304.

ANALYSE MATHÉMATIQUE. — *Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières, et des systèmes de substitutions conjuguées.*

C. R., T. XXI, p. 835 (13 octobre 1845).

§ I. — *Des substitutions régulières ou irrégulières.*

Considérons une substitution relative au système de plusieurs variables $x, y, z, \ldots$. En supposant cette substitution réduite à sa plus simple expression, je la nommerai *régulière* lorsqu'elle se réduira, soit à une seule substitution circulaire, soit au produit de plusieurs substitutions circulaires de même ordre. Je la nommerai au contraire *irrégulière* lorsqu'elle sera le produit de plusieurs substitutions circulaires d'ordres différents. Cela posé, l'ordre d'une substitution régulière sera évidemment l'ordre de chacun de ses facteurs circulaires. De plus, une telle substitution jouira de cette propriété remarquable, qu'une quelconque de ses puissances, distinctes de l'unité, sera encore une substitution régulière, qui renfermera toutes les variables comprises dans la première. Ainsi, en particulier, si l'on pose

$$P(x, y, z, u, v, w),$$

P sera une substitution régulière, et même circulaire du sixième ordre, dont les diverses puissances

$$P^2, \quad P^3, \quad P^4, \quad P^5$$

seront des substitutions régulières du troisième, du second et du sixième ordre. On aura, par exemple,

$$P^2 = (x, z, v)(y, u, w),$$
$$P^3 = (x, u)(y, v)(z, w).$$

Au contraire, les diverses puissances d'une substitution irrégulière

seront, les unes régulières, les autres irrégulières, et celles qui seront régulières ne renfermeront qu'une partie des variables comprises dans la substitution donnée. Ainsi, par exemple, si l'on pose

$$P = (x, y, z)(u, v),$$

P sera une substitution irrégulière du sixième ordre, et

$$P^5 = (x, z, y)(u, v)$$

sera encore une substitution irrégulière du sixième ordre. Mais

$$P^2 = (x, z, y), \qquad P^3 = (u, v), \qquad P^4 = (x, y, z)$$

seront des substitutions régulières du troisième ou du second ordre, dont chacune ne renfermera nécessairement qu'une partie des variables comprises dans P.

Si l'on désigne généralement par i le nombre des variables que renferme une substitution régulière P, l'ordre a de cette substitution et le nombre b de ses facteurs circulaires seront évidemment liés à i par la formule

$$i = ab.$$

Cela posé, concevons que l'on range sur a lignes horizontales distinctes, et sur b lignes verticales, les i variables comprises dans P, en plaçant à la suite l'une de l'autre, dans une même ligne horizontale, les variables qui se suivent immédiatement dans un même facteur circulaire de P. On obtiendra encore une substitution régulière Q de l'ordre i, en prenant, pour facteurs de Q, a substitutions circulaires de l'ordre b, dans chacune desquelles seront placées, à la suite l'une de l'autre, les variables que renferme une même ligne verticale. De plus, il est clair que les deux substitutions

$$P, \quad Q,$$

dont l'une aura pour effet unique d'échanger entre elles les lignes verticales, tandis que l'autre aura pour effet unique d'échanger entre elles les lignes horizontales, seront deux substitutions permutables entre elles, par conséquent deux substitutions dont les dérivées seront toutes comprises dans chacun des Tableaux

$$(1)\qquad \left\{\begin{array}{lllll} 1, & P, & P^2, & \ldots, & P^{a-1}, \\ Q, & QP, & QP^2, & \ldots, & QP^{a-1}, \\ Q^2, & Q^2P, & Q^2P^2, & \ldots, & Q^2P^{a-1}, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots, \\ Q^{b-1}, & Q^{b-1}P, & Q^{b-1}P^2, & \ldots, & Q^{b-1}P^{a-1}; \end{array}\right.$$

$$(2)\qquad \left\{\begin{array}{lllll} 1, & P, & P^2, & \ldots, & P^{a-1}, \\ Q, & PQ, & P^2Q, & \ldots, & P^{a-1}Q, \\ Q^2, & PQ^2, & P^2Q^2, & \ldots, & P^{a-1}Q^2, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots, \\ Q^{b-1}, & PQ^{b-1}, & P^2Q^{b-1}, & \ldots, & P^{a-1}Q^{b-1}, \end{array}\right.$$

et formeront un système de substitutions conjuguées de l'ordre $i=ab$.

Si, pour fixer les idées, on pose

$$i=4=2\times 2,$$

alors, avec les quatre variables

$$\begin{array}{ll} x, & y, \\ z, & u, \end{array}$$

rangées sur deux lignes horizontales et sur deux lignes verticales, on pourra composer les deux substitutions régulières

$$P=(x,y)(z,u) \quad \text{et} \quad Q=(x,z)(y,u),$$

qui seront permutables entre elles; et ces deux substitutions formeront, avec leurs dérivées

$$1 \quad \text{et} \quad PQ=QP,$$

un système de substitutions conjuguées

$$\begin{array}{ll} 1, & P, \\ Q, & PQ \end{array}$$

qui sera du quatrième ordre. Pareillement, si l'on pose

$$i=6=3\times 2,$$

alors, avec les six variables

$$\begin{array}{lll} x, & y, & z, \\ u, & v, & w, \end{array}$$

rangées sur deux lignes horizontales et sur trois lignes verticales, on pourra composer les deux substitutions régulières

$$P=(x,y,z)(u,v,w), \qquad Q=(x,u)(y,v)(z,w),$$

qui seront permutables entre elles; et ces deux substitutions formeront, avec leurs dérivées, un système de substitutions conjuguées qui sera du sixième ordre. Au reste, ce dernier système ne sera autre chose que le système des puissances de la substitution circulaire

$$(x,w,y,u,z,v),$$

dont P et Q représentent les facteurs primitifs.

Au lieu de ranger les i variables données sur a lignes horizontales et sur b lignes verticales, on pourrait représenter ces variables par une seule lettre s affectée de deux indices, et représenter même les deux systèmes d'indices par deux nouveaux systèmes de lettres

$$\alpha,\ \beta,\ \gamma,\ \ldots,\qquad \lambda,\ \mu,\ \nu,\ \ldots.$$

Ainsi, par exemple, on pourrait représenter les six variables

$$\begin{array}{lll} x, & y, & z, \\ u, & v, & w \end{array}$$

par

$$\begin{array}{lll} s_{\alpha,\lambda}, & s_{\beta,\lambda}, & s_{\gamma,\lambda}, \\ s_{\alpha,\mu}, & s_{\beta,\mu}, & s_{\gamma,\mu}, \end{array}$$

et alors les substitutions

$$P=(x,y,z)(u,v,w), \qquad Q=(x,u)(y,v)(z,w)$$

s'offriraient sous les formes

$$P=(\alpha,\beta,\gamma), \qquad Q=(\lambda,\mu),$$

qui rendraient sensibles les propriétés qu'ont ces deux substitutions d'être permutables entre elles.

Concevons maintenant que le nombre entier

$$i = abc\ldots$$

soit décomposable en plusieurs facteurs $a, b, c, \ldots$, égaux ou inégaux. Alors on pourra représenter i variables diverses

$$x,\ y,\ z,\ \ldots$$

par une seule lettre s affectée de plusieurs indices, le nombre l de ces indices étant égal au nombre des facteurs $a, b, c, \ldots$, et représenter même les divers systèmes d'indices par divers systèmes de lettres

$$\begin{array}{llll} \alpha, & \beta, & \gamma, & \ldots, \\ \lambda, & \mu, & \nu, & \ldots, \\ \varphi, & \chi, & \psi, & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots \end{array}$$

Cela posé, les substitutions P, Q, ... qui, étant exprimées à l'aide des lettres $\alpha, \beta, \gamma, \ldots, \lambda, \mu, \nu, \ldots, \varphi, \chi, \psi, \ldots$, se présenteront sous les formes

$$(3)\quad P = (\alpha, \beta, \gamma, \ldots), \qquad Q = (\lambda, \mu, \nu, \ldots), \qquad R = (\varphi, \chi, \psi, \ldots), \qquad \ldots,$$

seront évidemment des substitutions permutables entre elles, la première de l'ordre a, la seconde de l'ordre b, la troisième de l'ordre c, ..., et elles composeront, avec leurs dérivées, un système de substitutions conjuguées dont l'ordre sera

$$i = abc\ldots.$$

Ajoutons que, si les substitutions (3) sont exprimées à l'aide des i lettres

$$x,\ y,\ z,\ \ldots,$$

chacune d'elles sera une substitution régulière qui renfermera toutes ces lettres, P étant le produit de $\frac{i}{a}$ facteurs circulaires de l'ordre a, Q étant pareillement le produit de $\frac{i}{b}$ facteurs circulaires de l'ordre b, ...

Dans le cas particulier où les l facteurs $a, b, c, \ldots$ deviennent égaux entre eux, on a

$$i = a^l,$$

et les substitutions

$$P,\ Q,\ R,\ \ldots$$

forment avec leurs dérivées un système de a^l substitutions diverses qui sont toutes de l'ordre a, si a est un nombre premier, à l'exception de celle qui se réduit à l'unité.

§ II. — *Des substitutions semblables.*

Soient

$$A,\ B,\ C,\ D$$

quatre arrangements formés avec n variables

$$x,\ y,\ z,\ \ldots.$$

En vertu des définitions adoptées, les deux substitutions

$$(1)\qquad P = \binom{B}{A}, \qquad Q = \binom{D}{C}$$

seront *semblables* entre elles, si elles diffèrent uniquement par la forme des lettres qui, dans ces deux substitutions, occupent les mêmes places. Alors, non seulement les deux substitutions P, Q seront du même ordre, mais elles offriront le même nombre de facteurs circulaires et le même nombre de lettres dans les facteurs circulaires correspondants. Alors aussi on aura

$$(2)\qquad \binom{D}{B} = \binom{C}{A},$$

et réciproquement, si la condition (2) est remplie, les deux substitutions

$$P = \binom{B}{A}, \qquad Q = \binom{D}{C}$$

seront semblables l'une à l'autre.

Concevons maintenant que l'on pose

$$\begin{pmatrix}C\\A\end{pmatrix}=R.$$

Alors on tirera de la formule (2), non seulement

$$\begin{pmatrix}D\\B\end{pmatrix}=\begin{pmatrix}C\\A\end{pmatrix}=R,$$

mais encore

$$\begin{pmatrix}B\\D\end{pmatrix}=\begin{pmatrix}A\\C\end{pmatrix}=R^{-1}.$$

D'ailleurs, on aura identiquement

$$Q=\begin{pmatrix}D\\C\end{pmatrix}=\begin{pmatrix}D\\B\end{pmatrix}\begin{pmatrix}B\\A\end{pmatrix}\begin{pmatrix}A\\C\end{pmatrix}.$$

Donc, eu égard aux formules

$$\begin{pmatrix}D\\B\end{pmatrix}=R,\qquad \begin{pmatrix}B\\A\end{pmatrix}=P,\qquad \begin{pmatrix}A\\C\end{pmatrix}=R^{-1},$$

on aura encore

$$Q=RPR^{-1}.\tag{3}$$

Si l'on posait

$$S=R^{-1}=\begin{pmatrix}A\\C\end{pmatrix},$$

la formule (3) deviendrait

$$Q=S^{-1}QS.\tag{4}$$

Nous pouvons donc conclure de ce qui précède que, P étant une substitution quelconque, toute substitution semblable à P sera de la forme

$$RPR^{-1}$$

ou, ce qui revient au même, de la forme

$$S^{-1}PS.$$

En d'autres termes, *toute substitution semblable à* P *sera le produit de*

trois facteurs dont les deux extrêmes seront inverses l'un de l'autre, le facteur moyen étant précisément la substitution donnée P. Réciproquement, *tout produit de trois facteurs dont les deux extrêmes seront deux substitutions inverses l'une de l'autre, le facteur moyen étant la substitution* P, *sera une substitution semblable à* P.

Concevons maintenant que P, Q soient deux substitutions quelconques semblables ou dissemblables. Les produits

$$PQ,\quad QP$$

seront, dans tous les cas, non seulement des substitutions de même ordre, comme je l'ai remarqué dans un précédent article, mais encore des substitutions semblables entre elles. En effet, si l'on pose

$$R=PQ,\qquad S=QP,$$

on en conclura, d'une part,

$$P=Q^{-1}S$$

et, par suite,

$$R=Q^{-1}SQ;$$

d'autre part,

$$Q=P^{-1}R$$

et, par suite,

$$S=P^{-1}RP.$$

§ III. — *Des systèmes de substitutions régulières et conjuguées.*

Considérons un système de n variables

$$x,\ y,\ z,\ \ldots.$$

Soient d'ailleurs a un nombre entier égal ou inférieur à n, et ha un multiple de h contenu dans n. Enfin, concevons qu'avec ah variables, prises au hasard, on forme h groupes divers composés chacun de a lettres, et nommons

$$P_1,\ P_2,\ \ldots,\ P_h\tag{1}$$

h substitutions circulaires de l'ordre a, dont chacune soit formée avec les variables comprises dans un seul groupe. Ces substitutions étant permutables entre elles, le système de ces mêmes substitutions et de leurs dérivées sera de l'ordre

$$a^h.$$

Ajoutons que, si a est un nombre premier, le système dont il s'agit renfermera seulement des substitutions régulières de l'ordre a, dont quelques-unes, savoir les substitutions (1) et leurs puissances, se réduiront à des substitutions circulaires de l'ordre a.

Soient maintenant b un nombre égal ou inférieur à h, et kb un multiple de b contenu dans h. Avec plusieurs des précédents groupes que j'appellerai groupes de première espèce, on pourra composer des groupes de seconde espèce, dont chacun embrasse b groupes de première espèce, et dont le nombre soit égal à k. Cela posé, nommons

$$(2)\qquad Q_1,\ Q_2,\ \dots,\ Q_b$$

des substitutions dont chacune consiste à permuter circulairement entre eux les b groupes de première espèce compris dans un seul groupe de seconde espèce. Chacune des substitutions (2), exprimée à l'aide des variables primitives, sera une substitution régulière équivalente au produit de a facteurs circulaires dont chacun sera de l'ordre b; et ces substitutions seront permutables, non seulement entre elles, mais encore avec les substitutions (1). Par suite, le système des substitutions (1) et (2) et de leurs dérivées sera de l'ordre

$$a^h b^k.$$

Ajoutons que, si a et b sont des nombres premiers, le système dont il s'agit se composera uniquement de substitutions régulières, les unes de l'ordre a, les autres de l'ordre b.

En continuant ainsi, on établira généralement la proposition suivante :

Théorème I. — *Considérons un système de n variables $x, y, z, \dots$. Soient d'ailleurs a un nombre entier, égal ou inférieur à n, et $i = ha$ un multiple de a contenu dans n. Soient encore b un nombre entier, égal ou inférieur à h, et kb un multiple de b contenu dans h. Soient pareillement c un nombre entier, égal ou inférieur à k, et lc un multiple de c contenu dans k. On pourra toujours former, avec i variables arbitrairement choisies, un système de substitutions conjuguées dont l'ordre sera représenté par le produit*

$$a^h b^k c^l \dots,$$

les facteurs circulaires de l'une quelconque de ces substitutions étant tous des puissances de substitutions circulaires de l'ordre a, ou de l'ordre b, ou de l'ordre c, ... Par suite, si les divers nombres $a, b, c, \dots$ sont tous des nombres premiers, le système dont il s'agit se composera uniquement de substitutions régulières dont chacune sera de l'ordre a, ou de l'ordre b, ou de l'ordre c, ...

Corollaire. — En supposant les nombres $a, b, c, \dots$ tous égaux à un même nombre premier p, on déduit immédiatement du théorème I la proposition suivante :

Théorème II. — *Considérons un système de n variables. Soit d'ailleurs p un nombre premier égal ou inférieur à n. Soient encore $i = hp$ un multiple de p contenu dans n, kp un multiple de p contenu dans h, lp un multiple de p contenu dans k, ... Avec i variables arbitrairement choisies, on pourra toujours former un système de substitutions conjuguées et régulières, dont chacune sera de l'ordre p, l'ordre du système étant représenté par le produit*

$$p^h p^k p^l \dots = p^{h+k+l+\dots}.$$

Corollaire. — Rien n'empêche d'admettre que, dans le théorème précédent, on désigne par hp le plus grand multiple de p contenu dans n, par kp le plus grand multiple de p contenu dans h, par lp le plus grand multiple de p contenu dans k, ... Alors

$$p^{h+k+l+\dots}$$

se réduit à la plus haute puissance de p qui divise exactement le produit

$$N = 1.2.3\dots n,$$

et par suite on obtient, à la place du théorème II, la proposition suivante :

Théorème III. — *Considérons un système de n variables $x, y, z, \ldots$. Soient d'ailleurs p un nombre premier, égal ou inférieur à n, i le plus grand multiple de p contenu dans n, et p^f la plus haute puissance de p qui divise exactement le produit*

$$N = 1.2.3\ldots n.$$

Avec plusieurs des variables $x, y, z, \ldots$, choisies arbitrairement en nombre égal à i, on pourra toujours former un système de substitutions régulières conjuguées, dont chacune sera de l'ordre p, l'ordre du système étant p^f.

§ IV. — *Sur diverses propriétés remarquables des systèmes de substitutions conjuguées.*

Soient

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

les divers arrangements qui peuvent être formés avec n variables

$$x,\ y,\ z,\ \ldots,$$

et qui sont en nombre égal à N, la valeur de N étant

$$N = 1.2.3\ldots n.$$

Les substitutions

$$\binom{A}{A},\ \binom{B}{A},\ \binom{C}{A},\ \ldots, \tag{1}$$

dont le nombre est encore N, et dont la première se réduit à l'unité, formeront toujours un système de substitutions conjuguées, l'ordre de ce système étant précisément le nombre N.

Soit maintenant

$$1,\ P,\ Q,\ \ldots \tag{2}$$

un système de substitutions conjuguées qui, étant d'un ordre M infé-

rieur à N, renferme seulement quelques-uns des termes compris dans la suite (1), et désignons par U, V, W, ... des substitutions qui fassent partie de la suite (1), sans être comprises dans la suite (2). Si l'on désigne par m le nombre des termes de la suite

$$1,\ U,\ V,\ W,\ \ldots, \tag{3}$$

le Tableau

$$\left\{\begin{array}{lllll} 1, & P, & Q, & R, & \ldots, \\ U, & UP, & UQ, & UR, & \ldots, \\ V, & VP, & VQ, & VR, & \ldots, \\ W, & WP, & WQ, & WR, & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots \end{array}\right. \tag{4}$$

offrira m suites diverses composées chacune de M termes, et tous les termes de chaque suite seront distincts les uns des autres. Si d'ailleurs deux suites différentes, par exemple la seconde et la troisième, offraient des termes égaux, en sorte qu'on eût

$$VQ = UP,$$

on en conclurait

$$V = UPQ^{-1}$$

ou simplement

$$V = US,$$

$S = PQ^{-1}$ étant un terme de la suite (2). Donc alors, dans le Tableau (4), le premier terme V de la troisième suite serait déjà un des termes de la seconde. Donc tous les termes du Tableau (4) seront distincts les uns des autres, si le premier terme de chaque suite est pris en dehors des suites précédentes. Or, concevons que, en remplissant toujours cette condition, l'on ajoute sans cesse au Tableau (4) de nouvelles suites, en faisant croître ainsi le nombre m. On ne pourra être arrêté dans cette opération qu'à l'instant où le Tableau (4) renfermera les N termes compris dans la suite (1). Mais alors on aura évidemment

$$N = mM. \tag{5}$$

Donc M sera un diviseur de N, et l'on peut énoncer la proposition suivante :

THÉORÈME I. — *L'ordre d'un système de substitutions conjuguées, relatives à n variables, est toujours un diviseur du nombre N des arrangements que l'on peut former avec ces mêmes variables.*

Corollaire. — Il est bon d'observer qu'au Tableau (4) on pourrait substituer un autre Tableau de la forme

$$(6)\qquad \left\{\begin{array}{lllll} 1, & P, & Q, & R, & \ldots, \\ U, & PU, & QU, & RU, & \ldots, \\ V, & PV, & QV, & RV, & \ldots, \\ W, & PW, & QW, & RW, & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots \end{array}\right.$$

Soit maintenant

$$(7)\qquad 1,\ \mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots$$

un nouveau système de substitutions conjuguées, et nommons $\mathfrak{M}$ l'ordre de ce système. Soient, de plus,

$$(8)\qquad 1,\ \mathfrak{U},\ \mathfrak{V},\ \mathfrak{W},\ \ldots$$

quelques-unes des substitutions situées en dehors de la suite (7), et formons le Tableau

$$(9)\qquad \left\{\begin{array}{lllll} 1, & \mathfrak{P}, & \mathfrak{Q}, & \mathfrak{R}, & \ldots, \\ \mathfrak{U}, & \mathfrak{P}\mathfrak{U}, & \mathfrak{Q}\mathfrak{U}, & \mathfrak{R}\mathfrak{U}, & \ldots, \\ \mathfrak{V}, & \mathfrak{P}\mathfrak{V}, & \mathfrak{Q}\mathfrak{V}, & \mathfrak{R}\mathfrak{V}, & \ldots, \\ \mathfrak{W}, & \mathfrak{P}\mathfrak{W}, & \mathfrak{Q}\mathfrak{W}, & \mathfrak{R}\mathfrak{W}, & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots \end{array}\right.$$

Chacune des substitutions comprises dans ce Tableau, étant l'une de celles que l'on peut former avec les n variables $x, y, z, \ldots$, se confondra nécessairement avec l'un des termes du Tableau (4). De plus, si deux termes compris dans une même ligne horizontale du Tableau (9), par exemple $\mathfrak{P}\mathfrak{U}$ et $\mathfrak{Q}\mathfrak{U}$, se retrouvent dans une même ligne horizontale,

par exemple dans la troisième du Tableau (4), en sorte qu'on ait

$$(10)\qquad \mathfrak{P}\mathfrak{U} = VR, \qquad \mathfrak{Q}\mathfrak{U} = VS,$$

R, S étant deux termes quelconques de la suite (2), on tirera des équations (10), non seulement

$$\mathfrak{U}^{-1}\mathfrak{P}^{-1} = R^{-1}V^{-1},$$

mais encore

$$(11)\qquad \mathfrak{U}^{-1}\mathfrak{P}^{-1}\mathfrak{Q}\mathfrak{U} = R^{-1}S,$$

et par suite la substitution $\mathfrak{P}^{-1}\mathfrak{Q}$, que représente un terme de la suite (7), sera semblable à la substitution $R^{-1}S$, qui représente un terme de la suite (2). Enfin, si deux termes compris dans deux lignes horizontales du Tableau (9), par exemple

$$\mathfrak{P}\mathfrak{V} \quad \text{et} \quad \mathfrak{Q}\mathfrak{U},$$

se retrouvent dans une même ligne horizontale du Tableau (4), en sorte qu'on ait, par exemple,

$$\mathfrak{P}\mathfrak{V} = VR, \qquad \mathfrak{Q}\mathfrak{U} = VS,$$

on en conclura, non seulement

$$\mathfrak{V}^{-1}\mathfrak{P}^{-1} = R^{-1}V^{-1},$$

mais encore

$$\mathfrak{V}^{-1}\mathfrak{P}^{-1}\mathfrak{Q}\mathfrak{U} = R^{-1}S$$

et

$$(12)\qquad \mathfrak{V}R^{-1}S = \mathfrak{P}^{-1}\mathfrak{Q}\mathfrak{V}.$$

Donc alors la suite horizontale qui renfermerait le facteur $\mathfrak{V}$ dans le Tableau (4) renfermerait aussi un terme $\mathfrak{P}^{-1}\mathfrak{Q}\mathfrak{V}$ évidemment compris dans la troisième suite horizontale du Tableau (9). Cela posé, pour que les divers termes du Tableau (9) soient distincts les uns des autres, et appartiennent tous à des suites horizontales distinctes du Tableau (4), il suffira évidemment : 1° qu'aucune des substitutions

$$\mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots$$

ne soit semblable à l'une des substitutions

$$P,\ Q,\ R,\ \ldots,$$

2° que, après avoir formé une ou plusieurs lignes horizontales du Tableau (9), on prenne toujours pour premier terme de la ligne suivante une substitution située, non seulement en dehors des lignes précédentes, mais encore en dehors des lignes horizontales du Tableau (4) qui renferment les divers termes appartenant aux lignes déjà écrites du Tableau (9). Or, en supposant ces deux conditions remplies, concevons que l'on allonge de plus en plus le Tableau (9), en ajoutant sans cesse à ce Tableau de nouvelles suites horizontales. On ne pourra être arrêté dans cette opération qu'à l'instant où le Tableau (9) renfermera un terme pris dans chacune des lignes horizontales du Tableau (4); et comme d'ailleurs, à cet instant, deux termes distincts du Tableau (9) seront encore deux termes qui appartiendront à deux lignes horizontales distinctes du Tableau (4), il est clair que le nombre m de ces lignes horizontales sera égal au nombre des termes du Tableau (9), par conséquent à un multiple du nombre $\mathfrak{M}$ des termes

$$1,\ \mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots,$$

renfermés dans la première ligne horizontale du Tableau (9). On peut donc énoncer la proposition suivante :

Théorème II. — *Soient*

$$1,\ P,\ Q,\ R,\ \ldots,$$
$$1,\ \mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots$$

deux systèmes de substitutions conjuguées, et relatives à n variables diverses. Désignons par M et par $\mathfrak{M}$ les ordres de ces deux systèmes, et posons, non seulement

$$N = 1.2.3\ldots n,$$

mais encore

$$m = \frac{N}{M}, \qquad \mathfrak{m} = \frac{N}{\mathfrak{M}}.$$

Si aucune des substitutions

$$P,\ Q,\ R,\ \ldots$$

n'est semblable à l'une des substitutions

$$\mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots,$$

alors $\mathfrak{M}$ sera un diviseur de m, et M un diviseur de $\mathfrak{m}$, en sorte que chacun des rapports égaux

$$\frac{m}{\mathfrak{M}},\quad \frac{\mathfrak{m}}{M},\quad \frac{N}{\mathfrak{M}M},\quad \frac{m\mathfrak{m}}{N} \tag{13}$$

sera un nombre entier.

Le théorème II entraîne évidemment la proposition suivante :

Théorème III. — *Soient*

$$1,\ P,\ Q,\ R,\ \ldots,$$
$$1,\ \mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots$$

deux systèmes de substitutions conjuguées, et relatives à n variables diverses. Soient d'ailleurs M, $\mathfrak{M}$ les ordres de ces deux systèmes. Si le produit $M\mathfrak{M}$ n'est pas un diviseur du produit

$$N = 1.2.3\ldots n,$$

alors l'une au moins des substitutions

$$P,\ Q,\ R,\ \ldots$$

sera semblable à l'une des substitutions

$$\mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots.$$

Soient maintenant p un nombre premier égal ou inférieur à n, et p^f la plus haute puissance de p qui divise le produit

$$N = 1.2.3\ldots n.$$

On pourra, d'après ce qui a été dit dans le § III, supposer que la suite

$$1,\ \mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots$$

représente un système de substitutions régulières conjuguées dont chacune soit de l'ordre p, l'ordre $\mathfrak{M}$ du système étant égal à p^f. D'autre part, si le nombre m n'est pas un multiple de p^f, le rapport

$$M = \frac{N}{m},$$

dont le numérateur N est un multiple de p^f, sera certainement un nombre divisible par p. Donc le théorème III entraînera la proposition suivante :

Théorème IV. — *Soit M l'ordre d'un certain système*

$$1, \ P, \ Q, \ R, \ \ldots$$

de substitutions conjuguées. Si p est un facteur premier de M, le système dont il s'agit renfermera au moins une substitution régulière de l'ordre p.

Corollaire I. — Il suit, par exemple, du théorème précédent que, si l'ordre du système de substitutions conjuguées est un nombre pair, ce système renfermera au moins une substitution régulière du second ordre.

Corollaire II. — Lorsque le nombre p est supérieur à $\frac{n}{2}$, la substitution régulière de l'ordre p, comprise dans le système donné, ne peut être évidemment qu'une substitution circulaire.

§ V. — *Conséquences remarquables des principes établis dans les paragraphes précédents.*

Les principes établis dans les précédents paragraphes entraînent avec eux plusieurs conséquences, qu'il importe de signaler, relativement au nombre des valeurs égales ou distinctes que peut acquérir une fonction de n variables indépendantes, lorsqu'on permute ces variables entre elles de toutes les manières possibles. Ainsi, en particulier, les théorèmes II, III et IV du § IV entraînent immédiatement les propositions suivantes :

Théorème I. — *Soient Ω une fonction de n variables*

$$x, \ y, \ z, \ \ldots,$$

et m le nombre des valeurs distinctes de cette fonction. Soit encore $\mathfrak{M}$ l'ordre d'un certain système de substitutions conjuguées,

$$1, \ \mathfrak{P}, \ \mathfrak{Q}, \ \mathfrak{R}, \ \ldots.$$

Si aucune des substitutions

$$\mathfrak{P}, \ \mathfrak{Q}, \ \mathfrak{R}, \ \ldots$$

n'est semblable à l'une des substitutions

$$P, \ Q, \ R, \ \ldots,$$

qui possèdent la propriété de ne pas altérer la valeur de Ω, m sera divisible par $\mathfrak{M}$.

Nota. — On pourrait établir directement ce dernier théorème, en observant que, si

$$\Omega, \ \Omega', \ \Omega'', \ \ldots$$

représentent les valeurs distinctes de la fonction donnée, toute substitution semblable à l'une de celles qui n'altéreront pas Ω aura certainement la propriété de ne pas altérer une des fonctions Ω', Ω'', ...

Théorème II. — *Soient Ω une fonction de n variables*

$$x, \ y, \ z, \ \ldots,$$

et m le nombre des valeurs distinctes de cette fonction. Soit, de plus, $\mathfrak{M}$ l'ordre d'un certain système de substitutions conjuguées

$$1, \ \mathfrak{P}, \ \mathfrak{Q}, \ \mathfrak{R}, \ \ldots.$$

Si $\mathfrak{M}$ n'est pas un diviseur de m, l'une au moins des substitutions

$$P, \ Q, \ R, \ \ldots,$$

qui possèdent la propriété de ne pas altérer la valeur de la fonction Ω, sera semblable à l'une des substitutions

$$\mathfrak{P}, \ \mathfrak{Q}, \ \mathfrak{R}, \ \ldots.$$

Corollaire I. — Rien n'empêche de supposer que les substitutions $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{R}$, ... se réduisent à une seule substitution circulaire dont l'ordre soit un nombre premier quelconque p. Alors, à la place du théorème II, on obtient la proposition suivante :

Théorème III. — *Soient Ω une fonction de n variables, m le nombre des valeurs distinctes de cette fonction, et p un nombre premier quelconque inférieur à n. Si p n'est pas un diviseur de m, alors, parmi les substitutions circulaires de l'ordre p, on pourra en trouver une ou plusieurs qui auront la propriété de ne pas altérer la valeur de Ω.*

Corollaire I. — Il suit, en particulier, du théorème précédent que, si le nombre m des valeurs distinctes de Ω est un nombre impair, on pourra, sans altérer cette fonction, opérer au moins une substitution circulaire du second ordre. Donc alors cette fonction sera symétrique au moins par rapport au système des deux variables. Telle est, par exemple, quand on pose $n = 4$, la fonction

$$\Omega = xy + zu,$$

qui offre trois valeurs distinctes.

Corollaire II. — Il suit encore du théorème précédent que, si une fonction Ω de n variables indépendantes admet, sans être symétrique, un nombre impair de valeurs distinctes, elle sera toujours intransitive par rapport à n ou à $n - 1$ variables.

Théorème IV. — *Soient Ω une fonction de n variables $x, y, z, \ldots$ et M le nombre des valeurs égales de cette fonction. Si M est divisible par un certain nombre premier p, on pourra trouver une ou plusieurs substitutions régulières de l'ordre p qui posséderont la propriété de ne pas altérer la valeur de Ω. Dans d'autres articles, j'indiquerai encore d'autres conséquences importantes des principes ci-dessus établis.*

305.

Analyse mathématique. — *Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières, et des systèmes de substitutions conjuguées* (suite).

C. R., T. XXI, p. 895 (20 octobre 1845).

§ I. — *Sur les systèmes de substitutions permutables entre eux.*

Considérons n variables

$$x,\ y,\ z,\ \ldots,$$

et formons avec ces variables deux systèmes de substitutions conjuguées, l'un de l'ordre a, l'autre de l'ordre b. Représentons d'ailleurs par

$$(1)\qquad 1,\ P_1,\ P_2,\ \ldots,\ P_{a-1}$$

les substitutions dont se compose le premier système, et par

$$(2)\qquad 1,\ Q_1,\ Q_2,\ \ldots,\ Q_{b-1}$$

celles dont se compose le second système. Nous dirons que les deux systèmes sont *permutables* entre eux, si tout produit de la forme

$$P_h Q_k$$

est en même temps de la forme

$$Q_k P_h.$$

Il pourra d'ailleurs arriver, ou que les indices h et k restent invariables dans le passage de la première forme à la seconde, en sorte qu'on ait

$$P_h Q_k = Q_k P_h;$$

ou que les indices h et k varient dans ce passage, en sorte qu'on ait

$$P_h Q_k = Q_{k'} P_{h'},$$

h', k' étant de nouveaux indices, liés d'une certaine manière aux nombres h et k. Dans le premier cas, l'une quelconque des substitutions (1) sera permutable avec l'une quelconque des substitutions (2). Dans le second cas, au contraire, deux substitutions de la forme P_h, Q_k cesseront d'être généralement permutables entre elles, quoique le système des substitutions de la forme P_h soit permutable avec le système des substitutions de la forme Q_k.

Supposons maintenant que, les systèmes (1) et (2) étant permutables entre eux, on nomme S une dérivée quelconque des substitutions comprises dans les deux systèmes. Cette dérivée S sera le produit de facteurs dont chacun sera de la forme P_h ou Q_k, et l'on pourra, sans altérer ce produit : 1° échanger entre eux deux facteurs dont l'un serait de la forme P_h, l'autre de la forme Q_k, pourvu que l'on modifie convenablement les valeurs des indices h et k; 2° réduire deux facteurs consécutifs de la forme P_h à un seul facteur de cette forme; 3° réduire deux facteurs consécutifs de la forme Q_k à un seul facteur de cette forme. Or il est clair que, à l'aide de tels échanges et de telles réductions, on pourra toujours réduire définitivement la substitution S à l'une quelconque des deux formes

$$P_h Q_k, \quad Q_k P_h.$$

On peut donc énoncer la proposition suivante :

Théorème I. — *Soient*

$$(1) \qquad 1,\ P_1,\ P_2,\ \ldots,\ P_{a-1}$$

et

$$(2) \qquad 1,\ Q_1,\ Q_2,\ \ldots,\ Q_{b-1}$$

deux systèmes de substitutions conjuguées, permutables entre eux, le premier de l'ordre a, le second de l'ordre b. Toute substitution S, *dérivée des substitutions* (1) *et* (2), *pourra être réduite à chacune des formes*

$$P_h Q_k, \quad Q_k P_h.$$

Corollaire. — Concevons maintenant que l'on construise les deux Tableaux

$$(3) \qquad \left\{\begin{array}{lllll} 1, & P_1, & P_2, & \ldots, & P_{a-1}, \\ Q_1, & Q_1 P_1, & Q_1 P_2, & \ldots, & Q_1 P_{a-1}, \\ Q_2, & Q_2 P_1, & Q_2 P_2, & \ldots, & Q_2 P_{a-1}, \\ \ldots, & \ldots\ldots, & \ldots\ldots, & \ldots, & \ldots\ldots, \\ Q_{b-1}, & Q_{b-1} P_1, & Q_{b-1} P_2, & \ldots, & Q_{b-1} P_{a-1} \end{array}\right.$$

et

$$(4) \qquad \left\{\begin{array}{lllll} 1, & P_1, & P_2, & \ldots, & P_{a-1}, \\ Q_1, & P_1 Q_1, & P_2 Q_1, & \ldots, & P_{a-1} Q_1, \\ Q_2, & P_1 Q_2, & P_2 Q_2, & \ldots, & P_{a-1} Q_2, \\ \ldots, & \ldots\ldots, & \ldots\ldots, & \ldots, & \ldots\ldots, \\ Q_{b-1}, & P_1 Q_{b-1}, & P_2 Q_{b-1}, & \ldots, & P_{a-1} Q_{b-1}. \end{array}\right.$$

Deux termes pris au hasard, non seulement dans une même ligne horizontale, mais encore dans deux lignes horizontales différentes du Tableau (3), seront nécessairement distincts l'un de l'autre, si les séries (1) et (2) n'offrent pas de termes communs autres que l'unité. Car, si en nommant h, h' deux entiers inférieurs à a, et k, k' deux entiers inférieurs à b, on avait, par exemple,

$$(5) \qquad P_h Q_k = P_{h'} Q_{k'},$$

sans avoir à la fois

$$h' = h \quad \text{et} \quad k' = k,$$

l'équation (5) entraînerait la formule

$$Q_k Q_{k'}^{-1} = P_h^{-1} P_{h'},$$

en vertu de laquelle les deux séries offriraient un terme commun qui serait distinct de l'unité. Donc, dans l'hypothèse admise, les divers termes du Tableau (3), qui offrira toutes les valeurs possibles du produit

$$Q_k P_h,$$

seront distincts les uns des autres, et par suite les dérivées distinctes des substitutions (1) et (2) se réduiront aux termes de ce

Tableau. Donc le système de substitutions conjuguées, formé par ces dérivées, sera d'un ordre représenté par le nombre des termes du Tableau (3), c'est-à-dire par le produit ab. On pourra d'ailleurs évidemment remplacer le Tableau (3) par le Tableau (4), et, par conséquent, on peut énoncer la proposition suivante :

Théorème II. — *Les mêmes choses étant posées que dans le théorème I, les dérivées des substitutions* (1) *et* (2) *formeront un nouveau système de substitutions qui seront toutes comprises dans le Tableau* (3), *ainsi que dans le Tableau* (4); *et l'ordre de ce système sera le produit* ab *des ordres* a, b *des systèmes* (1) *et* (2).

On peut encore démontrer facilement la proposition suivante qui peut être considérée comme réciproque du second théorème :

Théorème III. — *Soient*

$$1,\ P_1,\ P_2,\ \ldots,\ P_{a-1}, \tag{1}$$

$$1,\ Q_1,\ Q_2,\ \ldots,\ Q_{b-1} \tag{2}$$

deux systèmes de substitutions conjuguées, le premier de l'ordre a, *le second de l'ordre* b, *qui n'offrent pas de termes communs autres que l'unité. Si les dérivées de ces deux systèmes forment un nouveau système de substitutions conjuguées, dont l'ordre se réduise au produit* ab, *toutes ces dérivées seront comprises dans chacun des Tableaux* (3) *et* (4), *et par conséquent les systèmes* (1) *et* (2) *seront permutables entre eux.*

Démonstration. — En effet, dans l'hypothèse admise, chacun des Tableaux (3), (4) se composera de termes qui seront tous distincts les uns des autres, et qui seront en nombre égal à celui des substitutions dérivées des substitutions (1) et (2). Donc il renfermera toutes ces substitutions, dont chacune sera tout à la fois de la forme $Q_k P_h$ et de la forme $P_h Q_k$.

Corollaire. — Les conditions énoncées dans le théorème III seront certainement remplies si aucune des substitutions comprises dans les systèmes (1) et (2) n'altère la valeur d'une certaine fonction Ω des

variables $x, y, z, \ldots$, et si d'ailleurs le nombre des valeurs égales de cette fonction est précisément le produit ab. On peut donc énoncer encore la proposition suivante :

Théorème IV. — *Soient*

$$1,\ P_1,\ P_2,\ \ldots,\ P_{a-1}, \tag{1}$$

$$1,\ Q_1,\ Q_2,\ \ldots,\ Q_{b-1} \tag{2}$$

deux systèmes de substitutions conjuguées, le premier de l'ordre a, *le second de l'ordre* b, *qui n'offrent pas de termes communs autres que l'unité. Soit d'ailleurs* Ω *une fonction dont la valeur ne soit altérée par aucune des substitutions* (1) *ou* (2). *Si le nombre des valeurs égales de la fonction* Ω *est précisément le produit* ab, *les systèmes* (1) *et* (2) *seront permutables entre eux, et par conséquent l'une quelconque des dérivées des substitutions comprises dans ces deux systèmes sera tout à la fois de la forme* $P_h Q_k$ *et de la forme* $P_k Q_h$.

Exemple. — Posons $n = 4$; la fonction

$$\Omega = (x-y)(x-z)(y-z)(y-u)(z-u)$$

offrira deux valeurs distinctes seulement, par conséquent 12 valeurs égales; et, parmi les substitutions qui n'altéreront pas la valeur de cette fonction, se trouveront, d'une part, les substitutions du second ordre

$$P_1 = (x, y)(z, u), \quad P_2 = (x, z)(y, u), \quad P_3 = (x, u)(y, z),$$

qui forment avec l'unité un système de substitutions régulières conjuguées du quatrième ordre; d'autre part, les substitutions du troisième ordre

$$Q = (y, z, u), \quad Q^2 = (y, u, z),$$

qui forment, avec l'unité, un système de substitutions conjuguées du troisième ordre. Cela posé, le produit 3×4 des ordres des deux systèmes étant précisément le nombre 12 des valeurs égales de la fonction Ω, on conclura du théorème IV que les deux systèmes de substitutions

$$1, \quad P_1, \quad P_2, \quad P_3,$$
$$1, \quad Q, \quad Q^2$$

sont permutables entre eux, et que les dérivées de ces substitutions, c'est-à-dire les diverses substitutions en vertu desquelles Ω ne changera pas de valeur, sont toutes comprises dans chacun des Tableaux

$$(6) \qquad \left\{\begin{array}{llll} 1, & P_1, & P_2, & P_3, \\ Q, & Q\,P_1, & Q\,P_2, & Q\,P_3, \\ Q^2, & Q^2P_1, & Q^2P_2, & Q^2P_3; \end{array}\right.$$

$$(7) \qquad \left\{\begin{array}{llll} 1, & P_1, & P_2, & P_3, \\ Q, & P_1Q, & P_2Q, & P_3Q, \\ Q^2, & P_1Q^2, & P_2Q^2, & P_3Q^2. \end{array}\right.$$

D'ailleurs les termes équivalents du premier et du second Tableau seront ce qu'indique la formule

$$(8) \qquad Q^k P_h = P_{h+k} Q^k,$$

pourvu que l'on considère les deux notations

$$P_h, \quad P_{h'}$$

comme exprimant une seule et même substitution, dans le cas où la différence des indices h, h' est divisible par 3.

§ II. — *Sur le partage des variables que renferme une fonction donnée en plusieurs groupes arbitrairement choisis.*

Soit Ω une fonction de n variables indépendantes $x, y, z, \ldots$, et supposons ces variables partagées en plusieurs groupes arbitrairement choisis, dont chacun, après une substitution quelconque, soit censé comprendre toujours les seules variables qui, dans la fonction, occupent certaines places. Parmi les substitutions qui n'altéreront pas la valeur de Ω, deux quelconques produiront des valeurs égales de Ω qui

offriront, ou les mêmes groupes tous composés de la même manière, ou deux modes distincts de composition des divers groupes. Cela posé, soient

$$(1) \qquad 1, \quad P, \quad Q, \quad R, \quad \ldots$$

les substitutions qui n'altèrent, ni la valeur de Ω, ni le mode de composition des divers groupes. Ces substitutions formeront évidemment un système de substitutions conjuguées, et l'ordre I de ce système représentera le nombre des valeurs égales de Ω qui correspondront à un mode quelconque de composition des divers groupes. Cela posé, si l'on nomme $\mathfrak{M}$ le nombre des divers modes de composition que les divers groupes peuvent offrir, $\mathfrak{M}I$ sera évidemment le nombre total M des valeurs égales de la fonction Ω. On peut donc énoncer la proposition suivante :

Théorème. — *Soit Ω une fonction de n variables indépendantes*

$$x, \quad y, \quad z, \quad \ldots,$$

et partageons ces variables en groupes arbitrairement choisis, dont chacun, après une substitution quelconque, soit censé comprendre les seules variables qui, dans la fonction Ω, occupent certaines places. Soit d'ailleurs I l'ordre du système des substitutions conjuguées

$$1, \quad P, \quad Q, \quad R, \quad \ldots,$$

qui, sans altérer Ω, se borneront à déplacer des variables dans les divers groupes ; et nommons $\mathfrak{M}$ le nombre des divers modes de composition que les divers groupes pourront offrir, sans que la valeur de Ω soit altérée. Le nombre total $\mathfrak{M}$ des valeurs égales de Ω sera déterminé par l'équation

$$(2) \qquad M = \mathfrak{M}I.$$

Corollaire. — Supposons que les divers groupes soient respectivement formés, le premier, de a variables ; le deuxième, de b variables ; le troisième, de c variables ; etc. Supposons encore que, pour un certain mode de composition des divers groupes, le premier groupe se compose des variables

$$\alpha,\quad \beta,\quad \gamma,\quad \ldots,$$

le deuxième des variables

$$\lambda,\quad \mu,\quad \nu,\quad \ldots,$$

le troisième des variables

$$\varphi,\quad \chi,\quad \psi,\quad \ldots.$$

Enfin, supposons que, dans ce cas, la fonction Ω puisse acquérir : 1° A valeurs égales en vertu de substitutions correspondantes à des permutations diverses des variables $\alpha, \beta, \gamma, \ldots$; 2° B valeurs égales en vertu de substitutions qui, sans déplacer $\alpha, \beta, \gamma, \ldots$, correspondent à des permutations diverses de $\lambda, \mu, \nu, \ldots$; 3° C valeurs égales en vertu de substitutions qui, sans déplacer ni $\alpha, \beta, \gamma, \ldots$, ni $\lambda, \mu, \nu, \ldots$, correspondent à des permutations diverses de $\varphi, \chi, \psi, \ldots$, les permutations diverses des variables comprises dans un groupe pouvant d'ailleurs entraîner des permutations correspondantes des variables comprises dans les groupes suivants. Alors on aura évidemment

$$I = ABC\ldots, \tag{3}$$

et par suite la formule (3) donnera

$$M = \mathfrak{M}ABC\ldots. \tag{4}$$

306.

Analyse mathématique. — *Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières, et des systèmes de substitutions conjuguées* (suite).

C. R., T. XXI, p. 931 (27 octobre 1845).

Soit Ω une fonction de n variables indépendantes

$$x,\quad y,\quad z,\quad \ldots.$$

Nommons

$$\Omega,\quad \Omega',\quad \Omega'',\quad \ldots \tag{1}$$

les valeurs distinctes de cette fonction qui résultent de permutations opérées entre les variables, et soit m le nombre de ces valeurs distinctes. Soient encore

P une substitution de l'ordre i, prise parmi celles qui n'altèrent pas la valeur de Ω;

P, P′, P″, … les diverses substitutions semblables à P;

ϖ le nombre des substitutions P, P′, P″, …;

h le nombre de celles des substitutions P, P′, P″, … qui n'altèrent pas la valeur de Ω;

k le nombre de celles des fonctions $\Omega, \Omega', \Omega'', \ldots$ qui ne sont pas altérées par la substitution P.

Si l'on applique successivement à chacune des fonctions

$$\Omega,\quad \Omega',\quad \Omega'',\quad \ldots$$

chacune des substitutions

$$\mathrm{P},\quad \mathrm{P}',\quad \mathrm{P}'',\quad \ldots,$$

le nombre total des opérations effectuées sera

$$m\varpi,$$

et, parmi ces opérations, celles qui s'effectueront sans altérer les valeurs des fonctions auxquelles on les applique seront évidemment en nombre égal à chacun des deux produits

$$hm,\quad k\varpi.$$

On aura donc nécessairement

$$hm = k\varpi. \tag{2}$$

Soient maintenant

$$\Phi,\quad \mathrm{X},\quad \Psi,\quad \ldots \tag{3}$$

ceux des termes de la suite (1) qui sont altérés par la substitution P. Le nombre de ces termes sera évidemment représenté par $m-k$.

Si l'ordre i de la substitution P se réduit à un nombre premier p, la suite (3) se décomposera en plusieurs suites nouvelles, composées chacune de p termes que l'on déduira l'un de l'autre, en appliquant à l'un d'eux les substitutions représentées par les diverses puissances de P. Donc alors $m-k$ sera un multiple de p, et l'on aura

(4) $$m-k\equiv 0 \pmod{p}.$$

En vertu de la formule (4), m ne pourra s'abaisser au-dessous du nombre premier p que dans le cas où l'on aura

$$m=k,$$

et, par suite, en vertu de la formule (2), $h=\varpi$, c'est-à-dire dans le cas où la fonction Ω ne serait altérée par aucune substitution semblable à P. Dans ce même cas, si P est une substitution circulaire, la fonction Ω sera symétrique ou offrira deux valeurs, en sorte qu'on aura

$$m=k=1 \quad \text{ou} \quad 2,$$

à moins toutefois que l'on n'ait

$$m=4 \quad \text{et} \quad m=3.$$

Ajoutons que le nombre p, étant l'ordre d'une substitution P qui n'altère pas Ω, pourra représenter, dans la formule (4), l'un quelconque des diviseurs premiers du produit

$$1.2.3\ldots n,$$

par conséquent, l'un quelconque des nombres premiers inférieurs à n.

Si de l'hypothèse admise on voulait passer au cas où la substitution P n'altérerait aucune des fonctions

$$\Omega,\ \Omega',\ \Omega'',\ \ldots,$$

il suffirait de poser dans la formule (4)

$$k=0;$$

mais alors cette formule donnerait simplement

$$m\equiv 0 \pmod{p};$$

en sorte que p serait un diviseur de m. On se trouverait ainsi ramené à une proposition évidemment comprise dans le théorème I de la page 359.

Si Ω était une fonction transitive, alors de la formule (2), jointe à l'équation (5) de la page 289, on pourrait déduire des conséquences remarquables que nous exposerons dans un prochain article.

307.

Analyse mathématique. — *Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières, et des systèmes de substitutions conjuguées* (suite).

C. R., T. XXI, p. 972 (3 novembre 1845).

§ I. — *Théorèmes relatifs à un système quelconque de substitutions conjuguées, que l'on suppose appliquées à une fonction de plusieurs variables indépendantes.*

Soient

Ω une fonction de n variables indépendantes $x, y, z, \ldots$;
M le nombre des valeurs égales de la fonction Ω;
m le nombre de ses valeurs distinctes.

Alors, en posant, pour abréger,

$$N=1.2.3\ldots n,$$

on aura

(1) $$mM=N;$$

et, par conséquent, chacun des nombres entiers m, M sera un diviseur de N. Soient d'ailleurs

(2) $$1,\quad P,\quad Q,\quad R,\quad \ldots$$

les diverses substitutions qui n'altèrent pas la valeur de Ω. Ces substitutions, dont le nombre sera précisément M, composeront, comme l'on sait, un système de substitutions conjuguées.

Soit maintenant

(3) $$1,\quad \mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots.$$

un autre système de substitutions conjuguées, et nommons $\mathfrak{M}$ l'ordre de ce dernier système.

Soient encore

(4) $$\Omega,\quad \Omega',\quad \Omega'',\quad \ldots$$

les valeurs distinctes de la fonction Ω, et

(5) $$\Phi,\quad X,\quad \Psi,\quad \ldots$$

celles de ces valeurs qui sont altérées par chacune des substitutions

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots.$$

Chacun des termes qui, étant compris dans la série (4), se trouve exclus de la série (5), représentera une fonction qui ne sera point altérée quand on effectuera les substitutions

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots,$$

ou du moins quelques-unes d'entre elles; et, si l'on nomme $\mathcal{X}$ le nombre de ces mêmes termes, $m - \mathcal{X}$ sera le nombre des termes de la série (5).

Concevons à présent que l'on applique à l'un des termes de la série (5), par exemple à la fonction Φ, les substitutions

$$1,\quad \mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots,$$

et soient

(6) $$\Phi,\quad \Phi',\quad \Phi'',\quad \Phi''',\quad \ldots$$

les diverses valeurs de Ω ainsi obtenues. Chacune d'elles ne pourra être qu'un terme de la série (5), c'est-à-dire une des fonctions qui sont altérées par l'application de l'une quelconque des substitutions

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots.$$

En effet, supposons un instant, s'il est possible, qu'on n'altérât pas la fonction Φ' en lui appliquant la substitution $\mathfrak{Q}$. Alors on pourrait passer de Φ à Φ', en appliquant à Φ l'une quelconque des deux substitutions

$$\mathfrak{P},\quad \mathfrak{Q}\mathfrak{P};$$

et, réciproquement, on pourrait passer de Φ' à Φ, en appliquant à Φ' l'une des substitutions inverses

$$\mathfrak{P}^{-1},\quad \mathfrak{P}^{-1}\mathfrak{Q}^{-1}.$$

Donc alors Φ ne serait point altéré par l'application de la substitution

$$\mathfrak{P}^{-1}\mathfrak{Q}\mathfrak{P}\quad \text{ou}\quad \mathfrak{P}^{-1}\mathfrak{Q}^{-1}\mathfrak{P},$$

qui serait semblable à $\mathfrak{Q}$, ou à $\mathfrak{Q}^{-1}$, et se confondrait avec une dérivée des substitutions

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots,$$

par conséquent avec l'une de ces mêmes substitutions. Or cette conclusion ne saurait être admise, puisque Φ, étant un terme de la suite (5), devra être altéré par chacune des substitutions

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots.$$

Il est même facile de voir que deux termes quelconques de la suite (6) devront être distincts l'un de l'autre. Car, supposons un instant que l'on pût avoir

$$\Phi'' = \Phi';$$

alors on pourrait passer de Φ à Φ', en appliquant à Φ l'une quelconque des substitutions

$$\mathfrak{P},\quad \mathfrak{Q},$$

et revenir de Φ' à Φ, en appliquant à Φ' l'une quelconque des substitutions inverses

$$\mathfrak{P}^{-1},\quad \mathfrak{Q}^{-1}.$$

Donc alors Φ ne serait point altéré quand on lui appliquerait l'une quelconque des substitutions

$$\mathfrak{P}^{-1}\mathfrak{Q} \quad \text{ou} \quad \mathfrak{Q}^{-1}\mathfrak{P},$$

dont chacune représente encore un terme de la suite

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots.$$

Cette conséquence étant inadmissible, nous devons conclure que les $\mathcal{M}$ termes de la série (6) seront des termes distincts, dont chacun faisait déjà partie de la série (5).

Soient maintenant

$$\mathfrak{U},\quad \mathfrak{V},\quad \mathfrak{W},\quad \ldots$$

quelques-unes des substitutions qui, étant appliquées à la fonction Ω, produisent les termes de la série (5), et formons le Tableau

$$(7)\qquad \begin{cases} \mathfrak{U}, & \mathfrak{P}\mathfrak{U}, & \mathfrak{Q}\mathfrak{U}, & \mathfrak{R}\mathfrak{U}, & \ldots, \\ \mathfrak{V}, & \mathfrak{P}\mathfrak{V}, & \mathfrak{Q}\mathfrak{V}, & \mathfrak{R}\mathfrak{V}, & \ldots, \\ \mathfrak{W}, & \mathfrak{P}\mathfrak{W}, & \mathfrak{Q}\mathfrak{W}, & \mathfrak{R}\mathfrak{W}, & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots. \end{cases}$$

Si l'on applique à la fonction Ω chacune des substitutions comprises dans ce Tableau, chacune des diverses fonctions que l'on obtiendra sera, d'après ce qu'on vient de dire, un terme de la série (5), et même les $\mathcal{M}$ fonctions, produites par les substitutions que renferme une ligne horizontale du Tableau (7), seront distinctes les unes des autres. De plus, si deux substitutions comprises dans deux lignes horizontales distinctes, par exemple

$$\mathfrak{P}\mathfrak{U} \quad \text{et} \quad \mathfrak{Q}\mathfrak{V},$$

produisent la même fonction X, on pourra revenir de X à Ω en appliquant à X l'une quelconque des substitutions inverses

$$\mathfrak{U}^{-1}\mathfrak{P}^{-1},\quad \mathfrak{V}^{-1}\mathfrak{Q}^{-1},$$

et par suite on n'altérera pas la fonction Ω en lui appliquant la substitution

$$\mathfrak{V}^{-1}\mathfrak{Q}^{-1}\mathfrak{P}\mathfrak{U},$$

ou, ce qui revient au même, en lui appliquant d'abord la substitution

$$\mathfrak{Q}^{-1}\mathfrak{P}\mathfrak{U}$$

déjà comprise dans la première ligne horizontale du Tableau (7), puis la substitution $\mathfrak{V}^{-1}$. Donc, si l'on nomme Ψ la fonction que l'on obtient quand on applique à Ω la substitution $\mathfrak{Q}^{-1}\mathfrak{P}\mathfrak{U}$, la substitution $\mathfrak{V}^{-1}$ transformera Ψ en Ω, et la substitution inverse $\mathfrak{V}$ transformera Ω en Ψ. Donc

$$\mathfrak{P}\mathfrak{U} \quad \text{et} \quad \mathfrak{Q}\mathfrak{V},$$

c'est-à-dire deux substitutions, comprises dans la deuxième et la troisième ligne horizontale du Tableau (7), ne pourront produire la même fonction X que dans le cas où la substitution représentée par le premier terme $\mathfrak{V}$ de la troisième ligne horizontale reproduirait l'une des fonctions déjà produites par un terme de la deuxième suite horizontale. Donc, pour que les diverses fonctions produites par les substitutions (7) soient toutes distinctes les unes des autres, il suffit que, après avoir formé une ou plusieurs lignes horizontales du Tableau (7), on prenne toujours pour premier terme de la ligne suivante une substitution qui, appliquée à Ω, reproduise un terme de la série (5), sans jamais reproduire un des termes fournis par les substitutions que renferment les lignes déjà écrites. Or, ces conditions étant supposées remplies, concevons que l'on allonge de plus en plus le Tableau (7), en ajoutant sans cesse à ce Tableau de nouvelles suites horizontales. On ne pourra être arrêté dans cette opération qu'à l'instant où l'on aura épuisé tous les termes de la série (5). Alors les substitutions (7), appliquées à Ω, reproduiront tous les termes de la suite (5). Donc les termes qui composent cette suite, et qui sont en nombre égal à $m - \mathcal{X}$, pourront être répartis entre diverses suites correspondantes aux lignes horizontales du Tableau (7) et composées chacune de $\mathcal{M}$ termes. Donc la différence

$M - \mathcal{N}$ sera un multiple de $\mathcal{M}$, et l'on peut énoncer la proposition suivante :

Théorème I. — *Soit Ω une fonction de plusieurs variables indépendantes $x, y, z, \ldots$. Soient encore*

$$\Omega, \quad \Omega', \quad \Omega'', \quad \ldots$$

les valeurs distinctes de Ω, et m le nombre de ces valeurs distinctes. Soit enfin

$$1, \quad \mathfrak{P}, \quad \mathfrak{Q}, \quad \mathfrak{R}, \quad \ldots$$

un système quelconque de substitutions conjuguées et relatives aux variables $x, y, z, \ldots$. Nommons $\mathcal{M}$ l'ordre de ce système et $\mathcal{N}$ le nombre de celles d'entre les fonctions $\Omega, \Omega', \Omega'', \ldots$ qui ne sont pas altérées quand on effectue les substitutions

$$\mathfrak{P}, \quad \mathfrak{Q}, \quad \mathfrak{R}, \quad \ldots,$$

ou du moins quelques-unes d'entre elles. La différence $m - \mathcal{N}$ sera un multiple de $\mathcal{M}$, en sorte qu'on aura

$$m - \mathcal{N} \equiv 0 \pmod{\mathcal{M}}. \tag{8}$$

Corollaire. — Soit U l'une des substitutions qui servent à déduire de la fonction Ω l'un des termes de la suite (5), par exemple le terme Φ. Soit encore

$$1, \quad P', \quad Q', \quad R', \quad \ldots$$

le système des substitutions conjuguées qui possèdent la propriété de ne pas altérer la fonction Φ. Les substitutions

$$P', \quad Q', \quad R', \quad \ldots$$

seront respectivement semblables à

$$P, \quad Q, \quad R, \quad \ldots,$$

de sorte qu'on aura, par exemple,

$$P' = UPU^{-1}, \qquad P'U = UP;$$

et, par suite, les substitutions diverses qui transformeront Ω en Φ, savoir

$$U, \quad P'U, \quad Q'U, \quad R'U, \quad \ldots,$$

se confondront avec celles que présente la série

$$U, \quad UP, \quad UQ, \quad UR, \quad \ldots.$$

Cela posé, les substitutions à l'aide desquelles on passera de la fonction Ω aux divers termes de la série

$$\Omega, \quad X, \quad \Psi, \quad \ldots$$

seront évidemment comprises dans un Tableau de la forme

$$\left\{\begin{array}{lllll} U, & UP, & UQ, & UR, & \ldots, \\ V, & VP, & VQ, & VR, & \ldots, \\ W, & WP, & WQ, & WR, & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots, \end{array}\right. \tag{9}$$

et toutes distinctes les unes des autres. D'ailleurs, chacun des termes de la série (5) devant être altéré quand on lui applique l'une des substitutions

$$\mathfrak{P}, \quad \mathfrak{Q}, \quad \mathfrak{R}, \quad \ldots,$$

deux termes pris au hasard dans une même ligne horizontale du Tableau (9), par exemple

$$UP, \quad UQ,$$

ne pourront satisfaire à une équation de la forme

$$\mathfrak{R}UP = UQ; \tag{10}$$

et réciproquement, si une équation de cette forme ne peut jamais avoir lieu, un terme quelconque de la série (5) sera toujours altéré quand on lui appliquera l'une des substitutions

$$\mathfrak{P}, \quad \mathfrak{Q}, \quad \mathfrak{R}, \quad \ldots.$$

Enfin, l'équation (10), de laquelle on tirera

$$\mathfrak{R}U = UQP^{-1},$$

se présentera sous la forme

$$\mathcal{R}U = US, \tag{11}$$

si, pour abréger, l'on désigne par S la substitution

$$QP^{-1}$$

qui sera toujours un des termes de la série

$$P, \quad Q, \quad \ldots;$$

et dire que l'équation (11) ne peut subsister, c'est dire qu'aucune substitution de la forme $\mathcal{P}U$ n'est en même temps de la forme UP, lorsque $\mathcal{P}$ et P ne se réduisent pas l'un et l'autre à l'unité. Donc le théorème I entraîne immédiatement la proposition suivante :

Théorème II. — *Formons avec n variables $x, y, z, \ldots$ deux systèmes de substitutions conjuguées, savoir*

$$1, \quad P, \quad Q, \quad R, \quad \ldots$$

et

$$1, \quad \mathcal{P}, \quad \mathcal{Q}, \quad \mathcal{R}, \quad \ldots.$$

Soient M l'ordre du premier système, $\mathcal{M}$ l'ordre du second système. Enfin nommons

$$U, \quad V, \quad W, \quad \ldots \tag{12}$$

des substitutions tellement choisies, que le produit

$$UP$$

de l'une des substitutions

$$P, \quad Q, \quad R, \quad \ldots$$

par un terme U *de la série* (12) *ne puisse jamais être équivalent, ni à un autre produit*

$$VQ$$

de la même forme, dans lequel V *serait différent de* U, *ni au produit*

$$\mathcal{P}U$$

du terme U *par l'une des substitutions*

$$\mathcal{P}, \quad \mathcal{Q}, \quad \mathcal{R}, \quad \ldots.$$

Si l'on pose, pour abréger,

$$m = \frac{N}{M} = \frac{1.2.3\ldots n}{M}, \tag{13}$$

et si l'on représente par $m - \mathcal{X}$ le nombre total des substitutions que l'on pourra faire entrer dans la série (12), *la différence*

$$m - \mathcal{X}$$

sera divisible par $\mathcal{M}$.

Nota. — On pourrait démontrer directement le théorème II en faisant voir que, dans l'hypothèse admise, toute substitution U, pour laquelle ne se vérifiera jamais une équation de la forme (11), sera nécessairement comprise dans le Tableau (9), et que l'on pourra extraire des diverses colonnes horizontales de ce Tableau, qui seront en nombre égal à $m - \mathcal{X}$, un pareil nombre de substitutions nouvelles

$$\mathcal{U}, \quad \mathcal{V}, \quad \mathcal{W}, \quad \ldots$$

tellement choisies, que le Tableau (7) sera uniquement composé de termes pris dans le Tableau (9), un seul terme étant pris dans chaque ligne horizontale du même Tableau.

Corollaire. — Il importe d'observer que

$$M(m - \mathcal{X}) = N - M\mathcal{X}$$

sera le nombre total des substitutions comprises dans le Tableau (9), c'est-à-dire des substitutions U pour lesquelles ne se vérifie jamais la formule (11). Donc $M\mathcal{X}$ représentera le nombre des substitutions U pour lesquelles se vérifie la même formule, et le théorème II peut être remplacé par la proposition suivante :

Théorème III. — *Formons avec n variables $x, y, z, \ldots$ deux systèmes* *de substitutions conjuguées, savoir*

$$1,\ P,\ Q,\ R,\ \ldots$$

et

$$1,\ \mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots;$$

soient d'ailleurs M, $\mathfrak{M}$ *les ordres de ces deux systèmes, et* $M\mathfrak{X}$ *le nombre des substitutions* U *qui vérifient une ou plusieurs équations de la forme*

$$\mathfrak{P}U = UP. \tag{14}$$

Si l'on pose, pour abréger,

$$N = 1.2.3\ldots n \quad \text{et} \quad m = \frac{N}{M},$$

la différence

$$m - \mathfrak{X}$$

sera divisible par $\mathfrak{M}$.

Les théorèmes I, II et III entraînent avec eux un grand nombre de conséquences qui sont encore dignes de remarque. Nous allons en indiquer quelques-unes.

La formule (14), de laquelle on tire

$$\mathfrak{P} = UPU^{-1}, \tag{15}$$

exprime que la substitution $\mathfrak{P}$ est semblable à la substitution P. Si cette condition ne peut jamais être remplie, c'est-à-dire si aucune des substitutions

$$\mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots$$

n'est semblable à l'une des substitutions

$$P,\ Q,\ R,\ \ldots,$$

on aura

$$\mathfrak{X} = 0,$$

et l'on conclura du théorème III que m est divisible par $\mathfrak{M}$. On se trouvera donc ainsi ramené au théorème II de la page 356.

Supposons maintenant que la condition (15) puisse être remplie, mais que l'on ait $\mathfrak{M} > m$; alors, pour que la différence $m - \mathfrak{X}$ soit divisible par $\mathfrak{M}$, il faudra que l'on ait précisément

$$\mathfrak{X} = m.$$

On peut donc déduire du théorème I la proposition suivante :

Théorème IV. — *Les mêmes choses étant posées que dans le théorème I, si l'on a*

$$m < \mathfrak{M}, \tag{16}$$

chacune des fonctions Ω, Ω', Ω'', ... *jouira de cette propriété, qu'elle ne sera point altérée quand on effectuera les substitutions*

$$\mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots,$$

ou du moins quelques-unes d'entre elles.

Il importe d'observer que, si l'on pose, pour abréger,

$$\mathrm{m} = \frac{N}{\mathfrak{M}},$$

la condition (16) donnera

$$m\mathrm{m} < N. \tag{17}$$

Rien n'empêche de faire coïncider les substitutions conjuguées

$$1,\ \mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots$$

avec les substitutions conjuguées

$$1,\ P,\ Q,\ R,\ \ldots,$$

qui possèdent seules la propriété de ne point altérer Ω. Alors on aura

$$\mathfrak{M} = M;$$

et, en nommant K ce que deviendra le nombre $\mathfrak{X}$, on tirera de la formule (8)

$$m - K \equiv 0 \pmod{M}.$$

On peut donc énoncer encore la proposition suivante :

THÉORÈME V. — *Soient*

Ω *une fonction de n variables* $x, y, z, \ldots$;
M le nombre de ses valeurs égales;
m le nombre de ses valeurs distinctes $\Omega, \Omega', \Omega'', \ldots$;
1, P, Q, R, ... *les substitutions conjuguées qui n'altèrent pas la valeur de* Ω;
K le nombre de celles d'entre les fonctions $\Omega, \Omega', \Omega'', \ldots$ *qui ne sont pas altérées quand on leur applique une ou plusieurs des substitutions* P, Q, R, ...

La différence $m - K$ *sera divisible par M, en sorte qu'on aura*

$$m - K \equiv 0 \pmod{M}. \tag{18}$$

Corollaire. — Si le nombre m des valeurs distinctes de la fonction Ω est inférieur à $\sqrt{N}$, on aura $m < M$, et par suite la formule (18) se réduira simplement à l'équation

$$K = m.$$

Donc alors la valeur de chacune des fonctions $\Omega, \Omega', \Omega'', \ldots$ demeurera intacte quand on effectuera les substitutions P, Q, R, ..., ou au moins l'une d'entre elles.

Si, dans le théorème I, on remplace le système des substitutions conjuguées $1, \mathfrak{P}, \mathfrak{Q}, \mathfrak{R}, \ldots$ par les diverses puissances d'une seule substitution P de l'ordre i, on obtiendra la proposition suivante :

THÉORÈME VI. — *Soit* Ω *une fonction de plusieurs variables indépendantes* $x, y, z, \ldots$; *soient encore*

$$\Omega, \quad \Omega', \quad \Omega'', \quad \ldots$$

les valeurs distinctes de cette fonction, et m le nombre de ses valeurs égales. Soient enfin P *une substitution de l'ordre i et k le nombre de celles d'entre les fonctions* $\Omega, \Omega', \Omega'', \ldots$ *qui ne sont pas altérées quand on effectue les substitutions*

$$P, \quad P^2, \quad P^3, \quad \ldots, \quad P^{i-1},$$

ou du moins quelques-unes d'entre elles. La différence $m - k$ *sera un multiple de i, en sorte qu'on aura*

$$m - k \equiv 0 \pmod{i}. \tag{19}$$

Corollaire I. — Si P et ses puissances sont les seules substitutions qui n'altèrent pas Ω, on aura $m = \frac{N}{i}$, et par suite la formule (19) donnera

$$\frac{N}{i} - k \equiv 0 \pmod{i}. \tag{20}$$

Si d'ailleurs l'ordre i de la substitution P se réduit à un nombre premier p, alors k sera simplement le nombre de celles d'entre les fonctions $\Omega, \Omega', \Omega'', \ldots$ qui ne seront pas altérées par la substitution P. Alors aussi, en nommant ϖ le nombre des substitutions P, P', P'', ... semblables à P, et h le nombre de celles des substitutions P, P', P'', ... qui n'altère pas Ω, on aura, d'après ce qu'on a vu dans un précédent article,

$$hm = k\varpi. \tag{21}$$

De plus, si P se réduit à une substitution circulaire de l'ordre p, on trouvera

$$\varpi = \frac{N}{[1.2\ldots(n-p)]p}, \qquad m = \frac{N}{p}, \qquad h = p - 1$$

et, par suite,

$$k = (p-1)[1.2\ldots(n-p)] \equiv -[1.2\ldots(n-p)] \pmod{p}.$$

Enfin, si l'on prend $n = p$, on aura simplement

$$k \equiv -1 \pmod{p},$$

et comme alors on trouvera

$$\frac{N}{i} = \frac{N}{p} = 1.2\ldots(p-1),$$

la formule (20), réduite à

$$1.2\ldots(p-1) + 1 \equiv 0 \pmod{p},$$

reproduira le théorème de Wilson.

§ II. — *Sur le dénombrement des substitutions diverses qui n'altèrent pas une fonction de plusieurs variables indépendantes.*

Soit Ω une fonction de n variables indépendantes

$$x,\quad y,\quad z,\quad \ldots.$$

Nommons

$$\Omega,\quad \Omega',\quad \Omega'',\quad \ldots \tag{1}$$

les valeurs distinctes de cette fonction qui résultent de permutations opérées entre les variables, et m le nombre de ces valeurs distinctes. Soient encore

P une substitution de l'ordre i, prise parmi celles qui n'altèrent pas la valeur de Ω;

P, P′, P″, ... les diverses substitutions semblables à P;

ϖ le nombre des substitutions P, P′, P″, ...;

h le nombre de celles des substitutions P, P′, P″, ... qui n'altèrent pas la valeur de Ω;

k le nombre de celles des fonctions Ω, Ω', Ω'', ... qui ne sont pas altérées par la substitution P.

On aura, comme nous l'avons déjà montré dans un précédent article,

$$hm = k\varpi; \tag{2}$$

et chacun des rapports égaux

$$\frac{h}{\varpi},\quad \frac{k}{m}$$

devra être évidemment, ou inférieur, ou tout au plus équivalent à l'unité. Si d'ailleurs on nomme M le nombre des valeurs égales de la fonction Ω, et N le produit $1.2.3\ldots n$, on aura, non seulement

$$mM = N, \tag{3}$$

mais encore

$$\Sigma h = M, \tag{4}$$

la somme qu'indique le signe Σ s'étendant à toutes les formes que peut revêtir la substitution P.

Concevons maintenant que Ω, étant une fonction transitive de n, de $n-1$, de $n-2$, et même de $n-l+1$ variables, soit une fonction intransitive de $n-l$ variables. La série (1) et, par suite, les valeurs de m et de k resteront les mêmes pour Ω considéré comme fonction de n variables, et pour Ω considéré comme fonction de $n-l$ variables. Soient d'ailleurs

$$\mathfrak{b},\quad \varphi\quad \text{et}\quad \mathfrak{M}$$

ce que deviendraient, pour Ω considéré comme fonction de $n-l$ variables, les quantités

$$h,\quad \varpi\quad \text{et}\quad M.$$

Alors, à la place des formules (2), (3), (4), on obtiendra les suivantes

$$\mathfrak{b}m = k\varphi, \tag{5}$$

$$m\mathfrak{M} = \mathfrak{N}, \tag{6}$$

la valeur de $\mathfrak{N}$ étant $1.2.3\ldots(n-l)$, et

$$\Sigma\mathfrak{b} = \mathfrak{M}. \tag{7}$$

Cela posé, on tirera des formules (2) et (5)

$$h = \theta\mathfrak{b},\qquad \mathfrak{b} = \frac{h}{\theta}, \tag{8}$$

la valeur de θ étant

$$\theta = \frac{\varpi}{\varphi}. \tag{9}$$

Enfin, si l'on nomme r le nombre des lettres qui demeurent immobiles quand on effectue sur Ω, considéré comme fonction de n variables, la substitution P, on aura, en vertu de la formule (5) de la page 289,

$$\frac{1}{\theta} = \frac{r(r-1)\ldots(r-l+1)}{n(n-1)\ldots(n-l+1)}. \tag{10}$$

On aura d'ailleurs, en vertu des formules (3) et (6),

$$\mathfrak{M} = \frac{\mathfrak{N}}{N}M = \frac{M}{n(n-1)\ldots(n-l+1)}. \tag{11}$$

Remarquons à présent que, en vertu des formules (7) et (8), on aura

$$\Sigma \frac{h}{\theta} = \mathfrak{M}. \tag{12}$$

Si, dans cette dernière équation, on substitue les valeurs de $\frac{h}{\theta}$ et de $\mathfrak{M}$ données par les formules (10) et (11), alors, en effaçant le dénominateur commun aux deux membres, on trouvera

$$\Sigma r(r-1)\ldots(r-l+1)h = M. \tag{13}$$

Il importe d'observer que, r étant le nombre des variables exclues de la substitution P, $n-r$ sera le nombre des variables nécessairement comprises dans cette même substitution. Cela posé, soient

$$1,\quad P,\quad Q,\quad \ldots$$

les diverses substitutions qui n'altèrent pas la valeur de Ω, et nommons H_{n-r} le nombre de celles d'entre elles qui renferment précisément $n-r$ lettres. Il est clair que les valeurs de h correspondantes à ces dernières seront multipliées, dans le premier membre de l'équation (13), par des valeurs identiquement égales du produit

$$r(r-1)\ldots(r-l+1).$$

Par conséquent, à l'équation (13) on pourra substituer la suivante

$$\Sigma r(r-1)\ldots(r-l+1)H_{n-r} = M, \tag{14}$$

la somme qu'indique le signe Σ s'étendant désormais aux diverses valeurs de r.

Ajoutons que, Ω étant, par hypothèse, une fonction transitive non seulement de $n-l+1$, mais encore de $n-l+2$, ..., et même de n variables, l'équation (14) devra continuer de subsister quand on y remplacera l par un quelconque des nombres

$$1,\quad 2,\quad 3,\quad \ldots,\quad l-1.$$

Elle continuera même de subsister, en se confondant avec la for-

mule (4), quand on remplacera l par zéro, pourvu que l'on substitue l'unité au coefficient

$$r(r-1)\ldots(r-l+1),$$

comme on est conduit à le faire quand on attribue à ce coefficient la forme fractionnaire

$$\frac{1.2\ldots r}{1.2\ldots(r-l)}.$$

En développant le premier membre de la formule (14), ou de celles qu'on en déduit lorsqu'on remplace l par un des nombres $0, 1, 2, 3, \ldots, l-1$, et en observant que l'on a évidemment

$$H_1 = 0,\qquad H_0 = 1,$$

on tirera de la formule (14) les équations

$$\left\{\begin{aligned}
M &= H_n + H_{n-1} + H_{n-2} + \ldots + H_2 + 1,\\
M &= H_{n-1} + 2H_{n-2} + \ldots + (n-2)H_2 + n,\\
M &= 1.2H_{n-2} + \ldots + (n-3)(n-2)H_2 + (n-1)n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
M &= 1.2.3\ldots l H_{n-l} + \ldots + (n-l+1)\ldots(n-1)n,
\end{aligned}\right. \tag{15}$$

desquelles on déduira immédiatement les valeurs de

$$H_n,\quad H_{n-1},\quad H_{n-2},\quad \ldots,\quad H_{n-l},$$

exprimées en fonction de M et de

$$H_{n-l-1},\quad H_{n-l-2},\quad \ldots,\quad H_2.$$

La méthode d'élimination très simple qui sert à effectuer ce calcul et les conséquences remarquables qui se déduisent des formules (15) seront exposées dans un prochain article.

308.

Analyse mathématique. — *Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières, et des systèmes de substitutions conjuguées* (suite).

C. R., T. XXI, p. 1025 (10 novembre 1845).

§ I. — *Sur le dénombrement des substitutions diverses qui n'altèrent pas une fonction transitive de plusieurs variables indépendantes.*

Soient

Ω une fonction de n variables indépendantes $x, y, z, \ldots$;
M le nombre des valeurs égales de Ω;
m le nombre de ses valeurs distinctes.

Soit encore

$$(1)\qquad 1,\quad P,\quad Q,\quad R,\quad \ldots$$

le système des substitutions conjuguées qui n'altèrent pas la valeur de Ω, et H_r le nombre de celles qui déplacent r variables. La substitution 1, qui forme le premier terme de la série (1), sera la seule qui ne déplace aucune variable, et toute substitution, distincte de l'unité, déplacera tout au moins deux variables à la fois. On aura donc

$$H_0 = 1,\qquad H_1 = 0.$$

Si d'ailleurs Ω est une fonction transitive de n, de $n-1$, etc., et même de $n-l+1$ variables; alors, comme on l'a vu dans le précédent article, les diverses valeurs de H_r, représentées par

$$H_n,\quad H_{n-1},\quad H_{n-2},\quad \ldots,\quad H_2,$$

vérifieront les formules

$$(2)\quad \begin{cases} M = H_n + H_{n-1} + H_{n-2} + \ldots + H_2 + 1, \\ M = H_{n-1} + 2H_{n-2} + \ldots + (n-2)H_2 + n, \\ M = 1.2H_{n-2} + \ldots + (n-3)(n-2)H_2 + (n-1)n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ M = 1.2.3\ldots l\,H_{n-l} + \ldots + (n-l+1)\ldots(n-1)n. \end{cases}$$

Supposons maintenant que l'on désigne par e_n la somme des $n+1$ premiers termes du développement de e^{-1}, et par $[n]_r$ la somme des $r+1$ premiers termes du développement de $(1-1)^n$, n, r étant des nombres entiers quelconques, en sorte qu'on ait

$$(3)\qquad e_n = 1 - \frac{1}{1} + \frac{1}{1.2} - \frac{1}{1.2.3} + \ldots + \frac{(-1)^n}{1.2.3\ldots n}$$

et

$$(4)\qquad [n]_r = 1 - \frac{n}{1} + \frac{n(n-1)}{1.2} - \ldots + (-1)^r \frac{n(n-1)\ldots(n-r+1)}{1.2\ldots r}.$$

On trouvera successivement

$$(5)\qquad e_0 = 1,\quad e_1 = 0,\quad e_2 = \frac{1}{2},\quad e_3 = \frac{1}{3},\quad e_4 = \frac{3}{8},\quad e_5 = \frac{11}{30},\quad \ldots$$

De plus, on aura : 1° pour $n \leqq r$,

$$(6)\qquad [n]_r = 0;$$

2° pour $n > r$,

$$(7)\qquad [n]_r + (-1)^n [n]_{n-r-1} = 0;$$

et, en ayant égard à la formule (7), on trouvera

$$(8)\quad \begin{cases} [n]_0 = 1, & [n]_{n-1} = -(-1)^n, \\ [n]_1 = 1 - \dfrac{n}{1}, & [n]_{n-2} = -(-1)^n\left(1 - \dfrac{n}{1}\right), \\ [n]_2 = 1 - \dfrac{n}{1} + \dfrac{n(n-1)}{1.2}, & [n]_{n-3} = -(-1)^n\left[1 - \dfrac{n}{1} + \dfrac{n(n-1)}{1.2}\right], \\ \ldots\ldots\ldots\ldots\ldots, & \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Cela posé, si l'on combine entre elles, par voie d'addition, les formules (2), respectivement multipliées par les divers termes

$$1,\quad -1,\quad +\frac{1}{1.2},\quad -\frac{1}{1.2.3},\quad \ldots$$

du développement de e^{-1}, on trouvera

$$(9)\quad Me_l = H_n + [l+1]_l H_{n-l-1} + [l+2]_l H_{n-l-2} + \ldots + [n-2]_l H_2 + [n]_l;$$

et, si l'on applique le même calcul, non plus au système des équations (2), mais seulement à celles qui restent quand on a effacé, ou la première équation, ou les deux premières, ou les trois premières, etc., on obtiendra des équations nouvelles qui seront comprises, avec l'équation (9), dans la formule générale

$$(10)\quad \left\{\begin{aligned} Me_{l-r} = 1.2\ldots r H_{n-r} &+ (l+1)\ldots(l-r+2)[l-r+1]_{l-r} H_{n-l-1} \\ &+ (l+2)\ldots(l-r+3)[l-r+2]_{l-r} H_{n-l-2} + \ldots \\ &+ (n-2)\ldots(n-r-1)[n-r-2]_{l-r} H_2 \\ &+ n(n-1)\ldots(n-r+1)[n-r]_{l-r}, \end{aligned}\right.$$

r étant l'un quelconque des nombres entiers

$$0,\quad 1,\quad 2,\quad 3,\quad \ldots,\quad l.$$

Donc, en désignant par r un de ces nombres, on aura généralement

$$(11)\quad \left\{\begin{aligned} H_{n-r} = \frac{M}{1.2\ldots r} e_{l-r} &- \frac{(l+1)\ldots(l-r+2)}{1.2\ldots r}[l-r+1]_{l-r} H_{n-l-1} \\ &- \frac{(l+2)\ldots(l-r+3)}{1.2\ldots r}[l-r+2]_{l-r} H_{n-l-2} \\ &- \ldots\ldots\ldots\ldots\ldots\ldots \\ &- \frac{(n-2)\ldots(n-r+1)}{1.2\ldots r}[n-r-2]_{l-r} H_2 \\ &- \frac{n(n-1)\ldots(n-r+1)}{1.2\ldots r}[n-r]_{l-r}. \end{aligned}\right.$$

Il en résulte qu'on pourra exprimer généralement

$$H_n,\quad H_{n-1},\quad H_{n-2},\quad \ldots,\quad H_{n-l}$$

en fonction de M et de

$$H_{n-l-1},\quad H_{n-l-2},\quad \ldots,\quad H_2.$$

Il est bon d'observer que, dans le second membre de la formule (11), tous les termes qui suivent le premier seront évidemment des nombres entiers. J'ajoute qu'on pourra en dire autant du premier terme représenté par le produit

$$\frac{M}{1.2\ldots r} e_{l-r}.$$

En effet, Ω étant, par hypothèse, une fonction transitive de n, de $n-1$, ..., et même de $n-l+1$ variables, si l'on nomme $\mathfrak{M}$ le nombre des valeurs égales de Ω considéré comme fonction de $n-l$ variables, on aura

$$M = n(n-1)\ldots(n-l+1)\mathfrak{M}$$

et, par suite,

$$(12)\qquad \frac{M}{1.2\ldots r} e_{l-r} = \frac{n(n-1)\ldots(n-l+1)}{1.2\ldots r} e_{l-r}\mathfrak{M}.$$

Or, en vertu de la formule (3), le produit

$$1.2\ldots(l-r)\, e_{l-r}$$

sera certainement un nombre entier, et il est clair que, pour obtenir le second membre de la formule (12), il suffira de multiplier ce produit : 1° par le facteur entier $\mathfrak{M}$; 2° par le rapport

$$\frac{n(n-1)\ldots(n-l+1)}{(1.2\ldots r)[1.2\ldots(l-r)]},$$

qui est lui-même un nombre entier, puisqu'il représente le coefficient du produit

$$s^r t^{l-r}$$

dans le développement de l'expression

$$(1+s+t)^n.$$

Ainsi, comme on devait s'y attendre, la formule (11) fournira toujours une valeur entière de H_{n-r}.

Observons encore que, dans le second membre de la formule (4), les divers termes, alternativement positifs et négatifs, offrent des valeurs numériques toujours croissantes lorsque r ne surpasse pas $\frac{n}{2}$. Il en résulte que, dans le cas où l'on a

$$r \leqq \frac{n}{2},$$

la valeur de $[n]_r$ est toujours positive pour des valeurs paires de r, et toujours négative pour des valeurs impaires de r.

Si, dans la formule (11), on pose successivement $r=l$, puis $r=l-1$, on obtiendra les deux suivantes :

$$(13)\quad \begin{cases} H_{n-l} = \dfrac{M}{1.2\ldots l} - \dfrac{(l+1)\ldots 3.2}{1.2\ldots l} H_{n-l-1} - \ldots \\ \qquad - \dfrac{(n-2)\ldots(n-l-1)}{1.2\ldots l} H_2 - \dfrac{n(n-1)\ldots(n-l+1)}{1.2\ldots l}, \end{cases}$$

$$(14)\quad \begin{cases} H_{n-l+1} = \dfrac{(l+1)\ldots 4.3}{1.2\ldots(l-1)} H_{n-l-1} + \dfrac{(l+2)\ldots 5.4}{1.2\ldots(l-1)} 2 H_{n-l-2} + \ldots \\ \qquad + \dfrac{(n-1)\ldots(n-l)}{1.2\ldots(l-1)}(n-l-2) H_2 + \dfrac{n(n-1)\ldots(n-l+2)}{1.2\ldots(l-1)}(n-l). \end{cases}$$

Si, dans la formule (14), on pose $l=1$, on devra y remplacer par l'unité chacun des produits

$$1.2\ldots(l-1) = \frac{1.2\ldots l}{l}, \qquad 3.4\ldots(l+1) = \frac{1.2\ldots(l+1)}{1.2}, \qquad \ldots,$$

et l'on obtiendra l'équation

$$(15)\qquad H_n = H_{n-2} + 2 H_{n-3} + \ldots + (n-3) H_2 + n - 1,$$

que l'on peut établir directement en combinant entre elles, par voie de soustraction, la première et la seconde des formules (2). D'ailleurs, comme on aura toujours, en vertu de la formule (13),

$$(16)\qquad H_{n-l+1} \mathop{=}\limits_{>} \frac{n(n-1)\ldots(n-l+2)}{1.2\ldots(l-1)}(n-l),$$

et, en vertu de la formule (15),

$$(17)\qquad H_n \mathop{=}\limits_{>} n-1,$$

il en résulte qu'on peut énoncer les propositions suivantes :

Théorème I. — *Si Ω est une fonction transitive de n, de $n-1$, ..., et même de $n-l+1$ variables, alors, parmi les substitutions qui posséderont la propriété de ne point altérer la valeur de Ω, celles qui déplaceront à la fois $n-l+1$ variables seront en nombre égal ou supérieur au produit*

$$\frac{n(n-1)\ldots(n-l+2)}{1.2\ldots l}(n-l).$$

Théorème II. — *Si Ω est une fonction transitive de n variables x, y, z, ..., alors, parmi les substitutions qui n'altéreront pas la valeur de Ω, celles qui déplaceront à la fois les n variables seront en nombre égal ou supérieur à $n-1$.*

Ainsi, par exemple, si l'on prend $n=4$ et

$$\Omega = xy + zu,$$

alors trois substitutions régulières dont chacune déplacera les quatre lettres x, y, z, u, savoir

$$(x,y)(z,u), \quad (x,z)(y,u), \quad (x,u)(y,z),$$

se trouveront comprises parmi celles qui n'altéreront pas la valeur de la fonction transitive Ω.

Si, Ω étant une fonction transitive de n, de $n-1$, de $n-2$, et même de $n-l+1$ variables, il suffit de rendre $l+1$ variables immobiles, pour que toutes le deviennent; alors on aura nécessairement

$$H_{n-l-1} = 0, \qquad H_{n-l-2} = 0, \qquad \ldots, \qquad H_2 = 0,$$

et, par suite, la formule (11) donnera simplement

$$(18)\qquad H_{n-r} = \frac{M}{1.2\ldots r} e_{l-r} - \frac{n(n-1)\ldots(n-r+1)}{1.2\ldots r}[n-r]_{l-r}.$$

Si, dans cette dernière formule, on substitue successivement à r chacun des nombres

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad l-1, \quad l,$$

on obtiendra les suivantes

$$(19)\quad \begin{cases} H_n = M e_l - [n]_l, \\ H_{n-1} = \dfrac{M}{1} e_{l-1} - \dfrac{n}{1}[n-1]_{l-1}, \\ H_{n-2} = \dfrac{M}{1.2} e_{l-2} - \dfrac{n(n-1)}{1.2}[n-2]_{l-2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ H_{n-l+1} = \dfrac{M}{1.2\ldots(l-1)} e_1 - \dfrac{n(n-1)\ldots(n-l+2)}{1.2\ldots(l-1)}[n-l+1]_1, \\ H_{n-l} = \dfrac{M}{1.2\ldots l} e_0 - \dfrac{n(n-1)\ldots(n-l+1)}{1.2\ldots l}[n-l]_0, \end{cases}$$

dont les deux dernières se réduiront à

$$H_{n-l+1} = \frac{n(n-1)\ldots(n-l+2)}{1.2\ldots(l-1)}(n-l), \tag{20}$$

$$H_{n-l} = \frac{M}{1.2\ldots l} - \frac{n(n-1)\ldots(n-l+1)}{1.2\ldots l}. \tag{21}$$

Appliquons maintenant les formules qui précèdent à quelques exemples.

Si Ω est une fonction symétrique de n variables $x, y, z, \ldots$, on aura simplement

$$m = 1, \qquad M = N,$$

la valeur de N étant

$$N = 1.2.3\ldots n.$$

Alors aussi, Ω étant fonction transitive de n, de $n-1$, de $n-2$, ..., et même de deux variables, on pourra prendre

$$l = n - 1;$$

et, en ayant égard aux deux formules

$$e_n - e_{n-1} = \frac{(-1)^n}{N}, \qquad [n]_{n-1} = (-1)^{n-1},$$

qui subsistent pour toutes les valeurs entières et positives de n, on tirera des équations (19)

$$\left\{\begin{aligned} H_n &= Ne_n, \\ H_{n-1} &= \frac{N}{1} e_{n-1}, \\ H_{n-2} &= \frac{N}{1.2} e_{n-2}, \\ &\ldots\ldots\ldots\ldots, \\ H_3 &= \frac{N}{1.2\ldots(n-3)} e_3, \\ H_2 &= \frac{N}{1.2\ldots(n-2)} e_2. \end{aligned}\right. \tag{22}$$

Ainsi, le nombre total des substitutions qui, renfermant n variables x, $y, z, \ldots$, déplacent à la fois toutes ces variables, est déterminé par la formule

$$H_n = Ne_n. \tag{23}$$

On pourrait aisément, de cette première formule, déduire toutes celles qui la suivent dans le Tableau (22). Ajoutons que, si l'on substitue dans la première des équations (2) les valeurs de $H_n, H_{n-1}, \ldots, H_2$, tirées des formules (22), on trouvera

$$e_n + \frac{e_{n-1}}{1} + \frac{e_{n-2}}{1.2} + \ldots + \frac{e_0}{1.2\ldots n} = 1. \tag{24}$$

Supposons encore que Ω représente une des fonctions qui, renfermant n variables, offrent seulement deux valeurs distinctes. Alors on aura

$$m = 2, \qquad M = \frac{N}{2}.$$

Alors aussi, Ω étant fonction transitive de n, de $n-1$, de $n-2$, ..., et même des trois variables, on pourra prendre

$$n - l + 1 = 3, \qquad l = n - 2;$$

et, en ayant égard à la formule

$$[n]_{n-2} = (-1)^n (n-1),$$

on tirera des équations (19) les suivantes

$$\left\{\begin{aligned} H_n &= \frac{N}{2} e_{n-2} - (-1)^n (n-1), \\ H_{n-1} &= \frac{N}{2}\frac{e_{n-3}}{1} - (-1)^{n-1}\frac{n}{1}(n-2), \\ H_{n-2} &= \frac{N}{2}\frac{e_{n-4}}{1.2} - (-1)^{n-2}\frac{n(n-1)}{1.2}(n-3), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ H_3 &= \frac{N}{2}\frac{e_1}{1.2\ldots(n-3)} - (-1)^3\frac{n(n-1)\ldots4}{1.2\ldots(n-3)}2, \\ H_2 &= \frac{N}{2}\frac{e_0}{1.2\ldots(n-2)} - (-1)^2\frac{n(n-1)\ldots3}{1.2\ldots(n-2)}, \end{aligned}\right. \tag{25}$$

dont les deux dernières se réduisent à

$$H_3 = \frac{n(n-1)(n-2)}{3}, \qquad H_2 = 0. \tag{26}$$

D'ailleurs, le rapport

$$\frac{n(n-1)(n-2)}{3}$$

étant précisément le nombre total des substitutions circulaires du troisième ordre que l'on peut former avec n lettres, les formules (26) exprimeront une propriété bien connue des fonctions qui offrent seulement deux valeurs distinctes, savoir que l'une quelconque de ces fonctions est toujours altérée par une substitution circulaire du second ordre, et n'est jamais altérée par aucune substitution circulaire du troisième ordre.

§ II. — *Théorèmes relatifs à deux systèmes de substitutions conjuguées.*

Formons avec n variables $x, y, z, \ldots$ deux systèmes de substitutions conjuguées

$$1,\ \mathrm{P},\ \mathrm{Q},\ \mathrm{R},\ \ldots \tag{1}$$

et

$$1,\ \mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots. \tag{2}$$

Soient M l'ordre du premier système, et $\mathfrak{M}$ l'ordre du second système. Si une ou plusieurs substitutions du second système sont semblables à une ou plusieurs substitutions du premier système; si, par exemple, on suppose la substitution $\mathfrak{Q}$ semblable à la substitution R, alors $\mathfrak{Q}$ sera lié à R par une ou plusieurs équations de la forme

$$\mathfrak{Q} = \mathrm{URU}^{-1}, \tag{3}$$

et, réciproquement, lorsque deux substitutions appartenant, l'une au premier système, l'autre au second, se trouveront liées entre elles par une équation de cette forme, elles seront semblables l'une à l'autre.

Observons d'ailleurs que l'équation (3) peut encore être présentée sous chacune des formes

$$\mathrm{R} = \mathrm{U}^{-1}\mathfrak{Q}\mathrm{U}, \tag{4}$$

$$\mathfrak{Q}\mathrm{U} = \mathrm{UR}. \tag{5}$$

Supposons maintenant que l'on nomme E le nombre des substitutions U pour lesquelles se vérifient des équations semblables à la formule (5), l'une de ces substitutions devant se réduire à l'unité dans le cas particulier où les systèmes (1) et (2) offrent des termes communs. Soit, au contraire, F le nombre des substitutions U pour lesquelles ne se vérifient jamais des équations semblables à l'équation (5). $E+F$ sera évidemment le nombre total des substitutions que l'on pourra former avec les n variables $x, y, z, \ldots$, en sorte qu'on aura

$$E + F = N, \tag{6}$$

la valeur de N étant

$$N = 1.2.3\ldots n. \tag{7}$$

Concevons maintenant que la suite

$$\mathrm{U},\ \mathrm{V},\ \mathrm{W},\ \ldots \tag{8}$$

renferme plusieurs des substitutions U pour lesquelles se vérifient des équations de la forme (5), et construisons le Tableau

$$\left\{\begin{array}{llll} \mathrm{U}, & \mathrm{UP}, & \mathrm{UQ}, & \mathrm{UR}, \\ \mathrm{V}, & \mathrm{VP}, & \mathrm{VQ}, & \mathrm{VR}, \\ \mathrm{W}, & \mathrm{WP}, & \mathrm{WQ}, & \mathrm{WR}, \\ \ldots, & \ldots\ldots, & \ldots\ldots, & \ldots\ldots \end{array}\right. \tag{9}$$

Il est facile de s'assurer que chacune des substitutions comprises dans ce Tableau sera encore du nombre de celles pour lesquelles se vérifient des équations de la forme (5). Car, si l'on pose, par exemple,

$$\mathrm{UP} = \mathrm{U}'$$

et, par suite,

$$\mathrm{U} = \mathrm{U}'\mathrm{P}^{-1}, \qquad \mathrm{U}^{-1} = \mathrm{PU}^{-1},$$

l'équation (3), qui coïncide avec l'équation (5), donnera

$$\mathcal{Q} = \mathrm{U'R'U'^{-1}}, \tag{10}$$

là valeur de R′ étant

$$\mathrm{R'} = \mathrm{P^{-1}RP}; \tag{11}$$

et comme, en vertu de la formule (11), R′ sera une substitution comprise dans la série (1), mais semblable à R, et par conséquent distincte de l'unité, l'équation (10), à laquelle satisfera la substitution U′, sera évidemment de la même forme que l'équation (3) ou (5). D'ailleurs, deux termes compris dans deux lignes horizontales du Tableau (9) seront certainement distincts l'un de l'autre; et, si deux termes compris dans deux lignes horizontales différentes, par exemple les termes

$$\mathrm{UP}, \quad \mathrm{VQ},$$

compris dans la seconde et la troisième ligne horizontale, deviennent égaux, alors l'équation

$$\mathrm{VQ} = \mathrm{UP} \tag{12}$$

entraînera la formule

$$\mathrm{V} = \mathrm{UPQ^{-1}}, \tag{13}$$

en vertu de laquelle V sera déjà un des termes compris dans la seconde ligne horizontale. Donc tous les termes du Tableau (9) seront distincts les uns des autres, si en construisant ce Tableau on a soin de prendre pour premier terme de chaque nouvelle ligne horizontale une des substitutions non comprises dans les lignes déjà écrites, mais pour lesquelles se vérifient des équations de la forme (5). Or, ces conditions étant supposées remplies, concevons que l'on donne au Tableau (9) la plus grande étendue possible; alors il renfermera nécessairement toutes les substitutions pour lesquelles se vérifie la formule (5), et par conséquent E termes distincts, répartis entre des lignes horizontales qui renfermeront chacune M termes. Donc, si l'on nomme $\mathcal{X}$ le

nombre de ces lignes horizontales, on aura

$$E = M\mathcal{X}. \tag{14}$$

Ajoutons que, si l'on pose, pour abréger,

$$m = \frac{N}{M},$$

on aura identiquement

$$N = mM, \tag{15}$$

et que, des formules (6), (14), (15), on tirera immédiatement l'équation

$$\mathrm{F} = M(m - \mathcal{X}), \tag{16}$$

en vertu de laquelle F sera encore un multiple de M. Au reste, pour établir directement cette conclusion, il suffit de concevoir que la série (8) se compose, non plus de substitutions pour chacune desquelles se vérifient toujours des équations de la forme (5), mais, au contraire, de substitutions pour lesquelles ne se vérifient jamais des équations de cette forme. En effet, cette supposition étant adoptée, un terme quelconque du Tableau (5), par exemple le terme

$$\mathrm{U'} = \mathrm{UP},$$

ne pourra vérifier une équation de la forme (5), par exemple l'équation (10), R′ étant l'une des substitutions P, Q, R, ... Car, en remettant pour U′ sa valeur UP dans l'équation (10), et posant

$$\mathrm{PR'P^{-1}} = \mathrm{R},$$

on reviendrait de l'équation (10) à la formule (4), que devrait vérifier, contrairement à l'hypothèse admise, la substitution U. D'ailleurs, pour que les termes du Tableau (9) soient encore tous distincts les uns des autres, il suffira, comme ci-dessus, qu'en prolongeant ce Tableau on prenne toujours pour premier terme de chaque nouvelle ligne horizontale un terme non compris dans les lignes horizontales déjà écrites. Cela posé, il est clair que, au moment où, en remplissant ces conditions, on aura donné au Tableau (9) la plus grande étendue possible, ce Tableau renfermera F termes différents répartis entre diverses lignes horizontales dont le nombre sera $m-\mathfrak{X}$, et dont chacune sera composée de M termes. Donc le nombre F sera toujours un multiple de M, ainsi que l'indique la formule (16).

Par des raisonnements semblables à ceux qui précèdent, on prouverait encore que chacun des nombres E, F est un multiple de $\mathfrak{M}$, et l'on obtiendrait ainsi, à la place des formules (14), (16), deux équations de la forme

$$E=\mathfrak{M}K, \tag{17}$$

$$F=\mathfrak{M}(m-K). \tag{18}$$

Concevons à présent que, le Tableau (9) étant composé de substitutions pour lesquelles ne se vérifient jamais des équations de la forme (5), on désigne par

$$\mathfrak{U},\quad \mathfrak{V},\quad \mathfrak{W},\quad \ldots \tag{19}$$

plusieurs termes de ce Tableau, pris dans les lignes horizontales distinctes, et construisons encore le Tableau suivant :

$$\left\{\begin{array}{lllll} \mathfrak{U}, & \mathfrak{P}\mathfrak{U}, & \mathfrak{Q}\mathfrak{U}, & \mathfrak{R}\mathfrak{U}, & \ldots, \\ \mathfrak{V}, & \mathfrak{P}\mathfrak{V}, & \mathfrak{Q}\mathfrak{V}, & \mathfrak{R}\mathfrak{V}, & \ldots, \\ \mathfrak{W}, & \mathfrak{P}\mathfrak{W}, & \mathfrak{Q}\mathfrak{W}, & \mathfrak{R}\mathfrak{W}, & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots. \end{array}\right. \tag{20}$$

Un terme quelconque de ce nouveau Tableau, par exemple le terme

$$\mathfrak{U}'=\mathfrak{P}\mathfrak{U},$$

ne pourra vérifier une équation de la forme (5), ou, ce qui revient au même, de la forme (4). Car, si l'on avait, par exemple,

$$\mathrm{R}=\mathfrak{U}'^{-1}\mathfrak{Q}'\mathfrak{U}',$$

$\mathfrak{Q}'$ étant l'une des substitutions $\mathfrak{P}, \mathfrak{Q}, \mathfrak{R}, \ldots$, on en conclurait

$$\mathrm{R}=\mathfrak{U}^{-1}\mathfrak{Q}\mathfrak{U},$$

la valeur de $\mathfrak{Q}$ étant

$$\mathfrak{Q}=\mathfrak{P}^{-1}\mathfrak{Q}'\mathfrak{P},$$

et, par suite, $\mathfrak{U}$ serait, contrairement à l'hypothèse admise, une substitution pour laquelle se vérifierait une équation de la forme (4) ou (5). Donc un terme quelconque du Tableau (20) sera l'un de ceux qui faisaient déjà partie du Tableau (8). Il y a plus : deux termes compris dans une même ligne horizontale du Tableau (20) ne pourront faire partie d'une même ligne horizontale du Tableau (9); car, si l'on avait à la fois, par exemple,

$$\mathfrak{P}\mathfrak{U}=\mathrm{VR},\qquad \mathfrak{Q}\mathfrak{U}=\mathrm{VS},$$

on en conclurait

$$\begin{aligned} \mathfrak{U}&=\mathfrak{P}^{-1}\mathrm{VR},\\ \mathfrak{Q}\mathfrak{P}^{-1}\mathrm{VR}&=\mathrm{VS},\\ \mathfrak{Q}\mathfrak{P}^{-1}\mathrm{V}&=\mathrm{VSR}^{-1}, \end{aligned}$$

et, par suite, V serait, contrairement à l'hypothèse admise, une des substitutions pour lesquelles se vérifierait une équation de la forme (5). Enfin, si deux termes compris dans deux lignes horizontales différentes du Tableau (20), par exemple les deux termes

$$\mathfrak{P}\mathfrak{U}\quad \text{et}\quad \mathfrak{Q}\mathfrak{V},$$

compris dans la seconde et la troisième ligne horizontale, appartenaient à une même ligne horizontale du Tableau (9), de sorte qu'on eût

$$\mathfrak{P}\mathfrak{U}=\mathrm{VR},\qquad \mathfrak{Q}\mathfrak{V}=\mathrm{VS},$$

on en conclurait

$$\mathfrak{Q}^{-1}\mathfrak{P}\mathfrak{U}=\mathfrak{Q}^{-1}\mathrm{VR},\qquad \mathfrak{V}=\mathfrak{Q}^{-1}\mathrm{VS}.$$

Mais alors, en nommant W le premier terme de la ligne horizontale du Tableau (9) qui renfermerait la substitution $\mathfrak{Q}^{-1}\mathfrak{P}\mathfrak{V}$, on pourrait satisfaire à la formule

$$\mathfrak{Q}^{-1}\mathfrak{P}\mathfrak{U}=\mathfrak{Q}^{-1}\mathrm{VR}=\mathrm{WT}$$

par une valeur de T prise dans la suite 1, P, Q, R, ..., et, des deux formules

$$\mathfrak{Q}^{-1}\mathrm{VR}=\mathrm{WT},\qquad \mathfrak{V}=\mathfrak{Q}^{-1}\mathrm{VS},$$

on tirerait

$$\mathfrak{V}=\mathrm{WTR}^{-1}\mathrm{S};$$

en sorte que $\mathcal{V}$ et $\mathcal{P}^{-1}\mathcal{Q}\mathcal{V}$ seraient deux termes pris dans la même suite horizontale du Tableau (9). Donc tous les termes du Tableau (20) appartiendront à des lignes horizontales distinctes du Tableau (9), si, en prolongeant le Tableau (20), on a soin de prendre pour premier terme de chaque nouvelle ligne horizontale une substitution comprise dans le Tableau (9), mais située hors des lignes de ce Tableau, qui ont fourni quelques-uns des termes déjà écrits dans le Tableau (20). Si, en remplissant cette condition, l'on donne au Tableau (20) la plus grande étendue possible, il renfermera définitivement autant de termes que le Tableau (9) renfermait de lignes horizontales, c'est-à-dire $m - \mathcal{K}$ termes répartis entre plusieurs lignes horizontales, dont chacune sera composée de $\mathfrak{M}$ termes. Donc $m - \mathcal{K}$ sera un multiple de $\mathfrak{M}$, en sorte qu'on aura

$$m - \mathcal{K} \equiv 0 \pmod{\mathfrak{M}}. \tag{21}$$

On prouverait de la même manière que l'on aura encore

$$m - K \equiv 0 \pmod{M}. \tag{22}$$

D'ailleurs, comme on tire des formules (16) et (18)

$$F = M(m - \mathcal{K}) = \mathfrak{M}(m - K) \tag{23}$$

et, par suite,

$$\frac{m-K}{M} = \frac{m-\mathcal{K}}{\mathfrak{M}}, \tag{24}$$

il est clair que la formule (21) devait entraîner la formule (22).

La formule (21) est l'expression du théorème énoncé à la page 380. Cette même formule, combinée avec l'équation (23), donne immédiatement

$$F \equiv 0 \pmod{M\mathfrak{M}} \tag{25}$$

ou, ce qui revient au même,

$$E \equiv N \pmod{M\mathfrak{M}}. \tag{26}$$

En conséquence, on peut énoncer la proposition suivante :

Théorème I. — *Formons avec n variables $x, y, z, \ldots$ deux systèmes de substitutions conjuguées, et soient*

$$1,\ P,\ Q,\ R,\ \ldots,$$
$$1,\ \mathcal{P},\ \mathcal{Q},\ \mathcal{R},\ \ldots$$

ces deux systèmes, le premier de l'ordre M, le second de l'ordre $\mathfrak{M}$. Nommons E le nombre total des substitutions U, pour lesquelles se vérifient des équations de la forme

$$\mathcal{P}U = UP, \tag{27}$$

et posons, pour abréger, $N = 1.2.3\ldots n$. Les nombres N, E fourniront le même reste lorsqu'on les divisera par le produit $M\mathfrak{M}$.

Corollaire. — Si les deux systèmes se réduisent à un seul, alors, au lieu du théorème I, on obtiendra la proposition suivante :

Théorème II. — *Soit*

$$1,\ P,\ Q,\ R,\ \ldots$$

un système de substitutions conjuguées de l'ordre M, et nommons E le nombre des substitutions U *pour lesquelles se vérifient des équations de la forme*

$$QU = UP, \tag{28}$$

Q *pouvant se confondre avec* P. *Le nombre E et le nombre $N = 1.2\ldots n$, divisés par le carré de M, fourniront le même reste, en sorte qu'on aura*

$$E \equiv N \pmod{M^2}. \tag{29}$$

Corollaire. — Si M^2 surpasse N, la formule (29) donnera nécessairement

$$E = N, \tag{30}$$

et par suite une substitution quelconque U sera du nombre de celles pour lesquelles peut se vérifier la formule (28).

Supposons maintenant que les M substitutions conjuguées

$$1,\ P,\ Q,\ R,\ \ldots$$

soient précisément celles qui n'altèrent pas la valeur d'une certaine fonction Ω. Soit, d'ailleurs, U l'une des substitutions pour lesquelles peut se vérifier la formule (5), ou, ce qui revient au même, la formule (27). Si l'on nomme Ω' ce que devient la fonction Ω quand on lui applique la substitution U, il est clair qu'on obtiendra encore Ω' en appliquant à Ω, ou la substitution UP, ou son égale $\mathfrak{P}$U, et par conséquent en appliquant à Ω' la substitution $\mathfrak{P}$. Donc, alors, Ω' sera l'une des fonctions que n'altère pas la substitution $\mathfrak{P}$. Ajoutons que, dans la même hypothèse, les M substitutions qui n'altéreront pas la fonction Ω' seront évidemment

$$\mathrm{U},\quad \mathrm{UP},\quad \mathrm{UQ},\quad \mathrm{UR},\quad \ldots.$$

D'autre part, si U est l'une des substitutions qui transforment Ω en Ω', et si la valeur de la fonction Ω' n'est pas altérée quand on lui applique l'une des substitutions $\mathfrak{P}, \mathfrak{Q}, \mathfrak{R}, \ldots$, par exemple la substitution $\mathfrak{P}$, on pourra passer de Ω à Ω' à l'aide de chacune des substitutions

$$\mathrm{U},\quad \mathfrak{P}\mathrm{U},$$

et revenir de Ω' à Ω à l'aide de l'une des substitutions inverses

$$\mathrm{U}^{-1},\quad \mathrm{U}^{-1}\mathfrak{P}^{-1}.$$

Donc on n'altérera pas la fonction Ω en lui appliquant la substitution

$$\mathrm{U}^{-1}\mathfrak{P}\mathrm{U},$$

et cette dernière substitution devra être égale à l'une des substitutions P, Q, R, ..., en sorte qu'on aura, par exemple,

$$\mathrm{U}^{-1}\mathfrak{P}\mathrm{U} = \mathrm{P}$$

et, par suite,

$$\mathfrak{P}\mathrm{U} = \mathrm{UP}.$$

De ces remarques il suit évidemment que le nombre E des substitutions pour lesquelles se vérifie la formule (27) est le produit de M par le nombre de celles des fonctions

$$\Omega,\quad \Omega',\quad \Omega'',\quad \ldots$$

qui ne sont pas altérées quand on effectue les substitutions $1, \mathfrak{P}, \mathfrak{Q}, \ldots$, ou au moins l'une d'entre elles. Donc ce dernier nombre est précisément celui qui, dans la formule (21), se trouve représenté par la lettre $\mathfrak{x}$. Il en résulte aussi que la formule (21) entraîne le théorème I de la page 376.

Dans un prochain article, je montrerai comment, étant données les substitutions $\mathfrak{P}$, P, on peut déterminer le nombre des substitutions U pour lesquelles se vérifie la formule (27). J'établirai à ce sujet quelques nouvelles propriétés des substitutions qui sont semblables entre elles.

309.

Analyse mathématique. — *Rapport sur un Mémoire présenté à l'Académie par* M. Bertrand, *et relatif au nombre des valeurs que peut prendre une fonction, quand on y permute les lettres qu'elle renferme.*

C. R., T. XXI, p. 1042 (10 novembre 1845).

Lorsque, dans une fonction de n variables, on permute les variables entre elles de toutes les manières possibles, on obtient diverses valeurs dont le nombre est précisément le produit $1.2.3\ldots n$. D'ailleurs, deux quelconques de ces valeurs de la fonction peuvent être, ou égales entre elles, quelles que soient les valeurs attribuées aux variables elles-mêmes, ou généralement distinctes, de manière à ne pouvoir se confondre que pour certains systèmes de valeurs des variables dont il s'agit. Enfin le nombre des valeurs distinctes de la fonction est toujours, comme on le démontre aisément, un diviseur du nombre total des valeurs égales ou inégales, c'est-à-dire du produit $1.2.3\ldots n$. Mais il n'est pas toujours possible de former une fonction pour laquelle le nombre des valeurs distinctes soit un diviseur donné de ce produit, par exemple l'un des nombres entiers

$$1,\quad 2,\quad 3,\quad \ldots,\quad n.$$

A la vérité, on peut, avec un nombre quelconque de lettres, former, outre les fonctions *symétriques*, qui n'ont qu'une valeur, des fonctions qui offrent seulement deux valeurs distinctes; et l'on peut encore, dans le cas singulier où l'on considère quatre lettres, former une fonction qui n'offre que trois valeurs distinctes. Mais, d'autre part, un géomètre italien, M. Ruffini, a démontré qu'on ne peut, avec cinq variables, former une fonction qui offre moins de cinq valeurs, si elle en a plus de deux; et un autre Italien, M. Pietro Abbati, a étendu cette proposition au cas où la fonction renferme un nombre quelconque de variables. En outre, l'un de nous a démontré, il y a environ trente ans, que, pour une fonction de n variables, le nombre des valeurs distinctes, quand il est supérieur à 2, ne peut être inférieur au plus grand nombre premier contenu dans n. Enfin, dans le Mémoire qui renferme cette démonstration, on trouve le passage suivant :

Il n'est pas toujours possible d'abaisser l'indice, c'est-à-dire le nombre des valeurs d'une fonction jusqu'à la limite que nous venons d'assigner; et, si l'on en excepte les fonctions du quatrième ordre qui peuvent obtenir trois valeurs, je ne connais pas de fonctions non symétriques dont l'indice soit inférieur à l'ordre (au nombre des lettres), *sans être égal à* 2. *Le théorème ci-dessus établi prouve du moins qu'il n'en existe pas de semblables, quand l'ordre de la fonction est un nombre premier, puisque alors la limite trouvée se confond avec ce nombre. On peut encore démontrer cette assertion, lorsque n est égal à* 6, *en faisant voir qu'une fonction de* 6 *lettres ne peut obtenir plus de six valeurs, quand elle en a plus de deux.*

La démonstration générale de la proposition que l'auteur du Mémoire avait énoncée dans ce passage, et qu'il avait rigoureusement établie dans le cas où n est un nombre premier ou bien encore le nombre 6, est aussi l'un des principaux objets des recherches dont nous avons à rendre compte. M. Bertrand est effectivement parvenu à la démontrer, en supposant qu'il existe toujours un nombre premier p compris entre les limites $n-2$ et $\frac{n}{2}$, et en s'appuyant sur la considération des substitutions circulaires formées avec $p+2$ lettres, partagées en deux groupes dont l'un renferme p lettres, et l'autre deux lettres seulement. Mais existe-t-il toujours, au moins quand n surpasse 7, un nombre premier compris entre $n-2$ et $\frac{n}{2}$? Cela est extrêmement probable, et l'on peut, à l'aide des Tables des nombres premiers, s'assurer de l'existence d'un tel nombre, au moins tant que n est inférieur à 6 millions. Ainsi, les calculs de M. Bertrand suffisent pour étendre à tout nombre qui ne surpasse pas cette limite la proposition énoncée. Ils prouvent aussi que, pour une valeur de n inférieure à cette limite, une fonction de n lettres qui offre seulement n valeurs distinctes est généralement symétrique par rapport à $n-1$ lettres.

Parmi les nombres non premiers dont la valeur n'est pas considérable, il en existe deux seulement auquel la démonstration de M. Bertrand ne s'applique pas : ce sont les nombres 4 et 6. M. Bertrand mentionne le nombre 4, qui, comme nous l'avons déjà dit, fait exception à la règle générale. Il aurait dû, pour plus d'exactitude, mentionner aussi le nombre 6, et observer que $2p$ cesse d'être supérieur à n, quand on a $p=3$, $n=6$. D'ailleurs, comme nous l'avons rappelé ci-dessus, le principal théorème se trouve depuis longtemps démontré, pour le cas où l'on a $n=6$.

Le Mémoire de M. Bertrand renferme encore quelques autres propositions dignes de remarque sur le nombre des valeurs qu'une fonction peut acquérir. Il prouve, entre autres choses, que, p, q étant deux nombres premiers dont la somme est inférieure à n, une fonction de n lettres aura précisément $2n$ valeurs distinctes, si le nombre des valeurs distinctes est inférieur au produit pq, et si d'ailleurs le nombre n des lettres est égal ou supérieur à 10.

En résumé, les Commissaires pensent que le Mémoire de M. Bertrand est digne d'être approuvé par l'Académie et inséré dans le *Recueil des Mémoires des Savants étrangers*.

310.

Analyse mathématique. — *Mémoire sur les premiers termes de la série des quantités qui sont propres à représenter le nombre des valeurs distinctes d'une fonction des n variables indépendantes.*

C. R., T. XXI, p. 1093 (17 novembre 1845).

§ I. — *Considérations générales.*

Soient

Ω une fonction de n variables $x, y, z, \ldots$;
m le nombre des valeurs distinctes de cette fonction;
M le nombre de ses valeurs égales.

On aura

$$mM = N, \tag{1}$$

$$N = 1.2.3\ldots n,$$

et par suite le nombre m des valeurs distinctes de Ω sera toujours un diviseur du produit N, c'est-à-dire du nombre des arrangements que l'on peut former avec n lettres. Donc, si l'on forme la série des nombres qui seront propres à représenter les diverses valeurs de m, tous les termes de cette série seront des diviseurs de N. Mais la proposition réciproque n'est pas vraie, et tous les diviseurs de N n'entrent pas dans la série en question. Nous allons, dans cette Note, rechercher les premiers termes de la série, c'est-à-dire ceux qui expriment les plus petites valeurs de m.

D'abord, puisque, avec un nombre quelconque n des variables, on peut toujours composer des fonctions symétriques, c'est-à-dire des fonctions qui ne sont point altérées par des échanges quelconques opérés entre les variables, et même des fonctions dont chacune offre deux valeurs distinctes, il en résulte que, pour une valeur quelconque de n, les deux premiers termes de la série formée avec les diverses valeurs de m seront toujours les nombres 1 et 2.

Il est d'ailleurs facile de s'assurer : 1° que toute fonction qui n'est altérée par aucune substitution circulaire du second ordre est nécessairement symétrique; 2° que toute fonction non symétrique qui n'est altérée par aucune substitution circulaire du troisième ordre offre seulement deux valeurs distinctes.

Pour savoir quelles sont les valeurs que peut acquérir le nombre m quand il devient supérieur à 2, il convient de distinguer le cas où la fonction Ω est *intransitive*, et le cas où elle est *transitive*.

Quand la fonction Ω est intransitive, c'est-à-dire quand les substitutions

$$1,\quad P,\quad Q,\quad R,\quad \ldots, \tag{2}$$

qui n'altèrent pas la valeur de Ω, ont pour effet unique d'échanger, séparément entre elles, des variables que renferment divers groupes composés, le premier, de a variables

$$\alpha,\quad \beta,\quad \gamma,\quad \ldots;$$

le second, de b variables

$$\lambda,\quad \mu,\quad \nu,\quad \ldots;$$

le troisième, de c variables

$$\varphi,\quad \chi,\quad \psi,\quad \ldots,$$
$$.,\quad .,\quad .,\quad \ldots,$$

on a évidemment

$$n = a + b + c + \ldots, \tag{3}$$

chacun des nombres $a, b, c, \ldots$ étant inférieur à n. Soient d'ailleurs, dans cette hypothèse, A le nombre de celles des substitutions (2) qui correspondent à des permutations diverses des variables $\alpha, \beta, \gamma, \ldots$ du premier groupe; B le nombre de celles des substitutions (2) qui, en laissant immobiles les variables $\alpha, \beta, \gamma, \ldots$ du premier groupe, correspondent à des permutations diverses des variables $\lambda, \mu, \nu, \ldots$ du second groupe, etc. On trouvera

$$M = ABC\ldots; \tag{4}$$

et par suite, si l'on pose, pour abréger,

$$(5)\qquad \mathfrak{A}=\frac{1.2\ldots a}{A},\qquad \mathfrak{B}=\frac{1.2\ldots b}{B},\qquad \mathfrak{C}=\frac{1.2\ldots c}{C},\qquad \ldots,$$

$$(6)\qquad \mathfrak{N}=\frac{1.2.3\ldots n}{(1.2\ldots a)(1.2\ldots b)(1.2\ldots c)},$$

on aura

$$(7)\qquad m=\mathfrak{N}\mathfrak{A}\mathfrak{B}\mathfrak{C}\ldots,$$

$\mathfrak{N}$ étant un entier qui sera évidemment supérieur à l'unité.

Il est bon d'observer que, dans la formule (3), on peut toujours supposer les nombres

$$a,\quad b,\quad c,\quad \ldots$$

rangés par ordre de grandeur, les plus grands d'entre eux étant représentés par les premières lettres de l'alphabet. Ajoutons que, en vertu de la formule (6), $\mathfrak{N}$ sera le coefficient du produit

$$r^a s^b t^c \ldots$$

dans le développement de l'expression

$$(r+s+t+\ldots)^n,$$

et que, par suite, $\mathfrak{N}$ sera toujours un multiple de l'un des coefficients numériques renfermés dans le développement de

$$(r+s)^n,$$

c'est-à-dire un multiple de l'un des nombres figurés compris dans la suite

$$(8)\qquad n,\quad \frac{n(n-1)}{1.2},\quad \frac{n(n-1)(n-2)}{1.2.3},\quad \ldots,$$

qui devra être arrêtée à l'instant où l'on aura écrit son plus grand terme. Le coefficient 1 se trouve exclu de cette suite, parce que, Ω étant une fonction intransitive, chacun des nombres $a, b, c, \ldots$ doit être, comme on l'a déjà remarqué, inférieur à n.

Quand la fonction Ω est transitive, c'est-à-dire lorsque, sans altérer

cette fonction, l'on peut faire passer à une place donnée une variable quelconque, le nombre m des valeurs distinctes de Ω considéré comme fonction des n variables données $x, y, z, \ldots$ est en même temps le nombre des valeurs distinctes de Ω considéré comme fonction des $n-1$ variables $y, z, \ldots$.

§ II. — *Détermination de quelques-unes des plus petites valeurs de m.*

Il est maintenant facile de trouver quelques-unes des plus petites valeurs que le nombre m puisse acquérir, quand il devient supérieur à 2.

En effet, n étant le plus petit terme de la série (8) du § I, il suit immédiatement des formules (6), (7) du même paragraphe que, si Ω est une fonction intransitive, le nombre m de ses valeurs distinctes ne pourra être inférieur à n.

Il y a plus : Ω étant une fonction intransitive, on ne tirera de la formule (7) du § I

$$(1)\qquad m=n$$

que dans le cas où l'on aura, non seulement

$$\mathfrak{N}=n$$

et, par suite,

$$a=n-1,\qquad b=1,\qquad \mathfrak{B}=1,$$

mais encore

$$\mathfrak{A}=1,$$

c'est-à-dire dans le cas où Ω sera fonction symétrique des $n-1$ variables renfermées dans le premier groupe.

Enfin si, Ω étant une fonction intransitive, m devient supérieur à n, il devra être au moins égal au plus petit des nombres

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

De ces deux valeurs de m on obtiendra la première

$$(2)\qquad m=2n,$$

en supposant, comme ci-dessus,

$$\mathcal{N} = n, \quad a = n-1, \quad b = 1, \quad \mathcal{B} = 1,$$

et, de plus,

$$\mathcal{A} = 2,$$

c'est-à-dire en supposant que Ω, considéré comme fonction de $n-1$ variables, offre seulement deux valeurs distinctes. Au contraire, on trouvera

$$m = \frac{n(n-1)}{2},$$

en supposant, non seulement

$$\mathcal{N} = \frac{n(n-1)}{2},$$

et, par suite,

$$a = n-2, \quad b = 2,$$

mais encore

$$\mathcal{A} = 1, \quad \mathcal{B} = 1,$$

c'est-à-dire en supposant que Ω est une fonction symétrique des $n-2$ variables comprises dans le premier groupe, et des deux variables comprises dans le second.

En résumant ce qu'on vient de dire, on obtient la proposition suivante :

Théorème I. — *Ω étant une fonction intransitive de n variables indépendantes, si l'on désigne par m le nombre des valeurs distinctes de Ω, les plus petites valeurs que m pourra prendre seront le nombre n et le plus petit des nombres*

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

D'ailleurs, on obtiendra la valeur n ou $2n$ du nombre m, en supposant que les variables se partagent en deux groupes dont l'un renferme une seule variable x, et que Ω, considéré comme fonction des $n-1$ variables restantes $y, z, \ldots$, est ou une fonction symétrique, ou une fonction qui offre seulement deux valeurs distinctes. On obtiendra, au contraire, la valeur $\frac{n(n-1)}{2}$ de m, en supposant que les variables

se partagent en deux groupes dont l'un renferme deux variables x, y, et que Ω est fonction symétrique des variables comprises dans chaque groupe.

Voyons maintenant ce qui arrivera si Ω est une fonction transitive des variables

$$x, \quad y, \quad z, \quad \ldots;$$

et cherchons d'abord, dans cette hypothèse, quelles valeurs pourra prendre le nombre m s'il est inférieur à n.

On rendra cette recherche plus facile, en commençant par établir la proposition suivante :

Théorème II. — *Soient Ω une fonction transitive de n variables indépendantes*

$$x, \quad y, \quad z, \quad \ldots,$$

et m le nombre des valeurs distinctes de Ω. Si, dans cette fonction, l'on peut faire passer à trois places données trois variables quelconques arbitrairement choisies, m ne pourra s'abaisser au-dessous de n, sans être l'un des nombres 1, 2.

Démonstration. — Les substitutions circulaires du second ordre qui renferment la lettre x, savoir

$$(3) \qquad (x, y), \quad (x, z), \quad \ldots,$$

sont en nombre égal à $n-1$; et, si l'on applique séparément chacune d'elles à la fonction Ω, on obtiendra $n-1$ valeurs nouvelles de cette fonction. Soient

$$\Omega', \quad \Omega'', \quad \Omega''', \quad \ldots$$

ces mêmes valeurs. Les n quantités

$$(4) \qquad \Omega, \quad \Omega', \quad \Omega'', \quad \Omega''', \quad \ldots,$$

c'est-à-dire les n valeurs que pourra prendre la fonction Ω, en vertu des substitutions

$$(x, x) = 1, \quad (x, y), \quad (x, z), \quad \ldots,$$

ne pourront être toutes distinctes les unes des autres, si l'on a $m < n$.

Donc alors le premier terme de la suite (4) sera équivalent à l'un des suivants, ou deux de ces derniers seront égaux entre eux. Dans le premier cas, la fonction Ω ne sera point altérée par une substitution circulaire du second ordre qui renfermera, outre la variable x, une autre variable y. Dans le second cas, la fonction Ω acquerra deux nouvelles valeurs Ω' égales entre elles, en vertu de deux substitutions circulaires du second ordre qui renfermeront, avec la variable x, deux nouvelles variables y, z. Mais l'inverse d'une substitution circulaire du second ordre étant cette substitution même, si chacune des deux substitutions

$$(x, y), \quad (x, z)$$

transforme Ω en Ω', chacune d'elles transformera réciproquement Ω' en Ω; et, en conséquence, Ω ne sera point altéré par l'une quelconque des substitutions du troisième ordre

$$(x, y)(x, z) = (x, z, y), \qquad (x, z)(x, y) = (x, y, z).$$

Enfin, si, la valeur de Ω n'étant pas altérée par la substitution circulaire

$$(x, y) \quad \text{ou} \quad (x, y, z),$$

on peut faire passer deux variables quelconques à la place de x et de y, ou même trois variables quelconques, arbitrairement choisies, aux places primitivement occupées par x, y et z, il s'ensuivra que la valeur de Ω ne pourra être altérée par aucune substitution circulaire semblable à (x, y), c'est-à-dire du second ordre, ou par aucune substitution circulaire semblable à (x, y, z), c'est-à-dire du troisième ordre. Mais alors Ω sera nécessairement, ou une fonction symétrique, ou une fonction qui offrira seulement deux valeurs distinctes.

Corollaire. — En vertu du théorème II, si Ω, étant une fonction transitive de n variables, offre un nombre m de valeurs distinctes supérieur à 2, le nombre m ne pourra s'abaisser au-dessous de n, que dans l'un des deux cas ci-après énoncés, savoir :

1° Lorsque Ω sera fonction transitive des n variables $x, y, z, \ldots$ et fonction intransitive des $n-1$ variables $y, z, \ldots$;

2° Lorsque Ω sera fonction transitive, non seulement des n variables $x, y, z, \ldots$, mais encore des $n-1$ variables $y, z, \ldots$ et fonction intransitive des $n-2$ variables $z, \ldots$.

Or, dans le premier cas, m étant le nombre des valeurs distinctes d'une fonction intransitive de $n-1$ variables ne pourra, d'après le théorème I, être inférieur à n, à moins que l'on n'ait

$$m = n - 1,$$

et que Ω ne devienne fonction symétrique de $n-2$ variables. Mais, d'après ce qu'on a vu dans un précédent Mémoire, page 309, Ω, que l'on suppose être une fonction transitive et non symétrique de n variables $x, y, z, \ldots$, ne pourra être en même temps une fonction symétrique de $n-2$ variables $z, \ldots$, que si l'on a

$$n = 4, \qquad n - 1 = 3.$$

Dans le second cas, m étant le nombre des valeurs distinctes d'une fonction intransitive de $n-2$ variables, les plus petites valeurs que m pourra prendre seront, en vertu du théorème I, le nombre $n-2$ et le plus petit des nombres

$$2(n-2), \quad \frac{(n-2)(n-3)}{2}.$$

D'ailleurs le nombre $2(n-2)$ ne peut devenir supérieur à 2 sans devenir en même temps égal ou supérieur à n; et, quant au nombre figuré $\frac{(n-2)(n-3)}{2}$, il ne peut être à la fois supérieur à 2 et distinct du nombre $n-2$ sans être supérieur à $n-1$. Donc, en vertu du théorème I, m ne pourra, dans le second des deux cas énoncés, s'abaisser au-dessous de n, à moins que l'on n'ait

$$m = n - 2,$$

et que Ω ne devienne fonction symétrique de $n-3$ variables. Mais alors Ω, étant tout à la fois fonction transitive de n, ou même de $n-1$ variables, et fonction symétrique de $n-3$ variables, devrait être nécessairement fonction symétrique de $n-1$, et, par suite, de n variables, quand on aurait

$$n-1>4,$$

et même lorsqu'on supposerait

$$n-1=4, \quad n=5.$$

Car, dans ce cas particulier, on trouverait $n-3=2$, et les deux variables, dont Ω serait fonction symétrique, pourraient être remplacées par deux variables quelconques sans que la valeur de Ω fût altérée. Donc, en définitive, le seul cas où m pourra s'abaisser au-dessous de n, sans être l'un des nombres 1, 2, sera le cas particulier où l'on aura

$$n=4, \quad m=3;$$

et l'on peut énoncer la proposition suivante :

Théorème III. — *Soit Ω une fonction transitive de n variables indépendantes*

$$x, y, z, \ldots,$$

et m le nombre des valeurs distinctes de Ω. Le nombre m pourra se réduire, pour une valeur quelconque de n, à l'unité ou au nombre 2. Mais, si m devient supérieur à 2, il ne pourra être inférieur à n que dans le cas particulier où l'on aura

$$n=4, \quad m=3,$$

et où la fonction Ω sera tout à la fois transitive par rapport à quatre variables, intransitive par rapport à trois, et symétrique par rapport à deux.

Corollaire. — La proposition précédente est précisément celle qui, dans l'un de mes Mémoires de 1812, se trouvait indiquée, pour une valeur quelconque de n, et rigoureusement démontrée pour le cas où n est ou un nombre premier quelconque, ou le nombre 6. La démonstration que M. Bertrand a donnée de la même proposition s'appuie sur un lemme dont l'exactitude a été vérifiée, à l'aide des Tables de nombres premiers, pour toute valeur de n inférieure à 6 millions.

Mais on voit par ce qui précède que, sans recourir à l'inspection des Tables de nombres premiers, on peut démontrer rigoureusement le théorème II, quel que soit d'ailleurs le nombre n des variables comprises dans la fonction Ω.

Je ferai voir, dans un prochain article, que, si, le nombre n étant supérieur à 10, le nombre m est supérieur à $n-1$, mais inférieur à la limite

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

on aura nécessairement, ou

$$m=n \quad \text{ou} \quad m=2n.$$

311.

Analyse mathématique. — *Mémoire sur la résolution des équations linéaires symboliques, et sur les conséquences remarquables que cette résolution entraîne après elle dans la théorie des permutations.*

C. R., T. XXI, p. 1123 (24 novembre 1845).

Les équations symboliques auxquelles je me suis trouvé conduit par mes recherches sur le nombre des valeurs des fonctions offrent cette circonstance singulière que chacun des produits symboliques qui s'y trouvent renfermés varie, en général, quand on échange ses facteurs entre eux. Considérons en particulier l'équation symbolique qui exprime que deux substitutions données sont semblables l'une à l'autre. Ses deux membres seront les produits des substitutions données par une troisième substitution qui devra entrer dans un des deux produits comme multiplicande, et dans l'autre produit comme multiplicateur. L'équation dont il s'agit sera donc une équation symbolique, *linéaire* par rapport à cette troisième substitution. Mais, il importe d'en faire la remarque, cette équation symbolique, bien différente en cela de toutes les équations linéaires connues, aura généralement plusieurs solutions. Le nombre de ces solutions dépendra du nombre total des substitutions semblables aux proposées, qui pourront être formées avec les variables que l'on considère, et sera précisément le quotient qu'on obtient quand on divise par ce dernier nombre le nombre des arrangements qui peuvent être formés avec ces variables. La règle très simple que je donne pour obtenir l'une quelconque de ces solutions consiste à écrire l'une au-dessus de l'autre les deux substitutions données, en ayant soin de faire correspondre les uns aux autres les facteurs circulaires composés d'un même nombre de variables, puis à effacer les virgules et parenthèses placées entre les diverses variables. Alors ces deux substitutions se trouvent transformées en de simples arrangements qui sont précisément les deux termes de la substitution cherchée. Cette seule règle fournit toutes les solutions de l'*équation symbolique linéaire*. La multiplicité des solutions provient, non seulement de ce qu'on peut, dans chaque facteur circulaire, faire passer à la première place une quelconque des variables dont ce facteur se compose, mais aussi de ce qu'on peut échanger entre eux les facteurs circulaires de même ordre, et spécialement les facteurs circulaires du premier ordre, c'est-à-dire ceux qui correspondent à des lettres immobiles.

Au lieu de supposer connues les deux substitutions semblables entre elles que renferme une équation linéaire symbolique, on pourrait supposer connue l'une de ces substitutions, et demander la valeur de l'autre correspondante à une solution donnée de l'équation linéaire. Ce dernier problème se résout encore très simplement, mais d'une seule manière. Pour obtenir la valeur unique de la substitution cherchée, il suffit de faire subir aux variables que comprend la substitution proposée les déplacements indiqués par la solution donnée de l'équation linéaire, en opérant comme si ces variables n'étaient pas séparées par des virgules et des parenthèses, et comme si leur système représentait un simple arrangement.

Des principes que je viens d'énoncer, on déduit, comme consé-

quences, diverses propositions qui sont d'une grande utilité dans la recherche du nombre des valeurs qu'une fonction peut acquérir, et l'on arrive en particulier à découvrir les conditions qui doivent être remplies pour que deux substitutions soient permutables entre elles. Ces conditions peuvent être ramenées à deux. La première condition est que les deux substitutions données, réduites à leurs plus simples expressions, soient décomposables en substitutions circulaires ou, du moins, en substitutions régulières, dont les unes soient formées avec des variables que renferme une seule des substitutions données, et dont les autres, prises deux à deux, renferment précisément les mêmes variables. La seconde condition est que les substitutions régulières correspondantes, qui, étant composées des mêmes variables, entrent comme facteurs dans les deux substitutions données, soient de la forme de celles qu'on en obtient, dans le cas où, avec plusieurs systèmes de variables, on construit divers Tableaux qui renferment tous, non seulement un même nombre de lignes horizontales, mais encore un même nombre de lignes verticales, et où, après avoir écrit ces Tableaux à la suite les uns des autres dans un certain ordre, on multiplie entre eux, d'une part, les facteurs circulaires dont l'un quelconque offre la suite des variables qui, dans les divers Tableaux, appartiennent à une ligne horizontale de rang déterminé, d'autre part, les facteurs circulaires dont l'un quelconque offre la suite des variables qui, dans les divers Tableaux, appartiennent à une ligne verticale de rang déterminé. Il en résulte que, si une substitution est circulaire et renferme toutes les variables données, elle ne pourra être permutable qu'avec ses puissances, et par conséquent avec des substitutions régulières qui renfermeront encore toutes les variables.

Il en résulte aussi que, dans le cas où une fonction transitive de n variables n'est pas altérée par une substitution circulaire de l'ordre n, le nombre des substitutions de cet ordre qui jouissent de la même propriété ne peut être inférieur au nombre des valeurs égales de Ω considéré comme fonction de $n-1$ variables.

Il en résulte enfin que, dans le cas où Ω est tout à la fois une fonction transitive de n variables, et une fonction intransitive de $n-1$ variables, et où l'immobilité de deux variables entraîne l'immobilité de toutes les autres, on peut trouver immédiatement, à l'aide des règles précédemment énoncées, plusieurs des substitutions qui jouissent de la propriété de ne point altérer Ω. Souvent même ces règles suffisent pour trouver toutes les substitutions de ce genre, et c'est ce qui arrive en particulier dans le cas où n est un nombre premier.

Je développerai, dans un prochain article, les corollaires importants des divers théorèmes que je viens d'indiquer.

§ I. — *Des diverses formes que peut revêtir une même substitution.*

Soit P l'une des substitutions que l'on peut former avec n variables $x, y, z, \ldots$, et posons

$$N = 1.2.3\ldots n.$$

Si l'on présente cette substitution sous la forme d'un rapport qui ait pour termes deux des arrangements composés avec les variables $x, y, z, \ldots$, on pourra prendre pour dénominateur de ce rapport un quelconque de ces arrangements, et par suite, en laissant toutes les variables en évidence, on pourra présenter la substitution P sous N formes diverses. Ainsi, par exemple, si l'on prend $n = 3$, on aura $N = 6$, et la substitution du second ordre, par laquelle on échangera entre elles les deux variables x, y, pourra être présentée sous l'une quelconque des six formes

$$\binom{yxz}{xyz}, \quad \binom{yzx}{xzy}, \quad \binom{xzy}{yzx}, \quad \binom{xyz}{yxz}, \quad \binom{zyx}{zxy}, \quad \binom{zxy}{zyx}.$$

Le nombre des formes que peut revêtir une même substitution P se trouve notablement diminué lorsqu'on l'exprime à l'aide des facteurs circulaires dont elle est le produit, et que, pour représenter chaque facteur circulaire, on écrit entre deux parenthèses les variables qu'il renferme, en les séparant par des virgules, et plaçant à la suite l'une de l'autre deux variables dont la seconde doit être substituée à la première. Alors le nombre des variables comprises dans chaque facteur circulaire indique précisément l'ordre de ce facteur, et le plus petit nombre qui soit simultanément divisible par les ordres des divers facteurs représente l'ordre i de la substitution P. Alors aussi toute variable qui reste immobile quand on effectue la substitution P, doit être censée comprise dans un facteur circulaire du premier ordre, qui renferme cette seule variable, et, par suite, un tel facteur, représenté par l'une des notations

$$(x), \quad (y), \quad (z), \quad \ldots,$$

est équivalent à l'unité. Les facteurs circulaires du premier ordre disparaîtront toujours si la substitution donnée P est réduite à son expression la plus simple. Mais ils reparaîtront nécessairement si l'on veut mettre en évidence toutes les variables. Il importe de connaître le nombre des formes différentes que peut revêtir, dans cette hypothèse, la substitution P. On y parvient aisément de la manière suivante :

Supposons, pour fixer les idées, que la substitution P, étant de l'ordre i, renferme

f facteurs circulaires de l'ordre a;
g facteurs circulaires de l'ordre b;

etc., et enfin

r facteurs circulaires du premier ordre, en sorte que r exprime le nombre des variables qui restent immobiles quand on effectue la substitution P.

On aura nécessairement

$$af + bg + \ldots + r = n. \tag{1}$$

Supposons encore que, après avoir exprimé la substitution P à l'aide de ses divers facteurs circulaires, représentés chacun par une série de lettres comprises entre deux parenthèses, et séparées par des virgules, on veuille déterminer le nombre ω des formes semblables que l'on peut donner à la substitution sans déplacer les parenthèses, et, par conséquent, sans altérer les nombres de lettres comprises dans les facteurs circulaires qui occupent des rangs déterminés. Tout ce que l'on pourra faire, pour modifier la forme de la substitution P, ce sera, ou de faire passer successivement à la première place, dans chaque facteur circulaire, une quelconque des lettres comprises dans ce facteur, ou d'échanger entre eux les facteurs circulaires de même ordre. Par suite, pour obtenir le nombre ω des formes, semblables entre elles, que peut revêtir la substitution P, il suffira de multiplier le produit

$$a^f b^g \ldots$$

des ordres de tous les facteurs circulaires par le nombre

$$(1.2\ldots f)(1.2\ldots g)\ldots(1.2\ldots r)$$

des arrangements divers que l'on peut former avec ces facteurs, lorsque, sans déplacer les parenthèses qui les renferment, on se borne à échanger entre eux de toutes les manières possibles les facteurs circulaires de même ordre. On aura donc

$$(2) \qquad \omega = (1.2\ldots f)(1.2\ldots g)\ldots(1.2\ldots r)a^f b^g \ldots.$$

Ainsi, par exemple, si l'on prend $n=5$, $a=3$, $f=1$, $r=2$, la formule (2) donnera

$$\omega = (1.2)3 = 6.$$

Effectivement, si l'on met en évidence les cinq variables x, y, z, u, v, dans la substitution

$$(x, y, z)$$

composée avec trois de ces variables, on pourra la présenter sous la forme

$$(x, y, z)(u)(v),$$

et, sans déplacer les parenthèses, on pourra donner à cette même substitution six formes semblables, savoir :

$$(x, y, z)(u)(v), \quad (y, z, x)(u)(v), \quad (z, x, y)(u, v),$$
$$(x, y, z)(v)(u), \quad (y, z, x)(v)(u), \quad (z, x, y)(v, u).$$

§ II. — *Résolution de l'équation linéaire et symbolique par laquelle se trouvent liées l'une à l'autre deux substitutions semblables entre elles.*

Deux substitutions formées avec n lettres

$$x, \ y, \ z, \ \ldots$$

seront *semblables* entre elles, si elles offrent le même nombre de facteurs circulaires, et si les facteurs circulaires de l'une et de l'autre, comparés deux à deux, sont du même ordre. Cela posé, nommons P l'une quelconque des substitutions relatives à n variables

$$x, \ y, \ z, \ \ldots;$$

et soient

$$P, \ P', \ P'', \ \ldots$$

les diverses substitutions semblables à P que l'on peut former avec ces mêmes variables. Supposons d'ailleurs que l'on représente chacune de ces substitutions par le produit de ses divers facteurs circulaires, en mettant toutes les variables en évidence, et en assignant aux parenthèses des places déterminées. Enfin, concevons que l'on donne à chacune des substitutions P, P′, P″, ... toutes les formes qu'elle peut revêtir dans cette hypothèse. Si l'on nomme ϖ le nombre total des substitutions P, P′, P″, ..., et ω le nombre des formes sous lesquelles se présentera chacune d'elles, le produit $\omega\varpi$ exprimera, non seulement le nombre total des formes que revêtiront la substitution P et les substitutions semblables à P, mais encore le nombre N des arrangements divers que l'on peut former avec n variables. Car on devra évidemment retrouver tous ces arrangements, en supprimant les virgules et les parenthèses dans les diverses formes obtenues. On aura donc

$$(1) \qquad \omega\varpi = N,$$

la valeur de N étant

$$N = 1.2\ldots n;$$

et par suite on aura encore

$$(2)\qquad \varpi = \frac{N}{\omega}.$$

Si la substitution P renferme f facteurs circulaires de l'ordre a, g facteurs circulaires de l'ordre b, ..., enfin r facteurs circulaires du premier ordre, on aura, comme on l'a vu dans le § I,

$$(3)\qquad \omega = (1.2\ldots f)(1.2\ldots g)\ldots(1.2\ldots r)a^f b^g\ldots.$$

En substituant cette valeur de ω dans la formule (2), on retrouvera, comme on devait s'y attendre, l'équation (5) de la page 289.

Soit maintenant Q l'une quelconque des substitutions semblables à P, et supposons

$$(4)\qquad P = (\alpha, 6, \gamma, \ldots, \eta)(\lambda, \mu, \nu, \ldots, \rho)\ldots(\varphi)(\chi)(\psi)\ldots,$$

$$(5)\qquad Q = (\alpha', 6', \gamma', \ldots, \eta')(\lambda', \mu', \nu', \ldots, \rho')\ldots(\varphi')(\chi')(\psi')\ldots,$$

α', $6'$, γ', ..., η'; λ', μ', ν', ..., ρ'; ...; φ', χ', ψ', ... désignant les variables qui, dans la substitution Q, ont pris les places qu'occupaient les variables α, 6, γ, ...; η, λ, μ, ν, ..., ρ; ...; φ, χ, ψ, ... dans la substitution P. Représentons par

A et C

les arrangements auxquels se réduisent les seconds membres des formules (4) et (5), quand on y supprime les parenthèses et les virgules placées entre les variables, en sorte qu'on ait

$$(6)\qquad A = \alpha\, 6\, \gamma\ldots\eta\,\lambda\,\mu\,\nu\ldots\rho\ldots\varphi\,\chi\,\psi\ldots,$$

$$(7)\qquad C = \alpha' 6' \gamma'\ldots\eta'\lambda'\mu'\nu'\ldots\rho'\ldots\varphi'\chi'\psi'\ldots.$$

Enfin, soient

$$(8)\qquad B = PA \quad \text{et} \quad D = QC$$

les nouveaux arrangements qu'on obtiendra en appliquant à l'arrangement A la substitution P, et à l'arrangement C la substitution Q. On

trouvera

$$(9)\qquad B = 6\,\gamma\ldots\eta\,\alpha\,\mu\,\nu\ldots\rho\,\lambda\ldots\varphi\,\chi\,\psi\ldots,$$

$$(10)\qquad D = 6'\gamma'\ldots\eta'\alpha'\mu'\nu'\ldots\rho'\lambda'\ldots\varphi'\chi'\psi'\ldots.$$

Par conséquent, les variables qui, prises deux à deux, se correspondront encore dans les arrangements A, C, se correspondront encore dans les arrangements B, D; et cela devait être ainsi, puisque les substitutions semblables P, Q, présentées sous les formes semblables (4) et (5), ont eu précisément pour effet de déplacer de la même manière les variables semblablement placées dans les arrangements A et C. On aura donc

$$(11)\qquad \binom{D}{B} = \binom{C}{A}.$$

Cela posé, faisons, pour abréger,

$$\binom{D}{B} = \binom{C}{A} = R.$$

On aura, par suite,

$$(12)\qquad D = RB, \qquad C = RA;$$

et des équations (12), jointes aux formules (8), on tirera

$$D = RPA, \qquad D = QRA,$$

par conséquent

$$(13)\qquad QRA = RPA$$

et

$$(14)\qquad QR = RP.$$

Réciproquement, si les substitutions P, Q sont liées entre elles par une équation semblable à l'équation (14), alors, en appliquant à un arrangement quelconque A la substitution

$$QR = RP,$$

on retrouvera l'équation (13), et, en posant, pour abréger,

$$P = \binom{B}{A}, \qquad R = \binom{C}{A}, \qquad Q = \binom{D}{C}$$

ou, ce qui revient au même,

$$B = PA, \qquad C = RA, \qquad D = QC,$$

on tirera de l'équation (13)

$$D = RB, \qquad R = \binom{D}{B}.$$

On aura donc alors

$$(15) \qquad R = \binom{C}{A} = \binom{D}{B};$$

et par suite les substitutions

$$P = \binom{B}{A}, \qquad Q = \binom{D}{C}$$

seront semblables l'une à l'autre, puisque, en vertu de la formule (15), elles devront déplacer de la même manière les variables qui se correspondent dans les deux termes de la substitution

$$\binom{C}{A}.$$

Il importe d'observer que les deux membres de la formule (14) sont les produits qu'on obtient en multipliant les deux substitutions semblables P et Q par une nouvelle substitution R dont la première puissance entre, dans l'un des produits, comme multiplicande, et dans l'autre produit, comme multiplicateur. Pour obtenir cette nouvelle substitution R, il suffit d'exprimer la substitution P à l'aide de ses facteurs circulaires, en mettant toutes les variables en évidence, et d'écrire au-dessus de P la substitution Q, présentée sous une forme semblable à celle de P, puis de transformer les deux substitutions Q, P en deux arrangements C, A par la suppression des parenthèses et des virgules placées entre les variables. Ces deux arrangements C, A

seront les deux termes d'une substitution R qui vérifiera la formule (14). Il y a plus : d'après ce qui a été dit ci-dessus, toute valeur de R propre à vérifier cette formule sera évidemment fournie par la comparaison des deux substitutions semblables P, Q, superposées l'une à l'autre, ainsi qu'on vient de l'expliquer. D'ailleurs, comme, en laissant P sous la même forme, on pourra donner successivement à Q diverses formes semblables à celle de P, et semblables entre elles, dont le nombre sera précisément celui que nous avons représenté par ω, il en résulte que la substitution R admet un nombre ω de valeurs distinctes. Donc, si l'on résout par rapport à R la formule (14), c'est-à-dire l'*équation symbolique et linéaire* à laquelle doit satisfaire la substitution R, on obtiendra un nombre ω de solutions diverses correspondantes aux diverses formes de la substitution Q.

Si, en supposant connues, non plus les substitutions semblables P, Q, mais l'une d'elles, P par exemple, et la substitution R, on demandait la valeur de Q déterminée par l'équation (14), ou, ce qui revient au même, par la suivante

$$(16) \qquad Q = RPR^{-1},$$

on remarquerait que, pour passer de la valeur de P, donnée par la formule (4), à la valeur de Q, donnée par la formule (5), il suffit de faire subir aux variables $x, y, z, \ldots$ les déplacements par lesquels on passe de la valeur de A, donnée par la formule (6), à la valeur de C, donnée par la formule (7), c'est-à-dire les déplacements qui sont indiqués par la substitution R. En opérant ainsi, on obtiendrait la seule valeur de Q qui vérifie la formule (16).

Nous savons donc maintenant résoudre les deux problèmes suivants :

PROBLÈME I. — *Étant données n variables $x, y, z, \ldots$, et deux substitutions semblables* P, Q, *formées avec ces variables, trouver une troisième substitution* R *qui soit propre à résoudre l'équation linéaire*

$$QR = RP.$$

Solution. — Exprimez la substitution P à l'aide de ses facteurs circulaires, en mettant toutes les variables en évidence, puis écrivez au-dessus de la substitution P la substitution Q, présentée sous une forme semblable à celle de P. Supprimez ensuite les parenthèses et les virgules placées entre les variables. Les deux substitutions Q, P seront ainsi transformées en deux arrangements qui seront propres à représenter les deux termes de la substitution R.

Corollaire. — Les substitutions P, Q peuvent ne renfermer qu'une partie des variables $x, y, z, \ldots$; mais, pour obtenir toutes les solutions de l'équation

$$QR = RP,$$

on devra, comme nous l'avons dit, mettre toutes les variables en évidence, même celles qui ne seraient renfermées dans aucune des deux substitutions P, Q, si ces substitutions étaient réduites à leur plus simple expression. Il en résulte que, les substitutions P, Q restant les mêmes, le nombre des solutions de l'équation symbolique linéaire

$$QR = RP$$

croîtra en même temps que le nombre des variables $x, y, z, \ldots$.

Pour éclaircir ce qu'on vient de dire, supposons que les substitutions P, Q, réduites à leur plus simple expression, soient deux substitutions circulaires du second ordre, et que l'on ait

$$P = (x, y), \qquad Q = (x, z).$$

Si les variables $x, y, z, \ldots$ se réduisent à trois, alors, P étant présenté sous la forme

$$(x, y)(z),$$

Q pourra être présenté sous l'une des formes semblables

$$(x, z)(y), \quad (z, x)(y),$$

et par suite la valeur de R devra se réduire à l'une des substitutions

$$\binom{xzy}{xyz}, \quad \binom{zxy}{xyz}$$

ou, ce qui revient au même, à l'une des substitutions

$$(y, z), \quad (x, z, y).$$

Si, au contraire, l'on considère quatre variables x, y, z, u, alors, P étant présenté sous la forme

$$(x, y)(z)(u),$$

Q pourra être présenté sous l'une quelconque des formes semblables

$$(x, z)(y)(u), \quad (z, x)(y)(u), \quad (x, z)(u)(y), \quad (z, x)(u)(y),$$

et par suite R pourra être l'une quelconque des quatre substitutions

$$\binom{xzyu}{xyzu}, \quad \binom{zxyu}{xyzu}, \quad \binom{xzuy}{xyzu}, \quad \binom{zxuy}{xyzu}$$

ou, ce qui revient au même, l'une quelconque des quatre substitutions

$$(y, z), \quad (x, z, y), \quad (y, z, u), \quad (x, z, u, y).$$

Problème II. — *Étant données n variables $x, y, z, \ldots$, et deux substitutions semblables* P, Q, *formées avec ces variables, trouver la substitution* Q *semblable à* P, *et déterminée par la formule*

$$Q = RPR^{-1}.$$

Solution. — Exprimez la substitution P à l'aide de ses facteurs circulaires, puis effectuez dans P les déplacements de variables indiqués par la substitution R, en opérant comme si P représentait un simple arrangement.

Corollaire. — Pour résoudre ce second problème, il n'est pas nécessaire de mettre toutes les variables en évidence, comme on doit le faire généralement quand il s'agit d'obtenir toutes les solutions du premier, et l'on peut se servir de substitutions réduites à leurs plus simples expressions. Si, pour fixer les idées, on prend

$$P = (x, y), \qquad R = (x, z, y),$$

alors, en appliquant la règle ci-dessus établie, on trouvera, quel que soit d'ailleurs le nombre des variables données,

$$\mathrm{RPR}^{-1}=(z,x),\qquad \mathrm{PRP}^{-1}=(y,z,x).$$

Si l'on supposait, au contraire,

$$\mathrm{P}=(x,y),\qquad \mathrm{R}=(x,z)(y,u),$$

on trouverait

$$\mathrm{RPR}^{-1}=(z,u),\qquad \mathrm{PRP}^{-1}=(y,z)(x,u).$$

312.

Analyse mathématique. — *Mémoire sur les substitutions permutables entre elles.*

C. R., T. XXI, p. 1188 (1er décembre 1845).

Soient P, U deux substitutions formées avec les n variables x, y, z, ... Soient, de plus, ω le nombre des formes diverses et semblables entre elles que l'on peut donner à la substitution P, en l'exprimant à l'aide de ses facteurs circulaires, et mettant toutes les variables en évidence. Les substitutions P, U seront *permutables* entre elles, si elles vérifient la formule

$$\mathrm{UP}=\mathrm{PU}. \tag{1}$$

Donc alors U sera nécessairement l'une des solutions de la formule (1). Mais il pourra se confondre avec l'une quelconque de ces solutions, dont le nombre est précisément ω. Ajoutons que, en vertu des principes établis dans le précédent Mémoire, on devra, pour obtenir U, écrire au-dessus de la substitution P la même substitution sous une seconde forme semblable à la première, puis réduire les deux formes de la substitution P à de simples arrangements, en supprimant les parenthèses et les virgules placées entre les variables, et prendre ces

arrangements pour les deux termes de la substitution cherchée. Comme, en passant de la première forme de P à la seconde, on peut échanger entre eux arbitrairement les facteurs circulaires du premier ordre, formés avec les variables immobiles qui disparaissent quand on réduit la valeur de P à sa plus simple expression, il en résulte que, dans la substitution cherchée U, ces variables peuvent composer des facteurs circulaires quelconques. Donc, pour obtenir les diverses valeurs de U, il suffira de multiplier les diverses substitutions formées avec les variables immobiles de P par les diverses valeurs de U qu'on obtiendrait en laissant de côté ces mêmes variables, et en supposant la valeur de P réduite à sa plus simple expression.

Ainsi la question peut toujours être ramenée au cas où les variables données seraient toutes comprises dans la substitution P, sans qu'il fût nécessaire de les mettre en évidence.

Plaçons-nous maintenant dans cette dernière hypothèse, et, pour bien voir ce qui arrivera, examinons encore les différents cas qui peuvent s'offrir à nous, en commençant par ceux qui sont les plus simples.

Si d'abord la substitution P se réduit à un seul facteur circulaire, en écrivant, dans ce facteur, à la suite de chaque variable celle qui devra lui être substituée, il n'y aura plus d'arbitraire que le choix de la variable placée en tête du facteur dont il s'agit, et les deux arrangements auxquels on réduira la première et la seconde forme de P représenteront les deux termes d'une nouvelle substitution qui sera une puissance de P. Donc, la substitution U se confondra nécessairement avec l'une de ces puissances. Si la seconde forme de P n'était pas distincte de la première, la puissance de P qui représenterait la substitution U se réduirait évidemment à l'unité.

Supposons, en second lieu, que P soit une substitution régulière équivalente au produit de f facteurs circulaires de l'ordre a. Si l'un de ces facteurs ne change pas de place, quand on passe de la première forme de P à la seconde, il se trouvera remplacé par une de ses puissances dans la substitution U. Mais il en sera autrement si plusieurs facteurs circulaires de P, dont chacun soit de l'ordre a, sont échangés entre eux. Nommons

$$\mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots$$

ces facteurs circulaires dont nous représenterons le nombre par i, et supposons qu'ils soient échangés entre eux dans l'ordre indiqué par la substitution circulaire

$$(\mathfrak{P}, \mathfrak{Q}, \mathfrak{R}, \ldots).$$

Concevons d'ailleurs que, après avoir réduit les deux formes de P à deux arrangements, on écrive à la suite l'une de l'autre les variables qui se correspondent mutuellement dans les facteurs circulaires de U, dont quelques-uns,

$$\mathfrak{u},\ \mathfrak{v},\ \mathfrak{w},\ \ldots$$

seront formés avec les variables qui entraient dans la composition des facteurs

$$\mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots$$

de la substitution P. Nommons j le nombre des facteurs circulaires

$$\mathfrak{u},\ \mathfrak{v},\ \mathfrak{w},\ \ldots.$$

Soit, de plus, b le nombre des variables comprises dans $\mathfrak{u}$, et représentons par

$$\alpha,\ 6,\ \gamma,\ \ldots,\ \lambda,\ \mu,\ \nu,\ \ldots,\ \varphi,\ \chi,\ \psi,\ \ldots$$

ces mêmes variables, en sorte qu'on ait

$$\mathfrak{u} = (\alpha, 6, \gamma, \ldots, \lambda, \mu, \nu, \ldots, \varphi, \chi, \psi, \ldots). \tag{2}$$

La suite des variables

$$\alpha,\ 6,\ \gamma,\ \ldots,\ \lambda,\ \mu,\ \nu,\ \ldots,\ \varphi,\ \chi,\ \psi,\ \ldots \tag{3}$$

pourra être évidemment décomposée en plusieurs autres suites

$$\left\{\begin{array}{llll} \alpha, & 6, & \gamma, & \ldots, \\ \lambda, & \mu, & \nu, & \ldots, \\ \varphi, & \chi, & \psi, & \ldots, \\ ., & ., & .., & \ldots, \end{array}\right. \tag{4}$$

formées chacune avec des variables qui se succéderont dans l'ordre indiqué par la substitution

$$(\mathfrak{P}, \mathfrak{Q}, \mathfrak{R}, \ldots).$$

en sorte que, dans chacune des suites horizontales du Tableau (4), le premier terme représente une variable tirée du facteur $\mathfrak{P}$, le second terme une variable tirée du facteur $\mathfrak{Q}$, le troisième terme une variable tirée du facteur $\mathfrak{R}$, etc. Cela posé, si l'on nomme θ le nombre des suites horizontales que renferme le Tableau (4), le nombre total b des termes de ce Tableau sera le produit du nombre θ par le nombre i des facteurs circulaires

$$\mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots.$$

On aura donc

$$b = \theta i, \tag{5}$$

et par conséquent l'ordre b de la substitution $\mathfrak{u}$ sera un multiple de i.

Soient maintenant

$$\alpha',\ 6',\ \gamma',\ \ldots,\quad \lambda',\ \mu',\ \nu',\ \ldots,\quad \varphi',\ \chi',\ \psi',\ \ldots \tag{6}$$

les variables qui, dans les facteurs circulaires

$$\mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots,$$

ou plutôt dans les cercles indicateurs correspondants, suivent immédiatement les variables

$$\alpha,\ 6,\ \gamma,\ \ldots,\quad \lambda,\ \mu,\ \nu,\ \ldots,\quad \varphi,\ \chi,\ \psi,\ \ldots.$$

Soient pareillement

$$\alpha'',\ 6'',\ \gamma'',\ \ldots,\quad \lambda'',\ \mu'',\ \nu'',\ \ldots,\quad \varphi'',\ \chi'',\ \psi'',\ \ldots \tag{7}$$

les variables qui, dans les mêmes cercles indicateurs, suivent immédiatement les variables

$$\alpha',\ 6',\ \gamma',\ \ldots,\quad \lambda',\ \mu',\ \nu',\ \ldots,\quad \varphi',\ \chi',\ \psi',\ \ldots,$$

etc. Chacune des suites (6), (7), ... se composera de termes propres à représenter les diverses variables qui succéderont les unes aux autres dans un des facteurs circulaires

$$\mathfrak{V},\quad \mathfrak{W},\quad \ldots.$$

On pourra donc supposer

$$(8)\qquad \begin{cases} \mathfrak{V}=(\alpha', \beta', \gamma', \ldots, \lambda', \mu', \nu', \ldots, \varphi', \chi', \psi', \ldots), \\ \mathfrak{W}=(\alpha'', \beta'', \gamma'', \ldots, \lambda'', \mu'', \nu'', \ldots, \varphi'', \chi'', \psi'', \ldots), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

D'autre part, les variables qui succéderont les unes aux autres dans le facteur $\mathfrak{P}$ seront évidemment

$$\alpha,\ \alpha',\ \alpha'',\ \ldots,\quad \lambda,\ \lambda',\ \lambda'',\ \ldots,\quad \varphi,\ \varphi',\ \varphi'',\ \ldots.$$

On pourra donc supposer encore

$$(9)\qquad \mathfrak{P}=(\alpha, \alpha', \alpha'', \ldots, \beta, \beta', \beta'', \ldots, \varphi, \varphi', \varphi'', \ldots),$$

et l'on trouvera de même

$$(10)\qquad \begin{cases} \mathfrak{Q}=(\beta, \beta', \beta'', \ldots, \mu, \mu', \mu'', \ldots, \chi, \chi', \chi'', \ldots), \\ \mathfrak{R}=(\gamma, \gamma', \gamma'', \ldots, \nu, \nu', \nu'', \ldots, \psi, \psi', \psi'', \ldots), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Donc les variables

$$(11)\qquad \begin{cases} \alpha, & \beta, & \gamma, & \ldots, & \lambda, & \mu, & \nu, & \ldots, & \varphi, & \chi, & \psi, & \ldots, \\ \alpha', & \beta', & \gamma', & \ldots, & \lambda', & \mu', & \nu', & \ldots, & \varphi', & \chi', & \psi', & \ldots, \\ \alpha'', & \beta'', & \gamma'', & \ldots, & \lambda'', & \mu'', & \nu'', & \ldots, & \varphi'', & \chi'', & \psi'', & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots \end{cases}$$

c'est-à-dire celles qui se trouvent renfermées, d'une part, dans les facteurs circulaires

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots$$

de la substitution P, d'autre part, dans les facteurs circulaires

$$\mathfrak{U},\quad \mathfrak{V},\quad \mathfrak{W},\quad \ldots$$

de la substitution U, entreront dans la composition de ces facteurs

suivant le mode indiqué par les équations (2), (8), (9) et (10). Si l'on nomme l le nombre total de ces variables, on aura évidemment

$$(12)\qquad l=ai=bj,$$

puisque a représentera le nombre des variables comprises dans chacun de i facteurs circulaires $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{R}$, ..., et b le nombre des variables comprises dans chacun des j facteurs circulaires $\mathfrak{U}$, $\mathfrak{V}$, $\mathfrak{W}$, ... D'ailleurs, on tirera de l'équation (12)

$$(13)\qquad \frac{a}{j}=\frac{b}{i},$$

et, de cette dernière, combinée avec la formule (5), on conclura

$$(14)\qquad a=\theta j.$$

Donc, non seulement l'ordre b de chacun des facteurs $\mathfrak{U}$, $\mathfrak{V}$, $\mathfrak{W}$, ... sera un multiple du nombre i des facteurs $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{R}$, ..., mais, réciproquement, l'ordre a de chacun des facteurs $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{R}$, ... sera un multiple du nombre j des facteurs $\mathfrak{U}$, $\mathfrak{V}$, $\mathfrak{W}$, ... Au reste, il serait facile d'établir directement l'équation (14), puisque les variables comprises dans $\mathfrak{P}$ se confondent avec les divers termes du Tableau

$$(15)\qquad \begin{cases} \alpha, & \alpha', & \alpha'', & \ldots, \\ \lambda, & \lambda', & \lambda'', & \ldots, \\ \varphi, & \varphi', & \varphi'', & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, \end{cases}$$

qui renferme un nombre θ de lignes horizontales, et un nombre j de lignes verticales.

Concevons maintenant que le produit des facteurs circulaires qui renferment les variables comprises dans le Tableau (11) soit désigné par $\mathfrak{s}$ dans la substitution P, et par $\mathfrak{E}$ dans la substitution U. Alors, en vertu des deux équations

$$(16)\qquad \mathfrak{s}=\mathfrak{P}\mathfrak{Q}\mathfrak{R}\ldots,\qquad \mathfrak{E}=\mathfrak{U}\mathfrak{V}\mathfrak{W}\ldots,$$

$\mathfrak{s}$ et $\mathfrak{E}$ seront deux substitutions régulières, la première de l'ordre

$a = \theta j$, la seconde de l'ordre $b = \theta i$. D'ailleurs, le Tableau (11) pourra être évidemment décomposé en plusieurs autres

$$(17)\qquad \left\{\begin{array}{llll} \alpha, & \beta, & \gamma, & \ldots, \\ \alpha', & \beta', & \gamma', & \ldots, \\ \alpha'', & \beta'', & \gamma'', & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, \end{array}\right.$$

$$(18)\qquad \left\{\begin{array}{llll} \lambda, & \mu, & \nu, & \ldots, \\ \lambda', & \mu', & \nu', & \ldots, \\ \lambda'', & \mu'', & \nu'', & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, \end{array}\right.$$

$$(19)\qquad \left\{\begin{array}{llll} \varphi, & \chi, & \psi, & \ldots, \\ \varphi', & \chi', & \psi', & \ldots, \\ \varphi'', & \chi'', & \psi'', & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, \end{array}\right.$$

$$\ldots,\quad \ldots,\quad \ldots,\quad \ldots,$$

dont le nombre sera θ, et dont chacun renfermera, non seulement i lignes verticales, mais encore j lignes horizontales. Enfin, on conclura des formules (9) et (10) que, pour obtenir l'un quelconque des facteurs circulaires

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots$$

de la substitution s, il suffit d'écrire à la suite les unes des autres, en les plaçant entre deux parenthèses et les séparant par des virgules, les variables qui appartiennent, dans les Tableaux (17), (18), (19), ..., à une ligne verticale de rang déterminé. On conclura, au contraire, des formules (2) et (8), que, pour obtenir l'un quelconque des facteurs circulaires

$$\mathfrak{U},\quad \mathfrak{V},\quad \mathfrak{W},\quad \ldots$$

de la substitution ε, il suffit d'écrire, à la suite les unes des autres, en les plaçant entre deux parenthèses et les séparant par des virgules, les variables qui appartiennent, dans les Tableaux (17), (18), (19), ..., à une ligne horizontale de rang déterminé.

Les observations que nous venons de faire relativement aux variables comprises dans le Tableau (11) s'appliquent évidemment à tout système de variables comprises dans des facteurs circulaires de P, qui se trouvent échangés entre eux quand on passe de la première forme de P à la seconde. De telles variables sont toujours du nombre de celles qui se montrent à la fois, sans qu'il soit nécessaire de les mettre en évidence, dans les deux substitutions P, U, supposées permutables entre elles; et, parmi les facteurs circulaires de ces deux substitutions, ceux qui renferment de telles variables donnent toujours pour produits respectifs deux substitutions régulières s, ε qui peuvent être formées, à l'aide de divers Tableaux analogues aux Tableaux (17), (18), (19), ..., suivant le mode que nous avons indiqué.

D'ailleurs, d'après ce qu'on a vu précédemment, si, des deux substitutions P, U, supposées permutables entre elles et réduites à leurs plus simples expressions, l'une renferme des variables qui ne soient pas comprises dans l'autre, ces variables pourront y être groupées arbitrairement de manière à composer des facteurs circulaires quelconques. En conséquence, on peut énoncer la proposition suivante :

Théorème I. — *Soient* P, U *deux substitutions formées avec n variables $x, y, z, \ldots$, et supposons ces deux substitutions réduites à leurs expressions les plus simples. Si elles sont permutables entre elles, leurs facteurs circulaires, dans le cas le plus général, seront de deux espèces. Les uns renfermeront les variables comprises dans une seule des deux substitutions* P, U, *et pourront être des facteurs quelconques. Quant aux facteurs circulaires qui renfermeront les variables communes aux deux substitutions, non seulement ils pourront être groupés entre eux de manière à offrir pour produits des substitutions régulières qui, prises deux à deux, représenteront des facteurs complexes et correspondants de* P *et de* U, *formés avec les mêmes variables, mais, de plus, les substitutions régulières qui représenteront les facteurs complexes et correspondants de* P *et de* U *pourront être réduites à la forme de celles qu'on obtient dans le cas où, avec plusieurs systèmes de variables, on construit divers Tableaux, qui renferment tous* *un même nombre de termes compris dans un même nombre de lignes horizontales et verticales, et où, après avoir placé ces Tableaux, à la suite les uns des autres, dans un certain ordre, on multiplie entre eux, d'une part, les facteurs circulaires dont l'un quelconque offre la série des variables qui, dans les divers Tableaux, appartiennent à une ligne horizontale de rang déterminé; d'autre part, les facteurs circulaires dont l'un quelconque offre la série des variables qui, dans les divers Tableaux, appartiennent à une ligne verticale de rang déterminé. Ajoutons que, réciproquement, si les diverses conditions que nous venons d'énoncer sont remplies, les deux substitutions* P, U *seront permutables entre elles.*

Corollaire I. — Pour éclaircir ce qu'on vient de dire par un exemple, supposons que, avec les variables

$$x,\quad y,\quad z,\quad u,\quad v,\quad w,\quad s,\quad t,$$

on construise les deux Tableaux

$$\begin{matrix} x, & y, \\ z, & u \end{matrix}$$

et

$$\begin{matrix} v, & w, \\ s, & t. \end{matrix}$$

Les facteurs circulaires du quatrième ordre, dont chacun renfermera les quatre variables comprises dans les premières ou dans les secondes lignes verticales des deux Tableaux, seront

$$(x, z, v, s) \quad \text{et} \quad (y, u, w, t).$$

Au contraire, les facteurs circulaires du quatrième ordre, dont chacun renfermera les quatre variables comprises dans les premières ou dans les secondes lignes horizontales des deux Tableaux, seront

$$(x, y, v, w) \quad \text{et} \quad (z, u, s, t).$$

Cela posé, il résulte du théorème I que, si l'on prend

$$\mathrm{P} = (x, z, v, s)(y, u, w, t)$$

et

$$\mathrm{U} = (x, y, v, w)(z, u, s, t),$$

P, Q seront deux substitutions permutables entre elles. Pour s'assurer qu'effectivement ces substitutions vérifient la formule

$$\mathrm{PU} = \mathrm{UP},$$

ou, ce qui revient au même, la suivante

$$\mathrm{P} = \mathrm{UPU}^{-1},$$

il suffit d'observer que, si l'on pose

$$\mathrm{A} = xzvsyuwt,$$

on trouvera

$$\mathrm{UA} = yuwtvsxz.$$

Donc, par suite, en vertu de l'une des règles établies dans le précédent article, on aura

$$\mathrm{UPU}^{-1} = (y, u, w, t)(v, s, x, z) = \mathrm{P}.$$

Corollaire II. — Si les divers Tableaux formés avec les l variables que renferment deux facteurs complexes et correspondants s, ϖ des substitutions P, U se réduisent à un seul Tableau, alors s, ϖ seront deux substitutions régulières du genre de celles dont nous nous sommes déjà occupés dans un précédent article (séance du 13 octobre), et dont les propriétés deviennent évidentes quand on représente les variables qu'elles renferment à l'aide de deux espèces d'indices appliqués à une seule lettre. C'est ce qui arrivera, par exemple, si l'on a

$$s = (x, u)(y, v)(z, w),$$
$$\varpi = (x, z, v)(y, u, w).$$

Alors les deux substitutions s, ϖ seront les produits des divers facteurs circulaires formés, d'une part, avec les variables que renferment les diverses lignes horizontales du Tableau

$$\begin{matrix} x, & z, & v, \\ u, & w, & y; \end{matrix}$$

d'autre part, avec les variables comprises dans les diverses lignes horizontales; et ces deux substitutions seront certainement permutables entre elles, car elles se réduiront au cube et au carré de la substitution du sixième ordre

$$(x, y, z, u, v, w).$$

Il est bon d'observer que, en vertu des équations (16), jointes aux formules (2), (8), (9) et (10), on aura généralement

$$\mathfrak{s}^j = \mathfrak{t}^i, \tag{20}$$

et que, si l'on pose en conséquence

$$\Theta = \mathfrak{s}^j = \mathfrak{t}^i, \tag{21}$$

Θ sera une substitution régulière de l'ordre

$$\theta = \frac{b}{i} = \frac{a}{j} = \frac{l}{ij}. \tag{22}$$

D'ailleurs, dans les formules (20), (21), l'exposant i de $\mathfrak{t}$ représentera le nombre des facteurs circulaires de $\mathfrak{s}$, et réciproquement l'exposant j de $\mathfrak{s}$ représentera le nombre des facteurs circulaires de $\mathfrak{t}$. Cela posé, on pourra énoncer encore la proposition suivante :

Théorème II. — *Lorsque deux substitutions* P, U *sont permutables entre elles, les facteurs circulaires qui renferment les lettres communes aux deux substitutions, supposées réduites à leurs expressions les plus simples, fournissent deux produits décomposables en substitutions régulières qui, comparées deux à deux, se correspondent de telle sorte que deux substitutions régulières* $\mathfrak{s}$ *et* $\mathfrak{t}$, *propres à représenter deux facteurs complexes et correspondants des substitutions données* P *et* U, *vérifient toujours la formule*

$$\mathfrak{s}^j = \mathfrak{t}^i,$$

i étant le nombre des facteurs circulaires de $\mathfrak{s}$, *et j le nombre des facteurs circulaires de* $\mathfrak{t}$. *Ajoutons que, si l'on désigne par l le nombre des variables comprises dans chacune des substitutions régulières* $\mathfrak{s}$, $\mathfrak{t}$, *la substitution*

$$\mathfrak{s}^j = \mathfrak{t}^i$$

sera une autre substitution régulière de l'ordre $\frac{l}{ij}$.

Corollaire I. — Si les facteurs complexes $\mathfrak{s}$ et $\mathfrak{t}$ composent à eux seuls les substitutions P et U, on aura

$$P = \mathfrak{s}, \qquad U = \mathfrak{t}, \tag{23}$$

et la formule (20) donnera

$$P^j = U^i, \tag{24}$$

i désignant le nombre des facteurs circulaires de P, et j le nombre des facteurs circulaires de U. Si, pour fixer les idées, on pose, comme dans le corollaire I du théorème I,

$$P = (x, z, v, s)(y, u, w, t),$$
$$U = (x, y, v, w)(z, u, s, t),$$

on aura

$$i = j = 2,$$

et par suite l'équation (24) donnera

$$P^2 = U^2.$$

Effectivement, en formant, dans cette hypothèse, le carré de chacune des substitutions P, U, on trouvera

$$P^2 = U^2 = (x, v)(z, s)(y, w)(u, t).$$

Corollaire II. — Si, parmi les facteurs circulaires de P, se trouve une seule substitution circulaire de l'ordre a, formée avec des variables que renferme aussi U, réduit à son expression la plus simple, cette substitution circulaire devra évidemment représenter une des valeurs de $\mathfrak{s}$. En la prenant effectivement pour $\mathfrak{s}$, on aura

$$i = 1,$$

et la formule (20) donnera

$$\mathfrak{t} = \mathfrak{s}^j.$$

Donc alors le facteur $\mathfrak{t}$ de U, correspondant au facteur $\mathfrak{s}$ de P, sera une puissance de la substitution circulaire de $\mathfrak{s}$. Cette conclusion s'accorde avec les remarques faites au commencement de cet article, puisque, dans le cas où $\mathfrak{s}$ représente, non seulement un des facteurs circulaires P, mais encore le seul de ces facteurs qui soit de l'ordre a, s ne peut être déplacé quand on passe d'une forme de P à une autre, de manière à ne jamais altérer les nombres de lettres comprises dans les facteurs qui occupent des places déterminées.

313.

Analyse mathématique. — *Note sur la réduction des fonctions transitives aux fonctions intransitives, et sur quelques propriétés remarquables des substitutions qui n'altèrent pas la valeur d'une fonction transitive.*

C. R., T. XXI, p. 1199 (1er décembre 1845).

Comme je l'ai remarqué dans une précédente séance, le nombre des valeurs distinctes d'une fonction transitive de plusieurs variables est aussi le nombre des valeurs distinctes qu'admet cette fonction dans le cas où l'une des variables devient immobile. Il peut d'ailleurs arriver qu'une fonction transitive de plusieurs variables ne cesse pas d'être transitive dans le cas où une, deux, trois, quatre, ... variables deviennent immobiles; et alors le nombre des valeurs distinctes de la fonction donnée se confond avec le nombre des valeurs distinctes d'une autre fonction qui renferme une, deux, trois, quatre, ... variables de moins. J'ajoute que cette autre fonction peut toujours être supposée intransitive. Car, si l'on fait croître de plus en plus le nombre des variables devenues immobiles, ce nombre ne s'élèvera jamais au delà d'une certaine limite, égale ou supérieure à celle qu'il peut atteindre quand la fonction donnée est symétrique, savoir, au nombre total des variables diminué de l'unité.

Mais ce qu'il importe surtout de remarquer, c'est que la fonction intransitive à laquelle on réduira une fonction transitive donnée, en supposant une ou plusieurs variables immobiles, ne saurait être une fonction intransitive quelconque. Tout au contraire, le nombre des formes que peut acquérir cette fonction intransitive est notablement restreint par un théorème que je suis parvenu à établir. Je prouve que toute fonction transitive de n variables, qui devient intransitive quand on suppose une variable immobile, est nécessairement ou une fonction transitive complexe de toutes les variables, ou une fonction pour laquelle le nombre des valeurs égales se trouve réduit, par l'immobilité d'une variable, au nombre des valeurs égales d'une autre fonction de l lettres, l étant inférieur à $n-1$ et diviseur de $n-1$. Ajoutons que de ces deux hypothèses une seule évidemment pourra être admise, si n ou $n-1$ est un nombre premier. Ainsi, par exemple, en vertu du théorème que je viens d'énoncer, le nombre des valeurs égales de toute fonction transitive de cinq variables qui sera intransitive par rapport à quatre devra se réduire au produit du facteur 5 par le nombre des valeurs égales d'une fonction de deux variables. Donc, toute fonction transitive de cinq variables qui sera intransitive par rapport à quatre offrira cinq ou dix valeurs égales, et, par suite, vingt-quatre ou douze valeurs distinctes. Au contraire, toute fonction de six variables, qui sera intransitive par rapport à cinq ne pourra être qu'une fonction transitive complexe.

Le théorème énoncé, joint à ceux que nous avons déjà établis dans les séances précédentes, sert encore à limiter le nombre des valeurs égales ou distinctes que peut acquérir une fonction transitive qui ne cesse pas de l'être, quand une ou plusieurs variables deviennent immobiles. On reconnaît ainsi, par exemple, que toute fonction de cinq lettres qui est transitive par rapport à cinq et à quatre variables offre nécessairement six valeurs distinctes, quand elle en a plus de deux, et qu'on peut en dire autant de toute fonction de six lettres qui est transitive par rapport à six, à cinq et à quatre variables.

Ajoutons que très souvent, à l'aide des formules auxquelles je suis parvenu, on peut déterminer le nombre et même la nature particulière des substitutions des divers ordres qui n'altèrent pas une fonction transitive de n variables, en supposant connu le nombre des variables dont l'immobilité réduit cette fonction transitive à une fonction intransitive et le nombre des valeurs distinctes que la fonction peut acquérir.

En finissant, j'observerai que M. Hermite m'a dit avoir depuis longtemps reconnu la fonction transitive de six variables dont j'ai parlé, savoir, de celle qui offre seulement six valeurs distinctes. Toutefois, la méthode par laquelle il était parvenu à constater l'existence de cette fonction est différente de celle que j'ai suivie moi-même, et qui, en raison de son utilité dans la solution de plusieurs problèmes, paraît assez digne d'intérêt pour que je croie devoir l'exposer dans un autre article.

314.

Analyse mathématique. — *Note sur les substitutions qui n'altèrent pas la valeur d'une fonction, et sur la forme régulière que prennent toujours celles d'entre elles qui renferment un moindre nombre de variables.*

C. R., T. XXI, p. 1234 (8 décembre 1845).

Considérons n variables indépendantes $x, y, z, \ldots$, et nommons P une substitution formée avec plusieurs de ces variables, en nombre égal à l. Si la substitution P n'est pas régulière, elle sera du moins le produit de plusieurs substitutions régulières

$$U, \quad V, \quad W, \quad \ldots.$$

Désignons par

$$a, \quad b, \quad c, \quad \ldots$$

les ordres de ces substitutions régulières, et supposons que

U soit le produit de f facteurs circulaires de l'ordre a;
V le produit de g facteurs circulaires de l'ordre b;
W le produit de h facteurs circulaires de l'ordre c;
....

Les nombres $a, b, c, \ldots$ seront tous inégaux entre eux, et l'on aura, non seulement

$$P = UVW\ldots, \tag{1}$$

mais encore

$$fa + gb + hc + \ldots = l. \tag{2}$$

Ajoutons que, si l'on nomme i l'ordre de la substitution P, i sera le plus petit nombre entier, divisible par chacun des nombres a, b, c, ...

Observons maintenant que les nombres

$$a, \quad b, \quad c, \quad \ldots,$$

étant tous inégaux, ne pourront tous offrir les mêmes facteurs premiers, élevés aux mêmes puissances. Donc, parmi les facteurs premiers de i, on pourra trouver un nombre premier p, qui sera tel que les termes de la suite

$$a, \quad b, \quad c, \quad \ldots,$$

ou ne seront pas tous divisibles par p, ou, du moins, ne seront pas tous divisibles par la même puissance de p. Alors

$$P^{\frac{i}{p}}$$

sera évidemment une substitution régulière de l'ordre p; et cette substitution $P^{\frac{i}{p}}$, réduite à son expression la plus simple, cessera de renfermer les variables comprises dans quelques-unes des substitutions régulières

$$U, \quad V, \quad W, \quad \ldots,$$

savoir, dans celles de ces substitutions dont les ordres n'étaient pas multiples de la plus haute puissance de p qui divise i. D'ailleurs, chacune des substitutions U, V, W, ... déplacera deux variables au moins, si l'ordre i de la substitution P est un nombre pair, et trois variables au moins si l'ordre i est un nombre impair. Donc le nombre des variables que déplacera la substitution $P^{\frac{i}{p}}$ sera égal ou inférieur à $l-2$, si la substitution P est d'ordre pair, et à $l-3$ si la substitution P est d'ordre impair. Ajoutons qu'on pourra encore supposer ce nombre égal ou inférieur à $l-3$, si, l'ordre i étant pair, l'un des entiers

$$a, \quad b, \quad c, \quad \ldots,$$

a par exemple, est impair. Car, dans ce cas, on pourra prendre $p=2$, et alors

$$\mathrm{P}^{\frac{i}{p}}$$

sera une substitution régulière du second ordre qui déplacera au plus $l-3$ variables, puisqu'elle cessera de comprendre les a variables renfermées dans la substitution U. Enfin, il suit de la formule (2) que l'un des entiers

$$a, \quad b, \quad c, \quad \ldots$$

sera certainement impair, si l, ou le nombre des variables comprises dans P, est un nombre impair. Par conséquent, on pourra énoncer la proposition suivante :

Théorème I. — *Soit* P *une substitution de l'ordre i, qui déplace l variables, et supposons cette substitution irrégulière. Alors, parmi les puissances de* P, *distinctes de l'unité, on trouvera une ou plusieurs substitutions régulières, dont chacune déplacera* $l-2$ *variables au plus, si l et i sont des nombres pairs, et* $l-3$ *variables au plus, si l ou i est impair.*

Soit maintenant Ω une fonction des n variables indépendantes x, y, z, ..., et nommons

$$1, \quad \mathrm{P}, \quad \mathrm{Q}, \quad \mathrm{R}, \quad \ldots$$

les substitutions, conjuguées entre elles, qui n'altèrent pas la valeur de cette fonction. Soit encore r le nombre des variables qui deviennent immobiles quand on effectue celles des substitutions P, Q, R, ... qui déplacent le plus petit nombre de variables possible. Chacune des substitutions P, Q, R, ... déplacera au moins $n-r$ variables. Supposons d'ailleurs que, parmi ces substitutions, l'une P soit irrégulière; nommons i son ordre et l le nombre des variables qu'elle déplace.

Parmi les puissances de P distinctes de l'unité, on trouvera toujours (théorème I) une substitution régulière qui déplacera $l-2$ variables au plus, et celle-ci sera encore un terme de la suite (3). On aura donc

$$l-2 \stackrel{=}{>} n-r,$$
$$l \stackrel{=}{>} n-r+2.$$

Il y a plus : en vertu du théorème I, on aura nécessairement

$$l-3 \stackrel{=}{>} n-r,$$
$$l \stackrel{=}{>} n-r+3,$$

si l est un nombre impair. On ne pourrait donc avoir précisément

$$l=n-r+2$$

que dans le cas où, l étant un nombre pair, $r=l-3$ serait un nombre impair. En conséquence, on peut énoncer la proposition suivante :

Théorème II. — *Soient* Ω *une fonction de n variables indépendantes x, y, z, ..., et r le nombre des variables qui deviennent immobiles quand on effectue les substitutions qui, en laissant intacte la valeur de* Ω, *déplacent le plus petit nombre de variables possible. Toute substitution qui, sans altérer* Ω, *déplacera* $n-r$ *ou* $n-r+1$ *variables, sera certainement une substitution régulière. Il y a plus : on pourra en dire autant de toute substitution qui, sans altérer* Ω, *déplacera* $n-r+2$ *variables, si r est un nombre pair.*

Corollaire I. — Si la fonction Ω est altérée par toute substitution circulaire du second ordre, on aura

$$n-r>2.$$

Donc alors, en vertu du théorème II, toute substitution P qui n'altérera pas la valeur de Ω sera nécessairement régulière, non seulement quand elle déplacera trois ou quatre variables seulement, mais aussi quand elle déplacera cinq variables.

Corollaire II. — Si la fonction Ω est altérée par toute substitution régulière du second ou du troisième ordre, on aura

$$n - r > 3.$$

Donc alors, en vertu du théorème II, toute substitution P qui n'altérera pas la valeur de Ω sera nécessairement régulière quand elle déplacera quatre ou cinq variables seulement. Elle pourrait devenir irrégulière, si elle déplaçait six variables; par exemple si l'on avait

$$P = (x, y, z, u)(v, w).$$

Effectivement si, en adoptant la valeur précédente de P, on réduit aux dérivées de P les substitutions conjuguées qui n'altèrent pas la valeur de Ω, ces substitutions seront, avec 1 et P, les puissances de P supérieures à la première, et distinctes de l'unité, savoir

$$P^2 = (x, z)(y, u), \qquad P^3 = (x, u, z, y)(v, w),$$

et par conséquent le système des substitutions conjuguées qui n'altéreront pas la valeur de Ω renfermera seulement, avec l'unité, deux substitutions irrégulières du sixième ordre et une substitution régulière du second ordre.

Corollaire III. — Si la fonction Ω est altérée par toute substitution circulaire du second, du troisième ou du quatrième ordre, et par toute substitution régulière du second ordre formée avec quatre variables, on aura

$$n - r > 4.$$

Donc alors, en vertu du théorème II, toute substitution P qui n'altérera pas la valeur de Ω sera nécessairement régulière, quand elle déplacera cinq, six ou sept variables.

315.

Analyse mathématique. — *Mémoire sur diverses propriétés des systèmes de substitutions, et particulièrement de ceux qui sont permutables entre eux.*

C. R., T. XXI, p. 1238 (8 décembre 1845).

Je me propose dans ce Mémoire de faire connaître plusieurs propriétés remarquables des systèmes de substitutions; je montrerai plus tard le parti qu'on peut tirer de cette connaissance dans la recherche du nombre des valeurs distinctes d'une fonction de plusieurs variables.

§ I. — *Sur quelques théorèmes fondamentaux.*

Je commencerai par établir la proposition suivante :

Théorème I. — *Soit*

$$(1) \qquad 1, \ P, \ Q, \ R, \ \ldots$$

un système de substitutions conjuguées, formées avec n variables x, y, z, ... Soient d'ailleurs $\mathfrak{P}$ une autre substitution arbitrairement choisie, et

$$\mathfrak{Q}, \ \mathfrak{R}, \ \ldots$$

d'autres substitutions, déduites de $\mathfrak{P}$ par la résolution des équations linéaires

$$(2) \qquad \mathfrak{P}P = U\mathfrak{Q}, \qquad \mathfrak{P}Q = V\mathfrak{R}, \qquad \ldots,$$

dans lesquelles

$$U, \ V, \ W, \ \ldots$$

représentent des substitutions égales, ou inégales, dont chacune se réduit à un terme de la série (1). *Alors les substitutions*

$$(3) \qquad 1, \ \mathfrak{P}, \ \mathfrak{Q}, \ \mathfrak{R}, \ \ldots,$$

jointes à leurs dérivées, formeront un système de substitutions conju-

guées, qui sera permutable avec le système des substitutions conjuguées

$$1,\quad P,\quad Q,\quad R,\quad \ldots.$$

Démonstration. — Soient T l'une quelconque des substitutions (1), et $\mathfrak{T}$ l'une quelconque des substitutions (3) ou de leurs dérivées. Pour établir le théorème énoncé, il suffira de faire voir que tout produit de la forme

$$\mathfrak{T}T$$

est en même temps de la forme

$$T\mathfrak{T},$$

les valeurs particulières de $\mathfrak{T}$ et de T pouvant varier lorsqu'on passe de la première forme à la seconde. Or, évidemment, en vertu des formules (2), chacun des produits

$$\mathfrak{P}P,\quad \mathfrak{P}Q,\quad \mathfrak{P}R,\quad \ldots \tag{4}$$

sera de la forme

$$Ss,$$

S désignant un terme de la suite (1), et s un terme de la suite (3). De plus, on pourra en dire autant de chacun des produits renfermés dans le Tableau

$$\left\{\begin{matrix} \mathfrak{P}P, & \mathfrak{P}Q, & \mathfrak{P}R, & \ldots, \\ \mathfrak{Q}P, & \mathfrak{Q}Q, & \mathfrak{Q}R, & \ldots, \\ \mathfrak{R}P, & \mathfrak{R}Q, & \mathfrak{R}R, & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots. \end{matrix}\right. \tag{5}$$

En effet, considérons, pour fixer les idées, le produit

$$\mathfrak{Q}P.$$

On pourra aisément le réduire à la forme Ss; car la première des équations (2) donnera

$$\mathfrak{Q} = U^{-1}\mathfrak{P}P$$

et, par conséquent,

$$\mathfrak{Q}P = U^{-1}\mathfrak{P}P^2.$$

Mais, P^2 étant un terme de la suite (1), $\mathfrak{P}P^2$ sera un terme de la suite (4),

et par conséquent une des équations (2) sera de la forme

$$\mathfrak{P}P^2 = Ws,$$

W étant lui-même un terme de la suite (1). On aura donc

$$\mathfrak{Q}P = U^{-1}Ws,$$

et l'on en conclura

$$\mathfrak{Q}P = Ss, \tag{6}$$

en posant, pour abréger,

$$S = U^{-1}W.$$

Or, comme la valeur précédente de S sera encore un terme de la suite (1), la formule (6) exprimera simplement que le produit $\mathfrak{Q}P$ est de la forme Ss, S désignant un terme de la suite (1), et s un terme de la suite (3).

De ce qu'on vient de dire, il résulte évidemment que, si T représente un terme quelconque de la suite (1), et $\mathfrak{T}$ un terme quelconque de la suite (3), on pourra toujours satisfaire à la condition

$$\mathfrak{T}T = Ss, \tag{7}$$

en prenant pour S un autre terme de la suite (1), et pour s un autre terme de la suite (3). J'ajoute qu'il en sera encore de même si l'on donne à la suite (3) une extension nouvelle, en y faisant entrer, avec les substitutions

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots,$$

toutes celles de leurs dérivées qui pourraient n'y être pas renfermées, c'est-à-dire les diverses puissances des substitutions $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{R}$, ..., et, plus généralement, les produits de ces mêmes substitutions multipliées l'une par l'autre deux à deux, trois à trois, ..., de toutes les manières possibles. Effectivement, T étant un terme quelconque de la suite (1), soient

$$\mathfrak{T},\quad \mathfrak{T}',\quad \mathfrak{T}'',\quad \ldots$$

divers termes égaux ou inégaux de la suite (3). La formule (7) fournira successivement plusieurs équations de la forme

$$(8)\qquad \mathfrak{T}\mathrm{T}=\mathrm{S}\mathfrak{s},\qquad \mathfrak{T}'\mathrm{S}=\mathrm{S}'\mathfrak{s}',\qquad \mathfrak{T}''\mathrm{S}'=\mathrm{S}''\mathfrak{s}'',\qquad \ldots,$$

S, S', S'', ... désignant des termes de la suite (1), et $\mathfrak{s}, \mathfrak{s}', \mathfrak{s}'', \ldots$ des termes de la suite (2). Or, des formules (8) on déduira successivement les équations

$$(9)\qquad \mathfrak{T}'\mathfrak{T}\mathrm{T}=\mathrm{S}'\mathfrak{s}'\mathfrak{s},\qquad \mathfrak{T}''\mathfrak{T}'\mathfrak{T}\mathrm{T}=\mathrm{S}''\mathfrak{s}''\mathfrak{s}'\mathfrak{s},\qquad \ldots,$$

et celles-ci seront encore semblables à la formule (7), avec cette seule différence que les substitutions

$$\mathfrak{T} \quad\text{et}\quad \mathfrak{s}$$

s'y trouveront remplacées par les produits

$$\mathfrak{T}'\mathfrak{T} \quad\text{et}\quad \mathfrak{s}'\mathfrak{s} \qquad\text{ou}\qquad \mathfrak{T}''\mathfrak{T}'\mathfrak{T} \quad\text{et}\quad \mathfrak{s}''\mathfrak{s}'\mathfrak{s},\quad \ldots,$$

c'est-à-dire par des substitutions dérivées de $\mathfrak{P}, \mathfrak{Q}, \mathfrak{R}, \ldots$. D'ailleurs, celles de ces substitutions qui se trouveront représentées par les produits

$$\mathfrak{T}'\mathfrak{T},\quad \mathfrak{T}''\mathfrak{T}'\mathfrak{T},\quad \ldots,$$

pourront être évidemment des dérivées quelconques des substitutions $\mathfrak{P}, \mathfrak{Q}, \mathfrak{R}, \ldots$.

Le premier théorème étant ainsi démontré, on peut en déduire immédiatement un grand nombre de propositions nouvelles que je vais successivement indiquer.

D'abord, si les substitutions P, Q, R, ... se réduisent aux diverses puissances d'une même substitution P, alors à la place du théorème I on obtiendra la proposition suivante :

Théorème II. — *Soient* P *une substitution formée avec plusieurs variables $x, y, z, \ldots$, et i l'ordre de cette substitution, dont les diverses puissances composeront, en conséquence, le système des substitutions conjuguées*

$$(10)\qquad 1,\quad \mathrm{P},\quad \mathrm{P}^2,\quad \ldots,\quad \mathrm{P}^{i-1}.$$

Soient encore

$$a,\quad b,\quad c,\quad \ldots,\quad f,\quad g$$

des nombres entiers quelconques égaux ou inégaux, et

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots,\quad \mathfrak{U},\quad \mathfrak{V},\quad \mathfrak{W}$$

de nouvelles substitutions, déterminées par le système des équations linéaires

$$(11)\quad \mathfrak{P}\mathrm{P}=\mathrm{P}^a\mathfrak{Q},\qquad \mathfrak{P}\mathrm{P}^2=\mathrm{P}^b\mathfrak{R},\qquad \ldots,\qquad \mathfrak{P}\mathrm{P}^{i-2}=\mathrm{P}^f\mathfrak{V},\qquad \mathfrak{P}\mathrm{P}^{i-1}=\mathrm{P}^g\mathfrak{W}.$$

Si, aux substitutions

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots,\quad \mathfrak{U},\quad \mathfrak{V},\quad \mathfrak{W},$$

on joint les dérivées de ces mêmes substitutions, on obtiendra un système de substitutions conjuguées qui sera permutable avec le système des puissances de P.

Si l'on prend pour a un nombre premier à i, la substitution P^a sera semblable à la substitution P, et par suite on pourra choisir $\mathfrak{P}$ de manière à vérifier la formule

$$(12)\qquad \mathfrak{P}\mathrm{P}=\mathrm{P}^a\mathfrak{P}.$$

Alors aussi la première des formules (11) se réduira simplement à l'équation (12). D'ailleurs, si, dans chacun des membres de cette dernière équation, on introduit plusieurs fois de suite le facteur P comme multiplicande, on en tirera successivement

$$\mathfrak{P}\mathrm{P}^2=\mathrm{P}^a\,\mathfrak{P}\mathrm{P}=\mathrm{P}^{2a}\mathfrak{P},$$
$$\mathfrak{P}\mathrm{P}^3=\mathrm{P}^{2a}\mathfrak{P}\mathrm{P}=\mathrm{P}^{3a}\mathfrak{P},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Donc le système des équations (11) pourra être remplacé par le système des formules

$$(13)\quad \mathfrak{P}\mathrm{P}=\mathrm{P}^a\mathfrak{P},\qquad \mathfrak{P}\mathrm{P}^2=\mathrm{P}^{2a}\mathfrak{P},\qquad \ldots,\qquad \mathfrak{P}\mathrm{P}^{(i-1)}=\mathrm{P}^{(i-1)a}\mathfrak{P},$$

toutes comprises dans la formule générale

$$(14)\qquad \mathfrak{P}\mathrm{P}^h=\mathrm{P}^{ah}\mathfrak{P},$$

et le théorème II entraînera la proposition suivante :

Théorème III. — *Si,* P *étant une substitution de l'ordre i, et a un* *nombre premier à i, on nomme* $\mathfrak{P}$ *l'une quelconque des solutions de l'équation linéaire*

$$\mathfrak{P}\mathrm{P} = \mathrm{P}^a\mathfrak{P},$$

le système des substitutions conjuguées qui représenteront les diverses puissances de $\mathfrak{P}$ *sera permutable avec le système des substitutions conjuguées qui représenteront les diverses puissances de* P.

Corollaire I. — Il est bon d'observer que, après avoir déduit de l'équation (12) la formule (14), on pourra, de cette dernière formule, déduire successivement les suivantes

$$\mathfrak{P}^2\mathrm{P}^h = \mathfrak{P}\mathrm{P}^{ah}\,\mathfrak{P} = \mathrm{P}^{a^2h}\mathfrak{P}^2,$$
$$\mathfrak{P}^3\mathrm{P}^h = \mathfrak{P}\mathrm{P}^{a^2h}\mathfrak{P}^2 = \mathrm{P}^{a^3h}\mathfrak{P}^3,$$
$$\dots\dots\dots\dots\dots\dots\dots\dots,$$

toutes comprises dans la formule générale

$$\mathfrak{P}^k\mathrm{P}^h = \mathrm{P}^{a^kh}\mathfrak{P}^k. \tag{15}$$

Corollaire II. — D'après ce qu'on a vu dans un précédent Mémoire, pour obtenir une solution quelconque $\mathfrak{P}$ de l'équation (12), il suffit de représenter chacune des substitutions semblables P, P^a, à l'aide de ses facteurs circulaires, en ayant soin de faire occuper les mêmes places, dans les deux substitutions, par des facteurs circulaires de même ordre. Alors $\mathfrak{P}$ pourra être représenté par la notation symbolique

$$\binom{\mathrm{P}^a}{\mathrm{P}},$$

pourvu que, en supprimant, dans P et dans P^a, les virgules et les parenthèses, on considère P et P^a comme représentant de simples arrangements. On peut donc énoncer encore la proposition suivante :

Théorème IV. — *Soient* P *une substitution de l'ordre i, et a un nombre premier à i. Supposons, d'ailleurs, que, après avoir représenté les substitutions* P *et* P^a *à l'aide de leurs facteurs circulaires, en ayant soin de faire occuper les mêmes places, dans ces deux substitutions, par des facteurs circulaires de même ordre, on supprime les virgules et parenthèses*

placées entre les variables, afin de réduire P *et* P^a *à de simples arrangements. Alors les puissances de la substitution*

$$\mathfrak{P} = \binom{\mathrm{P}^a}{\mathrm{P}} \tag{16}$$

formeront un système de substitutions conjuguées qui sera permutable avec le système des puissances de la substitution P.

Exemple. — Si l'on prend

$$\mathrm{P} = (x, y, z, u, v)$$

et $a = 2$, alors, en laissant x à la première place, on trouvera

$$\mathrm{P}^2 = (x, z, v, y, u),$$

et, en réduisant P, P^2 à de simples arrangements, on tirera de la formule (16)

$$\mathfrak{P} = \binom{xzvyu}{xyzuv} = (y, z, v, u).$$

Donc le système des puissances de la substitution circulaire du quatrième ordre

$$\mathfrak{P} = (y, z, v, u)$$

sera permutable avec le système des puissances de la substitution circulaire du cinquième ordre

$$\mathrm{P} = (x, y, z, u, v).$$

Si, en adoptant la valeur de P déterminée par la formule

$$\mathrm{P} = (x, y, z, u, v),$$

on attribuait successivement au nombre a les valeurs

$$2,\quad 3,\quad 4,$$

alors, en laissant toujours x à la première place dans chacune des substitutions

$$\mathrm{P}^2,\quad \mathrm{P}^3,\quad \mathrm{P}^4,$$

on obtiendrait successivement pour $\mathfrak{P}$ les trois substitutions

$$(y, z, v, u), \quad (y, u, v, z), \quad (y, v)(z, u),$$

c'est-à-dire celles des puissances de la substitution

$$(y, z, v, u)$$

qui sont distinctes de l'unité.

Généralement, si l'on représente par P une substitution circulaire dont l'ordre i soit un nombre premier, on pourra, en appliquant la formule (5) à la détermination de $\mathfrak{P}$, laisser toujours à la première place une même variable x, et alors, en posant successivement

$$a = 2, \quad a = 3, \quad \ldots, \quad a = i - 1,$$

on obtiendra i valeurs différentes de $\mathfrak{P}$.

Lorsque i cessera d'être un nombre premier, on ne pourra plus, dans la formule (16), prendre pour a l'un quelconque des nombres entiers inférieurs à i. Mais on pourra toujours y supposer

$$a = i - 1,$$

puisque $i - 1$ sera toujours premier à i. Alors l'équation (16) donnera

$$\mathfrak{P} = \begin{pmatrix} P^{i-1} \\ P \end{pmatrix} \tag{17}$$

ou plus simplement

$$\mathfrak{P} = \begin{pmatrix} P^{-1} \\ P \end{pmatrix}. \tag{18}$$

Exemple. — Si l'on prend $i = 6$ et

$$P = (x, y, z, u, v, w),$$

alors, en laissant x à la première place, on aura

$$P^{-1} = (x, w, v, u, z, y),$$

et, en réduisant P, P^{-1} à de simples arrangements, on tirera de la formule (18)

$$\begin{pmatrix} xwvuzy \\ xyzuvw \end{pmatrix} = (y, w)(z, v).$$

Donc le système des puissances de la substitution du second ordre

$$\mathfrak{P} = (y, w)(z, v)$$

sera permutable avec le système des puissances de la substitution circulaire du sixième ordre

$$P = (x, y, z, u, v, w).$$

Rien n'empêche de supposer, dans la formule (16),

$$a = 1.$$

Dans cette supposition, la formule (16) donnera

$$\mathfrak{P} = \begin{pmatrix} P' \\ P \end{pmatrix}, \tag{19}$$

P′ désignant une seconde forme de P, que l'on déduira de la première, en ayant soin de faire toujours occuper les mêmes places par des facteurs circulaires de même ordre. Alors aussi $\mathfrak{P}$ se réduira simplement à une puissance de P, si P se réduit à une substitution circulaire. Mais il n'en sera plus généralement de même si P est le produit de plusieurs facteurs circulaires du premier ordre, ou même d'ordres différents. Alors $\mathfrak{P}$ pourra être une substitution distincte de toutes les puissances de P, ainsi qu'on le voit dans les exemples suivants.

Exemple I. — Soit

$$P = (x, y)(z, u).$$

Alors, en posant

$$P' = (y, x)(z, u),$$

on tirera de la formule (7)

$$\mathfrak{P} = (x, y);$$

si l'on prend, au contraire,

$$P' = (z, u)(x, y),$$

on tirera de la formule (19)

$$\mathfrak{P} = \begin{pmatrix} zuxy \\ xyzu \end{pmatrix} = (x, z)(y, u);$$

enfin, si l'on prend

$$P' = (u, z,)(x, y),$$

la formule (19) donnera

$$\mathfrak{P} = \begin{pmatrix} uzxy \\ xyzu \end{pmatrix} = (x, u, y, z);$$

et, dans ces divers cas, le système des puissances de $\mathfrak{P}$ sera permutable avec le système des puissances de P.

Exemple II. — Soit

$$P = (x, y, z, u)(v, w),$$

et prenons

$$P' = (y, z, u, x)(v, w).$$

La formule (19) donnera

$$\mathfrak{P} = \begin{pmatrix} yzuxvw \\ xyzuvw \end{pmatrix} = (x, y, z, u),$$

et alors le système des puissances de $\mathfrak{P}$ sera permutable avec le système des puissances de P, qui seront toutes distinctes de $\mathfrak{P}$.

§ II. — *Conséquences des principes établis dans le premier paragraphe et dans les précédents Mémoires.*

Dans le Mémoire que j'ai publié, il y a trente ans environ (¹), *Sur le nombre des valeurs qu'une fonction peut acquérir, quand on y permute de toutes les manières possibles les quantités qu'elle renferme*, j'avais représenté ces quantités par des lettres affectées d'indices, et les indices par des nombres. Alors les substitutions, en vertu desquelles les diverses quantités étaient échangées les unes contre les autres, se trouvaient exprimées à l'aide de ces nombres, par conséquent à l'aide des indices eux-mêmes, comme je l'ai fait encore dans une des précédentes séances (*voir* les formules (3) de la page 346). C'est aussi en remplaçant par des nombres les diverses variables desquelles une fonction dépend, que M. Hermite m'a dit être parvenu, non seulement à constater l'existence de la fonction transitive de six variables qui

(¹) *Œuvres de Cauchy*, S. II, T. I.

offre six valeurs distinctes, mais encore à d'autres résultats spécialement relatifs aux nombres premiers 5, 7, 11, et applicables à la théorie des trois équations modulaires dont les degrés sont ces nombres premiers augmentés de l'unité. Quoique, dans l'entretien que nous avons eu ensemble le 19 novembre dernier, M. Hermite ne m'ait pas dit en quoi consiste précisément sa méthode, j'avouerai sans difficulté que cet entretien a excité en moi un vif désir d'approfondir de plus en plus les questions relatives à la théorie des permutations, et m'a engagé à rechercher avec plus de soin toutes les conséquences qui peuvent se déduire des principes que j'avais déjà établis dans les *Comptes rendus*. Mes recherches m'ont d'abord conduit aux résultats énoncés dans les deux dernières séances et dans le § I du présent Mémoire. Je vais maintenant en indiquer plusieurs autres qui peuvent être aisément tirés des formules auxquelles nous sommes déjà parvenus.

Soit

$$(1) \qquad P(x, y, z, \ldots)$$

une substitution circulaire de l'ordre i, formée avec i variables x, y, z, ... Soit de plus a un nombre premier à i. Enfin, supposons qu'on laisse la variable x à la première place dans la substitution P^a, semblable à P, et que, en réduisant les substitutions P, P^a à de simples arrangements, on prenne

$$(2) \qquad \mathfrak{P} = \begin{pmatrix} P^a \\ P \end{pmatrix}.$$

Alors $\mathfrak{P}$ sera une substitution qui déplacera seulement les variables

$$y, \quad z, \quad \ldots,$$

ou quelques-unes d'entre elles, et les puissances de $\mathfrak{P}$ formeront un système permutable avec le système des puissances de P. Il y a plus : la substitution $\mathfrak{P}$, comme on l'a vu dans le § I, vérifiera généralement la formule

$$(3) \qquad \mathfrak{P}^k P^h = P^{a^k h} \mathfrak{P}^k,$$

quels que soient les nombres entiers h et k. Or il suit de cette dernière formule que, des deux équations

$$\mathfrak{P}^k = 1, \qquad P^h = P^{a^k h}, \tag{4}$$

la première entrainera toujours la seconde, et réciproquement. On doit en conclure que l'ordre de la substitution $\mathfrak{P}$, c'est-à-dire la plus petite valeur de k propre à vérifier la formule

$$\mathfrak{P}^k = 1,$$

est aussi la plus petite valeur de k qui vérifie l'équivalence

$$a^k \equiv 1 \pmod{i}. \tag{5}$$

De cette simple remarque on déduit immédiatement les théorèmes VI et VII des pages 333 et 334, auxquels on parvient encore en remplaçant les variables $x, y, z, \ldots$ par des lettres affectées d'indices, et présentant en conséquence la substitution P, comme nous l'avons fait à la page 333, sous la forme

$$P = (x_0, x_1, x_2, \ldots, x_{i-1}). \tag{6}$$

Il suit aussi de la remarque précédente, que les *racines primitives* du nombre entier i seront précisément les valeurs de a qui fourniront pour valeur de

$$\binom{P^a}{P}$$

une substitution de l'ordre $i - 1$, si i est un nombre premier, et, dans le cas contraire, une substitution circulaire d'un ordre équivalant à l'*indicateur maximum* I.

Dans le cas particulier où l'on prend $a = i - 1$, la formule (6), réduite à l'équation

$$\mathfrak{P} = \binom{P^{-1}}{P}, \tag{7}$$

fournit pour valeur de $\mathfrak{P}$ une substitution circulaire du second ordre.

Revenons maintenant aux formules (11) du § I, et, en supposant que P désigne une substitution circulaire de l'ordre i, déterminée

par la formule (1), prenons encore pour $\mathfrak{P}$ une substitution qui déplace seulement quelques-unes des variables renfermées dans P, de manière à laisser immobile, à la première place, la variable x. On tirera des formules (11) du § I

$$\left\{\begin{array}{l} \mathfrak{Q} = P^{-a}\mathfrak{P}P, \\ \mathfrak{R} = P^{-b}\mathfrak{P}P^2, \\ \ldots\ldots\ldots\ldots, \\ \mathfrak{V} = P^{-f}\mathfrak{P}P^{i-2}, \\ \mathfrak{W} = P^{-g}\mathfrak{P}P^{i-1}. \end{array}\right. \tag{8}$$

D'ailleurs, on pourra donner au nombre a une valeur telle, que la substitution $\mathfrak{Q}$, déterminée par la première des équations (8), laisse immobile la variable x. Effectivement, nommons s la variable qui succède à x en vertu de la substitution $\mathfrak{P}$P. On remplira évidemment la condition énoncée en prenant pour P^a celle des puissances de P qui substituera s à x, puisque alors la substitution inverse P^{-a} aura pour effet de substituer x à s, et, par conséquent, de ramener x à la place que cette variable occupait primitivement. Ajoutons qu'une remarque semblable est applicable encore à chacun des nombres $b, \ldots, f, g$, compris dans les valeurs de $\mathfrak{R}, \ldots, \mathfrak{V}, \mathfrak{W}$ déterminées par la seconde, ..., l'avant-dernière, la dernière des équations (8). On peut donc énoncer généralement la proposition suivante :

Théorème I. — *Soit* P *une substitution circulaire de l'ordre i, formée avec i variables*

$$x, \quad y, \quad z, \quad \ldots.$$

Nommons $\mathfrak{P}$ une autre substitution qui renferme seulement quelques-unes de ces variables, de manière à laisser immobile une ou plusieurs d'entre elles, par exemple la variable x. Enfin, nommons $\mathfrak{Q}, \mathfrak{R}, \ldots, \mathfrak{V}, \mathfrak{W}$ les substitutions qui, en déplaçant les seules variables $y, z, \ldots$, vérifient des équations de la forme (8). *Le système des substitutions $\mathfrak{P}, \mathfrak{Q}, \mathfrak{R}, \ldots$ et de leurs dérivées sera permutable avec le système des puissances de la substitution circulaire* P.

Dans l'hypothèse admise, les substitutions

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots,\quad \mathfrak{U},\quad \mathfrak{V},$$

jointes à leurs dérivées, composeront un système de substitutions conjuguées dont chacune laissera immobile la variable x. Soit $\mathcal{M}$ l'ordre de ce système. Parmi les substitutions qu'il renfermera, aucune ne pourra se réduire à une puissance de P distincte de l'unité, puisqu'une telle puissance déplacera toujours chacune des variables x, y, z, ... Donc le système dont il s'agit et le système des i puissances de P n'auront pas de termes communs autres que l'unité. Donc, en vertu des principes établis dans la séance du 20 octobre, un troisième système, qui renfermerait toutes les dérivées des substitutions comprises dans les deux premiers, sera de l'ordre $\mathcal{M}i$. D'ailleurs, eu égard aux formules (8), ce troisième système se réduira au système des deux substitutions

$$\mathrm{P},\quad \mathfrak{P}$$

et de leurs dérivées des divers ordres. On peut donc énoncer encore la proposition suivante :

THÉORÈME II. — *Les mêmes choses étant posées que dans le théorème I, si l'on nomme $\mathcal{M}$ l'ordre du système qui renfermera les substitutions $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{R}$, ..., $\mathfrak{V}$, $\mathfrak{W}$ et toutes leurs dérivées, $\mathcal{M}i$ sera l'ordre du système de substitutions conjuguées qui renfermera les dérivées diverses des deux substitutions* P *et* $\mathfrak{P}$.

Il est important d'observer que, dans la série des substitutions

$$\mathfrak{Q},\quad \mathfrak{R},\quad \ldots,\quad \mathfrak{V},\quad \mathfrak{W}, \tag{9}$$

déduites successivement de la substitution $\mathfrak{P}$ à l'aide des équations (8), plusieurs termes peuvent être égaux entre eux. On peut même affirmer que, dans cette série, prolongée à partir d'un terme qui serait égal à $\mathfrak{P}$, les termes $\mathfrak{Q}$, $\mathfrak{R}$, ... se reproduiront dans le même ordre à la suite les uns des autres. En effet, supposons que l'un des termes de la

série (8) se réduise à $\mathfrak{P}$, et qu'en conséquence, l'une des équations (8) soit de la forme

$$\mathfrak{P} = \mathrm{P}^{-l}\mathfrak{P}\mathrm{P}^{j}, \tag{10}$$

j étant positif, mais inférieur à $i - 1$. On aura, par suite,

$$\mathfrak{P}\mathrm{P}^{j} = \mathrm{P}^{l}\mathfrak{P}, \tag{11}$$

et de cette dernière formule, combinée avec les équations

$$\mathfrak{P}\mathrm{P} = \mathrm{P}^{a}\mathfrak{Q},\qquad \mathfrak{P}\mathrm{P}^{2} = \mathrm{P}^{b}\mathfrak{R},\qquad \ldots, \tag{12}$$

on tirera successivement

$$\left\{\begin{array}{l} \mathfrak{P}\mathrm{P}^{j+1} = \mathrm{P}^{l}\mathfrak{P}\mathrm{P} = \mathrm{P}^{l+a}\mathfrak{Q}, \\ \mathfrak{P}\mathrm{P}^{j+2} = \mathrm{P}^{l}\mathfrak{P}\mathrm{P}^{2} = \mathrm{P}^{l+b}\mathfrak{R}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right. \tag{13}$$

ou, ce qui revient au même,

$$\mathfrak{Q} = \mathrm{P}^{-l-a}\mathfrak{P}\mathrm{P}^{j+1},\qquad \mathfrak{R} = \mathrm{P}^{-l-b}\mathfrak{P}\mathrm{P}^{j+2},\qquad \ldots. \tag{14}$$

Il y a plus : de la formule (11), jointe aux équations (12), on tirera non seulement

$$\mathfrak{P}\mathrm{P}^{hj} = \mathrm{P}^{hl}\mathfrak{P}, \tag{15}$$

mais encore

$$\mathfrak{P}\mathrm{P}^{hj+1} = \mathrm{P}^{hl+a}\mathfrak{Q},\qquad \mathfrak{P}\mathrm{P}^{hj+2} = \mathrm{P}^{hl+b}\mathfrak{R},\qquad \ldots \tag{16}$$

ou, ce qui revient au même,

$$\mathfrak{Q} = \mathrm{P}^{-hl-a}\mathfrak{P}\mathrm{P}^{hj+1},\qquad \mathfrak{R} = \mathrm{P}^{-hl-b}\mathfrak{P}\mathrm{P}^{hj+2},\qquad \ldots. \tag{17}$$

De ces remarques on peut déduire plusieurs conséquences importantes; et d'abord, puisque, en vertu des formules (17), les mêmes termes $\mathfrak{Q}$, $\mathfrak{R}$, ... se reproduiront toujours périodiquement dans les formules (8) et dans la série (9), à partir d'un terme qui serait égal à $\mathfrak{P}$, il en résulte que, si l'on attribue à j la plus petite des valeurs positives pour lesquelles se vérifie la formule (10), cette plus petite valeur divisera toutes les autres, et par conséquent le nombre i, qui représente l'ordre de la substitution P. De plus, il résulte de l'équation (15) que, des deux formules

$$P^{hj}=1, \qquad P^{hl}=1, \tag{18}$$

la première entrainera toujours la seconde, et réciproquement. Donc, par suite, j devra être un diviseur, non seulement de i, mais aussi de l, de sorte qu'on aura

$$l=\theta j, \tag{19}$$

θ étant un nombre entier, et même un nombre premier à i. Donc aussi l'équation (15) pourra être présentée sous la forme

$$\mathfrak{P}P^{hj}=P^{\theta hj}\mathfrak{P}, \tag{20}$$

θ étant premier à i.

On peut affirmer que, dans le cas où des termes de la série

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots,\quad \mathfrak{V},\quad \mathfrak{W} \tag{21}$$

deviennent égaux entre eux, le terme $\mathfrak{P}$ reparait toujours le premier, entrainant à sa suite les termes $\mathfrak{Q}$, $\mathfrak{R}$, ..., périodiquement reproduits dans le même ordre. En effet, supposons, pour fixer les idées, que la suite (21) offre deux termes égaux à $\mathfrak{Q}$. Alors l'une des équations (12) sera de la forme

$$\mathfrak{P}P^{j'}=P^{l'}\mathfrak{Q}, \tag{22}$$

j' étant supérieur à l'unité, mais inférieur à $i-1$. Or, de l'équation (22), combinée avec la première des formules (8), on tirera

$$\mathfrak{P}P^{j'-1}=P^{l'-a}\mathfrak{P}, \tag{23}$$

$j'-1$ étant positif, mais inférieur à $i-1$; et, en vertu de la formule (23), des deux termes $\mathfrak{P}$, $\mathfrak{Q}$, le premier aura dû reparaitre avant le second dans la série (21).

On peut remarquer encore que de la première des équations (12),

combinée avec celles qui la suivent, on tire d'autres équations de la forme

$$\mathfrak{Q}P=P^{b-a}\mathfrak{R}, \qquad \mathfrak{Q}P^{2}=P^{c-a}\mathfrak{S}, \qquad \ldots, \tag{24}$$

et que ces dernières sont semblables aux équations (12), avec cette seule différence que les nombres

$$a,\quad b,\quad c,\quad \ldots$$

y sont remplacés par d'autres nombres

$$b-a,\quad c-a,\quad \ldots.$$

Donc, tout ce qui a été dit de la substitution $\mathfrak{P}$ pourra se dire pareillement de la substitution $\mathfrak{Q}$, et généralement de tous les termes de la série (21).

Enfin, de la forme (20) on tirera immédiatement la suivante

$$\mathfrak{P}^k P^{hj}=P^{\theta^k hj}\mathfrak{P}^k. \tag{25}$$

Or il résulte de cette dernière que, des deux équations

$$\mathfrak{P}^k=1, \qquad P^{hj}=P^{\theta^k hj}, \tag{26}$$

la première entraîne toujours la seconde, et réciproquement, quel que soit d'ailleurs le nombre entier h. Donc, l'ordre de la substitution $\mathfrak{P}$ sera la plus petite des valeurs de k propres à vérifier l'équivalence

$$(\theta^k-1)j\equiv 0 \quad (\text{mod.}\, i), \tag{27}$$

que l'on peut aussi mettre sous la forme

$$\theta^k\equiv 1 \quad \left(\text{mod.}\, \frac{i}{j}\right). \tag{28}$$

Dans un prochain Mémoire, je montrerai les conséquences remarquables qui peuvent se déduire des diverses propositions et formules que je viens d'établir.

316.

ANALYSE MATHÉMATIQUE. — *Note sur les fonctions caractéristiques des substitutions.*

C. R., T. XXI, p. 1254 (8 décembre 1845).

Considérons n variables représentées par diverses lettres

$$x,\quad y,\quad z,\quad \ldots,$$

ou bien encore par une même lettre x successivement affectée des indices

$$0,\quad 1,\quad 2,\quad 3,\quad \ldots,\quad n-1,$$

en sorte que les variables données soient respectivement

$$x_0,\quad x_1,\quad x_2,\quad \ldots,\quad x_{n-1}.$$

Une substitution donnée P aura pour effet de remplacer une variable quelconque x_t, correspondante à l'indice t, par une autre variable x_s correspondante à un autre indice s qui pourra être considéré comme fonction de t. Supposons effectivement

$$s = \varphi(t),$$

$\varphi(t)$ sera ce que j'appelle la *fonction caractéristique* de la substitution P. Lorsque cette substitution sera donnée, on connaîtra les n valeurs de $\varphi(t)$ représentées par

$$\varphi(0),\quad \varphi(1),\quad \ldots,\quad \varphi(n-1),$$

c'est-à-dire les n valeurs de t qui répondent aux indices

$$0,\quad 1,\quad \ldots,\quad n-1$$

de la variable t. Par suite, si l'on nomme θ une racine quelconque de l'équation binôme

$$\theta^n = 1, \tag{1}$$

on aura, en vertu d'une formule connue,

$$\varphi(\theta) = \Sigma\theta^t f(\theta^{-1}), \tag{2}$$

la somme qu'indique le signe Σ s'étendant à toutes les valeurs de θ, et la fonction $f(\theta)$ étant elle-même déterminée par la formule

$$f(\theta) = \frac{1}{n}\Sigma\theta^t \varphi(t), \tag{3}$$

dans laquelle la somme indiquée par le signe Σ s'étend à toutes les valeurs de t comprises dans la suite

$$0,\quad 1,\quad 2,\quad \ldots,\quad n-1.$$

Dans un prochain article, je montrerai les avantages que présente l'emploi des fonctions caractéristiques dans la théorie des permutations.

317.

ANALYSE MATHÉMATIQUE. — *Mémoire sur le nombre et la forme des substitutions qui n'altèrent pas la valeur d'une fonction de plusieurs variables indépendantes.*

C. R., T. XXI, p. 1287 (15 décembre 1845).

§ I. — *Propriétés diverses des substitutions qui, étant semblables à une substitution donnée, n'altèrent pas la valeur d'une fonction de plusieurs variables.*

Soient

Ω une fonction de n variables indépendantes $x, y, z, \ldots$;
M le nombre de ses valeurs égales;
m le nombre de ses valeurs distinctes $\Omega, \Omega', \Omega'', \ldots$.

On aura

$$mM = N, \tag{1}$$

la valeur de N étant

$$N = 1.2.3\ldots n.$$

Soient d'ailleurs

(2) $$1,\ P,\ Q,\ R,\ \ldots,\ U,\ V,\ W$$

le système des substitutions conjuguées qui n'altèrent pas la valeur de Ω, et représentons par

(3) $$P,\ P',\ P'',\ \ldots$$

celles de ces substitutions qui sont semblables à une substitution donnée P. Enfin soient

h le nombre des substitutions $P, P', P'', \ldots$;
k le nombre de celles des fonctions $\Omega, \Omega', \Omega'', \ldots$ qui ne sont pas altérées par la substitution P;
ϖ le nombre total des substitutions semblables à P, qui peuvent être formées avec les n variables $x, y, z, \ldots$;
ω le nombre de formes que peut revêtir la substitution P, exprimée à l'aide de ses facteurs circulaires, quand on s'astreint à faire occuper toujours les mêmes places, dans cette substitution, par des facteurs circulaires de même ordre.

D'après ce qu'on a vu dans les précédents Mémoires, on aura, non seulement

(4) $$\omega\varpi = N,$$

mais encore

(5) $$hm = k\varpi.$$

D'ailleurs, on tirera des équations (1) et (4)

(6) $$\frac{\varpi}{m} = \frac{M}{\omega}.$$

Donc, par suite, l'équation (5) donnera

(7) $$h\omega = kM.$$

Or, cette dernière formule renferme évidemment le théorème dont voici l'énoncé :

Théorème I. — *Soient Ω une fonction de n variables indépendantes x, y, z, ..., et M le nombre de ces valeurs égales. Soient encore* P *l'une des substitutions qui n'altèrent pas Ω, et* $P, P', P'', \ldots$ *les substitutions, semblables à* P, *qui jouissent de la même propriété. Le nombre M sera un diviseur du nombre total des formes que peuvent revêtir les substitutions* $P, P', P'', \ldots$ *exprimées à l'aide de leurs facteurs circulaires, quand on s'astreint à faire occuper toujours les mêmes places, dans ces diverses substitutions, par des facteurs circulaires de même ordre.*

Corollaire. — Supposons, pour fixer les idées, que P représente une substitution circulaire de l'ordre n. Alors on aura précisément

(8) $$\omega = n.$$

Alors aussi Ω deviendra une fonction transitive des n variables x, y, z, ..., et l'on aura, par suite,

(9) $$M = n\mathfrak{M},$$

$\mathfrak{M}$ étant le nombre des valeurs égales de Ω considéré comme fonction des $n-1$ variables y, z, ... Cela posé, en divisant par n les deux membres de la formule (7), on trouvera

(10) $$h = k\mathfrak{M},$$

et le théorème I sera réduit à la proposition suivante :

Théorème II. — *Soit Ω une fonction transitive de n variables x, y, z, ..., et supposons que cette fonction ne soit pas altérée par une ou plusieurs substitutions circulaires de l'ordre n. Le nombre h de ces substitutions circulaires aura pour diviseur le nombre des valeurs égales de Ω considéré comme fonction des $n-1$ variables y, z, ...*

Corollaire. — Si les seules substitutions circulaires de l'ordre n, qui jouissent de la propriété de ne pas altérer Ω, se réduisent à des puissances d'une même substitution P, h sera précisément le nombre des entiers premiers à n. Donc alors le nombre des entiers premiers à n aura pour diviseur le nombre des valeurs égales de Ω considéré comme fonction de $n-1$ variables.

Exemple I. — Concevons que Ω représente une fonction transitive de cinq variables x, y, z, u, v. Le nombre de ses valeurs égales étant un multiple de 5, on trouvera nécessairement des substitutions du cinquième ordre parmi celles qui n'altéreront pas la valeur de Ω. Cela posé, il résulte du théorème II que, dans le cas où ces substitutions du cinquième ordre se réduisent aux puissances

$$P^1,\quad P^2,\quad P^3,\quad P^4$$

d'une même substitution P, le nombre $\mathfrak{M}$ de valeurs égales de Ω considéré comme fonction des quatre variables y, z, u, v doit être un diviseur de 4. Donc alors $\mathfrak{M}$ ne peut être que l'un des nombres 1, 2, 4.

Exemple II. — Concevons que Ω représente une fonction transitive de six variables x, y, z, u, v, w, et supposons que, parmi les substitutions qui n'altèrent pas la valeur de cette fonction, on trouve des substitutions circulaires du sixième ordre, représentées par des puissances d'une même substitution circulaire P. Ces puissances ne pourront être que P et P^5, et par suite le nombre 2, c'est-à-dire le nombre des entiers premiers à 6, aura pour diviseur le nombre $\mathfrak{M}$ des valeurs égales de Ω considéré comme fonction des cinq variables y, z, u, v, w. Donc alors $\mathfrak{M}$ ne pourra être que 1 ou 2.

Concevons maintenant que, Ω étant une fonction quelconque des n variables $x, y, z, \ldots$, on nomme

$$(3)\qquad P,\quad P',\quad P'',\quad \ldots$$

les substitutions qui, étant semblables entre elles et à une certaine substitution P, déplacent toutes les variables sans altérer la valeur de Ω. Soit, d'ailleurs,

$$(11)\qquad 1,\quad \mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots$$

le système des substitutions conjuguées qui n'altèrent pas Ω considéré comme fonction des $n-1$ variables $y, z, \ldots$. Si l'on nomme s l'un quelconque des termes de la série (11), le produit

$$sPs^{-1}$$

représentera certainement une substitution qui, étant semblable à P, n'altérera pas Ω considéré comme fonction des n variables $x, y, z, \ldots$. Donc ce produit devra se réduire à l'une des substitutions

$$P,\quad P',\quad P'',\quad \ldots;$$

en sorte qu'on aura

$$(12)\qquad sPs^{-1} = Q,$$

Q désignant encore un terme de la série (3), mais un terme tel que la variable x appartienne à des facteurs circulaires du même ordre dans les deux substitutions P et Q. Donc on pourra déterminer s à l'aide d'une équation symbolique de la forme

$$s = \left(\frac{Q}{P}\right),$$

en suivant la règle établie par le théorème dont voici l'énoncé :

Théorème III. — *Soit Ω une fonction de n variables $x, y, z, \ldots$. Soient encore* P *l'une des substitutions qui déplacent toutes ces variables, sans altérer la valeur de Ω, et*

$$(13)\qquad P,\quad Q,\quad R,\quad \ldots$$

les diverses substitutions qui, étant toutes semblables à P *et douées de la même propriété, présentent toutes la variable x dans des facteurs circulaires de même ordre. Soit enfin*

$$1,\quad \mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots$$

le système des substitutions conjuguées qui, en laissant la variable x immobile, n'altèrent pas la valeur de Ω, considéré comme fonction des $n-1$ variables $y, z, \ldots$. L'une quelconque s des substitutions

$$\mathfrak{P},\quad \mathfrak{Q},\quad \mathfrak{R},\quad \ldots$$

pourra se déduire de la substitution P *comparée à un certain terme de la suite* (13), *et sera donnée en conséquence par une équation de la forme*

$$s = \binom{Q}{P}, \tag{14}$$

pourvu que, après avoir exprimé les deux substitutions P, Q *à l'aide de leurs facteurs circulaires, et assigné les mêmes places, dans les deux substitutions, non seulement aux facteurs circulaires de même ordre, mais encore à la variable* x, *on réduise* P *et* Q *à de simples arrangements par la suppression des parenthèses et des virgules interposées entre les diverses variables. Ajoutons que l'on pourra prendre pour* Q, *ou un terme de la série* (13), *distinct de* P, *ou même une seconde forme de la substitution* P, *distincte de la première.*

Corollaire I. — Les formules (12) et (14) établissent des relations remarquables entre les substitutions

$$\mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots,$$

qui, sans altérer une fonction Ω de n variables $x, y, z, \ldots$, déplacent seulement quelques-unes de ces variables, en laissant x immobile, et les substitutions

$$P,\ Q,\ R,\ \ldots,$$

qui, étant semblables entre elles, et renfermant toutes la variable x dans des facteurs circulaires de même ordre, déplacent, sans altérer Ω, toutes les variables. Ces deux espèces de substitutions se trouvent tellement liées les unes aux autres que, étant données les substitutions $\mathfrak{P}, \mathfrak{Q}, \mathfrak{R}, \ldots$, avec l'une des substitutions

$$P,\ Q,\ R,\ \ldots,$$

on peut déterminer le système de ces dernières, ou du moins plusieurs d'entre elles, à l'aide de la formule (12). Lorsqu'au contraire on donne les substitutions

$$P,\ Q,\ R,\ \ldots,$$

les valeurs de s, déterminées par la formule (14), sont les divers

termes d'une suite dans laquelle se trouvent nécessairement comprises les substitutions $\mathfrak{P}, \mathfrak{Q}, \mathfrak{R}, \ldots$.

Corollaire II. — Lorsque P représente une substitution circulaire de l'ordre n, exprimée à l'aide des variables écrites l'une après l'autre et séparées par des virgules, il est impossible de donner à P une seconde forme semblable à la première et distincte de la première, sans déplacer x. Donc alors on ne peut supposer $Q = P$ dans l'équation (12) ou (14), sans réduire s à l'unité. Il y a plus : lorsque P représentera une substitution circulaire de l'ordre n, les formes des substitutions

$$P,\ Q,\ R,\ \ldots$$

seront complètement déterminées si, dans chacune d'elles, on assigne à la variable x une place déterminée, la première place par exemple. Donc alors la formule (14) fournira pour chaque valeur de Q une seule valeur de s; mais, Q venant à varier, s variera nécessairement. En conséquence, on peut énoncer la proposition suivante :

Théorème IV. — *Soit* Ω *une fonction de* n *variables indépendantes* $x, y, z, \ldots$. *Supposons d'ailleurs que certaines substitutions circulaires de l'ordre* n *n'altèrent pas la valeur de* Ω, *et soient*

$$P,\ Q,\ R,\ \ldots$$

les substitutions circulaires de l'ordre n *qui jouissent de cette propriété. Si, après avoir représenté chacune d'elles à l'aide des diverses variables séparées par des virgules, en assignant toujours la première place à la variable* x, *on réduit* P, Q, R, ... *à de simples arrangements, les divers termes de la suite*

$$\binom{P}{P} = 1,\quad \binom{Q}{P},\quad \binom{R}{P},\quad \ldots \tag{15}$$

seront tous distincts les uns des autres, et cette même suite renfermera toutes les substitutions

$$1,\ \mathfrak{P},\ \mathfrak{Q},\ \mathfrak{R},\ \ldots$$

qui, sans altérer Ω, *déplaceront seulement les* $n-1$ *variables* $y, z, \ldots$, *ou quelques-unes d'entre elles, en laissant immobile la variable* x.

Supposons à présent que, P, $\mathfrak{P}$ étant toujours deux substitutions qui n'altèrent pas la valeur de Ω, la lettre P représente, ou une substitution circulaire de l'ordre n, ou même l'une quelconque des substitutions qui déplacent la variable x. Supposons, au contraire, que $\mathfrak{P}$, étant une substitution circulaire de l'ordre $n-1$, déplace seulement les $n-1$ variables $y, z, \ldots$; et, en désignant par l un nombre entier quelconque, posons

$$P_l = \mathfrak{P}^l P \mathfrak{P}^{-l}. \tag{16}$$

En vertu de la formule (16), P_l reprendra toujours la même valeur quand on fera croitre ou décroitre l d'un multiple de $n-1$, en sorte qu'on aura, par exemple,

$$\begin{array}{l} P_0 \;\; = P_{n-1} = P_{2(n-1)} = \ldots = P, \\ P_1 \;\; = P_n \;\; = P_{2n-1} \;= \ldots = \mathfrak{P} P \mathfrak{P}^{-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ P_{n-2} = P_{2n-3} = P_{3n-4} \;= \ldots = \mathfrak{P}^{n-2} P \mathfrak{P}^{-n+2}. \end{array}$$

De plus, les divers termes de la suite

$$P_0 = P,\; P_1,\; P_2,\; \ldots,\; P_{n-2} \tag{17}$$

seront certainement distincts les uns des autres. En effet, nommons s la variable dont x prend la place quand on effectue la substitution P. Cette variable s se trouvera remplacée, dans les divers termes de la série (17), par les diverses variables qui succèdent à s quand on effectue les substitutions

$$1,\; \mathfrak{P},\; \mathfrak{P}^2,\; \ldots,\; \mathfrak{P}^{n-2}. \tag{18}$$

Mais, $\mathfrak{P}$ étant, par hypothèse, une substitution circulaire de l'ordre $n-1$, les variables qui succéderont à s en vertu des substitutions (18) se confondront respectivement avec les $n-1$ variables que renferme la substitution $\mathfrak{P}$, c'est-à-dire avec les variables $y, z, \ldots$ écrites à la suite l'une de l'autre, dans l'ordre qu'indique la substitution $\mathfrak{P}$, quand on assigne la première place à la variable s. Donc les

deux variables dont x viendra prendre la place dans deux des substitutions

$$P_0,\; P_1,\; P_2,\; \ldots,\; P_{n-2}$$

seront toujours deux variables distinctes; et il est clair qu'on pourrait en dire autant de deux variables qui succéderaient à x dans deux de ces mêmes substitutions. Donc la série (17) n'offrira pas de termes égaux. Cela posé, désignons, comme ci-dessus, par

$$1,\; \mathfrak{P},\; \mathfrak{Q},\; \mathfrak{R},\; \ldots \tag{11}$$

le système des substitutions conjuguées qui, en laissant immobile la variable x, déplacent seulement les variables $y, z, \ldots$ ou quelques-unes d'entre elles, sans altérer la valeur de Ω. Les divers termes compris dans le Tableau

$$\left\{\begin{array}{lllll} 1, & \mathfrak{P}, & \mathfrak{Q}, & \mathfrak{R}, & \ldots, \\ P, & \mathfrak{P}P, & \mathfrak{Q}P, & \mathfrak{R}P, & \ldots, \\ P_1, & \mathfrak{P}P_1, & \mathfrak{Q}P_1, & \mathfrak{R}P_1, & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots, \\ P_{n-2}, & \mathfrak{P}P_{n-2}, & \mathfrak{Q}P_{n-2}, & \mathfrak{R}P_{n-2}, & \ldots \end{array}\right. \tag{19}$$

seront nécessairement distincts les uns des autres. Car, si l'on suppose égaux entre eux deux termes de ce Tableau représentés par les produits

$$\mathfrak{S}P_l,\quad \mathfrak{T}P_{l'},$$

dans lesquels $\mathfrak{S}$, $\mathfrak{T}$ désignent deux termes de la suite (11), l'équation

$$\mathfrak{S}P_l = \mathfrak{T}P_{l'} \tag{20}$$

entrainera la formule

$$\mathfrak{T}^{-1}\mathfrak{S} = P_{l'} P_l^{-1};$$

et, comme le premier membre de cette formule sera encore un terme de la suite (11), c'est-à-dire une substitution en vertu de laquelle x restera immobile, le second membre devra remplir la même condition. Donc, si l'on conçoit que x succède à s en vertu de la substitution P_l, et par conséquent s à x en vertu de la substitution inverse P_l^{-1}, la substitution $P_{l'}$ devra ramener x à la place de s, ce qui suppose $l' = l$, et, par suite,

$$P_{l'} = P_l.$$

Mais, lorsque cette dernière condition sera remplie, l'équation (20) donnera

$$\mathcal{S} = \mathcal{T},$$

et par conséquent elle ne pourra être admise si l'on suppose $\mathcal{T}$ distinct de $\mathcal{S}$. Ce n'est pas tout : on prouvera encore de la même manière que les divers termes du Tableau

$$(21)\qquad \begin{cases} 1, & \mathfrak{P}, & \mathfrak{Q}, & \mathfrak{R}, & \ldots, \\ P, & P\mathfrak{P}, & P\mathfrak{Q}, & P\mathfrak{R}, & \ldots, \\ P_1, & P_1\mathfrak{P}, & P_1\mathfrak{Q}, & P_1\mathfrak{R}, & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots, \\ P_{n-2}, & P_{n-2}\mathfrak{P}, & P_{n-2}\mathfrak{Q}, & P_{n-2}\mathfrak{R}, & \ldots \end{cases}$$

seront tous distincts les uns des autres. Enfin, l'on peut affirmer que l'un quelconque des termes du Tableau (19) se confondra toujours avec l'un des termes du Tableau (21), c'est-à-dire que, l étant un nombre entier quelconque, et $\mathcal{S}$ l'une quelconque des substitutions (11), on pourra choisir un autre nombre entier l' et une autre substitution $\mathcal{T}$ prise dans la série (11), de manière à vérifier l'équation linéaire

$$(22)\qquad P_{l'}\mathcal{T} = \mathcal{S} P_l.$$

Effectivement, nommons s la variable qui succède à x, en vertu de la substitution $\mathcal{S} P_l$. La substitution $\mathcal{T}$, déterminée par la formule (22), savoir

$$(23)\qquad \mathcal{T} = P_{l'}^{-1} \mathcal{S} P_l,$$

ramènera certainement x à la place que cette variable occupait primitivement dans la fonction Ω, si l'on prend pour $P_{l'}$ celle des substitutions (17) qui fait succéder s à x, puisque alors la substitution inverse $P_{l'}^{-1}$ aura pour effet de faire succéder x à s. Donc alors la

valeur de $\mathcal{T}$, déterminée par la formule (23), sera, non seulement une dérivée des substitutions (11) et (17), par conséquent l'une des substitutions qui n'altèrent pas Ω, mais encore l'une de celles qui laissent immobile la variable x. Elle se réduira donc à l'un des termes de la série (17). On peut donc énoncer encore la proposition suivante :

THÉORÈME V. — *Soient Ω une fonction de n variables indépendantes x, y, z, ..., et*

$$P, \quad \mathfrak{P}$$

deux substitutions qui n'altèrent pas sa valeur. Supposons, d'ailleurs, que la substitution P, étant régulière ou irrégulière, déplace la variable x, et que la substitution $\mathfrak{P}$, étant circulaire, déplace les $n-1$ variables y, z, ... en laissant immobile la variable x. Enfin, posons généralement

$$\mathfrak{P}_l = \mathfrak{P}^l P \mathfrak{P}^{-l},$$

l étant un nombre entier quelconque, et nommons

$$1, \quad \mathfrak{P}, \quad \mathfrak{Q}, \quad \mathfrak{R}, \quad \ldots$$

le système des substitutions conjuguées qui, sans altérer Ω, déplacent les $n-1$ variables y, z, ..., ou quelques-unes d'entre elles. Non seulement les $n-1$ termes de la suite

$$P_0 = P, \ P_1, \ P_2, \ \ldots, \ P_{n-2},$$

qui représenteront des substitutions semblables entre elles, seront tous distincts les uns des autres, mais on pourra en dire autant des divers termes du Tableau (19) et des divers termes du Tableau (21); et, par conséquent, si l'on nomme $\mathcal{S}$ un terme quelconque de la série (11), toute substitution de la forme

$$\mathcal{S} P_l$$

sera en même temps un terme de la forme

$$P_l \mathcal{S}.$$

Corollaire I. — Soit $\mathfrak{M}$ le nombre des termes de la série (11). Le nombre des termes compris dans chacun des Tableaux (19), (21) sera évidemment représenté par le produit

$$n\mathfrak{M}.$$

Corollaire II. — Dans le cas où, comme nous le supposons ici, Ω n'est altéré, ni par une substitution P qui déplace la variable x, ni par une substitution circulaire du degré $n-1$, en vertu de laquelle x demeure immobile, Ω est nécessairement une fonction transitive de n et même de $n-1$ variables. Donc alors le nombre M des valeurs égales de Ω, ou, ce qui revient au même, le nombre M des substitutions

$$(3) \qquad 1, \ P, \ Q, \ R, \ U, \ V, \ W$$

qui n'altèrent pas Ω est déterminé par la formule

$$M = n\mathfrak{M},$$

et ces substitutions se réduisent aux divers termes de chacun des Tableaux (19), (21). Donc alors aussi les substitutions (2) se réduisent aux dérivées de la substitution P, jointe aux substitutions conjuguées

$$(11) \qquad 1, \ \mathfrak{P}, \ \mathfrak{Q}, \ \mathfrak{R}, \ \ldots$$

qui n'altèrent pas Ω considéré comme fonction des $n-1$ variables $y, z, \ldots$.

Corollaire III. — Lorsque, Ω étant une fonction transitive de n et même de $n-1$ variables, $n-1$ est un nombre premier, alors, parmi les substitutions qui, sans altérer Ω, déplacent $n-1$ variables, se trouvent nécessairement des substitutions circulaires de l'ordre $n-1$. Donc alors les substitutions qui n'altèrent pas Ω se réduisent aux dérivées des substitutions diverses qui laissent la variable x immobile, et d'une seule substitution prise parmi celles qui déplacent la variable x.

§ II. — *Sur le nombre des substitutions qui n'altèrent pas une fonction de plusieurs variables indépendantes.*

Soient

Ω une fonction transitive de n variables $x, y, z, \ldots$;
m le nombre de ses valeurs distinctes $\Omega, \Omega', \Omega'', \ldots$;
M le nombre de ses valeurs égales.

Soient encore

P l'une des substitutions qui n'altèrent pas la valeur de Ω;
ϖ le nombre des substitutions semblables à P qui peuvent être formées avec les variables $x, y, z, \ldots$;
h le nombre des substitutions semblables à P qui n'altèrent pas la valeur de Ω;
k le nombre de celles des fonctions $\Omega, \Omega', \Omega'', \ldots$ qui ne sont pas altérées par la substitution P.

Comme nous l'avons vu dans le précédent Mémoire, on aura, non seulement

$$(1) \qquad mM = N,$$

la valeur de N étant

$$N = 1.2.3\ldots n,$$

mais encore

$$(2) \qquad M = \Sigma h,$$

la somme qu'indique le signe Σ s'étendant aux divers systèmes de substitutions semblables entre elles, et

$$(3) \qquad hm = k\varpi.$$

Soit maintenant r le nombre des variables qui restent immobiles quand on effectue la substitution P; soient encore

$$a, \ b, \ c, \ \ldots$$

les nombres égaux ou inégaux qui représentent les ordres des divers facteurs circulaires de cette substitution réduite à sa plus simple expression. Enfin, pour mieux indiquer la forme de cette substitution à laquelle se rapportent les quantités exprimées par les lettres

$$\varpi,\quad h,\quad k,\quad \ldots,$$

plaçons au bas de ces lettres, comme indices, les nombres a, b, c, ..., en écrivant

$$\varpi_{a,b,c,\ldots},\quad h_{a,b,c,\ldots},\quad k_{a,b,c,\ldots}$$

au lieu de ϖ, h, k. Si l'on nomme H_{n-r} le nombre total des substitutions qui, sans altérer Ω, déplacent $n-r$ variables, en laissant les r autres variables immobiles, on aura

$$H_{n-r} = \Sigma h_{a,b,c,\ldots}, \tag{4}$$

la somme qu'indique le signe Σ s'étendant à toutes les valeurs de $a, b, c, \ldots$, égales ou inégales, mais supérieures à l'unité, qui vérifient l'équation

$$a+b+c+\ldots = n-r. \tag{5}$$

Cela posé, la formule (2) donnera simplement

$$M = \Sigma H_{n-r}, \tag{6}$$

la somme qu'indique le signe Σ s'étendant à toutes les valeurs de r comprises dans la suite

$$0,\quad 1,\quad 2,\quad \ldots,\quad n-1,\quad n,$$

et les valeurs de H_0, H_1 étant respectivement

$$H_0 = 1,\qquad H_1 = 0.$$

Quant à la formule (3), elle deviendra

$$h_{a,b,c,\ldots}\, m = k_{a,b,c,\ldots}\, \varpi_{a,b,c,\ldots}. \tag{7}$$

Lorsque Ω est une fonction transitive de n, de $n-1$, de $n-2$, ..., et même de $n-l+1$ variables, on peut aux formules (4), (6) et (7) joindre les formules analogues qu'on obtient en considérant Ω comme

fonction de $n-1$, de $n-2$, ou de $n-l$ variables seulement. Dans ces nouvelles formules, analogues aux premières, les quantités

$$m \quad \text{et} \quad k_{a,b,c,\ldots}$$

conservent toujours les valeurs qu'elles avaient dans les équations (4), (6) et (7). Mais il n'en est plus de même des quantités

$$M,\quad H_{n-r},\quad h_{a,b,c,\ldots},\quad \varpi_{a,b,c,\ldots},$$

dont les valeurs sont modifiées. Si, pour fixer les idées, on veut passer des formules (4), (6) et (7) aux formules analogues, qu'on obtiendra en considérant Ω comme fonction de $n-l$ variables, on devra, dans les formules (4), (6) et (7), diviser M par le produit

$$n(n-1)\ldots(n-l+1),$$

et

$$H_{n-r},\quad h_{a,b,c,\ldots},\quad \varpi_{a,b,c,\ldots}$$

par le nombre entier θ_{n-r}, que détermine la formule

$$\theta_{n-r} = \frac{n(n-1)\ldots(n-l+1)}{r(r-1)\ldots(r-l+1)}. \tag{8}$$

Ajoutons que les quotients ainsi obtenus devront encore être des nombres entiers.

Dans un prochain article, je donnerai de nombreuses applications des principes établis dans le présent Mémoire et dans ceux qui l'ont précédé. Je ferai voir, en particulier, comment, à l'aide de ces principes, on parvient à constater, non seulement l'existence de la fonction transitive Ω de six variables

$$x,\quad y,\quad z,\quad u,\quad v,\quad w,$$

qui offre cent vingt valeurs égales, par conséquent six valeurs distinctes, et que l'on peut caractériser en disant qu'elle n'est pas altérée par les dérivées des trois substitutions circulaires

$$P = (x, y, z, u, v, w),\qquad Q = (z, y, u, w, v),\qquad R = (y, z, w, v),$$

ou, ce qui revient au même, par les dérivées des deux substitutions P et Q, ou P et R, mais encore l'existence d'une autre fonction transitive des mêmes variables, qui offre soixante valeurs égales, par conséquent douze valeurs distinctes, et que l'on peut caractériser en disant qu'elle n'est pas altérée par les dérivées des trois substitutions régulières

$$P^2 = (x, z, v)(y, u, w), \qquad Q = (z, y, u, w, v), \qquad R^2 = (y, w)(z, v)$$

ou, ce qui revient au même, par les dérivées des deux substitutions P^2 et Q.

318.

Analyse mathématique. — *Applications diverses des principes établis dans les précédents Mémoires.*

C. R., T. XXI, p. 1356 (22 décembre 1845).

§ I. — *Considérations générales.*

Je vais, dans ce paragraphe, rappeler d'abord en peu de mots quelques-unes des formules établies dans les précédents Mémoires, et particulièrement celles qui servent à déterminer le nombre des valeurs que peut acquérir une fonction transitive ou intransitive de plusieurs variables.

Soient

Ω une fonction de n variables $x, y, z, \ldots$;
M le nombre de ses valeurs égales, et
m le nombre de ses valeurs distinctes, lié au nombre M par la formule

$$mM = N, \tag{1}$$

dans laquelle

$$N = 1.2.3\ldots n$$

représente le nombre des arrangements divers que l'on peut former avec n lettres.

Si la fonction Ω est intransitive, on pourra partager les variables

$x, y, z, \ldots$ en divers groupes, en s'astreignant à la seule condition de réunir toujours dans un même groupe deux variables dont l'une prendra la place de l'autre, en vertu d'une substitution qui n'altérera pas la valeur de Ω. Il pourra d'ailleurs arriver que certains déplacements de variables comprises dans certains groupes entraînent des déplacements correspondants de variables comprises dans d'autres groupes, en sorte qu'on soit obligé, pour ne pas altérer Ω, d'effectuer simultanément ces deux espèces de déplacements. Cela posé, soient

a le nombre des variables comprises dans le premier groupe;
b le nombre des variables comprises dans le second groupe;
c le nombre des variables comprises dans le troisième groupe;
Etc., et

r le nombre des variables dont chacune forme un groupe à elle seule, c'est-à-dire le nombre des variables qui ne peuvent être déplacées sans que la valeur de Ω soit altérée;

Soient de plus

A le nombre des valeurs égales que peut acquérir Ω en vertu de substitutions correspondantes à des arrangements divers des variables comprises dans le premier groupe;
B le nombre des valeurs égales que peut acquérir Ω en vertu de substitutions qui, sans déplacer les variables du premier groupe, correspondent à des arrangements divers des variables comprises dans le second groupe;
C le nombre des valeurs égales que peut acquérir Ω en vertu de substitutions qui, sans déplacer les variables des deux premiers groupes, correspondent à des arrangements divers des variables comprises dans le troisième groupe;
Etc.

On aura, non seulement

$$a + b + c + \ldots + r = n, \tag{2}$$

mais encore (séance du 22 septembre)

$$M = ABC\ldots, \tag{3}$$

et par suite, si l'on pose

$$\mathcal{N} = \frac{1.2.3\ldots n}{(1.2\ldots a)(1.2\ldots b)\ldots(1.2\ldots r)}, \tag{4}$$

$$\mathcal{A} = \frac{1.2\ldots a}{A}, \qquad \mathcal{B} = \frac{1.2\ldots b}{B}, \qquad \ldots, \tag{5}$$

la formule (3), jointe à l'équation (1), donnera

$$m = \mathcal{N}\mathcal{A}\mathcal{B}\mathcal{C}\ldots. \tag{6}$$

Il est bon de rappeler ici que le nombre désigné par $\mathcal{N}$ dans l'équation (6) est précisément le coefficient du produit

$$s^a t^b \ldots$$

dans le développement de l'expression

$$(1 + s + t + \ldots)^n.$$

Lorsque chacun des groupes auxquels se rapporte la formule (6) renferme le plus petit nombre possible de variables, alors deux variables comprises dans un même groupe sont toujours deux variables dont l'une peut passer à la place de l'autre, sans que la valeur de Ω soit altérée. Mais il n'est point nécessaire que cette dernière condition soit remplie; et, si, après avoir distribué les variables en groupes, de manière à la vérifier, on réunit plusieurs groupes en un seul, la formule (6) continuera de subsister. C'est ce qui arrivera en particulier si l'on réduit le système des variables comprises dans les second, troisième, quatrième, ... groupes à un groupe unique composé de $b + c + \ldots$ variables. Si, dans cette même hypothèse, le premier groupe ne renferme qu'une seule variable x, on aura

$$\mathcal{N} = n, \qquad \mathcal{A} = 1,$$

et la formule (6) donnera

$$m = n\mathcal{B}, \tag{7}$$

$\mathcal{B}$ étant le nombre des valeurs distinctes de Ω considéré comme fonction des $n - 1$ variables $y, z, \ldots$. En conséquence, on pourra énoncer la proposition suivante :

THÉORÈME I. — *Si une fonction de n variables $x, y, z, \ldots$ est toujours altérée quand on déplace une certaine variable x, le nombre des valeurs distinctes de Ω considéré comme fonction de $x, y, z, \ldots$ sera le produit de n par le nombre des valeurs distinctes de Ω considéré comme fonction des $n - 1$ variables $y, z, \ldots$.*

Si les groupes formés avec les diverses variables sont indépendants les uns des autres, en sorte que des déplacements, simultanément effectués dans les divers groupes, en vertu d'une substitution qui n'altère pas la valeur de Ω, puissent aussi s'effectuer séparément, sans altération de cette valeur, alors chacune des quantités désignées par $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ dans la formule (6) représentera précisément le nombre des valeurs distinctes de Ω considéré comme fonction des seules variables comprises dans le premier groupe, ou dans le second, ou dans le troisième, ... Il suit d'ailleurs des principes établis dans la séance du 6 octobre (pages 336 et suivantes), que l'on pourra effectivement trouver une fonction Ω qui offre un nombre de valeurs déterminé par la formule (6), si l'on peut former

avec a lettres, une fonction qui offre $\mathcal{A}$ valeurs distinctes;
avec b lettres, une fonction qui offre $\mathcal{B}$ valeurs distinctes;
....

En conséquence, on peut énoncer la proposition suivante :

THÉORÈME II. — *Supposons que l'on partage arbitrairement les n variables $x, y, z, \ldots$ en plusieurs groupes dont chacun renferme une ou plusieurs variables. Soient respectivement*

$$a, \quad b, \quad c, \quad \ldots$$

les nombres de variables comprises dans le premier, le second, le troisième, ... groupe, et nommons $\mathcal{N}$ le coefficient du produit

$$s^a t^b \ldots$$

dans le développement de l'expression

$$(1 + s + t + \ldots)^n.$$

Si l'on peut former

> avec a lettres une fonction qui offre $\mathcal{A}$ valeurs distinctes;
> avec b lettres une fonction qui offre $\mathcal{B}$ valeurs distinctes;
> avec c lettres une fonction qui offre $\mathcal{C}$ valeurs distinctes;
> ....

on pourra former avec les n variables données une fonction intransitive qui offrira m valeurs distinctes, la valeur de m étant déterminée par la formule

$$m = \mathcal{N}\mathcal{A}\mathcal{B}\mathcal{C}\ldots.$$

Corollaire I. — Il résulte des principes établis dans la séance du 22 septembre que le nombre des valeurs distinctes d'une fonction intransitive de n variables $x, y, z, \ldots$ est toujours une des valeurs de m que fournit le théorème précédent, non seulement dans le cas où les groupes formés avec ces variables sont tous indépendants les uns des autres, mais aussi dans le cas contraire.

Corollaire II. — Si l'on suppose que les groupes se réduisent à deux, et que le premier groupe, étant indépendant du second, renferme seulement une, ou deux, ou trois, ... variables, alors, à la place du théorème I, on obtiendra la proposition suivante :

Théorème III. — *Avec n variables $x, y, z, \ldots$, on peut toujours former une fonction intransitive qui offre m valeurs distinctes, m étant le produit de n par l'un quelconque des entiers propres à représenter le nombre des valeurs distinctes d'une fonction de $n - 1$ variables, ou le produit du nombre triangulaire $\frac{n(n-1)}{2}$ par l'un des facteurs 1, 2 et par l'un quelconque des entiers propres à représenter le nombre des valeurs distinctes d'une fonction de $n - 2$ variables, ou le produit du nombre pyramidal $\frac{n(n-1)(n-2)}{1.2.3}$ par l'un des facteurs 1, 2, 3, 6 et par l'un quelconque des entiers propres à représenter le nombre des valeurs distinctes d'une fonction de $n - 3$ variables, etc.*

Supposons maintenant que la fonction Ω cesse d'être intransitive et devienne transitive. Alors, en joignant à des résultats déjà connus ceux que nous avons trouvés dans les précédents Mémoires, on obtiendra les propositions suivantes :

Théorème IV. — *Si Ω est une fonction transitive de n variables $x, y, z, \ldots$, le nombre m des valeurs distinctes de Ω considéré comme fonction de ces n variables sera encore le nombre m des valeurs distinctes de Ω considéré comme fonction des $n - 1$ variables $y, z, \ldots$.*

Théorème V. — *Avec un nombre quelconque n de variables, on peut toujours former, non seulement des fonctions symétriques dont chacune offrira une seule valeur distincte, mais encore des fonctions dont chacune offre seulement deux valeurs distinctes.*

Corollaire I. — Parmi les fonctions qui offrent deux valeurs distinctes, on doit distinguer la fonction *alternée*, dont les deux valeurs sont égales au signe près, mais affectées de signes contraires. Telle est, en particulier, la fonction de n variables $x, y, z, \ldots$, qui se trouve représentée par le produit

$$\Pi = (x - y)(x - z)\ldots(y - z)\ldots, \tag{8}$$

dont les facteurs sont des différences entre ces variables rangées dans un ordre quelconque, et combinées deux à deux de toutes les manières possibles.

Corollaire II. — Si, Ω étant une fonction de $x, y, z, \ldots$ qui offre seulement deux valeurs distinctes

$$\Omega, \quad \Omega',$$

on pose

$$U = \frac{\Omega + \Omega'}{2}, \qquad V = \frac{\Omega - \Omega'}{2\Pi}, \tag{9}$$

la valeur de Π étant déterminée par l'équation (8), alors

$$U \text{ et } V$$

seront évidemment deux fonctions symétriques de $x, y, z, \ldots$. Or des formules (9) on déduit immédiatement l'équation

$$\Omega = \mathrm{U} + \mathrm{VII}, \tag{10}$$

qui, comme Abel en a fait la remarque, détermine la forme générale des fonctions dont les valeurs distinctes sont au nombre de deux seulement. Il est d'ailleurs évident que toute valeur de Ω, déterminée par l'équation (10), sera une fonction qui offrira seulement deux valeurs distinctes.

Corollaire III. — Eu égard au théorème V, le théorème III comprend, comme cas particulier, une proposition énoncée par M. Bertrand, savoir, qu'avec n variables on peut toujours composer une fonction qui offre $2n$ valeurs distinctes.

Théorème VI. — *Soient*

n un nombre entier quelconque;
I l'indicateur maximum correspondant au module n;
ν un diviseur quelconque de n;
ι un diviseur quelconque de I.

On pourra toujours, avec n lettres $x, y, z, \ldots$, former une fonction transitive Ω qui offre m valeurs distinctes, la valeur de m étant déterminée par la formule

$$m = \frac{1.2.3\ldots(n-1)}{I}, \tag{11}$$

ou même, plus généralement, par la formule

$$m = \frac{1.2.3\ldots(n-1)}{I}\nu\iota \tag{12}$$

(*voir* la séance du 6 octobre, page 341).

On peut encore, des principes établis dans les séances du 22 septembre et du 6 octobre, déduire immédiatement la proposition suivante :

Théorème VII. — *Soit*

$$n = la$$

un nombre entier, non premier, et par conséquent décomposable en deux

facteurs l, a, dont aucun ne se réduit à l'unité. Si l'on peut former avec a lettres une fonction qui offre $\mathcal{A}$ valeurs distinctes, et avec l lettres une fonction qui offre $\mathcal{L}$ valeurs distinctes, on pourra former, avec n lettres, une fonction transitive complexe qui offrira m valeurs distinctes, la valeur de m étant déterminée par la formule

$$m = \mathcal{N}\mathcal{L}\mathcal{A}^l, \tag{13}$$

dans laquelle on suppose

$$\mathcal{N} = \frac{1.2.3\ldots n}{(1.2\ldots l)(1.2\ldots a)^l}. \tag{14}$$

§ II. — *Recherche du nombre des valeurs que peut acquérir une fonction transitive ou intransitive qui ne renferme pas plus de six variables.*

Fonctions de deux variables.

Si Ω est une fonction de deux variables x, y, le nombre m de ses valeurs distinctes devra être un diviseur du produit

$$N = 1.2 = 2.$$

Ce nombre ne pourra donc être que 1 ou 2. On aura effectivement

$m = 2$ si la fonction est intransitive,
$m = 1$ si elle est symétrique, et par conséquent transitive.

Fonctions de trois variables.

Si Ω est une fonction de trois variables x, y, z, le nombre m de ses valeurs distinctes devra être un diviseur du produit

$$N = 1.2.3 = 6.$$

Ce nombre ne pourra donc être que l'un des termes de la suite

$$1, \quad 2, \quad 3, \quad 6.$$

D'ailleurs, il pourra être l'un quelconque d'entre eux. En effet, si la fonction Ω est supposée intransitive, alors, en vertu du théorème III du § I, m pourra être le produit du facteur 3 par l'un quelconque des nombres 1, 2; en sorte qu'on pourra supposer

$$m=3 \quad \text{ou} \quad m=6.$$

Si, au contraire, la fonction Ω est supposée transitive, elle pourra offrir, comme toute fonction d'un nombre quelconque de variables (*voir* le théorème V du § I), une ou deux valeurs distinctes. C'est ce que prouve aussi le théorème VI du § I; car, lorsqu'on suppose $n=3$, l'indicateur maximum I se réduit au nombre 2, et alors les formules (11) et (12) du § I donnent

$$m=\frac{1.2}{2}=1, \quad m=1.2=2.$$

Fonctions de quatre variables.

Si Ω est une fonction de quatre variables

$$x, \ y, \ z, \ u,$$

le nombre m de ses valeurs distinctes sera un diviseur du produit

$$N=1.2.3.4=24.$$

Ce nombre ne pourra donc être que l'un des termes de la suite

$$1, \ 2, \ 3, \ 4, \ 6, \ 8, \ 12, \ 24.$$

D'ailleurs, il pourra être l'un quelconque de ces termes, ainsi que nous allons l'expliquer.

D'abord, si la fonction Ω est supposée intransitive, alors, en vertu du théorème III du § I, le nombre m pourra être le produit du facteur 4 par l'un des nombres

$$1, \ 2, \ 3, \ 6,$$

ou le produit du facteur $6=\frac{4.3}{1.2}$ par l'un des nombres

$$1, \ 2,$$

ou par le carré de l'un d'entre eux. On pourra donc alors réduire m à

l'un quelconque des termes de l'une des deux suites

$$4, \ 8, \ 12, \ 24,$$
$$6, \ 12, \ 24,$$

c'est-à-dire que l'on pourra prendre pour m l'un quelconque des nombres

$$4, \ 6, \ 8, \ 12, \ 24.$$

En second lieu, si la fonction Ω est supposée transitive, on pourra, en vertu du théorème V du § I, supposer

$$m=1 \quad \text{ou} \quad m=2.$$

Il y a plus : comme l'indicateur maximum I correspondant au module 4 est le nombre 2, on pourra, en vertu du théorème VI du § I, réduire la valeur de m à celle que détermine l'une des formules

$$m=\frac{1.2.3}{2}=3, \quad m=1.2.3=6.$$

On pourra donc former une fonction transitive de trois variables qui offre seulement trois ou six valeurs distinctes.

Il est bon d'observer que, parmi les fonctions de quatre variables, celle qui, n'étant pas altérée par une substitution régulière du second ordre, c'est-à-dire par une substitution de la forme

$$(x, y)(z, u),$$

offre douze valeurs distinctes, est la seule qui présente les quatre variables partagées en deux groupes dépendants l'un de l'autre, non permutables entre eux, et composés chacun de variables que l'on puisse échanger entre elles sans altérer la valeur de la fonction.

Fonctions de cinq variables.

Si Ω est une fonction des cinq variables

$$x, \ y, \ z, \ u, \ v,$$

le nombre m de ses valeurs distinctes devra être un diviseur du produit

$$1.2.3.4.5=120.$$

Ce nombre ne pourra donc être que l'un des termes de l'une des suites

$$1,\quad 2,\quad 3,\quad 4,\quad 6,\quad 8,\quad 12,\quad 24,$$
$$5,\quad 10,\quad 15,\quad 20,\quad 30,\quad 40,\quad 60,\quad 120,$$

dont on obtient la seconde en multipliant les termes de la première par le facteur 5. Il reste à examiner quels sont les termes de ces deux suites qui pourront effectivement représenter le nombre des valeurs distinctes d'une fonction de cinq variables.

D'abord, si la fonction Ω est supposée intransitive, alors, en vertu du théorème III du § I, on pourra prendre pour m un terme quelconque de la seconde suite.

En second lieu, si Ω est une fonction transitive des cinq variables x, y, z, u, v, elle ne pourra être en même temps intransitive par rapport à quatre variables y, z, u, v que dans le cas où ces quatre variables resteront immobiles ou pourront être partagées en deux groupes dépendants l'un de l'autre, mais non permutables entre eux (séance du 29 septembre, pages 317 et suivantes), et composés chacun de variables que l'on puisse échanger entre elles sans altérer la valeur de Ω, par conséquent, dans le cas où le nombre des valeurs distinctes de Ω considéré comme fonction de y, z, u, v serait déterminé par l'une des formules

$$m = 1.2.3.4 = 24, \qquad m = \frac{1.2.3.4}{2} = 12.$$

En troisième lieu, si Ω est une fonction transitive de cinq variables x, y, z, u, v, et même de quatre variables y, z, u, v, alors m devra se réduire au nombre des valeurs distinctes de Ω considéré comme fonction de trois variables z, u, v. Donc alors m ne pourra être que l'un des nombres

$$1,\quad 2,\quad 3,\quad 6.$$

Mais on ne pourra supposer le nombre m inférieur à 5, s'il est supérieur à 2 (séance du 17 novembre). Donc, si la fonction Ω est transitive par rapport à cinq et à quatre variables, m ne pourra être que l'un des nombres

$$1,\quad 2,\quad 6.$$

Ainsi donc, si Ω est une fonction transitive des cinq variables

$$x,\quad y,\quad z,\quad u,\quad v,$$

le nombre m des valeurs distinctes de Ω devra se réduire à l'un des nombres

$$1,\quad 2,\quad 6,\quad 12,\quad 24.$$

D'ailleurs, dans cette hypothèse, on pourra prendre effectivement, en vertu du théorème V du § I,

$$m = 1 \quad \text{ou} \quad m = 2,$$

et, en vertu du théorème VI,

$$m = \frac{1.2.3.4}{4} = 6$$

ou

$$m = \frac{1.2.3.4}{2} = 12,$$

ou même

$$m = 1.2.3.4 = 24.$$

Donc, en résumé, si Ω est une fonction transitive ou intransitive de cinq variables

$$x,\quad y,\quad z,\quad u,\quad v,$$

le nombre m de ses valeurs distinctes pourra être l'un quelconque des termes de la suite

$$1,\quad 2,\quad 5,\quad 6,\quad 10,\quad 12,\quad 15,\quad 20,\quad 24,\quad 30,\quad 40,\quad 60,\quad 120.$$

Fonctions de six variables.

Si Ω est une fonction de six variables

$$x,\quad y,\quad z,\quad u,\quad v,\quad w,$$

le nombre m de ses valeurs distinctes devra être un diviseur du produit

$$N = 1.2.3.4.5.6 = 720.$$

Mais, si l'on veut savoir quels diviseurs de ce produit pourront être pris pour m, on devra considérer les divers cas qui peuvent se présenter.

D'abord, si la fonction Ω est intransitive, alors, en vertu du théorème III du § I, on pourra prendre pour m, non seulement le produit du facteur 6 par l'un quelconque des entiers

$$1,\quad 2,\quad 5,\quad 6,\quad 10,\quad 12,\quad 15,\quad 20,\quad 24,\quad 30,\quad 40,\quad 60,\quad 120,$$

qui sont propres à représenter le nombre des valeurs distinctes d'une fonction de cinq variables, mais encore le produit du nombre triangulaire

$$\frac{6.5}{2} = 15$$

par l'un des facteurs 1, 2 et par l'un quelconque des entiers

$$1,\quad 2,\quad 3,\quad 4,\quad 6,\quad 8,\quad 12,\quad 24,$$

qui sont propres à représenter le nombre des valeurs distinctes d'une fonction de quatre variables, et enfin le produit du nombre pyramidal

$$\frac{6.5.4}{1.2.3} = 20$$

par deux des facteurs 1, 2, 3, 6, ou par le carré de l'un d'entre eux. Donc alors on pourra prendre pour m l'un quelconque des termes de la suite

$$6,\quad 12,\quad 15,\quad 20,\quad 30,\quad 36,\quad 40,\quad 45,\quad 60,\quad 72,\quad 80,\quad 90,\quad 120,\quad 144,$$
$$150,\quad 180,\quad 240,\quad 360,\quad 720.$$

En second lieu, si Ω est une fonction transitive complexe, dans laquelle les six variables x, y, z, u, v, w se partagent en deux groupes de trois lettres ou en trois groupes de deux lettres, qui puissent être échangés entre eux, mais qui soient indépendants les uns des autres, le nombre m des valeurs distinctes de Ω pourra être déterminé à l'aide de l'équation (13) du § I, par conséquent à l'aide des formules

$$m = \frac{1.2.3.4.5.6}{(1.2)(1.2.3)^2}\mathcal{A}^2 = 10\mathcal{A}^2, \qquad \mathcal{A} = 1,\ 2 \text{ ou } 3,$$

ou à l'aide des formules

$$m = \frac{1.2.3.4.5.6}{(1.2.3)(1.2)^3}\mathcal{L} = 15\mathcal{L}, \qquad \mathcal{L} = 1,\ 2 \text{ ou } 3.$$

Donc alors on pourra prendre pour m l'un quelconque des nombres entiers

$$10,\quad 15,\quad 30,\quad 40,\quad 45,\quad 90.$$

Si, Ω étant une fonction transitive complexe, les groupes dans lesquels les variables se partagent cessaient d'être indépendants les uns des autres, le nombre m des valeurs distinctes de Ω, déterminé à l'aide de la formule (7) de la page 312 (séance du 29 septembre), pourrait être l'un quelconque des nombres

$$60,\quad 120,\quad 180.$$

Enfin, si Ω est une fonction transitive, non complexe, des six variables x, y, z, u, v, w, ou elle sera intransitive par rapport à cinq variables, qui ne pourront être déplacées qu'avec la sixième, et alors, en vertu du théorème VI du § I, cette fonction offrira 120 valeurs distinctes, ou bien elle devra encore être transitive par rapport à cinq variables (séance du 29 septembre), attendu que cinq variables ne peuvent être partagées en groupes qui soient tous indépendants les uns des autres et permutables entre eux, chaque groupe étant composé de variables que l'on puisse échanger entre elles. Dans le dernier cas, m devra se réduire au nombre des valeurs distinctes d'une fonction transitive de cinq variables, c'est-à-dire à l'un des termes de la suite

$$1,\quad 2,\quad 6,\quad 12,\quad 24.$$

D'ailleurs, il résulte du théorème V du § I qu'on pourra prendre effectivement

$$m = 1 \quad \text{ou} \quad m = 2.$$

Il reste à montrer que l'on pourra prendre aussi

$$m = 6 \quad \text{ou} \quad m = 12,$$

et qu'au contraire on ne peut supposer $m = 24$. On y parvient aisément à l'aide des théorèmes établis dans les précédentes séances, comme on le verra dans un prochain article.

319.

Analyse mathématique. — *Mémoire sur les fonctions de cinq ou six variables, et spécialement sur celles qui sont doublement transitives.*

C. R., T. XXI, p. 1401 (29 décembre 1845).

Dans le précédent Mémoire, j'ai recherché le nombre m des valeurs distinctes que peut acquérir une fonction qui ne renferme pas plus de six variables. Aux diverses valeurs de m que j'ai trouvées, correspondent généralement des fonctions que l'on formera sans peine, si l'on adopte le mode de formation indiqué dans la séance du 6 octobre, attendu qu'il sera généralement facile de déterminer le nombre et la nature des substitutions diverses qui n'altèrent pas les valeurs de ces fonctions. Toutefois, on doit excepter le cas où il s'agit d'une fonction doublement transitive de six variables, c'est-à-dire d'une fonction Ω, qui est tout à la fois transitive par rapport à six variables, et transitive par rapport à cinq. Dans ce cas particulier, le nombre m des valeurs distinctes de Ω se réduit nécessairement au nombre des valeurs distinctes d'une fonction transitive de cinq variables, c'est-à-dire à l'un des termes de la suite

$$1, \quad 2, \quad 6, \quad 12, \quad 24;$$

et, comme nous l'avons dit, on peut effectivement supposer

$$m = 1 \quad \text{ou} \quad m = 2.$$

Mais peut-on prendre pareillement pour m l'un des trois nombres

$$6, \quad 12, \quad 24?$$

C'est ce qui nous reste à examiner. On facilite cet examen en appliquant successivement les principes que nous avons établis dans les précédents Mémoires aux fonctions transitives de cinq variables, puis aux fonctions doublement transitives de six variables. C'est ce que nous ferons dans les paragraphes suivants.

§ I. — *Sur les fonctions qui sont transitives par rapport à cinq variables, et intransitives par rapport à quatre.*

Soient

Ω une fonction de cinq variables

$$x, \quad y, \quad z, \quad u, \quad v;$$

M le nombre de ses valeurs égales;
m le nombre de ses valeurs distinctes.

On aura

$$mM = 1.2.3.4.5,$$

par conséquent

$$mM = 120. \tag{1}$$

Si d'ailleurs la fonction Ω est transitive par rapport aux cinq variables x, y, z, u, v, alors m sera encore le nombre des valeurs distinctes de Ω considéré comme fonction des quatre variables y, z, u, v; donc m sera un diviseur du produit

$$1.2.3.4 = 24,$$

et le facteur 5 du produit

$$mM = 1.2.3.4.5,$$

n'étant pas diviseur de m, devra diviser M. On aura effectivement

$$M = 5\mathfrak{M},$$

$\mathfrak{M}$ étant le nombre des valeurs égales de Ω considéré comme fonction des quatre variables y, z, u, v. Cela posé, il résulte d'un théorème énoncé dans la séance du 13 octobre (*voir* le théorème IV de la page 360) que le système des substitutions conjuguées qui n'altéreront pas la valeur de Ω renfermera des substitutions circulaires du cinquième ordre. Soit P l'une de ces substitutions. Comme on peut disposer arbitrairement de la forme des lettres propres à représenter les diverses variables qui devront succéder l'une à l'autre en vertu de la substitution P, rien n'empêchera d'admettre que ces variables sont respectivement

$$x, \quad y, \quad z, \quad u, \quad v,$$

et, par conséquent, on pourra toujours supposer

$$\mathrm{P} = (x, y, z, u, v). \tag{2}$$

Concevons maintenant que la fonction Ω soit tout à la fois transitive par rapport à cinq variables, et intransitive par rapport à quatre. Alors il arrivera de deux choses l'une : ou Ω, considéré comme fonction des quatre variables y, z, u, v, sera toujours altéré par toute substitution distincte de l'unité, ou les quatre variables y, z, u, v se partageront en deux groupes dépendants l'un de l'autre, et non permutables entre eux (séance du 29 septembre), chaque groupe étant composé de deux variables que l'on pourra échanger entre elles sans altérer la valeur de Ω. D'ailleurs, la composition de ces deux groupes sera inaltérable, et par suite, dans le second cas comme dans le premier, toute substitution qui déplacera deux ou trois variables seulement altérera la valeur de Ω. Cela posé, soit H_l le nombre des substitutions qui déplaceront l variables, sans altérer la valeur de Ω. On aura, dans l'un et l'autre cas, non seulement

$$H_0 = 1, \qquad H_1 = 0,$$

mais encore

$$H_2 = 0, \qquad H_3 = 0.$$

Donc les substitutions qui n'altéreront pas la valeur de Ω se réduiront à des substitutions régulières qui déplaceront quatre ou cinq variables (séance du 8 décembre), et les nombres H_4, H_5 de ces deux espèces de substitutions seront liés au nombre M des valeurs égales de Ω (séance du 10 novembre) par les deux formules

$$M = H_5 + H_4 + 1,$$
$$M = \qquad H_4 + 5,$$

desquelles on tirera

$$H_5 = 4, \qquad H_4 = M - 5. \tag{3}$$

Donc, dans l'un et l'autre cas, le nombre H_5 des substitutions circulaires du cinquième ordre qui n'altéreront pas la valeur de Ω sera égal à 4, et, en conséquence, ces substitutions ne pourront être que les puissances

$$\mathrm{P}, \quad \mathrm{P}^2, \quad \mathrm{P}^3, \quad \mathrm{P}^4$$

de la substitution P. Ajoutons que, dans le premier cas, Ω considéré comme fonction de quatre variables offrira $1.2.3.4$, c'est-à-dire 24 valeurs distinctes, et qu'alors

$$m = 24 \tag{4}$$

sera encore le nombre des valeurs distinctes de Ω considéré comme fonction transitive de cinq variables. Donc alors aussi on aura

$$M = \frac{120}{24} = 5,$$

et par suite, comme on devait s'y attendre, la seconde des formules (3) donnera

$$H_4 = 0.$$

Alors enfin, le système des substitutions conjuguées qui n'altéreront pas la valeur de Ω se réduira au système

$$1, \quad \mathrm{P}, \quad \mathrm{P}^2, \quad \mathrm{P}^3, \quad \mathrm{P}^4 \tag{5}$$

des diverses puissances de P.

Dans le second cas, où les quatre variables y, z, u, v se partageront en deux groupes dépendants l'un de l'autre et permutables entre eux, la seule substitution qui n'altérera pas la valeur de Ω considéré comme fonction de y, z, u, v sera le produit de deux facteurs circulaires du second ordre. Alors aussi, Ω considéré comme fonction de quatre variables offrira deux valeurs égales, par conséquent $\frac{24}{2}$ ou 12 valeurs distinctes, et

$$m = 12 \tag{6}$$

sera encore le nombre des valeurs distinctes de Ω considéré comme fonction transitive de cinq variables. Donc, par suite, on aura

$$M = \frac{120}{12} = 10,$$

et le nombre total H_4 des substitutions régulières du second ordre qui déplaceront quatre des cinq variables x, y, z, u, v, sans altérer Ω, sera égal à 5. Enfin, si l'on nomme Q celle de ces substitutions qui déplacera les quatre variables y, z, u, v, elle pourra être déterminée (*voir* la séance du 8 décembre, page 456) par une équation symbolique de la forme

$$Q = \binom{P^a}{P}, \tag{7}$$

a étant un nombre entier convenablement choisi, pourvu que, après avoir assigné la même place dans P et dans P^a à la variable x, on réduise P et P^a à de simples arrangements. Il y a plus : comme on tirera de la formule (7)

$$Q^2 = \binom{P^{a^2}}{P},$$

l'équation

$$Q^2 = 1$$

entrainera la suivante

$$a^2 = 1.$$

Donc, puisqu'on ne pourrait supposer $a = 1$ sans réduire Q à l'unité, on aura nécessairement

$$a = -1,$$

et la formule (7) donnera

$$Q = \binom{P^{-1}}{P} = \binom{xvuzy}{xyzuv} \tag{8}$$

ou, ce qui revient au même,

$$Q = (y, v)(z, u). \tag{9}$$

D'ailleurs, l'équation (8) pouvant s'écrire comme il suit

$$QP = P^{-1}Q, \tag{10}$$

on en conclura généralement

$$Q^k P^h = P^{(-1)^k h} Q^k. \tag{11}$$

Donc les dérivées des substitutions P, Q pourront toutes être présentées sous chacune des formes

$$Q^k P^h, \quad P^h Q^k.$$

En d'autres termes, le système des puissances de P sera permutable avec le système des puissances de Q. Donc les dérivées des deux substitutions P, Q, dont l'une est du cinquième ordre, l'autre du second, formeront un système de substitutions conjuguées dont l'ordre sera

$$2.5 = 10.$$

Donc la fonction transitive Ω, dont le caractère sera de n'être altérée ni par la substitution

$$P = (x, y, z, u, v),$$

ni par la substitution

$$Q = (y, v)(z, u),$$

offrira effectivement 10 valeurs égales, et par conséquent $\frac{120}{10}$ ou 12 valeurs distinctes.

§ II. — *Sur les fonctions qui sont transitives par rapport à cinq et à quatre variables.*

Conservons les notations adoptées dans le § I, et supposons d'ailleurs que la fonction Ω soit transitive, non seulement par rapport aux cinq variables x, y, z, u, v, mais aussi par rapport à quatre variables $y, z,$

u, v. Alors le nombre m des valeurs distinctes restera le même pour Ω considéré comme fonction de cinq, de quatre ou même de trois variables. Donc m sera un diviseur du produit

$$1.2.3 = 6;$$

et, puisqu'on ne pourra supposer le nombre m inférieur à 5 quand il surpassera 2, m devra se réduire à l'un des termes de la suite

$$1, \quad 2, \quad 6.$$

D'autre part, on formera sans peine des fonctions de x, y, z, u, v qui offriront une ou deux valeurs distinctes. Il y a plus : il résulte des principes qui servent de base à la théorie des équations binômes, que l'on peut aussi trouver des fonctions de cinq variables qui offrent six valeurs distinctes. Ajoutons que l'on peut encore arriver à cette conclusion de la manière suivante.

Nous avons déjà remarqué (§ I) que, si la fonction Ω est transitive par rapport aux cinq variables x, y, z, u, v, la valeur de Ω ne sera point altérée par des substitutions du cinquième ordre, dont l'une pourra être supposée de la forme

$$\mathrm{P} = (x, y, z, u, v). \tag{1}$$

Si d'ailleurs la fonction Ω est transitive par rapport à quatre variables, et offre six valeurs distinctes, en sorte qu'on ait

$$m = 6, \tag{2}$$

alors, considéré comme fonction de trois variables, Ω offrira encore six valeurs distinctes, dont chacune sera toujours altérée par toute substitution qui déplacera seulement ces trois variables ou deux d'entre elles. Donc, si l'on nomme H_l le nombre des substitutions qui déplaceront l variables sans altérer Ω, on aura, comme dans le § I,

$$H_2 = 0, \qquad H_3 = 0$$

et, par suite,

$$H_4 = 4.$$

Donc les substitutions qui déplaceront les cinq variables x, y, z, u, v sans altérer Ω, et qui devront être régulières (séance du 8 décembre), se réduiront aux puissances de P distinctes de l'unité, c'est-à-dire à

$$\mathrm{P}, \quad \mathrm{P}^2, \quad \mathrm{P}^3, \quad \mathrm{P}^4.$$

D'autre part, puisque Ω, considéré comme fonction des quatre variables y, z, u, v, offrira six valeurs distinctes, par conséquent quatre valeurs égales, les substitutions distinctes de l'unité qui déplaceront ces quatre variables, sans altérer Ω, seront au nombre de trois seulement, et ces trois substitutions, qui devront être elles-mêmes régulières, pourront être représentées par les expressions symboliques

$$\binom{\mathrm{P}^2}{\mathrm{P}}, \quad \binom{\mathrm{P}^3}{\mathrm{P}}, \quad \binom{\mathrm{P}^4}{\mathrm{P}},$$

c'est-à-dire qu'elles se réduiront aux suivantes

$$\binom{xzvyu}{xyzuv}, \quad \binom{xuyvz}{xyzuv}, \quad \binom{xvuzy}{xyzuv},$$

que l'on peut écrire sous les formes

$$(y, z, v, u), \quad (y, u, v, z), \quad (y, v)(z, u).$$

Elles se réduiront donc aux trois puissances

$$\mathrm{Q}, \quad \mathrm{Q}^2, \quad \mathrm{Q}^3$$

de la substitution du quatrième ordre

$$\mathrm{Q} = (y, z, v, u) = \binom{\mathrm{P}^2}{\mathrm{P}}. \tag{3}$$

Ce n'est pas tout : comme l'équation (3) donnera

$$\mathrm{QP} = \mathrm{P}^2\mathrm{Q}, \tag{4}$$

on en conclura

$$\mathrm{Q}^k\mathrm{P}^h = \mathrm{P}^{2^k h}\mathrm{Q}^k. \tag{5}$$

Donc les dérivées des substitutions P, Q pourront toutes être présentées sous chacune des formes

$$Q^k P^h, \quad P^h Q^k,$$

et par suite le système des puissances de P sera permutable avec le système des puissances de Q. Donc les dérivées des deux substitutions P, Q, dont l'une est du cinquième ordre, l'autre du quatrième, formeront un système de substitutions conjuguées, dont l'ordre sera

$$4.5 = 20.$$

Donc la fonction transitive dont le caractère sera de n'être altérée ni par la substitution

$$P = (x, y, z, u, v),$$

ni par la substitution

$$Q = (y, z, v, u)$$

offrira vingt valeurs distinctes, et par conséquent $\frac{120}{20}$ ou 6 valeurs égales.

D'après ce qu'on vient de voir, lorsqu'une fonction transitive de cinq variables x, y, z, u, v offre six valeurs distinctes, les substitutions qui déplacent les quatre variables y, z, u, v sans altérer Ω, et en laissant x immobile, sont au nombre de trois. Mais il est clair que trois substitutions semblables peuvent, sans altérer Ω, déplacer quatre variables, en laissant immobile ou x, ou z, ou u, ou v. Donc le nombre total H_4 des substitutions qui déplaceront quatre variables, sans altérer Ω, sera

$$5.3 = 15.$$

Cette conclusion s'accorde avec les formules (3) du § I, dont la seconde, jointe aux équations

$$m = 6, \quad M = \frac{120}{m} = 20,$$

donne

$$H_4 = 20 - 5 = 15.$$

Il est important d'observer que les quinze substitutions dont il s'agit

se trouvent toutes comprises dans les trois formes symboliques

$$\binom{P^2}{P}, \quad \binom{P^3}{P}, \quad \binom{P^4}{P},$$

desquelles on les déduit, en faisant coïncider successivement la variable à laquelle on assigne la première place, dans la substitution P et dans ses puissances, avec chacune des cinq variables x, y, z, u, v.

FIN DU TOME IX DE LA PREMIÈRE SÉRIE.

TABLE DES MATIÈRES

DU TOME NEUVIÈME.

PREMIÈRE SÉRIE.

MÉMOIRES EXTRAITS DES RECUEILS DE L'ACADÉMIE DES SCIENCES DE L'INSTITUT DE FRANCE.

NOTES ET ARTICLES EXTRAITS DES COMPTES RENDUS HEBDOMADAIRES DES SÉANCES DE L'ACADÉMIE DES SCIENCES.

Pages

277. Analyse mathématique. — Mémoire sur l'emploi des variables complémentaires dans le développement des fonctions en séries 5

278. Analyse mathématique. — Mémoire sur des formules rigoureuses et dignes de remarque, auxquelles on se trouve conduit par la considération de séries multiples et divergentes 19

279. Analyse mathématique. — Mémoire sur diverses propriétés remarquables et très générales des fonctions continues 32

280. Analyse mathématique. — Mémoire sur les séries syntagmatiques et sur celles qu'on obtient quand on développe des fonctions d'une seule variable suivant les puissances entières de son argument 54

281. Analyse mathématique. — Mémoire sur les approximations des fonctions de très grands nombres 74

282. Analyse mathématique. — Note sur les modules principaux des fonctions ... 75

283. Analyse mathématique. — Mémoire sur les approximations des fonctions de très grands nombres 81

284. Analyse mathématique. — Mémoire sur les approximations des fonctions de très grands nombres 84

Pages

285. ASTRONOMIE. — Rapport sur un Mémoire de M. *Le Verrier*, qui a pour objet la détermination d'une grande inégalité du moyen mouvement de la planète Pallas 121

286. ASTRONOMIE. — Notes jointes au Rapport qui précède, et rédigées par le Rapporteur 124

287. ASTRONOMIE. — Suite des Notes annexées au Rapport sur le Mémoire de M. *Le Verrier*, et relatives à la détermination des inégalités périodiques des mouvements planétaires 141

288. CALCUL INTÉGRAL. — Mémoire sur la détermination approximative des fonctions représentées par des intégrales 164

289. ASTRONOMIE. — Note sur l'application des nouvelles formules à l'Astronomie .. 186

290. ASTRONOMIE. — Mémoire sur les séries nouvelles que l'on obtient, quand on applique les méthodes exposées dans les précédentes séances au développement de la fonction perturbatrice et à la détermination des inégalités périodiques des mouvements planétaires 190

291. ASTRONOMIE. — Mémoire sur des formules et des théorèmes remarquables, qui permettent de calculer très facilement les perturbations planétaires dont l'ordre est très élevé 205

292. Rapport sur la singulière aptitude d'un enfant de six ans et demi pour le calcul. 220

293. MÉCANIQUE. — Notes relatives à la Mécanique rationnelle 221

294. MÉCANIQUE. — Observations sur la pression que supporte un élément de surface plane dans un corps solide ou fluide 230

295. Mémoire sur les secours que les sciences de calcul peuvent fournir aux sciences physiques ou même aux sciences morales, et sur l'accord des théories mathématiques et physiques avec la véritable philosophie 240

296. GÉOMÉTRIE. — Mémoire sur de nouveaux théorèmes de Géométrie et, en particulier, sur le module de rotation d'un système de lignes droites menées par les divers points d'une directrice donnée 253

297. GÉOMÉTRIE ANALYTIQUE. — Sur divers théorèmes de Géométrie analytique 253

298. ANALYSE MATHÉMATIQUE. — Mémoire sur divers théorèmes d'Analyse et de Calcul intégral 266

299. GÉOMÉTRIE. — Rapport sur un Mémoire de M. *Ossian Bonnet*, concernant quelques propriétés générales des surfaces et des lignes tracées sur les surfaces 275

300. ANALYSE MATHÉMATIQUE. — Sur le nombre des valeurs égales ou inégales que peut acquérir une fonction de n variables indépendantes, quand on permute ces variables entre elles d'une manière quelconque 277

301. ANALYSE MATHÉMATIQUE. — Sur le nombre des valeurs égales ou distinctes que peut acquérir une fonction de n variables, quand on permute ces variables entre elles d'une manière quelconque (*suite*) 293

Pages

302. ANALYSE MATHÉMATIQUE. — Sur le nombre des valeurs égales ou distinctes que peut acquérir une fonction de n variables, quand on permute ces variables entre elles d'une manière quelconque 306

303. ANALYSE MATHÉMATIQUE. — Sur le nombre des valeurs égales ou inégales que peut acquérir une fonction de n variables indépendantes, quand on permute ces variables entre elles d'une manière quelconque 323

304. ANALYSE MATHÉMATIQUE. — Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières, et des systèmes de substitutions conjuguées 342

305. ANALYSE MATHÉMATIQUE. — Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières, et des systèmes de substitutions conjuguées (*suite*) 361

306. ANALYSE MATHÉMATIQUE. — Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières, et des systèmes de substitutions conjuguées (*suite*) 368

307. ANALYSE MATHÉMATIQUE. — Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières, et des systèmes de substitutions conjuguées (*suite*) 371

308. ANALYSE MATHÉMATIQUE. — Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières, et des systèmes de substitutions conjuguées (*suite*) 388

309. ANALYSE MATHÉMATIQUE. — Rapport sur un Mémoire présenté à l'Académie par M. *Bertrand*, et relatif au nombre des valeurs que peut prendre une fonction, quand on y permute les lettres qu'elle renferme 405

310. ANALYSE MATHÉMATIQUE. — Mémoire sur les premiers termes de la série des quantités qui sont propres à représenter le nombre des valeurs distinctes d'une fonction des n variables indépendantes 408

311. ANALYSE MATHÉMATIQUE. — Mémoire sur la résolution des équations linéaires symboliques, et sur les conséquences remarquables que cette résolution entraîne après elle dans la théorie des permutations 417

312. ANALYSE MATHÉMATIQUE. — Mémoire sur les substitutions permutables entre elles 430

313. ANALYSE MATHÉMATIQUE. — Note sur la réduction des fonctions transitives aux fonctions intransitives, et sur quelques propriétés remarquables des substitutions qui n'altèrent pas la valeur d'une fonction transitive 442

314. ANALYSE MATHÉMATIQUE. — Note sur les substitutions qui n'altèrent pas la valeur d'une fonction, et sur la forme régulière que prennent toujours celles d'entre elles qui renferment un moindre nombre de variables 444

315. ANALYSE MATHÉMATIQUE. — Mémoire sur diverses propriétés des systèmes de substitutions, et particulièrement de ceux qui sont permutables entre eux .. 449

Pages

316. Analyse mathématique. — Note sur les fonctions caractéristiques des substitutions ... 466

317. Analyse mathématique. — Mémoire sur le nombre et la forme des substitutions qui n'altèrent pas la valeur d'une fonction de plusieurs variables indépendantes ... 467

318. Analyse mathématique. — Applications diverses des propriétés établies dans les précédents Mémoires ... 482

319. Analyse mathématique. — Mémoire sur les fonctions de cinq ou six variables, et spécialement sur celles qui sont doublement transitives ... 496

FIN DE LA TABLE DES MATIÈRES DU TOME IX DE LA PREMIÈRE SÉRIE.

19554 Paris. — Imprimerie Gauthier-Villars et fils, quai des Grands-Augustins, 55.