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

H. POINCARÉ

# Les fonctions fuchsiennes et l'Arithmétique

*Journal de mathématiques pures et appliquées 4^e série*, tome 3 (1887), p. 405-464.
<http://www.numdam.org/item?id=JMPA_1887_4_3__405_0>

# *Les fonctions fuchsiennes et l'Arithmétique;*

PAR M. H. POINCARÉ.

## I. — NOTATIONS ET DÉFINITIONS.

Dans le Mémoire qui va suivre, et qui a pour objet l'étude arithmétique des fonctions fuchsiennes, nous ferons usage d'un système abrégé de notations qui a déjà été assez souvent employé.

Nous désignerons une substitution linéaire quelconque par une seule lettre.

Ainsi soit

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

une forme homogène en $x$, $y$ et $z$.

Considérons une substitution linéaire portant sur ces trois variables et définie par le système de neuf coefficients

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}.$$

Nous désignerons par exemple cette substitution par la lettre S.

Alors la notation

$$F.S$$

désignera la forme

$$F(a_1x + b_1y + c_1z, a_2x + b_2y + c_2z, a_3x + b_3y + c_3z).$$

Comme F.S sera aussi une forme homogène en $x$, $y$, $z$, nous pourrons lui appliquer une autre substitution linéaire

$$S' = \begin{vmatrix} a'_1 & b'_1 & c'_1 \\ a'_2 & b'_2 & c'_2 \\ a'_3 & b'_3 & c'_3 \end{vmatrix}.$$

Nous obtiendrons ainsi la forme

$$F\begin{bmatrix} a_1(a'_1x+b'_1y+c'_1z)+b_1(a'_2x+b'_2y+c'_2z)+c_1(a'_3x+b'_3y+c'_3z) \\ a_2(a'_1x+b'_1y+c'_1z)+b_2(a'_2x+b'_2y+c'_2z)+c_2(a'_3x+b'_3y+c'_3z) \\ a_3(a'_1x+b'_1y+c'_1z)+b_3(a'_2x+b'_2y+c'_2z)+c_3(a'_3x+b'_3y+c'_3z) \end{bmatrix},$$

que nous désignerons par la notation

$$(F.S)S',$$

ou plus simplement

$$F.S.S'.$$

Cela définit en même temps la substitution SS′ et montre que l'on a

$$F(SS') = (FS)S'.$$

Nous allons considérer en particulier la forme quadratique

$$\Phi = Y^2 - XZ,$$

dépendant des trois variables indépendantes X, Y et Z et les transformées de cette forme quadratique par diverses substitutions linéaires S. Il est aisé de trouver toutes les substitutions linéaires S qui n'altèrent pas $\Phi$, c'est-à-dire qui sont telles que

$$\Phi.S = \Phi.$$

Mais il convient d'abord de distinguer ces substitutions en deux sortes.

Une transformation qui n'altère pas une forme quadratique peut

s'écrire

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}.$$

Formons l'équation en S, du troisième degré

$$\begin{vmatrix} a_1 - S & b_1 & c_1 \\ a_2 & b_2 - S & c_2 \\ a_3 & b_3 & c_3 - S \end{vmatrix} = 0,$$

cette équation aura une racine égale à $+1$, ou une racine égale à $-1$. Dans le premier cas, la transformation sera dite droite; dans le second cas, elle sera gauche.

Dans ce qui va suivre nous ne nous occuperons que des transformations droites, de déterminant $+1$. Il est aisé de voir alors que les substitutions semblables droites de la forme $\Phi$ peuvent s'écrire

$$S = \begin{vmatrix} \delta^2 & -\delta\gamma & \gamma^2 \\ -2\delta\beta & \alpha\delta + \beta\gamma & -2\alpha\gamma \\ \beta^2 & -\alpha\beta & \alpha^2 \end{vmatrix},$$

où $\alpha$, $\beta$, $\gamma$, $\delta$ sont quatre quantités quelconques telles que

$$(\alpha\delta - \beta\gamma)^6 = 1.$$

Nous n'envisagerons que les substitutions à coefficients réels; nous supposerons donc que $\alpha$, $\beta$, $\gamma$, $\delta$ sont réels, de sorte qu'on devra avoir

$$\alpha\delta - \beta\gamma = \pm 1.$$

Nous rejetterons également les substitutions de déterminant $-1$, de sorte qu'on aura enfin

$$\alpha\delta - \beta\gamma = 1.$$

Nous avons appelé *substitutions fuchsiennes* les substitutions de la

forme

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right),$$

où $\alpha$, $\beta$, $\gamma$, $\delta$ sont des quantités réelles telles que

$$\alpha\delta - \beta\gamma = 1.$$

On voit ainsi qu'à la substitution S correspondra une substitution fuchsienne

$$s = \left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right).$$

Si S et S′ sont deux transformations linéaires qui n'altèrent pas $\Phi$, et que $s$ et $s'$ soient les substitutions fuchsiennes correspondantes, à la transformation SS′ correspondra la substitution fuchsienne $ss'$.

A tout groupe discontinu de transformations n'altérant pas $\Phi$ correspondra un groupe fuchsien, et réciproquement.

Soit maintenant T une transformation linéaire de déterminant quelconque et qui altère $\Phi$. Posons

$$F = \Phi . T.$$

La forme quadratique F sera inaltérée par certaines substitutions linéaires de déterminant 1, que nous appellerons, pour employer une expression consacrée par l'usage, *transformations semblables de* F.

A toute transformation semblable de F correspondra une transformation semblable de $\Phi$.

Si en effet S est une transformation semblable de $\Phi$, T$^{-1}$ST sera une transformation semblable de F.

Ainsi à tout groupe discontinu de transformations semblables de F correspondra un groupe de transformations semblables de $\Phi$, et par conséquent un groupe fuchsien; et réciproquement.

Supposons que F ait ses coefficients entiers; parmi les transformations semblables de F nous distinguerons celles dont les coefficients sont entiers. Elles forment un groupe discontinu qui a déjà attiré l'attention de nombreux arithméticiens désireux de parcourir la voie qu'a ouverte M. Hermite.

A ce groupe discontinu correspondra donc un groupe fuchsien et par conséquent un système de fonctions fuchsiennes. De pareilles fonctions fuchsiennes pourront s'appeler *fonctions fuchsiennes arithmétiques* (Cf. *Bulletin de l'Association française pour l'avancement des Sciences*, t. X, p. 132 et 138, et *Comptes rendus de l'Académie des Sciences*, Note du 29 mars 1886).

Le but du présent travail est l'étude de ces fonctions fuchsiennes arithmétiques et de leurs applications à la théorie des nombres.

Je me propose en particulier d'établir que ces fonctions admettent un théorème qui peut être regardé comme la généralisation du théorème d'addition des fonctions elliptiques, ce qui ne paraît pas avoir lieu pour les fonctions fuchsiennes ordinaires.

Pour compléter ce système de définitions qui me seront nécessaires dans la suite, je vais rappeler ce qu'on doit entendre par *indice* d'un sous-groupe.

On peut trouver dans le groupe principal un certain nombre de substitutions

$$(1) \qquad S_1, \quad S_2, \quad \ldots, \quad S_n$$

telles que toute substitution du groupe principal puisse se mettre d'une manière et d'une seule sous la forme

$$T_i S_k,$$

$T_i$ étant une substitution du sous-groupe et $S_k$ une substitution du système (1).

Le nombre des substitutions de ce système (qui peut d'ailleurs être infini) est l'indice du sous-groupe.

Le *groupe commun* à deux groupes G et G′ est le groupe formé de toutes les substitutions communes à G et à G′.

Deux groupes sont *commensurables* quand leur groupe commun est pour chacun d'eux un sous-groupe d'indice fini.

On définirait de même le groupe commun à trois groupes ou la commensurabilité de trois groupes.

Voici maintenant quelques propositions qu'on peut déduire immédiatement de ces définitions.

1° Soient G et G′ deux groupes quelconques, C leur groupe commun, soit $g$ un sous-groupe d'indice fini de G; soit $c$ le groupe commun à $g$ et à G′; $c$ sera un sous-groupe de C; je dis que ce sera un sous-groupe d'indice fini.

Soit $n$ l'indice du sous-groupe $g$.

Soient

$$S_1, \quad S_2, \quad \ldots, \quad S_n$$

$n$ substitutions convenablement choisies dans le groupe G. Toute substitution de G pourra se mettre sous la forme

$$T_i S_k \qquad (k = 1, 2, \ldots, n),$$

$T_i$ étant une substitution de $g$.

Nous pourrons toujours supposer que $S_1$ se réduit à la substitution identique

$$S_1 = 1.$$

Formons le tableau des substitutions de C, c'est-à-dire des substitutions communes à G et à G′. Nous pourrons les classer en $n$ classes. Chacune d'elles peut, en effet, se mettre sous la forme $T_i S_k$ et K peut prendre $n$ valeurs différentes. Il peut arriver toutefois qu'une ou plusieurs des classes ainsi définies ne contienne aucune substitution.

Soient

$$T_1, \quad T_2, \quad \ldots, \quad T_i, \quad \ldots, \quad \text{à l'infini},$$

les substitutions de la première classe qui correspond au cas de $k = 1$ et de

$$S_k = S_1 = 1.$$

Ce seront par définition les substitutions du sous-groupe $c$.

Nous pourrons supposer

$$T_1 = 1.$$

Soient maintenant

$$T'_1 S_2, \quad T'_2 S_2, \quad \ldots, \quad T'_i S_2, \quad \ldots$$

les substitutions de la seconde classe.

Je dis que toutes ces substitutions pourront se mettre sous la forme

$$T_i T'_1 S_2,$$

$T_i$ étant une substitution de la première classe, c'est-à-dire du groupe $c$.

Je dis que l'on aura par exemple

$$T'_i S_2 = T_i T'_1 S_2,$$

$T_i$ appartenant à $c$; cela revient à dire que

$$T'_i T'^{-1}_1$$

appartient à $c$. En effet, $T'_i$ et $T'_1$ appartenant par hypothèse à $g$, il en est de même de $T'_i T'^{-1}_1$; de plus, $T'_i S_2$ et $T'_1 S_2$ appartenant à G', il en sera encore de même de

$$T'_i S_2 (T'_1 S_2)^{-1} = T'_i T'^{-1}_1.$$

Cette dernière substitution faisant partie à la fois de $g$ et de G' fera partie du groupe commun $c$.

Ainsi le Tableau des substitutions du groupe C réparties en $n$ classes pourra s'écrire

| | | | | |
|---|---|---|---|---|
| $T_1,$ | $T_2$ | ..., | $T_i$ | ..., |
| $T'_1 S_2,$ | $T_2 T'_1 S_2,$ | ..., | $T_i T'_1 S_2,$ | ..., |
| $T''_1 S_3,$ | $T_2 T'_1 S_3,$ | ..., | $T_i T''_1 S_3,$ | ..., |
| ....., | ....., | ..., | ....., | ..., |
| $T^{(n)} S_n,$ | $T_2 T^{(n)}_1 S_n,$ | ..., | $T_i T^{(n)}_1 S_n,$ | ..., |

quelques-unes des classes pouvant manquer.

Par conséquent l'indice de $c$ par rapport à C est au plus égal à l'indice de $g$ par rapport à G.

2° Si $g$ et $g'$ sont deux sous-groupes d'indice fini de G et de G', leur groupe commun sera un sous-groupe d'indice fini par rapport au groupe commun de G et de G'.

Cette proposition se déduit immédiatement de la précédente.

3° Si $g$ et $g'$ sont deux sous-groupes d'indice fini par rapport à un même groupe G, leur groupe commun sera encore un sous-groupe d'indice fini de G.

4° Si deux groupes G et G′ sont commensurables à un même troisième G″, ils seront commensurables entre eux, et les trois groupes seront encore commensurables entre eux.

Soient en effet $C_1$, $C_2$ et $C_3$ les groupes communs, respectivement à G′ et à G″, à G″ et à G, et enfin à G et à G′.

Soit enfin $c$ le groupe commun aux trois groupes G, G′ et G″; $c$ sera évidemment aussi le groupe commun à deux quelconques des trois groupes $C_1$, $C_2$ et $C_3$.

Par hypothèse, les indices de $C_1$ par rapport à G′ et à G″, et de $C_2$ par rapport à G et à G″, sont finis.

Je dis que $c$ est un sous-groupe d'indice fini de G″; c'est en effet le groupe commun à $C_1$ et à $C_2$, sous-groupes d'indice fini de G″.

Je dis également que $c$ est un sous-groupe d'indice fini de G′; en effet, $c$ est le groupe commun à G′ et à $C_2$; $C_2$ est un sous-groupe d'indice fini de G″. Donc l'indice $c$ par rapport au groupe commun à G′ et à G″, c'est-à-dire par rapport à $C_1$, est fini. Or l'indice de $C_1$ par rapport à G′ est lui-même fini. Donc l'indice de $c$ par rapport à G′ est encore fini.

Rien ne distingue d'ailleurs G de G′. Donc l'indice de $c$ par rapport aux trois groupes G, G′ et G″ est fini; donc les trois groupes sont commensurables entre eux. C. Q. F. D.

$C_3$ contenant $c$ aura évidemment un indice fini par rapport à G et à G′; d'où il suit que ces deux derniers groupes sont aussi commensurables entre eux.

## II. — Réduction des formes.

Dans mon Mémoire sur les groupes kleinéens (*Acta mathematica*, t. III, *fig.* 1, § 2), j'ai exposé la distinction entre les groupes proprement discontinus et les groupes improprement discontinus. On a vu qu'un groupe peut être proprement discontinu dans une région donnée de l'espace et improprement dans une autre région.

Ici nous envisageons des formes quadratiques ternaires qui ont six

coefficients : elles peuvent donc être regardées comme des ensembles à six dimensions (ou à cinq seulement si l'on suppose le discriminant donné). Les groupes que nous envisageons peuvent donc être proprement discontinus quand les six coefficients sont soumis à certaines inégalités, et ne plus l'être qu'improprement quand ces inégalités cessent d'être remplies. Par exemple, ils pourront l'être proprement en ce qui concerne les formes définies et improprement en ce qui concerne les formes indéfinies.

Considérons donc un groupe G formé de substitutions linéaires et proprement discontinu par rapport à toutes les formes quadratiques ternaires définies. Soient F et F′ deux formes quadratiques ternaires définies; je dirai que ces deux formes sont équivalentes par rapport au groupe G quand on pourra passer de l'une à l'autre par une substitution de ce groupe. Parmi les formes équivalentes à F, il y en aura une que l'on regardera comme plus simple que toutes les autres et que l'on appellera la *réduite de* F.

Cette définition comporte évidemment un très grand arbitraire; on peut d'une infinité de manières trouver des inégalités telles que, parmi les formes équivalentes à F, il y en ait une et une seule qui y satisfasse (et cela quelle que soit F). Ce sont alors ces inégalités qui sont les conditions de réduction.

En d'autres termes, et pour employer un langage géométrique, considérons les six coefficients de notre forme quadratique comme les coordonnées d'un point dans l'espace à six dimensions. Cet espace sera divisé en deux régions, R correspondant aux formes définies et R′ correspondant aux formes indéfinies. Notre groupe G sera proprement discontinu dans R, improprement dans R′. On pourra donc partager R en une infinité de régions partielles $r_1$, $r_2$, ..., *ad inf.;* de telle façon que les substitutions de G changent ces régions partielles les unes dans les autres. Cette subdivistion sera tout à fait analogue à ce qu'est dans la théorie des groupes fuchsiens la subdivision du plan, ou d'une partie du plan, en une infinité de polygones curvilignes. Alors les formes réduites, par rapport au groupe G, seront celles qui correspondent à des points intérieurs à la première région partielle $r_1$.

Cette définition de la réduction par rapport à un groupe G est une généralisation immédiate de celle de la réduction arithmétique. Dans

le cas de la réduction arithmétique, en effet, G n'est autre chose que le *groupe arithmétique,* qui est formé des substitutions linéaires à coefficients entiers et de déterminant 1. On peut prendre alors pour conditions de réduction, soit celles qui ont été adoptées par M. Selling, soit celles de MM. Korkine et Zolotareff. Mais on pourrait en imaginer une infinité d'autres.

Un autre cas particulier intéressant est celui où G est un sous-groupe d'indice fini du groupe arithmétique. Alors une substitution quelconque du groupe arithmétique pourra se mettre d'une manière et d'une seule sous la forme

$$T_i S_k,$$

$T_i$ étant une substitution de G et

$$S_1, \quad S_2, \quad \ldots, \quad S_n$$

étant des substitutions du groupe arithmétique dont le nombre $n$ est précisément l'indice du sous-groupe.

Si alors F est une forme définie quelconque, sa réduite arithmétique s'écrira

$$FT_i S_k,$$

et nous pourrons convenir, pour définir la réduction par rapport au groupe G, de dire que sa réduite par rapport à ce groupe sera $FT_i$.

Tout cela ne peut pas s'étendre au cas des formes indéfinies, car les groupes qu'il pourrait être intéressant de considérer, et en particulier le groupe arithmétique, sont improprement discontinus pour ces formes indéfinies, c'est-à-dire dans la région que nous avons appelée R'.

Mais tous les arithméticiens connaissent l'ingénieux artifice par lequel M. Hermite, introduisant les variables continues dans la théorie des nombres, a le premier triomphé de cette difficulté.

En même temps que la forme indéfinie

$$\Phi = Y^2 - XZ,$$

envisageons la forme

$$H = Y^2 + \frac{X^2}{3} + \frac{Z^2}{3}$$

qui est définie. Si T est une substitution linéaire et si HT est une forme définie réduite par rapport au groupe G, nous dirons que la substitution T est réduite par rapport à G et que la forme indéfinie $\Phi T$ est également réduite par rapport à G.

Voici maintenant comment on pourra trouver les réduites d'une forme indéfinie

$$F = \Phi\tau.$$

On aura aussi

$$F = \Phi S\tau,$$

S étant une quelconque des substitutions

$$\begin{vmatrix} \delta^2 & -\delta\gamma & \gamma^2 \\ -2\delta\beta & \alpha\delta+\beta\gamma & -2\alpha\gamma \\ \beta^2 & -\alpha\beta & \alpha^2 \end{vmatrix},$$

où $\alpha$, $\beta$, $\gamma$, $\delta$ sont quatre quantités réelles quelconques telles que :

Ce groupe des substitutions S, qui n'altèrent pas $\Phi$, s'appellera *groupe reproductif de* $\Phi$.

Considérons la forme définie $HS\tau$; il y aura toujours, d'après ce qui précède, dans le groupe G une substitution T qui réduira cette forme quadratique définie par rapport au groupe G. La forme $HS\tau T$ sera alors réduite. La substitution $S\tau T$ sera réduite, et la forme indéfinie

$$\Phi S\tau T = F_1 T$$

sera réduite. La substitution T sera alors l'une des substitutions réductrices de F. Comme il y a une infinité de substitutions S, la forme F admettra en général une infinité de substitutions réductrices.

Il peut se faire que deux substitutions réductrices T et T′ conduisent à une même réduite, et qu'on ait

$$FT = FT'.$$

En ce cas, $T^{-1}T'$ est l'une des substitutions de G qui n'altèrent pas F.

Il peut donc arriver que le nombre des réduites soit fini, bien que

celui des substitutions réductrices soit infini. C'est ce qui se passe, par exemple, si F a ses coefficients entiers et si G est le groupe arithmétique.

Il en est encore de même si, les coefficients de F étant entiers, G est un sous-groupe d'indice fini du groupe arithmétique.

J'appellerai *groupe reproductif* de F le groupe des substitutions linéaires de déterminant $+1$ qui n'altèrent pas cette forme. Ce sera le transformé par la substitution $\tau$ du groupe reproductif de $\Phi$, car toute substitution qui n'altère pas F peut se mettre sous la forme

$$\tau^{-1} S \tau,$$

S n'altérant pas $\Phi$.

J'appellerai *sous-groupe inaltérant* de G par rapport à F le groupe commun à G et au groupe reproductif de F. Le transformé de ce sous-groupe par la substitution $\tau^{-1}$ sera le *groupe inaltérant transformé* relatif à G et à F. Ce sera un sous-groupe du groupe reproductif de $\Phi$.

Nous avons vu au numéro précédent qu'à toute substitution du groupe reproductif de $\Phi$ correspond une substitution fuchsienne $s$. Donc au groupe inaltérant transformé relatif à G et à F correspondra un certain groupe fuchsien que j'appellerai *groupe fuchsien relatif à* G *et à* F.

Nous adopterons des dénominations spéciales, pour abréger le langage, dans le cas où G sera le groupe arithmétique. Le sous-groupe inaltérant s'appellera le *groupe principal de* F; le groupe inaltérant transformé s'appellera le *groupe transformé principal de* F; enfin le groupe fuchsien relatif à F et au groupe arithmétique s'appellera le *groupe fuchsien principal de* F.

Il résulte de là que, pour étudier le groupe principal de F, formé des substitutions semblables de F, il suffit d'étudier le groupe fuchsien principal de F.

Nous adopterons le mode suivant de représentation géométrique.

Nous considérerons un plan représentant la variable imaginaire $z$; nous ferons correspondre à la substitution S la substitution

$$s = \left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right),$$

que nous représenterons elle-même par le point du plan des $z$ qui a pour affixe

$$\frac{\alpha\sqrt{-1}+\beta}{\gamma\sqrt{-1}+\delta}.$$

Ce point fait partie du dernier plan situé au-dessus de l'axe des quantités réelles. A chaque substitution S correspondra un point de ce demi-plan, mais à chaque point du demi-plan correspondront une infinité de substitutions S faisant partie du groupe reproductif de $\Phi$.

Nous regarderons comme donnés le groupe G et la transformation $\tau$ qui change $\Phi$ en F.

Voici alors comment se représentera géométriquement la réduction de F par rapport à G :

A chaque substitution S et, par conséquent, à chaque forme quadratique définie H.S correspondra un point de notre demi-plan. Je dis maintenant qu'à chaque point de ce demi-plan, auquel correspondent pourtant une infinité de substitutions S, ne correspondra pourtant qu'une seule forme définie H.S.

Soient, en effet, S et S′ deux substitutions correspondant à un même point P de notre demi-plan. Je dis que

$$H.S = HS',$$

c'est-à-dire

$$H.SS'^{-1} = H.$$

En effet, les substitutions fuchsiennes $s$ et $s'$ qui correspondent respectivement à S et S′ changent toutes deux le point $\sqrt{-1}$ dans le point P. Donc la substitution $ss'^{-1}$ n'altérera pas le point $\sqrt{-1}$.

On en conclura que les valeurs des quatre quantités $\alpha$, $\beta$, $\gamma$, $\delta$, qui correspondent à $ss'^{-1}$, ou ce qui revient au même à $SS'^{-1}$, sont

$$\alpha = \cos\varphi, \qquad \beta = \sin\varphi, \qquad \gamma = -\sin\varphi, \qquad \delta = \cos\varphi,$$

$\varphi$ étant un angle quelconque; d'où l'on déduira sans peine que la substi-

tution $SS'^{-1}$ s'écrit

$$\begin{vmatrix} \cos^2\varphi & +\frac{1}{2}\sin^2\varphi & \sin^2\varphi \\ -\sin^2\varphi & \cos^2\varphi & \sin^2\varphi \\ \sin^2\varphi & -\frac{1}{2}\sin^2\varphi & \cos^2\varphi \end{vmatrix},$$

et, par conséquent, qu'elle n'altère pas H. C. Q. F. D.

A chaque point du demi-plan correspond donc une seule forme H.S, par conséquent une seule forme ΦS. Connaissant la forme définie $HS\tau$, on connaîtra la substitution réductrice T qui fait partie du groupe G et réduit $HS\tau$ par rapport à G.

A chaque point du demi-plan correspondra de la sorte une substitution réductrice et une seule. Nous pourrons donc subdiviser ce demi-plan en une infinité de régions, telles que, pour tous les points d'une même région, la substitution réductrice soit la même.

Ce mode de représentation géométrique est analogue, mais non identique à celui qu'a employé M. Selling.

Nous avons vu que, dans certains cas, bien qu'il y ait une infinité de substitutions réductrices, il n'y avait qu'un nombre fini de réduites. Qu'arrive-t-il alors? Soient $f_1, f_2, \ldots, f_n$ nos $n$ réduites. Nous avons subdivisé le plan en une infinité de régions qui correspondent aux différentes substitutions réductrices. Soient $r_{10}, r_{11}, r_{12}, \ldots, r_{1i}$ une infinité de ces régions correspondant à la réduite $f_1$, elles seront les transformées les unes des autres par les diverses substitutions du groupe fuchsien relatif à F et à G. Soient de même $r_{20}, r_{21}, \ldots, r_{2i}$ les régions qui correspondent à la réduite $f_2$, .... Soient enfin $r_{n0}, r_{n1}, \ldots$ les régions qui correspondent à la réduite $f_n$.

Nous pourrons toujours supposer qu'on a choisi les indices de telle sorte que $r_{2i}, \ldots, r_{ni}$ soient les transformées de $r_{20}, \ldots, r_{n0}$ par la même substitution qui change $r_{10}$ en $r_{1i}$.

Cela posé, réunissons $r_{10}, r_{20}, \ldots, r_{n0}$ en une région unique $R_0$ et de même $r_{1i}, r_{2i}, \ldots, r_{ni}$ en une région unique $R_i$. Les diverses régions $R_i$ seront les transformées les unes des autres par les diverses substitutions du groupe fuchsien relatif à F et à G.

Il serait aisé de ramener ces régions $R_0, \ldots, R_i, \ldots$ à des polygones

curvilignes, comme je l'ai expliqué dans le § V de mon Mémoire sur les groupes fuchsiens (*Acta math.*, t. I).

Avant de terminer ce paragraphe, je dois faire une dernière remarque. Nous avons regardé comme donnée la substitution $\tau$ qui change $\Phi$ en F. Il ne suffit pas, pour cela, de se donner F. En effet, cette forme peut dériver de $\Phi$ d'une infinité de manières; on a non seulement

$$F = \Phi\tau,$$

mais encore

$$F = \Phi.S.\tau,$$

S étant une substitution quelconque du groupe reproductif de $\Phi$.

Il est clair, si l'on se reporte aux définitions qui précèdent, que le groupe fuchsien relatif à F et à G ne sera pas le même selon qu'on regardera F comme dérivée de $\Phi$ par la substitution $\tau$ ou par la substitution $S\tau$.

Quand cela sera nécessaire, afin d'éviter toute confusion, nous distinguerons ces deux cas en disant, dans le premier, le groupe fuchsien relatif à G et à $F = \Phi\tau$; dans le second, le groupe fuchsien relatif à G et à $F = \Phi S\tau$.

Le groupe fuchsien relatif à G et à $F = \Phi S\tau$ sera le transformé du groupe fuchsien relatif à G et $F = \Phi\tau$ par la substitution $s^{-1}$, $s$ étant la substitution fuchsienne qui correspond à S, en vertu des conventions faites. En particulier, le groupe fuchsien principal de $F = \Phi S\tau$ sera le transformé du groupe fuchsien principal de $F = \Phi\tau$ par $s^{-1}$.

## III. — Lemmes divers.

Lemme I. — *Si g est un sous-groupe d'indice fini de* G, *le groupe fuchsien relatif à g et à* F *sera un sous-groupe d'indice fini du groupe fuchsien relatif à* G *et à* F.

C'est une conséquence des lemmes démontrés à la fin du § I et des définitions du § II.

Lemme II. — *Si* G *et* G′ *sont deux groupes commensurables, les*

*groupes fuchsiens de* F *relatifs respectivement à* G *et à* G' *sont aussi commensurables.*

Ce lemme est une conséquence immédiate du précédent et des définitions.

LEMME III. — *Soit* $F = \Phi\tau$; *soient ensuite* T' *une substitution de* G *et* $F' = \Phi\tau T'$ *une forme équivalente à* F *par rapport au groupe* G. *Les deux formes* F *et* F' *auront même groupe fuchsien relatif à* G.

En effet, le sous-groupe inaltérant $g'$ de G par rapport à F' sera le transformé par la substitution T' du sous-groupe inaltérant $g$ de G par rapport à F.

Si, en effet, U est une substitution du second sous-groupe $g$, de telle sorte que

$$F = FU,$$

on aura

$$F' = FT' = FUT' = F'T'^{-1}UT',$$

de telle façon que $T'^{-1}UT'$ appartiendra au premier sous-groupe $g'$.

Le groupe inaltérant transformé de F sera le transformé de $g$ par $\tau^{-1}$, ce sera donc

$$\tau g \tau^{-1}.$$

De même, le groupe inaltérant transformé de $F' = \Phi\tau T'$ sera

$$\tau T' g' T'^{-1} \tau^{-1}.$$

Mais nous venons de voir que

$$g' = T'^{-1} g T'.$$

Il vient donc

$$\tau T' g' T'^{-1} \tau^{-1} = T'^{-1} g T',$$

de sorte que les deux groupes inaltérants transformés se confondent.

Les deux groupes fuchsiens se confondront donc également.

C. Q. F. D.

En particulier, si G est le groupe arithmétique, le groupe fuchsien de $F = \Phi\tau$ par rapport à un groupe commensurable à G sera commensurable avec le groupe fuchsien principal de $F = \Phi\tau$.

Si T' est une substitution à coefficients entiers, les deux formes équivalentes $F = \Phi\tau$ et $F' = \Phi\tau T'$ auront même groupe fuchsien principal.

LEMME IV. — *Si* G *et* G' *sont deux groupes commensurables, et* S *une substitution de* G', *une des puissances entières de* S (*d'exposant différent de* 0) *fera partie de* G.

Soit, en effet, $g$ le groupe commun de G et G'; soit $n$ l'indice du sous-groupe $g$ par rapport à G'; cet indice est fini par hypothèse.

Si alors on prend au hasard $n + 1$ substitutions dans G' (parmi lesquelles on peut toujours supposer que l'on comprend la substitution identique 1), on pourra toujours trouver parmi elles deux substitutions $S_i$ et $S_k$, telles que

$$S_i S_k^{-1}$$

appartienne à $g$ et, par conséquent, à G.

Prenons, par exemple,

$$S^0 = 1, \qquad S, \quad S^2, \quad S^3, \quad \ldots, \quad S^n,$$

qui toutes font partie du groupe G'; soient alors

$$S_i = S^i, \qquad S_k = S^k.$$

Alors

$$S_i S_k^{-1} = S^{i-k}$$

fera partie de G. C. Q. F. D.

Nous allons étudier maintenant quelques-uns des sous-groupes du groupe arithmétique. Ce groupe est formé, d'après sa définition, de toutes les substitutions

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix},$$

dont les coefficients sont entiers, et le déterminant égal à 1.

Pour définir un sous-groupe du groupe arithmétique, il faut donc assujettir les coefficients entiers $a$, $b$, $c$ à de nouvelles conditions.

Je distinguerai les *sous-groupes à congruences* où les neuf coefficients $a$, $b$, $c$ sont assujettis à satisfaire à certaines congruences suivant un certain module $q$ premier ou composé.

LEMME V. — *Un sous-groupe à congruences est toujours un sous-groupe d'indice fini du groupe arithmétique.*

Soit, en effet, $g$ un sous-groupe défini par les $k$ congruences

$$(1) \qquad P_1 \equiv P_2 \equiv \ldots \equiv P_k \equiv 0 \pmod{q},$$

où les P sont des polynômes entiers par rapport aux $a$, $b$, $c$.

Les congruences (1) devront être satisfaites si l'on fait

$$(2) \qquad \left\{ \begin{array}{l} a_1 \equiv b_2 \equiv c_3 \equiv 1, \\ a_2 \equiv a_3 \equiv b_1 \equiv b_3 \equiv c_1 \equiv c_2 \equiv 0 \end{array} \right\} \pmod{q},$$

et, en effet, la substitution identique

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}$$

devra faire partie de $g$.

Le sous-groupe $g'$ défini par les congruences (2) sera donc un sous-groupe du groupe $g$ qui est lui-même un sous-groupe du groupe arithmétique.

Il est évident que $g'$ sera un sous-groupe d'indice fini du groupe arithmétique; car cet indice sera certainement plus petit que $q^9$ (il se réduira à $q^8$ si $q$ est premier), puisque chacun des neuf coefficients $a$, $b$, $c$ peut prendre $q$ valeurs incongrues par rapport au module $q$.

Donc *a fortiori* $g$ sera un sous-groupe d'indice fini du groupe arithmétique. C. Q. F. D.

Considérons maintenant une transformation T' à coefficients entiers, mais dont le déterminant soit égal à un entier $\Delta$ plus grand que 1.

Soient G le groupe arithmétique, G′ son transformé par T′, $g$ le groupe commun à G et à G′; je dis que $g$ sera un sous-groupe à congruences.

Soit, en effet,

$$S = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$$

une substitution à coefficients entiers faisant partie de G.

Soit

$$T' = \begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix}$$

la substitution définie plus haut.

La transformée de S par T′ s'écrira

$$T'^{-1}ST' = \begin{vmatrix} \frac{P_1}{\Delta} & \frac{P_2}{\Delta} & \frac{P_3}{\Delta} \\ \frac{P_4}{\Delta} & \frac{P_5}{\Delta} & \frac{P_6}{\Delta} \\ \frac{P_7}{\Delta} & \frac{P_8}{\Delta} & \frac{P_9}{\Delta} \end{vmatrix},$$

les P étant des polynômes entiers homogènes et du premier degré par rapport aux $a$, $b$ et $c$, et dont les coefficients dépendent des $\alpha$, $\beta$ et $\gamma$.

Pour que cette substitution fasse partie de $g$, il faut et il suffit que ses coefficients soient entiers, ce qui s'exprime par les neuf congruences

$$P_i \equiv 0 \pmod{\Delta}.$$

Cela montre que $g$ est un sous-groupe à congruences; d'où l'on déduit aisément le lemme suivant :

LEMME VI. — *Le groupe arithmétique est commensurable avec son transformé par une substitution à coefficients entiers de déterminant plus grand que* 1.

Ou, ce qui revient au même,

*Le groupe arithmétique est commensurable avec son transformé par une substitution à coefficients fractionnaires.*

Soit maintenant T′ une substitution à coefficients fractionnaires; je dirai que *la forme* F *est commensurable* avec sa transformée FT′ par la substitution T′.

Lemme VII. — *Considérons deux formes commensurables* F *et* FT′; *le groupe fuchsien principal de* $F = \Phi\tau$ *sera commensurable avec le groupe fuchsien principal de* $FT' = \Phi\tau T'$.

En effet, le groupe arithmétique est commensurable avec le groupe G qui est son transformé par $T'^{-1}$.

Soit $g$ le sous-groupe inaltérant de G par rapport à F; il sera commensurable avec le groupe principal de F.

D'autre part, le groupe principal de FT′ sera le transformé de $g$ par T′.

Le groupe transformé principal de $F = \Phi\tau$ sera le transformé par $\tau^{-1}$ du groupe principal de F; le groupe transformé principal de $FT' = \Phi\tau T'$ sera le transformé par $(\tau T')^{-1} = T'^{-1}\tau^{-1}$ du groupe principal de FT′, et, par conséquent, le transformé par $\tau^{-1}$ du groupe $g$.

Or $g$ et le groupe principal de F sont commensurables.

Donc les groupes transformés principaux de $F = \Phi\tau$ et de $FT' = \Phi\tau T'$ le sont également.

Donc les groupes fuchsiens principaux de $F = \Phi\tau$ et de $FT' = \Phi\tau T'$ sont commensurables. C. Q. F. D.

## IV. — Substitutions fractionnaires.

On peut se proposer de rechercher quelles sont les substitutions à coefficients fractionnaires qui n'altèrent pas une forme F à coefficients entiers, ou, en d'autres termes, quelles sont les transformations semblables fractionnaires de F. Il est aisé de prévoir, d'ailleurs, que le groupe formé par ces transformations ne sera pas un groupe discontinu.

On voit aussi immédiatement que des substitutions semblables fractionnaires de F on pourra déduire les substitutions semblables fractionnaires d'une forme $F' = FT'$ commensurable avec F. En effet, les dernières seront les transformées des premières par la transformation T.

Soit donc à trouver les substitutions semblables fractionnaires de la forme

$$F = Ax^2 + A'y^2 + A''z^2 + 2Byz + 2B'xz + 2B''xy.$$

On a

$$A(AA' - B''^2)F = (AA' - B''^2)(Ax + B''y + B'z)^2 + [(AA' - B''^2)y + (AB - B''B')z]^2 + A\Delta z^2,$$

$\Delta$ désignant le discriminant de F, de telle sorte que la forme F est, à un facteur constant près, commensurable avec

$$F' = (AA' - B''^2)x^2 + y^2 + A\Delta z^2.$$

Nous sommes donc ramenés à étudier les substitutions semblables fractionnaires des formes telles que

$$Ax^2 + By^2 + Cz^2,$$

ou plutôt, puisque nous avons affaire à une forme indéfinie, et si nous voulons mettre les signes en évidence

$$Ax^2 + By^2 - Cz^2.$$

Nous allons d'abord nous poser le problème suivant :

*Quelles sont les substitutions fractionnaires qui n'altèrent ni z ni* $Ax^2 + By^2$ ?

Il faut alors trouver quatre nombres fractionnaires $\alpha$, $\beta$, $\gamma$, $\delta$, tels que

$$A(\alpha x + \beta y)^2 + B(\gamma x + \delta y)^2 = Ax^2 + By^2.$$

Nous mettrons les quatre nombres $\alpha$, $\beta$, $\gamma$, $\delta$ sous la forme

$$\alpha = \frac{\alpha_1}{\varepsilon}, \qquad \beta = \frac{\beta_1}{\varepsilon}, \qquad \gamma = \frac{\gamma_1}{\varepsilon}, \qquad \delta = \frac{\delta_1}{\varepsilon};$$

$\alpha_1$, $\beta_1$, $\gamma_1$, $\delta_1$, $\varepsilon$ étant entiers ou fractionnaires, nous pourrons toujours supposer que $\alpha_1$, $\gamma_1$ et $\varepsilon$ sont entiers : on aura alors

$$\begin{aligned}
\alpha_1\delta_1 - \beta_1\gamma_1 &= \varepsilon^2,\\
A\alpha_1^2 + B\gamma_1^2 &= A\varepsilon^2,\\
A\alpha_1\beta_1 + B\gamma_1\delta_1 &= 0,\\
A\beta_1^2 + B\delta_1^2 &= B\varepsilon^2.
\end{aligned}$$

Supposons que l'on ait trouvé trois entiers $\alpha_1$, $\gamma_1$ et $\varepsilon$ satisfaisant à

$$A\alpha_1^2 + B\gamma_1^2 = A\varepsilon^2,$$

il suffira de prendre

$$\beta_1 = -\frac{B\gamma_1}{A}, \qquad \delta_1 = \alpha_1$$

pour satisfaire aux trois autres équations.

Il reste donc à résoudre l'équation

$$B\gamma_1^2 = A(\varepsilon - \alpha_1)(\varepsilon + \alpha_1).$$

Nous multiplierons donc B par un carré quelconque $\gamma_1^2$, mais de telle façon que $B\gamma_1^2$ soit divisible par A, et de plus soit impair ou divisible par 4 (ainsi, si B est un multiple de $4 + 2$, $\gamma_1$ devra être pair; si $A = A_1 A_2^2$, $A_1$ n'étant divisible par aucun carré, $\gamma_1$ devra être divisible par $A_1 A_2$).

Il sera facile ensuite de décomposer $\frac{B\gamma_1^2}{A}$ en deux facteurs tous deux pairs ou tous deux impairs, $\varepsilon - \alpha_1$ et $\varepsilon + \alpha_1$, et d'en déduire, pour $\varepsilon$ et $\alpha_1$, deux valeurs entières.

Tel est donc le moyen de former les substitutions semblables fractionnaires de la forme binaire

$$Ax^2 + By^2.$$

Pour les étudier plus complètement, nous supposerons $A = 1$. Cette hypothèse est toujours permise; car, si l'on avait $A < 1$, on multiplierait la forme par A, et on changerait ensuite de variable en posant $Ax = x'$.

Considérons notre substitution fractionnaire

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \begin{vmatrix} \frac{\alpha_1}{\varepsilon} & -\frac{B\gamma_1}{\varepsilon} \\ \frac{\gamma_1}{\varepsilon} & \frac{\alpha_1}{\varepsilon} \end{vmatrix},$$

et la substitution fuchsienne correspondante. Cette dernière sera évidemment une substitution elliptique qui n'altérera pas un certain point du plan. Ce point, que j'appelle P, se détermine aisément, et l'on trouve qu'il est le même pour toutes les substitutions fractionnaires de notre forme

$$x^2 + By^2.$$

Pour définir une substitution fuchsienne elliptique, il faut se donner non seulement le point P qui n'est pas altéré par cette substitution, mais encore l'angle de rotation $\varphi$.

Ici nous avons

$$\cos\varphi = \alpha = \frac{\alpha_1}{\varepsilon},$$

d'où l'on déduit

$$\sin\varphi = \frac{\gamma_1\sqrt{B}}{\varepsilon}.$$

Nous aurons alors

$$(\alpha_1 + \gamma_1\sqrt{-B})(\alpha_1 - \gamma_1\sqrt{-B}) = \varepsilon^2.$$

Nous devons supposer que $\alpha_1$, $\gamma_1$ et $\varepsilon$ sont premiers entre eux, et par conséquent que $\alpha_1$ et $\gamma_1$ sont premiers entre eux. Les deux nombres complexes

$$\alpha_1 + \gamma_1\sqrt{-B} \quad \text{et} \quad \alpha_1 - \gamma_1\sqrt{-B}$$

seront alors aussi premiers entre eux, et l'on aura

$$\varepsilon = MN, \qquad \alpha_1 + \gamma_1\sqrt{-B} = M^2, \qquad \alpha_1 - \gamma_1\sqrt{-B} = N^2,$$

M et N étant deux nombres complexes existants ou idéaux, conjugués entre eux et de plus premiers entre eux.

Cela posé, cherchons d'abord si $\varphi$ peut être commensurable avec $2\pi$. Si cela était, on trouverait un nombre entier $m$, tel que

$$(\alpha_1 + \gamma_1\sqrt{-B})^m = \varepsilon^m$$

ou que

$$M^m = N^m;$$

M et N étant premiers entre eux, cette égalité est impossible. Il n'y aurait exception que si $\varepsilon$ était égal à 1 et que $\alpha_1 + \gamma_1\sqrt{-B}$ fût une unité complexe.

Mais il faut faire attention au sens que l'on doit attacher à ce mot. Pour que la théorie des nombres complexes idéaux soit applicable, il faut prendre pour base du système $\sqrt{-B}$, si $+B$ (que d'ailleurs nous supposerons n'être divisible par aucun carré) est multiple de 4 plus 2 ou plus 1; il faut prendre, au contraire,

$$\frac{1+\sqrt{-B}}{2},$$

si B est multiple de 4 plus 3. Dans ce dernier cas,

$$\frac{\alpha+\beta\sqrt{-B}}{2}$$

est considéré comme un entier complexe si $\alpha+\beta$ est pair (*voir* DEDEKIND, *Théorie des nombres entiers algébriques*, p. 91. Paris, Gauthier-Villars; 1877).

Alors on a, comme unités complexes,

$$\pm 1, \qquad \pm\sqrt{-1}, \qquad \frac{\pm 1 \pm \sqrt{-3}}{2}.$$

On doit donc conclure de cette discussion que l'angle $\varphi$ ne peut être commensurable avec $2\pi$ que s'il est égal à $\pi$, à $\pm\frac{\pi}{2}$, à $\pm\frac{\pi}{3}$ ou à $\pm\frac{2\pi}{3}$.

On voit, de plus, que les substitutions fractionnaires qui reproduisent à la fois les deux formes

$$z \quad \text{et} \quad x^2 + By^2$$

correspondent aux divers entiers complexes formés avec $\sqrt{-B}$, et que leur théorie dépend intimement de celle de ces nombres complexes et des idéaux correspondants.

Voilà donc une première catégorie de substitutions fractionnaires n'altérant pas la forme

$$x^2 + By^2 - Cz^2.$$

Une autre catégorie se composera des substitutions qui n'altèrent ni $y$, ni $x^2 - Cz^2$ (sans parler d'une autre catégorie qui sera formée de même des substitutions qui n'altèrent ni $x$, ni $By^2 - Cz^2$). Ces substitutions correspondront aux nombres complexes formés avec $\sqrt{C}$ comme celles de la première catégorie correspondaient aux nombres complexes formés avec $\sqrt{-B}$. Mais l'analogie de ces trois catégories de substitutions fractionnaires est trop évidente pour qu'il soit nécessaire d'insister.

Je dis maintenant que toute substitution fractionnaire peut toujours être ramenée à celles que nous venons d'étudier.

Soit, en effet,

$$S = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

une substitution fractionnaire quelconque qui n'altère pas une certaine forme quadratique F à coefficients entiers ou commensurables. Je supposerai, de plus, que cette substitution est droite au sens donné à ce mot dans le premier paragraphe de ce Mémoire.

On pourra trouver alors une forme linéaire

$$\alpha_1 x + \beta_1 y + \gamma_1 z$$

à coefficients entiers, qui ne sera pas altérée par la substitution.

On pourra ensuite trouver encore deux formes linéaires

$$\alpha_2 x + \beta_2 y + \gamma_2 z,$$
$$\alpha_3 x + \beta_3 y + \gamma_3 z$$

à coefficients entiers, et telles que l'on puisse écrire

$$\begin{aligned} F = \quad & A_1(\alpha_1 x + \beta_1 y + \gamma_1 z)^2 \\ & + A_2(\alpha_2 x + \beta_2 y + \gamma_2 z)^2 \\ & + A_3(\alpha_3 x + \beta_3 y + \gamma_3 z)^2, \end{aligned}$$

$A_1$, $A_2$ et $A_3$ étant des quantités commensurables positives ou négatives.

Faisons maintenant un changement linéaire de variables en faisant

$$\begin{aligned} x' &= \alpha_1 x + \beta_1 y + \gamma_1 z, \\ y' &= \alpha_2 x + \beta_2 y + \gamma_2 z, \\ z' &= \alpha_3 x + \beta_3 y + \gamma_3 z, \end{aligned}$$

il viendra

$$F = A_1 x'^2 + A_2 y'^2 + A_3 z'^2,$$

de telle sorte que, si l'on appelle T la substitution linéaire

$$\begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{vmatrix},$$

on aura

$$FT^{-1} = A_1 x^2 + A_2 y^2 + A_3 z^2.$$

La substitution

$$TST^{-1}$$

sera fractionnaire et n'altérera pas $FT^{-1}$. Mais il y a plus, elle n'altérera pas $z$, ni par conséquent

$$A_1 x^2 + A_2 y^2.$$

Nous sommes donc ramenés au cas précédent.

Il conviendrait peut-être, pour compléter cette théorie, de dire quelques mots des substitutions fractionnaires gauches qui n'altèrent pas une forme quadratique. Mais je ne crois pas devoir m'y arrêter pour le moment. Je me bornerai à observer que, si S est une substi-

tution fractionnaire gauche n'altérant pas F, $S^2$ sera une substitution fractionnaire droite n'altérant pas non plus F.

## V. — Calcul des multiplicateurs.

Soit

$$S = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

une substitution linéaire de déterminant 1, et

$$T^{-1}ST = \begin{vmatrix} a'_1 & b'_1 & c'_1 \\ a'_2 & b'_2 & c'_2 \\ a'_3 & b'_3 & c'_3 \end{vmatrix}$$

sa transformée par une substitution linéaire quelconque T. On aura

$$a_1 + b_2 + c_3 = a'_1 + b'_2 + c'_3.$$

En d'autres termes, la somme $a_1 + b_2 + c_3$ sera un invariant. On pourra choisir la substitution T, de telle façon que $T^{-1}ST$ soit de la forme canonique

$$\begin{vmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{vmatrix}.$$

Alors $\lambda_1$, $\lambda_2$ et $\lambda_3$ seront les multiplicateurs de la substitution S; ces multiplicateurs seront les racines de l'équation en $\lambda$,

$$\begin{vmatrix} a_1 - \lambda & b_1 & c_1 \\ a_2 & b_2 - \lambda & c_2 \\ a_3 & b_3 & c_3 - \lambda \end{vmatrix} = 0,$$

et l'on aura

$$\lambda_1 + \lambda_2 + \lambda_3 = a_1 + b_2 + c_3.$$

Si, en particulier, S n'altère pas une forme quadratique et est une substitution droite, l'un des multiplicateurs est égal à 1, et le produit des deux autres est aussi égal à 1.

Soit alors

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right)$$

la substitution fuchsienne correspondant à S; $\alpha + \delta$ sera, pour cette substitution, un invariant comme $a_1 + b_2 + c_3$ l'était pour S, et l'on aura d'ailleurs

$$(\alpha + \delta)^2 = a_1 + b_2 + c_3 + 1.$$

Il résulte de là que la connaissance de $\alpha + \delta$ suffit pour déterminer les trois multiplicateurs, qui devront satisfaire à l'équation du troisième degré

$$\lambda^3 - 1 - [(\alpha + \delta)^2 - 1](\lambda^2 - \lambda) = 0.$$

Si S est une substitution à coefficients entiers, la somme $a_1 + b_2 + c_3$ devra être un entier, et par conséquent $\alpha + \delta$ devra être la racine carrée d'un entier.

La somme $\alpha + \delta$ s'appellera l'*invariant de la substitution* S et s'écrira, pour abréger, [S].

Nous allons traiter maintenant le problème suivant :

*On se donne* [A], [B] *et l'invariant* [AB] *de la combinaison* AB *des deux substitutions* A *et* B. *On demande de calculer l'invariant d'une combinaison quelconque de ces deux substitutions*

$$A^m B^n, \quad A^m B^n A^p, \quad A^m B^n A^p B^q, \quad \ldots,$$

*m, n, p, q étant des entiers quelconques positifs ou négatifs.*

Tout d'abord, il est évident que deux substitutions inverses l'une de l'autre auront même invariant; on aura

$$[A] = [A^{-1}], \qquad [B] = [B^{-1}], \qquad \ldots.$$

De plus, une substitution aura même invariant que sa transformée

par une substitution quelconque; ainsi,

$$[A] = [B^{-1}AB],$$
$$[A^m B^n A^p B^q] = [B^q A^m B^n A^p],$$

et, en particulier,

$$[BA] = [AB] = [A^{-1}B^{-1}] = [B^{-1}A^{-1}].$$

Je vais maintenant chercher une relation entre

$$[A], \quad [B], \quad [AB] \quad \text{et} \quad [AB^2].$$

Nous pouvons toujours, par une transformation convenable, mettre la substitution fuchsienne qui correspond à B sous la forme

$$\left[z, \frac{\lambda z}{\left(\frac{1}{\lambda}\right)}\right].$$

Soit ensuite

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right)$$

la substitution fuchsienne correspondant à A. Alors

$$\left(z, \frac{\alpha\lambda z + \beta\lambda}{\frac{\gamma}{\lambda} z + \frac{\delta}{\lambda}}\right) \quad \text{et} \quad \left(z, \frac{\alpha\lambda^2 z + \beta\lambda^2}{\frac{\gamma}{\lambda^2} z + \frac{\delta}{\lambda^2}}\right)$$

seront les substitutions fuchsiennes correspondant respectivement à AB et à $AB^2$, de sorte qu'on aura

$$\left(\lambda + \frac{1}{\lambda}\right) = [B], \qquad \alpha + \delta = [A],$$
$$\alpha\lambda + \frac{\delta}{\lambda} = [AB], \qquad \alpha\lambda^2 + \frac{\delta}{\lambda^2} = [AB^2].$$

On en tire aisément, par l'élimination de $\alpha$, $\delta$ et $\lambda$,

$$[AB][B] = [A] + [AB^2].$$

Si, dans la formule précédente, on change A en $AB^n$, il vient

$$[AB^{n+2}] = [AB^{n+1}][B] - [AB^n].$$

C'est une formule de récurrence qui permet de calculer $[AB^n]$, où $n$ est un entier quelconque positif ou négatif, quand on connaît $[A]$, $[B]$ et $[AB]$.

Aussi, connaissant $[A]$, $[B]$ et $[AB]$, nous pouvons en déduire $|AB^n|$, et par conséquent $[B^nA]$, puisque

$$[B^nA] = [AB^n].$$

Nous connaissons ainsi

$$[B^nA], \quad [B^n] \quad \text{et} \quad [A],$$

ce qui permet de calculer $[B^nA^m]$, où $m$ et $n$ sont des entiers quelconques, par la formule de récurrence

$$|B^nA^{m+2}| = [B^nA^{m+1}][A] - [B^nA^m].$$

Nous avons d'ailleurs

$$[B^nA^m] = [A^mB^n] = [A^{m-p}B^nA^p] = [B^pA^mB^{n-p}],$$

ce qui permet de calculer

$$|A^mB^nA^p| \quad \text{et} \quad |B^mA^nB^p|,$$

où $m$, $n$, $p$ sont des entiers quelconques.

Cherchons maintenant

$$[A^mB^nA^pB^q],$$

où les quatre exposants sont entiers. On voit d'abord que, par notre formule de récurrence, nous pourrons calculer cet invariant, quel que soit $q$, pourvu que nous connaissions, outre $[B]$,

$$|A^mB^nA^p] \quad \text{et} \quad |A^mB^nA^pB].$$

La première de ces deux expressions est connue d'après ce qui précède; il reste donc à calculer

$$[A^m B^n A^p B] = [BA^m B^n A^p].$$

On verrait de même que le calcul de

$$[BA^m B^n A^p]$$

se ramène à celui de

$$[BA^m B^n A] = [ABA^m B^n],$$

qui se ramène lui-même à celui de

$$[ABA^m B] = [BABA^m]$$

ou enfin à celui de

$$[BABA].$$

Or, ce dernier invariant est connu, puisque c'est celui de $(BA)^2$ et que nous connaissons celui de BA.

Ce qui précède suffit pour faire comprendre comment on calculerait l'invariant d'une combinaison quelconque des deux substitutions A et B.

Imaginons maintenant que A et B sont des substitutions à coefficients entiers et de déterminant 1. Il en sera de même de toutes leurs combinaisons. Alors, dans la formule

$$[AB^2] + [A] = [AB][B],$$

les deux termes du premier membre, ainsi que le terme unique du second membre, devront être la racine carrée d'un entier.

Mais il est aisé de voir que, si l'on a

$$\sqrt{\mu_1} + \sqrt{\mu_2} = \sqrt{\mu_3}$$

($\mu$ étant des entiers), les trois expressions

$$\sqrt{\mu_2 \mu_3}, \quad \sqrt{\mu_3 \mu_1}, \quad \sqrt{\mu_1 \mu_2}$$

devront être des entiers.

Il suit de là que les produits

$$[A][AB^2],\quad [A][AB][B],\quad [AB^2][AB][B]$$

sont entiers.

Il est aisé d'en déduire que si [A] est égal à un nombre commensurable multiplié par $\sqrt{\alpha}$, et [B] égal à un nombre commensurable multiplié par $\sqrt{\beta}$, [AB] devra être égal à un nombre commensurable multiplié par $\sqrt{\alpha\beta}$, et $[AB^2]$ à un nombre commensurable multiplié par $\sqrt{\alpha}$ ou, ce qui revient au même, à un nombre commensurable multiplié par $\sqrt{\alpha\beta^2}$.

Plus généralement, on aura

$$[A^m B^n A^p B^q] = \mu_1 \sqrt{\alpha^{m+p}\beta^{n+q}} = \mu_2 \sqrt{\alpha^h \beta^k},$$

$\mu_1$ et $\mu_2$ étant commensurables, et $h$ et $k$ étant égaux soit à 0, soit à 1, suivant la parité des deux nombres $m+p$ et $n+q$, et de telle sorte que

$$h \equiv m+p, \qquad k \equiv n+q \qquad (\text{mod } 2).$$

Cela peut s'énoncer encore d'une autre manière.

Considérons le groupe dérivé des deux substitutions linéaires A et B. Pour que toutes les substitutions de ce groupe aient leurs invariants égaux à la racine carrée d'un entier, il faut et il suffit que

$$[A]^2,\quad [B]^2 \quad \text{et} \quad [A][B][AB]$$

soient des entiers.

Nous allons maintenant envisager un groupe dérivé de trois substitutions linéaires A, B et C. Je dis que l'on peut, à l'aide de la relation de récurrence démontrée plus haut, calculer les invariants de toutes les substitutions de ce groupe, à l'aide de sept invariants

$$[A],\quad [B],\quad [C],\quad [AB],\quad [BC],\quad [CA],\quad [ABC].$$

Pour le démontrer, je rappelle d'abord que cette relation de récurrence permet (M, N, P étant des substitutions quelconques) de calculer

$$[MN^p]$$

($p$ entier positif ou négatif), quand on connaît

$$[M],\quad [N]\quad \text{et}\quad [MN],$$

ou plus généralement de calculer

$$[MN^pP]$$

quand on connaît

$$[MP],\quad [N]\quad \text{et}\quad [MNP].$$

Elle permet ainsi, connaissant [A], [B] et [AB], de calculer les invariants de toutes les combinaisons de A et de B, ou, à l'aide de nos sept invariants, de calculer ceux de toutes les combinaisons A, B et C, où l'une de ces trois substitutions n'entre pas.

Je dis qu'on pourra trouver de même

$$[A^mB^nC^p].$$

En effet, le calcul de cet invariant se ramène à celui de $[A^mB^n]$, qui est connu et à celui de $[A^mB^nC]$. Ce dernier se ramène à $[A^mC]$, qui est connu, et à $[A^mBC]$. Ce dernier, à son tour, se ramène à [BC] et à [ABC], qui sont tous deux supposés connus.

Considérons maintenant une combinaison quelconque

$$[A^mB^nC^pB^qA^rC^sB^tC^u].$$

On ramènera, par le même procédé, le calcul de cet invariant à celui de

$$[ABCBACBC],$$

où les lettres sont restées les mêmes et dans le même ordre, mais où tous les exposants sont réduits à l'unité.

Je dis maintenant qu'on peut ramener le calcul de cet invariant à celui de

$$[ABC(AB)CBC],$$

où deux des lettres sont permutées.

En effet, notre formule de récurrence permet de réduire le calcul de

$$[ABC(BA)CBC]$$

à celui de

$$[ABC.CBC]$$

(où le nombre des lettres est moindre, et que, par conséquent, on peut supposer préalablement calculé) et à celui de

$$[ABC(BA)^{-1}CBC] = [ABCA^{-1}B^{-1}CBC];$$

en réduisant les exposants à l'unité, ce dernier devient

$$[ABCABCBC].$$

Il est clair qu'en appliquant d'une façon convenable le double procédé qui permet de permuter deux lettres quelconques et de réduire les exposants à l'unité, on arrivera à réduire de plus en plus le nombre des lettres de telle façon qu'on sera ramené finalement à l'invariant connu $[ABC]$.

On connaîtra donc ainsi l'invariant d'une substitution quelconque du groupe.

On peut en conclure ce qui suit :

Pour que toutes les substitutions du groupe aient pour invariant la racine carrée d'un entier (ce qui arrive nécessairement quand les substitutions A, B, C ont leurs coefficients entiers), il faut et il suffit que

$$[A]^2 \quad [B]^2, \quad [C]^2, \quad [A][B][AB], \quad [B][C][BC], \quad [C][A][CA]$$

et

$$[A][B][C][ABC]$$

soient des entiers.

Mais nos sept invariants eux-mêmes ne sont pas indépendants les uns des autres. Il y a entre eux une relation algébrique.

Cette relation se présente sous une forme plus symétrique, quand on considère, au lieu de nos sept invariants, les sept invariants suivants (ce

qui revient d'ailleurs au même)

$$[A]=\alpha, \quad [B]=\beta, \quad [C]=\beta', \quad [C^{-1}B^{-1}]=\beta'',$$
$$[BA]=\gamma, \quad [CA]=\gamma', \quad [C^{-1}B^{-1}A]=\gamma''.$$

J'ai représenté, pour abréger, les sept invariants par les lettres $\alpha$, $\beta$, $\gamma$.

La relation s'écrit alors

$$\begin{aligned}&\alpha^2+\beta^2+\gamma^2+\beta'^2+\gamma'^2+\beta''^2+\gamma''^2-4\\&\quad=\alpha\beta\gamma+\alpha\beta'\gamma'+\alpha\beta''\gamma''+\beta\gamma'\gamma''+\beta'\gamma\gamma''+\beta''\gamma\gamma'\\&\qquad-\alpha\beta\beta'\gamma''-\alpha\beta\beta''\gamma''-\alpha\beta'\beta''\gamma+\alpha^2\beta\beta'\beta''-\beta\beta'\beta''.\end{aligned}$$

On arrive à un résultat analogue dans le cas d'un groupe dérivé de quatre substitutions ou d'un plus grand nombre.

*Soit un groupe dérivé de n substitutions*

$$A_1, \quad A_2, \quad \ldots, \quad A_n.$$

*Pour que toutes les substitutions du groupe aient pour invariant la racine carrée d'un entier, il faut et il suffit que*

$$|A_1|^2, \quad |A_2|^2, \quad \ldots, \quad |A_n|^2,$$

*ainsi que toutes les combinaisons*

$$|A_1^{\varepsilon_1}A_2^{\varepsilon_2}A_3^{\varepsilon_3}\ldots A_n^{\varepsilon_n}|\,|A_1|^{\varepsilon_1}|A_2|^{\varepsilon_2}\ldots|A_n|^{\varepsilon_n}$$

(*où les exposants* $\varepsilon$ *sont égaux soit à* 0, *soit à* 1), *soient des entiers.*

## VI. — Réduction des substitutions.

Voici la question que je me propose de traiter dans ce paragraphe.

Soit S une substitution à coefficients entiers et de déterminant 1; soit T une autre substitution à coefficients entiers et de déterminant 1;

je dirai que la substitution S et sa transformée

$$T^{-1}ST$$

sont homologues et appartiennent à la même classe.

Cela posé, parmi toutes les substitutions d'une même classe, il y en a une qui est plus simple que toutes les autres, et que j'appellerai *substitution réduite*.

On peut se proposer, étant donnée une substitution S, de trouver la substitution réduite qui appartient à la même classe, ou, en d'autres termes, de *réduire* la substitution S.

On voit d'abord tout de suite que deux substitutions homologues ont mêmes multiplicateurs. Je supposerai, comme je l'ai fait jusqu'ici, qu'un des multiplicateurs est égal à 1, ainsi que le produit des deux autres.

Il résulte de là qu'il existera une forme linéaire

$$\lambda_1 x + \lambda_2 y + \lambda_3 z,$$

à coefficients entiers et premiers entre eux, qui sera inaltérée par la substitution.

On peut alors former une substitution linéaire

$$T = \begin{vmatrix} \lambda_1 & \lambda_2 & \lambda_3 \\ \mu_1 & \mu_2 & \mu_3 \\ \nu_1 & \nu_2 & \nu_3 \end{vmatrix}$$

à coefficients entiers et de déterminant 1.

La substitution $T^{-1}ST$, transformée de S par T, sera alors de la forme

$$S' = \begin{vmatrix} 1 & 0 & 0 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix},$$

ce qui constitue une première réduction.

Supposons d'abord que $b_1$ et $c_1$ soient nuls, et que la substitution S

s'écrive

$$S = \begin{vmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{vmatrix}$$

avec la condition

$$ad - bc = 1.$$

Si l'on transforme alors S par une substitution T de la forme

$$T = \begin{vmatrix} 1 & 0 & 0 \\ 0 & \lambda & \mu \\ 0 & \lambda' & \mu' \end{vmatrix}$$

à coefficients entiers et de déterminant 1, la substitution S conservera la même forme après cette transformation.

Envisageons la forme quadratique binaire

$$\psi = c\xi^2 + (d-a)\xi\eta - b\eta^2,$$

qui n'est pas altérée par la substitution linéaire

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix}.$$

Que deviendra cette forme lorsque l'on remplacera S par sa transformée

$$T^{-1}ST?$$

Tout se passera comme si l'on avait appliqué à cette forme la substitution

$$\begin{vmatrix} \lambda & \mu \\ \lambda' & \mu' \end{vmatrix}.$$

D'où cette conclusion :

Pour que deux substitutions

$$S = \begin{vmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{vmatrix}, \qquad S' = \begin{vmatrix} 1 & 0 & 0 \\ 0 & a' & b' \\ 0 & c' & d' \end{vmatrix}$$

appartiennent à la même classe, il faut et il suffit que les deux formes

$$c\xi^2+(d-a)\xi\eta-b\eta^2$$

et

$$c'\xi^2+(d'-a')\xi\eta-b'\eta^2$$

soient équivalentes.

Nous sommes donc conduits à dire par définition que la substitution S est réduite quand la forme $\psi$ l'est elle-même.

La somme des multiplicateurs de S est

$$a+d+1,$$

et son invariant

$$\sqrt{a+d+2}.$$

La substitution est elliptique si

$$(a+d)^2<4, \qquad \text{d'où} \qquad (a+d)=0, \qquad (a+d)=\pm 1,$$

parabolique si

$$(a+d)^2=4, \qquad \text{d'où} \qquad a+d=\pm 2,$$

hyperbolique si

$$(a+d)^2>4.$$

La forme $2\psi$ a pour discriminant

$$(d-a)^2+4bc=(a+d)^2-4.$$

Il résulte de là que le discriminant de $\psi$ est fonction de l'invariant de S, et par conséquent que *les substitutions* S *d'invariant donné se répartissent en un nombre fini de classes.*

La substitution S sera elliptique si $\psi$ est définie. Les conditions de réduction pourront alors s'écrire

$$|d-a|<|b|<|c|;$$

$b$ et $c$ seront d'ailleurs toujours de signe contraire.

La substitution S sera hyperbolique si $\psi$ est indéfinie. Il arrive alors que chaque classe de substitutions contiendra plusieurs réduites, comme cela arrive pour les formes indéfinies.

Nous prendrons alors pour unique condition de réduction que $b$ et $c$ soient de même signe.

Enfin la substitution S sera parabolique si $\psi$ se réduit à un carré parfait. Nous dirons alors que $\psi$ est réduite si elle s'écrit $\psi = c\xi^2$, de telle sorte que les conditions de réduction de S s'expriment comme il suit :

$$b = 0, \qquad \text{d'où} \qquad a = d = \pm 1.$$

Énumérons maintenant les substitutions elliptiques réduites.

Pour $a + d = 0$, le discriminant de $2\psi$ est égal à $-4$, et celui de $\psi$ à $-1$. Si $\psi$ est une réduite, on a donc

$$\psi = \xi^2 + \eta^2.$$

La substitution réduite S s'écrit alors

$$S_1 = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{vmatrix}.$$

Pour $a + d = 1$, le discriminant de $2\psi$ est égal à $-3$, et cette forme $2\psi$ est improprement primitive. On a alors, si $2\psi$ est réduite,

$$\psi = \xi^2 + \xi\eta + \eta^2,$$

de sorte que l'on trouve pour S

$$S_2 = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 1 \end{vmatrix}.$$

Pour $a + d = -1$, on trouve encore

$$\psi = \xi^2 + \xi\eta + \eta^2,$$

ce qui donne

$$S_3=\begin{vmatrix} 1 & 0 & 0 \\ 0 & -1 & -1 \\ 0 & 1 & 0 \end{vmatrix}.$$

Nous classerons encore parmi les substitutions elliptiques la substitution suivante

$$S_4=\begin{vmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{vmatrix},$$

pour laquelle la forme $\psi$, étant identiquement nulle, ne peut être regardée ni comme définie, ni comme indéfinie.

Il y aura donc en tout quatre classes de substitutions elliptiques.

Nous remarquerons que la substitution $S_3$ n'est autre chose que le carré de la substitution $S_2$.

Quant aux substitutions paraboliques réduites, elles s'écriront, soit

$$S_5=\begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & c & 1 \end{vmatrix},$$

soit

$$S_6=\begin{vmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & c & -1 \end{vmatrix},$$

où $c$ est un entier quelconque.

Ne supposons plus maintenant que $b_1$ et $c_1$ sont nuls et écrivons notre substitution S sous la forme suivante

$$\begin{vmatrix} 1 & 0 & 0 \\ b_1 & a & b \\ c_1 & c & d \end{vmatrix},$$

avec la condition

$$ad - bc = 1.$$

On peut supposer que la réduction a été faite comme si $b_1$ et $c_1$ étaient nuls et par conséquent que l'on a

$$|d - a| < |b| < |c| \tag{1}$$

ou

$$d = a = -1, \qquad b = c = 0 \tag{2}$$

si la substitution est elliptique;

$$bc > 0 \tag{3}$$

si elle est hyperbolique, et

$$b = 0 \tag{4}$$

si elle est parabolique.

Il s'agit maintenant de réduire autant que possible les coefficients $b_1$ et $c_1$.

Pour cela, écrivons les équations qui définissent la substitution S de la façon suivante :

$$\begin{aligned} x' &= x, \\ y' &= b_1 x + ay + bz, \\ z' &= c_1 x + cy + dz. \end{aligned}$$

Posons ensuite

$$y = y_1 + \alpha x, \qquad z = z_1 + \beta x;$$

d'où

$$y' = y'_1 + \alpha x', \qquad z = z'_1 + \beta x'.$$

Les deux dernières équations s'écriront alors

$$\begin{aligned} y'_1 &= x[b_1 + (a-1)\alpha + b\beta \qquad ] + ay_1 + bz_1, \\ z'_1 &= x[c_1 + c\alpha \qquad + (d-1)\beta] + cy_1 + dz_1. \end{aligned}$$

En d'autres termes, les coefficients de la substitution S n'ont pas changé par cette transformation, sauf que $b_1$ et $c_1$ sont devenus

$$b_1+(a-1)\alpha+b\beta,$$
$$c_1+c\alpha+(d-1)\beta.$$

Le problème consiste à déterminer les entiers $\alpha$ et $\beta$ pour diminuer autant que possible $b_1$ et $c_1$. Je dirai que deux systèmes de nombres $(b_1, c_1)$ et $(b'_1, c'_1)$ appartiennent à une même classe si l'on peut trouver deux entiers $\alpha$ et $\beta$, tels que

$$b'_1=b_1+(a-1)\alpha+b\beta,$$
$$c'_1=c_1+c\alpha+(d-1)\beta.$$

Le nombre des classes entre lesquelles se répartissent les systèmes $(b_1, c_1)$ est alors égal à

$$\left|\begin{matrix}(a-1) & b\\ c & (d-1)\end{matrix}\right|=|2-a-d|.$$

Parmi les systèmes $(b_1, c_1)$ appartenant à une même classe, il y en aura un que l'on regardera comme plus simple que les autres et que l'on appellera système réduit; le nombre des systèmes réduits est fini.

Alors, pour qu'une substitution

$$\left|\begin{matrix}1 & 0 & 0\\ b_1 & a & b\\ c_1 & c & d\end{matrix}\right|$$

soit réduite, il faudra non seulement que les quatre entiers $a$, $b$, $c$, $d$ satisfassent aux conditions (1), (2), (3) ou (4) énoncées plus haut, mais encore que le système $(b_1, c_1)$ soit réduit.

Nous avons vu plus haut que, si $b_1$ et $c_1$ sont nuls, les substitutions S d'invariant donné se répartissent en un nombre fini de classes. D'après ce qui précède, cela est encore vrai si $b_1$ et $c_1$ ne sont pas nuls.

Revenons au cas des substitutions elliptiques et cherchons à déterminer les systèmes réduits $(b_1, c_1)$. Il y a quatre cas à considérer, puisque les substitutions elliptiques, quand $b_1 = c_1 = 0$, se répartissent en quatre classes.

*Premier cas :*

$$a = d = 0, \qquad b = -1, \qquad c = 1;$$

$2 - a - d = 2$; il y a deux systèmes réduits

$$b_1 = c_1 = 0, \qquad b_1 = 1, \qquad c_1 = 0.$$

*Deuxième cas :*

$$a = 0, \qquad c = d = 1, \qquad b = -1;$$

$2 - a - d = 1$; il n'y a qu'un système réduit

$$b_1 = c_1 = 0.$$

*Troisième cas :*

$$a = b = -1, \qquad c = 1, \qquad d = 0;$$

$2 - a - d = 3$; il y a trois systèmes réduits

$$b_1 = 0, \quad c_1 = 0, \qquad b_1 = 1, \quad c_1 = 0, \qquad b_1 = 2, \quad c_1 = 0.$$

*Quatrième cas :*

$$a = d = -1, \qquad b = c = 0;$$

$2 - a - d = 4$; il y a quatre systèmes réduits

$$b_1 = 0 \text{ ou } 1, \qquad c_1 = 0 \text{ ou } 1.$$

Mais, si nous observons qu'en appliquant à $y$ et $z$ une transformation linéaire, on fait subir cette même transformation à $b_1$ et $c_1$ sans changer d'ailleurs les autres coefficients de S; nous verrons que ces quatre systèmes peuvent être réduits à deux.

Il y a donc huit substitutions elliptiques réduites que je vais énumérer.

$$S_1=\begin{vmatrix}1&0&0\\0&0&-1\\0&1&0\end{vmatrix},\qquad S'_1=\begin{vmatrix}1&0&0\\1&0&-1\\0&1&0\end{vmatrix},$$

$$S_2=\begin{vmatrix}1&0&0\\0&0&-1\\0&1&1\end{vmatrix},\qquad S_3=\begin{vmatrix}1&0&0\\0&-1&-1\\0&1&0\end{vmatrix},$$

$$S'_3=\begin{vmatrix}1&0&0\\1&-1&-1\\0&1&0\end{vmatrix},\qquad S''_3=\begin{vmatrix}1&0&0\\2&-1&-1\\0&1&-0\end{vmatrix},$$

$$S_4=\begin{vmatrix}1&0&0\\0&-1&0\\0&0&-1\end{vmatrix},\qquad S'_4=\begin{vmatrix}1&0&0\\1&-1&0\\1&0&-1\end{vmatrix}.$$

On peut faire une classification analogue pour les substitutions paraboliques, mais le nombre des classes est infini; on doit envisager d'abord le cas où les trois multiplicateurs sont égaux à 1; on trouve alors que la substitution doit être de la forme

$$S'_3=\begin{vmatrix}1&0&0\\a&1&0\\b&c&1\end{vmatrix}.$$

Les transformations qu'on peut faire ne peuvent changer la valeur de $a$ et de $c$. La seule réduction possible, c'est d'amener $b$ à être plus petit que le plus grand commun diviseur de $a$ et de $c$ (et par conséquent à être nul, si $a$ et $c$ sont premiers entre eux); on peut également supposer que $c$ n'est pas nul.

On considérera ensuite le cas où deux des multiplicateurs sont égaux à $-1$; on a alors

$$a=d=1,\qquad 2-a-d=4.$$

On a donc quatre systèmes réduits $(b_1, c_1)$ et quatre substitutions réduites

$$S_6 = \begin{vmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & c & -1 \end{vmatrix}, \qquad S'_6 = \begin{vmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 1 & c & -1 \end{vmatrix},$$

$$S''_6 = \begin{vmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & c & -1 \end{vmatrix}, \qquad S'''_6 = \begin{vmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & c & -1 \end{vmatrix}.$$

## VII. — Substitutions elliptiques.

Nous allons chercher dans ce paragraphe quelle est la condition pour qu'une forme quadratique admette une substitution semblable elliptique, et d'abord quelles sont les formes qui ne sont pas altérées par les huit substitutions réduites $S_1$, $S'_1$, $S_2$, $S_3$, $S'_3$, $S''_3$, $S_4$ et $S'_4$ définies dans le paragraphe précédent.

On a entre ces diverses substitutions les relations suivantes

$$S_1^2 = S_1, \quad S_1'^2 = S'_1, \quad S_1^2 = 1, \quad S_1'^2 = 1, \quad S_2^2 = S_3,$$
$$S_2^3 = S_1, \quad S_3^3 = 1, \quad S_3'^3 = 1, \quad S_3''^3 = 1 \quad S_2^6 = 1.$$

Cela posé, nous résoudrons successivement les problèmes suivants :

1° *Formes inaltérées par* $S_1$. — Ce sont les formes

$$Ax^2 + A'y^2 + 2Byz + A''z^2;$$

2° *Formes inaltérées par* $S'_1$. — Ce sont les formes

$$Ax^2 + A'y^2 + 2Byz + A''z^2 - (A' + B)xy - (A'' + B)xz,$$

où l'on doit avoir

$$A' \equiv A'' \equiv B \pmod 2.$$

3° *Formes inaltérées par* $S_1$ *et par conséquent par* $S_4$. — Ce sont les formes

$$Ax^2 + A'(y^2 + z^2).$$

4° *Formes inaltérées par* $S'_1$ *et par conséquent par* $S'_4$. — Ce sont les formes

$$Ax + A'(y^2 + z^2 - xy - xz),$$

où A′ doit être pair.

5° *Formes inaltérées par* $S_2$ *et par conséquent par* $S_3$ *et par* $S_4$. — Ce sont les formes

$$Ax^2 + A'(y^2 + yz + z^2),$$

où A′ doit être pair.

Il n'y a d'ailleurs pas d'autre forme inaltérée par $S_3$.

6° *Formes inaltérées par* $S'_3$. — Ce sont les formes

$$Ax^2 + A'(y^2 + yz + z^2 - xy - xz),$$

où A′ est pair.

7° *Formes inaltérées par* $S''_3$. — Ce sont les formes

$$Ax^2 + A'(y^2 + yz + z^2 - 2xy - 2xz),$$

où A′ est pair.

Nous allons chercher maintenant si une forme quadratique donnée admet une substitution elliptique; pour cela, il faut évidemment et il suffit qu'elle soit équivalente à l'une des sept formes que je viens d'énumérer.

Je dis d'abord qu'on pourra reconnaître s'il en est ainsi par un nombre limité d'essais.

En effet, prenons d'abord la première forme

$$Ax^2 + A'y^2 + 2Byz + A''z^2.$$

Elle a pour déterminant

$$A(A'A'' - B^2).$$

On décomposera donc le discriminant Δ de la forme donnée en deux facteurs

$$\Delta = AD,$$

ce qui ne peut se faire que d'un nombre limité de manières. On con-

struira ensuite une forme binaire *réduite*

$$A'y^2 + 2Byz + A''z^2$$

de déterminant D, ce qui ne peut se faire encore que d'un nombre limité de manières. On n'a plus ensuite qu'à examiner si la forme

$$Ax^2 + A'y^2 + 2Byz + A''z^2,$$

ainsi construite, est équivalente à la forme donnée.

La même méthode s'applique sans changement aux troisième et cinquième formes

$$Ax^2 + A'(y^2 + z^2) \quad \text{et} \quad Ax^2 + A'(y^2 + yz + z^2).$$

Mais le nombre des essais est encore plus limité; le déterminant de la troisième forme est égal à $AA'^2$ et celui de la troisième à $3AB^2$ (en posant $A' = 2B$), de sorte qu'une forme ne peut admettre une substitution semblable équivalente à $S_2$ que si son discriminant est divisible par 3.

En ce qui concerne la seconde forme

$$Ax^2 + A'y^2 + 2Byz + A''z^2 - (A' + B)xy - (A'' + B)xz,$$

que l'on peut écrire

$$(1) \quad Ax^2 - (2B'' + B)y^2 + 2Byz - (2B' + B)z^2 + 2B''xy + 2B'xz,$$

le nombre des essais est encore limité. En effet, son déterminant s'écrit

$$(2A + B' + B'')(2B'B'' + BB' + BB'').$$

On décomposera donc le déterminant $\Delta$ en deux facteurs

$$\Delta = CD.$$

Alors 2D désigne le déterminant de la forme binaire

$$-(2B'' + B)y^2 + 2Byz - (2B' + B)z^2.$$

Ces formes binaires, qu'on peut être conduit à essayer, se répartissent donc en un nombre fini de classes.

Si nous faisons subir à la forme (1) une transformation linéaire de déterminant 2, en posant

$$y = y_1 + x_1, \qquad z = z_1 + x_1, \qquad x = 2x_1,$$

elle deviendra

$$(2)\quad (4A + 2B' + 2B'')x_1^2 - (2B'' + B)y_1^2 + 2B + y_1 z_1 - (2B' + B)z_1^2.$$

On peut, de plus, supposer que la forme binaire

$$(3)\qquad (2B'' + B)y^2 - 2Byz + (2B' + B)z^2$$

a été réduite autant que possible par une substitution ne portant que sur $y$ et $z$.

Si B est pair, on peut appliquer à cette forme binaire une substitution linéaire quelconque sans faire cesser la particularité qui la caractérise, à savoir que les coefficients de $y^2$, de $z^2$ et de $2yz$ sont de même parité.

Nous pouvons donc toujours supposer que cette forme est réduite au sens ordinaire du mot, c'est-à-dire, si nous la supposons définie, que l'on a

$$|\ 2B\ | < |\ 2B'' + B\ | < |\ 2B' + B\ |.$$

On ne pourra donc former qu'un nombre fini de formes (2) et, par conséquent, qu'un nombre fini de formes (1) satisfaisant à la fois aux conditions

$$\Delta = (2A + B' + B'')(2B'B'' + BB' + BB''),$$
$$B \equiv 0 \pmod 2, \qquad |\ 2B\ | < |\ 2B'' + B\ | < |\ 2B' + B\ |.$$

On n'aura donc qu'un nombre limité d'essais à faire pour reconnaître si l'une de ces formes est équivalente à la forme donnée.

Supposons maintenant que B soit impair. On ne peut pas appliquer à notre forme binaire

$$(3)\qquad (2B'' + B)y^2 - 2Byz + (2B' + B)z^2$$

une substitution linéaire quelconque sans que les trois coefficients de $y^2$, de $2yz$ et de $z^2$ cessent d'être tous trois impairs. Pour qu'une substitution

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}$$

ne fasse pas cesser cette particularité, il faut que l'on ait

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \equiv \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} \quad \text{ou} \quad \equiv \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} \pmod 2.$$

Les substitutions qui satisfont à l'une de ces deux conditions forment un groupe G qui est un sous-groupe à congruences du groupe arithmétique.

Nous n'avons donc plus ici le droit de supposer que la forme (3) est réduite au sens ordinaire du mot, c'est-à-dire par rapport au groupe arithmétique, mais seulement qu'elle est réduite par rapport au groupe G.

Il est aisé de voir que les conditions de réduction s'écrivent alors

$$|B| < |2B'' + B| < |2B' + B|.$$

On ne pourra évidemment trouver qu'un nombre limité de formes (2) ou (1) satisfaisant simultanément aux conditions

$$\Delta = (2A + B' + B'')(2B'B'' + BB' + BB''),$$
$$B \equiv 1 \pmod 2, \qquad |B| < |2B'' + B| < |2B' + B|.$$

On n'aura donc encore qu'un nombre limité d'essais à faire pour reconnaître si l'une de ces formes est équivalente à la forme donnée.

Ce que je viens de dire s'applique sans changement à la forme

$$Ax^2 + A'(y^2 + z^2 - xy - xz)$$

reproductible par $S_1'$.

Il nous reste à examiner comment on pourra reconnaître si une forme donnée est susceptible d'être reproduite par une substitution homo-

logue à $S'_3$ ou à $S''_3$, c'est-à-dire si elle est équivalente à l'une des formes

$$(4) \qquad Ax^2 + 2B(y^2 + yz + z^2 - \beta xy - \beta xz),$$

où $\beta = 1$ ou $2$.

J'appellerai d'abord l'attention sur l'effet que produit sur cette forme la substitution suivante de déterminant 3

$$x = 3x_1, \qquad y = y_1 + \beta x_1, \qquad z = z_1 + \beta x_1.$$

La forme devient

$$(9A - 6B\beta^2)x_1^2 + 2B(y_1^2 + y_1 z_1 + z_1^2).$$

Le déterminant de la forme (4) est, d'ailleurs, égal à

$$3AB^2 - 2B^3\beta^2,$$

c'est-à-dire à

$$3AB^2 - 2B^3 \quad \text{ou} \quad 3AB^2 - 8B^3,$$

selon que $\beta$ est égal à 1 ou à 2.

Il est clair qu'on ne peut trouver que d'un nombre fini de manières deux nombres entiers A et B satisfaisant à l'une des deux conditions

$$3AB^2 - 2B^3 = \Delta \qquad \text{ou} \qquad 3AB^2 - 8B^3 = \Delta.$$

On n'aura donc qu'un nombre limité d'essais à faire pour reconnaître si une forme donnée de déterminant $\Delta$ est équivalente à l'une des formes (4).

Ainsi, dans tous les cas possibles, le nombre des essais à faire est limité, et il peut être diminué encore par la considération des ordres et des genres.

Il est clair, d'après ce qui précède et sans qu'il soit nécessaire d'insister, que toutes les formes n'admettront pas de substitution semblable elliptique.

Mais, en revanche, on voit tout de suite qu'une forme quadratique

quelconque F est toujours commensurable avec une forme qui admet une substitution semblable elliptique. Et, en effet, quelle que soit la forme F, on peut toujours trouver une substitution à coefficients commensurables T′, telle que

$$FT' = Ax^2 + By^2 + Cz^2.$$

Cette forme FT′, commensurable avec F, admet la substitution elliptique $S_4$.

Cherchons maintenant quelles sont les formes qui admettent une des substitutions paraboliques $S'_5$, $S_6$, $S'_6$ $S''_6$ et $S'''_6$.

En premier lieu, les seules formes qui sont reproduites par une des quatre substitutions $S_6$, $S'_6$, $S''_6$ et $S'''_6$ ont leur discriminant nul. Nous devons donc les laisser de côté et ne nous occuper que des formes reproduites par

$$S'_5 = \begin{vmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{vmatrix}.$$

Ces formes s'écriront

$$Ax^2 + A'y^2 + 2B'xz + 2B''xy \tag{5}$$

avec les conditions

$$Aa^2 + 2B'b + 2B''a = A'a + B'c = 0.$$

Pour qu'une forme quadratique admette une substitution parabolique, il faut et il suffit qu'elle soit équivalente à la forme (5) ou, en d'autres termes, qu'elle soit susceptible de représenter 0, conformément aux conditions du § CCXCIX des *Disquisitiones arithmeticæ*.

Cela est conforme à un résultat déjà obtenu par M. Selling.

## VIII. — Résumé.

Nous pouvons maintenant résumer ainsi les résultats encore très incomplets que nous avons obtenus.

Au groupe des substitutions à coefficients entiers qui n'altèrent pas une forme quadratique donnée F correspond toujours un groupe fuchsien qui le détermine entièrement.

Les formes F peuvent d'abord se répartir en quatre catégories :

1° Celles qui n'admettent ni substitutions elliptiques, ni substitutions paraboliques;

2° Celles qui admettent des substitutions elliptiques, mais pas de substitutions paraboliques;

3° Celles qui admettent des substitutions paraboliques, mais pas de substitutions elliptiques;

4° Celles qui admettent à la fois des substitutions elliptiques et paraboliques.

Nous avons vu, dans le paragraphe précédent, comment un nombre limité d'essais permet de reconnaître à laquelle de ces quatre catégories appartient une forme donnée.

Si la forme F est de la première ou de la deuxième catégorie, son groupe fuchsien principal sera de la première famille; si F est de la troisième catégorie, son groupe fuchsien est de la deuxième famille; si F est de la quatrième catégorie, son groupe fuchsien est de la sixième famille.

Si la forme F est de la première catégorie, le polygone générateur de son groupe fuchsien a $4p$ côtés, les côtés opposés étant conjugués. Les $4p$ sommets forment un seul cycle, et la somme des angles est égale à $2\pi$.

Si F est de la deuxième catégorie, les sommets du polygone générateur peuvent former plusieurs cycles. (Il convient d'ajouter que le plus souvent ils n'en forment qu'un seul et qu'il n'y aura plusieurs cycles que dans des cas exceptionnels.) Pour reconnaître combien ces sommets forment de cycles, on construira les formes

$$Ax^2 + A'y^2 + A''z^2 + 2Byz$$

(la forme binaire $A'y^2 + A''z^2 + 2Byz$ étant réduite) ou bien encore les formes (1) et (4) du paragraphe précédent. Si la forme F est équivalente à $n$ des formes ainsi construites, les sommets du polygone générateur formeront $n$ cycles.

La somme des angles de l'un quelconque de ces cycles sera égale à $\pi$, $\frac{\pi}{2}$, $\frac{\pi}{3}$ ou $\frac{2\pi}{3}$. Si F est équivalente à une forme reproductible par $S_1$ ou $S_1'$, la somme des angles du cycle correspondant sera $\pi$; si F est équivalente à une forme reproductible par $S_1$ ou $S_1'$, la somme des angles du cycle correspondant sera $\frac{\pi}{2}$; si F est équivalente à une forme reproductible par $S_2$, la somme des angles du cycle correspondant sera $\frac{\pi}{3}$; si, enfin, F est équivalente à une forme reproductible par $S_3'$ ou $S_3''$, la somme des angles du cycle correspondant sera $\frac{2\pi}{3}$.

Si F est de la troisième catégorie, les sommets du polygone générateur sont tous sur le cercle fondamental, et ils forment un ou plusieurs cycles (en général un seul), dont la somme des angles est nulle.

Si F est de la quatrième catégorie, les sommets du polygone générateur sont les uns sur le cercle fondamental, les autres à l'intérieur, et ils forment plusieurs cycles dont la somme des angles peut être 0, $\pi$, $\frac{\pi}{2}$, $\frac{\pi}{3}$ ou $\frac{2\pi}{3}$.

Nous avons rencontré aussi d'autres propriétés du groupe fuchsien principal d'une forme F. En premier lieu, les multiplicateurs des diverses substitutions devront satisfaire aux conditions exposées au § V. En second lieu, ce groupe fuchsien devra être commensurable avec ses transformés par une infinité de substitutions, correspondant aux substitutions fractionnaires étudiées au § IV.

Il me reste à parler des substitutions gauches.

Dans la théorie des groupes fuchsiens, on décompose le cercle fondamental en une infinité de polygones égaux entre eux au point de vue pseudogéométrique; les angles sont égaux entre eux au sens ordinaire du mot, et les côtés sont égaux à notre point de vue spécial, c'est-à-dire qu'ils ont même L.

Considérons une circonférence coupant orthogonalement le cercle fondamental, et supposons qu'on transforme un de nos polygones R par inversion (par rayons vecteurs réciproques) par rapport à cette circonférence. Nous dirons alors, au point de vue pseudogéométrique, que le polygone R et son transformé R′ sont symétriques par rapport à cette circonférence. Ces deux polygones auront mêmes angles et mêmes

côtés (à notre point de vue spécial), mais les éléments homologues seront disposés dans l'ordre inverse.

Si nous considérons ensuite un polygone R″, égal à R′ au point de vue pseudogéométrique, les deux polygones R et R″ auront aussi les éléments homologues égaux, mais disposés dans l'ordre inverse. Nous dirons alors qu'ils sont symétriques en grandeur, mais non en position.

Si la forme F admet une substitution gauche, on peut décomposer le cercle fondamental en une infinité de polygones curvilignes; deux quelconques de ces polygones sont égaux entre eux ou symétriques (en grandeur) au point de vue pseudogéométrique; deux polygones adjacents sont toujours symétriques, et la réunion de ces deux polygones adjacents symétriques constitue le polygone générateur du groupe fuchsien formé en ne considérant que les substitutions droites.

La substitution

$$S_4 = \begin{vmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{vmatrix}$$

peut être à volonté considérée comme droite ou gauche, puisqu'un de ses multiplicateurs est égal à $+1$, et deux à $-1$.

Nous avons vu que, pour savoir si la forme F est reproductible par une substitution homologue à $S_4$, il suffit de chercher si elle est équivalente à une forme, telle que

$$Ax^2 + A'y^2 + 2Byz + A''z^2.$$

Mais deux cas sont à distinguer : ou bien la forme binaire

$$A'y^2 + 2Byz + A''z^2$$

est définie, et alors nous regarderons la substitution $S_4$ comme droite et elliptique, ou bien cette forme binaire est indéfinie, et alors nous regarderons $S_4$ comme une substitution gauche.

On comprend ainsi ce qu'on doit entendre quand je dis que F est reproductible par une substitution gauche appartenant à la même classe que $S_4$. Si cela arrive, le polygone générateur peut se décom-

poser en deux polygones adjacents symétriques l'un de l'autre, non seulement en grandeur, mais encore en position, le côté commun servant d'axe de symétrie.

Les résultats que je viens d'exposer demanderaient évidemment à être complétés. Les propriétés nouvelles des groupes que nous avons étudiés ne suffisent pas pour les déterminer complètement; mais, en en faisant un usage judicieux, on peut notablement simplifier les anciens procédés de calcul qu'on employait autrefois pour former ces groupes.

## IX. — Généralisation du théorème d'addition.

Dans ce qui précède, je me suis efforcé de montrer la possibilité d'employer les fonctions fuchsiennes dans des questions d'Arithmétique. L'application inverse de l'Arithmétique à la théorie des fonctions fuchsiennes est au moins aussi féconde.

L'analogie des fonctions fuchsiennes et des fonctions elliptiques est évidente; les premières ne changent pas quand l'argument subit une substitution linéaire appartenant à un certain groupe, de même que les secondes ne changent pas quand l'argument augmente de certaines périodes. Il y a cependant une propriété des fonctions elliptiques qui ne s'étend pas immédiatement aux fonctions fuchsiennes, c'est le théorème d'addition.

Si l'on augmente l'argument d'une transcendante elliptique d'une quantité qui ne soit pas une période, il y a une relation algébrique entre l'ancienne et la nouvelle valeur de la transcendante. Si donc $F(z)$ est une fonction elliptique, il y aura une relation algébrique entre $F(z)$ et $F(z+h)$, $h$ étant une constante.

Voici quelle serait la généralisation la plus naturelle de cette propriété. Soient $F(z)$ une fonction fuchsienne, S une substitution linéaire n'appartenant pas à son groupe. Il devrait y avoir une relation algébrique entre $F(z)$ et $F(z, S)$. (Je désigne par $z$S, selon l'habitude, ce que devient $z$ quand on applique à cette variable la substitution S.) Il est aisé de voir que cette propriété ne peut subsister pour *toutes* les substitutions fuchsiennes S, c'est-à-dire pour toutes les substitutions linéaires S qui n'altèrent pas le cercle fondamental. D'autre part, il

arrivera, en général, que cette propriété n'appartiendra à aucune substitution fuchsienne; ce n'est donc que pour certaines fonctions fuchsiennes exceptionnelles qu'elle appartiendra à quelques substitutions fuchsiennes.

A ce double point de vue, on peut dire que le théorème d'addition des fonctions elliptiques ne s'étend pas, *en général,* aux fonctions fuchsiennes.

Je vais faire voir toutefois que, pour certaines fonctions fuchsiennes particulières $F(z)$, il existe une infinité de substitutions S, telles que $F(z)$ et $F(z, S)$ soient liées par une relation algébrique. Il est clair que, dans ce cas, ces substitutions S formeront un groupe.

Que faut-il pour qu'il en soit ainsi? Soit G le groupe de la fonction $F(z)$. La fonction $F(z, S)$ sera aussi une fonction fuchsienne, et son groupe sera le transformé de G par la substitution S, c'est-à-dire $S^{-1}GS$. Si les deux groupes G et $S^{-1}GS$ sont commensurables entre eux, leur groupe commun $g$ sera un sous-groupe d'indice fini pour chacun d'eux. Ce sera donc encore un groupe fuchsien. Mais alors on peut regarder $F(z)$ et $F(z, S)$ comme les fonctions fuchsiennes admettant le groupe $g$. Ces deux transcendantes seront donc liées par une relation algébrique.

D'où la conclusion suivante :

*Pour qu'il y ait une relation algébrique entre une fonction fuchsienne* $F(z)$ *de groupe* G *et sa transformée* $F(z, S)$ *par la substitution* S, *il faut et il suffit que les deux groupes* G *et* $S^{-1}GS$ *soient commensurables.*

Je citerai d'abord un premier exemple sur lequel je ne m'arrêterai pas. Soient G un groupe fuchsien et $g$ un second groupe fuchsien, sous-groupe du premier; soit $F(z)$ une fonction fuchsienne de groupe $g$. Soit enfin S une substitution appartenant à G, mais non à $g$. Je dis qu'il y aura une relation algébrique entre $F(z)$ et $F(z, S)$.

Soit, en effet, $\Phi(z)$ une fonction fuchsienne de groupe G; nous pourrons la regarder aussi comme une fonction de groupe $g$; elle sera donc liée algébriquement à $F(z)$. Mais nous pourrons de même regarder $\Phi(z)$ comme une fonction fuchsienne de groupe $S^{-1}gS$, puisque

$S^{-1}gS$ est aussi un sous-groupe de G. Donc $\Phi(z)$ sera aussi liée algébriquement à $F(z, S)$. Cela prouve que $F(z)$ et $F(z, S)$ sont liées algébriquement l'une à l'autre.

Les substitutions S forment, dans ce cas, un groupe G qui est discontinu. Aussi ce premier exemple n'offre-t-il pas grand intérêt. Nous le laisserons donc de côté pour ne nous occuper que des cas où les substitutions S, telles que $F(z)$ et $F(z, S)$, soient liées algébriquement, forment un groupe continu.

C'est ce que nous observerons dans un second exemple, à savoir quand $F(z)$ se réduit à la fonction modulaire J. Le groupe de cette fonction se compose alors de toutes les substitutions

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right),$$

où $\alpha$, $\beta$, $\gamma$, $\delta$ sont quatre entiers, tels que

$$\alpha\delta - \beta\gamma = 1.$$

Nous savons qu'il y a une relation algébrique entre $F(z)$ et $F\left(\frac{z}{n}\right)$; c'est cette relation algébrique qui est bien connue sous le nom d'*équation modulaire* dans la théorie de la transformation des fonctions elliptiques.

Vérifions que le groupe G, formé des substitutions

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right),$$

où $\alpha$, $\beta$, $\gamma$, $\delta$ sont entiers, est bien commensurable avec son transformé $S^{-1}GS$ par la substitution

$$S = \left(z, \frac{z}{n}\right),$$

où $n$ est entier.

En effet, le groupe $S^{-1}GS$ est formé des substitutions

$$\left(z, \frac{\alpha z + \frac{\beta}{n}}{\gamma n z + \delta}\right),$$

où $\alpha$, $\beta$, $\gamma$, $\delta$ sont entiers et tels que $\alpha\delta - \beta\gamma = 1$.

Le groupe commun $g$ aux deux groupes G et $S^{-1}GS$ est alors formé des substitutions

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right),$$

où $\alpha$, $\beta$, $\gamma$, $\delta$ sont des entiers satisfaisant aux conditions

$$\alpha\delta - \beta\gamma = 1, \qquad \gamma \equiv 0 \pmod{n}.$$

C'est donc, par rapport à G, un sous-groupe à congruences et par conséquent un sous-groupe d'indice fini. C. Q. F. D.

Pour la même raison, on a une relation algébrique entre la fonction modulaire $F(z)$ et $F\left(\frac{pz}{n}\right)$, $p$ et $n$ étant deux entiers premiers entre eux.

Plus généralement, je dis qu'il y aura une relation algébrique entre la fonction modulaire $F(z)$ et $F\left(\frac{az+b}{cz+d}\right)$, $a$, $b$, $c$ et $d$ étant des entiers quelconques.

Car la substitution

$$S = \left(z, \frac{az+b}{cz+d}\right),$$

où $a$, $b$, $c$, $d$ sont des entiers quelconques, peut toujours être regardée comme la résultante de plusieurs autres de la forme

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right) \quad \text{où} \quad \alpha\delta - \beta\gamma = 1,$$

ou de la forme

$$(z, pz) \quad \text{ou} \quad \left(z, \frac{z}{n}\right).$$

L'ensemble des substitutions S, telles que $F(z)$ et $F(z, S)$ soient liées algébriquement, forme donc un groupe continu.

Jusqu'à présent cet exemple était isolé, mais nous sommes maintenant à même d'en citer une infinité d'autres.

Envisageons une forme quadratique indéfinie F à coefficients entiers et reprenons les dénominations du § II. Considérons le groupe reproductif de F formé de toutes les substitutions à coefficients *quelconques*

qui n'altèrent pas cette forme, et le groupe principal de F formé de toutes les substitutions à coefficients *entiers* qui n'altèrent pas cette forme. A toute substitution du groupe reproductif correspondra une substitution fuchsienne et au groupe principal de F correspondra un groupe fuchsien G qui sera le groupe fuchsien principal de F.

Soit $f(z)$ une des fonctions fuchsiennes engendrées par le groupe G.

J'envisagerai également les substitutions du groupe reproductif qui ont des coefficients *fractionnaires* (ce sont celles que nous avons étudiées dans le § IV), les substitutions fuchsiennes correspondantes et le groupe Γ formé par ces substitutions fuchsiennes et qui sera un groupe *continu*.

Soit S une substitution fractionnaire du groupe reproductif de F; soit $s$ la substitution fuchsienne correspondante appartenant à Γ. En vertu des lemmes II et VI du § III, le groupe principal de F sera commensurable avec son transformé par S.

Donc G sera commensurable avec son transformé par $s$.

*Il y a donc une relation algébrique entre*

$$f(z) \quad \text{et} \quad f(z, s),$$

*s étant une substitution quelconque du groupe continu* Γ.

Les fonctions fuchsiennes arithmétiques jouissent donc, comme la fonction modulaire, de la propriété qui nous occupe. La fonction modulaire n'en est d'ailleurs qu'un cas particulier et on l'obtient en prenant, pour la forme quadratique F,

$$F = 2y^2 - 2xz.$$

Ainsi il y a une propriété que l'on peut regarder comme la généralisation du théorème d'addition, si l'on regarde les fonctions fuchsiennes comme la généralisation des fonctions elliptiques, mais que l'on peut aussi regarder comme la généralisation de la transformation, si l'on regarde les fonctions fuchsiennes comme la généralisation de la fonction modulaire.

Cette propriété n'appartient pas en général à toutes les fonctions fuchsiennes; mais elle appartient aux fonctions fuchsiennes arithmétiques.

Cela peut faire concevoir l'espoir que ces transcendantes arithmétiques rendront, dans la théorie de certaines classes d'équations algébriques, des services analogues à ceux qu'a rendus la fonction modulaire dans l'étude de l'équation du cinquième degré.

Paris, 18 mars 1887.