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

ÉMILE MATHIEU

Sur la fonction cinq fois transitive de 24 quantités

Journal de mathématiques pures et appliquées 2^e série, tome 18 (1873), p. 25-46.
<http://www.numdam.org/item?id=JMPA_1873_2_18__25_0>

Sur la fonction cinq fois transitive de 24 quantités;

PAR M. ÉMILE MATHIEU.

Dans mon Mémoire *sur les fonctions de plusieurs quantités* publié dans le tome VI de ce Journal, en 1861, j'ai déclaré (p. 274) que je possédais une fonction cinq fois transitive de 24 quantités, dont j'ai donné en même temps le nombre des valeurs distinctes.

Si j'avais indiqué deux substitutions qui la laissent invariable et qui la caractérisent complétement, il eût été facile de vérifier son existence; mais, au contraire, la seule indication du nombre de ses valeurs distinctes ne jette aucune lumière sur la formation de cette fonction. Aussi aucun géomètre n'a-t-il essayé, depuis cette époque, de la déterminer, et je me propose maintenant de prouver qu'elle existe effectivement et de montrer, de plus, comment je suis parvenu à la découvrir.

Si je n'ai point publié cette fonction dans le Mémoire cité, c'est que la méthode que je devais employer pour la faire connaître n'avait ni la netteté, ni l'élégance de mes autres résultats. Cependant cette méthode ne paraîtra pas sans intérêt à ceux qui se représenteront qu'il eût été bien difficile de découvrir autrement la fonction qui va nous occuper.

Indication du procédé de la recherche.

1. Désignons par p un nombre premier et représentons p quantités par $x_0, x_1, x_2, \ldots, x_{p-1}$, en convenant que, si m et n sont deux entiers, on a $x_m = x_n$ toutes les fois que m est congru à n suivant le module p. Il existe des fonctions transitives de ces quantités qui sont invariables

seulement par des substitutions de la forme

$$(x_z,\ x_{az+b});$$

comme ces fonctions transitives sont évidentes, ainsi que la fonction symétrique et celle qui a deux valeurs, il sera entendu, quand nous parlerons, dans ce qui va suivre, de fonctions transitives de p lettres, qu'on laisse de côté ces fonctions connues.

Cela posé, soit une fonction transitive d'un nombre premier p de quantités, et supposons que $\frac{p-1}{2}$ soit aussi un nombre premier q; j'ai démontré dans le Mémoire cité (Chap. IV), que, en désignant les p quantités dans un ordre convenable par $x_0, x_1, \ldots, x_{p-1}$, la fonction est invariable non-seulement par la substitution circulaire

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

mais encore par la substitution

$$(B) \qquad (x_1, x_{g^2}, x_{g^4}, \ldots, x_{g^{p-1}})(x_g, x_{g^3}, x_{g^5}, \ldots, x_{g^{p-2}}),$$

g étant une racine primitive de p; par suite, elle est invariable par les $\frac{p(p-1)}{2}$ substitutions dérivées, comprises dans la formule

$$(z, a^2z + b),$$

a et b étant quelconques.

Or voici le principe sur lequel je me suis appuyé pour déterminer la fonction dont il s'agit.

Représentons la substitution (B) *par*

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

et faisons

$$x'_0 = x_1, \quad x'_1 = x_{g^2}, \quad x'_2 = x_{g^4}, \ldots, \quad x'_{q-1} = x_{g^{p-1}};$$

alors, si le second cycle de (B) *est convenablement identifié avec le*

second cycle de (C), *la fonction transitive est nécessairement invariable par une substitution régulière de* $p-3$ *quantités de la forme*

$$(D) \qquad (x'_z, x'_{\gamma^u z})(x''_z, x''_{\gamma^u z}),$$

γ *étant une racine primitive de* q, u *un diviseur de* $q-1$, *plus petit que* $q-1$, *et les indices étant pris suivant le module* q.

Avant d'appliquer ce principe à la recherche d'une fonction transitive de 23 lettres, appliquons-le à la détermination des fonctions transitives de 7 et de 11 lettres, puisque $\frac{7-1}{2}$ et $\frac{11-1}{2}$ sont des nombres premiers.

Des fonctions transitives de 7 *et de* 11 *lettres.*

2. D'après ce que nous venons de rappeler, toute fonction transitive des 7 quantités $x_0, x_1, x_2, \ldots, x_6$ peut être considérée comme invariable par les substitutions

$$(z, z+1) \quad \text{et} \quad (z, 3^2 z),$$

ou par les substitutions

$$(e) \qquad (x_0, x_1, x_2, x_3, x_4, x_5, x_6),$$

$$(f) \qquad (x_1, x_2, x_4)(x_3, x_6, x_5).$$

Mettons cette dernière substitution sous la forme

$$(g) \qquad (x'_0, x'_1, x'_2)(x''_0, x''_1, x''_2),$$

et nous aurons pour la substitution (D)

$$(h) \qquad (x'_1, x'_2)(x''_1, x''_2).$$

Pour identifier (f) et (g), on commencera par faire

$$x'_0 = x_1, \quad x'_1 = x_2, \quad x'_2 = x_4,$$

et l'on aura, par la considération des seconds cycles, les trois hypothèses suivantes :

1° $x''_0 = x_3, \quad x''_1 = x_6, \quad x''_2 = x_5;$

2° $x''_0 = x_6, \quad x''_1 = x_5, \quad x''_2 = x_3;$

3° $x''_0 = x_5, \quad x''_1 = x_3, \quad x''_2 = x_6.$

Et, d'après cela, la substitution (h) sera une des trois qui suivent :

1° $(x_2 x_4)(x_6 x_5),$

2° $(x_2 x_4)(x_5 x_3),$

3° $(x_2 x_4)(x_3 x_6).$

Une quelconque des substitutions 1°, 2°, 3°, combinée avec (e) et (f), donne un système de $4 \times 6 \times 7$ substitutions conjuguées, qui appartient à une fonction deux fois transitive qui a $\frac{2.3.4.5}{4} = 30$ valeurs. Ces trois systèmes de substitutions conjuguées ou les trois fonctions correspondantes ne diffèrent que par la manière de désigner les 7 quantités.

Considérons, par exemple, la première de ces trois fonctions. D'après les substitutions (f) et 1°, on voit immédiatement qu'elle est transitive par rapport aux 6 quantités $x_1, x_2, x_3, x_4, x_5, x_6$; puis, considérée comme fonction des 5 quantités $x_2, x_3, \ldots, x_6$, elle est non-seulement invariable par 1°, mais encore par

$$(x_2 x_6)(x_4 x_5);$$

la fonction est donc transitive par rapport à x_2, x_4, x_6, x_5, et elle a bien 30 valeurs.

D'après un théorème général, une fonction transitive étant nécessairement invariable par la substitution (f), il suffit, pour caractériser la fonction actuelle, de dire qu'elle est invariable par les substitutions (e) et 1°.

Désignons par x_∞ une huitième quantité; il existe une fonction des 8 lettres $x_0, x_1, \ldots, x_6, x_\infty$ qui, considérée comme fonction des 7 pre-

mières lettres, est identique à la fonction précédente, de sorte qu'elle est invariable par les substitutions (e) et 1°; elle est, de plus, invariable par toutes les substitutions

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

pour lesquelles $AD - BC$ est résidu quadratique de 7; elle sera caractérisée par les substitutions (e) et 1°, et une quelconque de ces dernières substitutions renfermant x_{∞}, par exemple la suivante :

$$\left(x_z x_{-\frac{1}{z}}\right) = (x_0 x_{\infty})(x_1 x_6)(x_2 x_3)(x_4 x_5).$$

Cette fonction trois fois transitive de 8 quantités est renfermée dans une famille de fonctions deux fois transitives de p^{ν} quantités, qui deviennent trois fois transitives pour $p = 2$ et qui ont $\frac{1.2\ldots p^{\nu}}{p^{\nu}(p^{\nu}-1)\ldots(p^{\nu}-p^{\nu-1})}$ valeurs. J'ai donné cette famille de fonctions dans le Chapitre III du Mémoire cité, et j'y ai donné une méthode très-élégante pour les former. J'ai montré aussi que ces fonctions devaient être employées comme résolvantes des équations dont le degré est une puissance d'un nombre premier. (Voir *Mémoire sur la résolution des équations*, dans les *Annali di Matematica pura ed applicata*, t. IV, 1862.)

3. Appliquons la même méthode à la détermination des fonctions transitives de 11 lettres.

D'abord toute fonction transitive de 11 quantités peut être considérée comme invariable par les substitutions

$$(z, z+1), \quad (z, 2^2 z),$$

ou par les substitutions

$$(k) \qquad (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}),$$

$$(l) \qquad (x_1, x_4, x_5, x_9, x_3)(x_2, x_8, x_{10}, x_7, x_6).$$

Représentons la dernière substitution par

$$(m) \qquad (x'_0, x'_1, x'_2, x'_3, x'_4)(x''_0, x''_1, x''_2, x''_3, x''_4);$$

identifions (m) avec (l) en commençant par poser

$$x'_0 = x_1, \quad x'_1 = x_4, \quad x'_2 = x_5, \quad x'_3 = x_9, \quad x'_4 = x_3,$$

et nous aurons à faire une des cinq suppositions suivantes :

1° $x''_0 = x_2, \quad x''_1 = x_8, \quad x''_2 = x_{10}, \quad x''_3 = x_7, \quad x''_4 = x_6;$

2° $x''_0 = x_8, \quad x''_1 = x_{10}, \quad x''_2 = x_7, \quad x''_3 = x_6, \quad x''_4 = x_2;$

3° $x''_0 = x_{10}, \quad x''_1 = x_7, \quad x''_2 = x_6, \quad x''_3 = x_2, \quad x''_4 = x_8;$

4° $x''_0 = x_7, \quad x''_1 = x_6, \quad x''_2 = x_2, \quad x''_3 = x_8, \quad x''_4 = x_{10};$

5° $x''_0 = x_6, \quad x''_1 = x_2, \quad x''_2 = x_8, \quad x''_3 = x_{10}, \quad x''_4 = x_7.$

La substitution

$$(D) \qquad (x'_z x'_{\gamma^u z})(x''_z x''_{\gamma^u z}),$$

dont les indices sont pris suivant le module 5, sera, en prenant $\gamma = 2$, suivant qu'on fera $u = 2$ ou $u = 1$,

$$(n) \qquad (x'_1 x'_4)(x'_2 x'_3)(x''_1 x''_4)(x''_2 x''_3),$$

ou

$$(p) \qquad (x'_1 x'_2 x'_4 x'_3)(x''_1 x''_2 x''_4 x''_3).$$

La substitution (n) est la deuxième puissance de la substitution (p). Donc le système de substitutions conjuguées déduit de (k) et (p) renferme évidemment le système de substitutions conjuguées déduit de (k) et (n); donc, si le système déduit de (k) et (p) donne une fonction transitive de 11 lettres, on est assuré que l'autre système en donne une aussi, tandis que la réciproque n'est pas évidente.

Commençons donc par nous occuper du système de substitutions conjuguées déduit de (k) et (n). D'après les cinq suppositions possibles, (n) est une des cinq substitutions suivantes :

1° $(x_4 x_3)(x_5 x_9)(x_8 x_6)(x_{10} x_7),$

2° $(x_4 x_8)(x_5 x_9)(x_{10} x_2)(x_7 x_6),$

3° $(x_4 x_8)(x_5 x_9)(x_7 x_8)(x_6 x_2),$

4° $(x_4 x_3)(x_5 x_9)(x_6 x_{10})(x_2 x_8),$

5° $(x_4 x_8)(x_5 x_9)(x_2 x_7)(x_8 x_{10}).$

Les substitutions 1°, 3°, 5° ne conviennent pas, c'est-à-dire que le système de substitutions conjuguées dérivées de (k) et d'une de ces trois substitutions n'est autre chose que les $\frac{1.2.3\ldots11}{2}$ substitutions qui laissent invariable la fonction des 11 lettres qui a deux valeurs seulement. Il faut montrer comment on pourra le reconnaître.

Cela est très-aisé si l'on veut bien se servir de ce principe, qui m'a servi bien des fois dans mes recherches, mais non dans mes démonstrations : c'est qu'une fonction transitive d'un nombre premier p de quantités ne peut être invariable par une substitution s'effectuant sur moins de $\frac{p+1}{2}$ quantités [*].

Considérons, par exemple, le système déduit de (k) et de 1°. Faisons 1° une fois, puis (k) deux fois, et formons le tableau

$$\begin{array}{cccccccccccc} 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, \\ 0, & 1, & 2, & 4, & 3, & 9, & 8, & 10, & 6, & 5, & 7, \\ 2, & 3, & 4, & 6, & 5, & 0, & 10, & 1, & 8, & 7, & 9, \end{array}$$

nous aurons fait, en définitive, la substitution

$$(0, 2, 4, 5)(1, 3, 6, 10, 9, 7),$$

qui fait partie du système de substitutions conjuguées; faisons cette dernière substitution six fois, nous aurons la substitution

$$(q) \qquad (0, 4)(2, 5),$$

qui fait aussi partie de ce système, et qui n'a que quatre lettres;

---

[*] Dans un Mémoire présenté à l'Académie des Sciences le 31 mai 1858, j'ai démontré le théorème suivant, qui pourrait également servir au but que l'on se propose ici : *Si une fonction transitive de n lettres est transitive par rapport à un certain nombre α de ses lettres qui n'est pas plus grand que $\frac{n}{2}$, ces n lettres peuvent se diviser en groupes composés chacun d'un même nombre de lettres, de manière que la fonction est transitive par rapport à ces groupes, qui sont transitifs.*

Mais, quoique je n'aie jamais douté de l'exactitude de ce théorème, la démonstration ne m'ayant pas pleinement satisfait, je ne l'ai jamais publié.

donc, d'après le principe ci-dessus, la substitution 1° doit être rejetée.

Si l'on ne veut pas employer ce principe, voici comment on pourra constater qu'il n'existe pas de fonctions transitives invariables par (k) et 1°. On déduira de ces deux substitutions quelques autres qui ne renferment pas une même lettre, x_0 par exemple. Le plus souvent, on pourra se contenter de deux substitutions qui ne renferment pas x_0; on constatera que la fonction est transitive par rapport aux lettres restantes $x_1, x_2, \ldots, x_{10}$. Des substitutions obtenues sur ces 10 quantités, déduisons-en quelques autres ne renfermant pas x_1, et constatons que la fonction, d'après ces dernières substitutions, est transitive par rapport aux 9 lettres $x_2, x_3, \ldots, x_{10}$. Déterminons ensuite des substitutions dérivées ne contenant pas x_2, et ainsi de suite. En continuant ainsi, on prouverait que la fonction est transitive par rapport à 10 lettres, puis à 9 prises parmi les précédentes, puis à 8 prises parmi ces dernières, puis à 7, enfin à 6 lettres.

Or une fonction de n lettres ne peut être plus de $\frac{n}{2}$ fois transitive lorsqu'elle a plus de deux valeurs (*voir* notre Mémoire *sur le nombre de valeurs que peut acquérir une fonction,* t. V de ce Journal, 1860, p. 18); donc la fonction considérée ne saurait avoir plus de deux valeurs.

Cette méthode est très-longue, mais elle peut se simplifier beaucoup. En effet, dans le cas actuel par exemple, la fonction est invariable par la substitution (q). Donc, aussitôt qu'on aura reconnu que la fonction est quatre fois transitive, on en pourra conclure qu'elle est transitive par rapport à 4 lettres quelconques, et qu'elle n'a que deux valeurs, puisqu'à la place des 4 lettres de la substitution (q) on peut amener dans la fonction 4 lettres quelconques.

On reconnaîtra ainsi que la substitution 1° doit être rejetée, et il en est de même pour les substitutions 3° et 5°. Reste à considérer les deux substitutions 2° et 4° qui conviennent.

La fonction caractérisée par (k) et 2° est deux fois transitive, et, considérée comme fonction des 9 quantités $x_2, x_3, \ldots, x_{10}$, elle est invariable seulement par les substitutions dérivées de

$$(r) \qquad (2, 4, 7)(3, 10, 6)(5, 8, 9)$$

et de la substitution 2° ou de

$$(4, 3)(5, 9)(10, 2)(7, 6);$$

les substitutions dérivées de ces deux dernières sont la puissance deuxième de (r) et ces deux autres

$$(7, 10)(8, 5)(6, 4)(2, 3),$$
$$(2, 6)(9, 8)(3, 7)(4, 10).$$

Donc, en permutant les 9 quantités $x_2, x_3, \ldots, x_{10}$, on obtient 6 valeurs égales de la fonction, et cette fonction, qui est deux fois transitive, a $\frac{1.2.3.4.5.6.7.8.9}{6} = 60480$ valeurs. Elle a été donnée pour la première fois par M. Kronecker.

La fonction transitive caractérisée par (k) et 4° est deux fois transitive, et, considérée comme fonction des 9 lettres $x_2, x_3, \ldots, x_{10}$, elle est invariable par la substitution

$$(7, 4, 3)(2, 6, 9)(8, 5, 10),$$

la substitution 4° et celles qui en sont dérivées. Il est facile de voir que cette fonction ne diffère de la précédente que par la manière de désigner les 11 quantités qu'elle renferme.

Ainsi, de l'examen de la substitution (n), il résulte qu'*il existe une fonction deux fois transitive de onze lettres qui a* 60480 *valeurs et caractérisée par les substitutions*

$$(E) \qquad (x_0, x_1, x_2, \ldots, x_{10}),$$

$$(H) \qquad (x_4, x_3)(x_5, x_9)(x_{10}, x_2)(x_7, x_6).$$

En y ajoutant une quelconque des substitutions

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

pour lesquelles AD — BC *est résidu quadratique de* 11 *et renfermant* x_∞, *par exemple*

$$\left(z, -\frac{1}{z}\right) = (0, \infty)(1, 10)(2, 5)(3, 7)(4, 8)(6, 9),$$

on aura les trois substitutions qui caractérisent une fonction trois fois transitive des douze quantités $x_\infty, x_0, x_1, \ldots, x_{10}$, qui, considérée comme fonction des onze dernières quantités, est identique à la fonction deux fois transitive qui précède.

4. Passons maintenant à l'examen de la substitution (p). Les première, troisième et cinquième identifications ayant dû être rejetées dans l'examen de la substitution (n), elles doivent l'être à plus forte raison maintenant; il n'y a lieu, par conséquent, d'essayer que la deuxième et la quatrième identification, ce qui donne, pour la substitution (p), l'une de ces deux formules

$$(s) \qquad (x_4, x_5, x_3, x_9)(x_{10}, x_7, x_2, x_6),$$

$$(t) \qquad (x_4, x_5, x_3, x_9)(x_6, x_2, x_{10}, x_8).$$

Il existe une fonction transitive de 11 lettres, caractérisée par (k) et par (s) ou par (k) et par (t). Comme les substitutions (k) et (s) donnent le même système de substitutions conjuguées que (k) et (t), considérons seulement le premier cas.

La fonction caractérisée par (k) et (s) est évidemment invariable par tout le système de substitutions conjuguées de la fonction de M. Kronecker; par conséquent, elle est invariable par la substitution (r), et, en l'ajoutant à (l) et (s), on a les trois substitutions

$$(L) \qquad (x_1, x_4, x_5, x_9, x_8)(x_2, x_3, x_{10}, x_7, x_6),$$

$$(R) \qquad (x_2, x_4, x_7)(x_3, x_{10}, x_6)(x_5, x_8, x_9),$$

$$(S) \qquad (x_4, x_5, x_3, x_9)(x_{10}, x_7, x_2, x_6).$$

On peut reconnaître que le système de substitutions conjuguées dérivées de ces trois substitutions, qui s'effectuent sur les 10 quantités $x_1, x_2, \ldots, x_{10}$, est trois fois transitif et renferme $8.9.10$ substitutions (c'est une question sur laquelle nous allons d'ailleurs revenir). Et il en résulte une fonction quatre fois transitive de 11 lettres qui a $1.2.3.4.5.6.7$ valeurs.

Ainsi, de l'examen de la substitution (p), il résulte qu'*il y a une*

fonction quatre fois transitive de onze lettres, qui a $1.2.3.4.5.6.7 = 5040$ *valeurs, caractérisée par les substitutions*

$$(x_0, x_1, x_2, \ldots, x_{10}),$$
$$(x_4, x_5, x_3, x_9)\,(x_{10}, x_7, x_2, x_6),$$

et dont le système de substitutions conjuguées renferme le système de substitutions de la fonction deux fois transitive caractérisée par les substitutions (E) *et* (H). *Si à ces deux substitutions on ajoute la substitution* $\left(z, -\frac{1}{z}\right)$, *on a les trois substitutions qui caractérisent une fonction cinq fois transitive de douze quantités.*

J'ai présenté la découverte de cette fonction cinq fois transitive d'une manière toute différente à la fin du Chapitre II de mon Mémoire *sur les fonctions de plusieurs quantités*. Il est utile de comparer la forme sous laquelle elle se présente ici à celle sous laquelle nous l'avons d'abord fait connaître.

Désignons par ω une racine d'une congruence irréductible du second degré prise par rapport au module 3, par exemple une racine de la congruence

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

toutes les racines de

$$x^{3^2} \equiv x \pmod 3$$

sont égales à

$$0,\quad 1,\quad 2,\quad \omega,\quad 1+\omega,\quad 2+\omega,\quad 2\omega,\quad 1+2\omega,\quad 2+2\omega;$$

la quantité choisie pour ω est, de plus, une racine primitive de la congruence

$$x^{3^2-1} \equiv 1 \pmod 3;$$

et nous distinguerons les 8 racines de cette congruence en deux catégories : la première, qui renferme les puissances impaires de ω,

$$\omega,\quad \omega^3 \equiv 1 + 2\omega,\quad \omega^5 \equiv 1 + 2\omega,\quad \omega^7 \equiv 2 + \omega,$$

et que nous appelons des *non-résidus quadratiques;* la seconde, qui renferme les puissances paires de ω,

$$\omega^2 \equiv 1 + \omega, \quad \omega^4 \equiv 2, \quad \omega^6 \equiv 2 + 2\omega, \quad \omega^8 \equiv 1,$$

que nous appelons des *résidus quadratiques.*

D'après cela, changeons de notations et désignons les dix quantités

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

respectivement par

$$y_\omega, \quad y_{1+\omega}, \quad y_{2+2\omega}, \quad y_{1+2\omega}, \quad y_2, \quad y_1, \quad y_{2+\omega}, \quad y_{2\omega}, \quad y_0, \quad y_\infty,$$

alors les trois substitutions (L), (R), (S) deviennent

$$(y_\infty, y_{2+2\omega}, y_{1+2\omega}, y_{2+\omega}, y_{1+\omega})(y_\omega, y_0, y_{2\omega}, y_1, y_2),$$
$$(y_\omega, y_{2+2\omega}, y_1)(y_{1+\omega}, y_{2\omega}, y_2)(y_{1+2\omega}, y_0, y_{2+\omega}),$$
$$(y_{2+2\omega}, y_{1+2\omega}, y_{1+\omega}, y_{2+\omega})(y_{2\omega}, y_1, y_\omega, y_2),$$

et peuvent se mettre sous cette forme

$$\left(z, \frac{z+2\omega}{(1+\omega)z+1}\right),$$
$$(z, z+2+\omega),$$
$$(z, \omega z^3);$$

on en conclut facilement que toutes les substitutions de 8, de 9 et de 10 des quantités représentées par la notation y sont comprises dans les deux formules

$$\left(y_z, y_{\frac{Az+B}{Cz+D}}\right), \quad \left(y_z, y_{\frac{A_1 z^3 + B_1}{C_1 z^3 + D_1}}\right),$$

où AD — BC est résidu quadratique et $A_1 D_1 - B_1 C_1$ non-résidu, et ces deux formules représentent un système de $8.9.10$ substitutions conjuguées, trois fois transitif.

Nous nous sommes appuyés sur ce théorème que toute fonction

transitive de onze quantités est invariable par la substitution (l) ou

$$(z,\ 2^2 z);$$

mais ce théorème ne prouve pas qu'une telle fonction ne puisse être invariable par la substitution $(z,\ 2z)$ ou

$$(u) \qquad (x_1 x_2 x_4 x_8 x_5 x_{10} x_9 x_7 x_3 x_6),$$

dont la précédente est une puissance deuxième. Pour reconnaître si une telle fonction peut exister, on combinera cette substitution avec les deux substitutions (E) et (H), qui caractérisent la fonction deux fois transitive de 11 lettres, et l'on verra que le système de substitutions conjuguées qui s'en déduirait ne serait autre que les $1.2.3\ldots11$ substitutions qui laissent invariable la fonction symétrique. Il en résulte qu'il n'y a pas de fonctions transitives de 11 lettres invariables par la substitution (u), ou plus généralement par aucune substitution paire. (Nous appelons *substitution paire* celle qui change la fonction qui a deux valeurs.)

Fonctions transitives de 23 quantités.

5. Le nombre $\frac{23-1}{2}$ étant un nombre premier 11, nous pouvons appliquer la même méthode à la détermination des fonctions transitives de 23 quantités.

D'après ce que nous savons, toute fonction transitive de 23 quantités $x_0,\ x_1,\ x_2,\ldots,\ x_{22}$ peut être considérée comme invariable par les substitutions

$$(z,\ z+1) \quad \text{et} \quad (z,\ 5^2 z),$$

puisque 5 est racine primitive de 23, ou par les substitutions

$$(A) \qquad (x_0, x_1, x_2, x_3, \ldots, x_{22}),$$

$$(B) \qquad \begin{cases} (x_1, x_2, x_4, x_8, x_{16}, x_9, x_{18}, x_{13}, x_3, x_6, x_{12}), \\ (x_5, x_{10}, x_{20}, x_{17}, x_{11}, x_{22}, x_{21}, x_{19}, x_{15}, x_7, x_{14}). \end{cases}$$

Mettons cette dernière substitution sous cette forme

$$(C)\qquad \begin{cases} (x'_0, x'_1, x'_2, x'_3, x'_4, x'_5, x'_6, x'_7, x'_8, x'_9, x'_{10}), \\ (x''_0, x''_1, x''_2, x''_3, x''_4, x''_5, x''_6, x''_7, x''_8, x''_9, x''_{10}), \end{cases}$$

et regardons $x'_0, x'_1, \ldots, x'_{10}$ comme égales aux quantités de même rang du premier cycle de (B), en sorte que nous avons

$$x'_0 = x_1,\quad x'_1 = x_2,\quad x'_2 = x_4,\quad x'_3 = x_8,\quad x'_4 = x_{16},\quad x'_5 = x_9,$$
$$x'_6 = x_{18},\quad x'_7 = x_{13},\quad x'_8 = x_3,\quad x'_9 = x_6,\quad x'_{10} = x_{12};$$

mais l'identification du second cycle de (C) avec le second cycle de (B) peut se faire de onze manières différentes :

$$1^\circ \begin{cases} x''_0 = x_5,\quad x''_1 = x_{10},\quad x''_2 = x_{20},\quad x''_3 = x_{17},\quad x''_4 = x_{11},\quad x''_5 = x_{22}, \\ x''_6 = x_{21},\quad x''_7 = x_{19},\quad x''_8 = x_{15},\quad x''_9 = x_7,\quad x''_{10} = x_{14}; \end{cases}$$

$$2^\circ \begin{cases} x''_0 = x_{10},\quad x''_1 = x_{20},\quad x''_2 = x_{17},\quad x''_3 = x_{11},\quad x''_4 = x_{22},\quad x''_5 = x_{21}, \\ x''_6 = x_{19},\quad x''_{17} = x_{15},\quad x''_8 = x_7,\quad x''_9 = x_{14},\quad x''_{10} = x_5, \end{cases}$$

.....

Pour la substitution (D) du n° 1, nous devons prendre ou la substitution

$$(T)\qquad \begin{cases} (x'_1, x'_2, x'_4, x'_8, x'_5, x'_{10}, x'_9, x'_7, x'_3, x'_6), \\ (x''_1, x''_2, x''_4, x''_8, x''_5, x''_{10}, x''_9, x''_7, x''_3, x''_6), \end{cases}$$

composée de deux cycles de 10 quantités, ou sa puissance cinquième, ou sa puissance deuxième. Sa puissance cinquième est

$$(x'_1 x'_{10})(x'_2 x'_9)(x'_3 x'_8)(x'_4 x'_7)(x'_5 x'_6),$$
$$(x''_1 x''_{10})(x''_2 x''_9)(x''_3 x''_8)(x''_4 x''_7)(x''_5 x''_6),$$

et, après y avoir appliqué une des 11 identifications, on pourra vérifier qu'elle doit être rejetée. A plus forte raison, la substitution (T) doit être mise de côté.

Il reste donc à considérer la puissance deuxième de (T), qui est

$$(x'_1\,x'_4\,x'_5\,x'_9\,x'_3)(x'_2\,x'_8\,x'_{10}\,x'_7\,x'_6),$$
$$(x''_1\,x''_4\,x''_5\,x''_9\,x''_3)(x''_2\,x''_8\,x''_{10}\,x''_7\,x''_6).$$

Si l'on y applique la première identification, on obtient pour cette substitution

$$(U)\qquad \begin{cases} (x_2,\ x_{16}, x_9,\ x_6, x_8\ )(x_4,\ x_3,\ x_{12}, x_{13}, x_{18}), \\ (x_{10}, x_{11}, x_{22}, x_7, x_{17})(x_{20}, x_{15}, x_{14}, x_{19}, x_{21}), \end{cases}$$

qui fournit une fonction que nous allons examiner. Quant aux 10 autres identifications, elles ne donneraient pas d'autres fonctions. On cherchera des substitutions dérivées de (A) et (U) qui ne contiennent pas x_0, et par leur moyen on reconnaîtra que la fonction est transitive par rapport aux 22 quantités $x_1, x_2, \ldots, x_{22}$; on formera ensuite des substitutions qui, outre x_0, ne contiennent pas x_1; on verra que la fonction est transitive par rapport aux 21 quantités x_2, $x_3, \ldots, x_{22}$; puis on formera des substitutions qui ne contiennent aucune des trois quantités x_0, x_1, x_2 qui n'entrent pas dans (U), et l'on trouvera que la fonction est transitive par rapport aux 20 quantités restantes. La fonction est donc quatre fois transitive.

Enfin donnons les substitutions qui ne contiennent pas x_0, x_1, x_2, et une quatrième quantité, x_2 par exemple. Elles sont les dérivées :

1° Des substitutions

$$(Z)\qquad \begin{cases} (4,19)(15,12)(16,7\ )(10,8\ )(18,9\ )(6,13)(11,20)(21,22), \\ (4,16)(19,7\ )(15,10)(12,8\ )(18,11)(9,20)(\ 6,21)(13,22), \\ (4,18)(19,9\ )(15,6\ )(12,13)(16,11)(7,20)(10,21)(\ 8,22), \\ (4,12)(19,15)(16,8\ )(\ 7,10)(18,13)(9,6\ )(11,22)(20,21), \end{cases}$$

d'après lesquelles, comme on le voit du premier coup d'œil, la fonction est transitive par rapport aux 16 quantités qui ont pour indices : 4, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16, 18, 19, 20, 21, 22;

2° De la substitution

$$(3,14,17)(7,19,21)(13,15,12)(4,10,11)(9,8,16)(20,18,22).$$

On en peut conclure que le nombre des substitutions qui ne contiennent pas x_0, x_1, x_5, x_2 et qui laissent la fonction invariable est 16×3. Donc la fonction quatre fois transitive de 23 quantités a $\frac{1.2.3.4\ldots19}{16\times 3}$ valeurs.

Nous allons maintenant faire une remarque bien curieuse : c'est que, si l'on représente la substitution (U) cycle par cycle par

$$(V)\qquad \begin{cases} (y_0 y_1 y_2 y_3 y_4)(y'_0 y'_1 y'_2 y'_3 y'_4), \\ (y''_0 y''_1 y''_2 y''_3 y''_4)(y'''_0 y'''_1 y'''_2 y'''_3 y'''_4), \end{cases}$$

la fonction est invariable par la substitution $(y_z y_{4z})$, les indices étant pris suivant le module 5, c'est-à-dire par

$$(P)\qquad \begin{cases} (y_1 y_4)(y_2 y_3)(y'_1 y'_4)(y'_2 y'_3), \\ (y''_1 y''_4)(y''_2 y''_3)(y'''_1 y'''_4)(y'''_2 y'''_3), \end{cases}$$

pourvu que l'on identifie convenablement (U) et (V).

Les 20 lettres de la substitution (U) se composent des 16 lettres des substitutions (Z) et, en outre, de x_2, x_3, x_{17}, x_{14}, qui se trouvent dans quatre cycles différents de (U). Donc, pour que (P) puisse coïncider avec une des substitutions (Z) ou une de leurs dérivées, qui leur sont toutes semblables, nous ferons

$$y_0 = x_2, \quad y'_0 = x_3, \quad y''_0 = x_{17}, \quad y'''_0 = x_{14},$$

en identifiant (U) et (V), et il en résultera

$$\begin{array}{llll} y_1 = x_{16}, & y_2 = x_9, & y_3 = x_6, & y_4 = x_8; \\ y'_1 = x_{12}, & y'_2 = x_{13}, & y'_3 = x_{18}, & y'_4 = x_4; \\ y''_1 = x_{10}, & y''_2 = x_{11}, & y''_3 = x_{22}, & y''_4 = x_7; \\ y'''_1 = x_{19}, & y'''_2 = x_{21}, & y'''_3 = x_{20}, & y'''_{15} = x_{15}. \end{array}$$

On en conclut, pour la substitution (P),

$$(H)\qquad \begin{cases} (x_{16} x_8)(x_9\ x_6\ )(x_{12} x_4\ )(x_{18} x_{13}), \\ (x_{10} x_7)(x_{11} x_{22})(x_{19} x_{15})(x_{21} x_{20}), \end{cases}$$

qui représente précisément la quatrième des substitutions (Z).

Si l'on reprend la notation des x' et x'', cette substitution pourra s'écrire

$$(K)\qquad \begin{cases} (x'_4\,x'_3)\,(x'_5\,x'_9)\,(x'_{10}\,x'_2)\,(x'_7\,x'_6) \\ (x''_1\,x''_9)\,(x''_4\,x''_5)\,(x''_7\,x''_8)\,(x''_6\,x''_2). \end{cases}$$

Or le premier cycle de (B') ou de (C) et la première ligne de (K) sont les deux substitutions

$$(L)\qquad (x'_0\,x'_1\,x'_2\ldots x'_{10}),$$

$$(M)\qquad (x'_4\,x'_3)\,(x'_5\,x'_9)\,(x'_{10}\,x'_2)\,(x'_7\,x'_6),$$

qui caractérisent une fonction deux fois transitive de 11 quantités qui a $6\times 10\times 11$ valeurs égales (*voir* n° **3**). Le second cycle de (C) et la seconde ligne de (K) donnent les deux substitutions

$$(L')\qquad (x''_0\,x''_1\,x''_2\ldots\ldots x''_{10}),$$

$$(M')\qquad (x''_1\,x''_9)\,(x''_4\,x''_5)\,(x''_7\,x''_8)\,(x''_6\,x''_2),$$

qui caractérisent aussi une fonction deux fois transitive de 11 quantités.

Donc *la fonction quatre fois transitive de* 23 *quantités reste invariable si l'on fait sur les* 11 *quantités du premier cycle de* (B) *les* $6\times 10\times 11$ *substitutions dérivées de* (L) *et* (M) *qui caractérisent une fonction deux fois transitive de ces* 11 *quantités, pourvu qu'en même temps on fasse sur les quantités du second cycle de* (B) *des substitutions semblables dérivées de la même manière de* (L') *et* (M'), *qui caractérisent aussi une fonction deux fois transitive.*

Il existe une fonction cinq fois transitive de 24 *quantités, qui, considérée comme fonction des* 23 *premières* x_0, $x_1,\ldots$, x_{22}, *est identique à la fonction que nous venons d'obtenir.* Désignons la vingt-quatrième lettre par x_∞; cette fonction est invariable par les substitutions

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

pour lesquelles AD — BC est résidu quadratique; par conséquent, elle est caractérisée par deux substitutions qui caractérisent la fonction

précédente de 23 quantités et par une quelconque des dernières substitutions renfermant x_∞, par exemple par $\left(z, -\frac{1}{z}\right)$ ou

$$(0,\infty)(1,22)(2,11)(3,15)(4,17)(5,9)$$
$$(6,19)(7,13)(8,20)(10,16)(12,21)(18,14).$$

D'après ce que nous avons vu, toute fonction transitive de 23 quantités peut être considérée comme invariable par la substitution (A) et la substitution (U); mais il faut encore se demander si, outre la fonction que nous venons d'obtenir, il n'y en a pas une, invariable non-seulement par $(z, 5^2 z)$, mais aussi par la substitution circulaire de 22 lettres $(z, 5z)$. Toutefois on reconnaîtra facilement qu'une telle fonction n'existe pas.

Maintenant que nous savons qu'il n'existe qu'une seule fonction transitive de 23 quantités, il est évident que cette fonction est caractérisée par la substitution (A) et par une quelconque des substitutions qui la laissent invariable, pourvu que cette dernière soit prise en dehors des $\frac{23\times 22}{2}$ substitutions qui sont de la forme

$$(z, az+b),$$

a étant résidu quadratique de 23; et, si l'on remarque que les substitutions de cette fonction qui ont le moins de lettres sont celles qui en ont 16, on voit que toutes les dérivées d'une substitution circulaire de 23 lettres et d'une substitution de moins de 16 lettres prises parmi ces dernières forment les $1.2.3\ldots 23$ substitutions possibles, ou la moitié seulement, suivant que la seconde substitution est paire ou impaire.

Forme de la substitution qui caractérise toutes les fonctions transitives précédentes.

Recherchons sous quelle forme on peut écrire la substitution (D) du n° **1**, qui est

$$\text{(D)} \qquad (x'_z, x'_{mz})(x''_z, x''_{mz}),$$

en posant

$$\gamma^{\mu} \equiv m, \quad \left(\text{mod. } \frac{p-1}{2}\right),$$

lorsqu'on y rétablit les x sans accents : $x_1, x_2, \ldots$.

La première partie

$$(L) \qquad (x'_z, x'_{mz})$$

de la substitution (D) s'effectue sur les quantités $x'_0, x'_1, x'_2, \ldots$, ou

$$x_{g^0}, \quad x_{g^2}, \quad x_{g^4}, \ldots, \quad x_{g^{p-3}},$$

dont les indices sont des résidus quadratiques suivant le module p; elle revient à cette substitution sur les exposants des puissances paires de g

$$(2t, 2mt), \quad (\text{mod. } p-1);$$

ainsi g^{2t} est changé en g^{2mt}; donc, en désignant par a un résidu quadratique quelconque par rapport à p, la substitution (L) peut s'écrire

$$(a, a^m).$$

Considérons la seconde partie

$$(M) \qquad (x''_z, x''_{mz})$$

de la substitution (D), elle s'effectue sur $x_g, x_{g^3}, x_{g^5}, \ldots$; une seule de ces quantités n'est pas déplacée, et nous la représenterons par x_{g^β}, β étant impair. Alors, en général, $g^{\beta+2t}$ sera changé en $g^{\beta+2mt}$. Si l'on représente les non-résidus de p par b et qu'on pose, suivant le module p,

$$g^{\beta+2t} \equiv b,$$

on aura

$$g^{\beta+2mt} \equiv g^{(1-m)\beta} b^m,$$

et la substitution (M) pourra s'écrire

$$(b, g^{(1-m)\beta} b^m).$$

Nous venons d'obtenir deux formules pour représenter la substitution (D), suivant qu'il s'agit d'indices qui sont résidus quadratiques

ou d'indices qui sont non-résidus; mais on peut la représenter par la seule formule

$$\left(z,\ Az^{\frac{p-1}{2}+m} + Bz^m\right).$$

En effet, si a est un résidu de p, on a $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, et, en exprimant que la substitution change a en a^m, on obtient

$$A + B \equiv 1.$$

Si b est un non-résidu de p, on a $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, et, en se servant de la seconde partie de la substitution, on a

$$-A + B \equiv g^{(1-m)\beta}.$$

On en conclut

$$A \equiv \frac{1 - g^{\beta(1-m)}}{2}, \quad B \equiv \frac{1 + g^{\beta(1-m)}}{2}.$$

Les substitutions que nous avons désignées, dans le n° **2**, par 1°, 2°, 3° peuvent s'écrire respectivement

$$(z,\ -2z^5 + 3z^2) \pmod{7},$$
$$(z,\ z^5),$$
$$(z,\ -z^5 + 2z^2);$$

donc la fonction deux fois transitive de sept lettres est caractérisée par la substitution $(z,\ z+1)$ et une quelconque des trois substitutions précédentes.

Les substitutions que nous avons désignées, dans le n° **3**, par 2° et 4° peuvent s'écrire, suivant le module 11,

$$(z,\ 5z^9 - 4z^4),$$
$$(z,\ 3z^9 - 2z^4);$$

donc la fonction deux fois transitive de onze lettres est caractérisée par $(z,\ z+1)$ et une de ces deux substitutions.

On voit ensuite que la fonction quatre fois transitive de 11 lettres est déterminée par $(z, z+1)$ et une des deux substitutions

$$(z, -3z^7 + 4z^2),$$
$$(z, 2z^7 - z^2).$$

Enfin la fonction quatre fois transitive de 23 quantités est donnée par $(z, z+1)$ et par la substitution

$$(z, -3z^{15} + 4z^4).$$

Réflexions sur les fonctions transitives d'un nombre premier de quantités.

D'après les calculs précédents, il existe une fonction transitive de 7 quantités qui l'est deux fois, deux fonctions transitives de 11 quantités dont l'une l'est deux fois et l'autre quatre fois, enfin une seule fonction transitive de 23 quantités qui l'est quatre fois. Si nous désignons généralement par p le nombre des quantités renfermées dans ces fonctions, ces fonctions sont invariables par les substitutions de la forme

$$(g) \qquad (z, a^2z + b),$$

et, ∞ étant l'indice d'une nouvelle quantité, elles donnent des fonctions de $p+1$ quantités qui sont transitives une fois de plus et invariables par les substitutions

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

pour lesquelles AD — BC est résidu quadratique.

Entre 11 et 23 se trouvent les trois nombres premiers 13, 17, 19, et je devais me demander s'il existe des fonctions transitives de 13, 17 ou 19 lettres invariables par toutes les substitutions (g). Après avoir fait les calculs nécessaires, j'ai reconnu qu'il n'y en avait point. D'après les essais que j'ai faits, je suis, de plus, extrêmement porté à croire

qu'il n'existe pas de fonctions plusieurs fois transitives de 13 ni de 19 lettres. Quant aux fonctions transitives de 17 quantités, il en existe trois, et qui sont trois fois transitives, fournies par ce théorème que j'ai donné dans mon Mémoire *sur les fonctions de plusieurs quantités* (Chapitre II) : « Si τ est un diviseur de ν, il existe une fonction trois fois transitive de $p^\nu+1$ quantités, qui a $\frac{1.2.3\ldots(p^\nu-2)\times\tau}{\nu}$ valeurs. On les obtient en faisant $p=2$, $\nu=4$ et τ successivement égal à 1, 2, 4. »

Ainsi les fonctions plusieurs fois transitives de 7, 11 et 23 quantités, et celles de 8, 12 et 24, qui ont été calculées dans le Mémoire actuel, sont bien dues à ce que les nombres premiers 7, 11 et 23 sont des doubles de nombres premiers augmentés d'une unité. D'ailleurs, comme il est aisé de le voir, une fonction transitive dont le nombre des lettres est à la fois un nombre premier et le double d'un nombre premier augmenté d'une unité est au moins deux fois transitive.