NOTE SUR QUELQUES PROPOSITIONS

RELATIVES

A LA THÉORIE DES NOMBRES

Diverses propositions relatives à la théorie des nombres se déduisent aisément du théorème dont voici l'énoncé :

THÉORÈME I. — *Supposons le nombre entier i décomposé en facteurs a, b, c, ... premiers entre eux; et soit l un nombre entier quelconque inférieur à i. On pourra toujours satisfaire à l'équivalence*

$$i\left(\frac{x}{a}+\frac{y}{b}+\frac{z}{c}+\dots\right)\equiv l \pmod{i}, \tag{1}$$

par des valeurs entières de

$$x,\ y,\ z,\ \dots$$

respectivement inférieures à

$$a,\ b,\ c,\ \dots.$$

Démonstration. — Pour abréger, désignons par

$$s=i\left(\frac{x}{a}+\frac{y}{b}+\frac{z}{c}+\dots\right) \tag{2}$$

la fonction linéaire de x, y, z, ... qui représente le premier membre de la formule (1), et supposons que l'on attribue successivement aux variables x, y, z, ..., renfermées dans la fonction s, tous les systèmes de valeurs qu'on peut obtenir en combinant une valeur de x prise dans la suite

$$0,\ 1,\ 2,\ \dots,\ a-1,$$

avec une valeur de y prise dans la suite

$$0,\ 1,\ 2,\ \dots,\ b-1,$$

puis avec une valeur de z prise dans la suite

$$0,\quad 1,\quad 2,\quad \ldots,\quad c-1,$$

etc.... On obtiendra ainsi pour s des valeurs entières, dont le nombre, représenté par le produit

$$abc\ldots = i,$$

sera en conséquence égal au nombre des termes de la suite

$$0,\quad 1,\quad 2,\quad \ldots,\quad i-1;$$

et il est clair que parmi ces i valeurs de s il en existera toujours une équivalente, suivant le module i, à l'un quelconque des termes de la suite

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

s'il est prouvé que ces valeurs de s, divisées par i, donnent des restes différents. Cela posé, soient

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

les accroissements positifs ou négatifs que prendront x, y, z, ... quand on passera d'une valeur de s à une autre, et nommons Δs l'accroissement correspondant de s, ou la différence des deux valeurs de s, déterminée par la formule

$$\Delta s = i\left(\frac{\Delta x}{a} + \frac{\Delta y}{b} + \frac{\Delta z}{c} + \ldots\right). \tag{3}$$

Pour établir le théorème énoncé, il suffira de prouver que Δs ne peut être divisible par i, si Δx, Δy, Δz, ... ne s'évanouissent tous à la fois. Or, effectivement, Δs ne pourra être divisible par i, s'il n'est divisible par chacun des facteurs

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

D'ailleurs, dans la valeur de Δs, mise sous la forme

$$\Delta s = \frac{i}{a}\Delta x + \frac{i}{b}\Delta y + \frac{i}{c}\Delta z + \ldots, \tag{4}$$

tous les termes seront évidemment divisibles par a, hormis le premier $\frac{i}{a}\Delta x$; et celui-ci ne pourra devenir divisible par a que dans le cas où l'accroissement Δx, dont la valeur numérique est inférieure à a, sera divisible par a, et par conséquent nul. Pareillement, dans la valeur de Δs fournie par l'équation (4), tous les termes seront évidemment divisibles par b, hormis le second, et celui-ci ne pourra devenir divisible par b que dans le cas où Δy sera nul; etc....

Corollaire. — Si l'on veut que le nombre entier l fournisse des restes donnés quand on le divise par les nombres a, b, c, ..., par exemple le reste p quand on le divise par a, le reste q quand on le divise par b, le reste r quand on le divise par c, ..., il suffira évidemment de prendre

$$x = px, \qquad y = qy, \qquad z = rz, \qquad \ldots \tag{5}$$

en assujettissant

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

à vérifier les formules

$$\frac{i}{a}x \equiv 1 \pmod{a}, \qquad \frac{i}{b}y \equiv 1 \pmod{b}, \qquad \frac{i}{c}z \equiv 1 \pmod{c}, \qquad \ldots \tag{6}$$

En effet, dans le second membre de l'équation (1) présentée sous la forme

$$l \equiv \frac{i}{a}x + \frac{i}{b}y + \frac{i}{c}z + \ldots \pmod{i}, \tag{7}$$

$\frac{i}{a}x$ sera le seul terme qui ne soit pas divisible par a, et il est clair que ce terme, divisé par a, donnera pour reste p, si l'on pose $x = px$, en choisissant x de manière à vérifier l'équivalence

$$\frac{i}{a}x \equiv 1 \pmod{a}.$$

D'ailleurs, cette équivalence du premier degré se résoudra aisément par les méthodes connues, attendu que les deux nombres

$$a \quad \text{et} \quad \frac{i}{a} = bc\ldots$$

seront premiers entre eux. On prouvera de même, non seulement

que, dans l'hypothèse admise, on peut satisfaire à l'une quelconque des formules (6) par une valeur entière de x, ou y, ou z, ..., mais encore qu'aux valeurs x, y, z, ..., ainsi obtenues, répondra, en vertu des équations (5) et (7), une valeur de l qui fournira le reste p quand on la divisera par a, le reste q quand on la divisera par b, le reste r quand on la divisera par c, etc. Si, pour abréger, on représente par

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

les premiers membres des formules (6), c'est-à-dire si l'on pose

$$A=\frac{i}{a}x,\qquad B=\frac{i}{b}y,\qquad C=\frac{i}{c}z,\qquad \ldots. \tag{8}$$

la formule (7) deviendra

$$l\equiv Ap+Bq+Cr+\ldots \pmod{i}. \tag{9}$$

Ainsi le théorème I entraîne la proposition suivante :

THÉORÈME II. — *Soient $a, b, c, \ldots$ des nombres donnés premiers entre eux, et $i=abc\ldots$ le produit de ces deux nombres. Si l'on veut obtenir un entier l, qui, étant divisé par les nombres donnés*

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

fournisse des restes donnés

$$p,\quad q,\quad r,\quad \ldots,$$

il suffira de prendre

$$l=Ap+Bq+Cr+\ldots+mabc\ldots, \tag{10}$$

A étant un multiple de $\frac{i}{a}=bc\ldots$ qui, divisé par a, donne 1 pour reste, B étant un multiple de $\frac{i}{a}=ac\ldots$ qui, divisé par b, donne encore 1 pour reste, etc., et m étant, d'ailleurs, un nombre entier quelconque.

La proposition que nous venons d'énoncer a été donnée par Euler; elle se trouve dans le Mémoire intitulé : *Solutio problematis arithmetici de inveniendo numero qui per datos numeros divisus relinquat data residua* (voir le tome VII des *Mémoires de Saint-Pétersbourg*,

années 1734-1735). On voit qu'elle se déduit aisément du théorème I; mais on pourrait aussi déduire le théorème I du second, et la formule (7) de l'équation (9). En effet, soit i un nombre entier quelconque décomposé en facteurs $a, b, c, \ldots$ premiers entre eux; soit, de plus, l un quelconque des nombres inférieurs à i, et nommons $p, q, r, \ldots$ les restes que l'on obtient quand on divise l par les facteurs $a, b, c, \ldots$. On pourra, d'après le théorème II, déterminer l par la formule (9) jointe aux équations (8), x, y, z, ... étant choisis de manière à vérifier les conditions (6). Cela posé, concevons que, dans les formules (9), on substitue les valeurs de $A, B, C, \ldots$ tirées des équations (8); alors, en prenant

$$x=px,\qquad y=qy,\qquad z=rz,\qquad \ldots,$$

on retrouvera précisément la formule (7), qui ne sera point altérée quand on fera croître ou décroître x d'un multiple quelconque de a, y d'un multiple quelconque de b, ...; d'où il suit que l'on pourra supposer, dans la formule (7), x réduit à l'un des nombres

$$0,\quad 1,\quad 2,\quad \ldots,\quad a-1,$$

y réduit à l'un des nombres

$$0,\quad 1,\quad 2,\quad \ldots,\quad b-1,$$

etc....

Supposons maintenant que l soit un nombre premier à i. Le théorème I continuera encore de subsister, et, par suite, on pourra vérifier la formule (7), en prenant pour x un entier inférieur à a, pour y un entier inférieur à b, ... Mais les deux nombres

$$l \quad \text{et} \quad i=abc\ldots$$

étant, par hypothèse, premiers entre eux, il est clair que, dans le second membre de la formule (7), le seul terme non divisible par a, ou le produit

$$\frac{i}{a}x=bc\ldots x,$$

devra être premier à a; donc x lui-même devra être premier à a. Pareillement, y devra être premier à b, z à c, ... Donc, lorsque l est premier à i, on peut vérifier la formule (7), en prenant pour x un entier inférieur et premier à a, pour y un entier inférieur et premier à b, etc. On peut donc énoncer encore la proposition suivante :

THÉORÈME III. — *Supposons le nombre entier i décomposé en facteurs $a, b, c, \ldots$ premiers entre eux. L'expression générale des nombres l premiers à i sera*

$$l = \frac{i}{a}x + \frac{i}{b}y + \frac{i}{c}z + \ldots + mabc,$$

x étant un nombre inférieur et premier à a, y un nombre inférieur et premier à b, z un nombre inférieur et premier à c, ..., et m représentant un nombre entier quelconque.

Le théorème III a été énoncé par M. Poinsot dans le *Journal des Mathématiques* de M. Liouville [février 1845]. La démonstration qu'il en a donnée repose en partie sur les considérations que nous avons reproduites en les appliquant à l'établissement du théorème I, en partie sur la formule qui indique combien il existe de nombres inférieurs à i et premiers à i. Mais, comme on le voit, on peut se dispenser de recourir à cette dernière formule, et déduire le troisième théorème du premier. On pourrait aussi le déduire du second, ou, ce qui revient au même, de la formule (10) donnée par Euler.

Il est bon d'observer que l'on pourrait encore tirer immédiatement la formule (1) d'une proposition établie par M. Gauss, savoir, que, *dans le cas où plusieurs nombres entiers $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ... n'offrent pas de diviseur commun, on peut toujours satisfaire, par des valeurs entières, positives ou négatives de* x, y, z, ..., *à l'équation*

$$\mathfrak{a}x + \mathfrak{b}y + \mathfrak{c}z + \ldots = 1. \tag{11}$$

En effet, cette proposition étant admise, multiplions par un entier quelconque l les deux membres de la formule (11), et posons

$$x = lx, \qquad y = ly, \qquad z = lz, \qquad \ldots;$$

on trouvera

$$\mathfrak{a}x + \mathfrak{b}y + \mathfrak{c}z + \ldots = l. \tag{12}$$

Soient maintenant $a, b, c, \ldots$ des nombres premiers entre eux. Nommons i leur produit, et posons

$$\mathfrak{a} = \frac{i}{a} = bc\ldots, \qquad \mathfrak{b} = \frac{i}{b} = ac\ldots, \qquad \mathfrak{c} = \frac{i}{c} = ab\ldots \tag{13}$$

Il est clair que $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ... n'auront pas de diviseur commun. Donc l'équation (12) donnera

$$\frac{i}{a}x + \frac{i}{b}y + \frac{i}{c}z + \ldots = l. \tag{14}$$

On pourra donc encore satisfaire, par des valeurs entières de x, y, z, ..., à l'équation (14), de laquelle on déduira immédiatement la formule (1), en supposant l inférieur à i et faisant croître ou décroître, s'il est nécessaire, x d'un multiple de a, y d'un multiple de b, z d'un multiple de c, ...

Observons enfin que, du théorème III, joint aux théorèmes connus de Wilson et de Fermat, on peut immédiatement déduire une proposition énoncée par M. Gauss, savoir : que *le produit de tous les nombres inférieurs à i et premiers à i, étant divisé par i, fournit un reste équivalent à -1, quand i est une puissance d'un nombre premier, ou le double d'une telle puissance, ou le nombre 4, et fournit, dans tous les autres cas, un reste équivalent à l'unité.*

Les théorèmes divers que nous venons de rappeler sont particulièrement utiles dans la théorie des permutations, ainsi qu'on le verra dans les Mémoires qui suivront la présente Note.

MÉMOIRE
SUR
LES ARRANGEMENTS QUE L'ON PEUT FORMER
AVEC DES LETTRES DONNÉES
ET
SUR LES PERMUTATIONS OU SUBSTITUTIONS A L'AIDE DESQUELLES ON PASSE D'UN ARRANGEMENT A UN AUTRE

I. — *Considérations générales.*

Soient

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

diverses lettres, qui soient censées représenter des variables indépendantes. Si l'on numérote les places occupées par ces variables dans une certaine fonction Ω, et si l'on écrit à la suite les unes des autres ces variables x, y, z, ... rangées d'après l'ordre de grandeur des numéros assignés aux places qu'elles occupent, on obtiendra un certain *arrangement*

$$xyz\ldots,$$

et quand les variables seront déplacées, cet arrangement se trouvera remplacé par un autre, qu'il suffira de comparer au premier pour connaître la nature des déplacements. Cela posé, les diverses valeurs d'une fonction de n lettres correspondront évidemment aux divers arrangements que l'on pourra former avec ces n lettres. D'ailleurs, le nombre de ces arrangements est, comme l'on sait, représenté par le produit

$$1.2.3\ldots n.$$

Si donc on pose, pour abréger,

$$N = 1.2.3\ldots n,$$

N sera le nombre des valeurs diverses, égales ou distinctes, qu'une fonction de n variables acquerra successivement quand on déplacera de toutes les manières, en les substituant l'une à l'autre, les variables dontil s'agit.

On appelle *permutation* ou *substitution* l'opération qui consiste à déplacer les variables, en les substituant les unes aux autres, dans une valeur donnée de la fonction Ω, ou dans l'arrangement correspondant. Pour indiquer cette substitution, nous écrirons le nouvel arrangement qu'elle produit au-dessus du premier, et nous renfermerons le système de ces deux arrangements entre parenthèses. Ainsi, par exemple, étant donnée la fonction

$$\Omega = x + 2y + 3z,$$

où les variables x, y, z occupent respectivement la première, la seconde et la troisième place, et se succèdent en conséquence dans l'ordre indiqué par l'arrangement

$$xyz,$$

si l'on échange entre elles les variables y, z qui occupent les deux dernières places, on obtiendra une nouvelle valeur Ω′ de Ω, qui sera distincte de la première, et déterminée par la formule

$$\Omega' = x + 2z + 3y.$$

D'ailleurs, le nouvel arrangement, correspondant à cette nouvelle valeur, sera

$$xzy,$$

et la substitution par laquelle on passe de la première valeur à la seconde se trouvera représentée par la notation

$$\begin{pmatrix} xzy \\ xyz \end{pmatrix},$$

qui indique suffisamment de quelle manière les variables ont été déplacées. Les deux arrangements xzy, xyz, compris dans cette substitution, forment ce que nous appellerons ses *deux termes*, ou son *numérateur* et son *dénominateur*. Comme les numéros qu'on assigne

aux diverses places qu'occupent les variables dans une fonction sont entièrement arbitraires, il est clair que l'arrangement correspondant à une valeur donnée de la fonction est pareillement arbitraire, et que le dénominateur d'une substitution quelconque peut être l'un quelconque des N arrangements formés avec les n variables données. On arrivera immédiatement à la même conclusion en observant qu'une substitution quelconque peut être censée indiquer un système déterminé d'opérations simples dont chacune consiste à remplacer une lettre du dénominateur par une lettre du numérateur, et que ce système d'opérations ne variera pas si l'on échange entre elles d'une manière quelconque les lettres du dénominateur, pourvu que l'on échange entre elles, de la même manière, les lettres correspondantes du numérateur. Il en résulte qu'une substitution, relative à un système de n variables, peut être présentée sous N formes différentes dont nous indiquerons l'équivalence par le signe =. Ainsi, par exemple, on aura

$$\begin{pmatrix} xzy \\ xyz \end{pmatrix} = \begin{pmatrix} xyz \\ xzy \end{pmatrix} = \begin{pmatrix} yxz \\ zxy \end{pmatrix}, \quad \dots$$

Observons encore que l'on peut, sans inconvénient, effacer toute lettre qui se présente à la même place dans les deux termes d'une substitution donnée, cette circonstance indiquant que la lettre ne doit pas être déplacée. Ainsi, en particulier, on aura

$$\begin{pmatrix} xzy \\ xyz \end{pmatrix} = \begin{pmatrix} zy \\ yz \end{pmatrix}.$$

Lorsqu'on a ainsi éliminé d'une substitution donnée toutes les lettres qu'il est possible d'effacer, cette substitution se trouve réduite *à sa plus simple expression*.

Le *produit* d'un arrangement donné xyz par une substitution $\begin{pmatrix} xzy \\ xyz \end{pmatrix}$ est le nouvel arrangement xzy qu'on obtient en appliquant cette substitution même à l'arrangement donné. Le *produit* de deux substitutions est la substitution nouvelle qui fournit toujours le résultat auquel conduirait l'application des deux premières, opérées l'une

après l'autre, à un arrangement quelconque. Les deux substitutions données sont les deux *facteurs* du produit. Le produit d'un arrangement par une substitution ou d'une substitution par une autre s'indiquera par l'une des notations qui servent à indiquer le produit de deux quantités, le multiplicande étant placé, suivant la coutume, à la droite du multiplicateur. On trouvera ainsi, par exemple,

$$\binom{xzy}{xyz}xyz = xzy$$

et

$$\binom{yxuz}{xyzu} = \binom{yx}{xy}\binom{uz}{zu}.$$

Il y a plus; on pourra, dans le second membre de la dernière équation, échanger sans inconvénient les deux facteurs entre eux, de sorte qu'on aura encore

$$\binom{yxuz}{xyzu} = \binom{uz}{zu}\binom{yx}{xy}.$$

Mais cet échange ne sera pas toujours possible, et souvent le produit de deux substitutions variera quand on échangera les deux facteurs entre eux. Ainsi, en particulier, on trouvera

$$\binom{yx}{xy}\binom{zy}{yz} = \binom{yzx}{xyz} \quad \text{et} \quad \binom{zy}{yz}\binom{yx}{xy} = \binom{zxy}{xyz}.$$

Nous dirons que deux substitutions sont *permutables* entre elles, lorsque leur produit sera indépendant de l'ordre dans lequel se suivront les deux facteurs.

Rien n'empêche de représenter par de simples lettres

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

ou par des lettres affectées d'indices

$$A_1,\ A_2,\ A_3,\ \ldots,$$

les arrangements formés avec plusieurs variables. Alors la substitution qui aura pour termes A et B se présentera simplement sous la forme

$$\binom{B}{A}.$$

et l'on aura

$$\binom{B}{A}A = B,$$
$$\binom{C}{B}\binom{B}{A} = \binom{C}{A},$$
$$\ldots\ldots\ldots\ldots$$

De plus, si, en appliquant à l'arrangement C la substitution $\binom{B}{A}$, on produit l'arrangement D, on aura non seulement

$$\binom{B}{A}C = D,$$

mais encore

$$\binom{B}{A} = \binom{D}{C}.$$

Le nombre total des substitutions relatives au système de n variables $x, y, z, \ldots$ est évidemment égal au nombre N des arrangements que l'on peut former avec ces variables, puisqu'en prenant pour dénominateur un seul de ces arrangements, le premier par exemple, on peut prendre pour numérateur l'un quelconque d'entre eux. La substitution, dont le numérateur est le dénominateur même, peut être censée se réduire à l'unité, puisqu'on peut évidemment la remplacer par le facteur 1, dans les produits

$$\binom{A}{A}C = C,$$
$$\binom{A}{A}\binom{D}{C} = \binom{D}{C}\binom{A}{A} = \binom{D}{C}.$$

Une substitution $\binom{B}{A}$, multipliée par elle-même plusieurs fois de suite, donne pour produits successifs son *carré*, son *cube*, et généralement ses diverses *puissances*, qui sont naturellement représentées par les notations

$$\binom{B}{A}^2,\ \binom{B}{A}^3,\ \ldots.$$

D'ailleurs, la série qui aura pour termes la substitution $\binom{B}{A}$ et ses

diverses puissances, savoir,

$$\left(\frac{B}{A}\right),\quad \left(\frac{B}{A}\right)^2,\quad \left(\frac{B}{A}\right)^3,\quad \ldots,$$

ne pourra jamais offrir plus de N substitutions réellement distinctes. Donc, en prolongeant cette série, on verra bientôt reparaître les mêmes substitutions.

D'autre part, si l'on suppose

$$\left(\frac{B}{A}\right)^h = \left(\frac{B}{A}\right)^l,$$

h étant $< l$, alors, en faisant, pour abréger,

$$l = i + h,$$

on aura

$$\left(\frac{B}{A}\right)^h = \left(\frac{B}{A}\right)^{i+h} = \left(\frac{B}{A}\right)^i \left(\frac{B}{A}\right)^h,$$

par conséquent

$$\left(\frac{B}{A}\right)^i = 1,$$

i étant évidemment inférieur à l. Il y a plus; si, en supposant la valeur de i déterminée par la formule précédente, on nomme l un nombre entier quelconque, k le quotient de la division de l par i, et j le reste de cette division, en sorte qu'on ait

$$l = ki + j,$$

j étant inférieur à i, on trouvera non seulement

$$\left(\frac{B}{A}\right)^{ki} = \left[\left(\frac{B}{A}\right)^i\right]^k = 1^k = 1,$$

mais, en outre,

$$\left(\frac{B}{A}\right)^l = \left(\frac{B}{A}\right)^{ki}\left(\frac{B}{A}\right)^j = \left(\frac{B}{A}\right)^j;$$

et, en étendant l'avant-dernière formule au cas même où le nombre k se réduit à zéro, on aura encore

$$\left(\frac{B}{A}\right)^0 = 1.$$

En vertu des remarques que nous venons de faire, si l'on prolonge

indéfiniment la série dont les divers termes sont

$$\left(\frac{B}{A}\right)^0 = 1,\quad \left(\frac{B}{A}\right),\quad \left(\frac{B}{A}\right)^2,\quad \left(\frac{B}{A}\right)^3,\quad \ldots,$$

le premier des termes qu'on verra reparaître sera précisément l'unité, et à partir de celui-ci les termes déjà trouvés se reproduiront périodiquement dans le même ordre, puisqu'on aura, par exemple,

$$1 = \left(\frac{B}{A}\right)^i = \left(\frac{B}{A}\right)^{2i} = \ldots,$$
$$\left(\frac{B}{A}\right) = \left(\frac{B}{A}\right)^{i+1} = \left(\frac{B}{A}\right)^{2i+1} = \ldots,$$
$$\left(\frac{B}{A}\right)^2 = \left(\frac{B}{A}\right)^{i+2} = \left(\frac{B}{A}\right)^{2i+2} = \ldots,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Donc le nombre i des termes distincts de la série sera toujours la plus petite des valeurs entières de i pour lesquelles se vérifiera la formule

$$\left(\frac{B}{A}\right)^i = 1.$$

Le nombre i, ainsi déterminé, ou le degré de la plus petite des puissances de $\left(\frac{B}{A}\right)$ équivalentes à l'unité, est ce que nous appellerons le degré ou l'*ordre* de la substitution $\left(\frac{B}{A}\right)$.

Supposons maintenant qu'une substitution réduite à sa plus simple expression se présente sous la forme

$$\begin{pmatrix} yz\ldots ewx \\ xy\ldots uvw \end{pmatrix},$$

c'est-à-dire qu'elle ait pour objet de remplacer x par y, puis y par z, et ainsi de suite jusqu'à ce que l'on parvienne à une dernière variable w qui devra être remplacée par la variable x de laquelle on était parti. Pour effectuer cette substitution, il suffira évidemment de ranger sur la circonférence d'un cercle *indicateur*, divisée en parties égales, les diverses variables

$$x, y, z, \ldots, u, v, w,$$

en plaçant la première, la seconde, la troisième, ... sur le premier,

le second, le troisième, ... point de division, puis de remplacer chaque variable par celle qui la première viendra prendre sa place, lorsqu'on fera tourner dans un certain sens le cercle indicateur. Pour ce motit nous donnons à la substitution dont il s'agit le nom de *substitution circulaire*. Nous la représenterons, pour abréger, par la notation

$$(x, y, z, \ldots, u, v, w);$$

et il est clair que, dans cette notation, une quelconque des variables

$$x, y, z, \ldots, u, v, w$$

pourra occuper la première place. Ainsi, par exemple, on aura identiquement

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

Si l'on nomme i le nombre des variables comprises dans une substitution circulaire

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

alors, pour opérer cette substitution l fois de suite, ou, ce qui revient au même, pour l'élever à la puissance du degré l, il suffira évidemment de faire tourner le cercle indicateur, de manière que le point de division correspondant à chaque lettre parcoure une portion de la circonférence mesurée par le rapport $\frac{l}{i}$. Cela posé, pour ramener chaque lettre à sa place, il faudra évidemment que $\frac{l}{i}$ soit un nombre entier, et que l'on ait au moins $l = i$. Donc l'ordre d'une substitution circulaire sera précisément le nombre i des lettres qu'elle renferme.

Si, dans le cercle indicateur, on joint par une corde deux points de division correspondants à deux variables dont l'une prendrait la place de l'autre, en vertu de la substitution circulaire

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

l fois répétée, ou, ce qui revient au même, en vertu de la substitution

$$(x, y, z, \ldots, u, v, w)^l,$$

le système des cordes ainsi tracées offrira évidemment ou un polygone régulier, ou un système de polygones réguliers.

Si le degré l est premier à i, c'est-à-dire au nombre qui représente l'ordre de la substitution circulaire

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

le système des cordes dont il s'agit constituera simplement un polygone régulier, qui pourra être du genre de ceux que M. Poinsot a nommés *polygones étoilés*. Mais si les nombres l et i offrant un ou plusieurs facteurs communs, on nomme k le plus grand commun diviseur de ces deux nombres, et a le quotient de la division de i par k, alors le système des cordes tracées constituera un système de k polygones réguliers, étoilés ou non étoilés, dont chacun renfermera a côtés seulement. Donc alors aussi la substitution

$$(x, y, z, \ldots, u, v, w)^l$$

sera le produit de k substitutions circulaires de l'ordre a. Si, pour fixer les idées, on pose $i = 4$, alors, en élevant à la seconde et à la troisième puissance la substitution circulaire

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

on trouvera

$$(x, y, z, u)^2 = (x, z)(y, u), \qquad (x, y, z, u)^3 = (x, u, z, y).$$

Si, au contraire, on pose $i = 6$, alors, en élevant à diverses puissances la substitution circulaire

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

on trouvera

$$(x, y, z, u, v, w)^2 = (x, z, v)(y, u, w), \qquad (x, y, z, u, v, w)^3 = (x, u)(y, v)(z, w),$$
$$(x, y, z, u, v, w)^4 = (x, v, z)(y, w, u), \qquad (x, y, z, u, v, w)^5 = (x, w, v, u, z, y).$$

Soient maintenant

A et B

deux quelconques des arrangements que l'on peut former avec n variables $x, y, z, \ldots$. Pour substituer le second arrangement au

premier, il suffira évidemment d'opérer une ou plusieurs substitutions circulaires, que l'on formera sans peine en écrivant à la suite l'une de l'autre deux variables, dont l'une sera remplacée par l'autre quand on passera du premier arrangement au second. En conséquence, la substitution $\begin{pmatrix} B \\ A \end{pmatrix}$, réduite à sa plus simple expression, sera nécessairement, ou une substitution circulaire, ou le produit de plusieurs substitutions circulaires. On trouvera, par exemple, en supposant que $\begin{pmatrix} B \\ A \end{pmatrix}$ renferme quatre ou cinq variables

$$\begin{pmatrix} uzyx \\ xyzu \end{pmatrix} = (x, u)(y, z), \qquad \begin{pmatrix} zuvyx \\ xyzuv \end{pmatrix} = (x, z, v)(y, u).$$

Les substitutions circulaires dont une substitution quelconque $\begin{pmatrix} B \\ A \end{pmatrix}$ sera le produit, sont ce que nous appellerons les *facteurs circulaires* de $\begin{pmatrix} B \\ A \end{pmatrix}$. Deux quelconques d'entre elles, étant composées de lettres diverses, seront évidemment permutables. Donc, tous les facteurs circulaires de $\begin{pmatrix} B \\ A \end{pmatrix}$ seront permutables entre eux, et représenteront des substitutions qui pourront être effectuées dans un ordre quelconque. Il y a plus: comme deux substitutions égales seront nécessairement permutables entre elles, si l'on élève $\begin{pmatrix} B \\ A \end{pmatrix}$ à des puissances quelconques, on obtiendra de nouvelles substitutions qui seront permutables entre elles, ainsi que leurs facteurs représentés par des puissances des facteurs circulaires de $\begin{pmatrix} B \\ A \end{pmatrix}$.

Supposons, pour fixer les idées, que les variables comprises dans les divers facteurs circulaires de $\begin{pmatrix} B \\ A \end{pmatrix}$ soient respectivement :

Dans le premier facteur..... $\alpha, \beta, \gamma, \ldots$
Dans le second facteur..... $\lambda, \mu, \nu, \ldots$
Dans le troisième facteur..... $\varphi, \chi, \psi, \ldots$
.....

en sorte qu'on ait

$$(1) \qquad \begin{pmatrix} B \\ A \end{pmatrix} = (\alpha, \beta, \gamma, \ldots)(\lambda, \mu, \nu, \ldots)(\varphi, \chi, \psi, \ldots)\ldots.$$

Alors, l étant un nombre entier quelconque, on aura encore

$$\begin{pmatrix} B \\ A \end{pmatrix}^l = (\alpha, \beta, \gamma, \ldots)^l (\lambda, \mu, \nu, \ldots)^l (\varphi, \chi, \psi, \ldots)^l \ldots;$$

et, pour que l vérifie l'équation

$$(2) \qquad \begin{pmatrix} B \\ A \end{pmatrix}^l = 1,$$

il faudra qu'on ait séparément

$$(3) \quad (\alpha, \beta, \gamma, \ldots)^l = 1, \quad (\lambda, \mu, \nu, \ldots)^l = 1, \quad (\varphi, \chi, \psi, \ldots)^l = 1, \quad \ldots.$$

Or, les seules valeurs de l, propres à vérifier l'équation (2), seront l'ordre i de la substitution $\begin{pmatrix} B \\ A \end{pmatrix}$ et les multiples de i. Pareillement les valeurs de l propres à vérifier l'une quelconque des formules (3) seront l'ordre du facteur circulaire qui entre dans cette formule et les multiples de cet ordre. Cela posé, soient

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

les nombres qui représentent les ordres respectifs des substitutions circulaires

$$(\alpha, \beta, \gamma, \ldots), \quad (\lambda, \mu, \nu, \ldots), \quad (\varphi, \chi, \psi, \ldots), \quad \ldots;$$

et r le nombre des variables qui se trouvent exclues de la substitution $\begin{pmatrix} B \\ A \end{pmatrix}$ quand elle est réduite à son expression la plus simple. Non seulement on aura

$$(4) \qquad a + b + c + \ldots + r = n,$$

attendu que les divers groupes

$$\alpha, \beta, \gamma, \ldots,$$
$$\lambda, \mu, \nu, \ldots,$$
$$\varphi, \chi, \psi, \ldots,$$
$$\ldots\ldots\ldots$$

devront renfermer en somme les $n - r$ lettres auxquelles se rapporte la substitution $\begin{pmatrix} B \\ A \end{pmatrix}$; mais, de plus, on conclura évidemment de ce qui

précède, que l'ordre i de la substitution $\begin{pmatrix} B \\ A \end{pmatrix}$ sera le plus petit nombre divisible à la fois par a, par b, par c, ...

Considérons maintenant en particulier, parmi les variables x, y, z, ..., celles qui ne sont pas déplacées par la substitution $\begin{pmatrix} B \\ A \end{pmatrix}$ et nommons u l'une de ces dernières. Comme nous l'avons remarqué, la variable u se trouvera exclue de la substitution $\begin{pmatrix} B \\ A \end{pmatrix}$ réduite à son expression la plus simple; mais, d'autre part, rien n'empêchera de mettre cette variable *u en évidence*, et de la considérer comme formant à elle seule un facteur circulaire du premier ordre, savoir, le suivant :

$$\begin{pmatrix} u \\ u \end{pmatrix} = 1.$$

On pourra même présenter ce facteur du premier ordre sous une forme analogue à celles des facteurs circulaires

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

en écrivant simplement (u) au lieu de $\begin{pmatrix} u \\ u \end{pmatrix}$, de même qu'on écrit (x, y), (x, y, z), ... au lieu de $\begin{pmatrix} yx \\ xy \end{pmatrix}$, $\begin{pmatrix} yzx \\ xyz \end{pmatrix}$, ...

Il suit de cette observation que, dans la formule (4), on peut regarder la lettre r comme exprimant le nombre des facteurs circulaires du premier ordre, renfermés dans la substitution $\begin{pmatrix} B \\ A \end{pmatrix}$. Ajoutons que, dans la formule (4), deux ou plusieurs des nombres

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

peuvent être supposés égaux entre eux. Si l'on se place dans cette hypothèse, et si, pour plus de commodité, on suppose la substitution $\begin{pmatrix} B \\ A \end{pmatrix}$ équivalente au produit que l'on obtient quand on multiplie entre eux

f facteurs circulaires de l'ordre a,
g facteurs circulaires de l'ordre b,
h facteurs circulaires de l'ordre c,
.....,

r facteurs circulaires du premier ordre; la formule (4) se trouvera évidemment remplacée par la suivante :

$$fa + gb + hc + \ldots + r = n. \tag{5}$$

Une substitution quelconque $\begin{pmatrix} B \\ A \end{pmatrix}$ sera dite *régulière*, lorsqu'elle sera, ou une substitution circulaire, ou le produit de plusieurs substitutions circulaires de même ordre. Elle sera *irrégulière* dans le cas contraire. Cela posé, l'ordre d'une substitution régulière est évidemment l'ordre de ses facteurs circulaires; de plus, toute substitution régulière est une puissance d'une certaine substitution circulaire. Ainsi, par exemple, la substitution régulière

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

est le cube de la substitution circulaire

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

Enfin, étant donnée une substitution régulière qui renferme plusieurs variables x, y, z, ..., celles de ses puissances qui ne se réduiront pas à l'unité seront des substitutions régulières qui renfermeront nécessairement toutes ces variables. Au contraire, les puissances d'une substitution irrégulière seront, les unes irrégulières, les autres régulières; et celles qui seront régulières renfermeront un moindre nombre de variables. Ainsi, par exemple, la substitution irrégulière

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

qui renferme les variables

$$x, \quad y, \quad z, \quad u, \quad v,$$

aura pour cinquième puissance la substitution irrégulière

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

qui renfermera encore les cinq variables données; mais elle aura pour carré, pour cube et pour quatrième puissance les substitutions régu-

lières

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

dont chacune renfermera deux ou trois variables seulement.

Il est bon d'observer que si, après avoir substitué à l'arrangement A un autre arrangement B, on veut revenir de l'arrangement B à l'arrangement A, cette seconde opération, inverse de la première, sera représentée, non plus par la notation $\binom{B}{A}$, mais par la notation $\binom{A}{B}$. En conséquence, il est naturel de dire que les deux substitutions

$$\binom{B}{A}, \quad \binom{A}{B}$$

sont *inverses* l'une de l'autre. Cela posé, il est clair que, si la substitution $\binom{B}{A}$ fait passer à la place de x une autre variable y, la substitution inverse $\binom{A}{B}$ fera passer, au contraire, x à la place de y. Si la substitution $\binom{B}{A}$ se réduisait à une substitution circulaire du second ordre, en sorte qu'on eût, par exemple,

$$\binom{B}{A} = (x, y),$$

elle aurait pour effet unique d'échanger entre elles les deux variables x, y, et se confondrait avec la substitution inverse

$$\binom{A}{B} = (y, x).$$

Ajoutons que les facteurs circulaires de $\binom{A}{B}$ seront évidemment *inverses* des facteurs circulaires de $\binom{B}{A}$.

II. — *Extension des notations adoptées dans le premier paragraphe. Substitutions semblables entre elles.*

Considérons n variables indépendantes

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

et soient

$$A, \quad B, \quad C, \quad D, \quad \ldots$$

les arrangements divers qui peuvent être formés avec ces variables. Rien n'empêchera de représenter par de simples lettres

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

les substitutions qui consistent à remplacer ces arrangements l'un par l'autre, et de prendre, par exemple,

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

Cela posé, les diverses puissances d'une substitution P se trouveront représentées par les notations

$$P^0 = 1, \quad P, \quad P^2, \quad P^3, \quad \ldots;$$

et si l'on nomme i l'ordre de la substitution P, c'est-à-dire la plus petite des valeurs entières de l pour lesquelles se vérifie la formule

$$P^l = 1; \tag{1}$$

alors, en désignant par k et par l des nombres entiers quelconques, on aura

$$P^{ki+l} = P^l. \tag{2}$$

En généralisant la formule (2), on est naturellement amené à considérer non seulement des puissances positives, mais encore des puissances négatives de la substitution P. En effet, pour assigner une signification précise à la notation

$$P^{-l},$$

il suffit d'étendre, par analogie, la formule (2) au cas même où l devient négatif. Alors on trouve

$$P^{-l} = P^{ki-l}, \tag{3}$$

et, en particulier,

$$P^{-1} = P^{i-1}. \tag{4}$$

Si, pour fixer les idées, on suppose $i = 6$, et

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

on aura

$$P^{-1} = P^5 = (x, z, y)(u, v).$$

La substitution P^{-1} n'étant pas distincte de la substitution P^{i-1}, il en résulte que chacun des produits

$$PP^{-1} \quad \text{ou} \quad P^{-1}P$$

se réduit, comme on devait s'y attendre, à

$$P^i = P^0 = 1.$$

Donc, par suite, si l'on a

$$P = \begin{pmatrix} B \\ A \end{pmatrix},$$

P^{-1} sera la substitution qui, multipliée par $\begin{pmatrix} B \\ A \end{pmatrix}$, donne pour produit l'unité, c'est-à-dire la substitution $\begin{pmatrix} A \\ B \end{pmatrix}$, inverse de $\begin{pmatrix} B \\ A \end{pmatrix}$. Ainsi, les notations

$$P, \quad P^{-1}$$

désignent généralement deux substitutions *inverses* l'une de l'autre.

Ajoutons que l'inverse de la substitution P^i sera évidemment P^{-i}.

Deux substitutions étant toujours inverses l'une de l'autre, quand leur produit est l'unité, on en conclut que la substitution PQ a pour inverse $Q^{-1}P^{-1}$, et que, pareillement, la substitution P^hQ^k a pour inverse $Q^{-k}P^{-h}$.

Deux substitutions distinctes

$$P = \begin{pmatrix} B \\ A \end{pmatrix}, \qquad Q = \begin{pmatrix} D \\ C \end{pmatrix}$$

seront dites *semblables* entre elles, quand elles offriront le même nombre de facteurs circulaires et le même nombre de lettres dans les facteurs circulaires correspondants, en sorte que les facteurs circulaires, comparés deux à deux, soient de même ordre.

D'après cette définition, deux substitutions circulaires de même ordre seront toujours semblables entre elles, et l'on pourra en dire autant de deux substitutions régulières qui, étant de même ordre, offriront le même nombre de facteurs circulaires. Ainsi, par exemple, la substitution circulaire de second ordre

$$(x, y)$$

sera semblable à chacune des substitutions

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

La substitution du troisième ordre

$$(x, y, z)$$

sera semblable, non seulement à son carré

$$(x, z, y),$$

mais encore à chacune des substitutions

$$(x, y, u), \quad (x, z, u), \quad \ldots, \quad (y, z, u), \quad \ldots, \quad (u, v, w), \quad \ldots.$$

Ainsi encore les trois substitutions régulières, du second ordre, que l'on peut former avec quatre variables x, y, z, u, savoir :

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

sont semblables l'une à l'autre.

Étant données deux substitutions P, Q semblables entre elles, on peut toujours écrire la seconde au-dessus de la première, de telle sorte que les facteurs circulaires de même ordre se correspondent deux à deux. Alors, aux diverses variables que renfermait la substitution P, correspondront, dans la substitution Q, d'autres variables qui remplaceront les premières. Cela posé, concevons que l'on présente les deux substitutions P, Q sous les formes

$$P = \begin{pmatrix} B \\ A \end{pmatrix}, \qquad Q = \begin{pmatrix} D \\ C \end{pmatrix},$$

en prenant pour A un arrangement quelconque, et en nommant C celui que l'on obtient, lorsque dans l'arrangement A on remplace chaque variable par la variable correspondante, prise dans la substitution Q. Il est clair que les deux substitutions

$$P = \begin{pmatrix} B \\ A \end{pmatrix} \quad \text{et} \quad Q = \begin{pmatrix} D \\ C \end{pmatrix},$$

quand elles seront semblables l'une à l'autre, déplaceront, de la même manière, les variables qui occupaient les mêmes places dans les

arrangements A et C. Donc alors, si l'on écrit l'un au-dessus de l'autre, d'une part, les arrangements A et C, d'autre part, les arrangements B et D, les variables qui se correspondront dans les arrangements A et C se correspondront encore dans les arrangements B et D, produits, le premier, par l'application de la substitution P à l'arrangement A; le second, par l'application de la substitution Q à l'arrangement C. Donc on aura, dans l'hypothèse admise,

$$\binom{D}{B}=\binom{C}{A}. \tag{5}$$

Réciproquement, si la condition (5) est remplie, les deux substitutions

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

appliquées la première à l'arrangement A, la seconde à l'arrangement C, déplaceront certainement, de la même manière, les variables qui, dans ces deux arrangements, occupaient les mêmes places. Donc, par suite, ces deux substitutions devront offrir le même nombre de facteurs circulaires, et le même nombre de lettres dans les facteurs circulaires correspondants, c'est-à-dire qu'elles seront semblables l'une à l'autre.

Il est bon d'observer que les arrangements ci-dessus désignés par les lettres A, B, C, D sont censés comprendre généralement toutes les variables que l'on considère. Donc, pour trouver les variables qui doivent se correspondre dans les arrangements A et C, il est nécessaire de mettre en évidence toutes les variables, et non pas seulement celles qui se trouveraient renfermées dans les valeurs des substitutions P, Q, réduites à leurs plus simples expressions. Ainsi, par exemple, si les substitutions P, Q, formées chacune avec cinq des six variables

$$x,\ y,\ z,\ u,\ v,\ w,$$

se réduisent aux suivantes

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

elles seront semblables l'une à l'autre. Mais, si l'on veut les présenter sous la forme

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

A, B, C, D étant des arrangements qui vérifient la condition (5), on devra commencer par mettre en évidence les six variables

$$x,\ y,\ z,\ u,\ v,\ w,$$

dans chacune des substitutions P, Q, en introduisant dans la substitution P le facteur de premier ordre (w), et, dans la substitution Q, le facteur (x). Alors, en écrivant Q au-dessus de P, de manière à faire correspondre les uns aux autres les facteurs circulaires de même ordre, on trouvera

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

et, par suite, on pourra prendre

$$A=xyzuvw, \qquad C=yzuvwx.$$

Si l'on adopte effectivement ces valeurs de A et de C, on trouvera encore

$$B=PA=yzxvuw, \qquad D=QB=zuywvx,$$

et, par suite, on aura non seulement

$$\binom{C}{A}=\binom{yzuvwx}{xyzuvw}=(x, y, z, u, v, w),$$

mais aussi

$$\binom{D}{B}=\binom{zuywvx}{yzxvuw}=(y, z, u, v, w, x)=\binom{C}{A}.$$

Donc, les arrangements A, B, C, D seront, comme on devait s'y attendre, du nombre de ceux qui vérifient la formule (5).

Concevons maintenant que, les deux substitutions

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

étant semblables l'une à l'autre, et représentées à l'aide de quatre

arrangements A, B, C, D qui vérifient la condition (5), on pose

$$\binom{C}{A} = R.$$

Alors on tirera de la formule (5), non seulement

$$\binom{D}{B} = \binom{C}{A} = R,$$

mais aussi

$$\binom{B}{D} = \binom{A}{C} = R^{-1}.$$

D'ailleurs on aura identiquement

$$Q = \binom{D}{C} = \binom{D}{B}\binom{B}{A}\binom{A}{C}.$$

Donc, eu égard aux formules

$$\binom{D}{B} = R, \quad \binom{B}{A} = P, \quad \binom{A}{C} = R^{-1},$$

on aura encore

$$Q = RPR^{-1}. \tag{6}$$

Si l'on posait

$$S = R^{-1} = \binom{A}{C},$$

la formule (6) deviendrait

$$Q = S^{-1}PS. \tag{7}$$

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.

On peut remarquer encore que de la formule (6) on tire

$$QR = RP.$$

En conséquence, deux substitutions P, Q sont semblables l'une à l'autre, lorsqu'elles vérifient une équation de la forme

$$QR = RP. \tag{8}$$

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

$$PQ, \quad QP$$

seront certainement des substitutions semblables entre elles. En effet, si l'on pose

$$R = PQ, \quad S = QP, \tag{9}$$

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,

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

On arriverait encore à la même conclusion, en observant que des formules (9) on déduit immédiatement l'équation

$$RP = PS. \tag{10}$$

analogue à la formule (8). On peut donc énoncer la proposition suivante :

Théorème. — *Les deux produits que l'on peut former avec deux substitutions données, en prenant l'une ou l'autre pour multiplicande, sont deux nouvelles substitutions, non seulement de même ordre, mais encore semblables entre elles.*

Ainsi, par exemple, si l'on multiplie 1° (x, y) par (y, z); 2° (y, z)

par (x, y), on obtiendra, dans le second cas comme dans le premier, une substitution du second ordre, et l'on trouvera

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

III. — *Sur les diverses formes que peut revêtir une même substitution, et sur le nombre des substitutions semblables à une substitution donnée.*

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, ..., alors, comme nous l'avons remarqué dans le paragraphe I, 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

$$\begin{pmatrix} yxz \\ xyz \end{pmatrix}, \quad \begin{pmatrix} yzx \\ xzy \end{pmatrix}, \quad \begin{pmatrix} xzy \\ yzx \end{pmatrix}, \quad \begin{pmatrix} xyz \\ yxz \end{pmatrix}, \quad \begin{pmatrix} zyx \\ zxy \end{pmatrix}, \quad \begin{pmatrix} zxy \\ zyx \end{pmatrix}.$$

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,

. . . . . ,

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 qu'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 fac-

teur, 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

$$a^f b^g \dots$$

des ordres de tous les facteurs circulaires par le nombre

$$(1.2\dots f)(1.2\dots g)\dots(1.2\dots r)$$

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

$$\omega = (1.2\dots f)(1.2\dots g)\dots(1.2\dots r)a^f b^g \dots. \tag{2}$$

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 :

$$\begin{array}{lll} (x, y, z)(u)(v), & (y, z, x)(u)(v), & (z, x, y)(u)(v), \\ (x, y, z)(v)(u), & (y, z, x)(v)(u), & (z, x, y)(v)(u). \end{array}$$

Il sera maintenant facile de calculer le nombre des substitutions semblables entre elles, et à une substitution donnée P, qui peuvent être composées avec n variables

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

En effet, nommons

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

ces substitutions semblables à P. Supposons d'ailleurs que l'on représente chacune d'elles 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

$$\omega\varpi = \mathrm{N}, \tag{3}$$

la valeur de N étant

$$\mathrm{N} = 1.2\dots n;$$

et, par suite, on aura encore

$$\varpi = \frac{\mathrm{N}}{\omega}. \tag{4}$$

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, en vertu de la formule (2),

$$\omega = (1.2\dots f)(1.2\dots g)\dots(1.2\dots r)a^f b^g \dots,$$

et par conséquent la formule (3) donnera

$$\varpi = \frac{\mathrm{N}}{(1.2\dots f)(1.2\dots g)\dots(1.2\dots r)\dots a^f b^g \dots}. \tag{5}$$

Si maintenant on désigne par

$$\Sigma\varpi$$

la somme des valeurs de ϖ correspondantes aux divers systèmes de nombres qui peuvent représenter des valeurs de $a, b, c, \dots$, propres

à vérifier l'équation (1) ou, en d'autres termes, si l'on désigne par $\Sigma\varpi$ la somme des valeurs de ϖ correspondantes aux diverses manières de partager le nombre n en parties égales ou inégales, alors $\Sigma\varpi$ devra être précisément le nombre total des substitutions que l'on peut former avec n lettres. On aura donc

$$\Sigma\varpi = N, \tag{6}$$

et, par suite, eu égard à la formule (5),

$$\sum \frac{1}{(1.2\dots f)(1.2\dots g)(1.2\dots h)\dots a^f b^g c^h \dots} = 1. \tag{7}$$

Cette dernière équation paraît digne de remarque. Si, pour fixer les idées, on pose $n = 5$, on trouvera

$$n = 5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1,$$

et, par suite, l'équation (7) donnera

$$\frac{1}{5} + \frac{1}{4}+\frac{1}{2}\frac{1}{3} + \frac{1}{1.2}\frac{1}{3} + \frac{1}{1.2}\frac{1}{2^2} + \frac{2}{1.1.3}\frac{1}{2} + \frac{1}{1.2.3.4.5} = 1,$$

ce qui est exact.

IV. — *Résolution de l'équation linéaire et symbolique par laquelle se trouvent liées l'une à l'autre deux substitutions semblables entre elles.*

Soient P, Q deux substitutions semblables entre elles, formées avec n variables

$$x, \quad y, \quad z, \quad \dots,$$

ou du moins avec plusieurs de ces variables; et supposons

$$\text{P} = (\alpha, \beta, \gamma, \dots, \eta)(\lambda, \mu, \nu, \dots, \rho)\dots(\varphi)(\chi)(\psi)\dots, \tag{1}$$
$$\text{Q} = (\alpha', \beta', \gamma', \dots, \eta')(\lambda', \mu', \nu', \dots, \rho')\dots(\varphi')(\chi')(\psi')\dots, \tag{2}$$

$\alpha', \beta', \gamma', \dots, \eta'$; $\lambda', \mu', \nu', \dots, \rho', \dots$; $\varphi', \chi', \psi', \dots$ désignant les variables qui, dans la substitution Q, ont pris les places qu'occupaient les variables $\alpha, \beta, \gamma, \dots, \eta$; $\lambda, \mu, \nu, \dots, \rho, \dots$; $\varphi, \chi, \psi, \dots$ dans la substitution P. Représentons par

A et C

les arrangements auxquels se réduisent les seconds membres des formules (1) et (2), quand on y supprime les parenthèses et les virgules placées entre les variables, en sorte qu'on ait

$$\text{A} = \alpha\beta\gamma\dots\eta\lambda\mu\nu\dots\rho\dots\varphi\chi\psi\dots, \tag{3}$$
$$\text{C} = \alpha'\beta'\gamma'\dots\eta'\lambda'\mu'\nu'\dots\rho'\dots\varphi'\chi'\psi'\dots. \tag{4}$$

Enfin, soient

$$\text{B} = \text{PA} \quad \text{et} \quad \text{D} = \text{QC} \tag{5}$$

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

$$\text{B} = \beta\gamma\dots\eta\alpha\mu\nu\dots\rho\lambda\dots\varphi\chi\psi\dots, \tag{6}$$
$$\text{D} = \beta'\gamma'\dots\eta'\alpha'\mu'\nu'\dots\rho'\lambda'\dots\varphi'\chi'\psi'\dots. \tag{7}$$

Par conséquent, les variables qui, prises deux à deux, se correspondaient mutuellement 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 (1) et (2), ont eu précisément pour effet de déplacer de la même manière les variables semblablement placées dans les arrangements A et C. On aura donc

$$\binom{\text{D}}{\text{B}} = \binom{\text{C}}{\text{A}}. \tag{8}$$

Cela posé, faisons, pour abréger,

$$\binom{\text{D}}{\text{B}} = \binom{\text{C}}{\text{A}} = \text{R}.$$

On aura, par suite,

$$\text{D} = \text{RB}, \quad \text{C} = \text{RA}; \tag{9}$$

et des équations (9), jointes aux formules (5), on tirera

$$\text{D} = \text{RPA}, \quad \text{D} = \text{QRA},$$

par conséquent

$$\text{QRA} = \text{RPA}, \tag{10}$$

et

$$QR = RP. \tag{11}$$

Réciproquement, si les substitutions P, Q sont liées entre elles par une équation semblable à la formule (11), alors, en appliquant à un arrangement quelconque A la substitution

$$QR = RP,$$

on retrouvera l'équation (10), et, en posant, pour abréger,

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

ou, ce qui revient au même,

$$B = PA, \quad C = RA, \quad D = QC,$$

on tirera de l'équation (10)

$$D = RB, \quad R = \begin{pmatrix} D \\ B \end{pmatrix}.$$

On aura donc alors

$$R = \begin{pmatrix} C \\ A \end{pmatrix} = \begin{pmatrix} D \\ B \end{pmatrix}; \tag{12}$$

et, par suite, les substitutions

$$P = \begin{pmatrix} B \\ A \end{pmatrix}, \quad Q = \begin{pmatrix} D \\ C \end{pmatrix}$$

seront semblables l'une à l'autre, puisque, en vertu de la formule (12), elles devront déplacer de la même manière les variables qui se correspondent dans les deux termes de la substitution

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

Il importe d'observer que les deux membres de la formule (11) 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 (11). 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, 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 ω sera déterminé par l'équation (2) du paragraphe précédent; et, par suite, il est clair que la substitution R admettra un nombre ω de valeurs distinctes. Donc, si l'on résout par rapport à R la formule (11), 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 la formule (11), ou, ce qui revient au même, par la suivante

$$Q = RPR^{-1}, \tag{13}$$

on remarquerait que, pour passer de la valeur de P, donnée par la formule (1), à la valeur de Q, donnée par la formule (2), il suffit de faire subir aux variables x, y, z, ... les déplacements par lesquels on passe de la valeur de A, donnée par la formule (3), à la valeur de C, donnée par la formule (4), 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 (13).

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*

$$RP = QR.$$

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

$$RP = QR,$$

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

$$RP = QR$$

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

$$\begin{pmatrix} xzy \\ xyz \end{pmatrix}, \quad \begin{pmatrix} zxy \\ xyz \end{pmatrix},$$

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

$$\begin{pmatrix} xzyu \\ xyzu \end{pmatrix}, \quad \begin{pmatrix} zxyu \\ xyzu \end{pmatrix}, \quad \begin{pmatrix} xzuy \\ xyzu \end{pmatrix}, \quad \begin{pmatrix} zxuy \\ xyzu \end{pmatrix},$$

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, l'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,

$$RPR^{-1}=(z,x),\qquad PRP^{-1}=(y,z,x).$$

Si l'on supposait, au contraire,

$$P=(x,y),\qquad R=(x,z)(y,u),$$

on trouverait

$$RPR^{-1}=(z,u),\qquad PRP^{-1}=(y,z)(x,u).$$

V. — *Sur les facteurs primitifs d'une substitution donnée.*

Nommons P l'une des substitutions que l'on peut former avec n variables

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

et concevons que l'ordre i de cette substitution ait été décomposé en facteurs

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

premiers entre eux; enfin, soit l un nombre entier quelconque. En vertu d'un théorème précédemment établi (p. 164), on pourra toujours satisfaire à l'équivalence

$$(1)\qquad i\left(\frac{\alpha}{a}+\frac{\beta}{b}+\frac{\gamma}{c}+\ldots\right)\equiv l\pmod i$$

par des valeurs entières de α, β, γ, ... D'ailleurs, i étant l'ordre de la substitution P, une équivalence de la forme

$$l\equiv l'+l''+\ldots\pmod i$$

entraînera toujours l'équation

$$P^l=P^{l'+l''+\ldots}=P^{l'}P^{l''}\ldots,$$

Donc la formule (1) entraînera la suivante :

$$P^l=P^{\frac{l}{a}\alpha}P^{\frac{l}{b}\beta}P^{\frac{l}{c}\gamma}\ldots;$$

et comme, en posant, pour abréger,

$$(2)\qquad P^{\frac{i}{a}}=U,\qquad P^{\frac{i}{b}}=V,\qquad P^{\frac{i}{c}}=W,\qquad \ldots,$$

on aura encore

$$P^{\frac{l}{a}\alpha}=U^\alpha,\qquad P^{\frac{l}{b}\beta}=V^\beta,\qquad P^{\frac{l}{c}\gamma}=W^\gamma,\qquad \ldots,$$

on tirera définitivement de la formule (1), jointe aux équations (2),

$$(3)\qquad P^l=U^\alpha V^\beta W^\gamma\ldots.$$

Dans le cas particulier où l se réduit à l'unité, les exposants α, β, γ, ... sont uniquement assujettis à vérifier l'équivalence

$$(4)\qquad i\left(\frac{\alpha}{a}+\frac{\beta}{b}+\frac{\gamma}{c}+\ldots\right)\equiv 1\pmod i,$$

et la formule (3) donne

$$(5)\qquad P=U^\alpha V^\beta W^\gamma\ldots.$$

Il est bon d'observer que, l'ordre i de la substitution P étant la plus petite valeur entière et positive de l propre à vérifier l'équation

$$P^l=1,$$

l'ordre de la substitution

$$U=P^{\frac{i}{a}},$$

ou la plus petite valeur entière et positive de k propre à vérifier la formule

$$P^{\frac{ik}{a}}=1,$$

sera nécessairement

$$k=a.$$

Pareillement, les ordres des substitutions

$$V=P^{\frac{i}{b}},\qquad W=P^{\frac{i}{c}},\quad \ldots$$

se trouveront représentés par les facteurs b, c, ... du nombre i.

Concevons à présent que, p, q, r, ... étant les facteurs premiers de i, on ait

$$i = p^f q^g r^h \dots. \tag{6}$$

On pourra prendre

$$a = p^f, \quad b = q^g, \quad c = r^h, \quad \dots, \tag{7}$$

et, par suite, les nombres

$$p^f, \quad q^g, \quad r^h, \quad \dots$$

exprimeront les ordres respectifs des substitutions

$$U, \quad V, \quad W, \quad \dots.$$

D'ailleurs, d'après ce qui a été dit à la page 182, l'ordre d'une substitution quelconque P est divisible par l'ordre de chacun des facteurs circulaires de P. Donc l'ordre p^f de la substitution U devra être divisible par l'ordre de chacun des facteurs circulaires de U. Donc, puisque les diviseurs de p^f ne pourront être que des puissances du nombre premier p, la substitution U jouira de cette propriété remarquable, que les ordres de ses divers facteurs circulaires seront tous des puissances d'un même nombre premier p. Pareillement, les ordres des divers facteurs de la substitution V, ou W, ..., seront tous des puissances du nombre premier q ou r, ...

D'autre part, puisque U^α représente le produit de α facteurs égaux à U, que V^β représente le produit de β facteurs égaux à V, ..., il résulte de la formule (5) que la substitution P peut être décomposée en facteurs dont chacun se confonde avec l'une des puissances de P désignées par les lettres U, V, W, ... Cela posé, les substitutions

$$U, \quad V, \quad W, \quad \dots$$

joueront, par rapport à la substitution P de l'ordre i, un rôle analogue à celui que les facteurs

$$p^f, \quad q^g, \quad r^h, \quad \dots,$$

dont chacun est une puissance d'un nombre premier, jouent eux-mêmes par rapport au nombre entier i. On peut remarquer aussi que les substitutions U, V, W, ... représentent des puissances de P desquelles on peut déduire toutes les autres à l'aide des formules (3) et (5). Elles offrent donc encore, pour cette raison, une certaine analogie avec certaines racines des équations binomes, savoir, avec celles qui sont désignées sous le nom de primitives, et qui, élevées à des puissances diverses, reproduisent toutes les autres racines. Pour conserver le souvenir de ces diverses analogies, nous dirons que les substitutions

$$U, \quad V, \quad W, \quad \dots,$$

déterminées par les formules (2) sont les *facteurs primitifs* de la substitution P.

De plus, nous appellerons *substitution primitive* celle qui n'aura d'autres facteurs primitifs qu'elle-même, ou, en d'autres termes, celle dont l'ordre sera une puissance d'un nombre premier.

Cela posé, la substitution

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

formée avec six variables, sera une substitution primitive du quatrième ordre, représentée par le produit de deux facteurs circulaires dont les ordres 2 et 4 se réduiront à la première et à la seconde puissance du nombre premier 2.

Au contraire, la substitution circulaire

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

dont l'ordre est exprimé par le nombre

$$6 = 2.3,$$

sera décomposable en facteurs primitifs, représentés chacun par l'une des substitutions régulières

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

Effectivement, en adoptant les valeurs précédentes de U et V, on trouvera

$$U^2 V = P^7 = P;$$

et, par conséquent,

$$P = U^3 V.$$

Enfin, si l'on pose

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

P sera une substitution du sixième ordre, que l'on pourra décomposer en facteurs primitifs représentés chacun par l'une des deux substitutions circulaires

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

et que l'on déduira encore de ces facteurs à l'aide de la formule

$$P = U^2 V.$$

VI. — *Sur les dérivées d'une ou de plusieurs substitutions, et sur les systèmes de substitutions conjuguées.*

Étant données une ou plusieurs substitutions qui renferment les n lettres $x, y, z, \ldots$, ou du moins plusieurs d'entre elles, je nommerai substitutions *dérivées* toutes celles que l'on pourra déduire des substitutions données, multipliées une ou plusieurs fois les unes par les autres, ou par elles-mêmes, dans un ordre quelconque; et les substitutions données, jointes aux substitutions dérivées, formeront ce que j'appellerai un *système de substitutions conjuguées*. L'ordre de ce système sera le nombre total des substitutions qu'il présente, y compris la substitution qui offre deux termes égaux et se réduit à l'unité.

Lorsque les substitutions données se réduisent à une seule P, les substitutions dérivées se confondent avec les puissances de P et forment un système de substitutions conjuguées qui est d'un ordre représenté par l'ordre de la substitution P.

Le système de toutes les substitutions que l'on peut former avec n lettres $x, y, z, \ldots$ est évidemment un système de substitutions conjuguées. Si l'on nomme

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

les divers arrangements qui peuvent être formés avec les n variables $x, y, z, \ldots$, les substitutions comprises dans le système dont il s'agit seront

$$\text{(1)} \qquad \binom{A}{A}, \quad \binom{B}{A}, \quad \binom{C}{A}, \quad \ldots,$$

et le nombre N de ces substitutions, ou l'ordre du système, sera déterminé par la formule

$$N = 1.2.3 \ldots n.$$

Soit maintenant

$$\text{(2)} \qquad 1, \quad P, \quad Q, \quad R, \quad \ldots$$

un système quelconque de substitutions conjuguées. D'après la définition même d'un tel système, on devra toujours reproduire les mêmes substitutions, rangées seulement d'une autre manière, si on les multiplie séparément par l'une quelconque d'entre elles, ou bien encore si l'une quelconque d'entre elles est séparément multipliée par elle-même et par toutes les autres. Donc, si l'on nomme S l'une quelconque des substitutions (2), les divers termes de la série

$$\text{(3)} \qquad S, \quad SP, \quad SQ, \quad SR, \quad \ldots,$$

ou bien encore de la série

$$\text{(4)} \qquad S, \quad PS, \quad QS, \quad RS, \quad \ldots,$$

se confondront avec les termes de la série (2) rangés dans un nouvel ordre.

Ajoutons qu'il est facile d'établir les propositions suivantes :

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 variables.*

Démonstration. — Supposons que le système donné soit celui que présente la série (2), et nommons M l'ordre de ce système. Si la série (2) se confond avec la série (1), on aura précisément $M = N$; dans le cas contraire, désignons par U, V, W, ... des substitutions qui fassent partie de la série (1) sans appartenir à la série (2). Si l'on nomme m le nombre des termes de la série

$$\text{(5)} \qquad 1, \quad U, \quad V, \quad W, \quad \ldots,$$

le tableau

$$\text{(6)} \qquad \begin{cases} 1, & P, & Q, & R, & \ldots, \\ U, & UP, & UQ, & UR, & \ldots, \\ V, & VP, & VQ, & VR, & \ldots, \\ W, & WP, & WQ, & WR, & \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

offrira m suites horizontales composées chacune de M termes, et tous les termes de chaque suite seront distincts les uns des autres. Si, d'ailleurs, deux suites horizontales différentes, par exemple la deuxième 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 série (2). Donc alors, dans le tableau (6), le premier terme V de la troisième suite horizontale serait déjà un des termes de la seconde. Donc tous les termes du tableau (6) seront distincts les uns des autres, si le premier terme de chaque suite horizontale est pris en dehors des suites précédentes. Or concevons qu'en remplissant toujours cette condition, on ajoute sans cesse au tableau (6) 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 (6) renfermera les N termes compris dans la suite (1); mais alors on aura évidemment

$$N = mM. \tag{7}$$

Donc M sera un diviseur de N.

Corollaire. — Il est bon d'observer qu'au tableau (6) on pourrait substituer un autre tableau de la forme

$$\left\{\begin{array}{llll} 1, & P, & Q, & R, \ldots, \\ U, & PU, & QU, & RU, \ldots, \\ V, & PV, & QV, & RV, \ldots, \\ W, & PW, & QW, & RW, \ldots, \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \end{array}\right. \tag{8}$$

THÉORÈME II. — *L'ordre d'un système de substitutions conjuguées est divisible par l'ordre de chacune de ces substitutions.*

Démonstration. — Supposons toujours que le système donné soit celui que présente la série (2). Si l'on nomme a l'ordre de la substitution P, la suite (5) devra renfermer en premier lieu les substitutions

$$1, \quad P, \quad P^2, \quad \ldots, \quad P^{a-1}. \tag{9}$$

Soit d'ailleurs Q l'une des substitutions qui appartiennent à la série (2) sans faire partie de la suite (9). La suite (2) renfermera les substitutions

$$Q, \quad PQ, \quad P^2Q, \quad \ldots, \quad P^{a-1}Q, \tag{10}$$

et aucune de celles-ci ne pourra se confondre avec l'une des substitutions

$$1, \quad P, \quad P^2, \quad \ldots, \quad P^{a-1};$$

car si l'on avait, par exemple,

$$P^kQ = P^h,$$

on en conclurait

$$Q = P^{h-k}.$$

Soit encore R une substitution qui fasse partie de la suite (2), sans être renfermée, ni dans la suite (9), ni dans la suite (10). La suite (2) renfermera nécessairement les substitutions

$$R, \quad PR, \quad P^2R, \quad \ldots, \quad P^{a-1}R;$$

et aucune de ces dernières ne sera comprise, ni dans la suite (9), ni même dans la suite (10); car, si l'on avait, par exemple,

$$P^kR = P^hQ,$$

on en conclurait

$$R = P^{h-k}Q.$$

En continuant ainsi, on partagera facilement la suite des substitutions conjuguées

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

en plusieurs suites,

$$\left\{\begin{array}{llll} 1, & P, & P^2, & \ldots, \quad P^{a-1}, \\ Q, & PQ, & P^2Q, & \ldots, \quad P^{a-1}Q, \\ R, & PR, & P^2R, & \ldots, \quad P^{a-1}R, \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \end{array}\right. \tag{11}$$

dont chacune renfermera a substitutions diverses. Donc, si l'on

nomme M le nombre des substitutions conjuguées

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

ou, ce qui revient au même, l'ordre de leur système, M sera un multiple de a.

Corollaire. — Il importe d'observer qu'en opérant toujours de la même manière, on pourrait intervertir l'ordre des facteurs, et substituer ainsi au tableau (11) un tableau de la forme

$$(12)\qquad \begin{cases} 1, & P, & P^2, & \ldots, & P^{a-1}, \\ Q, & QP, & QP^2, & \ldots, & QP^{a-1}, \\ R, & RP, & RP^2, & \ldots, & RP^{a-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Théorème III. — *Soient*

$$P,\quad Q$$

deux substitutions, la première de l'ordre a, la seconde de l'ordre b; et supposons ces deux substitutions permutables entre elles, en sorte qu'on ait

$$(13)\qquad QP = PQ.$$

Si d'ailleurs, h, k étant deux entiers quelconques, l'équation

$$(14)\qquad P^hQ^k = 1$$

ne se vérifie jamais, excepté dans le cas où l'on a

$$(15)\qquad P^h = 1,\qquad Q^k = 1,$$

les deux substitutions P, Q *et leurs dérivées composeront un système de substitutions conjuguées dont l'ordre sera précisément le produit ab.*

Démonstration. — En effet, soit S une dérivée quelconque des deux substitutions P, Q. Cette dérivée sera le produit de facteurs égaux, les uns à P, les autres à Q; mais, en vertu de la formule (13), l'ordre dans lequel ces facteurs seront écrits pourra être interverti arbitrairement. Donc on pourra faire en sorte que chacun des facteurs égaux à P précède chacun des facteurs égaux à Q, et réduire S à la forme

$$(16)\qquad S = P^hQ^k.$$

Cela posé, comme les valeurs distinctes de P^h répondront aux valeurs

$$0,\quad 1,\quad 2,\quad \ldots,\quad a-1$$

de l'exposant h, et les valeurs distinctes de Q^k aux valeurs

$$0,\quad 1,\quad 2,\quad \ldots,\quad b-1$$

de l'exposant k, il est clair que les valeurs distinctes de S seront toutes comprises dans le tableau

$$(17)\qquad \begin{cases} 1, & P, & P^2, & \ldots, & P^{a-1}, \\ Q, & PQ, & P^2Q, & \ldots, & P^{a-1}Q, \\ Q^2, & PQ^2, & P^2Q^2, & \ldots, & P^{a-1}Q^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ Q^{b-1}, & PQ^{b-1}, & P^2Q^{b-1}, & \ldots, & P^{a-1}Q^{b-1}. \end{cases}$$

Elles seront donc représentées par les divers termes de ce tableau, si ces termes sont tous inégaux entre eux. Or, c'est ce qui arrivera certainement dans l'hypothèse admise; car, si l'on suppose

$$(18)\qquad P^hQ^k = P^{h'}Q^{k'},$$

h, h' désignant deux nombres dont chacun soit inférieur à l'ordre a de la substitution P, et k, k' deux nombres dont chacun soit inférieur à l'ordre b de la substitution Q, l'équation (18) donnera

$$(19)\qquad P^{h-h'}Q^{k-k'} = 1;$$

et puisque, dans l'hypothèse admise, la formule (14) entraîne toujours les formules (15), l'équation (19) entraînera les suivantes :

$$P^{h-h'} = 1,\qquad Q^{k-k'} = 1,$$

desquelles on tirera

$$(20)\qquad P^{h'} = P^h,\qquad Q^{k'} = Q^k.$$

Donc, si les conditions (20) ne sont pas remplies, l'équation (18) ne pourra subsister, et l'on peut affirmer que deux termes distincts du tableau (17) auront des valeurs distinctes. D'ailleurs les termes de ce tableau, qui renferme a lignes verticales et b lignes horizontales, sont en nombre égal au produit ab. Donc, dans l'hypothèse admise, ce produit représentera précisément le nombre des valeurs distinctes

de S, ou, ce qui revient au même, l'ordre du système des substitutions dérivées de P et de Q.

Observons au reste que, dans l'hypothèse admise, on aura identiquement

$$P^h Q^k = Q^k P^h,$$

et qu'en conséquence les substitutions (17) se confondront respectivement avec celles que renferme le tableau

$$(21)\qquad \begin{cases} 1, & P, & P^2, & \ldots, & P^{a-1}, \\ Q, & QP, & QP^2, & \ldots, & QP^{a-1}, \\ Q^2, & Q^2P, & Q^2P^2, & \ldots, & Q^2P^{a-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ Q^{b-1}, & Q^{b-1}P, & Q^{b-1}P^2, & \ldots, & Q^{b-1}P^{a-1}. \end{cases}$$

Des raisonnements entièrement semblables à ceux dont nous venons de faire usage suffiraient encore pour établir les propositions suivantes :

Théorème IV. — *Soient*

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

diverses substitutions permutables entre elles, en sorte qu'on ait

$$(22)\qquad QP = PQ, \quad RP = PR, \quad \ldots, \quad RQ = QR, \quad \ldots;$$

et nommons

a l'ordre de la substitution P,
b l'ordre de la substitution Q,
c l'ordre de la substitution R,
. . . .

Si, d'ailleurs, h, k, l, . . . étant des entiers quelconques, l'équation

$$(23)\qquad P^h Q^k R^l \ldots = 1$$

ne se vérifie jamais, excepté dans le cas où l'on a

$$(24)\qquad P^h = 1, \quad Q^k = 1, \quad R^l = 1, \quad \ldots;$$

les substitutions P, Q, R, . . . *et leurs dérivées composeront un système de*

substitutions conjuguées dont l'ordre sera précisément le produit abc. . . des ordres des substitutions données P, Q, R, ...

Corollaire. — Il est clair que l'équation (23) entrainera toujours les équations (24), si les substitutions

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

réduites à leurs plus simples expressions, sont formées avec des variables diverses, en sorte que jamais deux de ces substitutions ne renferment la même variable. En effet, concevons que les substitutions

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

soient formées, la première avec les seules variables $\alpha, \beta, \gamma, \ldots$, la seconde avec les seules variables $\lambda, \mu, \nu, \ldots$, la troisième avec les seules variables $\varphi, \chi, \psi, \ldots$. Ces divers systèmes de variables seront encore ceux qui serviront respectivement à former les substitutions

$$P^h, \quad Q^k, \quad R^l, \quad \ldots,$$

$h, k, l, \ldots$ étant des nombres entiers quelconque. Cela posé, pour appliquer à un facteur quelconque une substitution de la forme

$$S = P^h Q^k R^l \ldots,$$

il suffira de faire subir aux variables $\alpha, \beta, \gamma, \ldots$ les déplacements indiqués par la substitution P^h, aux variables $\lambda, \mu, \nu, \ldots$ les déplacements indiqués par la substitution Q^k, aux variables $\varphi, \chi, \psi, \ldots$ les déplacements indiqués par la substitution R^l, ... Donc, pour que l'équation (23) subsiste, ou, ce qui revient au même, pour qu'aucune des variables données ne soit déplacée par la substitution S, il sera nécessaire et il suffira que les variables $\alpha, \beta, \gamma, \ldots$ ne se trouvent point déplacées par la substitution P^h, ni les variables $\lambda, \mu, \nu, \ldots$ par la substitution Q^k, ni les variables $\varphi, \chi, \psi, \ldots$ par la substitution R^l, . . . , et que l'on ait en conséquence

$$P^h = 1, \quad Q^k = 1, \quad R^l = 1, \quad \ldots.$$

On peut énoncer encore la proposition suivante :

THÉORÈME V. — *Soient*

(25) P, Q, R, ...

diverses substitutions formées avec des variables diverses. *Non seulement ces substitutions seront permutables entre elles, mais, de plus, étant jointes à leurs dérivées, elles fourniront un système de substitutions conjuguées, qui sera d'un ordre représenté par le produit des ordres des substitutions* P, Q, R, ...

Corollaire. — Si la série (25) renferme une seule substitution de l'ordre a, une seule de l'ordre b, une seule de l'ordre c, ...; l'ordre du système des substitutions P, Q, R, ... et de leurs dérivées sera le produit $abc\ldots$. Si, au contraire, la série (25) renferme h substitutions de l'ordre a, k substitutions de l'ordre b, l substitutions de l'ordre c, ..., ces diverses solutions, jointes à leurs dérivées, composeront un système dont l'ordre sera représenté par le produit

$$a^h b^k c^l \ldots.$$

VII. — *Sur les systèmes de substitutions primitives et conjuguées.*

Soient P une substitution régulière qui renferme n variables x, y, z, ..., a l'ordre de cette substitution, b le nombre de ses facteurs circulaires; les trois nombres a, b, n seront liés entre eux par la formule

$$n = ab.$$

Cela posé, concevons que l'on range sur b lignes horizontales distinctes, et sur a lignes verticales, les n 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 n, en prenant pour facteurs de Q a substitutions circulaires de l'ordre b, dans chacune desquelles seraient 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, 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

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

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

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

Si, pour fixer les idées, on pose

$$n = 4 = 2 \times 2,$$

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

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

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

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

alors, avec les six variables

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

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 n variables données sur b lignes horizontales et sur a 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

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

Ainsi, par exemple, on pourrait représenter les six variables

$$\begin{matrix} x, & y, & z, \\ u, & v, & w. \end{matrix}$$

par

$$\begin{matrix} s_{\alpha,\lambda}, & s_{\beta,\lambda}, & s_{\gamma,\lambda}, \\ s_{\alpha,\mu}, & s_{\beta,\mu}, & s_{\gamma,\mu}; \end{matrix}$$

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 sensible la propriété qu'ont ces deux substitutions d'être permutables entre elles.

Concevons maintenant que le nombre entier

$$n = abc\ldots$$

soit décomposable en plusieurs facteurs a, b, c, ..., égaux ou inégaux. Alors on pourra représenter n variables diverses

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

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

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

Cela posé, les substitutions P, Q, ... qui, étant exprimées à l'aide des lettres α, β, γ, ..., λ, μ, ν, ..., φ, χ, ψ, ..., se présenteront sous les formes

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

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

$$n = abc\ldots.$$

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

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

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

Q étant pareillement le produit de $\frac{n}{b}$ facteurs circulaires de l'ordre b.

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

$$n = a^l,$$

et les substitutions

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

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.

Au reste, les propositions diverses auxquelles nous venons de parvenir peuvent encore être généralisées, ainsi que nous allons l'expliquer.

Considérons toujours un système de n variables

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

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

$$(4) \qquad P_1, \quad P_2, \quad \ldots, \quad P_h$$

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 leur 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 (4) 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 pre-

mière espèce, et dont le nombre soit égal à k. Cela posé, nommons

$$(5) \qquad Q_1, \quad Q_2, \quad \ldots, \quad Q_k$$

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 (5), 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 (4). Par suite, le système des substitutions (4) et (5), et de leurs dérivées, sera de l'ordre

$$a^h b^k.$$

En continuant ainsi, on établira généralement la proposition suivante :

THÉORÈME I. — *Considérons un système de n variables x, y, z, ... 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*

$$a^h b^k c^l \ldots.$$

Corollaire. — En supposant les nombres a, b, c, ... 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 primitives, dont l'ordre sera représenté par le produit*

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

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 (1) à la plus haute puissance de p qui divise exactement le

(1) Soit p^f la plus haute puissance de p qui divise exactement le produit

$$N = 1.2.3\dots n.$$

Pour que $p^{h+k+l+\dots}$ se réduise à p^f, il sera nécessaire et il suffira que l'on ait

$$h + k + l + \dots = f.$$

Or, effectivement, on sait que l'exposant f de la plus haute puissance de p, qui divise N, est la somme des entiers contenus dans les fractions

$$\frac{n}{p}, \quad \frac{n}{p^2}, \quad \frac{n}{p^3}, \quad \dots,$$

et il est clair que, dans l'hypothèse admise, ces entiers seront précisément les nombres représentés par

$$h, \quad k, \quad l, \quad \dots.$$

Au reste, on peut arriver très simplement à l'équation

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

de la manière suivante :

Soient, comme ci-dessus,

hp le plus grand multiple de p contenu dans n,
kp le plus grand multiple de p contenu dans h,
lp le plus grand multiple de p contenu dans k,
.....

Évidemment p^f, ou la plus haute puissance de p qui divise le produit

$$N = 1.2.3\dots n,$$

sera en même temps la plus haute puissance de p qui divisera le produit

$$p.2p.3p\dots hp = 1.2.3\dots hp^h.$$

Donc, par suite,

$$\frac{p^f}{p^h} = p^{f-h}$$

sera la plus haute puissance de p qui divisera le produit

$$1.2.3\dots h;$$

mais kp étant le plus grand multiple de p contenu dans h, p^{f-h} sera encore la

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, ... 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*

$$N = 1.2.3\dots n.$$

Avec plusieurs des variables x, y, z, ... choisies arbitrairement en nombre égal à i, on pourra toujours former un système de substitutions primitives conjuguées, qui sera de l'ordre p^f.

plus haute puissance de p qui divisera le produit

$$p.2p.3p\dots kp = 1.2.3\dots kp^k.$$

Donc, par suite,

$$\frac{p^{f-h}}{p^k} = p^{f-h-k}$$

sera la plus haute puissance de p qui divisera le produit

$$1.2\dots k.$$

En continuant ainsi, on reconnaîtra que les plus hautes puissances de p qui diviseront les produits

$$1.2.3\dots n, \quad 1.2.3\dots h, \quad 1.2.3\dots k, \quad 1.2.3\dots l, \quad \dots$$

sont respectivement les divers termes de la suite

$$p^f, \quad p^{f-h}, \quad p^{f-h-k}, \quad p^{f-h-k-l}, \quad \dots.$$

Or, cette même suite aura nécessairement pour dernier terme

$$p^0 = 1,$$

et comme ce dernier terme sera aussi de la forme

$$p^{f-h-k-l-\dots},$$

on aura définitivement

$$p^{f-h-k-l-\dots} = 1,$$

ou, ce qui revient au même,

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

Pour montrer une application des principes que nous venons d'établir, considérons en particulier cinq variables

$$x,\ y,\ z,\ u,\ v,$$

et supposons d'ailleurs $p = 2$. On aura, dans ce cas,

$$n = 5, \qquad N = 1.2.3.4.5 = 120,$$
$$i = 4 = 2p, \qquad h = 2, \qquad k = 1,$$

et, par suite,

$$f = h + k = 3, \qquad p^f = 4.2 = 8.$$

Donc, si l'on prend au hasard quatre des cinq variables données, on pourra toujours, avec ces quatre variables, par exemple avec x, y, z, u, former un système de substitutions régulières conjuguées, qui sera d'un ordre représenté par le nombre 8. Effectivement, partageons les quatre variables

$$x,\ y,\ z,\ u$$

en deux groupes

$$x,\ y,$$
$$z,\ u,$$

composés chacun de deux variables, et nommons

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

deux substitutions circulaires du second ordre, dont chacune soit formée avec les variables comprises dans un seul groupe. Soit, de plus,

$$Q = (x, z)(y, u)$$

la substitution qui consiste à échanger les deux groupes

$$x,\ y,$$
$$z,\ u,$$

l'un contre l'autre. Les trois substitutions

$$P_1, \quad P_2, \quad \text{et} \quad Q$$

seront permutables entre elles, et, en les joignant à leurs dérivées, on obtiendra un système de huit substitutions régulières et conjuguées,

qui seront respectivement

$$1, \quad P_1, \quad P_2, \quad P_1P_2,$$
$$Q, \quad P_1Q, \quad P_2Q, \quad P_1P_2Q,$$

ou, ce qui revient au même,

$$1, \qquad (x, y), \qquad (z, u), \qquad (x, y)(z, u),$$
$$(x, z)(y, u), \quad (x, z, y, u), \quad (x, u, y, z), \quad (x, u)(y, z).$$

Concevons maintenant que les variables données

$$x,\ y,\ z,\ u,\ v,\ w$$

soient au nombre de six, et que l'on prenne $p = 3$. Alors on aura

$$n = 6, \qquad N = 1.2.3.4.5.6 = 720,$$
$$i = 6 = 2p, \qquad h = 2,$$

et, par suite,

$$f = h = 2, \qquad p^f = 3^2 = 9.$$

Cela posé, on conclura du théorème III qu'avec les six variables x, y, z, u, v, w on peut former un système de neuf substitutions régulières et conjuguées. Effectivement, partageons ces six variables en deux groupes

$$x,\ y,\ z,$$
$$u,\ v,\ w,$$

composés chacun de trois variables, et nommons

$$P_1 = (x, y, z), \qquad P_2 = (u, v, w)$$

deux substitutions circulaires du troisième ordre, dont chacune soit formée avec les variables comprises dans un seul groupe. Ces deux substitutions seront permutables entre elles, et, en les joignant à leurs dérivées, on obtiendra un système de neuf substitutions régulières et conjuguées qui seront respectivement

$$1, \quad P_1, \quad P_1^2,$$
$$P_2, \quad P_1P_2, \quad P_1^2P_2,$$
$$P_2^2, \quad P_1P_2^2, \quad P_1^2P_2^2,$$

ou, ce qui revient au même,

$$1, \qquad (x, y, z), \qquad (x, z, y),$$
$$(u, v, w), \quad (x, y, z)(u, v, w), \quad (x, z, y)(u, v, w),$$
$$(u, w, v), \quad (x, y, z)(u, w, v), \quad (x, z, y)(u, w, v).$$

Concevons, enfin, que les variables données

$$x, \quad y, \quad z, \quad u, \quad v, \quad w$$

étant toujours au nombre de six, on prenne $p = 2$. Alors on aura non seulement

$$n = 6, \qquad N = 1.2.3.4.5.6,$$

mais encore

$$i = n = 6 = 3p, \qquad h = 3, \qquad k = 1,$$

et par suite

$$f = h + k = 4, \qquad p^f = 2^4 = 16.$$

Cela posé, on conclura du théorème III, qu'avec les six variables x, y, z, u, v, w on peut former seize substitutions primitives et conjuguées. Effectivement, partageons ces six variables en trois groupes

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

et nommons

$$P_1 = (x, y), \qquad P_2 = (z, u), \qquad P_3 = (v, w)$$

trois substitutions circulaires du second ordre dont chacune soit formée avec les variables comprises dans un seul groupe. Soit, de plus,

$$Q = (x, z)(y, u)$$

la substitution qui consiste à échanger les deux premiers groupes

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

l'un contre l'autre. Les quatre substitutions

$$P_1, \quad P_2, \quad P_3 \quad \text{et} \quad Q$$

seront permutables entre elles; et, en les joignant à leurs dérivées, on obtiendra un système de seize substitutions primitives et conjuguées qui seront respectivement

$$\begin{matrix} 1, & P_1, & P_2, & P_3, \\ P_1P_2P_3, & P_3P_2, & P_2P_1, & P_1P_3, \\ Q, & P_1Q, & P_2Q, & P_3Q, \\ P_1P_2P_3Q, & P_2P_3Q, & P_3P_1Q, & P_1P_2Q; \end{matrix}$$

ou, ce qui revient au même,

$$\begin{matrix} 1, & (x, y), & (z, u), & (v, w), \\ (x, y)(z, u)(v, w), & (z, u)(v, w), & (v, w)(x, y), & (x, y)(z, u), \\ (x, z)(y, u), & (x, z, y, u), & (x, u, y, z), & (x, z)(y, u)(v, w), \\ (x, u)(y, z)(v, w), & (x, u, y, z)(v, w), & (x, z, y, u)(v, w), & (x, u)(y, z). \end{matrix}$$

Il est bon d'observer que ce dernier système de substitutions conjuguées renferme, avec l'unité, trois substitutions circulaires du second ordre, savoir

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

huit substitutions régulières du second ordre, savoir

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

et

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

deux substitutions régulières du quatrième ordre, savoir

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

dont l'une est le cube de l'autre; enfin deux substitutions primitives du quatrième ordre, savoir

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

dont l'une est encore le cube de l'autre.

VIII. — *Sur les diverses puissances d'une même substitution.*

Soient P une substitution quelconque, et i l'ordre de cette substitution. Les diverses puissances de P, ou, ce qui revient au même, les dérivées diverses de P, se réduiront aux divers termes de la suite

$$(1) \qquad 1, \quad P, \quad P^2, \quad \ldots, \quad P^{i-1},$$

dont le premier peut encore être représenté par P^0; et si, en nommant r un des nombres

$$(2) \qquad 0, \quad 1, \quad 2, \quad \ldots, \quad i-1,$$

on désigne par l un entier qui, divisé par i, donne r pour reste, la

formule

$$l \equiv r \pmod{i}$$

entraînera la suivante

$$P^l = P^r.$$

Soient maintenant

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

les divers facteurs circulaires de P formés avec des variables qui sont toutes distinctes les unes des autres. L'équation

$$P = \mathfrak{U}\mathfrak{V}\mathfrak{W}\ldots \tag{3}$$

entraînera la suivante

$$P^l = \mathfrak{U}^l\mathfrak{V}^l\mathfrak{W}^l\ldots, \tag{4}$$

quel que soit l'exposant l; et, comme les divers facteurs $\mathfrak{U}^l$, $\mathfrak{V}^l$, $\mathfrak{W}^l$, ... de la substitution P^l sont formés avec des variables diverses, le seul cas où la substitution P^l ne déplacera aucune variable sera évidemment celui où chacun des facteurs $\mathfrak{U}^l$, $\mathfrak{V}^l$, $\mathfrak{W}^l$, ... remplira cette même condition. En d'autres termes, pour que l'on ait

$$P^l = 1, \tag{5}$$

il sera nécessaire et il suffira que l'on ait séparément

$$\mathfrak{U}^l = 1, \quad \mathfrak{V}^l = 1, \quad \mathfrak{W}^l = 1, \quad \ldots. \tag{6}$$

D'ailleurs, les diverses valeurs entières et positives de l propres à vérifier la formule (3) seront l'ordre i de la substitution P et les multiples de cet ordre. Pareillement, les diverses valeurs de l propres à vérifier l'une quelconque des formules (4) seront l'ordre du facteur circulaire qui entre dans cette formule et les multiples de cet ordre. Cela posé, il est clair que la plus petite des valeurs positives de l propres à vérifier la formule (3) ou l'ordre i de la substitution P, devra être le plus petit nombre divisible à la fois par les ordres des divers facteurs circulaires $\mathfrak{U}$, $\mathfrak{V}$, $\mathfrak{W}$, ... Ainsi se trouve rigoureusement établie la proposition que nous avons déjà indiquée page 182, et que l'on peut énoncer comme il suit :

THÉORÈME I. — *L'ordre d'une substitution quelconque* P, *représentée par le produit de plusieurs facteurs circulaires*

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

est le plus petit nombre qui soit divisible par l'ordre de chacun de ces facteurs.

Soit maintenant h un nombre entier quelconque, et posons

$$S = P^h. \tag{7}$$

La substitution S sera l'une quelconque des dérivées de P. D'ailleurs, l'équation (7) entraînera la suivante

$$S^l = P^{hl}, \tag{8}$$

et, par suite, la formule

$$S^l = 1 \tag{9}$$

donnera

$$P^{hl} = 1. \tag{10}$$

Donc l'ordre de la substitution S, ou la plus petite des valeurs de l propres à vérifier la formule (9), sera en même temps la plus petite des valeurs de l propres à vérifier la formule (10) et, par conséquent, l'équivalence

$$hl \equiv 0 \pmod{i}, \tag{11}$$

ou, ce qui revient au même, la plus petite des valeurs de l qui rendront le produit hl divisible par i. Or, si l'on nomme θ le plus grand commun diviseur de h et de i, les seules valeurs de l qui rendront le produit hl divisible par i seront le rapport $\frac{i}{\theta}$ et les multiples de ce rapport. Donc l'ordre de la substitution $S = P^h$ sera précisément le rapport $\frac{i}{\theta}$, et l'on pourra énoncer encore la proposition suivante :

THÉORÈME II. — *Soit* P *une substitution de l'ordre* i. *Soient, de plus,* h *un nombre entier quelconque, et* θ *le plus gand commun diviseur des entiers* h *et* i. *L'ordre de la substitution* P^h *sera représenté par le rapport* $\frac{i}{\theta}$.

Corollaire. — Pour que $\frac{i}{\theta}$ se réduise à i, il est nécessaire et il suffit que l'on ait $\theta = 1$, c'est-à-dire que le plus grand commun diviseur de h et de i se réduise à l'unité; en d'autres termes, il est nécessaire et il suffit que h soit premier à i. D'ailleurs, lorsque cette condition se trouve remplie, h est nécessairement premier à chacun des facteurs de i, par conséquent à l'ordre de chacun des facteurs circulaires

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

de la substitution P. Donc alors les ordres de ces divers facteurs sont respectivement égaux à ceux des substitutions

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

et la formule

$$\mathrm{P}^h = \mathfrak{U}^h \mathfrak{V}^h \mathfrak{W}^h \ldots, \tag{12}$$

qui se déduit immédiatement de l'équation (3), fournit pour valeur de P^h une substitution semblable à la substitution P. On peut donc énoncer encore la proposition suivante :

Théorème III. — *P étant une substitution de l'ordre i, les substitutions qui seront de cet ordre, parmi les diverses puissances de* P, *se confondront avec les puissances dont les degrés sont premiers à i. De plus, ces substitutions seront toutes semblables à* P; *en conséquence, la suite*

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

offrira autant de termes semblables à P *qu'il y a de nombres entiers inférieurs à i et premiers à i.*

Corollaire. — Soit θ un diviseur quelconque de i, et posons

$$i = \theta j. \tag{13}$$

En vertu du deuxième théorème, une puissance P^h de P sera de l'ordre $j = \frac{i}{\theta}$ lorsque h sera de la forme

$$h = \theta k, \tag{14}$$

k étant premier à j. Or, dans cette hypothèse, en faisant, pour

abréger,

$$\mathrm{P}^\theta = \Theta, \tag{15}$$

on trouvera

$$\mathrm{P}^h = \Theta^k; \tag{16}$$

et comme, en vertu de la formule (15), Θ sera une substitution de l'ordre j, on conclura de la formule (16), jointe au troisième théorème, que P^h est une substitution semblable à $\mathrm{P}^\theta = \Theta$. Enfin il est clair que le nombre h déterminé par la formule (14) sera inférieur à i et premier à i, si le nombre k est inférieur à j et premier à j. Cela posé, on pourra évidemment énoncer la proposition suivante :

Théorème IV. — *P étant une substitution de l'ordre i, θ un diviseur quelconque de i, et j la valeur entière du rapport $\frac{i}{\theta}$, les substitutions qui seront de l'ordre j, parmi les diverses puissances de* P, *se confondront avec les puissances dont les degrés, divisés par θ, donneront pour quotients des nombres entiers premiers à j. De plus, ces substitutions seront toutes semblables à P^θ; en conséquence, la suite*

$$1, \quad \mathrm{P}, \quad \mathrm{P}^2, \quad \ldots, \quad \mathrm{P}^{j-1}$$

offrira autant de termes semblables à P^θ qu'il y a de nombres entiers inférieurs à j et premiers à j.

Pour montrer une application des théorèmes qui précèdent, considérons en particulier la substitution circulaire de même ordre

$$\mathrm{P} = (x, y, z, u, v, w).$$

Dans ce cas le nombre

$$i = 6$$

aura pour diviseurs, outre l'unité, les nombres

$$2, \quad 3, \quad 6,$$

et les puissances distinctes de P seront

$$1, \quad \mathrm{P}, \quad \mathrm{P}^2, \quad \mathrm{P}^3, \quad \mathrm{P}^4, \quad \mathrm{P}^5.$$

D'ailleurs, parmi les nombres

$$0,\quad 1,\quad 2,\quad 3,\quad 4,\quad 5,$$

qui représenteront les degrés de ces puissances, deux seulement, savoir : 1 et 5, seront premiers à 6; deux autres, savoir 2 et 4, seront les produits du diviseur 2 par des facteurs 1 et 2 premiers à $3=\frac{6}{2}$; enfin le seul nombre 3 pourra être considéré comme le produit du diviseur 3 par un facteur 1 premier à $2=\frac{6}{3}$. Donc, en vertu des théorèmes III et IV, parmi les cinq puissances de P distinctes de l'unité, on trouvera deux substitutions circulaires du sixième ordre, savoir

$$P \quad \text{et} \quad P^5,$$

deux substitutions circulaires du troisième ordre, savoir

$$P^2 \quad \text{et} \quad P^4,$$

et une seule substitution circulaire du second ordre, savoir

$$P^3.$$

On aura effectivement

$$\begin{aligned} P &= (x, y, z, u, v, w), & P^2 &= (x, w, v, u, z, y),\\ P^3 &= (x, z, v)(y, u, w), & P^4 &= (x, v, z)(y, w, u),\\ & & P^5 &= (x, u)(y, v)(z, w). \end{aligned}$$

Lorsque l'ordre de la substitution P est représenté par un nombre premier, alors, en vertu du théorème III, les puissances de P distinctes de l'unité sont toutes semblables à P. Ainsi, par exemple, si l'on prend pour P la substitution régulière du deuxième ordre

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

les puissances de P distinctes de l'unité, savoir

$$P, \quad P^2,$$

sont toutes deux des substitutions régulières du troisième ordre. On trouvera, en effet,

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

Pareillement, si l'on prend pour P la substitution circulaire du

cinquième ordre

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

les quatre puissances de P distinctes de l'unité, savoir

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

seront toutes des substitutions circulaires du cinquième ordre. On aura, en effet,

$$\begin{aligned} P &= (x, y, z, u, v), & P^2 &= (x, z, v, y, u),\\ P^3 &= (x, u, y, v, z), & P^4 &= (x, v, u, z, y). \end{aligned}$$

Lorsque la substitution P est, comme dans le premier et le dernier des exemples précédents, une substitution circulaire, alors, en vertu des principes établis dans le paragraphe I (p. 179), toute puissance P^h de P est le produit de plusieurs facteurs circulaires de même ordre, et par conséquent une substitution régulière dont l'ordre se confond avec $\frac{i}{\theta}$, θ étant le plus grand commun diviseur de h et de i. Ajoutons que la substitution P^h renfermera toutes les variables comprises dans la substitution circulaire P.

Si la lettre P représente, non plus une substitution circulaire, mais une substitution régulière équivalente au produit de plusieurs facteurs circulaires

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

dont chacun est de l'ordre i, alors, θ étant toujours le plus grand commun diviseur de i et de h, les divers facteurs

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

de la substitution P^h déterminée par la formule (12) renferment toutes les variables comprises dans P, et se réduisent tous à des substitutions régulières de l'ordre $\frac{i}{\theta}$. Il en résulte qu'on peut en dire autant de la substitution P^h elle-même. On peut donc énoncer encore la proposition suivante :

THÉORÈME V. — *Soient* P *une substitution régulière de l'ordre* i, *et* h *un nombre entier quelconque. Soient encore* θ *le plus grand commun divi-*

seur des nombres h, i, et j la valeur entière du rapport $\frac{i}{j}$. *Alors* P^h *sera une substitution régulière de l'ordre j, dans laquelle se trouveront comprises toutes les variables que renfermait la substitution* P.

Corollaire. — Lorsque l'ordre i de la substitution régulière P est une puissance p^f d'un nombre premier p, les deux diviseurs de i, représentés par 0 et j, se réduisent eux-mêmes à des puissances de p d'un degré inférieur ou tout au plus égal à f, et le théorème V fournit la proposition suivante :

Théorème VI. — *Nommons* P *une substitution régulière dont l'ordre soit une certaine puissance* p^f *d'un nombre premier p. Soient, de plus, h un nombre entier quelconque, et* p^g *la plus haute puissance de p qui divise h. La substitution* P^h *sera une substitution régulière de l'ordre*

$$\frac{p^f}{p^g} = p^{f-g},$$

dans laquelle se trouveront comprises toutes les variables que renfermait la substitution P.

Supposons maintenant que P représente une substitution sinon régulière, du moins primitive, c'est-à-dire une substitution régulière ou irrégulière dont l'ordre soit une puissance p^f d'un nombre premier p. Alors P sera nécessairement le produit de plusieurs substitutions régulières

$$U, \quad V, \quad W, \quad \ldots,$$

dont les ordres

$$p^f, \quad p^g, \quad \ldots$$

se trouveront représentés par diverses puissances de p correspondantes à des exposants

$$f, \quad g, \quad \ldots,$$

qui pourront être censés former une suite décroissante, f étant le plus considérable d'entre eux. D'ailleurs, si l'on désigne par h un nombre entier quelconque, l'équation

$$P = UVW\ldots \tag{17}$$

entraînera la suivante

$$P^h = U^h V^h W^h \ldots, \tag{18}$$

et de l'équation (18), jointe au théorème VI, il résulte évidemment que P^h sera, comme P, une substitution primitive. Enfin il suffira de poser, dans l'équation (18),

$$h = p^g,$$

ou plus généralement

$$h = kp^g,$$

k étant premier à p, pour réduire à l'unité la substitution V^h, et à plus forte raison les substitutions W^h, ... Mais alors, en vertu des formules

$$V^h = 1, \quad W^h = 1, \quad \ldots,$$

jointes à l'équation (18), on aura

$$P^h = U^h. \tag{19}$$

Donc la puissance P^h de la substitution P sera équivalente à la puissance U^h de la substitution régulière U, et l'on conclura du théorème VII que, dans l'hypothèse admise, l'ordre de la substitution P^h se réduit encore à p^{f-g}. D'autre part, comme la substitution $P^h = U^h$ comprendra toutes les variables renfermées dans U, elle sera certainement distincte de l'unité. On peut donc énoncer la proposition suivante :

Théorème VII. — *Nommons* P *une substitution primitive dont l'ordre soit la puissance* p^f *d'un nombre premier p. Si l'on désigne par h un nombre entier quelconque,* P^h *sera encore une substitution primitive qui aura pour ordre une certaine puissance de p. Concevons maintenant que l'on décompose* P *en facteurs représentés par des substitutions régulières*

$$U, \quad V, \quad W, \quad \ldots,$$

dont les ordres

$$p^f, \quad p^g, \quad \ldots$$

forment une suite décroissante. Si l'on prend pour h, ou le second terme p^g *de cette suite, ou le produit de ce second terme par un nombre k premier à p, alors* P^h *sera une substitution distincte de l'unité, non seule-*

ment primitive, mais régulière et de l'ordre p^{f-g}, dans laquelle se trouveront comprises toutes les variables que renfermait le premier facteur régulier U *de la substitution* P.

Pour montrer une application du théorème VII, considérons la substitution primitive du quatrième ordre

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

On aura, dans ce cas,

$$U = (x, y, z, u), \qquad V = (v, w),$$
$$i = 4, \quad p = 2, \quad f = 2, \quad g = 1, \quad p^f = 4, \quad p^g = 2.$$

Cela posé, on obtiendra évidemment un nombre h équivalent au produit de $p^g = 2$ par un facteur premier à p, si l'on prend

$$h = 2.$$

Donc, en vertu du théorème VIII,

$$P^2$$

sera une substitution régulière de l'ordre

$$p^{f-g} = 2.$$

On trouvera effectivement

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

Supposons à présent que la substitution P de l'ordre i ne soit ni régulière, ni même primitive. Alors, en nommant p l'un quelconque des facteurs premiers de i, et en posant

$$i = pl,$$

on conclura du théorème II que P^l est une substitution de l'ordre p. Donc, puisqu'une substitution dont l'ordre se réduit au nombre premier p est nécessairement régulière, on pourra énoncer la proposition suivante :

Théorème VIII. — *Soient* P *une substitution quelconque régulière ou irrégulière, i l'ordre de cette substitution, et p l'un quelconque des facteurs premiers de i. On pourra toujours choisir le nombre entier l de*

manière à faire coïncider la puissance P^l de P *avec une substitution de l'ordre p.*

Dans ce qui précède, nous avons généralement supposé que les exposants des puissances d'une substitution donnée P étaient positifs. Cette supposition embrasse tous les cas possibles, puisqu'on peut ajouter à un exposant quelconque un multiple quelconque de l'ordre i de la substitution donnée, et transformer ainsi un exposant négatif en un exposant positif. D'ailleurs, l étant un nombre entier quelconque, il est facile d'établir, à l'égard des substitutions de la forme

$$P^{-1} \quad \text{et} \quad P^{-l},$$

les deux théorèmes que nous allons énoncer.

Théorème IX. — *Quelle que soit la substitution* P, *la substitution inverse P^{-1} sera toujours semblable à* P.

Démonstration. — En effet, nommons i l'ordre de la substitution P. On aura

$$P^{-1} = P^{i-1};$$

et, comme le nombre $i - 1$ sera premier à i, on conclura du théorème IV, que P^{i-1} est semblable à P.

Corollaire. — Soit maintenant l un nombre entier quelconque. L'inverse de P^l, c'est-à-dire la substitution qui, étant multipliée par P^l, donnera pour produit l'unité, sera évidemment P^{-l}. Car, si l'on nomme l' un exposant positif assujetti à vérifier la condition

$$l' \equiv -l \pmod{i},$$

on aura non seulement

$$P^{l'} = P^{-l},$$

mais encore

$$P^l P^{l'} = P^{l+l'} = P^0 = 1,$$

et, par suite,

$$P^l P^{-l} = 1.$$

Donc, en vertu du théorème IX, on pourra énoncer encore la proposition suivante :

THÉORÈME X. — *P étant une substitution quelconque, et l un nombre entier quelconque, la puissance négative* P^{-l} *de* P *sera toujours semblable à la puissance positive* P^{l}.

IX. — *Des substitutions permutables entre elles.*

Soient

$$P, \quad Q$$

deux substitutions formées avec les n variables

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

Ces deux substitutions P, Q seront *permutables* entre elles si elles vérifient l'équation linéaire et symbolique

$$QP = PQ. \tag{1}$$

Donc, la substitution P étant donnée, il suffira, pour obtenir une substitution Q permutable avec P, de résoudre l'équation (1). Si d'ailleurs on nomme ω le nombre des formes diverses et semblables entre elles que l'on peut faire prendre à la substitution P en l'exprimant à l'aide de ses facteurs circulaires, et, mettant toutes les variables en évidence, ω sera précisément le nombre des solutions diverses de l'équation (1), ou, ce qui revient au même, le nombre des valeurs diverses de la substitution Q. Ajoutons qu'en vertu des principes établis dans le paragraphe IV, on devra, pour obtenir Q, 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 Q.

D'autre part, ainsi que nous l'avons déjà expliqué page 193, 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 des facteurs circulaires de même

ordre. Cela posé, comme le produit de plusieurs facteurs circulaires de même ordre est ce que nous appelons une substitution *régulière*, il arrivera nécessairement de deux choses l'une : ou P sera une substitution régulière équivalente au produit de plusieurs facteurs circulaires de même ordre qui tous seront échangés circulairement entre eux quand on passera de la première forme de P à la seconde; ou, du moins, P sera le produit de plusieurs substitutions régulières, dont chacune remplira la condition que nous venons d'indiquer.

Arrêtons-nous d'abord à la première hypothèse, et, en admettant que P se réduise au produit de h facteurs circulaires dont chacun soit de l'ordre a, nommons

$$\mathfrak{R}, \quad \mathfrak{S}, \quad \mathfrak{T}, \quad \ldots$$

ces mêmes facteurs que nous supposerons échangés circulairement entre eux dans l'ordre indiqué par la substitution

$$(\mathfrak{R}, \quad \mathfrak{S}, \quad \mathfrak{T}, \quad \ldots).$$

Puisqu'il suffira d'opérer cet échange pour passer de la première forme de P à la seconde, il est clair que, dans ce passage, chacune des variables qui appartiennent au facteur $\mathfrak{R}$ se trouvera remplacée par une variable correspondante qui appartiendra au facteur $\mathfrak{S}$, puis celle-ci par une troisième variable appartenant au facteur $\mathfrak{T}$, et ainsi de suite. Cela posé, soit α la variable qui occupait la première place dans le facteur $\mathfrak{R}$; désignons par $\beta, \gamma, \ldots$ les variables correspondantes tirées des facteurs $\mathfrak{S}, \mathfrak{T}, \ldots$, enfin soit

$$(\alpha, \beta, \gamma, \quad \ldots, \quad \lambda, \mu, \nu, \quad \ldots, \quad \varphi, \chi, \psi, \quad \ldots)$$

le facteur circulaire qui renferme la variable α dans la substitution Q. La suite des variables

$$\alpha, \beta, \gamma, \quad \ldots, \quad \lambda, \mu, \nu, \quad \ldots, \quad \varphi, \chi, \psi, \quad \ldots \tag{2}$$

pourra être évidemment décomposée en plusieurs autres suites

$$\left\{\begin{array}{llll} \alpha, & \beta, & \gamma, & \ldots, \\ \lambda, & \mu, & \nu, & \ldots, \\ \varphi, & \chi, & \psi, & \ldots, \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \end{array}\right. \tag{3}$$

formées chacune avec des variables qui se succéderont dans l'ordre indiqué par la substitution

$$(\mathcal{R},\ \mathcal{S},\ \mathcal{T},\ \ldots),$$

en sorte que, dans chacune des lignes horizontales du tableau (3), le premier terme représente une variable tirée du facteur $\mathcal{R}$, le second une variable tirée du facteur $\mathcal{S}$, le troisième une variable tirée du facteur $\mathcal{T}$, ... Or, puisque, dans le tableau (3) construit comme on vient de le dire, le nombre des colonnes verticales sera précisément le nombre h des facteurs circulaires

$$\mathcal{R},\ \mathcal{S},\ \mathcal{T},\ \ldots,$$

il est clair que, si l'on nomme b le nombre total des termes renfermés dans ce même tableau, et θ le nombre des suites horizontales qui le comparent, on aura

$$b = \theta h. \tag{4}$$

Ajoutons que le nombre b des termes compris dans le tableau (3) sera précisément l'ordre de la substitution circulaire

$$(\alpha, \beta, \gamma,\ \ldots,\ \lambda, \mu, \nu,\ \ldots,\ \varphi, \chi, \psi,\ \ldots).$$

Soient maintenant

$$\alpha', \beta', \gamma',\ \ldots,\ \lambda', \mu', \nu',\ \ldots,\ \varphi', \chi', \psi',\ \ldots \tag{5}$$

les variables qui, dans les facteurs circulaires

$$\mathcal{R},\ \mathcal{S},\ \mathcal{T},\ \ldots,$$

ou plutôt dans les cercles indicateurs correspondants, suivent immédiatement les variables

$$\alpha, \beta, \gamma,\ \ldots,\ \lambda, \mu, \nu,\ \ldots,\ \varphi, \chi, \psi,\ \ldots.$$

Soient pareillement

$$\alpha'', \beta'', \gamma'',\ \ldots,\ \lambda'', \mu'', \nu'',\ \ldots,\ \varphi'', \chi'', \psi'',\ \ldots \tag{6}$$

les variables qui, dans les mêmes cercles indicateurs, suivent immédiatement les variables

$$\alpha', \beta', \gamma',\ \ldots,\ \lambda', \mu', \nu',\ \ldots,\ \varphi', \chi', \psi',\ \ldots.$$

Chacune des suites (5), (6), ... renfermera, comme la suite (4), b termes différents, et ces termes seront encore propres à représenter les variables qui succéderont les unes aux autres, en vertu d'un facteur circulaire de la substitution Q. Cela posé, si l'on nomme

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

les divers facteurs circulaires de Q, tous ces facteurs seront de même ordre, et l'on pourra supposer

$$\left\{\begin{array}{l} \mathcal{U} = (\alpha,\ \beta,\ \gamma,\ \ldots,\ \lambda,\ \mu,\ \nu,\ \ldots,\ \varphi,\ \chi,\ \psi,\ \ldots),\\ \mathcal{V} = (\alpha', \beta', \gamma',\ \ldots,\ \lambda', \mu', \nu',\ \ldots,\ \varphi', \chi', \psi',\ \ldots),\\ \mathcal{W} = (\alpha'', \beta'', \gamma'',\ \ldots,\ \lambda'', \mu'', \nu'',\ \ldots,\ \varphi'', \chi'', \psi'',\ \ldots),\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right. \tag{7}$$

D'autre part, les variables qui succéderont les unes aux autres, en vertu du facteur circulaire $\mathcal{R}$ de la substitution P, seront évidemment

$$\alpha, \alpha', \alpha'', \ldots;\ \ \lambda, \lambda', \lambda'', \ldots;\ \ \varphi, \varphi', \varphi'', \ldots. \tag{8}$$

Pareillement, les variables qui succéderont les unes aux autres dans le facteur $\mathcal{S}$ de la substitution P, seront

$$\beta, \beta', \beta'', \ldots;\ \ \mu, \mu', \mu'', \ldots;\ \ \chi, \chi', \chi'', \ldots. \tag{9}$$

De même aussi les variables, qui succéderont les unes aux autres dans le facteur $\mathcal{T}$ de la substitution P, seront

$$\gamma, \gamma', \gamma'', \ldots;\ \ \nu, \nu', \nu'', \ldots;\ \ \psi, \psi', \psi'', \ldots, \tag{10}$$

etc. On aura donc encore

$$\left\{\begin{array}{l} \mathcal{R} = (\alpha, \alpha', \alpha'', \ldots;\ \ \lambda, \lambda', \lambda'', \ldots;\ \ \varphi, \varphi', \varphi'', \ldots),\\ \mathcal{S} = (\beta, \beta', \beta'', \ldots;\ \ \mu, \mu', \mu'', \ldots;\ \ \chi, \chi', \chi'', \ldots),\\ \mathcal{T} = (\gamma, \gamma', \gamma'', \ldots;\ \ \nu, \nu', \nu'', \ldots;\ \ \psi, \psi', \psi'', \ldots),\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right. \tag{11}$$

Observons d'ailleurs que, si l'on nomme k le nombre des facteurs circulaires

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

de la substitution Q, les diverses variables comprises dans la substitu-

tion $\mathcal{R}$ pourront être réparties entre les k suites verticales du tableau

$$(12)\qquad \begin{cases} \alpha, & \alpha', & \alpha'', & \dots, \\ \lambda, & \lambda', & \lambda'', & \dots, \\ \varphi, & \varphi', & \varphi'', & \dots, \\ \dots, & \dots, & \dots, & \dots, \end{cases}$$

qui renferme, comme le tableau (3), θ lignes horizontales. Donc l'ordre a de la substitution $\mathcal{R}$, représenté par le nombre total des termes du tableau (12), sera

$$(13)\qquad a = \theta k.$$

Remarquons à présent que, dans l'hypothèse admise, les substitutions P, Q, toutes deux régulières, seront déterminées par les formules

$$(14)\qquad P = \mathcal{R}\mathcal{S}\mathfrak{T}\dots, \qquad Q = \mathfrak{U}\mathfrak{V}\mathfrak{W}\dots,$$

et que les n variables données

$$x, \quad y, \quad z, \quad \dots$$

se confondront avec les variables comprises dans les seconds membres des formules (7), ou, ce qui revient au même, dans les seconds membres des formules (11). D'ailleurs ces mêmes variables, dont le nombre n se trouvera représenté par chacun des produits égaux

$$ah, \quad bk, \quad \theta hk,$$

pourront être réparties entre les divers tableaux

$$(15)\qquad \begin{cases} \alpha, & \beta, & \gamma, & \dots, \\ \alpha', & \beta', & \gamma', & \dots, \\ \alpha'', & \beta'', & \gamma'', & \dots, \\ \dots, & \dots, & \dots, & \dots; \end{cases}$$

$$(16)\qquad \begin{cases} \lambda, & \mu, & \nu, & \dots, \\ \lambda', & \mu', & \nu', & \dots, \\ \lambda'', & \mu'', & \nu'', & \dots, \\ \dots, & \dots, & \dots, & \dots; \end{cases}$$

$$(17)\qquad \begin{cases} \varphi, & \chi, & \psi, & \dots, \\ \varphi', & \chi', & \psi', & \dots, \\ \varphi'', & \chi'', & \psi'', & \dots, \\ \dots, & \dots, & \dots, & \dots; \end{cases}$$

$$\dots\dots\dots\dots,$$

dont le nombre sera θ, et dont chacun renfermera non seulement h lignes verticales, mais encore k lignes horizontales. Cela posé, on conclura immédiatement des formules (11), que, pour obtenir, dans l'hypothèse admise, l'un quelconque des facteurs circulaires

$$\mathcal{R}, \quad \mathcal{S}, \quad \mathfrak{T}, \quad \dots$$

de la substitution P, 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 (15), (16), (17), etc., à une ligne verticale de rang déterminé. On conclura, au contraire, des formules (7), que, pour obtenir l'un quelconque des facteurs circulaires

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

de la substitution Q, 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 (15), (16), (17), etc., à une ligne horizontale de rang déterminé.

Remarquons encore que, le nombre des lignes horizontales ou verticales comprises dans chacun des tableaux (15), (16), (17), etc., étant désigné, pour les lignes horizontales par la lettre k, et, pour les lignes verticales, par la lettre h, on tirera immédiatement des formules (7)

$$(18)\qquad \begin{cases} \mathfrak{U}^h = (\alpha, \lambda, \varphi, \dots)(\beta, \mu, \chi, \dots)(\gamma, \nu, \psi, \dots)\dots, \\ \mathfrak{V}^h = (\alpha', \lambda', \varphi', \dots)(\beta', \mu', \chi', \dots)(\gamma', \nu', \psi', \dots)\dots, \\ \mathfrak{W}^h = (\alpha'', \lambda'', \varphi'', \dots)(\beta'', \mu'', \chi'', \dots)(\gamma'', \nu'', \psi'', \dots)\dots, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots, \end{cases}$$

et des formules (11)

$$(19)\qquad \begin{cases} \mathcal{R}^k = (\alpha, \lambda, \varphi, \dots)(\alpha', \lambda', \varphi', \dots)(\alpha'', \lambda'', \varphi'', \dots)\dots, \\ \mathcal{S}^k = (\beta, \mu, \chi, \dots)(\beta', \mu', \chi', \dots)(\beta'', \mu'', \chi'', \dots)\dots, \\ \mathfrak{T}^k = (\gamma, \nu, \psi, \dots)(\gamma', \nu', \psi', \dots)(\gamma'', \nu'', \psi'', \dots)\dots, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \end{cases}$$

D'autre part, les équations (14) donneront

$$(20)\qquad P^k = \mathcal{R}^k\mathcal{S}^k\mathfrak{T}^k\dots, \qquad Q^k = \mathfrak{U}^h\mathfrak{V}^h\mathfrak{W}^h\dots.$$

Donc, eu égard aux formules (18), (19), chacune des substitutions P^k, Q^h sera équivalente au produit de tous les facteurs circulaires que renferme le tableau

$$(21)\qquad \begin{cases} (\alpha, \lambda, \varphi, \ldots), & (\beta, \mu, \chi, \ldots), & (\gamma, \nu, \psi, \ldots), \\ (\alpha', \lambda', \varphi', \ldots), & (\beta', \mu', \chi', \ldots), & (\gamma', \nu', \psi', \ldots), \\ (\alpha'', \lambda'', \varphi'', \ldots), & (\beta'', \mu'', \chi'', \ldots), & (\gamma'', \nu'', \psi'', \ldots), \\ \ldots\ldots\ldots\ldots, & \ldots\ldots\ldots\ldots, & \ldots\ldots\ldots\ldots. \end{cases}$$

Donc, si l'on nomme Θ le produit de tous ces facteurs circulaires, on aura simultanément

$$(22)\qquad P^k = \Theta, \qquad Q^h = \Theta,$$

et, par suite,

$$(23)\qquad P^k = Q^h.$$

De plus, θ étant précisément le nombre des variables comprises dans chaque ligne verticale du tableau (3), la valeur commune Θ de P^k et de Q^h sera évidemment une substitution régulière de l'ordre θ; et, d'ailleurs, à la seule inspection du tableau (21), on reconnaîtra immédiatement que, pour obtenir l'un quelconque des facteurs circulaires de la substitution Θ, il suffit d'écrire à la suite les unes des autres, en les renfermant entre deux parenthèses et en les séparant par des virgules, les variables semblablement placées dans les tableaux (15), (16), (17), etc.

Remarquons enfin qu'en vertu des formules (11), un facteur quelconque de P, le facteur $\mathfrak{R}$ par exemple, renfermera une ou plusieurs des variables comprises dans chacun des facteurs circulaires de Q, et que, réciproquement, en vertu des formules (7), un facteur quelconque de Q, le facteur $\mathfrak{U}$ par exemple, renfermera une ou plusieurs variables comprises dans chacun des facteurs circulaires de P. Il est aisé d'en conclure que, dans l'hypothèse admise, on ne pourra décomposer les deux substitutions P, Q, toutes deux régulières et permutables entre elles, en facteurs qui soient distincts de ces substitutions elles-mêmes, et qui, comparés deux à deux, restent permutables entre eux. En effet, pour qu'une telle décomposition fût possible, il

faudrait qu'avec une partie des variables données $x, y, z, \ldots$, on pût former deux substitutions $\mathfrak{T}$, $\mathfrak{Z}$, permutables entre elles, qui eussent respectivement pour facteurs circulaires, la première un ou plusieurs des facteurs $\mathfrak{R}$, $\mathfrak{S}$, $\mathfrak{T}, \ldots$, la seconde un ou plusieurs des facteurs $\mathfrak{U}$, $\mathfrak{V}$, $\mathfrak{W}$, ... Or, cette dernière supposition devra être évidemment rejetée; car, d'après la remarque énoncée, la substitution $\mathfrak{T}$ ne pourra renfermer un seul des facteurs $\mathfrak{R}$, $\mathfrak{S}$, $\mathfrak{T}, \ldots$ sans renfermer une ou plusieurs des variables comprises dans chacun des facteurs $\mathfrak{U}$, $\mathfrak{V}$, $\mathfrak{W}, \ldots$, et, si cette condition était remplie, la substitution $\mathfrak{Z}$ deviendrait nécessairement équivalente au produit de tous les facteurs $\mathfrak{U}$, $\mathfrak{V}$, $\mathfrak{W}, \ldots$ Donc alors $\mathfrak{Z}$ et $\mathfrak{T}$ renfermeraient toutes les variables données, et non plus seulement une partie de ces variables.

Jusqu'à présent nous avons supposé, d'une part, que P était une substitution régulière, c'est-à-dire équivalente à un produit de facteurs circulaires de même ordre; d'autre part, que ces facteurs circulaires étaient tous échangés circulairement entre eux quand on passait d'une première forme de P à une seconde forme distincte de la première, afin d'obtenir, par la comparaison de ces deux formes, une substitution Q permutable avec la substitution P.

Dans le cas général où la lettre P désigne une substitution quelconque, cette substitution régulière ou irrégulière peut du moins être considérée comme le produit de plusieurs substitutions régulières

$$\mathfrak{T}, \mathfrak{T}_1, \mathfrak{T}_2, \ldots,$$

dont chacune remplit la condition que nous venons d'indiquer. Alors on a

$$(24)\qquad P = \mathfrak{T}\mathfrak{T}_1\mathfrak{T}_2\ldots;$$

et aux substitutions régulières

$$\mathfrak{T}, \mathfrak{T}_1, \mathfrak{T}_2, \ldots,$$

qui représentent divers facteurs de P, correspondent des facteurs de Q représentés eux-mêmes par d'autres substitutions régulières

$$\mathfrak{Z}, \mathfrak{Z}_1, \mathfrak{Z}_2, \ldots,$$

de sorte qu'on a encore

$$Q = \mathfrak{Q}\mathfrak{Q}_1\mathfrak{Q}_2\ldots, \tag{25}$$

le facteur $\mathfrak{Q}$ étant permutable avec le facteur $\mathfrak{P}$, le facteur $\mathfrak{Q}_1$ avec le facteur $\mathfrak{P}_1$, et ainsi de suite. Lorsque les facteurs $\mathfrak{P}, \mathfrak{P}_1, \mathfrak{P}_2, \ldots$ se réduisent à un seul facteur $\mathfrak{P}$, les facteurs $\mathfrak{Q}, \mathfrak{Q}_1, \mathfrak{Q}_2, \ldots$ se réduisent aussi à un seul facteur $\mathfrak{Q}$, et l'on se trouve ramené au cas particulier que nous avons examiné ci-dessus. Mais ce cas particulier est le seul cas où les substitutions P, Q soient permutables entre elles sans pouvoir être décomposées en facteurs plus simples qui, comparés deux à deux, restent permutables entre eux. Cela posé, il résulte des principes établis dans ce paragraphe, qu'on peut énoncer les propositions suivantes :

Théorème I. — *Soient* P, Q *deux substitutions permutables entre elles, mais que l'on ne puisse décomposer en facteurs plus simples qui, comparés deux à deux, restent permutables entre eux. Ces substitutions seront toutes deux régulières et de 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, dans l'hypothèse admise, les deux substitutions régulières* P, Q *satisfont à l'équation de condition*

$$P^k = Q^h,$$

h étant le nombre des facteurs circulaires de la substitution P, *et k le nombre des facteurs circulaires de la substitution* Q.

Corollaire I. — Concevons qu'en faisant usage des notations précédemment adoptées, on nomme

n le nombre des variables comprises dans chacune des substitutions P, Q;

a l'ordre de la substitution régulière P;

b l'ordre de la substitution régulière Q;

θ le nombre des tableaux mentionnés dans le théorème I.

Les nombres a, b, n, seront liés aux nombres h, k, θ par les formules

$$a = \theta k, \qquad b = \theta h, \qquad n = \theta h k, \tag{26}$$

et l'ordre de la substitution $P^k = Q^h$ sera précisément le nombre θ déterminé par la formule

$$\theta = \frac{a}{k} = \frac{b}{h} = \frac{n}{hk} = \frac{ab}{n}, \tag{27}$$

de laquelle on tire encore

$$\theta = \left(\frac{ab}{hk}\right)^{\frac{1}{2}}. \tag{28}$$

Corollaire II. — Pour montrer une application du théorème I, supposons qu'avec les variables

$$x, \quad y, \quad z, \quad u, \quad v, \quad w, \quad s, \quad t,$$

on construise les deux tableaux

$$\begin{cases} x, & y, \\ z, & u, \end{cases} \tag{29}$$

$$\begin{cases} v, & w, \\ s, & t. \end{cases} \tag{30}$$

Le facteur circulaire qui présentera, écrites à la suite l'une de l'autre, les quatre premières lignes verticales des deux tableaux sera

$$(x, z, v, s);$$

et le facteur circulaire semblablement formé avec les quatre variables comprises dans les secondes lignes verticales des deux tableaux sera

$$(y, u, w, t).$$

Au contraire, le facteur circulaire qui présentera, écrites à la suite l'une de l'autre, les quatre variables comprises dans les premières lignes horizontales des deux tableaux sera

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

et le facteur circulaire semblablement formé avec les quatre variables comprises dans les secondes lignes horizontales des deux tableaux sera

$$(z, u, s, t).$$

Cela posé, il résulte du théorème I que, si l'on prend

$$\mathrm{P} = (x, z, v, s)\,(y, u, w, t) \tag{31}$$

et

$$\mathrm{Q} = (x, y, v, w)\,(z, u, s, t), \tag{32}$$

P, Q seront deux substitutions permutables entre elles, c'est-à-dire deux substitutions qui vérifieront la formule

$$\mathrm{PQ} = \mathrm{QP},$$

ou, ce qui revient au même, la formule

$$\mathrm{P} = \mathrm{QPQ}^{-1}.$$

Effectivement, il suit d'une règle précédemment énoncée (page 201) que, pour obtenir le produit

$$\mathrm{QPQ}^{-1},$$

il suffit d'exprimer la substitution P à l'aide de ses facteurs circulaires, puis d'effectuer dans P les déplacements de variables indiqués par la substitution Q, en opérant comme si P représentait un simple arrangement. Or, en écrivant, à la place de la substitution

$$\mathrm{P} = (x, z, v, s)\,(y, u, w, t),$$

l'arrangement

$$\mathrm{A} = xzvsyuwt,$$

et en appliquant à cet arrangement la substitution

$$\mathrm{Q} = (x, y, v, w)\,(z, u, s, t),$$

on trouverait

$$\mathrm{QA} = yuwtvsxz.$$

Donc, en vertu de la règle que nous venons de rappeler, on aura

$$\mathrm{QPQ}^{-1} = (y, u, w, t)\,(v, s, x, z),$$

ou, ce qui revient au même,

$$\mathrm{QPQ}^{-1} = (x, z, v, s)\,(y, u, w, t) = \mathrm{P}.$$

Ajoutons que, dans le cas présent, 2 étant tout à la fois le nombre des facteurs circulaires de P et le nombre des facteurs circulaires de Q, on aura

$$h = k = 2.$$

Donc, le théorème I donnera encore

$$\mathrm{P}^2 = \mathrm{Q}^2.$$

Enfin la valeur commune des deux substitutions P^2, Q^2 devra être, conformément à une remarque précédemment faite, le produit des quatre facteurs circulaires du second ordre

$$\begin{cases} (x, v), & (y, w), \\ (z, s), & (u, t), \end{cases} \tag{33}$$

dont chacun est formé avec deux variables qui occupent la même place dans les tableaux (29) et (30). Effectivement on tirera des formules (31) et (32)

$$\mathrm{P}^2 = \mathrm{Q}^2 = (x, v)\,(y, w)\,(z, s)\,(u, t).$$

Corollaire III. — Si les divers tableaux formés avec les n variables que renferment les substitutions P, Q se réduisent à un seul, alors P, Q seront deux substitutions régulières du genre de celles dont nous nous sommes déjà occupés dans le paragraphe VII (page 217), 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. Alors aussi l'équation

$$\theta = 1$$

entraînera les formules

$$k = a, \qquad k = b,$$
$$\mathrm{P}^k = \mathrm{Q}^k = 1.$$

Supposons, pour fixer les idées, qu'avec les six variables

$$x, \quad y, \quad z, \quad u, \quad v, \quad w,$$

on construise le tableau

$$(34) \qquad \begin{cases} x, & y, & z, \\ u, & v, & w. \end{cases}$$

Alors, en prenant pour P une substitution dont chaque facteur circulaire renferme les deux variables comprises dans une même ligne verticale du tableau (34), on trouvera

$$(35) \qquad P = (x, u)(y, v)(z, w).$$

Au contraire, en prenant pour Q une substitution dont chaque facteur circulaire présente, écrites à la suite l'une de l'autre, les trois variables comprises dans une même ligne horizontale du tableau (34), on trouvera

$$(36) \qquad Q = (x, y, z)(u, v, w).$$

Or, les substitutions P, Q, déterminées par les formules (35), (36), seront certainement permutables entre elles; car elles se réduiront au cube et au carré de la substitution du sixième ordre

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

De plus, le nombre k se confondant avec l'ordre $a = 2$ de la substitution P, et le nombre h avec l'ordre $b = 3$ de la substitution Q, l'équation (23) donnera

$$P^2 = Q^3 = 1.$$

Corollaire IV. — Si la substitution P se réduit à un seul facteur circulaire, alors tout ce que l'on pourra faire pour modifier la forme de P, ce sera de faire passer successivement à la première place l'une quelconque des variables écrites à la suite l'une de l'autre dans ce même facteur. Cela posé, les deux arrangements auxquels se réduiront les deux formes assignées à P quand on supprimera les parenthèses et les virgules placées entre les variables, représenteront évidemment les deux termes d'une substitution qui sera une puissance de P. Donc la substitution Q se confondra nécessairement avec l'une de ces puissances. Alors aussi le tableau unique, construit avec les diverses variables, ne renfermera plus qu'une seule ligne verticale.

THÉORÈME II. — *Soient* P, Q *deux substitutions permutables entre elles et formées avec les n variables*

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

Si ces deux substitutions ne sont pas de la forme indiquée dans le théorème I elles pourront, du moins, être décomposées en facteurs correspondants

$$\mathfrak{x}, \quad \mathfrak{x}, \quad \mathfrak{x}, \quad \ldots,$$
$$\mathfrak{z}, \quad \mathfrak{z}, \quad \mathfrak{z}, \quad \ldots,$$

qui, pris deux à deux, seront de cette forme et, par conséquent, permutables entre eux.

Corollaire I. — Soit 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; ω sera précisément le nombre des solutions diverses de l'équation *symbolique et linéaire*

$$QP = PQ,$$

résolue par rapport à Q (*voir* § IV, page 199); ou, ce qui revient au même, ω sera le nombre des substitutions permutables avec P, qui pourront être formées avec les n variables $x, y, z, \ldots$. D'ailleurs, comme nous l'avons déjà remarqué, il suffira, pour obtenir une valeur de Q, d'écrire, au-dessus de la substitution P exprimée à l'aide de ses facteurs circulaires, la même substitution sous une seconde forme semblable à la première, puis de prendre pour termes de la substitution Q les deux arrangements auxquels se réduiront les deux formes de P quand on supprimera, dans ces deux formes, les parenthèses et les virgules placées entre les diverses variables. Enfin, il peut arriver que la substitution P renferme des variables immobiles qui disparaissent quand on la réduit à sa plus simple expression; et il est clair que, dans le passage d'une première forme de P à une seconde, on pourra

échanger entre eux arbitrairement les facteurs circulaires du premier ordre formés avec ces variables immobiles. Il en résulte que les variables immobiles de P peuvent, dans la substitution Q, composer des facteurs circulaires quelconques. Donc, pour obtenir les diverses valeurs de Q, il suffira toujours de multiplier les diverses substitutions formées avec les variables immobiles de P, par les diverses valeurs de Q que l'on obtiendrait en laissant de côté ces mêmes variables et en supposant la valeur de P réduite à sa plus simple expression.

Corollaire II. — Pour montrer une application des principes établis dans le précédent corollaire, supposons que, les variables données

$$x, \quad y, \quad z, \quad u, \quad v, \quad w, \quad s, \quad t$$

étant au nombre de huit, la substitution P, réduite à sa plus simple expression, renferme seulement les six variables

$$x, \quad y, \quad z, \quad u, \quad v, \quad w,$$

et soit déterminée par la formule

$$\text{P} = (x, u)(y, v)(z, w). \tag{35}$$

La même substitution, quand toutes les variables seront mises en évidence, pourra être présentée sous la forme

$$\text{P} = (x, u)(y, v)(z, w)(s)(t). \tag{37}$$

D'ailleurs, si on laisse de côté les deux variables immobiles s, t, le nombre des formes semblables entre elles, sous lesquelles on pourra présenter la valeur de P fournie par l'équation (35), sera exprimé [*voir* la formule (2) de la page 194] par le produit

$$1.2.3.2^3 = 48.$$

Donc avec les six variables

$$x, \quad y \quad z, \quad u, \quad v, \quad w,$$

on pourra former 48 valeurs diverses de Q, c'est-à-dire 48 substitutions dont chacune sera permutable avec la substitution P. Au contraire, si l'on fait entrer en ligne de compte les deux variables s et t,

le nombre des formes, semblables entre elles, sous lesquelles on pourra présenter la valeur de P fournie par l'équation (37), sera

$$(1.2)(1.2.3.2^3) = 2.48 = 96.$$

Donc, avec les huit variables

$$x, \quad y, \quad z, \quad u, \quad v, \quad w, \quad s, \quad t,$$

on pourra former 2×48, ou 96 valeurs diverses de Q, c'est-à-dire 96 substitutions dont chacune sera permutable avec la substitution P. Il y a plus : pour obtenir les 96 valeurs de Q que l'on peut former avec les huit variables

$$x, \quad y, \quad z, \quad u, \quad v, \quad w, \quad s, \quad t,$$

il suffira de multiplier les 48 valeurs de Q, formées avec les six variables

$$x, \quad y, \quad z, \quad u, \quad v, \quad w,$$

par les deux substitutions

$$1 \quad \text{et} \quad (s, t),$$

qui peuvent être formées avec les variables immobiles de P ; et à chacune des valeurs que l'on pourra obtenir par la substitution Q, en laissant de côté les deux variables s, t, correspondra une seconde valeur qui sera le produit de la première par le facteur circulaire (s, t). Ainsi, par exemple, à la valeur de Q déterminée par l'équation (36), c'est-à-dire par la formule

$$\text{Q} = (x, y, z)(u, v, w),$$

correspondra une seconde valeur de Q déterminée par la formule

$$\text{Q} = (x, y, z)(u, v, w)(s, t),$$

et permutable, comme la première, avec la substitution P.

Avant de terminer ce paragraphe, nous allons encore établir, à l'égard des substitutions permutables entre elles, quelques propositions qui paraissent dignes d'être remarquées.

Théorème III. — *Désignons par*

$$\text{Q}, \quad \text{R}, \quad \text{S}, \quad \ldots$$

diverses substitutions dont chacune soit permutable avec une substitution donnée P. *Le produit de deux ou de plusieurs des substitutions* Q, R, S, ... *multipliées l'une par l'autre dans un ordre quelconque, sera encore permutable avec la substitution* P.

Démonstration. — En effet, lorsque chacune des substitutions

$$Q,\quad R,\quad S,\quad \ldots$$

sera permutable avec P, on aura

$$QP = PQ, \qquad RP = PR, \qquad SP = PS, \qquad \ldots, \tag{38}$$

ou, ce qui revient au même,

$$Q = PQP^{-1}, \qquad R = PRP^{-1}, \qquad S = PSP^{-1}, \qquad \ldots. \tag{39}$$

Or, on tirera immédiatement des équations (39)

$$QR = PQRP^{-1}, \qquad QRS = PQRSP^{-1}, \qquad \ldots, \tag{40}$$

ou, ce qui revient au même,

$$QRP = PQR, \qquad QRSP = PQRS, \qquad \ldots; \tag{41}$$

et il résulte immédiatement des formules (41), que chacun des produits

$$QR,\quad QRS,\quad \ldots,$$

formés par la multiplication de deux ou de plusieurs des substitutions

$$Q,\quad R,\quad S,\quad \ldots,$$

est permutable avec la substitution P.

Corollaire. — Désignons toujours par n le nombre des variables

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

comprises dans la substitution P, et par ω le nombre des formes, semblables entre elles, que peut prendre P exprimé à l'aide de ces variables; ω sera le nombre total des substitutions permutables avec P qui pourront être formées avec les n variables $x, y, z, \ldots$. Soient

$$1,\quad Q_1,\quad Q_2,\quad \ldots,\quad Q_{\omega-1} \tag{42}$$

ces mêmes substitutions, dont l'une se réduira toujours à l'unité. En

vertu du théorème III, les dérivées des substitutions

$$Q_1,\quad Q_2,\quad \ldots,\quad Q_{\omega-1}$$

seront toutes permutables avec P. Donc ces dérivées seront toutes comprises dans la série (42), et cette série offrira un système de substitutions conjuguées. On peut donc énoncer encore la proposition suivante :

Théorème IV. — *Une substitution quelconque* P *étant formée avec les* n *variables* $x, y, z, \ldots$, *les diverses substitutions formées avec les mêmes variables, et permutables avec* P, *offriront un système de substitutions conjuguées.*

Exemple. — Soit

$$P = (x, y)(z, u). \tag{43}$$

Le nombre des formes, semblables entre elles, que pourra prendre la substitution P exprimée à l'aide des quatre variables x, y, z, u, sera

$$1.2.2^2 = 8.$$

Donc ces mêmes variables pourront former huit substitutions permutables avec P. D'ailleurs, pour obtenir ces huit substitutions, il suffira de comparer à la forme sous laquelle P se présente dans la formule (43), les huit formes, semblables entre elles, que peut acquérir P exprimé à l'aide des variables x, y, z, u. Ces huit formes, savoir

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

se réduiront, si l'on supprime les virgules et les parenthèses, aux huit arrangements

$$xyzu, \quad yxzu, \quad xyuz, \quad yxuz,$$
$$zuxy, \quad zuyx, \quad uzxy, \quad uzyx.$$

Donc, en vertu de la règle énoncée à la page 200, les huit substitutions permutables avec P seront les suivantes :

$$\begin{pmatrix} xyzu \\ xyzu \end{pmatrix}, \quad \begin{pmatrix} yxzu \\ xyzu \end{pmatrix}, \quad \begin{pmatrix} xyuz \\ xyzu \end{pmatrix}, \quad \begin{pmatrix} yxuz \\ xyzu \end{pmatrix},$$
$$\begin{pmatrix} zuxy \\ xyzu \end{pmatrix}, \quad \begin{pmatrix} zuyx \\ xyzu \end{pmatrix}, \quad \begin{pmatrix} uzxy \\ xyzu \end{pmatrix}, \quad \begin{pmatrix} uzyx \\ xyzu \end{pmatrix},$$

ou, ce qui revient au même, les suivantes :

$$(44)\qquad \begin{cases} 1, & (x,y), & (z,u), & (x,y)(z,u), \\ (x,z)(y,u), & (x,z,y,u), & (x,u,y,z), & (x,u)(y,z). \end{cases}$$

Or, il est aisé de s'assurer que, si l'on multiplie ces huit substitutions par l'une quelconque d'entre elles, les huit produits ainsi obtenus se confondront avec ces mêmes substitutions, rangées seulement dans un nouvel ordre. Donc le système des huit substitutions permutables avec P sera, conformément au théorème IV, un système de substitutions conjuguées.

X. — *Sur les systèmes de substitutions permutables entre eux.*

Considérons n variables

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

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

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

les substitutions dont se compose le premier système, et par

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

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 qu'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*

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

et

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

deux systèmes de substitutions conjuguées, permutables entre eux, le premier de l'ordre a, le second de l'ordre b. Toute substitution S, *dérivée de 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

$$(3)\quad \left\{\begin{array}{lllll} 1, & P_1, & P_2, & \dots, & P_{a-1},\\ Q_1, & Q_1P_1, & Q_1P_2, & \dots, & Q_1P_{a-1},\\ Q_2, & Q_2P_1, & Q_2P_2, & \dots, & Q_2P_{a-1},\\ \dots, & \dots\dots, & \dots\dots, & \dots, & \dots\dots,\\ Q_{b-1}, & Q_{b-1}P_1, & Q_{b-1}P_2, & \dots, & Q_{b-1}P_{a-1}; \end{array}\right.$$

$$(4)\quad \left\{\begin{array}{lllll} 1, & P_1, & P_2, & \dots, & P_{a-1},\\ Q_1, & P_1Q_1, & P_2Q_1, & \dots, & P_{a-1}Q_1,\\ Q_2, & P_1Q_2, & P_2Q_2, & \dots, & P_{a-1}Q_2,\\ \dots, & \dots\dots, & \dots\dots, & \dots, & \dots\dots,\\ Q_{b-1}, & P_1Q_{b-1}, & P_2Q_{b-1}, & \dots, & P_{a-1}Q_{b-1}. \end{array}\right.$$

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,

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

sans avoir à la fois

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

l'équation (5) entraînerait la formule

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

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

$$Q_kP_h,$$

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), *si ces derniers systèmes n'offrent pas de termes communs autres que l'unité.*

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

THÉORÈME III. — *Soient*

$$(1)\qquad 1,\ P_1,\ P_2,\ \dots,\ P_{a-1},$$
$$(2)\qquad 1,\ Q_1,\ Q_2,\ \dots,\ Q_{b-1},$$

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 dérivées des substitutions (1) et (2). Donc il renfermera toutes ces dérivées, dont chacune sera tout à la fois de la forme Q_kP_h et de la forme P_hQ_k.

Considérons maintenant le cas particulier où les divers termes de la suite (1) se réduisent aux diverses puissances

$$(6)\qquad 1,\ P,\ P^2,\ \dots,\ P^{a-1}$$

d'une substitution P dont l'ordre est représenté par la lettre a, et où pareillement les divers termes de la suite (2) se réduisent aux diverses puissances

$$(7)\qquad 1,\ Q,\ Q^2,\ \dots,\ Q^{b-1}$$

d'une substitution Q dont l'ordre est représenté par la lettre b. Alors, pour que le système des substitutions (6) soit permutable avec le système des substitutions (7), il suffira que les deux suites

(8) $$Q,\quad PQ,\quad P^2Q,\quad \ldots,\quad P^{a-1}Q$$

et

(9) $$Q,\quad QP,\quad QP^2,\quad \ldots,\quad QP^{a-1}$$

offrent les mêmes termes rangés dans le même ordre ou dans deux ordres différents. En effet, cette condition étant supposée remplie, tout produit de la forme P^hQ sera en même temps de la forme $QP^{h'}$, le nombre h' pouvant être distinct du nombre h. Donc, par suite, tout produit de la forme

$$P^hQ^2 = P^hQQ$$

sera aussi de la forme

$$QP^{h'}Q,$$

et même de la forme

$$QQP^{h''} = Q^2P^{h''},$$

h'' pouvant être distinct de h et de h'. Généralement, toute substitution de la forme

$$P^hQ^k$$

pouvant être considérée comme le produit de k facteurs égaux à Q par le multiplicateur P^h, on pourra, sans altérer cette substitution, échanger successivement le facteur P^h avec chacun des facteurs égaux à Q, pourvu que chaque fois on modifie convenablement la valeur de l'exposant h; et lorsque, en vertu de semblables échanges, les k facteurs égaux à Q auront été déplacés de manière à précéder tous les facteurs égaux à P, la substitution

$$P^hQ^k$$

se présentera évidemment sous la forme

$$Q^kP^{h'}.$$

On peut donc énoncer la proposition suivante :

THÉORÈME IV. — *Soient*

$$P,\quad Q$$

deux substitutions distinctes, la première de l'ordre a, la seconde de l'ordre b. Si les deux suites

$$Q,\quad PQ,\quad P^2Q,\quad \ldots,\quad P^{a-1}Q,$$
$$Q,\quad QP,\quad QP^2,\quad \ldots,\quad QP^{a-1}$$

offrent précisément les mêmes termes rangés dans le même ordre ou dans deux ordres différents, alors les deux systèmes de substitutions conjuguées

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

et

$$1,\quad Q,\quad Q^2,\quad \ldots,\quad Q^{b-1},$$

formés, l'un avec les diverses puissances de P, *l'autre avec les diverses puissances de* Q, *seront deux systèmes permutables entre eux.*

De ce dernier théorème, joint aux théorèmes I et II, on déduit immédiatement la proposition suivante :

THÉORÈME V. — *Les mêmes choses étant posées que dans le théorème IV, admettons, en outre, qu'aucune des substitutions*

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

ne se retrouve parmi les substitutions

$$Q,\quad Q^2,\quad \ldots,\quad Q^{b-1},$$

en sorte que l'équation

$$P^h = Q^k$$

ne se vérifie jamais, excepté dans le cas où l'on a

$$P^h = 1,\qquad Q^k = 1.$$

Alors toutes les dérivées des deux substitutions P, Q seront comprises dans chacune des formes

$$P^hQ^k,\qquad Q^kP^h,$$

la valeur de k devant rester la même quand on passera de la première forme à la seconde; et, par suite, ces dérivées offriront un système de substitutions conjuguées dont l'ordre sera le produit ab.

Corollaire. — Dans l'hypothèse admise, les diverses dérivées des

substitutions P, Q se confondront évidemment avec les divers termes du tableau

$$(10)\qquad \left\{\begin{array}{lllll} 1, & P, & P^2, & \ldots, & P^{a-1}, \\ Q, & PQ, & P^2Q, & \ldots, & P^{a-1}Q, \\ Q^2, & PQ^2, & P^2Q^2, & \ldots, & P^{a-1}Q^2, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots\ldots, \\ Q^{b-1}, & PQ^{b-1}, & P^2Q^{b-1}, & \ldots, & P^{a-1}Q^{b-1}, \end{array}\right.$$

et aussi avec les divers termes du tableau

$$(11)\qquad \left\{\begin{array}{lllll} 1, & P, & P^2, & \ldots, & P^{a-1}, \\ Q, & QP, & QP^2, & \ldots, & QP^{a-1}, \\ Q^2, & Q^2P, & Q^2P^2, & \ldots, & Q^2P^{a-1}, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots\ldots, \\ Q^{b-1}, & Q^{b-1}P, & Q^{b-1}P^2, & \ldots, & Q^{b-1}P^{a-1}, \end{array}\right.$$

XI. — *Des substitutions arithmétiques et des substitutions géométriques.*

Considérons n variables

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

Supposons, d'ailleurs, que l'on représente ces diverses variables par une même lettre x successivement affectée des indices

$$0,\quad 1,\quad 2,\quad \ldots,\quad n-1;$$

et, en conséquence, à la place de

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

écrivons

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

Enfin concevons que l'on regarde comme pouvant être indifféremment remplacés l'un par l'autre deux indices, dont la différence se réduit à un multiple de n; en sorte qu'on ait, pour toute valeur entière positive ou même négative de l,

$$x_l = x_{l+n} = x_{l+2n} = \ldots = x_{l-n} = x_{l-2n} = \ldots$$

Pour reproduire la suite (1), ou du moins les termes de cette suite

rangés dans un nouvel ordre, il suffira d'ajouter aux indices de ces divers termes une même quantité h, ou bien encore de multiplier ces indices par un même nombre r premier à n. Dans le premier cas, à la place de la série (1), on obtiendra la suivante

$$(2)\qquad x_h,\quad x_{h+1},\quad x_{h+2},\quad \ldots,\quad x_{h+n-1}.$$

Dans le second cas, au contraire, la série (1) sera remplacée par celle-ci

$$(3)\qquad x_0,\quad x_r,\quad x_{2r},\quad \ldots,\quad x_{(n-1)r}.$$

Il est bon d'observer qu'au terme x_l de la série (1) correspond le terme x_{l+h} de la série (2), et que le *rapport arithmétique* des indices

$$l+h,\quad l,$$

qui affectent la lettre x dans ces deux termes, se réduit précisément à la constante h. Au contraire, au terme x_l de la série (1) correspond le terme x_{rl} de la série (3), et le *rapport géométrique* des indices

$$rl,\quad l,$$

qui affectent la lettre x dans ces deux termes, se réduit précisément à la constante r. Pour ce motif, en supposant, comme ci-dessus, que les variables données sont représentées par une seule lettre successivement affectée des indices

$$0,\quad 1,\quad 2,\quad \ldots,\quad n-1,$$

nous appellerons *substitution arithmétique* la substitution qui consiste à remplacer chaque terme de la série (1) par le terme correspondant de la série (2), et nous appellerons, au contraire, *substitution géométrique* la substitution qui consiste à remplacer chaque terme de la série (1) par le terme correspondant de la série (3). Cela posé, la substitution arithmétique la plus simple sera la substitution circulaire

$$(4)\qquad P = (x_0, x_1, x_2, \ldots, x_{n-1}),$$

qui consiste à remplacer généralement x_l par x_{l+1}, et il suffira évidemment d'élever celle-ci à la puissance du degré h pour obtenir la substitution qui consiste à remplacer généralement x_l par x_{l+h}. Ainsi, la valeur de P étant déterminée par la formule (4), chaque terme de la

série (1) se trouvera remplacé par le terme correspondant de la série (2) en vertu de la substitution circulaire ou régulière P^h.

Soit maintenant Q la substitution géométrique qui consiste à remplacer généralement le terme x_l de la série (1) par le terme correspondant x_{rl} de la série (3) en sorte qu'on ait

$$Q=\begin{pmatrix} x_0 x_1 x_2 \dots x_{(n-1)r} \\ x_0 x_1 x_2 \dots x_{n-1} \end{pmatrix}. \tag{5}$$

Alors, k étant un nombre entier quelconque, la substitution Q^k sera celle qui consiste à remplacer la variable x_l par la variable $x_{r^k l}$; et, par suite, pour que l'on ait identiquement

$$Q^k = 1, \tag{6}$$

il faudra que l'on ait, quel que soit l,

$$r^k l \equiv l \pmod{n}. \tag{7}$$

D'ailleurs, r étant, par hypothèse, premier à n, la formule (7), que l'on peut écrire comme il suit

$$(r^k - 1) l \equiv 0 \pmod{n},$$

donnera

$$r^k - 1 \equiv 0 \pmod{n},$$

ou, ce qui revient au même,

$$r^k \equiv 1 \pmod{n}. \tag{8}$$

Donc l'équation (6) entraînera toujours la formule (8); et l'ordre i de la substitution géométrique Q, c'est-à-dire la plus petite des valeurs de k, pour lesquelles se vérifiera l'équation (6), sera en même temps la plus petite des valeurs de k pour lesquelles se vérifiera la formule (8).

n étant un nombre entier quelconque, et r l'un des nombres premiers à n, l'exposant k de la puissance à laquelle il faut élever la *base* r pour obtenir un nombre équivalent, suivant le module n, à un reste donné, est ce qu'on nomme l'*indice* de ce reste. Cela posé, le nombre i, ou la plus petite des valeurs de k pour lesquelles se vérifie la formule (8), n'est évidemment autre chose que le plus petit des indices

de l'unité. Ce même nombre i est encore celui qui indique combien l'on peut obtenir de restes différents en divisant par n les termes de la progression géométrique

$$1, \quad r, \quad r^2, \quad r^3, \quad \dots,$$

et qui, pour cette raison, a été désigné, dans un précédent Mémoire, sous le nom d'*indicateur*. En conséquence, on peut énoncer la proposition suivante :

THÉORÈME I. — *n étant un nombre entier quelconque, et r étant l'un des nombres premiers à n, l'ordre de la substitution géométrique* Q, *déterminée par la formule* (8), *se confond avec l'indicateur i relatif à la base r.*

Concevons à présent que, h, k étant deux nombres entiers quelconques, on forme, avec les variables

$$x_0, \quad x_1, \quad x_2, \quad \dots, \quad x_{n-1},$$

les trois substitutions

$$P^h, \quad Q^k \quad \text{et} \quad Q^k P^h.$$

Ces substitutions consisteront évidemment, la première à remplacer l'indice l d'une variable quelconque par l'indice $l+h$, la deuxième à remplacer l'indice l par l'indice $r^k l$, et la troisième à remplacer l'indice l par l'indice

$$r^k(l+h).$$

Au contraire, h' étant un entier distinct de h, la substitution

$$P^{h'} Q^k$$

consisterait à remplacer l'indice l d'une variable quelconque par l'indice

$$h' + r^k l.$$

Donc on aura généralement

$$Q^k P^h = P^{h'} Q^k, \tag{9}$$

si l'on a

$$h' + r^k l = r^k (l+h),$$

ou, ce qui revient au même, si l'on a

$$h' = r^k h.$$

Mais alors l'équation (9) donnera

$$Q^i P^h = P^{r^k h} Q^i,$$

et il est d'ailleurs facile de s'assurer que cette dernière formule s'étend à des valeurs entières quelconques non seulement positives, mais encore négatives de h. On peut donc énoncer généralement la proposition suivante :

THÉORÈME II. — *Représentons n variables distinctes par une même lettre x successivement affectée des indices*

$$0, \quad 1, \quad 2, \quad \ldots, \quad n-1,$$

et concevons que l'on regarde comme pouvant être indifféremment remplacés l'un par l'autre deux indices dont la différence se réduit à un multiple de n. Soit d'ailleurs r un nombre entier, premier à n. Enfin soient

$$P, \quad Q$$

deux substitutions, l'une arithmétique, l'autre géométrique, déterminées par les formules (4) *et* (5), *c'est-à-dire deux substitutions qui consistent, la première à remplacer l'indice l d'une variable quelconque par l'indice l + 1, la seconde à remplacer l'indice l par l'indice rl. Alors on aura, pour des valeurs entières quelconques de h, et pour des valeurs entières et positives de k,*

$$Q^i P^h = P^{r^k h} Q^i. \tag{10}$$

Corollaire I. — Poser l'équation (10), c'est dire que l'équation (9), savoir

$$Q^i P^h = P^{h'} Q^i,$$

subsiste quand les exposants h, h' vérifient la condition

$$h' = r^k h.$$

D'ailleurs, de cette dernière formule, combinée avec l'équation

$$r^i \equiv 1 \pmod n,$$

on tire, en supposant $k < i$,

$$r^i h' \equiv r^k h \pmod n,$$

ou, ce qui revient au même,

$$h \equiv r^{i-k} h' \pmod n,$$

et plus généralement, en désignant par i' un multiple de i supérieur à k,

$$h \equiv r^{i'-k} h' \pmod n.$$

Donc, poser l'équation (10), c'est dire encore que l'équation (9) subsiste quand les exposants h, h' vérifient la condition

$$h = r^{i'-k} h'.$$

Il résulte de ces observations qu'on peut, dans la formule (9), choisir arbitrairement l'un quelconque des exposants h, h'. Il en résulte aussi que tout produit de la forme

$$Q^i P^h$$

est en même temps de la forme

$$P^h Q^i,$$

et réciproquement, la valeur de l'exposant h devant seule varier quand on passe d'une forme à l'autre. Donc, en vertu de l'équation (9), les diverses puissances de P, savoir

$$1, \quad P, \quad P^2, \quad \ldots, \quad P^{n-1}, \tag{11}$$

offrent un système de substitutions permutables avec le système des substitutions

$$1, \quad Q, \quad Q^2, \quad \ldots, \quad Q^{i-1}, \tag{12}$$

qui représentent les diverses puissances de Q.

Corollaire II. — Il est bon d'observer encore que la substitution arithmétique P et celles de ses puissances qui ne se réduisent pas à l'unité, déplacent les n variables données

$$x_0, \quad x_1, \quad x_2, \quad \ldots, \quad x_{n-1}.$$

Au contraire, la substitution géométrique Q, déterminée par la formule (5), ou, ce qui revient au même, par la suivante,

$$Q=\begin{pmatrix} x_0 x_{0r}\dots x_{n-1|r} \\ x_0 x_1 \dots x_{n-1}\end{pmatrix}, \tag{13}$$

laisse immobiles la variable x_0 quand n est un nombre impair, et les deux variables x_0, $x_{\frac{n}{2}}$ quand n est un nombre pair. La même propriété devant évidemment appartenir à celles des puissances de Q qui diffèrent de l'unité, il est clair que les deux substitutions

$$P,\quad Q$$

ne pourront jamais vérifier la formule

$$P^h=Q^k,$$

excepté dans le cas où l'on aura

$$P^h=1,\qquad Q^k=1.$$

Corollaire III. — Les deux corollaires précédents, joints au théorème III du paragraphe X, entraînent évidemment la proposition suivante :

THÉORÈME III. — *Les mêmes choses étant posées que dans le théorème* II, *les dérivées des deux substitutions* P, Q *seront toutes comprises sous chacune des deux formes*

$$P^h Q^k,\quad Q^k P^h,$$

et composeront un système de substitutions conjuguées qui sera d'un ordre représenté par le produit

$$ni,$$

i étant l'indicateur correspondant à la base r, c'est-à-dire la plus petite des valeurs de k propres à vérifier la formule (8).

Nota. — On arriverait encore aux mêmes conclusions en observant qu'il suffit de poser $k=1$ dans l'équation (10) pour obtenir la formule

$$QP^h=P^{r^h}Q. \tag{14}$$

Or, il résulte de cette dernière formule que les deux suites

$$\begin{aligned} &Q,\ PQ,\ P^2Q,\ \dots,\ P^{n-1}Q,\\ &Q,\ QP,\ QP^2,\ \dots,\ QP^{n-1}\end{aligned}$$

offrent les mêmes termes, rangés seulement dans deux ordres différents. Cela posé, il est clair que le théorème III sera une conséquence immédiate du théorème V du paragraphe X.

Soit maintenant a un diviseur de n, distinct de l'unité; et posons

$$\nu=\frac{n}{a}, \tag{15}$$

$$R=P^a. \tag{16}$$

R sera précisément la substitution arithmétique qui consiste à remplacer x_l par $x_{l+\frac{n}{a}}$, ou, ce qui revient au même, par $x_{l+\nu}$. D'ailleurs on tirera de l'équation (10), en y remplaçant h par ah, et ayant égard à la formule (16),

$$Q^k R^h = R^{r^{ah}} Q^k. \tag{17}$$

Enfin, comme la substitution R et ses puissances d'un degré inférieur à ν déplaceront toutes les variables données, tandis que la substitution Q et ses puissances d'un degré inférieur à i laissent immobile au moins la variable x_0, il est clair que les deux suites

$$\begin{aligned} &1,\ P,\ P^2,\ \dots,\ P^{\nu-1},\\ &1,\ Q,\ Q^2,\ \dots,\ Q^{i-1}\end{aligned}$$

n'offriront pas de termes communs autres que l'unité. Cela posé, des raisonnements semblables à ceux dont nous avons fait usage pour établir le théorème III suffiront pour déduire de la formule (17) la proposition suivante :

THÉORÈME IV. — *Les mêmes choses étant posées que dans le théorème* II, *nommons* ν *un diviseur de n distinct de l'unité, et soit* R *la substitution arithmétique qui consiste à remplacer généralement* x_l *par* $x_{l+\nu}$. *Les dérivées des deux substitutions* R, Q *seront toutes comprises sous chacune des deux formes*

$$Q^k R^h,\quad R^h Q^k,$$

et composeront un système de substitutions conjuguées qui sera d'un ordre représenté par le produit

$$vi.$$

Appliquons maintenant les théorèmes que nous venons d'établir à quelques exemples.

Supposons d'abord $n = 7$, $r = 3$. Alors les deux substitutions P, Q, déterminées par les formules

$$(18) \qquad P = (x_0, x_1, x_3, x_2, x_6, x_5, x_4),$$

$$(19) \qquad Q = (x_1, x_2, x_3, x_6, x_4, x_5),$$

seront, la première du septième ordre, la seconde du sixième ordre. On aura donc $i = 6$; et, en effet, le nombre 7 étant pris pour module, 6 sera l'indicateur correspondant à la base $r = 3$, puisque, dans la progression géométrique

$$3, \quad 3^2, \quad 3^3, \quad 3^4, \quad 3^5, \quad 3^6, \quad \ldots,$$

3^6 sera le premier terme qui, divisé par 7, donne pour reste l'unité. Cela posé, on conclura du théorème III que les substitutions arithmétique et géométrique P, Q, déterminées par les formules (18), (19), composent, avec leurs dérivées, un système dont l'ordre est représenté par le produit

$$6.7 = 42.$$

Supposons en second lieu $n = 7$, $r = 2$. Alors la substitution géométrique Q, déterminée, non plus par la formule (19), mais par la suivante

$$(20) \qquad Q = (x_1, x_2, x_4)(x_3, x_6, x_5),$$

sera du troisième ordre. On aura donc $i = 3$; et, en effet, le nombre 7 étant pris pour module, 3 sera l'indicateur correspondant à la base 2, puisque, dans la progression géométrique

$$2, \quad 2^2, \quad 2^3, \quad \ldots,$$

$2^3 = 8$ sera le premier terme qui, divisé par 7, donne pour reste l'unité. Cela posé, on conclura du théorème III que les substitutions

arithmétique et géométrique P, Q, déterminées par les formules (18) et (20), composent, avec leurs dérivées, un système dont l'ordre est représenté par le produit

$$3 \times 7 = 21.$$

Supposons encore $n = 9$, $r = 2$. Alors les deux substitutions P, Q, déterminées par les formules

$$(21) \qquad P = (x_0, x_1, x_{21}, x_2, x_4, x_3, x_6, x_7, x_8),$$

$$(22) \qquad Q = (x_1, x_2, x_4, x_8, x_5)(x_3, x_6),$$

seront, la première du neuvième ordre, la seconde du sixième ordre. On aura donc $i = 6$; et, en effet, le nombre 9 étant pris pour module, 6 sera l'indicateur correspondant à la base 2, puisque, dans la progression géométrique

$$2, \quad 2^2, \quad 2^3, \quad 2^4, \quad 2^5, \quad 2^6, \quad \ldots,$$

$2^6 = 64$ sera le premier terme qui, divisé par 9, donne pour reste l'unité. Cela posé, on conclura du théorème III que les deux substitutions arithmétique et géométrique P, Q, déterminées par les formules (21) et (22), composent, avec leurs dérivées, un système dont l'ordre est représenté par le produit

$$6.9 = 54.$$

Supposons enfin qu'à la substitution Q, déterminée par la formule (22), on joigne, non plus la substitution P, déterminée par la formule (21), mais la substitution R, dont la valeur est fournie par l'équation

$$(23) \qquad R = P^3,$$

ou, ce qui revient au même, par la suivante

$$(24) \qquad R = (x_0, x_3, x_6)(x_1, x_4, x_7)(x_2, x_5, x_8).$$

Alors R sera une substitution arithmétique de l'ordre

$$\frac{n}{3} = 3,$$

et l'on conclura du théorème IV que les substitutions arithmétique et géométrique Q, R, déterminées par les formules (22) et (24), composent, avec leurs dérivées, un système dont l'ordre est représenté par le produit

$$3.9=27.$$

Pour un module quelconque n, l'indicateur i dépend de la base r, et devient un *maximum* quand cette base r est une *racine primitive* correspondante au module n. Si l'on nomme I cet indicateur maximum, chacun des indicateurs qui correspondront aux diverses bases représentées par les divers nombres premiers à n sera égal à I ou à un diviseur de I. D'ailleurs, si l'on suppose

$$n=p^f q^g \ldots,$$

p et q, ... étant les facteurs premiers de n, l'indicateur maximum I sera le plus petit nombre entier divisible à la fois par chacun des produits

$$p^{f-1}(p-1), \quad q^{g-1}(q-1), \quad \ldots,$$

l'un de ces produits, savoir celui qui répondra au facteur 2, devant être remplacé par sa moitié quand n sera pair et divisible par 8.

Si n se réduit à une puissance d'un nombre premier et impair p, en sorte qu'on ait

$$n=p^f,$$

on trouvera

$$\mathrm{I}=p^{f-1}(p-1)=n\left(1-\frac{1}{p}\right).$$

Si n se réduit à un nombre premier p, on aura simplement

$$\mathrm{I}=n-1.$$

Eu égard aux remarques qu'on vient de faire, les théorèmes III et IV entraîneront évidemment les propositions suivantes :

Théorème V. — *Les mêmes choses étant posées que dans le théorème II, si l'on nomme r une des racines primitives correspondantes au module n, et* I *l'indicateur maximum relatif à ce module, c'est-à-dire le plus petit des indices de l'unité correspondants à la base r, la substitution géométrique* Q, *qui aura pour objet de remplacer généralement* x_l *par* x_{rl}, *sera de l'ordre* I.

Alors aussi les dérivées des deux substitutions P, Q seront toutes comprises sous chacune des deux formes

$$\mathrm{Q}^k\mathrm{P}^h, \quad \mathrm{P}^h\mathrm{Q}^k,$$

et composeront un système dont l'ordre sera représenté par le produit

$$n\mathrm{I}.$$

Corollaire. — Si n est un nombre premier, on aura simplement

$$\mathrm{I}=n-1,$$

et, par suite, les dérivées des deux substitutions

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

composeront un système dont l'ordre sera représenté par le produit

$$n(n-1).$$

Théorème VI. — *Les mêmes choses étant posées que dans le théorème* V, *soit* ν *un diviseur de n autre que l'unité, et nommons* R *la substitution arithmétique qui consiste à remplacer généralement* x_l *par* $x_{l+\nu}$. *Les dérivées des deux substitutions* Q, R *seront toutes comprises sous chacune des deux formes*

$$\mathrm{Q}^k\mathrm{R}^h, \quad \mathrm{R}^h\mathrm{Q}^k,$$

et composeront un système dont l'ordre sera exprimé par le produit νI.

Au lieu de représenter les diverses variables par une même lettre successivement accompagnée d'indices divers, on pourrait continuer à les représenter par différentes lettres

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

puis assigner à chaque variable un numéro propre à indiquer, ou le rang qu'elle occupe dans la série de ces lettres écrites à la suite l'une de l'autre, suivant un ordre déterminé, ou, mieux encore, ce même rang diminué de l'unité. Alors la substitution désignée par Q dans les

théorèmes précédents serait celle qui consiste à remplacer la variable correspondante au numéro l par la variable correspondante au numéro rl, ou plutôt au numéro équivalent au reste de la division du produit rl par le numéro l.

Supposons, pour fixer les idées, $n = 5$; alors cinq variables représentées par les lettres

$$x, \quad y, \quad z, \quad u, \quad v$$

pourront être censées correspondre aux numéros

$$0, \quad 1, \quad 2, \quad 3, \quad 4.$$

Alors aussi, en multipliant les quatre derniers numéros par le facteur r, on obtiendra les produits

$$r, \quad 2r, \quad 3r, \quad 4r;$$

et, si l'on pose $r = 2$, ces produits, divisés par 5, donneront pour restes

$$2, \quad 4, \quad 1, \quad 3.$$

Ainsi, dans cette hypothèse, la substitution désignée par Q aura pour effet de substituer aux variables dont les numéros étaient

$$1, \quad 2, \quad 3, \quad 4,$$

les variables dont les numéros sont

$$2, \quad 4, \quad 1, \quad 3,$$

c'est-à-dire de substituer aux variables

$$y, \quad z, \quad u, \quad v$$

les variables

$$z, \quad v, \quad y, \quad u.$$

On aura donc

$$Q = (y, z, v, u).$$

Cela posé, on conclura du théorème II que les dérivées des deux substitutions

$$P = (x, y, z, u, v), \qquad Q = (y, z, v, u) \tag{25}$$

sont toutes comprises sous chacune des formes

$$P^k Q^l, \quad Q^l P^k,$$

et que l'ordre du système de ces dérivées est égal au produit

$$5.4 = 20$$

des nombres 5 et 4 qui représentent les ordres des substitutions P et Q. Effectivement les dérivées des substitutions P, Q dont les valeurs sont données par les formules (25) se réduiront aux vingt substitutions comprises dans le tableau

$$(26) \quad \begin{cases} 1, & P, & P^2, & P^3, & P^4, \\ Q, & QP, & QP^2, & QP^3, & QP^4, \\ Q^2, & Q^2P, & Q^2P^2, & Q^2P^3, & Q^2P^4, \\ Q^3, & Q^3P, & Q^3P^2, & Q^3P^3, & Q^3P^4, \end{cases}$$

ou, ce qui revient au même, dans le suivant :

$$(27) \quad \begin{cases} 1, & (x, y, z, u, v), & (x, z, v, y, u), & (x, u, y, v, z), & (x, v, u, z, y), \\ (y, z, v, u), & (v, x, z, y), & (z, u, x, v), & (x, y, u, z), & (u, v, y, x), \\ (y, v)(z, u) & (u, y)(v, x), & (x, u)(y, z), & (z, x)(u, v), & (v, z)(x, y), \\ (y, x, v, z) & (z, v, x, u), & (u, x, y, v), & (v, y, z, x), & (x, z, u, y). \end{cases}$$

Ajoutons qu'en vertu de la formule (10), on aura généralement

$$Q^k P^h = P^{2^k h} Q^k, \tag{28}$$

et, par suite,

$$(29) \quad \begin{cases} QP = P^2Q, & QP^2 = P^4Q, & QP^3 = PQ, & QP^4 = P^3Q, \\ Q^2P = P^4Q^2, & Q^2P^2 = P^3Q^2, & Q^2P^3 = P^2Q^2, & Q^2P^4 = PQ^2, \\ Q^3P = P^2Q^3, & Q^3P^2 = P\,Q^3, & Q^3P^3 = P^4Q^3, & Q^3P^4 = P^2Q^3. \end{cases}$$

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

Considérons n variables

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

Le nombre total N des arrangements, ou bien encore des substitutions que l'on pourra former avec ces variables, sera représenté par le produit

$$N = 1.2.3 \ldots n;$$

et l'un quelconque des systèmes de substitutions conjuguées, formés avec ces mêmes variables, sera toujours d'un ordre exprimé par un diviseur de N. De plus, ces systèmes jouiront encore de diverses propriétés remarquables dont quelques-unes ont été déjà établies dans le paragraphe VI. Je vais maintenant en démontrer quelques autres, qui se trouvent exprimées par les théorèmes suivants :

THÉORÈME I. — *Formons avec n variables*

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

deux systèmes de substitutions conjuguées; et soient

$$(1) \qquad 1, \quad P_1, \quad P_2, \quad \ldots, \quad P_{a-1},$$
$$(2) \qquad 1, \quad Q_1, \quad Q_2, \quad \ldots, \quad Q_{b-1},$$

ces deux systèmes, le premier de l'ordre a, le second de l'ordre b. Soit d'ailleurs I *le nombre des substitutions* R *pour lesquelles se vérifient des équations symboliques et linéaires de la forme*

$$(3) \qquad RP_k = Q_k R,$$

h étant l'un quelconque des entiers

$$1, \quad 2, \quad \ldots, \quad a-1,$$

et k l'un quelconque des entiers

$$1, \quad 2, \quad \ldots, \quad b-1.$$

Le nombre I, *divisé par le produit ab, fournira le même reste que le nombre*

$$N = 1.2.3 \ldots n,$$

et l'on aura, en conséquence,

$$(4) \qquad I \equiv N \pmod{ab}.$$

Démonstration. — Faisons, pour abréger,

$$(5) \qquad J = N - I.$$

Parmi les substitutions que l'on pourra former avec $x, y, z, \ldots$, celles pour lesquelles ne se vérifieront jamais des équations semblables à la

formule (3) seront en nombre égal à J. Nommons U l'une de ces dernières substitutions. Les divers termes du tableau

$$(6) \qquad \begin{cases} U, & UP_1, & UP_2, & \ldots, & UP_{a-1}, \\ Q_1U, & Q_1UP_1, & Q_1UP_2, & \ldots, & Q_1UP_{a-1}, \\ Q_2U, & Q_2UP_1, & Q_2UP_2, & \ldots, & Q_2UP_{a-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ Q_{b-1}U, & Q_{b-1}UP_1, & Q_{b-1}UP_2, & \ldots, & Q_{b-1}UP_{a-1} \end{cases}$$

seront tous inégaux entre eux. Car, si l'on avait

$$Q_kUP_h = Q_{k'}UP_{h'},$$

et, par suite,

$$(7) \qquad UP_hP_{h'}^{-1} = Q_k^{-1}Q_{k'}U,$$

sans avoir en même temps

$$P_h = P_{h'} \quad \text{et} \quad Q_k = Q_{k'},$$

on réduirait l'équation (5) à la forme

$$(8) \qquad U\mathfrak{T} = \mathfrak{Q}U,$$

en posant

$$\mathfrak{T} = P_hP_{h'}^{-1}, \qquad \mathfrak{Q} = Q_k^{-1}Q_{k'}.$$

Mais alors, des deux substitutions $\mathfrak{T}$, $\mathfrak{Q}$, dont l'une au moins serait distincte de l'unité, la première représenterait encore un terme de la série (1), et la seconde un terme de la série (2). Donc la formule (7) ou (8), considérée comme propre à déterminer U, serait semblable à l'équation (3), et la substitution U se réduirait, contre l'hypothèse admise, à l'une des valeurs de R.

Soit maintenant V une substitution nouvelle qui, étant formée avec les variables $x, y, z, \ldots$, ne se réduise ni à l'une des valeurs de R, ni à aucune des substitutions comprises dans le tableau (6). Les divers termes du tableau

$$(9) \qquad \begin{cases} V, & VP_1, & VP_2, & \ldots, & VP_{a-1}, \\ Q_1V, & Q_1VP_1, & Q_1VP_2, & \ldots, & Q_1VP_{a-1}, \\ Q_2V, & Q_2VP_1, & Q_2VP_2, & \ldots, & Q_2VP_{a-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ Q_{b-1}V, & Q_{b-1}VP_1, & Q_{b-1}VP_2, & \ldots, & Q_{b-1}VP_{a-1} \end{cases}$$

seront encore tous inégaux entre eux, et même ils seront distincts de tous ceux que renferme le tableau (6); car, si l'on avait

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

on en conclurait

$$V = Q_{k'}^{-1} Q_k U P_h P_{h'}^{-1}; \tag{10}$$

puis, en posant, pour abréger,

$$\mathfrak{P} = P_h P_{h'}^{-1}, \qquad \mathfrak{Q} = Q_{k'}^{-1} Q_k,$$

on réduirait l'équation (9) à la formule

$$V = \mathfrak{Q} U \mathfrak{P}; \tag{11}$$

et, comme les deux produits $\mathfrak{P}$, $\mathfrak{Q}$ représenteraient encore, le premier un terme de la série (1), le second un terme de la série (2), il est clair qu'en vertu de la formule (11), V se réduirait, contre l'hypothèse admise, à l'un des termes renfermés dans le tableau (6).

En continuant de la sorte, on répartira les J substitutions, pour lesquelles ne se vérifieront jamais des équations semblables à la formule (3), entre plusieurs tableaux que l'on déduira successivement du tableau (6), en remplaçant dans celui-ci la substitution U, qui représente le premier terme, par une autre substitution V, ou W, etc. D'ailleurs, les termes qui se trouveront renfermés dans chaque tableau, en nombre équivalent au produit ab, seront tous inégaux entre eux. Il y a plus : les termes que comprendra le système des divers tableaux seront encore tous distincts les uns des autres, si l'on a soin de prendre pour premier terme de chaque nouveau tableau une substitution non comprise dans les tableaux déjà formés. Cette condition étant supposée remplie, le nombre total des termes compris dans les divers tableaux sera nécessairement le nombre représenté par J. Donc le nombre J ou N — I sera un multiple du nombre des termes renfermés dans chaque tableau, c'est-à-dire du produit ab. Donc les nombres I et N, divisés par le produit ab, fourniront le même reste.

Corollaire. — Si les deux systèmes de substitutions conjuguées,

mentionnés dans le théorème I, se réduisent à un seul, alors, à la place de ce théorème, on obtiendra la proposition suivante :

THÉORÈME II. — *Soit a l'ordre d'un système de substitutions conjuguées*

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

formées avec les n variables

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

et nommons I *le nombre des substitutions* R *pour lesquelles se vérifient des équations de la forme*

$$RP_h = P_k R, \tag{12}$$

h, k étant des nombres entiers égaux ou inégaux, pris dans la suite

$$0, \quad 1, \quad 2, \quad \ldots, \quad a-1.$$

Le nombre I, *divisé par le carré de a, fournira le même reste que le produit*

$$N = 1.2.3 \ldots n,$$

en sorte qu'on aura

$$I \equiv N \pmod{a^2}. \tag{13}$$

Corollaire. — Si a^2 surpasse N, la formule (13) donnera nécessairement

$$I = N, \tag{14}$$

et, par suite, une substitution quelconque R sera du nombre de celles pour lesquelles peut se vérifier l'équation (12).

Revenons maintenant à la formule (3). Cette formule exprime évidemment que les deux substitutions

$$P_h, \quad Q_k,$$

dont la première est l'un des termes qui suivent l'unité dans la série (1), et la seconde l'un des termes qui suivent l'unité dans la série (2), sont semblables l'une à l'autre. Donc il sera impossible de satisfaire à l'équation (3) si aucune des substitutions

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

n'est semblable à l'une des substitutions

$$Q_1,\quad Q_2,\quad \ldots,\quad Q_{b-1}.$$

Donc alors on aura

$$I = 0,$$

et la formule (4), réduite à celle-ci

$$N \equiv 0 \pmod{ab}, \tag{15}$$

exprimera que le nombre N est divisible par le produit ab. En conséquence, on peut énoncer la proposition suivante :

THÉORÈME III. — *Formons avec n variables*

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

deux systèmes de substitutions conjuguées, et supposons que ces deux systèmes étant, le premier de l'ordre a, le second de l'ordre b, renferment, outre l'unité, d'une part, les substitutions

$$P_1,\quad P_2,\quad \ldots,\quad P_{a-1}, \tag{16}$$

d'autre part, les substitutions

$$Q_1,\quad Q_2,\quad \ldots,\quad Q_{b-1}. \tag{17}$$

Si aucune des substitutions (16) *n'est semblable à l'une des substitutions* (17), *le nombre*

$$N = 1.2.3\ldots n$$

sera divisible par le produit ab.

Le théorème que nous venons d'énoncer entraîne encore évidemment la proposition suivante :

THÉORÈME IV. — *Soient*

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

et

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

deux systèmes de substitutions conjuguées, le premier de l'ordre a, le second de l'ordre b, formés l'un et l'autre avec les n variables

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

Si le produit ab n'est pas un diviseur du nombre

$$N = 1.2.3\ldots n,$$

alors, des substitutions

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

une ou plusieurs seront semblables à une ou plusieurs des substitutions

$$Q_1,\quad Q_2,\quad \ldots,\quad Q_{b-1}.$$

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

$$N = 1.2.3\ldots n.$$

D'après ce qui a été dit dans le paragraphe VII (p. 221), on pourra former avec les n variables $x, y, z, \ldots$ un système de substitutions primitives et conjuguées qui sera de l'ordre p^f; et rien n'empêchera de supposer que l'on prend ces mêmes substitutions pour termes de la suite

$$1,\quad Q_1,\quad Q_2,\quad \ldots,\quad Q_{b-1}.$$

Or, dans cette hypothèse, b étant égal à p^f, le produit ab ne pourra diviser N si a est divisible par p; et, d'ailleurs, chacune des substitutions

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

étant une substitution primitive dont l'ordre sera représenté par l'un des nombres

$$p,\quad p^2,\quad \ldots,\quad p^f,$$

aura pour dérivées d'autres termes de la suite

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

parmi lesquels (*voir* le théorème VIII du paragraphe VIII) on trouvera au moins une substitution régulière de l'ordre p. Donc, en vertu du théorème IV, si l'ordre a du système de substitutions

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

est divisible par le nombre premier p, l'une au moins des substi-

tutions

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

sera régulière et de l'ordre p.

Corollaire II. — Si l'on représente par des lettres diverses

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

les substitutions qui, dans le théorème IV, sont désignées à l'aide d'une seule lettre P successivement affectée des indices

$$1,\quad 2,\quad 3,\quad \ldots,\quad a-1,$$

et si, d'ailleurs, on nomme M l'ordre du système des substitutions conjuguées

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

alors la proposition établie dans le corollaire I sera réduite à celle dont voici l'énoncé :

THÉORÈME V. — *Soit* M *l'ordre du système des substitutions conjuguées*

$$(18)\qquad 1,\quad P,\quad Q,\quad R,\quad \ldots$$

formées avec les n variables $x, y, z, \ldots$, et nommons p un nombre premier égal ou inférieur à n. Si M *est divisible par p, l'une au moins des substitutions*

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

sera une substitution régulière de l'ordre p.

Corollaire. — Lorsque le nombre premier p devient supérieur à $\frac{n}{2}$, une substitution régulière et de l'ordre p, formée avec les n variables $x, y, z, \ldots$, ne peut être qu'une substitution circulaire. Donc le théorème VII entraîne encore la proposition suivante :

THÉORÈME VI. — *Soit* M *l'ordre du système des substitutions conjuguées*

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

formées avec les n variables $x, y, z, \ldots$, et nommons p un nombre premier égal ou inférieur à n, mais supérieur à $\frac{n}{2}$. Si M *est divisible par p,*

l'une au moins des substitutions

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

sera une substitution circulaire de l'ordre p.

Pour montrer une application du théorème VI, supposons que, n étant égal à 5, les variables données soient

$$x,\quad y,\quad z,\quad u,\quad v.$$

Au module 5 correspondront, d'une part, les racines primitives 2 et 3, d'autre part, l'indicateur *maximum*

$$n-1=4,$$

dont les diviseurs

$$1,\quad 2,\quad 4$$

représenteront les divers indicateurs correspondants à des bases quelconques; et l'on conclura du troisième des théorèmes démontrés dans le paragraphe XI, qu'avec cinq variables on peut former non seulement une substitution circulaire du cinquième ordre, mais encore un système de substitutions conjuguées dont l'ordre soit représenté par le produit

$$5\times 2=10,$$

ou par le produit

$$5\times 4=20.$$

Ainsi, en particulier, on pourra former, avec les cinq variables x, y, z, u, v, le système du vingtième ordre que composent les substitutions écrites dans le tableau (27) de la page 273. Cela posé, il résultera immédiatement du théorème VI que tout système du dixième ou du vingtième ordre, formé avec les cinq variables x, y, z, u, v, comprendra, comme le système dont il est ici question, des substitutions régulières dont les ordres seront représentés par les facteurs premiers des nombres 10 et 20, c'est-à-dire des substitutions circulaires du cinquième ordre et des substitutions régulières du deuxième ordre.

D'après ce qu'on a vu dans le paragraphe VI (théorème II), l'ordre M d'un système de substitutions conjuguées

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

est divisible par l'ordre de chacune des substitutions P, Q, R, ..., et en conséquence par a, si a représente l'ordre de la substitution P. La proposition réciproque se vérifie, en vertu du théorème VI, quand a est un diviseur premier de M, c'est-à-dire qu'alors un système de substitutions conjuguées ne peut être de l'ordre M sans renfermer au moins une substitution de l'ordre a. Mais on ne devrait plus en dire autant si, l'ordre M du système n'étant pas un nombre premier, a représentait un diviseur non premier de M, par exemple le nombre M lui-même. Alors, en effet, il pourrait arriver que le système ne renfermât aucune substitution de l'ordre a. Ainsi, en particulier, si l'on pose

$$P=(x,y)(z,u), \qquad Q=(x,z)(y,u), \qquad R=PQ=QP,$$

les quatre substitutions

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

formeront, comme on l'a déjà remarqué dans le paragraphe VII, un système de substitutions conjuguées; et ce système du quatrième ordre ne renfermera pourtant point de substitutions du quatrième ordre, mais seulement trois substitutions régulières du deuxième ordre, attendu que P, Q, R se réduiront à

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

MÉMOIRE

SUR

LES LIGNES QUI DIVISENT EN PARTIES ÉGALES

LES ANGLES FORMÉS PAR DEUX DROITES

ET SUR

LA ROTATION D'UNE DROITE MOBILE DANS L'ESPACE

Nous allons, dans ce Mémoire, réunir diverses formules de Géométrie analytique, à l'aide desquelles nous rechercherons plus tard les propriétés de deux systèmes de courbes tracées sur une même surface.

I. — *Sur les lignes qui divisent en parties égales les angles formés par deux droites.*

Considérons d'abord deux droites qui, partant d'un même point O, se prolongent indéfiniment dans des directions déterminées OA, OB. Supposons d'ailleurs que, le point O étant pris pour origine des coordonnées, tous les points de l'espace soient rapportés à trois axes rectangulaires de x, y, z; et que les cosinus des angles formés par les deux droites OA, OB, avec les demi-axes des x, y, z positives, soient désignés,

pour la première droite, par α, β, γ;
pour la seconde droite, par α_1, β_1, γ_1.

Si, à partir du point O, on porte sur les deux droites données des longueurs OA, OB, dont chacune soit représentée par l'unité; alors α, β, γ seront précisément les coordonnées du point A, et α_1, β_1, γ_1 les coordonnées du point B. Par suite, les différences

$$\alpha_1-\alpha, \quad \beta_1-\beta, \quad \gamma_1-\gamma$$

représenteront précisément les projections algébriques de la longueur AB comptée à partir du point A. Ajoutons que, si l'on désigne par C le milieu de AB, les demi-sommes

$$\frac{\alpha_1+\alpha}{2},\quad \frac{\beta_1+\beta}{2},\quad \frac{\gamma_1+\gamma}{2}$$

représenteront les projections algébriques de la droite OC, comptées à partir du point O. D'autre part, si l'on nomme δ l'angle aigu ou obtus, mais inférieur à deux droits, qui se trouve compris entre les directions OA, OB, l'angle $\frac{1}{2}\delta$ sera aigu, et l'on aura évidemment

$$OC=\cos\frac{\delta}{2},\qquad AB=2\sin\frac{\delta}{2}.$$

Enfin, pour obtenir le cosinus de l'angle que forme avec le demi-axe des x, y ou z positives une droite prolongée dans une certaine direction, il suffit de diviser la projection algébrique d'une longueur mesurée dans cette direction par cette longueur même. Donc, pour obtenir les cosinus des angles formés par la direction AB avec les demi-axes des coordonnées positives, il suffira de diviser les différences

$$\alpha_1-\alpha,\quad \beta_1-\beta,\quad \gamma_1-\gamma$$

par $2\sin\frac{\delta}{2}$; et si l'on nomme λ, μ, ν ces trois cosinus, on aura

$$\lambda=\frac{\alpha_1-\alpha}{2\sin\frac{\delta}{2}},\qquad \mu=\frac{\beta_1-\beta}{2\sin\frac{\delta}{2}},\qquad \nu=\frac{\gamma_1-\gamma}{2\sin\frac{\delta}{2}}. \tag{1}$$

Au contraire, pour obtenir les cosinus λ_1, μ_1, ν_1 des angles formés par la direction OC avec les demi-axes des coordonnées positives, il suffira de diviser les trois demi-sommes

$$\frac{\alpha_1+\alpha}{2},\quad \frac{\beta_1+\beta}{2},\quad \frac{\gamma_1+\gamma}{2}$$

par $\cos\frac{\delta}{2}$, en sorte qu'on aura encore

$$\lambda_1=\frac{\alpha_1+\alpha}{2\cos\frac{\delta}{2}},\qquad \mu_1=\frac{\beta_1+\beta}{2\cos\frac{\delta}{2}},\qquad \nu_1=\frac{\gamma_1+\gamma}{2\cos\frac{\delta}{2}}. \tag{2}$$

Observons au reste que la direction OC est précisément celle de la ligne qui divise en parties égales l'angle δ compris entre les directions OA, OB. Quant à la direction AB, elle est évidemment parallèle à celle d'une ligne qui diviserait en parties égales, non plus l'angle δ compris entre les droites données, mais l'angle $\pi-\delta$ compris entre l'une de ces droites et le prolongement de l'autre.

Ainsi, en définitive, les valeurs de λ_1, μ_1, ν_1 déterminées par les formules (2), et les valeurs de λ, μ, ν déterminées par les formules (1), représentent les cosinus des angles formés, avec les demi-axes des coordonnées positives, par deux lignes qui divisent en parties égales les angles δ et $\pi-\delta$ compris entre les deux droites données, ou entre l'une de ces droites et le prolongement de l'autre.

Supposons maintenant que α, β, γ et α_1, β_1, γ_1 représentent les cosinus des angles formés avec les demi-axes des x, y, z positives, non plus par deux droites qui partent de l'origine des coordonnées, mais par deux droites dirigées d'une manière quelconque dans l'espace. Alors ce qu'on nommera l'*angle des deux droites* ne sera autre chose que l'angle δ compris entre deux droites parallèles partant d'un même point; et, si l'on désigne toujours par λ_1, μ_1, ν_1 ou par λ, μ, ν les cosinus des angles formés, avec les demi-axes des x, y, z positives, par les lignes qui diviseront en parties égales l'angle δ ou son supplément, les formules (1) et (2) continueront de subsister.

Il est bon d'observer que les équations (1) peuvent être remplacées par la seule formule

$$2\sin\frac{\delta}{2}=\frac{\alpha_1-\alpha}{\lambda}=\frac{\beta_1-\beta}{\mu}=\frac{\gamma_1-\gamma}{\nu}, \tag{3}$$

et les équations (2) par la seule formule

$$2\cos\frac{\delta}{2}=\frac{\alpha_1+\alpha}{\lambda_1}=\frac{\beta_1+\beta}{\mu_1}=\frac{\gamma_1+\gamma}{\nu_1}. \tag{4}$$

D'ailleurs les cosinus α, β, γ des trois angles formés par une même droite avec les demi-axes des x, y, z supposés rectangulaires, vérifieront toujours la condition

$$\alpha^2+\beta^2+\gamma^2=1, \tag{5}$$

et l'on aura pareillement

$$\alpha_1^2+\beta_1^2+\gamma_1^2=1. \tag{6}$$

On trouvera de même

$$\lambda^2+\mu^2+\nu^2=1 \tag{7}$$

et

$$\lambda_1^2+\mu_1^2+\nu_1^2=1. \tag{8}$$

Enfin, l'on aura, d'une part,

$$\sin\delta=2\sin\frac{\delta}{2}\cos\frac{\delta}{2},$$

et, d'autre part,

$$\cos\delta=\cos^2\frac{\delta}{2}-\sin^2\frac{\delta}{2}.$$

Cela posé, on tirera des formules (3) et (4), non seulement

$$2\sin\delta=\frac{0}{\lambda\lambda_1+\mu\mu_1+\nu\nu_1},$$

et, par suite,

$$\lambda\lambda_1+\mu\mu_1+\nu\nu_1=0, \tag{9}$$

mais encore

$$\begin{cases}\sin^2\dfrac{\delta}{2}=\dfrac{(\alpha_1-\alpha)^2+(\beta_1-\beta)^2+(\gamma_1-\gamma)^2}{4},\\ \cos^2\dfrac{\delta}{2}=\dfrac{(\alpha_1+\alpha)^2+(\beta_1+\beta)^2+(\gamma_1+\gamma)^2}{4},\end{cases} \tag{10}$$

et, par suite,

$$\cos\delta=\alpha\alpha_1+\beta\beta_1+\gamma\gamma_1. \tag{11}$$

La formule (11), bien connue depuis longtemps, est celle qui sert à exprimer le cosinus de l'angle compris entre deux droites en fonction des cosinus des angles que forment ces deux droites avec les demi-axes des coordonnées positives, supposés rectangulaires. Quant à la formule (9), elle exprime simplement que les deux lignes qui divisent les quatre angles formés par deux droites en parties égales sont perpendiculaires entre elles.

Les valeurs de $\sin\frac{\delta}{2}$ et de $\cos\frac{\delta}{2}$, tirées des équations (10), sont respectivement

$$\begin{cases}\sin\dfrac{\delta}{2}=\dfrac{1}{2}\sqrt{(\alpha_1-\alpha)^2+(\beta_1-\beta)^2+(\gamma_1-\gamma)^2},\\ \cos\dfrac{\delta}{2}=\dfrac{1}{2}\sqrt{(\alpha_1+\alpha)^2+(\beta_1+\beta)^2+(\gamma_1+\gamma)^2}.\end{cases} \tag{12}$$

Si l'on substitue ces mêmes valeurs dans les formules (3) et (4), on trouvera

$$\frac{\lambda}{\alpha_1-\alpha}=\frac{\mu}{\beta_1-\beta}=\frac{\nu}{\gamma_1-\gamma}=\frac{1}{\sqrt{(\alpha_1-\alpha)^2+(\beta_1-\beta)^2+(\gamma_1-\gamma)^2}}, \tag{13}$$

$$\frac{\lambda_1}{\alpha_1+\alpha}=\frac{\mu_1}{\beta_1+\beta}=\frac{\nu_1}{\gamma_1+\gamma}=\frac{1}{\sqrt{(\alpha_1+\alpha)^2+(\beta_1+\beta)^2+(\gamma_1+\gamma)^2}}. \tag{14}$$

Lorsque les valeurs de α, β, γ, α_1, β_1, γ_1 seront données, celles de λ, μ, ν, λ_1, μ_1, ν_1 se déduiront immédiatement des formules (13) et (14).

Si les deux droites données représentent une droite mobile considérée successivement dans deux positions diverses, alors, en désignant par $\Delta\alpha$, $\Delta\beta$, $\Delta\gamma$ les accroissements que prendront les cosinus α, β, γ quand on passera de la première position à la seconde, on aura

$$\alpha_1=\alpha+\Delta\alpha,\qquad \beta_1=\beta+\Delta\beta,\qquad \gamma_1=\gamma+\Delta\gamma,$$

et, par suite, la formule (13) donnera simplement

$$\frac{\lambda}{\Delta\alpha}=\frac{\mu}{\Delta\beta}=\frac{\nu}{\Delta\gamma}=\frac{1}{\sqrt{(\Delta\alpha)^2+(\Delta\beta)^2+(\Delta\gamma)^2}}, \tag{15}$$

tandis que la première des formules (12) donnera

$$\sin\frac{\delta}{2}=\frac{1}{2}\sqrt{(\Delta\alpha)^2+(\Delta\beta)^2+(\Delta\gamma)^2}. \tag{16}$$

II. — *Sur la rotation d'une droite mobile dans l'espace.*

Concevons qu'une droite se meuve dans l'espace de manière que sa position et sa direction varient, par degrés insensibles, avec la valeur d'une certaine variable indépendante, qui sera désignée par t; et supposons d'abord, pour plus de simplicité, que cette droite mobile ait constamment pour origine un certain point fixe O. Concevons encore que, ce point fixe étant pris pour origine des coordonnées, on rapporte

tous les points de l'espace à trois axes rectangulaires des x, y, z. Enfin, considérons deux directions distinctes et successives de la droite mobile. Si l'on nomme α, β, γ les cosinus des angles que forme, avec les demi-axes des coordonnées positives, la première de ces deux directions, et si l'on indique, à l'aide de la caractéristique Δ, l'accroissement que prend une fonction quelconque de la variable indépendante, tandis que la droite mobile passe de la première direction à la seconde, l'angle δ compris entre les deux directions sera déterminé par l'équation (16) du paragraphe I, c'est-à-dire par la formule

$$\sin\frac{\delta}{2}=\frac{1}{2}\sqrt{(\Delta\alpha)^2+(\Delta\beta)^2+(\Delta\gamma)^2}; \tag{1}$$

et cet angle représentera ce qu'on peut appeler la *rotation de la droite mobile*, dans le passage d'une direction à l'autre. Soient d'ailleurs OA, OB deux longueurs égales à l'unité, qui se mesurent, à partir de l'origine O des coordonnées, sur les deux directions successives de la droite mobile, et nommons λ, μ, ν les cosinus des angles formés, avec les demi-axes des coordonnées positives, par la droite AB comptée à partir du point A. On aura encore, en vertu de la formule (15) du paragraphe I,

$$\frac{\lambda}{\Delta\alpha}=\frac{\mu}{\Delta\beta}=\frac{\nu}{\Delta\gamma}=\frac{1}{\sqrt{(\Delta\alpha)^2+(\Delta\beta)^2+(\Delta\gamma)^2}}, \tag{2}$$

ou, ce qui revient au même,

$$\frac{\Delta\alpha}{\lambda}=\frac{\Delta\beta}{\mu}=\frac{\Delta\gamma}{\nu}=\sqrt{(\Delta\alpha)^2+(\Delta\beta)^2+(\Delta\gamma)^2}; \tag{3}$$

et si l'on divise les deux membres de l'équation (3) par l'accroissement Δt de la variable indépendante t, on trouvera

$$\frac{1}{\lambda}\frac{\Delta\alpha}{\Delta t}=\frac{1}{\mu}\frac{\Delta\beta}{\Delta t}=\frac{1}{\nu}\frac{\Delta\gamma}{\Delta t}=\sqrt{\left(\frac{\Delta\alpha}{\Delta t}\right)^2+\left(\frac{\Delta\beta}{\Delta t}\right)^2+\left(\frac{\Delta\gamma}{\Delta t}\right)^2}. \tag{4}$$

Si au contraire on divise par Δt les deux membres de l'équation (1), celle qu'on obtiendra pourra être présentée sous la forme suivante :

$$\frac{\delta}{\Delta t}=\frac{\frac{1}{2}\delta}{\sin\left(\frac{1}{2}\delta\right)}\sqrt{\left(\frac{\Delta\alpha}{\Delta t}\right)^2+\left(\frac{\Delta\beta}{\Delta t}\right)^2+\left(\frac{\Delta\gamma}{\Delta t}\right)^2}. \tag{5}$$

Concevons maintenant que l'accroissement Δt de la variable indépendante devienne infiniment petit; l'angle δ deviendra lui-même infiniment petit, aussi bien que les accroissements $\Delta\alpha$, $\Delta\beta$, $\Delta\gamma$ des variables α, β, γ : alors, tandis que Δt décroîtra indéfiniment, la fraction $\frac{\delta}{\Delta t}$, c'est-à-dire le rapport entre l'angle δ et l'accroissement de la variable indépendante, convergera vers une certaine limite que nous nommerons le *module de rotation* de la droite mobile. En désignant par $\varkappa$ cette limite, et en observant que, pour des valeurs infiniment petites de Δt, les rapports

$$\frac{\frac{1}{2}\delta}{\sin\frac{1}{2}\delta},\quad \frac{\Delta\alpha}{\Delta t},\quad \frac{\Delta\beta}{\Delta t},\quad \frac{\Delta\gamma}{\Delta t}$$

convergent eux-mêmes vers les limites

$$1,\quad D_t\alpha,\quad D_t\beta,\quad D_t\gamma,$$

on tirera de la formule (5)

$$\varkappa=\sqrt{(D_t\alpha)^2+(D_t\beta)^2+(D_t\gamma)^2}. \tag{6}$$

De plus, quand Δt deviendra infiniment petit, la formule (4) donnera évidemment

$$\frac{1}{\lambda}D_t\alpha=\frac{1}{\mu}D_t\beta=\frac{1}{\nu}D_t\gamma=\sqrt{(D_t\alpha)^2+(D_t\beta)^2+(D_t\gamma)^2}, \tag{7}$$

ou, ce qui revient au même,

$$\frac{1}{\lambda}D_t\alpha=\frac{1}{\mu}D_t\beta=\frac{1}{\nu}D_t\gamma=\varkappa; \tag{8}$$

et l'on en conclura

$$\lambda=\frac{D_t\alpha}{\varkappa},\qquad \mu=\frac{D_t\beta}{\varkappa},\qquad \nu=\frac{D_t\gamma}{\varkappa}. \tag{9}$$

Mais alors aussi, l'angle δ étant infiniment petit, les deux autres angles du triangle isocèle OAB seront sensiblement droits, et, par suite, la base AB de ce triangle sera sensiblement perpendiculaire à chacun des côtés OA, OB. Il y a plus : les droites OA, OB étant deux arêtes du

cône qui a pour sommet le point O et pour génératrice la droite mobile, le plan qui renfermera ces deux arêtes se rapprochera indéfiniment, pour des valeurs infiniment petites de $\hat{\varepsilon}$, du plan qui touchera le cône suivant l'arête OA. Cela posé, les valeurs de λ, μ, ν, déterminées par les équations (9), exprimeront évidemment les cosinus des angles formés, avec les demi-axes des coordonnées positives, par une perpendiculaire menée à la droite mobile dans le plan tangent au cône qu'elle décrit, cette perpendiculaire étant d'ailleurs dirigée dans le sens qu'indique le mouvement de rotation de la génératrice du cône. Nous représenterons généralement le module de rotation $\varkappa$ par une longueur mesurée sur la perpendiculaire dont il s'agit, et dirigée dans le même sens qu'elle. Dès lors les projections algébriques de ce module sur les axes des x, y, z seront évidemment exprimées par les trois produits

$$\varkappa\lambda, \quad \varkappa\mu, \quad \varkappa\nu,$$

ou, ce qui revient au même, eu égard aux formules (9), par les trois dérivées

$$D_t\alpha, \quad D_t\beta, \quad D_t\gamma.$$

Nous avons supposé jusqu'ici que la droite mobile OA passait constamment par un point fixe O. Si cette condition n'était pas remplie, on pourrait imaginer une seconde droite qui, partant d'un point fixe de l'espace, resterait constamment parallèle à la droite mobile OA, et le module de rotation de cette seconde droite, transporté parallèlement à lui-même, de manière à offrir pour première extrémité un point de la droite mobile, serait ce que nous appellerions le *module de rotation* de cette dernière. Ainsi défini, le module de rotation de la droite mobile se confond avec la limite du rapport qu'on obtient quand on divise l'angle infiniment petit compris entre deux directions de cette droite, successivement considérée dans deux positions infiniment voisines, par l'accroissement qu'acquiert la variable indépendante, tandis que l'on passe de la première direction à la seconde. Ajoutons que ce même module se mesure sur une perpendiculaire menée à la première direction dans le plan qui la renferme, et qui est parallèle à la seconde

direction, ou plutôt sur le demi-axe dont s'approche infiniment cette perpendiculaire, prolongée à partir d'un point situé sur la direction de la droite mobile, dans le sens indiqué par le mouvement de rotation de cette droite. Cela posé, soient toujours :

t la variable indépendante;

α, β, γ les cosinus des angles formés par la droite mobile OA avec les demi-axes des x, y, z positives;

$\varkappa$ le module de rotation de la droite mobile;

λ, μ, ν les cosinus des angles formés par le module de rotation $\varkappa$ avec les demi-axes des x, y, z positives.

Les quantités $\varkappa$, λ, μ, ν se trouveront généralement liées aux cosinus α, β, γ par les formules (6), (9); et, en conséquence, les projections algébriques du module $\varkappa$ seront exprimées par les trois produits

$$\varkappa\lambda = D_t\alpha, \qquad \varkappa\mu = D_t\beta, \qquad \varkappa\nu = D_t\gamma. \tag{10}$$

Il est bon d'observer que les cosinus α, β, γ des trois angles formés par la droite mobile, avec les demi-axes des coordonnées positives, vérifient l'équation de condition

$$\alpha^2 + \beta^2 + \gamma^2 = 1. \tag{11}$$

Or, de cette équation, différentiée par rapport à t, on tire

$$\alpha D_t\alpha + \beta D_t\beta + \gamma D_t\gamma = 0,$$

et par suite, eu égard aux formules (10),

$$\alpha\lambda + \beta\mu + \gamma\nu = 0. \tag{12}$$

Le résultat auquel nous venons de parvenir pouvait être aisément prévu, car l'équation (11) exprime simplement que la direction du module $\varkappa$ est perpendiculaire à celle de la droite mobile.

Quel que soit, sur une droite mobile, le point à partir duquel se mesure le module de rotation de cette droite, il est clair que la direction de ce module variera généralement, comme la direction de la droite elle-même, avec la variable indépendante t. On pourra donc

rechercher non seulement le module de rotation $\varkappa$ de la droite mobile, mais encore le module de rotation υ du module $\varkappa$, puis le module de rotation du module υ, ... On trouvera ainsi successivement ce que nous appellerons les *modules de rotation des divers ordres* de la droite mobile, le module du module étant désigné sous le nom de *module du second ordre*, tout comme la différentielle de la différentielle d'une fonction quelconque est désignée sous le nom de *différentielle du second ordre*. Si d'ailleurs on représente par

$$\varphi, \quad \chi, \quad \psi$$

les cosinus des angles que formera le module du second ordre υ, ou plutôt la direction de ce module, avec les demi-axes des x, y, z positives, les quantités

$$\upsilon, \quad \varphi, \quad \chi, \quad \psi$$

auront évidemment, avec les cosinus λ, μ, ν, des relations semblables à celles que les formules (6) et (9) établissent entre les quantités

$$\varkappa, \quad \lambda, \quad \mu, \quad \nu$$

et les cosinus α, β, γ. Donc le module du second ordre υ, et les cosinus φ, χ, ψ des angles qui déterminent la direction de ce module, se déduiront des cosinus λ, μ, ν, à l'aide des équations

$$\upsilon = \sqrt{(D_t\lambda)^2 + (D_t\mu)^2 + (D_t\nu)^2}, \tag{13}$$

$$\gamma\upsilon = D_t\lambda, \qquad \nu\chi = D_t\mu, \qquad \nu\psi = D_t\nu. \tag{14}$$

De plus, aux formules (11) et (12) on pourra joindre les formules semblables

$$\lambda^2 + \mu^2 + \nu^2 = 1, \tag{15}$$

$$\lambda\varphi + \mu\chi + \nu\psi = 0, \tag{16}$$

dont la seconde exprime que les directions sur lesquelles se mesurent les modules du premier et du second ordre sont perpendiculaires l'une à l'autre. On obtiendra des résultats du même genre, en considérant les modules de rotation des ordres supérieurs au second. Ajoutons que des équations (12), (16), différentiées par rapport à t, on déduira des formules nouvelles. Ainsi, en particulier, la formule (12)

donnera

$$\lambda D_t\alpha + \mu D_t\beta + \nu D_t\gamma + \alpha D_t\lambda + \beta D_t\mu + \gamma D_t\nu = 0.$$

Mais, des formules (10) jointes à l'équation (15), on tirera

$$\varkappa = \lambda D_t\alpha + \mu D_t\beta + \nu D_t\gamma.$$

On aura donc encore

$$\varkappa + \alpha D_t\lambda + \beta D_t\mu + \gamma D_t\nu = 0,$$

ou, ce qui revient au même,

$$\varkappa = -(\alpha D_t\lambda + \beta D_t\mu + \gamma D_t\nu), \tag{17}$$

puis on tirera de l'équation (17), jointe aux formules (14),

$$\varkappa = -\upsilon(\alpha\varphi + \beta\chi + \gamma\psi).$$

D'ailleurs le trinome

$$\alpha\varphi + \beta\chi + \gamma\psi$$

représente le cosinus de l'angle formé par la droite mobile avec la direction du module υ. Donc, si l'on désigne par ω une longueur mesurée dans la direction de la droite mobile, et par $\left(\widehat{\omega, \upsilon}\right)$ l'angle compris entre cette direction et celle du module υ, on aura

$$\alpha\varphi + \beta\chi + \gamma\psi = \cos\left(\widehat{\omega, \upsilon}\right), \tag{18}$$

et, par suite,

$$\varkappa = -\upsilon\cos\left(\widehat{\omega, \upsilon}\right). \tag{19}$$

Cette dernière équation fournit immédiatement la proposition suivante :

THÉORÈME I. — *Le module de rotation du premier ordre d'une droite mobile est numériquement égal au module de rotation du second ordre, projeté sur cette droite. Mais la droite mobile et son module de rotation du second ordre, projeté sur elle-même, sont dirigés en sens inverse.*

Soient maintenant

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

les cosinus des angles formés, avec les demi-axes des x, y, z positives, par une perpendiculaire au plan qui renferme à la fois la droite mobile et son module de rotation $\varkappa$ du premier ordre. On aura non seulement

$$\alpha a + \beta b + \gamma c = 0, \tag{20}$$

mais encore

$$\lambda a + \mu b + \nu c = 0, \tag{21}$$

et, par suite,

$$\frac{a}{\beta\nu - \gamma\mu} = \frac{b}{\gamma\lambda - \alpha\nu} = \frac{c}{\alpha\mu - \beta\lambda}. \tag{22}$$

Comme on aura d'ailleurs

$$a^2 + b^2 + c^2 = 1, \tag{23}$$

et, en vertu des équations (11), (12), (15),

$$\begin{aligned}&(\beta\nu - \gamma\mu)^2 + (\gamma\lambda - \alpha\nu)^2 + (\alpha\mu - \beta\lambda)^2\\ &= (\alpha^2 + \beta^2 + \gamma^2)(\lambda^2 + \mu^2 + \nu^2) - (\alpha\lambda + \beta\mu + \gamma\nu)^2 = 1,\end{aligned}$$

on tirera de la formule (22)

$$\frac{a}{\beta\nu - \gamma\mu} = \frac{b}{\gamma\lambda - \alpha\nu} = \frac{c}{\alpha\mu - \beta\lambda} = \pm 1. \tag{24}$$

La formule (24) fournira, pour a, b, c, deux systèmes de valeurs correspondants aux deux directions, opposées l'une à l'autre, suivant lesquelles peut se prolonger une droite perpendiculaire au plan qui renferme à la fois la droite mobile et le module $\varkappa$. Si entre ces deux directions on choisit celle qui réduit le double signe $\pm$ au signe $+$, dans le second membre de la formule (24), on aura simplement

$$\frac{a}{\beta\nu - \gamma\mu} = \frac{b}{\gamma\lambda - \alpha\nu} = \frac{c}{\alpha\mu - \beta\lambda} = 1, \tag{25}$$

et, par suite,

$$a = \beta\nu - \gamma\mu, \qquad b = \gamma\lambda - \alpha\nu, \qquad c = \alpha\mu - \beta\lambda. \tag{26}$$

Concevons à présent que la droite mobile qui formait, avec les demi-axes des x, y, z positives, des angles dont les cosinus étaient α, β, γ,

soit remplacée par une nouvelle droite, savoir, par celle qui forme, avec les demi-axes des coordonnées positives, des angles dont les cosinus a, b, c se déduisent des équations (26). Nommons ϑ le module de rotation de cette nouvelle droite, et l, m, n les cosinus des angles formés par la direction de ce module avec les demi-axes des x, y, z positives. Des relations semblables à celles que les formules (6) et (10) établissaient entre les quantités

$$\alpha, \quad \beta, \quad \gamma \quad \text{et} \quad \varkappa, \quad \lambda, \quad \mu, \quad \nu$$

subsisteront encore évidemment entre les quantités

$$a, \quad b, \quad c \quad \text{et} \quad \vartheta, \quad l, \quad m, \quad n.$$

Donc le module ϑ et les cosinus l, m, n se déduiront des cosinus a, b, c à l'aide des formules

$$\vartheta = \sqrt{(\mathrm{D}_t a)^2 + (\mathrm{D}_t b)^2 + (\mathrm{D}_t c)^2}, \tag{27}$$

$$\vartheta l = \mathrm{D}_t a, \qquad \vartheta m = \mathrm{D}_t b, \qquad \vartheta n = \mathrm{D}_t c. \tag{28}$$

D'ailleurs, en ayant égard aux formules (10), on tirera des équations (26)

$$\mathrm{D}_t a = \beta \mathrm{D}_t \nu - \gamma \mathrm{D}_t \mu, \qquad \mathrm{D}_t b = \gamma \mathrm{D}_t \lambda - \alpha \mathrm{D}_t \nu, \qquad \mathrm{D}_t c = \alpha \mathrm{D}_t \mu - \beta \mathrm{D}_t \lambda, \tag{29}$$

et, par suite,

$$\alpha \mathrm{D}_t a + \beta \mathrm{D}_t b + \gamma \mathrm{D}_t c = 0, \tag{30}$$

ce que l'on pourrait aussi conclure de l'équation (20), différentiée par rapport à t et combinée avec les formules (10) et (26). De plus, l'équation (23), différentiée par rapport à t, donnera

$$a \mathrm{D}_t a + b \mathrm{D}_t b + c \mathrm{D}_t c = 0; \tag{31}$$

et des formules (30), (31), jointes aux équations (28), on tirera

$$\begin{cases} \alpha l + \beta m + \gamma n = 0, \\ a l + b m + c n = 0. \end{cases} \tag{32}$$

Or, pour obtenir les équations (32), qui sont linéaires par rapport à l, m, n, il suffit évidemment de remplacer, dans les équations (12) et (21), λ par l, μ par m, ν par n. Donc les valeurs des rapports $\frac{m}{l}$, $\frac{n}{l}$,

tirées des formules (32), seront respectivement égales aux valeurs des rapports $\frac{\mu}{\lambda}, \frac{\nu}{\lambda}$, tirées des formules (12) et (19), et l'on aura

$$\frac{\mu}{\lambda}=\frac{m}{l}, \qquad \frac{\nu}{\lambda}=\frac{n}{l},$$

ou, ce qui revient au même,

$$\frac{l}{\lambda}=\frac{m}{\mu}=\frac{n}{\nu}; \tag{33}$$

puis, en ayant égard à l'équation (15) et à la suivante,

$$l^2+m^2+n^2=1, \tag{34}$$

on conclura de la formule (33)

$$\frac{l}{\lambda}=\frac{m}{\mu}=\frac{n}{\nu}=\pm 1. \tag{35}$$

Donc la direction, sur laquelle se mesurera le module de rotation θ, ne pourra être que la direction sur laquelle se mesurait déjà le module de rotation $\varkappa$, ou la direction opposée. On arriverait encore, sans calcul, aux mêmes conclusions, en se bornant à comparer les formules (32) aux formules (12) et (21), et en observant que ces formules fournissent, pour direction du module θ ou du module $\varkappa$, celle d'une perpendiculaire aux deux droites qui forment, avec les demi-axes des x, y, z positives, des angles dont les cosinus sont, d'une part, α, β, γ, et, d'autre part, a, b, c. D'ailleurs, rien ne détermine *a priori* le signe qui doit précéder l'unité dans le dernier membre de la formule (35). On peut donc énoncer la proposition suivante :

THÉORÈME II. — *Si, après avoir construit le module de rotation $\varkappa$ d'une droite mobile, on élève une perpendiculaire au plan qui renferme à la fois ce module et la droite elle-même, le module de rotation θ de cette perpendiculaire et le module de rotation $\varkappa$ de la droite mobile se mesureront sur un même axe; mais ils pourront offrir ou une direction unique, ou des directions opposées.*

Revenons maintenant aux formules (29). De ces formules, jointes

aux équations (14) et (28), on tirera

$$\theta l=\upsilon(\beta\psi-\gamma\chi), \qquad \theta m=\upsilon(\gamma\varphi-\alpha\psi), \qquad \theta n=\upsilon(\alpha\chi-\beta\varphi), \tag{36}$$

et par suite, eu égard à la formule (34),

$$\theta^2=\upsilon^2[(\beta\psi-\gamma\chi)^2+(\gamma\varphi-\alpha\psi)^2+(\alpha\chi-\beta\varphi)^2],$$

ou, ce qui revient au même,

$$\theta=\upsilon\sqrt{(\beta\psi-\gamma\chi)^2+(\gamma\varphi-\alpha\psi)^2+(\alpha\chi-\beta\varphi)^2}. \tag{37}$$

Mais, d'autre part, en ayant égard aux formules (11), (18) et à l'équation

$$\varphi^2+\chi^2+\psi^2=1, \tag{38}$$

on trouvera

$$\begin{aligned}&(\beta\psi-\gamma\chi)^2+(\gamma\varphi-\alpha\psi)^2+(\alpha\chi-\beta\varphi)^2\\&=(\alpha^2+\beta^2+\gamma^2)(\varphi^2+\chi^2+\psi^2)-(\alpha\varphi+\beta\chi+\gamma\psi)^2\\&=1-\cos^2\left(\widehat{\omega,\upsilon}\right)=\sin^2\left(\widehat{\omega,\upsilon}\right).\end{aligned}$$

Donc la formule (37) donnera

$$\theta=\upsilon\sin\left(\widehat{\omega,\upsilon}\right). \tag{39}$$

Mais $\upsilon\sin\left(\widehat{\omega,\upsilon}\right)$ représentera évidemment le module du second ordre υ projeté sur un plan perpendiculaire à la direction de la droite mobile. Donc la formule (39) entraînera immédiatement la proposition suivante :

THÉORÈME III. — *Si, après avoir construit les deux premiers modules de rotation d'une droite mobile, c'est-à-dire les modules de rotation du premier et du second ordre $\varkappa$ et υ, on élève une perpendiculaire au plan qui renferme à la fois ce module et la droite elle-même, le module de rotation de cette perpendiculaire se déduira aisément du module du second ordre υ, et sera numériquement égal à la projection de ce module sur un plan perpendiculaire à la droite.*

En ayant égard à l'équation identique

$$\cos^2\left(\widehat{\omega,\upsilon}\right)+\sin^2\left(\widehat{\omega,\upsilon}\right)=1,$$

on tire immédiatement des formules (19) et (39)

$$\varkappa^2 + \theta^2 = \upsilon^2. \tag{40}$$

On arriverait aussi à la même conclusion, en observant que l'on tire des formules (28) et (29)

$$\theta^2 = (\beta D_t\nu - \gamma D_t\mu)^2 + (\gamma D_t\lambda - \alpha D_t\nu)^2 + (\alpha D_t\mu - \beta D_t\lambda)^2,$$

et de cette dernière, jointe aux formules (11), (17) et (14),

$$\varkappa^2 + \theta^2 = (D_t\lambda)^2 + (D_t\mu)^2 + (D_t\nu)^2 = \upsilon^2.$$

On peut donc énoncer encore la proposition suivante :

THÉORÈME IV. — *Si, après avoir construit les deux premiers modules de rotation d'une droite mobile, c'est-à-dire les modules du premier et du second ordre $\varkappa$ et υ, on élève une perpendiculaire au plan qui renferme à la fois le module du premier ordre $\varkappa$ et la droite elle-même, le module de rotation θ de cette perpendiculaire offrira un carré θ^2, qui, étant ajouté au carré $\varkappa^2$ du module du premier ordre $\varkappa$, donnera pour somme le carré υ^2 du module du second ordre υ.*

Jusqu'ici nous n'avons point spécifié la nature de la variable indépendante t. Dans le cas particulier où cette variable représente le temps, et où la droite mobile OA passe par un point fixe O, le module $\varkappa$, c'est-à-dire le module de rotation du premier ordre de la droite OA, n'est évidemment autre chose que la vitesse du point A situé sur la droite mobile à l'unité de distance du point fixe. Donc alors le module de rotation $\varkappa$ se réduit à ce qu'on doit appeler la *vitesse angulaire de rotation* de la droite mobile. Alors aussi, pour établir directement les formules (10), il suffit d'observer que, le point O étant pris pour origine,

$$\alpha, \quad \beta, \quad \gamma \quad \text{et} \quad D_t\alpha, \quad D_t\beta, \quad D_t\gamma$$

représenteront, d'une part, les coordonnées du point A, et, d'autre part, les projections algébriques de la vitesse de ce même point, ou, ce qui revient au même, les projections algébriques de la vitesse angulaire de rotation de la droite OA.

Si, le temps t étant toujours pris pour variable indépendante, la droite mobile OA se meut d'une manière quelconque dans l'espace, en changeant de position et de direction par degrés insensibles, mais sans être assujettie à passer constamment par le même point fixe O, la *vitesse angulaire de rotation* de cette droite ne sera autre chose que la vitesse angulaire de rotation d'une droite parallèle, par conséquent d'une droite qui formera les mêmes angles avec les axes coordonnés. Donc, si l'on nomme toujours α, β, γ les cosinus des trois angles formés par la droite mobile avec les demi-axes des x, y, z positives, la vitesse angulaire $\varkappa$ de cette droite offrira encore des projections algébriques représentées par les trois dérivées

$$D_t\alpha, \quad D_t\beta, \quad D_t\gamma,$$

et ces trois dérivées seront encore liées à la vitesse angulaire et aux cosinus λ, μ, ν des angles que formera la direction de la vitesse $\varkappa$, avec les demi-axes des x, y, z positives, par les équations (9).

III. — *Modules de rotation d'une droite mobile qui s'appuie constamment sur une courbe donnée.*

Supposons qu'une droite mobile s'appuie constamment sur une courbe dont les coordonnées, relatives à trois axes rectangulaires, soient représentées par

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

Nommons s l'arc de cette courbe, compté positivement dans un certain sens, et aboutissant au point (x, y, z). Prenons cet arc pour variable indépendante, et soient

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

les fonctions de s qui représentent les cosinus des angles formés, par la droite mobile prolongée dans une certaine direction, avec les demi-axes des x, y, z positives. Enfin, Δs étant un très petit accroissement attribué à l'arc s, nommons δ l'angle infiniment petit que décrit la droite mobile tandis que son point d'appui sur la courbe donnée par-

court l'arc infiniment petit Δs; en sorte que δ désigne l'angle compris entre les deux directions extrêmes de la droite mobile correspondantes aux deux extrémités de l'arc Δs. Si par la première de ces deux directions on fait passer un plan parallèle à la seconde, et si, dans ce plan, on porte une longueur numériquement représentée par le rapport $\frac{\delta}{\Delta s}$, sur une perpendiculaire à la première direction, cette perpendiculaire étant prolongée dans le sens indiqué par le mouvement de rotation de la droite mobile OA; le rapport dont il s'agit, ou plutôt la limite $\varkappa$ vers laquelle convergera ce rapport, tandis que l'arc élémentaire Δs deviendra de plus en plus petit, représentera, en grandeur et en direction, d'après les définitions adoptées dans le paragraphe II, ce qu'on devra nommer le *module de rotation* de la droite mobile. Soient d'ailleurs

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

les cosinus des angles formés, par la direction du module $\varkappa$, avec les demi-axes des coordonnées positives. Les valeurs des quantités

$$\varkappa, \quad \lambda, \quad \mu, \quad \nu$$

seront celles que fourniront les équations (6) et (10) du paragraphe II, quand on y remplacera la variable indépendante t par la variable indépendante s. On aura donc

$$\varkappa = \sqrt{(\mathrm{D}_s\alpha)^2 + (\mathrm{D}_s\beta)^2 + (\mathrm{D}_s\gamma)^2} \tag{1}$$

et

$$\varkappa\lambda = \mathrm{D}_s\alpha, \qquad \varkappa\mu = \mathrm{D}_s\beta, \qquad \varkappa\nu = \mathrm{D}_s\gamma. \tag{2}$$

Pareillement, si l'on nomme υ le module du module de rotation de la droite mobile, ou, en d'autres termes, le *module de rotation du second ordre*, et φ, χ, ψ les cosinus des angles formés, par la direction du module υ, avec les demi-axes des x, y, z positives, on aura, en prenant toujours l'arc s pour variable indépendante,

$$\upsilon = \sqrt{(\mathrm{D}_s\lambda)^2 + (\mathrm{D}_s\mu)^2 + (\mathrm{D}_s\nu)^2}, \tag{3}$$

$$\upsilon\varphi = \mathrm{D}_s\lambda, \qquad \upsilon\chi = \mathrm{D}_s\mu, \qquad \upsilon\psi = \mathrm{D}_s\nu. \tag{4}$$

Enfin, si par un point de la droite mobile on élève une perpendiculaire au plan qui renferme, avec cette droite, son module de rotation du premier ordre, non seulement cette perpendiculaire, prolongée dans un certain sens, formera, avec les demi-axes des x, y, z positives, des angles dont les cosinus a, b, c seront déterminés par les formules

$$a = \beta\nu - \gamma\mu, \qquad b = \lambda\gamma - \alpha\nu, \qquad c = \alpha\mu - \beta\lambda; \tag{5}$$

mais, de plus, le module de rotation θ de cette perpendiculaire, considérée comme fonction de l'arc s pris pour variable indépendante, sera déterminé par la formule

$$\theta = \sqrt{(\mathrm{D}_s a)^2 + (\mathrm{D}_s b)^2 + (\mathrm{D}_s c)^2}, \tag{6}$$

et se mesurera sur le même axe que le module $\varkappa$, sans que l'on puisse toutefois affirmer qu'il se mesurera dans le même sens.

Soit maintenant ω une longueur mesurée sur la droite mobile, et sur la direction même qui forme, avec les demi-axes des x, y, z positives, les angles dont les cosinus sont représentés par α, β, γ. Si l'on se sert de la notation $\left(\widehat{\omega, \upsilon}\right)$ pour exprimer l'angle compris entre les directions de ω et de υ, on aura, en vertu des formules (19), (39), (40) du paragraphe II,

$$\varkappa = -\upsilon\cos\left(\widehat{\omega, \upsilon}\right), \qquad \theta = \upsilon\sin\left(\widehat{\omega, \upsilon}\right), \tag{7}$$

et, par suite,

$$\varkappa^2 + \theta^2 = \upsilon^2. \tag{8}$$

Donc, si l'on projette le module du second ordre υ : 1° sur la droite mobile; 2° sur un plan perpendiculaire à la direction de cette droite, les projections ainsi obtenues seront exprimées numériquement par le module du premier ordre $\varkappa$ et par le module θ; et ces deux derniers modules pourront représenter les deux côtés d'un triangle rectangle qui aurait pour hypoténuse le module $\varkappa$.

Concevons à présent que l'on désigne par les lettres

$$\rho, \quad r, \quad \varepsilon$$

les rapports inverses des modules

$$\varkappa,\quad \vartheta,\quad \upsilon;$$

en sorte qu'on ait

$$\rho=\frac{1}{\varkappa},\qquad r=\frac{1}{\vartheta},\qquad \iota=\frac{1}{\upsilon}, \tag{9}$$

et, par suite,

$$\varkappa=\frac{1}{\rho},\qquad \vartheta=\frac{1}{r},\qquad \upsilon=\frac{1}{\iota}. \tag{10}$$

Chacune des quantités

$$\rho,\quad r,\quad \iota$$

pourra être représentée, comme le module qui lui correspond, par une longueur portée sur la direction de ce module. On peut même observer qu'elle se trouvera tout naturellement représentée par une longueur, si l'on exprime, suivant l'usage, les angles par de simples nombres. Car la quantité ρ, par exemple, étant l'inverse du module $\varkappa$ qui représente la limite du rapport $\frac{\delta}{\Delta s}$, sera elle-même la limite du rapport $\frac{\Delta s}{\delta}$. Elle sera donc de même nature que ce rapport et, par suite, de même nature que l'arc Δs, si l'angle δ est réduit à un simple nombre. Donc alors la quantité ρ sera de la nature des longueurs. Ajoutons qu'en vertu des formules (9) ou (10), les équations (1), (2), (3), (4), (6) donneront

$$\frac{1}{\rho}=\sqrt{(\mathrm{D}_s\alpha)^2+(\mathrm{D}_s\beta)^2+(\mathrm{D}_s\gamma)^2}, \tag{11}$$

$$\lambda=\rho\mathrm{D}_s\alpha,\qquad \mu=\rho\mathrm{D}_s\beta,\qquad \nu=\rho\mathrm{D}_s\gamma, \tag{12}$$

$$\frac{1}{\iota}=\sqrt{(\mathrm{D}_s\lambda)^2+(\mathrm{D}_s\mu)^2+(\mathrm{D}_s\nu)^2}, \tag{13}$$

$$\varphi=\iota\mathrm{D}_s\lambda,\qquad \chi=\iota\mathrm{D}_s\mu,\qquad \psi=\iota\mathrm{D}_s\nu, \tag{14}$$

$$\frac{1}{r}=\sqrt{(\mathrm{D}_s a)^2+(\mathrm{D}_s b)^2+(\mathrm{D}_s c)^2}. \tag{15}$$

Observons enfin que, la longueur ι étant mesurée sur la direction du module υ, l'angle $\left(\widehat{\omega,\upsilon}\right)$ pourra être encore exprimé par la notation $\left(\widehat{\omega,\iota}\right)$. Donc les formules (7), jointes aux équations (10), donneront

$$\frac{1}{\rho}=-\frac{1}{\iota}\cos\left(\widehat{\omega,\iota}\right),\qquad \frac{1}{r}=\frac{1}{\iota}\sin\left(\widehat{\omega,\iota}\right), \tag{16}$$

tandis que la formule (8) donnera

$$\frac{1}{\rho^2}+\frac{1}{r^2}=\frac{1}{\iota^2}. \tag{17}$$

Pour montrer une application très simple des formules diverses que nous venons d'établir, considérons, en particulier, le cas où la droite mobile se confond avec la tangente menée à la courbe proposée par l'extrémité de l'arc s, c'est-à-dire par le point dont les coordonnées sont x, y, z; cette tangente étant d'ailleurs dirigée dans le sens suivant lequel se mesurent les arcs positifs. Dans ce cas, les cosinus α, β, γ des angles formés par la droite mobile avec les demi-axes des x, y, z positives seront respectivement

$$\alpha=\mathrm{D}_s x,\qquad \beta=\mathrm{D}_s y,\qquad \gamma=\mathrm{D}_s z. \tag{18}$$

Alors aussi δ sera l'angle compris entre les deux tangentes menées par les deux extrémités de l'arc Δs. En d'autres termes, δ sera ce qu'on nomme l'*angle de contingence*; et, comme l'arc Δs, compté à partir de l'extrémité de l'arc s, sera d'autant plus courbe que l'angle δ sera plus considérable, le rapport

$$\frac{\delta}{\Delta s}$$

représentera naturellement ce qu'on peut appeler la *courbure moyenne* de l'arc Δs. Ajoutons qu'en faisant décroître indéfiniment l'arc Δs, on verra sa courbure moyenne converger vers une certaine limite $\varkappa$ qui sera précisément ce qu'on appelle la *courbure* de l'arc s, mesurée à l'extrémité de cet arc. Donc cette courbure ne différera pas du module de rotation de la tangente, déterminé par la formule (1). Quant aux cosinus λ, μ, ν des angles formés, avec les demi-axes des x, y, z positives, par la ligne sur laquelle se mesurera le module $\varkappa$, ils seront déterminés par les formules (2) desquelles on tirera, eu égard à la

formule (1),

$$\frac{\lambda}{D_s\alpha}=\frac{\mu}{D_s\beta}=\frac{\nu}{D_s\gamma}=\frac{1}{\sqrt{(D_s\alpha)^2+(D_s\beta)^2+(D_s\gamma)^2}}, \tag{19}$$

ou, ce qui revient au même, eu égard aux équations (18),

$$\frac{\lambda}{D_s^2x}=\frac{\mu}{D_s^2y}=\frac{\nu}{D_s^2z}=\frac{1}{\sqrt{(D_s^2x)^2+(D_s^2y)^2+(D_s^2z)^2}}. \tag{20}$$

Donc cette ligne sera non seulement une perpendiculaire à la tangente, ou, en d'autres termes, une des normales menées à la courbe par le point (x, y, z), mais encore celle de ces normales qui a été désignée sous le nom de *normale principale*, et qui se trouve comprise dans le plan osculateur (voir les *Leçons sur les applications du Calcul infinitésimal à la Géométrie*, t. I, p. 287) (1).

Si la courbe donnée se réduit à un cercle, l'angle de contingence $\hat{o}$ sera équivalent à l'angle au centre qui renfermera l'arc Δs entre ses côtés. Donc le rapport $\frac{\Delta s}{\hat{o}}$ représentera le rayon du cercle, et ce rayon sera encore représenté par la limite $\frac{1}{\varkappa}$ de ce rapport, c'est-à-dire par la longueur ρ. Donc, dans un cercle, le rayon ρ est l'inverse de la courbure $\varkappa$, et, réciproquement, la courbure $\varkappa$ est l'inverse du rayon ρ. Donc, si, après avoir désigné par $\varkappa$ la courbure d'une courbe quelconque en un certain point (x, y, z), on nomme ρ une longueur liée à la courbure $\varkappa$ par la première des équations (9), cette longueur sera le rayon d'un cercle qui offrira la même courbure que la courbe, ou, en d'autres termes, elle sera ce qu'on appelle le *rayon de courbure* de la courbe donnée au point (x, y, z). Si cette même longueur est portée, à partir du point (x, y, z), dans le sens suivant lequel se mesurait le module de rotation de la tangente, elle aboutira au point appelé le *centre de courbure*, et le cercle décrit de ce dernier point, comme centre, avec un rayon égal au rayon de courbure, sera le cercle qui aura un contact du second ordre avec la courbe, et que l'on nomme, pour cette raison, le *cercle osculateur* (*voir* les Leçons déjà citées). Cela

(1) *Œuvres de Cauchy*, série II, t. V, p. 295.

posé, il suffira évidemment d'attribuer aux cosinus α, β, γ les valeurs fournies par les équations (18), pour que la valeur de ρ, déterminée par la formule (11), représente le rayon du cercle osculateur, et pour que les valeurs de λ, μ, ν, déterminées par les formules (12), représentent les cosinus des angles formés, avec les demi-axes des x, y, z positives, par la droite menée du point (x, y, z) au centre de courbure. Observons, au reste, que les équations ainsi obtenues, savoir :

$$\frac{1}{\rho}=\sqrt{(D_s^2x)^2+(D_s^2y)^2+(D_s^2z)^2}, \tag{21}$$

$$\lambda=\rho D_s^2x, \qquad \mu=\rho D_s^2y, \qquad \nu=\rho D_s^2z, \tag{22}$$

entraînent la formule (20), à laquelle on parvient en égalant entre elles les quatre valeurs que ces mêmes équations fournissent pour le rayon de courbure ρ.

Considérons maintenant, parmi les modules de rotation de la courbe donnée, celui qui est du second ordre. Ce module, déterminé par la formule (3), et mesuré dans une direction qui forme, avec les demi-axes des coordonnées positives, des angles dont les cosinus φ, χ, ψ se déterminent par les formules (4), sera ce que j'ai nommé la *seconde courbure*, et ce que M. de Saint-Venant appelle la *cambrure* de la courbe proposée. L'inverse de ce même module, ou le rayon ι, déterminé par la formule (13), sera le *rayon de seconde courbure*, ou le *rayon de cambrure*, qui se mesurera sur la droite tracée de manière à former, avec les demi-axes des coordonnées positives, des angles dont les cosinus φ, χ, ψ seront déterminés par les équations (14). Supposons d'ailleurs que par le point (x, y, z) de la courbe donnée on mène une droite perpendiculaire au plan osculateur. Cette droite, étant perpendiculaire à la tangente et au rayon de courbure, sera précisément celle qui, prolongée dans un certain sens, forme, avec les demi-axes des x, y, z positives, des angles dont les cosinus a, b, c se déterminent par les formules (5); et si, en nommant θ le module de rotation de cette droite, on représente le rapport inverse de ce module par une longueur r mesurée sur cette même droite dans le sens que nous venons d'indiquer, la longueur r, le rayon de courbure ρ et le rayon

de cambrure τ vérifieront la formule (17), en vertu de laquelle $\frac{1}{\rho}$ et $\frac{1}{r}$ seront les deux côtés d'un triangle rectangle qui aura pour hypoténuse $\frac{1}{\tau}$. Ajoutons que si l'on désigne par ω une longueur mesurée sur la tangente à la courbe donnée, dans le sens suivant lequel se mesure positivement l'arc s, et par $(\widehat{\omega, \tau})$ l'angle que forme cette tangente avec le rayon de cambrure, les longueurs ρ et r seront liées à la longueur τ et à l'angle $(\widehat{\omega, \tau})$ par les équations (16). La formule (17) a été donnée par M. de Saint-Venant (dans le Tome XIX des *Comptes rendus des séances de l'Académie des Sciences*), et, comme il l'a remarqué lui-même, elle se trouve implicitement comprise dans une équation de M. Lancret.

MÉMOIRE SUR QUELQUES PROPRIÉTÉS DES
RÉSULTANTES A DEUX TERMES

I. — *Formules analytiques.*

Considérons deux systèmes de variables dont les unes, en nombre égal à n, soient représentées par les lettres italiques

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

les autres, en pareil nombre, étant représentées par les lettres romaines

(2) $$\mathrm{x}, \quad \mathrm{y}, \quad \mathrm{z}, \quad \ldots.$$

Concevons, d'ailleurs, que l'on range quatre de ces variables sur deux lignes horizontales et en même temps sur deux lignes verticales, en plaçant, dans la première ligne horizontale, deux termes de la suite (1) et, dans la seconde ligne horizontale, les termes correspondants de la suite (2). On obtiendra ainsi un tableau de la forme

(3) $$\begin{cases} x, & y, \\ \mathrm{x}, & \mathrm{y}, \end{cases}$$

et si, après avoir construit, avec les quatre termes de ce tableau, les deux produits

$$x\mathrm{y}, \quad y\mathrm{x},$$

dont chacun a pour facteurs deux variables situées non seulement dans les deux lignes horizontales, mais encore dans les deux lignes verticales, on retranche le second produit du premier, la différence ainsi trouvée, savoir,

$$x\mathrm{y} - y\mathrm{x},$$

sera une *résultante* composée seulement de *deux termes*, l'un positif xy, l'autre négatif $-xy$. Or, les résultantes de cette espèce jouissent de quelques propriétés qui méritent d'être remarquées, et dont l'énoncé fournit diverses propositions que nous allons établir.

THÉORÈME I. — *Soient*

$$u, \quad v$$

deux fonctions homogènes et linéaires des n variables

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

et nommons

$$\mathrm{u}, \quad \mathrm{v}$$

ce que deviennent les fonctions u, v quand on remplace les n variables x, y, z, ... par n autres variables

$$\mathrm{x}, \quad \mathrm{y}, \quad \mathrm{z}, \quad \ldots.$$

La résultante formée avec les quatre termes du tableau

$$\begin{cases} u, & v, \\ \mathrm{u}, & \mathrm{v}, \end{cases} \tag{4}$$

c'est-à-dire la différence

$$uv - \mathrm{u}v,$$

sera une fonction homogène et linéaire des résultantes

$$xy - \mathrm{x}y, \quad xz - \mathrm{x}z, \quad \ldots, \quad yz - \mathrm{y}z, \quad \ldots, \tag{5}$$

dont chacune est fournie par un tableau qui renferme pareillement quatre termes, savoir, deux termes quelconques de la suite

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

écrits au-dessus des termes correspondants de la suite

$$\mathrm{x}, \quad \mathrm{y}, \quad \mathrm{z}, \quad \ldots$$

Démonstration. — Supposons

$$u = Xx + Yy + Zz + \ldots, \qquad v = \mathrm{X}x + \mathrm{Y}y + \mathrm{Z}z + \ldots, \tag{6}$$

$X, Y, Z, \ldots, \mathrm{X}, \mathrm{Y}, \mathrm{Z}, \ldots$ étant deux suites de coefficients constants. Puisque u et v sont ce que deviennent u et v quand aux variables $x, y,$

$z, \ldots$ on substitue les variables x, y, z, ... ; les équations (6) entraîneront les suivantes :

$$\mathrm{u} = X\mathrm{x} + Y\mathrm{y} + Z\mathrm{z} + \ldots, \qquad \mathrm{v} = \mathrm{X}\mathrm{x} + \mathrm{Y}\mathrm{y} + \mathrm{Z}\mathrm{z} + \ldots. \tag{7}$$

Cela posé, on aura identiquement

$$\begin{aligned} uv - \mathrm{u}v = {} & (Xx + Yy + Zz + \ldots)(\mathrm{X}\mathrm{x} + \mathrm{Y}\mathrm{y} + \mathrm{Z}\mathrm{z} + \ldots) \\ & - (X\mathrm{x} + Y\mathrm{y} + Z\mathrm{z} + \ldots)(\mathrm{X}x + \mathrm{Y}y + \mathrm{Z}z + \ldots). \end{aligned} \tag{8}$$

Or, en vertu de l'équation (8), la résultante binome $uv - \mathrm{u}v$ sera évidemment composée de plusieurs parties respectivement proportionnelles aux coefficients $X, Y, Z, \ldots$. D'ailleurs, la partie proportionnelle au coefficient X, étant le produit de ce coefficient par la différence

$$\begin{aligned} xv - \mathrm{x}v &= (\mathrm{X}\mathrm{x} + \mathrm{Y}\mathrm{y} + \mathrm{Z}\mathrm{z} + \ldots)x - (\mathrm{X}x + \mathrm{Y}y + \mathrm{Z}z + \ldots)\mathrm{x} \\ &= \mathrm{Y}(xy - \mathrm{x}y) + \mathrm{Z}(xz - \mathrm{x}z) + \ldots, \end{aligned}$$

sera, ainsi que cette différence elle-même, une fonction homogène et linéaire de plusieurs termes de la suite (5); et l'on pourra en dire autant des diverses parties qui, dans le développement de la résultante $uv - \mathrm{u}v$, seront respectivement proportionnelles aux coefficients Y, Z. Donc cette résultante sera une fonction homogène et linéaire des divers termes de la suite (5).

THÉORÈME II. — *Les mêmes choses étant posées que dans le théorème précédent, écrivons l'une au-dessus de l'autre, non seulement les deux suites de variables*

$$\begin{cases} x, & y, & z, & \ldots, \\ \mathrm{x}, & \mathrm{y}, & \mathrm{z}, & \ldots, \end{cases} \tag{9}$$

mais encore les deux suites de coefficients

$$\begin{cases} X, & Y, & Z, & \ldots, \\ \mathrm{X}, & \mathrm{Y}, & \mathrm{Z}, & \ldots, \end{cases} \tag{10}$$

qui représentent les constantes par lesquelles les variables

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

se trouvent respectivement multipliées : 1° dans la fonction u; 2° dans la

fonction v; et considérons, outre les résultantes

$$(5) \qquad xy - xy, \quad xz - xz, \quad \ldots, \quad yz - yz, \quad \ldots,$$

dont chacune est formée avec quatre termes compris dans deux lignes verticales du tableau (9), *les résultantes semblables*

$$(11) \qquad XY - XY, \quad XZ - XZ, \quad \ldots, \quad YZ - YZ \ldots,$$

qui se déduisent des premières quand on remplace les termes du tableau (9) *par les termes correspondants du tableau* (10). *Il suffira de multiplier chaque terme de la série* (5) *par le terme correspondant de la série* (11), *puis d'ajouter entre eux les divers produits ainsi formés, pour obtenir une somme équivalente au produit de la résultante*

$$uv - uv,$$

en sorte qu'on aura

$$(12) \qquad uv - uv = \Sigma(XY - XY)(xy - xy),$$

le signe Σ *indiquant une somme de termes semblables entre eux.*

Démonstration. — En effet, pour obtenir le coefficient de l'un des termes de la série (5), par exemple du binome

$$xy - xy,$$

dans le développement de l'expression

$$uv - uv,$$

il suffira de chercher le coefficient du produit xy dans le développement du second membre de la formule (8). D'ailleurs, ce dernier coefficient sera évidemment celui que l'on obtiendra si l'on suppose réduits à zéro tous les termes de la série (1), à l'exception du premier x, et tous les termes de la série (2), à l'exception du second y; et, comme, dans cette hypothèse, on aurait

$$u = Xx, \qquad v = Xx,$$
$$u = Yy, \qquad v = Yy,$$

par conséquent

$$uv - uv = (XY - XY)xy,$$

nous devons conclure que, dans le développement général de l'expression

$$uv - uv,$$

le coefficient du binome

$$xy - xy$$

sera

$$XY - XY.$$

Corollaire. — Si, dans la formule (12), on substitue, pour u, v, u, v, leurs valeurs tirées des formules (6), (7), on obtiendra l'équation identique

$$(13) \qquad \begin{aligned} &(Xx + Yy + Zz + \ldots)(\mathrm{X}x + \mathrm{Y}y + \mathrm{Z}z + \ldots) \\ &- (Xx + Yy + Zz + \ldots)(\mathrm{X}x + \mathrm{Y}y + \mathrm{Z}z + \ldots) \\ &= \Sigma(XY - XY)(xy - xy). \end{aligned}$$

Cette équation, qui était déjà connue, comprend évidemment les théorèmes I et II.

THÉORÈME III. — *Soient*

$$(14) \qquad u, \quad v, \quad w, \quad \ldots$$

et

$$(15) \qquad U, \quad V, \quad W, \quad \ldots$$

deux suites composées d'un pareil nombre de termes, dont chacun représente une fonction homogène et linéaire des n variables x, y, z, ... *Soient encore*

$$(16) \qquad \mathrm{u}, \quad \mathrm{v}, \quad \mathrm{w}, \quad \ldots$$

et

$$(17) \qquad \mathrm{U}, \quad \mathrm{V}, \quad \mathrm{W}, \quad \ldots$$

ce que deviennent les deux premières séries quand on remplace les variables x, y, z, ... *par les variables* x, y, z, ... *Concevons, d'ailleurs, que l'on ajoute entre eux les termes de la série* (14) *ou* (16), *respectivement multipliés par les termes correspondants de la série* (15) *ou* (17), *et construisons ainsi les quatre sommes*

$$(18) \qquad \begin{cases} P = Uu + Vv + Ww + \ldots, & Q = \mathrm{U}u + \mathrm{V}v + \mathrm{W}w + \ldots, \\ Q = Uu + Vv + Ww + \ldots, & P = \mathrm{U}u + \mathrm{V}v + \mathrm{W}w + \ldots. \end{cases}$$

La résultante

$$PP - QQ,$$

formée avec ces quatre sommes, dépendra uniquement des binomes qui représentent les divers termes de la série (5), *et sera une fonction de ces binomes, non seulement entière, mais encore homogène et du second degré.*

Démonstration. — Concevons qu'avec les termes des suites (14) et (16), pris quatre à quatre, on forme les résultantes

$$(19) \qquad uv - \mathrm{u}v, \quad uw - \mathrm{u}w, \quad \ldots, \quad vw - \mathrm{v}w, \quad \ldots,$$

et, avec les termes correspondants des suites (15) et (17), les résultantes

$$(20) \qquad UV - \mathrm{U}V, \quad UW - \mathrm{U}W, \quad \ldots, \quad VW - \mathrm{V}W, \quad \ldots.$$

Eu égard au théorème II, il suffira de multiplier chaque terme de la série (19) par le terme correspondant de la série (20) pour obtenir la résultante

$$PP - QQ.$$

On aura donc

$$(21) \qquad PP - QQ = \Sigma(UV - \mathrm{U}V)(uv - \mathrm{u}v),$$

le signe Σ indiquant une somme de termes semblables entre eux. D'ailleurs, en vertu du théorème I, chacun des binomes (19) ou (20) sera une fonction homogène et linéaire des termes de la série (5). Donc tout produit de la forme

$$(UV - \mathrm{U}V)(uv - \mathrm{u}v)$$

sera une fonction de ces mêmes termes, entière, homogène et du second degré, aussi bien que la résultante binome

$$PP - QQ,$$

représentée par une somme de semblables produits.

Corollaire I. — Il est bon d'observer qu'en vertu des formules (18), P sera une fonction des variables $x, y, z, \ldots$, non seulement entière, mais encore homogène et du second degré. De plus, P sera évidemment ce que devient P, et Q ce que devient Q, quand on remplace les variables $x, y, z, \ldots$ par les variables x, y, z, ...

Corollaire II. — Si l'on réduit les fonctions

$$U, \quad V, \quad W, \quad \ldots$$

aux variables

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

les fonctions

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

se réduiront elles-mêmes aux variables

$$\mathrm{x}, \quad \mathrm{y}, \quad \mathrm{z}, \quad \ldots.$$

et la valeur de P, déterminée par la première des formules (18), deviendra

$$P = ux + vy + wz + \ldots.$$

Si d'ailleurs les fonctions linéaires, par lesquelles les variables $x, y, z, \ldots$ se trouvent respectivement multipliées dans cette valeur de P, sont représentées, non plus par diverses lettres

$$u, \quad v, \quad w, \quad \ldots,$$

mais à l'aide de la seule lettre P successivement affectée des indices $x, y, z, \ldots$, c'est-à-dire à l'aide des notations

$$P_x, \quad P_y, \quad P_z, \quad \ldots;$$

et si, pareillement, pour exprimer ce que deviennent ces mêmes fonctions linéaires quand on remplace les variables $x, y, z, \ldots$ par les variables x, y, z, ..., on se sert, non plus des lettres

$$\mathrm{u}, \quad \mathrm{v}, \quad \mathrm{w}, \quad \ldots,$$

mais des notations

$$\mathrm{P}_x, \quad \mathrm{P}_y, \quad \mathrm{P}_z, \quad \ldots;$$

alors, à la place du théorème III, on obtiendra la proposition suivante :

THÉORÈME IV. — *Soient*

$$(22) \qquad P_x, \quad P_y, \quad P_z, \quad \ldots$$

n fonctions homogènes et linéaires de n variables

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

et nommons

$$(23) \qquad \mathrm{P}_x, \quad \mathrm{P}_y, \quad \mathrm{P}_z, \quad \ldots$$

ce que deviennent les fonctions P_x, P_y, P_z, ... *quand on remplace les n variables* $x, y, z, \ldots$ *par n autres variables*

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

Concevons, d'ailleurs, que l'on ajoute entre eux les termes de la suite

$$P_x, \quad P_y, \quad P_z, \quad \ldots,$$

ou de la suite

$$P_x, \quad P_y, \quad P_z, \quad \ldots,$$

respectivement multipliés par les variables

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

ou par les variables

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

et nommons

$$P, \quad Q,$$
$$Q, \quad P,$$

les quatre sommes ainsi obtenues, P *étant celle qui renferme les seules variables* $x, y, z, \ldots$, *et* P *celle qui renferme les seules variables* x, y, z, ..., *en sorte qu'on ait*

$$(24)\quad \begin{cases} P = xP_x + yP_y + zP_z + \ldots, & Q = xP_x + yP_y + zP_z + \ldots, \\ Q = xP_x + yP_y + zP_z + \ldots, & P = xP_x + yP_y + zP_z + \ldots. \end{cases}$$

La résultante

$$PP - QQ,$$

formée avec ces quatre sommes, dépendra uniquement des binomes qui représentent les divers termes de la série (5), *et sera une fonction de ces binomes, non seulement entière, mais encore homogène et du second degré.*

Corollaire I. — Il est bon d'observer qu'en passant du théorème III au théorème IV on obtiendra, au lieu de l'équation (21), la formule

$$(25)\qquad PP - QQ = \Sigma(P_x P_y - P_x P_y)(xy - xy).$$

Supposons maintenant que, *s*, *t* étant deux termes quelconques de la suite

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

et s, t les deux termes correspondants de la suite

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

on désigne par $P_{s,t}$ le coefficient de *t* dans la fonction linéaire P_s. Alors $P_{s,t}$ sera une constante qui représentera encore le coefficient de t dans la fonction linéaire P_s, et la formule (25) pourra s'écrire comme il suit :

$$(26)\qquad PP - QQ = \Sigma(P_s P_t - P_s P_t)(st - st),$$

le signe Σ indiquant une somme de termes semblables entre eux. Comme on aura d'ailleurs

$$(27)\quad \begin{cases} P_s = xP_{s,x} + yP_{s,y} + zP_{s,z} + \ldots, & P_t = xP_{t,x} + yP_{t,y} + zP_{t,z} + \ldots, \\ P_s = xP_{s,x} + yP_{s,y} + zP_{s,z} + \ldots, & P_t = xP_{t,x} + yP_{t,y} + zP_{t,z} + \ldots, \end{cases}$$

il suffira de substituer aux formules (6) et (7) les formules (27), pour obtenir, à la place de l'équation (12), l'équation semblable

$$(28)\qquad P_s P_t - P_s P_t = \Sigma(P_{s,x} P_{t,y} - P_{t,x} P_{s,y})(xy - xy).$$

Cela posé, on tirera de la formule (26), jointe à l'équation (27),

$$(29)\qquad PP - QQ = \Sigma\Sigma(P_{s,x} P_{t,y} - P_{t,x} P_{s,y})(st - st)(xy - xy),$$

les deux signes $\Sigma\Sigma$ indiquant une double somme de termes semblables que l'on obtiendra en remplaçant successivement chacun des binomes

$$st - st, \quad xy - xy$$

par les divers termes de la série (5). Ajoutons qu'en vertu de la première des équations (27), on aura

$$(30)\quad \begin{cases} P_x = xP_{x,x} + yP_{x,y} + zP_{x,z} + \ldots, \\ P_y = xP_{y,x} + yP_{y,y} + zP_{y,z} + \ldots, \\ P_z = xP_{z,x} + yP_{z,y} + zP_{z,z} + \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{cases}$$

et qu'en conséquence la première des formules (24) donnera

$$(31)\quad P = x^2 P_{x,x} + y^2 P_{y,y} + z^2 P_{z,z} + \ldots + xy(P_{x,y} + P_{y,x}) + xz(P_{x,z} + P_{z,x}) + \ldots yz(P_{y,z} + P_{z,y}) + \ldots,$$

tandis que la seconde donnera

$$(32)\quad Q = xxP_{x,x} + yyP_{y,y} + zzP_{z,z} + \ldots + xyP_{x,y} + xyP_{y,x} + xzP_{x,z} + xzP_{z,x} + \ldots + yzP_{y,z} + yzP_{z,y} + \ldots.$$

Au contraire, la quatrième et la troisième des formules (24) donneront

$$(33)\quad \mathrm{P}=\mathrm{x}^2P_{x,x}+\mathrm{y}^2P_{y,y}+\mathrm{z}^2P_{z,z}+\ldots$$
$$+\mathrm{xy}(P_{x,y}+P_{y,x})+\mathrm{xz}(P_{x,z}+P_{z,x})+\ldots+\mathrm{yz}(P_{y,z}+\mathrm{P}_{z,y})+\ldots,$$

$$(34)\quad \mathrm{Q}=x\mathrm{x}P_{x,x}+y\mathrm{y}P_{y,y}+z\mathrm{z}\mathrm{P}_{z,z}+\ldots$$
$$+x\mathrm{y}P_{x,y}+\mathrm{x}yP_{y,x}+x\mathrm{z}P_{x,z}+\mathrm{x}zP_{z,x}+\ldots+y\mathrm{z}P_{y,z}+\mathrm{y}z\mathrm{P}_{z,y}+\ldots.$$

Corollaire II. — Si le coefficient constant de t dans P_s devient généralement égal au coefficient constant de s dans P_t, en sorte qu'on ait

$$(35)\qquad P_{t,s}=P_{s,t},$$

alors les formules (31), (32) donneront

$$(36)\quad P=x^2P_{x,x}+y^2P_{y,y}+z^2P_{z,z}+\ldots$$
$$+2xyP_{x,y}+2xzP_{x,z}+\ldots+2yzP_{y,z}+\ldots$$

et

$$(37)\quad Q=x\mathrm{x}P_{x,x}+y\mathrm{y}P_{y,y}+z\mathrm{z}P_{z,z}+\ldots$$
$$+(x\mathrm{y}+\mathrm{x}y)P_{x,y}+(x\mathrm{z}+\mathrm{x}z)P_{x,z}+\ldots+(y\mathrm{z}+\mathrm{y}z)P_{y,z}+\ldots.$$

D'ailleurs, les valeurs des coefficients

$$P_{x,x},\quad P_{y,y},\quad P_{z,z},\quad \ldots,\quad P_{x,y},\quad P_{x,z},\quad \ldots,\quad P_{y,z},\quad \ldots$$

pouvant être choisies arbitrairement, la fonction P déterminée par la formule (36) pourra être, parmi les fonctions entières de $x, y, z, \ldots$, l'une quelconque de celles qui seront homogènes et du second degré. Quant à la fonction P, elle sera toujours ce que devient P quand on remplace les variables $x, y, z, \ldots$ par les variables x, y, z, ..., en sorte qu'on aura

$$(38)\quad \mathrm{P}=\mathrm{x}^2P_{x,x}+\mathrm{y}^2P_{y,y}+\mathrm{z}^2P_{z,z}+\ldots$$
$$+2\mathrm{xy}P_{x,y}+2\mathrm{xz}P_{x,z}+\ldots+2\mathrm{yz}P_{y,z}+\ldots.$$

Ajoutons que, si l'on désigne par s, t deux quelconques des termes de la suite

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

et par s, t les deux termes correspondants de la suite

$$\mathrm{x},\quad \mathrm{y},\quad \mathrm{z},\quad \ldots,$$

il suffira, pour obtenir la valeur de Q déterminée par l'équation (37),

de remplacer généralement, dans la valeur de P, le carré s^2 d'une variable par le produit $s\mathrm{s}$, et le produit $s\mathrm{t}$ de deux variables par la demi-somme $\frac{s\mathrm{t}+\mathrm{s}t}{2}$. Enfin, comme la valeur de Q ainsi formée ne sera point altérée quand on échangera entre eux les deux systèmes de variables

$$x,\quad y,\quad z,\quad \ldots,$$
$$\mathrm{x},\quad \mathrm{y},\quad \mathrm{z},\quad \ldots,$$

il en résulte qu'on aura, dans l'hypothèse admise,

$$(39)\qquad \mathrm{Q}=Q,$$

et que, par suite, la résultante

$$PP-QQ$$

sera réduite à la forme

$$PP-Q^2.$$

Cela posé, l'équation (29) deviendra

$$(40)\qquad PP-Q^2=\Sigma\Sigma(P_{s,x}P_{t,y}-P_{t,x}P_{s,y})(s\mathrm{t}-\mathrm{s}t)(x\mathrm{y}-\mathrm{x}y),$$

et le théorème IV entraînera évidemment la proposition suivante :

Théorème V. — *Soit P une fonction des n variables*

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

entière, homogène et du second degré. Nommons P *ce que devient P quand on remplace les n variables* $x, y, z, \ldots$ *par n autres variables* x, y, z, ... *Enfin, nommons Q ce que devient P quand on y remplace les carrés*

$$x^2,\quad y^2,\quad z^2,\quad \ldots$$

des variables $x, y, z, \ldots$ *par les produits*

$$x\mathrm{x},\quad y\mathrm{y},\quad z\mathrm{z},\quad \ldots$$

et les produits

$$x\mathrm{y},\quad x\mathrm{z},\quad \ldots,\quad y\mathrm{z},\quad \ldots$$

des variables $x, y, z, \ldots$, *combinées deux à deux, par les demi-sommes*

$$\frac{x\mathrm{y}+\mathrm{x}y}{2},\quad \frac{x\mathrm{z}+\mathrm{x}z}{2},\quad \ldots,\quad \frac{y\mathrm{z}+\mathrm{y}z}{2},\quad \ldots.$$

La différence

$$PP - Q^2$$

dépendra uniquement des binomes

$$xy - xy, \quad xz - xz, \quad \ldots, \quad yz - yz, \quad \ldots,$$

et sera une fonction de ces binomes, non seulement entière, mais encore homogène et du second degré. Ajoutons que si s, t étant deux quelconques des variables

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

on désigne par $P_{s,s}$ le coefficient du carré s^2, et par $2P_{s,t}$ le coefficient du produit st dans la fonction P, on aura non seulement

$$P = x^2 P_{x,x} + y^2 P_{y,y} + z^2 P_{z,z} + \ldots + 2xy P_{x,y} + 2xz P_{x,z} + \ldots + 2yz P_{y,z} + \ldots, \tag{36}$$

mais encore

$$PP - Q^2 = \Sigma\Sigma (P_{s,x} P_{t,y} - P_{t,x} P_{s,y})(st - st)(xy - xy), \tag{40}$$

les deux signes $\Sigma\Sigma$ désignant une double somme de termes semblables, que l'on obtiendra en remplaçant successivement, dans le second membre de la formule (40), chacun des binomes

$$st - st, \quad xy - xy$$

par les divers termes de la suite (5).

Corollaire I. — n étant le nombre des variables $x, y, z, \ldots$, le nombre des termes de la suite (5) sera $\frac{n(n-1)}{2}$, et, en remplaçant successivement chacun des binomes

$$st - st, \quad xy - xy$$

par ces divers termes dans le produit

$$(P_{s,x} P_{t,y} - P_{t,x} P_{s,y})(st - st)(xy - xy), \tag{41}$$

on obtiendra, en tout,

$$\left[\frac{n(n-1)}{2}\right]^2$$

produits dont la somme constituera le second membre de l'équation (40), ou la valeur de la différence $PP - Q^2$. D'ailleurs, lorsque

les deux binomes

$$st - st, \quad xy - xy$$

deviennent égaux, c'est-à-dire lorsqu'on suppose

$$s = x, \qquad t = y,$$

et, en conséquence,

$$s = x, \qquad t = y,$$

le produit (41) se réduit au suivant :

$$(P_{x,x} P_{y,y} - P_{x,y}^2)(xy - xy)^2. \tag{42}$$

Enfin, lorsque les deux binomes

$$st - st, \quad xy - xy$$

restent distincts, le produit (41) est évidemment égal à un autre produit de la même forme, savoir, à celui qu'on obtient quand on échange les deux binomes entre eux. Donc les produits qui représenteront les divers termes de la double somme comprise dans le second membre de l'équation (40) seront de deux espèces, et, parmi ces produits, les uns, en nombre évidemment égal à

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

seront de la forme (42), tandis que les autres, étant de la forme (41) sans être de la forme (42), seront deux à deux égaux entre eux. Ajoutons que le nombre de ces derniers sera évidemment exprimé par la différence

$$\left[\frac{n(n-1)}{2}\right]^2 - \frac{n(n-1)}{2}; \tag{43}$$

de sorte qu'en représentant ce nombre par $2N$, on aura

$$N = \frac{(n-2)(n-1)n(n+1)}{8}. \tag{44}$$

Corollaire II. — Pour montrer une application du théorème V, supposons que les variables x, y soient réduites à deux, et qu'en conséquence la fonction P soit de la forme

$$P = ax^2 + by^2 + 2cxy, \tag{45}$$

a, b, c étant des coefficients constants. Alors on aura

$$n=2, \qquad \frac{n(n-1)}{2}=1, \qquad N=0;$$

et, comme la suite (5) ne renfermera plus qu'un seul terme, l'équation (40) se trouvera réduite à

$$PP-Q^2=(P_{x,x}P_{y,y}-P_{x,y}^2)(x\mathrm{y}-\mathrm{x}y)^2. \tag{46}$$

Comme on aura d'ailleurs, dans cette hypothèse,

$$P_{x,x}=a, \qquad P_{y,y}=b, \qquad P_{x,y}=c,$$

l'équation (46) donnera

$$PP-Q^2=(ab-c^2)(x\mathrm{y}-\mathrm{x}y)^2. \tag{47}$$

En substituant, dans la formule (47), aux fonctions P, P, Q leurs valeurs déduites de la formule (45) à l'aide des règles indiquées dans l'énoncé du théorème V, on obtiendra l'équation identique

$$\left\{\begin{array}{l}(ax^2+by^2+2cxy)(a\mathrm{x}^2+b\mathrm{y}^2+2c\mathrm{xy})-[ax\mathrm{x}+by\mathrm{y}+c(x\mathrm{y}+\mathrm{x}y)]^2\\ \qquad=(ab-c^2)(x\mathrm{y}-\mathrm{x}y)^2,\end{array}\right. \tag{48}$$

qui a été donnée par Lagrange dans les *Mémoires de Berlin* de 1773.

Corollaire III. — Supposons maintenant que les variables x, y, z, ... soient au nombre de 3, et qu'en conséquence la fonction P soit de la forme

$$P=ax^2+by^2+cz^2+2dyz+2ezx+2fxy, \tag{49}$$

a, b, c, d, e, f désignant des coefficients constants. Alors on aura

$$n=3, \qquad \frac{n(n-1)}{2}=3, \qquad N=3;$$

et si l'on pose, pour abréger,

$$\mathfrak{X}=y\mathrm{z}-\mathrm{y}z, \qquad \mathfrak{Y}=z\mathrm{x}-\mathrm{z}x, \qquad \mathfrak{Z}=x\mathrm{y}-\mathrm{x}y, \tag{50}$$

les termes de la série (5) se réduiront, abstraction faite des signes, aux trois binomes désignés ici par les trois lettres $\mathfrak{X}$, $\mathfrak{Y}$, $\mathfrak{Z}$. Cela posé, la formule (40) donnera

$$PP-Q^2=A\mathfrak{X}^2+B\mathfrak{Y}^2+C\mathfrak{Z}^2+2D\mathfrak{Y}\mathfrak{Z}+2E\mathfrak{Z}\mathfrak{X}+2F\mathfrak{X}\mathfrak{Y}, \tag{51}$$

A, B, C, D, E, F étant des constantes déterminées par les équations

$$\left\{\begin{array}{ll}A=P_{y,y}P_{z,z}-P_{y,z}^2, & D=P_{z,x}P_{x,y}-P_{x,x}P_{y,z},\\ B=P_{z,z}P_{x,x}-P_{z,x}^2, & E=P_{x,y}P_{y,z}-P_{y,y}P_{z,x},\\ C=P_{x,x}P_{y,y}-P_{x,y}^2, & F=P_{y,z}P_{z,x}-P_{z,z}P_{x,y}.\end{array}\right. \tag{52}$$

Comme on aura d'ailleurs

$$P_{x,x}=a, \qquad P_{y,y}=b, \qquad P_{z,z}=c,$$
$$P_{y,z}=d, \qquad P_{z,x}=e, \qquad P_{x,y}=f,$$

les équations (52) donneront

$$\left\{\begin{array}{lll}A=bc-d^2, & B=ca-e^2, & C=ab-f^2,\\ D=ef-ad, & E=fd-be, & F=de-cf.\end{array}\right. \tag{53}$$

Enfin, si, dans la formule (51), on substitue aux fonctions P, P, Q leurs valeurs déduites de la formule (49) à l'aide des règles indiquées dans l'énoncé du premier théorème, on obtiendra l'équation identique

$$\begin{aligned}&(ax^2+by^2+cz^2+2dyz+2ezx+2fxy)\\ &\quad\times(a\mathrm{x}^2+b\mathrm{y}^2+c\mathrm{z}^2+2d\mathrm{yz}+2e\mathrm{zx}+2f\mathrm{xy})\\ &\quad-[ax\mathrm{x}+by\mathrm{y}+cz\mathrm{z}+d(y\mathrm{z}+\mathrm{y}z)+e(z\mathrm{x}+\mathrm{z}x)+f(x\mathrm{y}+\mathrm{x}y)]^2\\ &=A\mathfrak{X}^2+B\mathfrak{Y}^2+C\mathfrak{Z}^2+2D\mathfrak{Y}\mathfrak{Z}+2E\mathfrak{Z}\mathfrak{X}+2F\mathfrak{X}\mathfrak{Y},\end{aligned} \tag{54}$$

que l'on pourrait déduire de l'une des formules données par M. Binet dans le XVI^e^ cahier du *Journal de l'École Polytechnique*.

Corollaire IV. — Il est bon d'observer que les coefficients constants

$$P_{x,x}, \quad P_{y,y}, \quad P_{z,z}, \quad \ldots, \quad P_{x,y}, \quad P_{x,z}, \quad \ldots, \quad P_{y,z}, \quad \ldots,$$

renfermés dans les seconds membres des formules (36) et (40), sont précisément les moitiés des dérivées du second ordre de la fonction P. En effet, de l'équation (36), différentiée deux fois de suite par rapport à une même variable, ou par rapport à deux variables distinctes, on déduit immédiatement les formules

$$\left\{\begin{array}{llll}P_{x,x}=\frac{1}{2}\mathrm{D}_x^2P, & P_{y,y}=\frac{1}{2}\mathrm{D}_y^2P, & P_{z,z}=\frac{1}{2}\mathrm{D}_z^2P, & \ldots,\\ P_{x,y}=\frac{1}{2}\mathrm{D}_x\mathrm{D}_yP, & P_{x,z}=\frac{1}{2}\mathrm{D}_x\mathrm{D}_zP, & P_{y,z}=\frac{1}{2}\mathrm{D}_y\mathrm{D}_zP, & \ldots,\end{array}\right. \tag{55}$$

toutes comprises dans la formule générale

$$P_{x,t} = \frac{1}{2} D_x D_t P, \tag{56}$$

qui subsiste dans le cas même où l'on suppose $t = s$. Ajoutons encore qu'en vertu des équations (55), la formule (36) donnera

$$\begin{aligned} 2P = {} & x^2 D_x^2 P + y^2 D_y^2 P + z^2 D_z^2 P + \dots \\ & + 2xy D_x D_y P + 2xz D_x D_z P + \dots + 2yz D_y D_z P + \dots . \end{aligned} \tag{57}$$

Au reste, l'équation (57) peut se déduire immédiatement du théorème des fonctions homogènes. Effectivement, en vertu de ce théorème, la fonction P, étant homogène et du second degré par rapport aux variables $x, y, z, \dots$, vérifiera la formule

$$2P = x D_x P + y D_y P + z D_z P + \dots ; \tag{58}$$

tandis que les fonctions $D_x P$, $D_y P$, $D_z P$, ..., étant homogènes et du premier degré, vérifieront les formules

$$\left\{ \begin{array}{l} D_x P = x D_x^2 P + y D_y D_x P + z D_z D_x P + \dots , \\ D_y P = x D_x D_y P + y D_y^2 P + z D_z D_y P + \dots , \\ D_z P = x D_x D_z P + y D_y D_z P + z D_z^2 P + \dots , \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \end{array} \right. \tag{59}$$

et il est clair qu'en substituant dans l'équation (58) les valeurs de

$$D_x P, \quad D_y P, \quad D_z P, \quad \dots ,$$

fournies par les équations (59), on retrouvera la formule (57). Observons enfin que les équations (30), jointes aux formules (55), donneront

$$P_x = \frac{1}{2}(x D_x^2 P + y D_y D_x P + z D_z D_x P + \dots),$$

$$P_y = \frac{1}{2}(x D_x D_y P + y D_y^2 P + z D_z D_y P + \dots),$$

$$P_z = \frac{1}{2}(x D_x D_z P + y D_y D_z P + z D_z^2 P + \dots),$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

Donc, eu égard aux formules (59), on aura

$$P_x = \frac{1}{2} D_x P, \qquad P_y = \frac{1}{2} D_y P, \qquad P_z = \frac{1}{2} D_z P, \qquad \dots . \tag{60}$$

Ainsi, dans l'hypothèse qui nous a conduits au théorème V, les fonctions précédemment représentées par les notations

$$P_x, \quad P_y, \quad P_z, \quad \dots ,$$

se réduisent aux moitiés des fonctions dérivées

$$D_x P, \quad D_y P, \quad D_z P, \quad \dots .$$

II. — *Interprétations géométriques de plusieurs formules établies dans le premier paragraphe.*

Plusieurs des formules établies dans le paragraphe I admettent des interprétations géométriques qui méritent d'être remarquées et que nous allons indiquer.

Supposons d'abord que la suite

$$x, \quad y, \quad z, \quad \dots$$

renferme seulement deux variables x, y, et concevons que ces deux variables représentent les coordonnées d'un point mobile. La distance r de ce point à l'origine sera déterminée par la formule

$$r = \sqrt{x^2 + y^2}.$$

Supposons d'ailleurs que a, b, c, k étant des quantités constantes, le point mobile (x, y) soit assujetti à rester sur une courbe du second degré représentée par l'équation

$$ax^2 + by^2 + 2cxy = k. \tag{1}$$

Cette courbe sera une ellipse ou une hyperbole, qui aura pour centre l'origine des coordonnées; elle sera une ellipse si l'on a

$$ab - c^2 > 0, \quad k > 0.$$

Elle sera une hyperbole si l'on a

$$ab - c^2 < 0;$$

et, dans cette dernière hypothèse, il suffira de changer le signe du second membre de la formule (1) pour obtenir l'équation

$$ax^2 + by^2 + 2cxy = -k \tag{2}$$

d'une seconde hyperbole conjuguée à la première, deux *hyperboles conjuguées* étant celles qui, avec le même centre et les mêmes asymptotes, offrent des axes réels respectivement égaux et parallèles aux deux côtés d'un rectangle dont les diagonales sont dirigées suivant ces asymptotes.

Concevons à présent que par le point (x, y) on mène une tangente à la courbe représentée par l'équation (1) ou (2), et nommons

$$\xi, \quad \eta$$

les coordonnées courantes de cette tangente. On aura

$$(ax + cy)(\xi - x) + (cx + by)(\eta - y) = 0, \tag{3}$$

et par suite, eu égard à l'équation (1),

$$ax\xi + by\eta + c(x\eta + \xi y) = k, \tag{4}$$

ou, eu égard à l'équation (2),

$$ax\xi + by\eta + c(x\eta + \xi y) = -k. \tag{5}$$

Ajoutons que, pour obtenir l'équation de la parallèle menée à cette tangente par l'origine des coordonnées, il suffira de remplacer k par zéro dans la formule (4) ou (5). L'équation de cette parallèle sera donc de la forme

$$ax\xi + by\eta + c(x\eta + \xi y) = 0. \tag{6}$$

Soient maintenant

$$x, \quad y$$

les coordonnées d'un nouveau point situé sur l'ellipse représentée par l'équation (1) ou sur l'une des hyperboles conjuguées représentées par les équations (1) et (2). On aura encore

$$ax^2 + by^2 + 2cxy = k, \tag{7}$$

ou

$$ax^2 + by^2 + 2cxy = -k. \tag{8}$$

Soit d'ailleurs s le rayon mené de l'origine au point (x, y), en sorte qu'on ait

$$s = \sqrt{x^2 + y^2}. \tag{9}$$

Si ce rayon est parallèle à la tangente menée par le point (x, y) à la courbe (1), on vérifiera l'équation (6) en posant

$$\xi = x, \quad \eta = y.$$

On aura donc alors

$$axx + byy + c(xy + xy) = 0. \tag{10}$$

Si, au contraire, le rayon s n'est pas parallèle à la tangente dont il s'agit, il suffira de le prolonger indéfiniment dans les deux sens pour qu'il rencontre cette tangente en un certain point dont les coordonnées ξ, η vérifieront l'équation (4), et dont la distance à l'origine sera une longueur ς déterminée par la formule

$$\varsigma = \sqrt{\xi^2 + \eta^2}. \tag{11}$$

Mais alors, en posant, pour abréger,

$$\vartheta = \frac{s}{\varsigma}, \tag{12}$$

on aura nécessairement

$$\frac{\xi}{x} = \frac{\eta}{y} = \pm\frac{s}{\varsigma} = \pm\vartheta, \tag{13}$$

le double signe $\pm$ devant être réduit au signe $+$ ou au signe $-$, suivant que les deux longueurs s, ς se compteront, à partir de l'origine, dans le même sens ou dans des sens opposés. Or, de l'équation (13), réduite à la forme

$$\frac{\xi}{x} = \frac{\eta}{y} = \pm\frac{1}{\vartheta},$$

et combinée avec l'équation (4), on tire

$$axx + byy + c(xy + xy) = \pm\vartheta k, \tag{14}$$

par conséquent,

$$\vartheta = \pm\frac{axx + byy + c(xy + xy)}{k}. \tag{15}$$

On peut donc énoncer la proposition suivante :

THÉORÈME I. — *Soient r, s deux rayons menés de l'origine des coordonnées supposées rectangulaires, le premier à la courbe représentée par*

l'équation (1), *le second à l'une des courbes représentées par les équations* (1) *et* (2). *Soit, de plus,* ς *la longueur mesurée, à partir de l'origine, sur le rayon s indéfiniment prolongé dans les deux sens, jusqu'à la tangente menée à la courbe* (1) *par l'extrémité du rayon r. Enfin nommons x, y les coordonnées de l'extrémité du rayon r, et* x, y *les coordonnées de l'extrémité du rayon s. Les deux longueurs s et* ς *seront dirigées, à partir de l'origine, dans le même sens ou dans deux sens opposés, suivant que la quantité*

$$\frac{axx + byy + c(xy + xy)}{k}$$

sera positive ou négative, et la valeur numérique de cette quantité sera précisément la valeur du rapport

$$\theta = \frac{s}{\varsigma}.$$

Corollaire I. — Lorsque la tangente menée par le point (x, y) à la courbe (1) est parallèle au rayon s, la longueur représentée par ς devient infinie. On a donc alors $\theta = 0$, et, par suite, l'équation (15) se réduit, comme on devait s'y attendre, à la formule (10).

Corollaire II. — Concevons à présent que, par l'extrémité du rayon s, c'est-à-dire par le point (x, y), on mène une tangente à la courbe (1) ou (2), sur laquelle est situé ce même point; et nommons ρ la longueur mesurée, à partir de l'origine, sur le rayon r indéfiniment prolongé, dans les deux sens, jusqu'à la tangente dont il s'agit. Alors, en posant

$$\theta = \frac{r}{\rho}, \tag{16}$$

on prouvera, comme ci-dessus, que θ se réduit à la valeur numérique de la quantité

$$\frac{axx + byy + c(xy + xy)}{k}.$$

Donc les valeurs de θ fournies par les équations (12) et (16) seront égales entre elles, et l'on aura

$$\frac{s}{\varsigma} = \frac{r}{\rho}, \tag{17}$$

en sorte que les *deux longueurs* ρ, ς *seront respectivement proportionnelles aux deux longueurs r, s.* Cette dernière proposition peut être considérée comme offrant une interprétation géométrique de la formule (39) du paragraphe I, et, comme cette formule, elle exprime la propriété qu'a la fonction

$$axx + byy + c(xy + xy)$$

de n'être pas altérée quand on échange entre eux les deux systèmes de variables

$$x, \quad y,$$
$$x, \quad y.$$

Corollaire III. — Supposons maintenant que le rayon s aboutisse, comme le rayon r, à la courbe représentée par l'équation (1). Alors, non seulement les longueurs ρ et ς seront respectivement proportionnelles aux longueurs r et s, mais, de plus, ces quatre longueurs étant comptées à partir de l'origine, ρ se mesurera dans le sens de r, et ς dans le sens de s, si la quantité

$$\frac{axx + byy + c(xy + xy)}{k}$$

est positive. Au contraire, si cette quantité devient négative, la direction de ρ sera opposée à celle de r, et la direction de ς opposée à celle de s. Donc, par suite, les longueurs r, s, d'une part, et les longueurs ρ, ς, d'autre part, représenteront des côtés homologues de deux triangles semblables dont les bases seront parallèles. On peut donc énoncer encore la proposition suivante :

THÉORÈME II. — *Soient*

$$r, \quad s$$

deux rayons menés du centre d'une ellipse ou d'une hyperbole à deux points de cette courbe. Soient encore

$$\rho, \quad \varsigma$$

deux longueurs mesurées depuis le centre de la courbe : 1° *sur le rayon r indéfiniment prolongé jusqu'à la tangente menée par l'extrémité du*

rayon s; 2° *sur le rayon s indéfiniment prolongé jusqu'à la tangente menée par l'extrémité du rayon r. Les deux longueurs* ρ, ζ *seront respectivement proportionnelles aux deux longueurs r, s, et la droite qui joindra les extrémités des deux longueurs* ρ, ζ *sera parallèle à la droite qui joindra les extrémités des deux longueurs r, s.*

Corollaire I. — Le théorème précédent est l'un de ceux auxquels on se trouve conduit par les propriétés connues des diamètres conjugués de l'ellipse et de l'hyperbole. D'ailleurs, ce théorème devient évident quand la courbe proposée se réduit à un cercle; et, du cas où la courbe est un cercle, on passe facilement au cas où la courbe est une ellipse, en observant que toute ellipse peut être considérée comme la projection orthogonale d'un cercle dont un diamètre est égal et parallèle au grand axe de l'ellipse, et dont le plan forme, avec le plan de l'ellipse, un angle qui a pour cosinus le rapport du petit axe au grand axe.

Corollaire II. — Le théorème II fournit un moyen très simple de mener, par un point donné P d'une ellipse ou d'une hyperbole, une tangente à cette courbe. En effet, soit r le rayon mené du centre de la courbe au point donné, et faisons coïncider le rayon s avec l'un des demi-axes de l'ellipse, ou avec un demi-axe réel de l'hyperbole. L'extrémité S du rayon s sera un sommet de la courbe, et la tangente menée à la courbe par ce sommet sera perpendiculaire au rayon s. Nommez R le point où cette tangente rencontrera le rayon r indéfiniment prolongé; par ce point R, menez une parallèle RT à la droite PS, qui joint le point donné P au sommet S; et soit T le point où le rayon s, indéfiniment prolongé, rencontrera la droite RT. La tangente menée à la courbe par le point donné P devra passer par le point T, ce qui permettra de la construire immédiatement.

Corollaire III. — Si le centre de la courbe proposée s'éloigne à une distance infinie de l'origine des coordonnées, cette courbe se transformera en une parabole, et les droites sur lesquelles se mesuraient les rayons r, s, en deux droites parallèles à l'axe de la parabole. Donc, pour mener une tangente à une parabole en un point donné P, il suffit de mener, par le sommet S de la parabole et par le point P, deux droites, l'une perpendiculaire, l'autre parallèle à l'axe de la parabole, de mener par le point R, où ces deux droites se coupent, une parallèle RT à la droite PS, puis de joindre le point T, où la droite RT rencontre l'axe de la parabole, avec le point P. En opérant ainsi, on obtient pour ST une longueur égale à la projection de la distance PS sur l'axe de la parabole, ce qui devait être, attendu que, dans le cas où, en supposant les coordonnées rectangulaires, on prend le sommet S pour origine, et l'axe de la parabole pour axe des abscisses, l'abscisse du point P est tout à la fois la projection de PS sur l'aire de la parabole et la moitié de la sous-tangente correspondante au point P.

Concevons maintenant que l'on combine l'équation (14), jointe à la formule (7) ou (8), avec l'équation identique

$$(18)\quad (ax^2+by^2+2cxy)(ax^2+by^2+2cxy)-[axx+byy+c(xy+xy)]^2 = (ab-c^2)(xy-xy)^2,$$

déjà obtenue dans le paragraphe I. On trouvera ainsi

$$\pm k^2-b^2k^2=(ab-c^2)(xy-xy)^2,$$

et en posant, pour abréger,

$$(19)\qquad K=\frac{k^2}{ab-c^2},$$

on aura simplement

$$(20)\qquad \pm 1-b^2=\frac{(xy-xy)^2}{K},$$

le signe $\pm$ devant être réduit au signe + ou au signe −, suivant que le point (x, y) sera situé sur la courbe représentée par l'équation (1), ou sur la courbe représentée par l'équation (2), c'est-à-dire, en d'autres termes, suivant que les deux rayons r, s aboutiront à une même courbe ou à deux courbes distinctes.

D'autre part, si l'on nomme δ l'angle $\left(\widehat{r,s}\right)$ compris entre les directions des deux rayons r et s, on aura, en vertu d'une formule connue,

$$(21)\qquad xy-xy=\pm rs\sin\delta.$$

Donc la formule (20) donnera

$$\pm 1 - \gamma^2 = \frac{r^2 s^2 \sin^2\delta}{K}. \tag{22}$$

Il reste à savoir ce qu'exprime, dans la formule (22), la constante K, dont la valeur est fournie par l'équation (19). Or, on peut facilement résoudre cette question, à l'aide de l'équation (22) elle-même, en présentant cette équation sous la forme

$$K = \frac{r^2 s^2 \sin^2\delta}{\pm 1 - \gamma^2}, \tag{23}$$

ou, ce qui revient au même, puisque l'on a

$$\gamma = \frac{s}{\varsigma},$$

sous la forme

$$K = \frac{r^2 \varsigma^2 \sin^2\delta}{\pm \frac{\varsigma^2}{s^2} - 1}, \tag{24}$$

et en attribuant aux rayons r, s des valeurs déterminées. En effet, supposons d'abord que la courbe représentée par l'équation (1) soit une ellipse, et nommons a, b les deux demi-axes de cette ellipse. Alors, en posant

$$r = a, \qquad s = b,$$

on aura

$$\delta = (\widehat{r, s}) = \frac{\pi}{2}, \qquad \sin\delta = 1, \qquad \varsigma = \infty,$$
$$rs\sin\delta = ab, \qquad \gamma = 0,$$

et, par suite, l'équation (23), dans laquelle on devra réduire le double signe $\pm$ au signe $+$, donnera

$$K = a^2 b^2. \tag{25}$$

Supposons, en second lieu, que l'équation (1) représente une hyperbole, et nommons a le demi-axe réel de cette hyperbole, b étant le demi-axe réel de l'hyperbole conjuguée. Alors il suffira de poser

$$r = a, \qquad s = \infty,$$

pour que la direction du rayon s se réduise à la direction de l'une des

asymptotes de l'hyperbole (1), et pour que ς représente la longueur mesurée sur cette asymptote entre le centre de l'hyperbole et la tangente menée à cette courbe par l'un des sommets. Mais la portion de la tangente comprise entre ce sommet et l'asymptote sera précisément le demi-axe réel b de l'hyperbole conjuguée à celle que l'on considère, et cette portion aura pour mesure le produit

$$\varsigma \sin(\widehat{r, s}) = \varsigma \sin\delta.$$

Donc, en posant

$$r = a, \qquad s = \infty,$$

on aura nécessairement

$$\varsigma \sin\delta = b,$$

et, par suite, on réduira l'équation (24) à la formule

$$K = -a^2 b^2. \tag{26}$$

Les équations (25) et (26) peuvent aussi être démontrées directement avec la plus grande facilité. En effet, lorsque la courbe représentée par l'équation (1) est une ellipse, ses demi-axes a et b sont les valeurs *maximum* et *minimum* du rayon r déterminé à l'aide de cette équation, jointe à la formule

$$r^2 = x^2 + y^2, \tag{27}$$

et, par suite, ils se confondent avec les deux valeurs de r fournies par le système des deux équations

$$(a - u)(b - u) - c^2 = 0, \tag{28}$$

$$u = \frac{k}{r^2}. \tag{29}$$

Donc alors l'équation (28), que l'on peut réduire à la forme

$$u^2 - (a + b)u + ab - c^2 = 0, \tag{30}$$

étant résolue par rapport à u, offrira pour racines les deux rapports

$$\frac{k}{a^2}, \quad \frac{k}{b^2},$$

et le produit de ces rapports sera équivalent à la constante $ab - c^2$, en

sorte qu'on aura

$$\frac{k^2}{a^2b^2} = ab - c^2,$$

et, par suite,

$$\frac{k^2}{ab - c^2} = a^2b^2,$$

ou, ce qui revient au même,

$$K = a^2b^2.$$

Si, au contraire, la courbe représentée par l'équation (1) est une hyperbole, le demi-axe réel a ou b de cette hyperbole ou de l'hyperbole conjuguée sera la valeur *maximum* de r déduite de la formule (27), jointe à l'équation (1) ou (2). Donc alors a ou b sera la valeur réelle et positive de r, qui se déduira de l'équation (28), jointe à la formule (29) ou à la suivante :

$$u = -\frac{k}{r^2}. \tag{31}$$

Donc, par suite,

$$\frac{k}{a^2} \quad \text{et} \quad -\frac{k}{b^2}$$

seront les deux racines de l'équation (27), et l'on aura

$$-\frac{k^2}{a^2b^2} = ab - c^2,$$

et

$$\frac{k^2}{ab - c^2} = -a^2b^2,$$

ou, ce qui revient au même,

$$K = -a^2b^2.$$

En résumé, si la courbe représentée par l'équation (1) est une ellipse, la valeur de K sera déterminée par la formule (25), et, en conséquence, l'équation (22), dans laquelle on devra réduire le double signe $\pm$ au signe $+$, donnera

$$1 - \theta^2 = \Theta^2, \tag{32}$$

la valeur de Θ étant

$$\Theta = \frac{rs\sin\delta}{ab}. \tag{33}$$

Au contraire, si la courbe représentée par l'équation (1) est une hyperbole, la valeur de K sera déterminée par la formule (26); et, en conséquence, l'équation (22) donnera

$$\theta^2 \mp 1 = \Theta^2, \tag{34}$$

la valeur de Θ étant toujours déterminée par la formule (1), et le double signe $\mp$ devant être réduit au signe $-$ ou au signe $+$, suivant que l'extrémité du rayon s sera située sur l'hyperbole (1) ou sur l'hyperbole (2).

Il importe d'observer que le produit

$$rs\sin\delta = rs\sin\left(\widehat{r, s}\right)$$

représente l'aire du parallélogramme construit sur les rayons r, s, tandis que le produit

$$ab$$

représente l'aire du rectangle construit sur les demi-axes a, b. Cela posé, la quantité désignée par Θ, dans l'équation (33), représentera évidemment le rapport de ces deux aires, et les formules (32), (34) entraîneront les propositions suivantes :

THÉORÈME III. — *Soient :*

a, b *les deux demi-axes d'une ellipse ;*

r, s *deux rayons menés du centre de l'ellipse à deux points de cette courbe ;*

$\delta = \left(\widehat{r, s}\right)$ *l'angle compris entre ces rayons ;*

ς *une longueur mesurée sur le rayon s entre le centre de l'ellipse et la tangente menée à cette courbe par l'extrémité du rayon r ;*

enfin posons

$$\theta = \frac{s}{\varsigma} \quad \text{et} \quad \Theta = \frac{rs\sin\delta}{ab},$$

en sorte que Θ représente le quotient qu'on obtient quand on divise l'aire du parallélogramme construit sur les rayons r et s par l'aire du rectangle construit sur les demi-axes a *et* b. *Les deux rapports θ, Θ vérifieront la*

formule

$$\theta^2 + \Theta^2 = 1, \tag{35}$$

Théorème IV. — *Soient :*

a *le demi-axe réel d'une certaine hyperbole ;*

b *le demi-axe réel d'une seconde hyperbole conjuguée à la première ;*

r *un rayon mené du centre commun des deux hyperboles à un point de la première ;*

s *un rayon mené du même centre à un nouveau point de la première hyperbole, ou à un point quelconque de la seconde ;*

$\delta = (\widehat{r, s})$ *l'angle compris entre les rayons r, s ;*

ς *une longueur mesurée sur le rayon s entre le centre commun des deux hyperboles et la tangente menée à la première par l'extrémité du rayon r ;*

enfin posons

$$\theta = \frac{s}{\varsigma}, \qquad \Theta = \frac{rs\sin\delta}{ab},$$

en sorte que Θ *représente le quotient qu'on obtient quand on divise l'aire du parallélogramme construit sur les rayons r et s par l'aire du rectangle construit sur les demi-axes* a *et* b. *Les deux rapports* θ, Θ *vérifieront la formule*

$$\theta^2 - \Theta^2 = \pm 1, \tag{36}$$

le signe ± *devant être réduit au signe* + *ou au signe* −, *suivant que le rayon vecteur s aura pour extrémité un point situé sur la première ou sur la seconde hyperbole.*

Lorsque le rayon *s* devient parallèle à la tangente menée par l'extrémité du rayon *r*, on a évidemment

$$\varsigma = \infty, \qquad \theta = 0,$$

et l'on tire de la formule (35) ou de la formule (36), dans laquelle le signe ± se trouve réduit au signe −,

$$\Theta^2 = 1, \qquad \Theta = 1,$$

par conséquent,

$$rs\sin\delta = ab. \tag{37}$$

Mais alors les rayons *r*, *s*, qui offrent pour extrémités deux points d'une même ellipse ou de deux hyperboles conjuguées, sont deux *rayons conjugués*, c'est-à-dire les moitiés de deux *diamètres conjugués* de l'ellipse ou des deux hyperboles ; et l'équation (37), présentée sous la forme

$$4rs\sin\delta = 4ab,$$

exprime une proposition bien connue, savoir, que *l'aire du parallélogramme construit sur les diamètres conjugués* 2*r*, 2*s*, *est équivalente à l'aire du rectangle construit sur les axes* 2a, 2b.

On pourrait encore déduire des théorèmes III et IV diverses propositions relatives à l'ellipse ou à l'hyperbole, dont quelques-unes semblent dignes d'attention. Nous citerons comme exemples les deux suivantes :

Théorème V. — *Soient, dans une ellipse,*

a, b *les deux demi-axes ;*

s, *t deux rayons conjugués ;*

r un rayon quelconque ;

δ, ε *les angles* $(\widehat{r, s})$, $(\widehat{r, t})$, *que forme le rayon r avec les deux rayons s et t.*

On aura

$$r^2(s^2\sin^2\delta + t^2\sin^2\varepsilon) = a^2b^2. \tag{38}$$

Démonstration. — Soient

$$\rho, \quad \rho'$$

les longueurs mesurées, sur la direction du rayon *r*, à partir du centre de l'ellipse jusqu'aux deux tangentes menées à cette courbe par les extrémités des rayons *s* et *t*. On aura, en vertu du théorème III,

$$\frac{r^2s^2\sin^2\delta}{a^2b^2} = 1 - \frac{r^2}{\rho^2}, \qquad \frac{r^2t^2\sin^2\varepsilon}{a^2b^2} = 1 - \frac{r^2}{\rho'^2}. \tag{39}$$

Mais, d'après une proposition établie dans les *Exercices de Mathématiques* (III^e volume, page 50 (1)), on aura aussi

$$\frac{1}{\rho^2}+\frac{1}{\rho'^2}=\frac{1}{r^2}, \tag{40}$$

par conséquent,

$$\frac{r^2}{\rho^2}+\frac{r^2}{\rho'^2}=1.$$

Donc les formules (39), combinées l'une avec l'autre par voie d'addition, produiront la suivante

$$\frac{r^2(s^2\sin^2\delta+t^2\sin^2\varepsilon}{a^2b^2}=1,$$

qui coïncide avec l'équation (38).

THÉORÈME VI. — *Soient :*

a *le demi-axe réel d'une première hyperbole ;*

b *le demi-axe réel d'une seconde hyperbole conjuguée à la première ;*

s, t *deux rayons conjugués de la première et de la seconde hyperbole ;*

r *un rayon quelconque de la première hyperbole ;*

δ, ε *les angles* $(\widehat{r,s})$, $(\widehat{r,t})$ *que forme le rayon r avec les deux rayons s et t.*

On aura

$$r^2(t^2\sin^2\varepsilon-s^2\sin^2\delta)=a^2b^2. \tag{41}$$

Démonstration. — Soient

$$\rho,\quad \rho'$$

les longueurs mesurées, sur la direction du rayon r, à partir du centre commun des deux hyperboles jusqu'aux deux tangentes menées à ces courbes par les extrémités des rayons s et t. On aura, en vertu du théorème IV,

$$\frac{r^2s^2\sin^2\delta}{a^2b^2}=\frac{r^2}{\rho^2}-1,\qquad \frac{r^2t^2\sin^2\varepsilon}{a^2b^2}=\frac{r^2}{\rho'^2}+1. \tag{42}$$

Mais, d'après une proposition établie dans les *Exercices de Mathématiques* (III^e volume, page 52) (1), on aura aussi

$$\frac{1}{\rho^2}-\frac{1}{\rho'^2}=\frac{1}{r^2}, \tag{43}$$

par conséquent,

$$\frac{r^2}{\rho^2}-\frac{r^2}{\rho'^2}=1.$$

Donc les formules (42), combinées l'une avec l'autre par voie de soustraction, produiront la suivante

$$\frac{r^2(t^2\sin^2\varepsilon-s^2\sin^2\delta)}{a^2b^2}=1,$$

qui coïncide avec l'équation (41).

Si, dans l'équation (38), on fait coïncider le rayon r avec le demi-axe a, alors, en nommant μ, ν les angles formés avec ce demi-axe par les rayons conjugués s, t, on trouvera

$$s^2\sin^2\mu+t^2\sin^2\nu=b^2. \tag{44}$$

Si, au contraire, on fait coïncider le rayon vecteur r avec le demi-axe b, perpendiculaire au demi-axe a, les valeurs numériques de

$$\sin\delta,\quad \sin\varepsilon$$

se réduiront évidemment aux valeurs numériques de

$$\cos\mu,\quad \cos\nu.$$

Par conséquent, on trouvera

$$s^2\cos^2\mu+t^2\cos^2\nu=a^2, \tag{45}$$

puis on tirera des formules (44), (45), combinées l'une avec l'autre par voie d'addition,

$$s^2+t^2=a^2+b^2. \tag{46}$$

Si, dans l'équation (41), on fait coïncider le rayon r avec le demi-axe réel a, alors, en nommant μ, ν les angles formés avec ce demi-axe par les rayons conjugués s, t, on trouvera

$$t^2\sin^2\nu-s^2\sin^2\mu=b^2. \tag{47}$$

(1) *Œuvres de Cauchy*, série II, t. VIII, p. 65.

(1) *Œuvres de Cauchy*, série II, t. VIII, p. 67.

Si maintenant on remplace l'hyperbole à laquelle appartiennent le rayon s et le demi-axe réel a, par l'hyperbole conjuguée à laquelle appartiennent le rayon t et le demi-axe réel b perpendiculaire au demi-axe a, alors, à la place de la formule (47), on obtiendra la suivante :

$$s^2\cos^2\mu - t^2\cos^2\nu = a^2; \tag{48}$$

puis on tirera des formules (47), (48), combinées entre elles par voie de soustraction,

$$s^2 - t^2 = a^2 - b^2. \tag{49}$$

Les formules (44), (45), (46), (47), (48), (49) expriment des propriétés connues des rayons conjugués d'une ellipse ou de deux hyperboles.

Il est bon d'observer encore que, si l'on nomme ι l'angle $(\widehat{s, t})$ compris entre les deux rayons conjugués s, t, ces rayons seront liés à l'angle ι dans les théorèmes V et VI, par l'équation

$$st\sin\iota = ab, \tag{50}$$

analogue à la formule (37).

Dans les formules (38), (41), (50), les lettres

$$\delta, \quad \varepsilon, \quad \iota$$

représentent des angles dont chacun est censé positif et inférieur à deux droits. On pourrait, d'ailleurs, introduire dans les deux premières, à la place des angles δ, ε, l'angle ι et un *angle polaire* p mesuré à partir du rayon s, jusqu'au rayon t, en considérant l'angle p comme positif ou comme négatif, suivant qu'il se mesurerait dans le sens de l'angle ι ou en sens inverse. Alors on trouverait

$$\sin\delta = \pm\sin p, \qquad \sin\varepsilon = \pm\sin(p-\iota), \tag{51}$$

et les équations (38), (41) deviendraient respectivement

$$r^2[s^2\sin^2 p + t^2\sin^2(p-\iota)] = a^2b^2, \tag{52}$$

$$r^2[t^2\sin^2(p-\iota) - s^2\sin^2 p] = a^2b^2, \tag{53}$$

les longueurs s, t des deux rayons conjugués pouvant être déterminées

en fonction de ι à l'aide de la formule (46) ou (49), et de la formule (50).

Lorsque les directions des deux rayons conjugués demeurent fixes, les longueurs s, t de ces deux rayons demeurent constantes, ainsi que la quantité ι. Alors l'équation (44) ou (45), ne renfermant plus d'autres variables que le rayon vecteur mobile r et l'angle polaire p formé par ce rayon mobile avec un rayon fixe s, devient l'*équation polaire* d'une ellipse ou d'une hyperbole. Cette équation polaire suppose, d'ailleurs, que le centre de la courbe est pris pour origine des coordonnées.

Si l'on fait coïncider le rayon s avec le demi-axe a, on aura

$$s = a, \qquad t = b, \qquad \varpi = \frac{\pi}{2}.$$

Donc alors l'équation polaire de l'ellipse se réduira, ainsi qu'on devait s'y attendre, à la formule

$$r^2(a^2\sin^2 p + b^2\cos^2 p) = a^2b^2, \tag{54}$$

et l'équation polaire de l'hyperbole, à la formule

$$r^2(b^2\cos^2 p - a^2\sin^2 p) = a^2b^2. \tag{55}$$

Si la suite

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

renfermait trois termes au lieu de deux, on pourrait considérer ces trois termes x, y, z comme représentant les coordonnées rectangulaires d'un point mobile. Alors aussi, à la place de l'équation (48) du paragraphe I, on obtiendrait l'équation (54) du même paragraphe; et, en recherchant l'interprétation géométrique dont cette équation serait susceptible, on se trouverait conduit à certaines propriétés d'un ellipsoïde ou de deux hyperboloïdes conjugués. Mais ces propriétés, étant relatives à des points situés dans un plan diamétral, se réduiraient, en dernière analyse, à des propriétés d'une ellipse ou de deux hyperboles conjuguées, et, par conséquent, aux théorèmes que nous avons déduits de la formule (48) du paragraphe I.