 1}{u}$ fonctions $\psi, \psi_1, \psi_2, \ldots$, et en formant une fonction symétrique de ces fonctions, nous aurons une fonction Ψ invariable par toutes les substitutions $(x_z\, x_{a^u z+b})$, a et b étant de la forme (1).

D'après cela, p étant un nombre premier et u un diviseur de $p^\nu - 1$, il y a toujours une fonction transitive de p^ν variables qui a

$$1.2\ldots(p^\nu - 2) \times u \text{ valeurs.}$$

Dans le cas où u est égal à 1, cette fonction est deux fois transitive.

Soit φ une fonction invariable par la substitution régulière $(x_z\, x_{\omega^u z})$; faisons sur φ toutes les substitutions $(x_z\, x_{z+m})$, et formons une fonction symétrique Φ des fonctions ainsi obtenues, Φ est aussi une fonction invariable par toutes les substitutions $(x_z\, x_{a^u z+b})$.

Désignons par

$$\Phi\left(x_0, x_1, x_\omega, x_{\omega^2}, \ldots, x_{\omega^{p^\nu-2}}\right),$$

une fonction deux fois transitive invariable par toutes les substitutions $(x_z\, x_{az+b})$; faisons sur cette fonction toutes les substitutions $(x'_z\, x'_{z+m})$, x'_z étant égal à $x_{\frac{1}{\alpha}}$; nous obtiendrons ainsi p^ν fonctions; ajoutons-y la fonction

$$\Phi\left(x'_0, x_1, x_{\omega^{p^\nu-2}}, x_{\omega^{p^\nu-3}}, \ldots, x_\omega\right);$$

enfin, formons une fonction symétrique de ces $p^\nu + 1$ fonctions, nous aurons une fonction trois fois transitive Θ invariable par toutes les substitutions

$$\left(x_z\ x_{\frac{Az+B}{Cz+D}}\right), \tag{3}$$

A, B, C, D étant des quantités de la forme (1).

Soient P et P′ deux fonctions semblables à Θ, et soit χ la fonction des mêmes variables qui n'a que deux valeurs. Si p est un nombre premier autre que 2, $P + P'\chi$ est une fonction deux fois transitive qui a $1.2\ldots(p^\nu - 2) \times 2$ valeurs, et qui est invariable par toutes les substitutions pour lesquelles AD — BC est résidu quadratique.

Parlons maintenant des substitutions (3). Considérons la quantité

$$(A + D)^2 - 4(AD - BC). \tag{4}$$

Si cette quantité est $\equiv 0$, la substitution (3) s'effectue sur p^ν variables. Si p est différent de 2, la quantité (4) est un résidu quadratique, quand la substitution s'effectue sur $p^\nu - 1$ variables. Si p est différent de 2, la quantité (4) est un non-résidu, quand la substitution s'effectue sur $p^\nu + 1$ variables.

Toutes les substitutions de p^ν variables sont des substitutions régulières composées de $p^{\nu-1}$ cycles de p lettres; elles sont renfermées dans les deux formules

$$\left[x_z\, x_{\frac{(1+ur)z - u^2 r}{rz + 1 - ur}}\right], \quad (x_z\, x_{z+u}).$$

Les substitutions circulaires distinctes de $p^\nu - 1$ variables sont toutes comprises dans l'expression

$$\left[x_z\, x_{\frac{\left(\frac{1}{1-\omega} + ru\right)z - u(1+ur)}{rz - ru + \frac{\omega}{1-\omega}}}\right], \tag{5}$$

ω étant une racine primitive de (2). En donnant à u et r les p^ν valeurs dont ils sont susceptibles, on aurait $p^{2\nu}$ substitutions circulaires de $p^\nu - 1$ variables; mais groupons ces substitutions deux à deux, de manière que si u et r ont les valeurs u' et r' pour l'une des substitutions, et les valeurs u'' et r'' pour l'autre, on ait

$$u' \equiv \frac{1}{r''} + u'', \quad \frac{1}{r'} + u' \equiv u'';$$

les substitutions de chaque groupe seront inverses l'une de l'autre, et par conséquent il suffira de prendre une substitution de chacun de

ces groupes. Il faut toutefois remarquer que les p^ν substitutions pour lesquelles r est $\equiv 0$, ne peuvent être groupées avec aucune autre; l'expression (5) donne donc $\frac{p^\nu(p^\nu+1)}{2}$ substitutions circulaires distinctes.

La puissance $\alpha^{ième}$ de la substitution (5) s'obtient en changeant ω en ω^α.

Occupons-nous enfin des substitutions circulaires de $p^\nu+1$ variables. Ces substitutions seront encore données par l'expression

$$\left[\begin{array}{c} x_z \quad x^{\frac{\left(\frac{1}{r(1-\omega)}+u\right)z-u\left(\frac{1}{r}+u\right)}{z-u+\frac{\omega}{r(1-\omega)}}} \end{array}\right];$$

mais alors ω sera une racine primitive de $\omega^{p^\nu+1}\equiv 1$, et r et u seront des imaginaires de la forme $\mu_0+\mu_1\omega$, μ_0 et μ_1 étant des quantités de la forme (1). De plus, r et u devront être tels, que l'on ait

$$\frac{1}{r(1-\omega)}+u\equiv\frac{A}{C},\quad -u\left(\frac{1}{r}+u\right)\equiv\frac{B}{C},\quad -u+\frac{\omega}{r(1-\omega)}\equiv\frac{D}{C},$$

A, B, C, D étant des nombres de la forme (1).

On tire de ces congruences

$$\frac{AD-BC}{(A+D)^2}\equiv\frac{\omega}{(1+\omega)^2}; \tag{6}$$

on peut poser

$$\frac{AD-BC}{(A+D)^2}\equiv\frac{1}{k+2}, \tag{7}$$

k étant un nombre de même forme que A, B, C, D, et la congruence (6) devient

$$\omega^2-k\omega+1\equiv 0. \tag{8}$$

Cette congruence doit être irréductible, et à cause de la forme de k, ses deux racines peuvent être représentées par ω et ω^{p^ν}, de sorte que l'on a $\omega^{p^\nu+1}\equiv 1 \pmod{p}$. On cherchera donc une racine primitive de la congruence $z^{p^\nu+1}\equiv 1 \pmod{p}$, on l'ajoutera à la racine primitive

inverse; soit k leur somme : ces deux racines primitives sont les racines de la congruence (8).

k étant ainsi déterminé, on calculera A, B, C, D de manière qu'ils satisfassent à la congruence (7); à cet effet on posera

$$AD - BC \equiv k + 2, \quad A + D \equiv k + 2,$$

et l'on en tirera

$$B \equiv \frac{-A^2 + (A - 1)(k + 2)}{C}, \quad D \equiv k + 2 - A.$$

On aura ainsi les valeurs de B et D au moyen de celles de A et C, et la substitution circulaire de $p^\nu + 1$ variables aura la forme (3), A, B, C, D étant des nombres de la forme (1).