N° D'ORDRE
218.

THÈSES

PRÉSENTÉES

A LA FACULTÉ DES SCIENCES DE PARIS

POUR OBTENIR

LE GRADE DE DOCTEUR ÈS SCIENCES MATHÉMATIQUES,

PAR M. ÉMILE MATHIEU.

THÈSE D'ANALYSE MATHÉMATIQUE. — Sur le nombre de valeurs que peut acquérir une fonction quand on y permute ses lettres de toutes les manières possibles.

THÈSE D'ASTRONOMIE. — Proposition d'Astronomie donnée par la Faculté.

Soutenues le 28 Mars 1859 devant la Commission d'Examen.

MM. LAMÉ, *Président*.
LIOUVILLE, } *Examinateurs*.
SERRET, }

PARIS,
MALLET-BACHELIER, IMPRIMEUR-LIBRAIRE
DE L'ÉCOLE IMPÉRIALE POLYTECHNIQUE, DU BUREAU DES LONGITUDES,
Quai des Augustins, 55.

1859.

ACADÉMIE DE PARIS.

FACULTÉ DES SCIENCES DE PARIS.

DOYEN .... MILNE EDWARDS, Professeur. Zoologie, Anatomie, Physiologie.

PROFESSEURS HONORAIRES. BIOT.
PONCELET.

PROFESSEURS ....

DUMAS	Chimie.
DESPRETZ	Physique.
DELAFOSSE	Minéralogie.
BALARD	Chimie.
LEFÉBURE DE FOURCY ...	Calcul différentiel et intégral.
CHASLES	Géométrie supérieure.
LE VERRIER	Astronomie.
DUHAMEL	Algèbre supérieure.
GEOFFROY-SAINT-HILAIRE.	Anatomie, Physiologie comparée, Zoologie.
LAMÉ	Calcul des probabilités, Physique mathématique.
DELAUNAY	Mécanique physique.
PAYER	Botanique.
C. BERNARD	Physiologie générale.
P. DESAINS	Physique.
LIOUVILLE	Mécanique rationnelle.
HÉBERT	Géologie.
PUISEUX	Astronomie.

AGRÉGÉS ....

BERTRAND	Sciences mathématiques.
J. VIEILLE	Sciences mathématiques.
MASSON	Sciences physiques.
PELIGOT	Sciences physiques.
DUCHARTRE	Sciences naturelles.

SECRÉTAIRE ... . E. PREZ-REYNIER.

THÈSE D'ANALYSE MATHÉMATIQUE.

SUR LE NOMBRE DE VALEURS QUE PEUT ACQUÉRIR UNE FONCTION

QUAND ON Y PERMUTE SES LETTRES DE TOUTES LES MANIÈRES POSSIBLES.

HISTOIRE.

Lagrange, en s'occupant de la théorie algébrique des équations, établit le premier théorème de cette science : *Le nombre de valeurs d'une fonction de* n *lettres est nécessairement un diviseur du produit* $1.2.3\ldots n$.

C'était ensuite pour la résolution générale des équations une question bien importante que celle de connaître le plus petit nombre de valeurs que peut acquérir une fonction de n lettres. Aussi n'a-t-on pas tardé à s'occuper de cette question.

Ruffini la résolut le premier pour les fonctions de cinq lettres, et démontra ce théorème : *Si une fonction de cinq lettres a plus de deux valeurs, elle en a au moins cinq.*

Ce théorème de Ruffini a été ensuite étendu à une fonction d'un nombre quelconque de variables par Pietro Abatti, qui a démontré que *si* n *est* >4, *toute fonction de* n *lettres qui a plus de deux valeurs, en a au moins cinq.*

M. Cauchy alla beaucoup plus loin, et au nombre 5, qui se trouve dans le théorème d'Abatti, il substitua le plus grand nombre premier p contenu dans n. Il a donc démontré que *toute fonction de* n *lettres qui a plus de deux valeurs, en a au moins* p.

Enfin M. Bertrand a démontré qu'à ce nombre p on pouvait substituer le nombre n même, et qu'ainsi *une fonction de* n *lettres qui a plus de deux valeurs, en a au moins* n, *si* n *est* >4.

Par le théorème de M. Bertrand, la question du plus petit nombre de valeurs que peut acquérir une fonction se trouve complétement traitée; car une fonction de n lettres peut avoir effectivement n valeurs, il suffit évidemment qu'elle soit symétrique par rapport à $n-1$ lettres. M. Bertrand a aussi déduit comme corollaire de son théorème cette proposition démontrée auparavant par Abel dans le cas de $n=5$: *Si une fonction de n lettres a n valeurs, elle est symétrique par rapport à* $n-1$ *lettres*.

M. Bertrand fit reposer la démonstration de son théorème sûr le postulatum suivant : *Si n est* >7, *il y a au moins un nombre premier compris entre* $n-2$ *et* $\frac{n}{2}$. Mais aujourd'hui la démonstration de M. Bertrand a pris toute la rigueur mathématique; car M. Tchebichef a démontré depuis la proposition admise comme postulatum par M. Bertrand.

M. Cauchy et M. Serret ont aussi donné une démonstration du théorème de M. Bertrand à une époque où M. Tchebichef n'avait pas encore démontré la proposition dont nous venons de parler.

On dut ensuite rechercher quels étaient les plus petits nombres après n, qui pouvaient représenter les valeurs d'une fonction de n lettres.

M. Bertrand démontra d'abord ce théorème : *Une fonction de n lettres, qui a plus de n valeurs, en a au moins* $2n$, *si n est* >9.

Dans un Mémoire que j'ai présenté à l'Académie des Sciences, j'ai démontré qu'on pouvait à la limite $n>9$ substituer $n>6$; d'ailleurs cette limite ne saurait être abaissée davantage, car une fonction de six lettres qui a plus de six valeurs, peut n'en avoir que dix.

Dans le même Mémoire où M. Serret a démontré le théorème de M. Bertrand, il a démontré cet autre théorème : *Une fonction de n lettres, qui a plus de* $2n$ *valeurs, en a au moins* $\frac{n(n-1)}{2}$, *si n est* >12.

J'ai reconnu que ce théorème est vrai, quel que soit n, et qu'ainsi la restriction $n>12$ n'était pas nécessaire.

Enfin j'ai encore démontré ce théorème : *Une fonction de n lettres qui a plus de* $\frac{n(n-1)}{2}$ *valeurs, en a au moins* $n(n-1)$, *si n est* >8.

M. Cauchy est le premier qui ait recherché quels étaient tous les nombres propres à représenter les valeurs d'une fonction d'un nombre donné de lettres. Sa méthode consiste à considérer deux espèces de fonctions : les fonctions transitives et les fonctions intransitives. Les nombres de valeurs que peut acquérir une fonction intransitive de n lettres se déterminent immédiatement, quand on connaît toutes les fonctions transitives qui ont moins de n lettres, et alors les recherches doivent entièrement se porter sur les fonctions transitives.

Pour déterminer ces fonctions transitives, M. Cauchy emploie la méthode des *systèmes de substitutions conjuguées,* et au moyen du symbole, il soumet les permutations aux premières opérations de l'algèbre. M. Cauchy est parvenu de la sorte à déterminer tous les nombres de valeurs que peut acquérir une fonction de quatre, de cinq et de six lettres.

M. Serret a repris ensuite l'étude des mêmes fonctions sous un point de vue tout différent.

Enfin je me suis occupé à mon tour de déterminer tous les nombres qui peuvent représenter les valeurs d'une fonction d'un nombre déterminé de lettres; dans cette étude, j'ai repris la très-belle idée de M. Cauchy, qui consiste à partager toutes les fonctions en fonctions transitives et intransitives; mais la méthode que j'ai employée pour déterminer les fonctions transitives est entièrement différente de celle de M. Cauchy. Par cette nouvelle méthode, j'ai pu non-seulement reprendre l'étude de toutes les fonctions de quatre, de cinq et de six lettres, mais j'ai pu encore déterminer toutes les fonctions de sept lettres et de huit lettres.

Puisque dans cette théorie toute l'étude des fonctions est ramenée à celle des fonctions transitives, on comprend combien sont utiles des théorèmes généraux qui donnent ces fonctions transitives.

Parmi ces théorèmes, on a les deux suivants, qui sont dus à Lagrange :

1°. *Il y a toujours une fonction transitive de* n *lettres qui a* $1.2\ldots(n-1)$ *valeurs.*

2°. *Si* n *est premier, il y a une fonction deux fois transitive de* n *lettres qui a* $1.2\ldots(n-2)$ *valeurs.*

On peut encore citer ce théorème d'Abel :

Quel que soit n*, il y a toujours une fonction de* n *lettres qui a deux valeurs.*

Enfin j'ai établi les théorèmes suivants :

1°. *Quel que soit* n*, il y a une fonction transitive de* n *lettres, qui a* $\frac{1.2\ldots(n-1)}{2}$ *valeurs.*

2°. *Si* n *est premier et* u *un diviseur quelconque de* $n-1$*, il y a une fonction transitive de* n *lettres qui a* $1.2\ldots(n-2)\times u$ *valeurs.*

3°. *Si* $n-1$ *est un nombre premier, il y a une fonction trois fois transitive de* n *lettres qui a* $1.2\ldots(n-3)$ *valeurs.*

4°. *Si* $n-1$ *est un nombre premier, il y a une fonction deux fois transitive de* n *lettres qui a* $1.2\ldots(n-3)\times 2$ *valeurs.*

Le troisième de ces théorèmes est le plus remarquable. Car avant que je me fusse occupé de la question du nombre de valeurs d'une fonction, il n'avait encore été signalé qu'une seule fonction trois fois transitive : c'est la fonction trois fois transitive de six lettres qui a six valeurs, et qui, comme on le voit, est donnée par mon théorème. Cette fonction de six lettres, qui a six valeurs, a été rencontrée pour la première fois par M. Hermite en étudiant les équations modulaires, elle est aussi remarquable parce qu'elle fait seule exception à ce théorème : *Une fonction de n lettres qui a n valeurs est symétrique par rapport à $n-1$ lettres.*

Le quatrième théorème donne une fonction de six lettres qui a douze valeurs, et qui peut à son tour être remarquée parce qu'elle fait seule exception à ce théorème : *Si une fonction de n lettres a $2n$ valeurs, il y a $n-1$ de ses lettres par les permutations desquelles elle n'acquiert que deux valeurs.*

L'Académie des Sciences a choisi la question du nombre de valeurs d'une fonction pour le sujet du grand prix de Mathématiques à décerner en 1860.

OBJET DE LA THÈSE.

Dans cette thèse, à l'exemple de M. Cauchy, je partagerai les fonctions en deux classes : l'une comprenant les fonctions transitives, l'autre les fonctions intransitives. Je ferai d'abord connaître une formule qui indique les nombres susceptibles d'exprimer combien une fonction intransitive de n lettres peut prendre de valeurs; cette formule renferme dans son expression des inconnues qui représentent les nombres de valeurs que peuvent acquérir différentes fonctions transitives de moins de n lettres. Je donnerai ensuite quelques propositions générales relatives aux fonctions une ou plusieurs fois transitives, puis j'exposerai une démonstration du théorème de M. Bertrand qui a été donnée par M. Cauchy.

Enfin j'établirai les théorèmes nouveaux auxquels j'ai été conduit par mes propres recherches, et qui donnent des classes de fonctions transitives.

DÉFINITIONS ET CONSIDÉRATIONS GÉNÉRALES.

Des substitutions.

Rangeons n lettres $a, b, c, \ldots, l$ sur un cercle, puis mettons chacune d'elles à la place de celle qui la précède, nous aurons ainsi fait sur ces lettres une permutation ou substitution qui est dite *circulaire;* ainsi la substitution

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

est circulaire ; on l'écrit plus simplement

$$(abcd \ldots l).$$

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

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

pourra 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*.

Distinction des fonctions en fonctions transitives et en fonctions intransitives

On appelle 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.

Toute fonction qui n'est pas transitive est dite *intransitive*.

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 la lettre g qui occupe la $\beta^{ième}$ place dans la permutation, à la place de la lettre a dans la fonction, il est clair qu'il suffira de faire cette substitution $\beta - 1$ fois.

Ainsi, par exemple, la fonction de trois lettres

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

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 de n'être pas changée par une substitution circulaire effectuée sur toutes ses lettres. Ainsi, 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

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

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, c, $\ldots$, 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.

Concevons maintenant que l'on puisse partager les n lettres d'une fonction en groupes d'un même nombre :

$$\begin{array}{l} a,\ b,\ c,\ldots, \\ f,\ g,\ h,\ldots, \\ m,\ p,\ q,\ldots, \\ \ldots\ldots\ldots \end{array}$$

et que les lettres d'un quelconque de ces groupes puissent remplacer respectivement les lettres de même rang d'un autre quelconque de ces groupes, pourvu que l'on échange convenablement tous les groupes restants, de manière que les lettres d'un même groupe soient toutes remplacées par les lettres de même rang d'un autre même groupe. Nous dirons alors que la fonction est transitive par rapport à ces groupes de lettres.

Ainsi, par exemple, la fonction de neuf lettres

$$\begin{array}{r} (a+d^2+e^3)\,(b+f^2+g^3)^2\,(c+h^2+i^3)^3 \\ +\,(b+f^2+g^3)\,(c+h^2+i^3)^2\,(a+d^2+e^3)^3 \\ +\,(c+h^2+i^3)\,(a+d^2+e^3)^2\,(b+f^2+g^3)^3 \end{array}$$

est transitive par rapport aux trois groupes

$$a,\ d,\ e,\quad b,\ f,\ g,\quad c,\ h,\ i.$$

La fonction de six lettres

$$ab^2+cd^2+ef^2$$

est aussi transitive par rapport à trois groupes qui sont

$$a, b, \quad c, d, \quad e, f;$$

dans ce cas on peut encore dire que la fonction est symétrique par rapport à ces trois groupes.

Concevons ensuite une fonction dont on puisse partager les lettres en groupes d'un même nombre

$$\begin{array}{l} a, \quad b, \quad c, \ldots, \\ f, \quad g, \quad h, \ldots, \\ \ldots\ldots\ldots \end{array}$$

de telle sorte que la fonction soit transitive par rapport à ces groupes, et supposons de plus que la fonction soit transitive par rapport aux lettres de chaque groupe ; ce que l'on pourra exprimer en disant que les groupes sont *transitifs*. Il est facile de reconnaître que cette fonction sera transitive.

Supposons, par exemple, que l'on mette une lettre g d'un groupe quelconque à la place de la lettre a du premier groupe. Pour produire ce déplacement, on pourra commencer par amener la lettre g à la place de la lettre f, qui occupe la première place dans le groupe qui contient g, et faire mouvoir seulement les lettres de ce groupe, de manière que la fonction ne change pas de valeur. Cela fait, on pourra mettre ce groupe à la place du premier, sans que la valeur de la fonction soit changée, si on permute convenablement tous ces groupes, et l'on voit enfin que la lettre f sera venue à la place de la lettre a, sans que la fonction ait changé de valeur. On peut donc amener une lettre quelconque à telle place que l'on veut sans que la fonction change de valeur, et par suite cette fonction est transitive.

Donc une fonction *transitive par rapport à des groupes transitifs* est une fonction transitive.

Ainsi, par exemple, la fonction

$$abcd^2e^2f^2g^3h^3i^3 + defg^2h^2i^2a^3b^3c^3 + ghi\,a^2b^2c^2d^3e^3f^3$$

est transitive par rapport aux trois groupes

$$a, \; b, \; c, \quad d, \; e, \; f, \quad g, \; h, \; i;$$

et ces groupes sont transitifs, puisqu'ils sont symétriques ; donc cette fonction est transitive.

Formule qui donne le nombre de valeurs d'une fonction intransitive.

Proposons-nous maintenant de trouver une formule qui donne le nombre de valeurs d'une fonction intransitive F de n lettres.

Supposons d'abord que les lettres de la fonction puissent être partagées en groupes

$$\begin{array}{lll} a, & b, & c,\ldots, \\ f, & g, & h,\ldots, \\ l, & m, & n,\ldots, \\ \ldots & \ldots & \ldots \end{array}$$

tels que, sans changer la valeur de la fonction, on puisse amener une lettre quelconque d'un de ces groupes à la place d'une autre, en ne déplaçant que les lettres de ce groupe; et supposons de plus qu'une lettre quelconque ne puisse sortir de son groupe, sans que la valeur de la fonction en soit altérée. F, considérée comme fonction des lettres d'un seul de ces groupes, sera une fonction transitive.

Soient α, β, γ,... les nombres de lettres qui se trouvent respectivement dans le premier groupe, dans le deuxième groupe, etc., et soient M, N, P,... les nombres de valeurs égales qu'acquiert la fonction, quand on permute respectivement les lettres du premier groupe, les lettres du second, etc. Il est aisé de comprendre que le nombre des valeurs distinctes de la fonction F sera donné par la formule

$$\frac{1.2.3\ldots n}{M \times N \times P \times \ldots}.$$

Si maintenant nous désignons par A, B, C,... les nombres de valeurs distinctes qu'acquiert la fonction, quand on permute respectivement les lettres du premier groupe, les lettres du second, etc., nous aurons les égalités

$$M = \frac{1.2.3\ldots\alpha}{A}, \quad N = \frac{1.2.3\ldots\beta}{B}, \quad P = \frac{1.2.3\ldots\gamma}{C}, \ldots,$$

et, par conséquent, le nombre des valeurs distinctes de la fonction F sera donné par la formule

$$(i) \qquad \frac{1.2.3\ldots n}{\frac{1.2.3\ldots\alpha}{A} \times \frac{1.2.3\ldots\beta}{B} \times \frac{1.2.3\ldots\gamma}{C} \times \ldots},$$

ou encore par cette autre

$$(u)\qquad \frac{1.2.3\ldots n}{1.2.3\ldots\alpha\times 1.2\ldots\beta\times 1.2\ldots\gamma\times\ldots}\,\mathrm{ABC}\ldots$$

Ainsi lorsqu'on connaîtra les nombres de valeurs de toutes les fonctions transitives qui ont moins de n lettres, rien ne sera plus facile que de déterminer au moyen de la formule (u) le nombre de valeurs d'une fonction intransitive quelconque de n lettres, qui satisfera aux conditions remplies par la fonction F.

Supposons, par exemple, que nous voulions trouver le nombre de valeurs de la fonction de dix lettres

$$abc + (d - e)(f - g)(ik^2 l^3 + kl^2 i^3 + li^2 k^3).$$

Les lettres de la fonction pourront être partagées en les trois groupes

$$\begin{array}{llll} a, & b, & c, & \\ d, & e, & f, & g, \\ i, & k, & l; & \end{array}$$

la fonction est transitive par rapport aux lettres de chacun de ces groupes, et si l'on fait une permutation qui échange une lettre d'un des groupes avec une lettre d'un autre, la fonction change nécessairement de valeur. Ainsi le nombre des valeurs de la fonction considérée sera donné par la formule (i) ou par la formule (u). Nous avons d'abord

$$\alpha = 3, \quad \beta = 4, \quad \gamma = 3;$$

reste à déterminer A, B, C.

La fonction est symétrique par rapport aux trois lettres a, b, c, on a donc $\mathrm{A} = 1$; il est ensuite aisé de reconnaître que la fonction acquiert six valeurs distinctes par les permutations des lettres d, e, f, g, et qu'elle n'en acquiert que deux par les permutations des lettres i, k, l; on a donc

$$\mathrm{B} = 6 \quad \text{et} \quad \mathrm{C} = 2,$$

et le nombre des valeurs de la fonction considérée est

$$\frac{1.2.3.4.5.6.7.8.9.10}{1.2.3 \times \frac{1.2.3.4}{6} \times \frac{1.2.3}{2}} \quad \text{ou} \quad 50400.$$

Le nombre des lettres d'un ou plusieurs groupes pourrait se réduire à l'unité. Ainsi, soit la fonction

$$(ab + cd)e^2 f^3;$$

cette fonction par les permutations des quatre lettres a, b, c, d acquiert trois valeurs; on aura le nombre des valeurs de cette fonction en faisant

$$\alpha = 4, \quad \beta = 1, \quad \gamma = 1, \quad \mathrm{A} = 3, \quad \mathrm{B} = 1, \quad \mathrm{C} = 1;$$

le nombre des valeurs de cette fonction est donc

$$\frac{1.2.3.4.5.6}{\frac{1.2.3.4}{3} \times 1 \times 1} \quad \text{ou} \quad 90.$$

Nous venons de supposer que l'on puisse partager les lettres de la fonction en groupes tels, que la fonction soit transitive par rapport aux lettres de chaque groupe, et que de plus une lettre ne puisse sortir d'un de ces groupes, sans que la fonction change de valeur. Mais il n'en est pas toujours ainsi; car la fonction peut être transitive par rapport à des groupes de lettres.

Dans ce cas les lettres de la fonction peuvent être décomposées en deux sortes de groupes : 1° en groupes (A) tels, que la fonction soit transitive par rapport à une série de ces groupes, puis transitive par rapport à une série de ceux qui restent, et ainsi de suite; 2° en groupes (B) tels, que la fonction soit transitive par rapport aux lettres de chacun. On commencera par former les séries des groupes (A), qui devront être telles, qu'une lettre ne puisse passer d'une série dans une autre, sans que la valeur de la fonction en soit altérée, puis on décomposera les lettres qui resteront en groupes (B).

Cela posé, cherchons une formule qui détermine le nombre de valeurs distinctes de la fonction. Soient encore α, β, γ,... les nombres de lettres qui se trouvent respectivement dans le premier groupe (B), dans le deuxième groupes (B), etc., et soient A, B, C,... les nombres de valeurs distinctes qu'acquiert F considérée comme fonction de ces α lettres, de ces β lettres, de ces γ lettres, etc. Désignons ensnite par ν, ρ,... les nombres de lettres qui se trouvent respectivement dans la première série des groupes (A), dans la deuxième série de ces groupes, etc.; enfin désignons par $\mathcal{A}$, $\mathcal{B}$,... les nombres de valeurs distinctes que F acquiert considérée comme fonction des ν lettres de la première série, des ρ lettres de la seconde série, etc.

Alors, par des raisonnements tout à fait semblables à ceux qui nous ont conduit à la formule (u), nous trouverons pour le nombre de valeurs de la fonction considérée

$$(\nu) \quad \frac{1.2.3...n}{1.2...\alpha \times 1.2...\beta \times 1.2...\gamma \times ... \times 1.2...\nu \times 1.2...\rho \times ...} \mathrm{ABC}...\mathcal{A}\mathcal{B}....$$

Si l'on suppose connus les nombres de valeurs de toutes les fonctions transitives qui ont moins de n lettres, A, B, C... seront connues, et il n'y aura plus à déterminer, dans cette formule, que $\mathcal{A}$, $\mathcal{B}$...; c'est ce qui est facile. Cherchons en effet le nombre de valeurs d'une fonction φ de ν lettres qui se décomposent en k groupes contenant chacun q lettres, et tels, que la fonction soit transitive par rapport à ces groupes.

Si la fonction n'était pas transitive par rapport à ces groupes, le nombre de ses valeurs serait

$$\frac{1.2.3...\nu}{\left(\frac{1.2...q}{\mathrm{P}}\right)^k},$$

P étant le nombre de valeurs de φ considérée comme fonction des q lettres d'un des groupes. Mais la fonction étant transitive par rapport aux k groupes, si l'on permute ces k groupes de toutes les manières possibles, on trouvera R valeurs égales, et le nombre des valeurs distinctes de la fonction φ sera

$$\frac{1.2.3...\nu}{\mathrm{R}\left(\frac{1.2...q}{\mathrm{P}}\right)^k};$$

soit encore M le nombre de valeurs distinctes qu'acquiert la fonction quand on permute les k groupes, on aura

$$\mathrm{R} = \frac{1.2...k}{\mathrm{M}},$$

et le nombre des valeurs distinctes de la fonction φ pourra encore être représenté par la formule

$$(t) \qquad \frac{1.2\ldots\nu}{(1.2\ldots k)(1.2\ldots q)^k}\mathrm{MP}^k.$$

On voit donc comment on calculera les quantités $\mathcal{A}$, $\mathcal{B}$,..., et par conséquent comment on pourra déterminer, par la formule (ν), le nombre de valeurs d'une fonction intransitive quelconque de n lettres, quand on connaîtra toutes les fonctions transitives qui ont moins de n lettres.

Comme application de la formule (ν), cherchons le nombre des valeurs de la fonction de vingt lettres

$$(ab^2+cd^2+e)(a'b'^2+c'd'^2+e')(a''b''^2+c''d''^2+e'')+fg(hi^2k^3+ik^2h^3+kh^2i^3).$$

Nous commençons par former ce que nous avons appelé les groupes (A), ils sont au nombre de trois

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

et forment une seule série, c'est-à-dire que la fonction est transitive par rapport à ces trois groupes. Pour obtenir le nombre des valeurs de cette fonction, nous ferons dans la formule (ν) $\alpha=2$, $\beta=3$, $\nu=15$, $\mathrm{A}=1$, $\mathrm{B}=2$, ce qui donnera pour le nombre de valeurs de la fonction

$$(z) \qquad \frac{1.2.3\ldots 19.20}{1.2\times 1.2.3\times 1.2.3.4\ldots 15}\,2\times\mathcal{A}.$$

Nous déterminerons ensuite $\mathcal{A}$ par la formule (t), et nous aurons

$$\mathcal{A}=\frac{1.2.3\ldots 15}{(1.2.3)(1.2.3.4.5)^3}\mathrm{P}^3.$$

Enfin P désigne le nombre de valeurs qu'acquiert la fonction considérée comme fonction des cinq lettres a, b, c, d, e, et on a

$$\mathrm{P}=\frac{1.2.3.4.5}{2}.$$

Par conséquent l'expression (z) devient

$$\frac{1.2.3\ldots 19.20}{1.2\times 1.2.3\times 1.2.3\times 2^2},$$

et c'est le nombre des valeurs de la fonction considérée.

Des fonctions plusieurs fois transitives.

Imaginons une fonction transitive de n lettres ; cette fonction, considérée comme fonction de $n-1$ lettres, pourra elle-même 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 p fois transitive prend toutes ses valeurs considérée comme fonction de $n-p$ lettres. On voit encore qu'une fonction symétrique est une fonction $n-1$ fois transitive.

Une fonction de n lettres qui n'est pas changée par une substitution circulaire de ses n lettres, ni par une substitution circulaire de $n-1$ lettres, ni par une troisième substitution circulaire faite sur $n-2$ d'entre ces dernières, etc., ni par une $\mu^{ième}$ permutation faite sur $n-\mu+1$ lettres obtenues en agissant comme précédemment, est μ fois transitive.

THÉORÈME. — *Si une fonction de n lettres est ω 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 $n-\omega+1$ lettres quelconques.*

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

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

puis par rapport aux lettres

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

puis par rapport aux lettres

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

et ainsi de suite. La fonction étant transitive par rapport aux lettres a, b, $c, \ldots, k, l$, nous pouvons amener une lettre quelconque a' à la place de 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

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

puis par rapport aux lettres

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

et ainsi de suite. Parmi les $n-1$ lettres $b', c', \ldots, k', l'$, nous pouvons en prendre une, 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 les lettres $c'', d'', \ldots, k'', l''$. 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 ω fois transitive, on peut amener ω lettres quelconques à telles places que l'on veut.*

Car dans la démonstration précédente nous avons vu que l'on pouvait amener une lettre quelconque a' à la place de a, ensuite sans déplacer a', nous avons pu amener une quelconque b'' des lettres restantes à la place de b, et ainsi de suite.

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

Supposons, en effet, que dans une fonction on puisse amener ω lettres quelconques à la place de ω autres lettres quelconques. Puisqu'on peut amener une lettre quelconque a' à la place d'une 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 des 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 sera 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 $n-k+1$ lettres, elle est k 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 sera 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 k fois transitive.

THÉORÈME. — *Une fonction ω fois transitive, qui n'est pas changée par une certaine substitution qui ne comprend pas plus de ω 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 ω 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 ω lettres. La fonction étant ω fois transitive à la place des lettres $a, b, c, \ldots, p$, on peut y 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 trois 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 permutation 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 permutation 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 permutation peut s'effectuer par une série de transpositions successives. Si 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 que si une fonction est deux fois transitive, elle est changée par toute transposition de deux lettres (ab). Or si la fonction n'était pas changée par la transposition des deux lettres a et b, c'est-à-dire si elle était symétrique par rapport à ces deux lettres, comme dans la fonction on peut remplacer les lettres a et b par deux lettres quelconques, la fonction serait symétrique par rapport à deux lettres quelconques; donc la fonction serait symétrique par rapport à toutes ses lettres. Donc enfin le théorème est démontré.

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

Car supposons qu'une fonction de n lettres soit ω fois transitive, et que ω soit $> \frac{n}{2}$, et par suite $n - \omega < \frac{n}{2}$. La fonction étant ω fois transitive est changée par toute substitution faite sur ω lettres, elle a donc au moins $1.2.3\ldots\omega$ valeurs. Mais le nombre des valeurs de la fonction doit être aussi un diviseur de $1.2\ldots(n-\omega)$; ce qui est impossible, puisque $n - \omega$ est $< \frac{n}{2}$ et à plus forte raison $< \omega$.

On peut donner de ce qui précède une application assez remarquable. Écrivons la fonction

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

cette fonction n'est pas changée par une quelconque des trois permutations circulaires

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

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.

THÉORÈME. — *Le nombre de valeurs d'une fonction ω fois transitive est divisible par $1.2.3\ldots\omega$, lorsqu'elle a plus de deux valeurs.*

Posons

$$1.2.3\ldots\omega = \Omega$$

et désignons par

$$(1)\qquad V_1,\quad V_2,\quad V_3,\ldots,\quad V_\mu$$

les μ valeurs distinctes de la fonction. Faisons dans V_1 et sur ω lettres déterminées $a, b, \ldots, k$ les Ω permutations possibles, nous aurons Ω valeurs qui sont distinctes d'après le théorème précédent, et qui faisant partie de la série (1) pourront être représentées par

$$(2) \qquad V_1, \quad V_2, \ldots, \quad V_\Omega.$$

Donc on a $\mu = \Omega$ ou $\mu > \Omega$. Si $\mu = \Omega$, la proposition a lieu. Si μ est $> \Omega$, faisons sur $V_{\Omega+1}$ les Ω permutations des lettres $a, b, \ldots, k$, nous aurons la nouvelle série de valeurs distinctes

$$(3) \qquad V_{\Omega+1}, \quad V_{\Omega+2}, \ldots, \quad V_{2\Omega}.$$

et ces valeurs seront toutes distinctes de celles de la série (2); car $V_{\Omega+1}$ n'appartenant pas à la série (2), aucun terme de la série (3) ne saurait lui appartenir. On conclut de là que $\mu = 2\Omega$ ou que μ est $> 2\Omega$.

Si l'on imagine que l'on continue ainsi jusqu'à ce que l'on ait épuisé tous les termes de la série (1), il devient évident que l'on a $\mu = \Omega u$, u étant un nombre entier, et le théorème est démontré.

Théorème de M. Bertrand.

Pour démontrer ce théorème, nous allons commencer par établir le lemme suivant :

Lemme. — Si une fonction transitive de n lettres $a, b, \ldots, f, g, h, \ldots, l$ est symétrique par rapport à plus de la moitié de ses lettres $a, b, \ldots, f$, elle est symétrique par rapport à toutes ses lettres.

En effet, portons une lettre k, prise parmi les lettres $g, h, \ldots, l$, à la place de la lettre a, et permutons toutes les autres de manière que la fonction ne change pas de valeur, la fonction sera nécessairement symétrique par rapport à la lettre k et à une des lettres $a, b \ldots, f$; donc elle sera symétrique par rapport aux lettres $a, b, \ldots, f, k$, et comme ce qui a été dit de k, peut être dit d'une quelconque des lettres $g, h, \ldots, l$, la fonction est symétrique par rapport à toutes ses lettres.

Théorème. — *Une fonction de* n *lettres qui a plus de deux valeurs, en a au moins* n, *si* n *est* > 4.

Considérons d'abord une fonction intransitive. Nous avons vu que le nombre de valeurs d'une fonction intransitive de n lettres était, en général, donné par la formule

$$(\nu)\qquad \frac{1.2.3\ldots n}{1.2\ldots\alpha\times 1.2\ldots\beta\times 1.2\ldots\gamma\times\ldots\times 1.2\ldots\nu\times 1.2\ldots\rho\times\ldots}\mathrm{ABC}\ldots\mathcal{A}\mathcal{B}\ldots$$

La plus grande valeur que puisse avoir le dénominateur est

$$1.2.3\ldots(n-1)\times 1;$$

donc la plus petite valeur que puisse avoir l'expression (ν) est évidemment n.

Il y a cependant un cas où le nombre des valeurs d'une fonction intransitive de n lettres n'est pas donné par la formule (ν) : c'est le cas où toutes les lettres peuvent se décomposer en groupes par rapport auxquels la fonction est transitive. Une telle fonction ne pourra évidemment avoir moins de quatre lettres; si même elle ne renferme que quatre lettres, cette fonction sera nécessairement semblable au type

$$ab^2 + cd^2,$$

et elle aura $\frac{1.2.3.4}{2} = 12$ valeurs. En général, nous avons vu que le nombre de valeurs d'nne telle fonction était donné par la formule

$$(t)\qquad \frac{1.2.3\ldots n}{(1.2\ldots k)(1.2\ldots q)^k}\mathrm{MP}^k;$$

k étant le nombre des groupes, q le nombre des lettres de chaque groupe, M le nombre de valeurs distinctes qu'acquiert la fonction quand on permute les groupes et P le nombre de valeurs distinctes qu'acquiert la fonction quand on permute les lettres d'un groupe. Or nous allons démontrer que l'expression (t) est non-seulement plus grande que n, mais même qu'elle est plus grande que $n(n-1)$.

Cette fonction, considérée comme fonction des q lettres de chaque groupe, est intransitive; car si la fonction était transitive par rapport aux q lettres de chaque groupe, elle serait transitive par rapport à ses n lettres, ce qui est contraire à l'hypothèse. On peut aussi supposer que les q lettres de chaque groupe ne soient pas décomposables en groupes de t lettres tels, que la fonction soit transitive par rapport à ces groupes; car, s'il en était ainsi, on voit aisément que toutes les lettres de la fonction pourraient être partagées en groupes de t lettres de manière que la fonction fût transitive par rapport à tous ces groupes. Donc la fonction considérée comme fonction des q lettres d'un des groupes aura au moins q valeurs; ainsi P est au moins égal à q. Donc, pour démontrer que l'expression (t) est $> n(n-1)$, il suffit de prouver que l'on a

$$\frac{1.2\ldots n}{(1.2\ldots k)(1.2\ldots q)^k} q^k > n(n-1).$$

q^k est $> kq$ ou $> n$ et par suite $> n-1$; il suffit donc de prouver que l'on a l'inégalité

$$\frac{1.2\ldots n}{1.2\ldots k(1.2\ldots q)^k} > n,$$

ou

$$(a) \qquad 1.2\ldots(kq-1) > 1.2\ldots k(1.2\ldots q)^k.$$

Remarquons que l'inégalité (a) a lieu pour $k=2$, $q=3$, et pour $k=3$, $q=2$; nous allons démontrer que si l'inégalité (a) a lieu, on peut dans cette inégalité changer k en $k+1$, ou q en $q+1$ sans que l'inégalité cesse d'avoir lieu, et il est clair qu'il sera alors démontré que l'inégalité (a) aura lieu, quels que soient k et q.

D'abord, si on a l'inégalité (a), on aura aussi l'inégalité

$$(b) \qquad 1.2\ldots[(k+1)q-1] > 1.2\ldots(k+1)(1.2\ldots q)^{k+1},$$

qui est l'inégalité (a) dans laquelle on a changé k en $k+1$. Car pour prouver l'inégalité (b) il suffit de prouver que l'on a

$$kq(kq+1)\ldots(kq+q-1) > (k+1).2.3\ldots q,$$

et cette inégalité est évidente.

En second lieu, si on a l'inégalité (a), on aura aussi l'inégalité

$$(c) \qquad 1.2\ldots[k(q+1)-1] > 1.2\ldots k[1.2\ldots(q+1)]^k,$$

qui est l'inégalité (a), dans laquelle on a changé q en $q+1$; car, pour prouver l'inégalité (c), il suffit de prouver que l'on a

$$kq\,(kq+1)\ldots(kq+k-1) > (q+1)^k;$$

ce qui est évident.

Donc l'inégalité (a) aura lieu si n est >4, et la fonction considérée aura plus de $n\,(n-1)$ valeurs, excepté toutefois dans le cas de $n=4$; dans ce cas le nombre des valeurs est précisément $n\,(n-1)$.

Donc aussi une fonction intransitive de n lettres quelconque a au moins n valeurs.

Actuellement revenons à la formule (ν); la partie fractionnaire de cette expression est le coefficient de $r^\alpha s^\beta t^\gamma \ldots r'^\nu s'^\rho \ldots$ dans le développement de

$$(r+s+t+\ldots+r'+s'+\ldots)^n;$$

elle est donc un multiple de l'un des coefficients renfermés dans le développement de $(r+s)^n$, c'est-à-dire un multiple de l'un des nombres de la suite

$$n,\quad \frac{n(n-1)}{2},\quad \frac{n(n-1)(n-2)}{1.2.3},\ \ldots,$$

qui devra être arrêtée à son plus grand terme.

La formule (ν) ne peut donner n pour résultat, qu'autant qu'elle devient

$$\frac{1.2.3\ldots n}{1.2\ldots(n-1)\times 1},$$

et par conséquent une fonction intransitive de n lettres, qui a n valeurs, est symétrique par rapport à $n-1$ lettres.

Considérons maintenant une fonction transitive. Cette fonction transitive prendra toutes ses valeurs considérée comme fonction de $n-1$ lettres.

Supposons-la d'abord intransitive considérée comme fonction de ces $n-1$ lettres. Si le nombre des valeurs de la fonction est donné par la formule (ν) (lorsqu'on y change n en $n-1$), il sera un multiple de l'un des nombres

$$n-1,\quad \frac{(n-1)(n-2)}{1.2},\ \ldots$$

Le nombre des valeurs de la fonction ne peut être $n-1$; car cette fonction serait symétrique par rapport à $n - 2$ lettres, ce qui est impossible, d'après le lemme démontré ci-dessus, à moins que n ne soit égal à 4. Donc si n est > 4, le nombre des valeurs de la fonction sera au moins égal à $2(n-1)$ ou à $\frac{(n-1)(n-2)}{2}$, nombres $> n$.

Si le nombre des valeurs de la fonction intransitive de $n - 1$ lettres n'est pas donné par la formule (ν), le nombre des valeurs de la fonction sera au moins égal à $(n-1)(n-2)$; or dans ce cas $n - 1$ n'est pas < 4, et par suite $(n-1)(n-2)$ est $> n$. Donc enfin une fonction une seule fois transitive a plus de n valeurs, si n est > 4.

Supposons en second lieu que la fonction soit deux fois transitive, et qu'elle ne le soit pas davantage. Considérée comme fonction de $n-2$ lettres, elle sera intransitive, et si le nombre de ses valeurs est donné par la formule (ν), il sera un multiple de l'un des nombres

$$n-2, \qquad \frac{(n-2)(n-3)}{1.2}, \ldots.$$

Si ce nombre était $n - 2$, la fonction serait symétrique par rapport à $n - 3$ lettres; or une fonction deux fois transitive ne peut être symétrique par rapport à deux lettres; donc si n est > 4, la fonction aura plus de $n - 2$ valeurs. Donc la fonction aura un nombre de valeurs au moins égal à l'un des nombres $2(n-2)$ et $\frac{(n-2)(n-3)}{2}$, et ces nombres ne peuvent être supérieurs à $n - 2$, sans être au moins égaux à n.

Si le nombre des valeurs de la fonction intransitive de $n - 2$ lettres n'est pas donné par la formule (ν) le nombre des valeurs de la fonction sera $> (n-2)(n-3)$; or dans ce cas $n - 2$ n'est pas < 4, et par suite $(n-2)(n-3)$ est $> n$. Donc enfin une fonction qui est deux fois transitive sans l'être davantage, a au moins n valeurs, si n est > 4.

Supposons en dernier lieu que la fonction soit trois fois transitive; la fonction aura encore au moins n valeurs. Imaginons, en effet, qu'elle puisse avoir moins de n valeurs, et transposons dans la fonction la lettre a avec chacune des $n - 1$ autres; nous aurons ainsi, en comptant la première fonction, n fonctions résultantes. La fonction considérée ayant moins de n valeurs, ces n fonctions ne seront pas distinctes. Donc au moins deux des n transpositions que nous avons faites donneront des résultats équivalents, et la transposition (ac) donnera par exemple la même fonction que la transposition (ad). Donc si on fait sur la fonction la transposition (ac), puis la transposition (ad), ou, ce qui est la même chose, la permutation circulaire de trois lettres (acd), la fonction ne changera pas de valeur. Or, comme la fonction est trois fois transitive, on peut y mettre à la place des lettres a, c, d trois lettres quelconques; la fonction n'est donc changée par aucune permutation circulaire de trois lettres, et, par suite, elle a au plus deux valeurs. Donc une fonction trois fois transitive qui a plus de deux valeurs en a au moins n, et le théorème qui nous occupait, est enfin démontré.

ÉTUDE DE PLUSIEURS FONCTIONS TRANSITIVES.

Étude de la fonction de n lettres, qui a deux valeurs.

THÉORÈME. — *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 v de toutes les différences de ces n lettres, nous aurons

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

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

Toute fonction de n lettres, qui a deux valeurs, est $n-2$ fois transitive.

En effet, rappelons-nous qu'une fonction intransitive quelconque de n lettres a au moins n valeurs; donc une fonction de n lettres qui n'a que deux valeurs est transitive : la même fonction considérée comme fonction de $n-1$ lettres n'aura que deux valeurs; donc elle est encore transitive par rapport à ces $n-1$ lettres, et si on imagine que l'on continue ainsi, il devient évident que la fonction est $n-2$ fois transitive. Par conséquent aussi la fonction acquiert toutes ses valeurs par les permutations de deux lettres, ou, ce qui revient au même, la fonction est changée par une transposition quelconque.

On peut, d'après cela, trouver facilement la forme générale des fonctions qui ont deux valeurs. Soit en effet F une telle fonction, et désignons par F et F_1 ces deux valeurs. Le produit Fv n'aura aussi que deux valeurs; car une transposition quelconque change F en F_1 et v en $-v$, et deux transpositions ne changent pas F et v. Si donc on fait une permutation qui équivaut à un nombre impair de transpositions, F et v seront changés respectivement en F_1 et $-v$, et si on fait une permutation qui équivaut à un nombre pair de transpositions, F et v ne seront pas changés. Il est donc clair que Fv n'a que deux valeurs, qui sont Fv et $-F_1v$; on a donc

$$F + F_1 = \varphi,$$
$$Fv - F_1 v = \psi,$$

φ et ψ étant des fonctions symétriques. De ces équations, on déduit

$$F = \frac{\varphi}{2} + \frac{\psi}{2v^2}v,$$

ou

$$F = \Phi + \Psi v,$$

si l'on pose

$$\Phi = \frac{\varphi}{2}, \quad \Psi = \frac{\psi}{2v^2},$$

Φ et Ψ étant par conséquent deux fonctions symétriques.

THÉORÈME. — *La fonction de n lettres qui a deux valeurs, est changée par toute permutation circulaire faite sur un nombre pair de lettres, et elle n'est changée par aucune permutation circulaire faite sur un nombre impair de lettres.*

Supposons que l'on ait à faire une permutation circulaire sur α lettres, et qu'elle soit $(a, b, c, d, \ldots, g)$. Pour faire cette permutation, on pourra transposer a avec b, puis a avec c, puis a avec d, et ainsi de suite; et l'on fera ainsi $\alpha - 1$ transpositions. Or, à chaque transposition, la fonction change de valeur; donc si α est pair, la fonction change de valeur après la substitution circulaire, 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 permutation 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 permutation; si le nombre de ces cycles est impair, la fonction est changée par la permutation.

COROLLAIRE. — *Si l'on multiplie une fonction φ, qui n'est pas changée par* *une substitution circulaire de $2r$ lettres par la fonction des mêmes lettres, qui a deux valeurs, on obtient une fonction* F, *qui a un nombre de valeurs double de la première.*

En effet, imaginons écrites les μ valeurs de la fonction φ, puis multiplions-les par la fonction qui a deux valeurs, nous aurons μ valeurs de la fonction F. Faisons ensuite sur chacune de ces μ valeurs de F la permutation circulaire de $2r$ lettres qui ne change pas φ. Cette permutation changera la fonction qui a deux valeurs; on obtiendra donc ainsi μ valeurs de F différentes entre elles et différentes des premières. La fonction F a donc effectivement 2μ valeurs.

Ainsi par exemple la fonction

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

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

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

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 ne sera pas changée par les permutations

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

elle sera donc aussi deux fois transitive.

D'une fonction transitive de n lettres qui a $\dfrac{1.2\ldots(n-1)}{2}$ valeurs.

THÉORÈME. — *On peut toujours former une fonction transitive de n lettres qui ait $\dfrac{1.2\ldots(n-1)}{2}$ valeurs.*

Supposons d'abord que n soit impair, et soient $a, b, \ldots, f, g, h, g_1, \ldots, b_1, a_1$ les n lettres; considérons la fonction

$$\varphi\,[a,\, b,\, c, \ldots,\, f,\, g,\, (h),\, g_1, f_1, \ldots,\, c_1,\, b_1,\, a_1]$$

qui n'est pas changée par la substitution de $n-1$ lettres

$$(\beta) \qquad (aa_1)(bb_1)(cc_1)\ldots(gg_1).$$

Faisons sur cette fonction $n-1$ fois la permutation circulaire

$$(\alpha) \qquad (abc\ldots fghg_1f_1\ldots b_1a_1)$$

et nous aurons les n fonctions suivantes :

$$\left\{\begin{array}{l}
\varphi[a, b, c, \ldots\ldots, e, f, g, (h), g_1, f_1, e_1, \ldots\ldots c_1, b_1, a_1], \\
\varphi[b, c, d, \ldots\ldots, f, g, h, (g_1), f_1, e_1, \ldots\ldots c_1, b_1, a_1, a], \\
\varphi[c, d, \ldots\ldots, g, h, g_1, (f_1), e_1, \ldots\ldots b_1, a_1, a, b], \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\varphi[b_1, a_1, a, \ldots\ldots e, (f), g, h, g_1, \ldots\ldots d_1, c_1], \\
\varphi[a_1, a, b, c, \ldots\ldots f, (g), h_1, g_1, \ldots\ldots d_1, c_1, b_1].
\end{array}\right.$$

Prenons une fonction symétrique de ces n fonctions; cette fonction F n'est pas changée par la permutation (α) et aussi par la permutation (β), comme il est aisé de le reconnaître. La fonction F est donc transitive, et si on rend immobile la lettre h, les lettres restantes pourront se décomposer en deux gronpes $a, b, c, \ldots, g$ et $a_1, b_1, c_1, \ldots, g_1$, tels, que la fonction soit symétrique par rapport à ces deux groupes; elle a donc bien $\frac{1.2\ldots(n-1)}{2}$ valeurs.

Supposons en second lieu que n soit pair. Soient

$$a, b, c, \ldots, g, h, g_1, f_1, \ldots, a_1, h_1$$

les n lettres, et soit

$$\varphi[a, b, c, \ldots, e, f, g, (h), g_1, f_1, e_1, \ldots, c_1, b_1, a_1, (h_1)]$$

une fonction qui n'est pas changée par la substitution

$$(\gamma) \qquad (aa_1)(bb_1)(cc_1)\ldots(gg_1).$$

Faisons sur cette fonction la substitution circulaire

$$(\delta) \qquad (abc\ldots efghg_1f_1e_1\ldots b_1, a_1, h_1)$$

et nous aurons les n fonctions

$$\left\{\begin{array}{l}
\varphi\,[a,\, b,\, c,\ldots\ldots,\, e,\, f,\, g,\, (h),\, g_1,\, f_1,\, e_1,\ldots\ldots,\, c_1,\, b_1,\, a_1,\, (h_1)],\\
\varphi\,[b,\, c,\, d,\ldots\ldots,\, f,\, g,\, h,\, (g_1),\, f_1,\, e_1,\ldots\ldots,\, c_1,\, b_1,\, a_1,\, h_1,\, (a)\,],\\
\varphi\,[c,\, d,\ldots\ldots,\, g,\, h,\, g_1,\, (f_1),\, e_1,\ldots\ldots\ldots,\, b_1,\, a_1,\, h_1,\, a,\, (b)],\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\varphi\,[a_1,\, h_1,\, a,\, b,\ldots\ldots,\, e,\, (f),\, g,\, h,\, g_1,\ldots\ldots\ldots\ldots,\, d_1,\, c_1,\, (b_1)],\\
\varphi\,[h_1,\, a,\, b,\, c,\ldots\ldots\ldots,\, f,\, (g),\, h,\, g_1,\, f_1,\, \ldots\ldots\ldots,\, c_1,\, b_1,\, (a_1)].
\end{array}\right.$$

Prenons une fonction symétrique de ces n fonctions; cette fonction sera transitive, puisqu'elle n'est pas changée par la substitution circulaire (δ); il est aisé de reconnaître que la fonction n'est pas changée par la permutation (γ); elle a donc $\frac{1.2\ldots(n-1)}{2}$ valeurs.

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

Soit m un nombre premier, et substituons dans l'expression

$$(x_0 + a x_1 + a^2 x_2 + \ldots + a^{m-1} x_{m-1})^m$$

à la place de a chacune des racines imaginaires $\alpha, \alpha^2, \ldots, \alpha^{m-1}$ de l'équation

$$x^m - 1 = 0,$$

nous aurons les $m-1$ expressions suivantes :

$$(\mathrm{A})\quad \left\{\begin{array}{l}
\theta_1\;\;\;\; = (x_0 + \alpha x_1 \quad + \alpha^2 x_2 \quad + \ldots + \alpha^{m-1} x_{m-1})^m,\\
\theta_2\;\;\;\; = (x_0 + \alpha^2 x_1 \quad + \alpha^{2.2} x_2 \quad + \ldots + \alpha^{2(m-1)} x_{m-1})^m,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\theta_p\;\;\;\; = (x_0 + \alpha^p x_1 \quad + \alpha^{p.2} x_2 \quad + \ldots + \alpha^{p(m-1)} x_{m-1})^m,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\theta_{m-1} = (x_0 + \alpha^{m-1} x_1 + \alpha^{(m-1)2} x_2 + \ldots + \alpha^{(m-1)(m-1)} x_{m-1})^m.
\end{array}\right.$$

Prenons ensuite une fonction symétrique de ces θ, et nous aurons une fonction qui a été considérée pour la première fois par Lagrange, et que nous allons étudier avec détail.

Nous reconnaissons d'abord que les différentes expressions (A) ne sont pas changées par la permutation circulaire $(x_0 x_1 x_2 \ldots x_{m-1})$. En effet, considérons

$$(c) \qquad \theta_p = (x_0 + \alpha^p x_1 + \alpha^{p.2} x_2 + \ldots + \alpha^{p(m-1)} x_{m-1})^m.$$

Sans changer la valeur de θ_p, nous pouvons multiplier le polynôme par α^{m-p} avant de l'élever à la puissance $m^{ième}$ et écrire

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

ou encore, puisque l'on a $\alpha^m = 1$,

$$(d) \qquad \theta_p = (x_1 + \alpha^p x_2 + \alpha^{2p} x_3 + \ldots + \alpha^{(m-2)p} x_{m-1} + \alpha^{(m-1)p} x_0)^m.$$

On passe de l'expression (c) à l'expression (d) par la permutation circulaire de m lettres

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

donc θ_p n'est pas changé par cette permutation, et par suite aussi cette permutation ne change pas la fonction symétrique des expressions (A).

Écrivons l'expression (c) de θ_p

$$\theta_p = (\Sigma \alpha^{\mu p} x_\mu)^m$$

et convenons que si β et γ sont deux entiers, on aura

$$x_{\beta m + \gamma} = x_\gamma \quad \text{et} \quad \theta_{\beta m + \gamma} = \theta_\gamma.$$

Déterminons les deux nombres entiers s et n, compris entre 0 et m, qui satisfont aux deux congruences

$$sp \equiv 1 \pmod m, \qquad \mu p \equiv n \pmod m;$$

nous tirerons de là

$$\mu p \equiv nps \pmod{m};$$

et puisque m est un nombre premier et que p est $< m$, on a

$$\mu \equiv ns \pmod{m}.$$

L'expression de θ_p peut donc s'écrire

$$(f) \qquad \theta_p = (\Sigma \alpha^n x_{ns})^m.$$

Actuellement, désignons par k une racine primitive de m, et par ω la racine primitive de m associée à k telle, par conséquent, que l'on ait

$$\omega k \equiv 1 \pmod{m};$$

puis faisons dans la formule (f) successivement $p = 1$ et $s = 1$, $p = k$ et $s = \omega$, $p = k^2$ et $s = \omega^2$, et ainsi de suite, nous aurons

$$(g) \qquad \left\{ \begin{array}{ll} \theta_1 & = (\Sigma \alpha^n x_n)^m, \\ \theta_k & = (\Sigma a^n x_{n\omega})^m, \\ \theta_{k^2} & = (\Sigma \alpha^n x_{n\omega^2})^m, \\ \multicolumn{2}{l}{\dots\dots\dots\dots\dots,} \\ \theta_{k^{m-2}} & = (\Sigma \alpha^n x_{n\omega^{m-2}})^m, \end{array} \right.$$

qui sont évidemment les expressions (A) prises dans un autre ordre. Or il est aisé de voir que l'on passe de θ_{k^i} à $\theta_{k^{i+1}}$ en changeant en général $x_{n\omega_i}$ en $x_{n\omega^{i+1}}$, et comme on peut poser $n\omega^i = \omega^\nu \pmod{m}$, on passe de θ_{k^i} à $\theta_{k^{i+1}}$ en changeant en général x_{ω^ν} en $x_{\omega^{\nu+1}}$. Il suit de là évidemment que l'on passe d'une des expressions (g) à la suivante au moyen de la substitution circulaire

$$(x_1 \, x_\omega \, x_{\omega^2} \dots x_{\omega^{m-2}}).$$

Donc la fonction symétrique des expressions (g), ou, ce qui est la même chose, la fonction symétrique des expressions (A), n'est pas changée par cette permutation.

La fonction symétrique des expressions (A) est évidemment changée par toute permutation faite sur moins de $m-1$ lettres; elle n'est pas changée par les deux substitutions circulaires

$$(p)\qquad (x_0, x_1, x_2, \ldots, x_{m-1}),\ (x_1, x_\omega, x_{\omega^2}, \ldots, x_{\omega^{m-2}});$$

donc cette fonction est deux fois transitive, et elle a $1.2\ldots(m-2)$ valeurs. Faisons sur cette fonction la première de ces deux permutations, les variables x_1, x_{ω^2}, x_{ω^3}, etc., seront remplacées respectivement par x_2, $x_{1+\omega}$, $x_{1+\omega^2}$, etc., et, par conséquent, puisque la fonction n'est pas changée par $(x_1\ x_\omega\ x_{\omega^2}\ldots x_{\omega^{m-2}})$, elle n'est pas changée non plus par la substitution circulaire

$$(x_2, x_{1+\omega}, x_{1+\omega^2}, \ldots, x_{1+\omega^{m-2}});$$

on voit de la même manière que la fonction n'est pas changée par les permutations circulaires

$$\begin{array}{llll}
(x_3 & x_{2+\omega} & x_{2+\omega^2}\ldots & x_{2+\omega^{m-2}}),\\
(x_4 & x_{3+\omega} & x_{3+\omega^2}\ldots & x_{3+\omega^{m-2}}),\\
\ldots & \ldots & \ldots & \ldots\\
(x_0 & x_{m-1+\omega} & x_{m-1+\omega^2}\ldots & x_{m-1+\omega^{m-2}}),
\end{array}$$

et ainsi la fonction symétrique des expressions (A) n'est pas changée par une permutation circulaire de m lettres, et par m permutations circulaires de $m-1$ lettres.

Actuellement soit $\varphi[(x_0), x_1, x_\omega, x_{\omega^2}, \ldots, x_{\omega^{m-2}}]$ une fonction qui ne soit pas changée par la permutation circulaire $(x_1, x_\omega, x_{\omega^2}, \ldots, x_{\omega^{m-2}})$, faisons sur cette fonction m fois la permutation circulaire

$$(q)\qquad (x_0\, x_1\, x_2\ldots x_{m-1}),$$

nous aurons les m fonctions

$$(C)\quad \left\{\begin{array}{lllll}
\varphi[(x_0), & x_1, & x_\omega, & x_{\omega^2}, \ldots, & x_{\omega^{m-2}}] = \varphi_0\\
\varphi[(x_1), & x_2, & x_{1+\omega}, & x_{1+\omega^2}, \ldots, & x_{1+\omega^{m-2}}] = \varphi_1,\\
\varphi[(x_2), & x_3, & x_{2+\omega}, & x_{2+\omega^2}, \ldots, & x_{2+\omega^{m-2}}] = \varphi_2,\\
\ldots & \ldots & \ldots & \ldots & \ldots\\
\varphi[(x_{m-1}), & x_0, & x_{m-1+\omega}, & x_{m-1+\omega^2}, \ldots, & x_{m-1+\omega^{m-2}}] = \varphi_{m-1}.
\end{array}\right.$$

Prenons une portion symétrique Φ des fonctions (C), et nous aurons la forme générale des fonctions deux fois transitives de m lettres, qui sont semblables à la fonction symétrique des expressions (A).

Remarquons d'abord que la fonction Φ n'est pas changée par la substitution (q), puisqu'on passe d'une des fonctions (C) à la suivante par cette permutation ; je dis, en second lieu, qu'elle n'est pas changée par la permutation

$$(r) \qquad (x_1\, x_\omega\, x_{\omega^2} \ldots x_{\omega^{m-2}});$$

en effet, par cette permutation, φ_0 ne sera pas changé, et φ_k, qui a pour expression

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

deviendra

$$\varphi\left[(x_{k\omega}),\ x_{k\omega+\omega},\ x_{k\omega+\omega^2},\ x_{k\omega+\omega^3},\ldots,\ x_{k\omega+1}\right].$$

Or, puisque cette dernière fonction n'est pas changée par la permutation

$$(x_{k\omega+\omega}\, x_{k\omega+\omega^2}\, x_{k\omega+\omega^3} \ldots x_{k\omega+1}),$$

si nous lui faisons subir cette substitution $m-2$ fois, elle ne changera pas de valeur; elle est donc égale à

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

c'est-à-dire à $\varphi_{k\omega}$; ainsi la permutation (r) change la fonction φ_k en $\varphi_{k\omega}$. D'après cela, dans une circonférence inscrivons un polygone régulier de m côtés; aux sommets successifs de ce polygone, mettons respectivement $\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_{m-1}$; faisons sur ces fonctions φ la permutation (r), les fonctions $\varphi_0, \varphi_1, \ldots \varphi_{m-1}$ se trouveront par cette permutation transportées respectivement aux sommets successifs d'un polygone régulier étoilé de m côtés, donc le côté sous-tendra un arc égal à $\omega\frac{2\pi}{m}$. La fonction Φ n'est donc pas changée par la permutation (r); enfin la fonction Φ n'étant pas changée par les deux permutations (p), elle est semblable à la fonction symétrique des expressions (A).

Reprenons les expressions (A); elles sont, à l'ordre près,

$$
\text{(D)}\quad\left\{
\begin{array}{l}
(x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{m-1} x_{m-1})^m, \\
(x_0 + \alpha x_\omega + \alpha^2 x_{2\omega} + \ldots + \alpha^{m-1} x_{(m-1)\omega})^m, \\
(x_0 + \alpha x_{\omega^2} + \alpha^2 x_{2\omega^2} + \ldots + \alpha^{m-1} x_{(m-1)\omega^2})^m, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
(x_0 + \alpha x_{\omega^s} + \alpha^2 x_{2\omega^s} + \ldots + \alpha^{m-1} x_{(m-1)\omega^s})^m, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,
\end{array}
\right.
$$

Supposons que $m-1$ soit égal à su; prenons parmi les fonctions (D) celles qui occupent les rangs marqués par les nombres $1, s+1, 2s+1, 3s+1, \ldots, (u-1)s+1$; la fonction symétrique de ces u termes ne sera évidemment pas changée par la permutation circulaire

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

et elle ne sera pas changée non plus si on fait sur elle s fois la substitution circulaire

$$(x_1\, x_\omega\, x_{\omega^2} \ldots x_{\omega^{m-2}}),$$

autrement dit, elle ne sera pas changée non plus par la permutation régulière

$$(\nu)\ (x_1\, x_{\omega^s}\, x_{\omega^{2s}} \ldots x_{\omega^{(u-1)s}})(x_\omega\, x_{\omega^{s+1}}\, x_{\omega^{2s+1}} \ldots x_{\omega^{(u-1)s+1}}) \ldots (x_{\omega^{s-1}}\, x_{\omega^{2s-1}}\, x_{\omega^{3s-1}} \ldots x_{\omega^{m-2}}).$$

Remarquons ensuite que cette permutation faite sur les $m-1$ lettres $x_1, x_2, \ldots x_{m-1}$ revient à une permutation circulaire sur les u groupes de s lettres

$$
\begin{array}{lllll}
x_1, & x_\omega, & x_{\omega^2}, \ldots, & x_{\omega^{s-1}}, \\
x_{\omega^s}, & x_{\omega^{s+1}}, & x_{\omega^{s+2}}, \ldots, & x_{\omega^{2s-1}}, \\
x_{\omega^{2s}}, & x_{\omega^{2s+1}}, & x_{\omega^{2s+2}}, \ldots, & x_{\omega^{3s-1}}, \\
\ldots & \ldots & \ldots & \ldots
\end{array}
$$

Cette fonction qui acquiert toutes ses valeurs, considérée comme fonction des $m-1$ lettres $x_1, x_2, \ldots, x_{m-1}$ a donc $\dfrac{1.2\ldots(m-1)}{\dfrac{1.2\ldots u}{1.2\ldots(u-1)}}$ ou $\dfrac{1.2\ldots(m-1)}{u}$ valeurs, et nous avons le théorème suivant :

Soit m un nombre premier, et u un diviseur de $m-1$, il y a toujours une fonction transitive de m lettres qui a $\dfrac{1.2\ldots(m-1)}{u}$ valeurs.

Ainsi dans le cas particulier où m est égal à 7, u est égal à 1, 2, 3 ou 6, et ce théorème donne quatre fonctions transitives de 7 lettres, qui ont respectivement pour le nombre de leurs valeurs :

$$1.2.3.4.5.6=720,\ \frac{1.2.3.4.5.6}{2}=360,\ \frac{1.2.3.4.5.6}{3}=240,\ \frac{1.2.3.4.5.6}{6}=120.$$

Considérons de nouveau les fonctions (C), et ne supposons plus que la fonction φ_0 ne soit pas changée par la permutation

$$(x_1 \quad x_\omega \quad x_{\omega^2}\ldots \quad x_{\omega^{m-2}}),$$

mais supposons qu'elle ne soit pas changée seulement par la permutation régulière (ν) ; il est encore aisé de voir que la fonction symétrique Φ des fonctions (C) n'est pas changée par la permutation circulaire

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

et par la permutation (ν).

La fonction Φ n'est évidemment pas changée par la première de ces permutations, puisqu'on passe d'une des fonctions (C) à la suivante par cette permutation.

Faisons ensuite la permutation (ν), φ_0 ne change pas de valeur, et

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

se change en

$$\varphi\left[(x_{k\omega^s}), \quad x_{k\omega^s+\omega^s}, \quad x_{k\omega^s+\omega^{s+1}}, \ldots, \quad x_{k\omega^s+\omega^{m-2+s}}\right];$$

or, on a

$$\varphi_{k\omega^s} = \varphi\left[(x_{k\omega^s}), \quad x_{k\omega^s+1}, \quad x_{k\omega^s+\omega}, \ldots, \quad x_{k\omega^s+\omega^{m-2}}\right];$$

et de même que φ_0 n'est pas changée par la permutation (ν), $\varphi_{k\omega^s}$ n'est pas changée par la permutation

$$(x_{k\omega^s+1} \quad x_{k\omega^s+\omega^s} \quad x_{k\omega^s+\omega^{2s}} \ldots)(x_{k\omega^s+\omega} \quad x_{k\omega^s+\omega^{s+1}} \quad x_{k\omega^s+\omega^{2s+1}} \ldots)\ldots,$$

on a donc

$$\varphi_{k\omega^s} = \varphi\left[(x_{k\omega^s}), \quad x_{k\omega^s+\omega^s}, \quad x_{k\omega^s+\omega^{s+1}}, \ldots, \quad x_{k\omega^s+\omega^{m-2+s}}\right].$$

Ainsi la permutation (ν) change φ_k en $\varphi_{k\omega^s}$, et les expressions φ_0, φ_1, $\varphi_2, \ldots, \varphi_{m-1}$ sont changées par cette permutation en φ_0, φ_{ω^s}, $\varphi_{2\omega^s}, \ldots,$ $\varphi_{(m-1)\omega^s}$ qui sont les mêmes fonctions prises dans un autre ordre; donc la fonction Φ n'est pas changée par la permutation (ν) et par la permutation $(x_0, x_1, x_2, \ldots, x_{m-1})$ et elle a $\frac{1.2\ldots(m-1)}{u}$ valeurs.

Nous avons trouvé la forme générale des fonctions deux fois transitives de m lettres, qui ont $1.2\ldots(m-2)$ valeurs, lorsque m est un nombre premier; nous sommes alors conduits tout naturellement à nous demander s'il n'existe pas une fonction trois fois transitive de $m+1$ lettres, qui ait $1.2.3\ldots(m-2)$ valeurs, et qui, considérée comme fonction de m lettres, soit la fonction deux fois transitive que nous avons étudiée, et qui, par conséquent, ne soit pas changée par les deux substitutions

$$(z) \qquad (x_0 x_1 x_2 \ldots x_{m-1}), \qquad (x_1 x_\omega x_{\omega^2} \ldots x_{\omega^{m-2}});$$

or nous allons démontrer que cette fonction existe effectivement, en sorte que l'on a ce théorème :

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

Nous allons donner de plus la forme générale de cette fonction.

Soit

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

une fonction qui ne soit pas changée par la permutation circulaire

$$(x_1 x_\omega x_{\omega^2} \ldots x_{\omega^{m-2}});$$

nous avons vu que l'on a la forme générale des fonctions deux fois transitives, qui ont $1.2\ldots(m-2)$ valeurs en prenant une fonction symétrique des fonctions suivantes :

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

Désignons la fonction symétrique des fonctions (C) par

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

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

$$(k)\qquad (x'_0\, x'_1\, x'_2\, x'_3\ldots x'_{m-1}),$$

x'_1, x'_2, x'_3, etc., étant déterminés par les égalités

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

nous obtiendrons, en faisant cette permutation 1 fois, 2 fois,..., $m-1$ fois, m fonctions en comptant la fonction (F). Considérons encore la fonction

$$(\mathrm{G})\qquad \Phi(x'_0, x_1, x_{\omega^{m-2}}, x_{\omega^{m-3}},\ldots, x_\omega),$$

que nous obtenons en changeant, dans la fonction (F), x_0, x_1, $x_2\ldots$, x_{m-1}, x'_0 respectivement en x'_0, x'_1, x'_2,..., x'_{m-1}, x_0 ; enfin prenons une fonction symétrique Θ de ces $m+1$ fonctions; je dis que cette fonction Θ n'est pas changée par les permutations (z) et (k), et, par suite, qu'elle est trois fois transitive et qu'elle a $1.2\ldots(m-2)$ valeurs.

Il est facile de reconnaître d'abord que la fonction Θ n'est pas changée par la permutation (k) et par la permutation

$$(n)\qquad (x_1\, x_\omega\, x_{\omega^2}\ldots x_{\omega^{m-2}}).$$

En effet la fonction (F) n'est pas changée par la permutation (n), et, par suite, elle n'est pas changée par

$$(x_1\, x_{\omega^{m-1}}\, x_{\omega^{m-2}} \ldots x_{\omega^2}\, x_{\omega}),$$

ou par

$$(k') \qquad (x'_1\, x'_{\omega}\, x'_{\omega^2} \ldots x'_{\omega^{m-1}});$$

donc, d'après ce que nous avons démontré précédemment, la fonction (F) n'étant pas changée par la permutation (k'), si on fait sur la fonction (F) 1 fois, 2 fois,..., m fois la permutation (k), on obtiendra m fonctions, et toute fonction symétrique de ces m fonctions n'est pas changée par les permutations (k) et (k') ou par les permutations (k) et (n). D'ailleurs, de même que la fonction (F) n'est pas changée par les permutations (z), la fonction (G) n'est pas changée par les permutations (k) et (k'); donc la fonction Θ n'est pas changée par les permutations (k) et (n).

Reste donc à démontrer que la fonction Θ n'est pas changée par la permutation

$$(l) \qquad (x_0\, x_1\, x_2 \ldots x_{m-1}).$$

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

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

En général, si on a $x_a = x'_b$, c'est que l'on a

$$ab \equiv 1 \pmod{m}.$$

Convenons que dans ce qui va suivre $\frac{1}{a}$ représentera le nombre entier b, et que $\frac{1}{b}$ représentera le nombre entier a, alors les fonctions (C) pourront s'écrire

$$
(\mathrm{H})\left\{\begin{array}{l}
\varphi\left[(x_0),\quad x'_1,\quad x'_{\frac{1}{\omega}},\quad x'_{\frac{1}{\omega^2}},\quad x'_{\frac{1}{\omega^3}},\ldots\ldots,\quad x'_{\frac{1}{\omega^{m-2}}}\right],\\
\varphi\left[(x'_1),\quad x'_{\frac{1}{2}},\quad x'_{\frac{1}{1+\omega}},\quad x'_{\frac{1}{1+\omega^2}},\quad x'_{\frac{1}{1+\omega^3}},\ldots\ldots,\quad x'_{\frac{1}{1+\omega^{m-2}}}\right],\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\varphi\left[\left(x'_{\frac{1}{r}}\right),\quad x'_{\frac{1}{r+1}},\quad x'_{\frac{1}{r+\omega}},\quad x'_{\frac{1}{r+\omega^2}},\quad x'_{\frac{1}{r+\omega^3}},\ldots\ldots,\quad x'_{\frac{1}{r+\omega^{m-2}}}\right],\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\varphi\left[\left(x'_{\frac{1}{m-1}}\right),\quad x_0,\quad x'_{\frac{1}{m-1+\omega}},\quad x'_{\frac{1}{m-1+\omega^2}},\quad x'_{\frac{1}{m-1+\omega^3}},\ldots,\quad x'_{\frac{1}{m-1+\omega^{m-2}}}\right].
\end{array}\right.
$$

La fonction (F) est une fonction symétrique des fonctions (H). Faisons sur (F) t fois la permutation (k), la fonction qui résultera sera la fonction symétrique de ces fonctions :

$$
(\mathrm{I})\left\{\begin{array}{l}
\varphi\left[(x_0),\quad x'_{1+t},\quad x'_{\frac{1}{\omega}+t},\quad x'_{\frac{1}{\omega^2}+t},\quad x'_{\frac{1}{\omega^3}+t},\ldots\ldots,\quad x'_{\frac{1}{\omega^{m-2}}+t}\right],\\
\varphi\left[(x'_{1+t}),\quad x'_{\frac{1}{2}+t},\quad x'_{\frac{1}{1+\omega}+t},\quad x'_{\frac{1}{1+\omega^2}+t},\quad x'_{\frac{1}{1+\omega^3}+t},\ldots\ldots,\quad x'_{\frac{1}{1+\omega^{m-2}}+t}\right],\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\varphi\left[\left(x'_{\frac{1}{r}+t}\right),\quad x'_{\frac{1}{r+1}+t},\quad x'_{\frac{1}{r+\omega}+t},\quad x'_{\frac{1}{r+\omega^2}+t},\quad x'_{\frac{1}{r+\omega^3}+t},\ldots\ldots,\quad x'_{\frac{1}{r+\omega^{m-2}}+t}\right],\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\varphi\left[\left(x'_{\frac{1}{m-1}+t}\right),\quad x_0,\quad x'_{\frac{1}{m-1+\omega}+t},\quad x'_{\frac{1}{m-1+\omega^2}+t},\quad x'_{\frac{1}{m-1+\omega^3}+t},\ldots,\quad x'_{\frac{1}{m-1+\omega^{m-2}}+t}\right].
\end{array}\right.
$$

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

$$
(\mathrm{K})\quad\left\{\begin{array}{l}
\varphi\left[(x'_0), \quad x_1, \quad x_{\frac{1}{\omega}}, \quad x_{\frac{1}{\omega^2}}, \quad x_{\frac{1}{\omega^3}}, \ldots, \quad x_{\frac{1}{\omega^{m-2}}}\right],\\
\varphi\left[(x_1) \quad x_{\frac{1}{2}}, \quad x_{\frac{1}{1+\omega}}, \quad x_{\frac{1}{1+\omega^2}}, \quad x_{\frac{1}{1+\omega^3}}, \ldots, \quad x_{\frac{1}{1+\omega^{m-2}}}\right],\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\varphi\left[\left(x_{\frac{1}{r}}\right), \quad x_{\frac{1}{r+1}}, \quad x_{\frac{1}{r+\omega}}, \quad x_{\frac{1}{r+\omega^2}}, \quad x_{\frac{1}{r+\omega^3}}, \ldots, \quad x_{\frac{1}{r+\omega^{m-2}}}\right],\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\varphi\left[\left(x_{\frac{1}{m-1}}\right), \quad x'_0, \quad x_{\frac{1}{m-1+\omega}}, \quad x_{\frac{1}{m-1+\omega^2}}, \quad x_{\frac{1}{m-1+\omega^3}}, \ldots, \quad x_{\frac{1}{m-1+\omega^{m-2}}}\right],
\end{array}\right.
$$

et si l'on fait sur la fonction (G) u fois la permutation (l), on aura une fonction symétrique de ces fonctions :

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

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

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

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

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

d'où les congruences :

$$
(a)\qquad \left.\begin{array}{r}
\dfrac{1}{r} + u \equiv 0 \\[2ex]
(1+t)\left(\dfrac{1}{r+\omega^{\sigma}} + u\right) \equiv 1 \\[2ex]
\left(\dfrac{1}{\omega} + t\right)\left(\dfrac{1}{r+\omega^{\sigma+1}} + u\right) \equiv 1 \\[2ex]
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\[2ex]
\left(\dfrac{1}{\omega^{p}} + t\right)\left(\dfrac{1}{r+\omega^{\sigma+p}} + u\right) \equiv 1 \\[2ex]
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{array}\right\} \pmod{m}
$$

Au moyen des trois premières congruences, on trouve :

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

et ces valeurs satisfont effectivement à la congruence générale (a). Ainsi la première des fonctions (I) est égale à la $(r+1)^{ième}$ des fonctions (L), si r, u et ω^{σ} ont les valeurs (b).

Recherchons maintenant si r, u et ω^{σ} ayant les valeurs (b), toutes les fonctions (I) sont égales aux fonctions (L); voyons donc si la deuxième des fonctions (I) est égale à la $(r+1+\tau)^{ième}$ des fonctions (L), la troisième des fonctions (I) égale à la $(r+1+2\tau)^{ième}$ des fonctions (L), etc., et en général si la $(\nu+1)^{ième}$ des fonctions (I) est égale à la $(r+1+\nu\tau)^{ième}$ des fonctions (L).

Si la deuxième des fonctions (I) est égale à la $(r+1+\tau)^{ième}$ des fonctions (L), on a les congruences :

$$
\left.\begin{array}{l}
(1+t)\left(\dfrac{1}{r+\tau} + u\right) \equiv 1, \\[2ex]
\left(\dfrac{1}{1+\omega^{0}} + t\right)\left(\dfrac{1}{r+\tau+\omega^{\sigma}} + u\right) \equiv 1, \\[2ex]
\left(\dfrac{1}{1+\omega} + t\right)\left(\dfrac{1}{r+\tau+\omega^{\sigma+1}} + u\right) \equiv 1, \\[2ex]
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\[2ex]
\left(\dfrac{1}{1+\omega^{p}} + t\right)\left(\dfrac{1}{r+\tau+\omega^{\sigma+p}} + u\right) \equiv 1, \\[2ex]
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{array}\right\} \pmod{m}.
$$

En général, si la $(\nu+1)^{ième}$ des fonctions (I) est égale à la $(r+1+\nu\tau)^{ième}$ des fonctions (K), on a les congruences :

$$\left.\begin{array}{l}
\left(\frac{1}{\nu}+t\right)\left(\frac{1}{r+\tau\nu}+u\right)\equiv 1,\\
\left(\frac{1}{\nu+\omega^{0}}+t\right)\left(\frac{1}{r+\tau\nu+\omega^{\sigma}}+u\right)\equiv 1,\\
\left(\frac{1}{\nu+\omega}+t\right)\left(\frac{1}{r+\tau\nu+\omega^{\sigma+1}}+u\right)\equiv 1,\\
\dots\dots\dots\dots\dots\dots\\
\left(\frac{1}{\nu+\omega^{p}}+t\right)\left(\frac{1}{r+\tau\nu+\omega^{\sigma+p}}+u\right)\equiv 1,\\
\dots\dots\dots\dots\dots\dots
\end{array}\right\}\pmod m.$$

On trouve que ces congruences sont satisfaites pour les valeurs (b) 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 permutations (z) et (k).

Ayant déterminé cette fonction trois fois transitive, nous reconnaissons immédiatement qu'*il y a une fonction deux fois transitive de* $m+1$ *lettres qui a* $1.2\ldots(m-2)\times 2$ *valeurs.*

Soient, en effet, P et P′ deux fonctions semblables à Θ, et soit

$$\psi=(x_0-x_1)(x_0-x_2)\ldots(x_0-x_{m-1})(x_0-x'_0)(x_1-x_2)\ldots(x_{m-1}-x'_0);$$

$P+P'\psi$ est une fonction qui n'est pas changée par les permutations

$$\begin{array}{l}
(x_1\,x_{\omega^2}\,x_{\omega^4}\ldots x_{\omega^{m-3}})(x_{\omega}\,x_{\omega^3}\,x_{\omega^5}\ldots x_{\omega^{m-2}}),\\
(x_0\,x_1\,x_2\,x_3\ldots x_{m-1}),\\
(x'_0\,x'_1\,x'_2\,x'_3\ldots x'_{m-1});
\end{array}$$

elle est donc transitive par rapport à $m+1$ lettres et par rapport à m lettres, mais elle ne l'est pas par rapport à $m-1$ lettres; c'est donc bien une fonction deux fois transitive qui a $1.2\ldots(m-2)\times 2$ valeurs.

Vu et approuvé,
Le 20 janvier 1859,
LE DOYEN DE LA FACULTÉ DES SCIENCES,
MILNE EDWARDS.

Permis d'imprimer,
Le 20 janvier 1859,
LE VICE-RECTEUR DE L'ACADÉMIE DE PARIS,
ARTAUD.

THÈSE D'ASTRONOMIE.

PROPOSITION D'ASTRONOMIE DONNÉE PAR LA FACULTÉ.

Donner l'explication mathématique des principales inégalités des satellites de Jupiter.

Vu et approuvé,

Le 20 janvier 1859,

LE DOYEN DE LA FACULTÉ DES SCIENCES,

MILNE EDWARDS.

Permis d'imprimer,

Le 20 janvier 1859,

LE VICE-RECTEUR DE L'ACADÉMIE DE PARIS,

ARTAUD.

Paris. — Imprimerie de Mallet-Bachelier, rue du Jardinet, 12.