SUR

CERTAINS GROUPES FUCHSIENS

ET SUR

UNE EXTENSION DE LA THÉORIE DES FORMES QUADRATIQUES;

PAR M. X. STOUFF.

Ce travail a pour objet l'étude d'une classe très étendue de groupes fuchsiens. La formation de ces groupes dépend de certains entiers fixes appelés *modules,* qui forment un ou plusieurs systèmes distincts. Voici d'abord la théorie des groupes à un seul *système de modules*.

I.

Tout système de modules se compose de nombres premiers entre eux, deux à deux, $a_1, a_2, \ldots, a_n$. Soit L leur produit; soient P_i un produit de modules où chacun d'eux n'entre pas plus d'une fois comme facteur, et P'_i le produit des autres modules. Toutes les substitutions représentées par la formule

$$\left(z, \frac{\alpha P_i z + L\beta}{\gamma z + \delta P_i}\right), \tag{1}$$

où

$$P_i \alpha\delta - P'_i \beta\gamma = 1, \tag{1'}$$

forment un groupe. En effet, le produit d'une de ces substitutions par une autre est

$$\left[z, \frac{(\alpha\alpha' P_i P_j + \gamma\beta' L) z + (\beta\alpha' P_j + \delta\beta' P_i) L}{(\alpha\gamma' P_i + \gamma\delta' P_j) z + (\beta\gamma' L + \delta\delta' P_i P_j)}\right].$$

Soit P_h le produit des modules communs à P_i et à P_j, et $P_k = \frac{P_i P_j}{P_h^2}$. Le déterminant de la substitution précédente est $P_i P_j$; mais le premier, le troisième, le quatrième coefficient et le quotient du second coefficient par

L sont divisibles par P_h. En effectuant cette division, il vient

$$\left[z, \frac{(\alpha\alpha' P_h P_k + \gamma\beta' P'_h)\, z + \left(\beta\alpha' \frac{P_j}{P_h} + \delta\beta' \frac{P_i}{P_h}\right) L}{\left(\alpha\gamma' \frac{P_i}{P_h} + \gamma\delta' \frac{P_j}{P_h}\right) z + (\beta\gamma' P'_h + \delta\delta' P_k P_h)}\right];$$

dans cette substitution, le déterminant est P_k. Je remarque que le premier et le quatrième coefficient sont divisibles par P_k : en effet, en divisant $P_i P_j$ par P_h^2, on fait disparaître les modules qui divisent P_h. Par suite, P_k et P_h sont premiers entre eux. Donc P_k divise P'_h. La substitution prend alors la forme

$$\left(z, \frac{A P_k z + B L}{\Gamma z + \Delta P_k}\right),$$

où

$$P_k A \Delta - P'_k B \Gamma = 1;$$

elle rentre donc dans la formule (1).

Soient H et G deux groupes ainsi définis. Pour que H contienne G, il faut et il suffit que chacun des modules de G soit un produit des modules de H, chacun de ces derniers n'entrant qu'une fois comme facteur, et que le produit des modules de G soit divisible par le produit des modules de H. Cette dernière condition, combinée avec la première, entraîne l'égalité des deux produits. Désignons par

$$\left(z, \frac{\alpha P_i z + \beta L}{\gamma z + \delta P_i}\right) \quad \text{et} \quad \left(z, \frac{\lambda Q_j z + \mu L}{\nu z + \rho Q_j}\right)$$

deux substitutions quelconques, l'une de H, l'autre de G. La transformée de la seconde par la première est, après quelques simplifications,

$$(2)\quad \left\{z, \frac{(\alpha\gamma\mu Q'_j - \alpha\delta\lambda P_i + \beta\gamma\rho P'_i - \beta\delta\nu Q'_j)\, Q_j z - [\alpha^2\mu P_i - \alpha\beta(\lambda-\rho) Q_j - \beta^2\nu P'_i] L}{[\gamma^2\mu P'_i - \gamma\delta(\lambda-\rho) Q_j - \delta^2\nu P_i]\, z - (\alpha\gamma\mu Q'_j - \beta\gamma\lambda P'_i + \alpha\beta\rho P_i - \beta\delta\nu Q'_j)\, Q_j}\right\};$$

elle appartient encore au groupe G. Donc G *est sous-groupe distingué de* H.

Ainsi le groupe défini par le système de modules 2, 3, 5 a pour sous-groupes distingués les groupes à modules 2, 15; 6, 5; 3, 10; 1, 30.

II.

Lorsqu'un des groupes est donné par ses modules, on peut se proposer de déterminer un système de substitutions fondamentales du groupe. Quand les modules sont des nombres premiers absolus, on démontre aisément que les substitutions génératrices sont en nombre fini.

Supposons que ce cas se présente. Je prouverai que dans les substitutions

$$(z,\ z+\mathrm{L}) \tag{3}$$

et

$$\left(z,\ \mathrm{P}_i\mathrm{R}_{ik} - \frac{\mathrm{P}_i}{z+\mathrm{P}_i\mathrm{R}'_{ik}}\right), \tag{4}$$

dans lesquelles P_i représente tous les produits de modules où chacun d'eux n'entre qu'une fois, R_{ik} prend toutes les valeurs inférieures à P'_i et premières à ce nombre, et R'_{ik} est un nombre choisi, de telle sorte que

$$\mathrm{P}_i\mathrm{R}_{ik}\mathrm{R}'_{ik} \equiv 1 \bmod \mathrm{P}'_i$$

forment un système fondamental. Il est toujours possible de faire correspondre à chaque nombre R_{ik} un nombre R'_{ik} de manière à satisfaire à cette dernière congruence. Le nombre des substitutions ainsi obtenues est évidemment limité.

En effet, imaginons une substitution quelconque du groupe

$$\left(z,\ \frac{\alpha\mathrm{Q}_j z+\beta\mathrm{L}}{\gamma z+\delta\mathrm{Q}_j}\right), \tag{5}$$

soit

$$\alpha = \gamma q + \gamma', \qquad \beta\mathrm{Q}'_j = \delta q + \delta',$$

où γ' est moindre que γ en valeur absolue. L'emploi de la substitution $(z,\ z+\mathrm{L})$ permet de retrancher de la fraction (5) des multiples de L et, par suite, de ramener q à être compris entre 0 et Q'_j.

Posons

$$q\mathrm{Q}_j = \mathrm{R}_{ik}\mathrm{P}_i, \tag{6}$$

$$\frac{\gamma'\mathrm{Q}_j z+\delta'\mathrm{Q}_j}{\gamma z+\delta\mathrm{Q}_j} = -\frac{\mathrm{P}'_i}{z_1+\mathrm{R}'_{ik}\mathrm{P}_i}; \tag{7}$$

je me propose de déterminer une substitution (4), de telle sorte que les égalités (6) et (7) soient réalisées. Distinguons deux cas :

1° q est premier avec Q'_j; on pourra alors prendre

$$\mathrm{P}_i = \mathrm{Q}_j, \qquad \mathrm{R}_{ik} = q;$$

z_1 s'exprime alors en z par une fraction dans laquelle, après simplification, le coefficient de z au dénominateur est γ' et, par conséquent, moindre en valeur absolue que γ.

2° q n'est pas premier avec Q'_j; tous les modules étant premiers et Q'_j ne les contenant pas plus d'une fois, le diviseur D commun à q et à Q'_j est un produit de modules pris chacun une fois au plus, soit $P_i = DQ_j$ et $q = q_1 D$; $P'_i = \frac{Q'_j}{D}$ ne contient plus de facteurs premiers divisant q_1 et est, par suite, premier avec q_1. On pourra donc poser $R_{ik} = q_1$. La substitution se trouve alors ramenée, comme dans le cas précédent, à une substitution où le coefficient de z au dénominateur est γ'. En continuant ainsi, on pourra réduire à o le coefficient de z au dénominateur; mais si, dans l'égalité

$$\alpha\delta Q_j - \beta\gamma Q'_j = 1,$$

on a $\gamma = 0$, il en résulte $\alpha = \delta = \pm 1$. La substitution prend la forme $(z, z + \beta L)$, et l'on peut évidemment la réduire à la substitution identique à l'aide de $(z, z + L)$.

Les substitutions (4), quoique suffisantes pour engendrer tout le groupe, ne sont pas, en général, toutes nécessaires. Il est facile de voir d'abord qu'elles se ramènent, deux à deux, l'une à l'autre. Soient

$$z_1 = P_i R_{ik} - \frac{P_i}{z + P_i R'_{ik}}, \qquad z = - P_i R'_{ik} - \frac{P_i}{z_1 - P_i R_{ik}};$$

nous pouvons supposer R'_{ik} compris entre o et P'_i; écrivons la dernière équation sous la forme

$$z + L = P_i(P'_i - R'_{ik}) - \frac{P_i}{z - L + P_i(P'_i - R_{ik})};$$

$P'_i - R'_{ik}$ est compris entre o et P'_i. Les deux substitutions caractérisées par R_{ik} et $P'_i - R'_{ik}$ se ramènent donc l'une à l'autre. On peut encore pousser la réduction plus loin. Je prendrai pour exemple le groupe défini par les modules 2, 3, 5. D'après la remarque précédente, il suffit de donner à $P_i R_{ik}$ les valeurs

$$P_i R_{ik} = 0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 15, 16, 18, 21, 25.$$

Je dis maintenant que les substitutions

$$(8) \quad (z, z+30), \quad \left(z, -\frac{30}{z}\right), \quad \left(z, 8 - \frac{2}{z+4}\right), \quad \left(z, 10 - \frac{10}{z+10}\right), \quad \left(z, 15 - \frac{15}{z+15}\right)$$

forment un système fondamental. Les inverses des trois dernières sont

$$(9) \qquad \left(z,\ -4-\frac{2}{z-8}\right), \qquad \left(z,\ -10-\frac{10}{z-10}\right), \qquad \left(z,\ -15-\frac{15}{z-15}\right).$$

Je m'appuie sur la remarque suivante : soit une fraction linéaire

$$\frac{mz+n}{pz+q}, \qquad \frac{m}{p}=A+\cfrac{a}{B+\cfrac{b}{C+r}};$$

on a aussi

$$\frac{mz+n}{pz+q}=A+\cfrac{a}{B+\cfrac{b}{C+r+\cfrac{s}{z+t}}}.$$

Or on voit aisément que toute substitution de notre groupe, où

$$(10) \qquad \frac{m}{p}=0,\ 8,\ 10,\ 15,\ -4,\ -10,\ -15,$$

est une combinaison simple de $(z,\ z+30)$ avec une des autres substitutions (8) et (9). Il ne reste plus qu'à montrer que les valeurs trouvées pour P_iR_{ik} (en exceptant 8, 10 et 15) peuvent se développer suivant des fractions continues formées en combinant les substitutions (8) et (9), et en donnant à z, dans la substitution extrême, les valeurs (10). On trouve

$$1=-\frac{30}{-30+0}, \qquad 2=-\frac{30}{-30+15}, \qquad 3=-\frac{30}{-10},$$

$$4=-\cfrac{30}{-10-\cfrac{10}{-10-\cfrac{30}{-10-\cfrac{10}{-10+8}}}}, \qquad 5=-\cfrac{30}{-4-\cfrac{2}{-8+10-\cfrac{10}{10+0}}}.$$

$$6=-\cfrac{30}{-10-\cfrac{10}{-10+8}}, \qquad 7=8-\cfrac{2}{4-\cfrac{30}{15}}, \qquad 11=10-\frac{10}{10-30+10},$$

$$12=10-\frac{10}{10-30+15}, \qquad 13=15-\cfrac{15}{10-\cfrac{10}{10-4-\cfrac{2}{-8+10-\cfrac{10}{10+0}}}}$$

et

$$16 = 30 - 15 - \frac{15}{-15+0}, \qquad 18 = 30 - 15 - \frac{15}{-15+10},$$

$$21 = 30 - 10 - \frac{10}{-10+0}, \qquad 25 = 30 - 10 - \frac{10}{-10+8}.$$

On peut prendre pour polygone générateur du groupe un polygone $i\infty$ABCDEFGH$i\infty$. Les côtés A$i\infty$ et H$i\infty$ sont conjugués par $(z, z+30)$, AB et HG par $\left(z, 15 - \frac{15}{z+15}\right)$, BC et GF par $\left(z, 10 - \frac{10}{z+10}\right)$, CD et FE par $\left(z, 8 - \frac{2}{z+4}\right)$; chaque moitié du côté DE est conjuguée avec l'autre par la substitution $\left(z, -\frac{30}{z}\right)$. A et H, B et G, C et F, D et E forment respectivement des cycles d'angle π.

Les groupes dans lesquels tous les modules ne sont pas premiers présentent des circonstances analogues. Par exemple, le groupe défini par le module unique 8 admet pour système fondamental

$$(z, z+8), \qquad \left(z, 3 - \frac{1}{z+3}\right), \qquad \left(z, -\frac{8}{z}\right).$$

On peut prendre pour polygone générateur un pentagone $i\infty$ABCD$i\infty$, dans lequel A$i\infty$ et D$i\infty$ sont conjugués par $(z, z+8)$, AB et DC par $\left(z, 3 - \frac{1}{z+3}\right)$, et les deux moitiés de BC par $\left(z, -\frac{8}{z}\right)$. A et D forment un cycle parabolique, B et C un cycle d'angle π.

Les groupes les plus simples sont les groupes aux modules uniques 2 et 3; ils sont engendrés respectivement par

$$(z, z+2), \qquad \left(z, -\frac{2}{z}\right), \qquad (z, z+3), \qquad \left(z, -\frac{3}{z}\right).$$

Les équations fuchsiennes correspondantes ont chacune trois points singuliers; les différences des racines des équations déterminantes sont $0, \frac{1}{4}, \frac{1}{2}$; $0, \frac{1}{6}, \frac{1}{2}$.

III.

On peut se proposer de déterminer, *a priori*, les points singuliers que présentent les équations fuchsiennes engendrées par les groupes à déterminants limités. Cherchons d'abord de quelles périodes est susceptible une substitution linéaire $\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right)$ à coefficients entiers. En désignant par n

la période de cette substitution, on a

$$\frac{\alpha+\delta}{\sqrt{\alpha\delta-\beta\gamma}}=2\cos\frac{\pi}{n}.$$

Il faut donc que $\cos\frac{\pi}{n}$ ne contienne en facteur pas d'autres irrationnelles qu'un radical carré. On en déduit que n peut seulement prendre les valeurs 2, 3, 4, 6.

La recherche des points singuliers eux-mêmes se rattache à une extension de la théorie des formes quadratiques. Étant donné un groupe défini par ses modules, je considère une expression de la forme

$$(11)\qquad ax^2+bP_ixy+cLy^2\qquad (a, b, c),$$

où a, b, c sont des entiers, tels que a, c et bP_i n'aient pas de facteurs communs, et où x et y sont respectivement de la forme $x_0\sqrt{Q_j}$ et $\frac{y_0}{\sqrt{Q_j}}$, x_0 et y_0 étant entiers. Si tous les modules sont premiers, on supposera b premier avec P'_i, ce qui ne diminue pas la généralité. Dans le cas contraire, P_i désignera le plus grand produit de modules qui divise le coefficient de xy; j'appelle ϖ le plus grand commun diviseur de b et de P'_i. Je nomme les expressions (11) *formes quadratiques attachées au groupe* donné.

L'expression générale d'une substitution de ce groupe étant

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

j'envisage la substitution à deux variables

$$(12)\qquad \left|\begin{array}{l} x, \dfrac{\alpha Q_j x+\beta L y}{\sqrt{Q_j}} \\ y, \dfrac{\gamma x+\delta Q_j y}{\sqrt{Q_j}} \end{array}\right|;$$

si x et y sont de la forme $x_0\sqrt{Q_j}$ et $\frac{y_0}{\sqrt{Q_j}}$, cette substitution change ces quantités en des quantités de la même forme. L'expression (11) devient

$$(13)\qquad \left\{\begin{array}{l} (a\alpha^2 Q_j+b\alpha\gamma P_i+c\gamma^2 Q'_j)x^2+(2a\alpha\beta P'_i+b\alpha\delta Q_j+b\beta\gamma Q'_j+2c\gamma\delta P'_i)P_i xy \\ \quad +(a\beta^2 Q'_j+b\beta\delta P_i+c\delta^2 Q_j)Ly^2; \end{array}\right.$$

elle reste donc attachée au même groupe. Nous dirons que les formes (11) et (13) sont *équivalentes*. Dans (13), le plus grand commun diviseur entre le multiplicateur de $P_i xy$ et P'_i est encore ϖ.

Le déterminant de la substitution (12) étant égal à 1, les formes (11) et (13) ont un même discriminant, qu'on peut représenter par DP_i, D étant entier, et l'on a

$$b^2 P_i - 4ac P'_i = D. \tag{14}$$

On nommera *classe*, comme dans la théorie ordinaire, l'ensemble des formes équivalentes à une forme donnée. D, ϖ et P_i sont les mêmes pour toutes les formes d'une même classe.

Le premier problème qui s'offre à l'esprit est de représenter un nombre entier donné m par une forme donnée

$$m = a Q_j x_0^2 + b P_i x_0 y_0 + c Q'_j y_0^2. \tag{15}$$

On est conduit immédiatement à limiter les conditions du problème; car on peut supposer, sans diminuer la généralité :

1° x_0 et y_0 premiers entre eux. S'ils avaient pour plus grand commun diviseur un nombre δ, on serait ramené au même problème, le nombre à représenter étant $\frac{m}{\delta^2}$ et x_0, y_0 étant premiers entre eux;

2° x_0 premier avec Q'_j et y_0 avec Q_j. En effet, si δ était le diviseur commun à x_0 et à Q'_j, en enlevant aux modules de Q'_j les facteurs premiers qui entrent dans δ, on serait ramené à représenter $\frac{m}{\delta}$ par une forme attachée à un groupe plus simple;

3° m premier avec P_i pour une raison analogue.

Nous pourrons alors déterminer deux nombres ξ_0 et η_0, tels que

$$x_0 \eta_0 Q_j - y_0 \xi_0 Q'_j = 1, \tag{16}$$

et la substitution

$$\left| \begin{array}{ll} u, & \dfrac{u x_0 Q_j + v \xi_0 L}{\sqrt{Q_j}} \\[2ex] v, & \dfrac{u x_0 + v \eta_0 Q_j}{\sqrt{Q_j}} \end{array} \right|$$

change la forme donnée en la forme

$$m u^2 + n P_i u v + l L v^2 \qquad (m, n, l); \tag{17}$$

comme le discriminant est resté invariable, on a

$$n^2 P_i - 4 m l P'_i = D;$$

m étant donné, il faut donc que la congruence

$$(18) \qquad n^2 P_i \equiv D \pmod{4 m P'_i}$$

soit possible. Une courte discussion donne les résultats suivants :

1° Si P_i est impair, il faut que DP_i soit reste quadratique de $4mP'_i$.

2° P_i est simplement pair, alors D est pair; il faut que $\frac{DP_i}{4}$ soit reste quadratique de $2mP'_i$.

3° P_i est doublement pair, il faut que $\frac{DP_i}{16}$ soit reste quadratique de mP'_i.

Toutes les solutions de l'équation (16) correspondent à des racines de la congruence (18) congrues (mod. $2mP'_i$).

Pour résoudre le problème proposé, on formera d'abord un système de solutions de la congruence (18) incongrues (mod. $2mP'_i$). A chacune de ces solutions correspond une forme (m, n, l). Nous aurons à voir, comme dans la théorie ordinaire :

1° Si la forme (m, n, l) est équivalente à (a, b, c);

2° A trouver toutes les substitutions qui transforment (a, b, c) dans (m, n, l).

Ces dernières substitutions peuvent se ramener à une substitution unique transformant (a, b, c) dans (m, n, l) et aux substitutions qui transforment (a, b, c) en elle-même. Je me propose de trouver celles-ci tout d'abord.

Pour que la substitution (12) transforme (a, b, c) en elle-même, il faut et il suffit que l'on ait

$$(19) \qquad \begin{cases} a = a\alpha^2 Q_j + b\alpha\gamma P_i + c\gamma^2 Q'_j, \\ b = 2a\alpha\beta P'_i + b(\alpha\delta Q_j + \beta\gamma Q'_j) + 2c\gamma\delta P'_i; \end{cases}$$

on en déduit

$$\frac{\delta - \alpha}{b Q'_j} = \frac{\beta}{-c P'_i} = \frac{\gamma}{a P'_i};$$

θ_j étant le plus grand diviseur commun aux trois dénominateurs, on aura

$$(20) \qquad \delta - \alpha = \frac{b Q'_j}{\theta_j} u, \qquad \beta = \frac{-c P'_i}{\theta_j} u, \qquad \gamma = \frac{a P'_i}{\theta_j} u,$$

u étant entier.

Étudions la formation du nombre θ_j. Le facteur ϖ est évidemment commun aux trois nombres $b Q'_j$, $-cP'_i$, aP'_i. Soit $b = b_1 \varpi$. Il reste à trouver le facteur commun à $b_1 Q'_j$, $-c\frac{P'_i}{\varpi}$, $a\frac{P'_i}{\varpi}$. Si un diviseur quelconque commun aux trois nombres divisait b_1, comme b_1 est premier avec $\frac{P'_i}{\varpi}$, il devrait diviser a et c, ce qui est contre l'hypothèse. Donc le facteur commun divise Q'_j. Soit $d'd''$ ce facteur, dans lequel je suppose que d'' divise $\frac{P'_i}{\varpi}$ et que d' est premier avec $\frac{P'_i}{\varpi d''}$; d' devrait diviser a et c, d'ailleurs il divise ϖP_i; a, bP_i et c auraient donc un facteur commun, ce qui est contre l'hypothèse. Donc $\frac{\theta_j}{\varpi}$ est le plus grand commun diviseur entre Q'_j et $\frac{P'_i}{\varpi}$; par suite, θ_j le plus grand commun diviseur entre $\varpi Q'_j$ et P'_i.

En posant

$$\alpha + \delta = t,$$

on trouve ensuite que t et u doivent vérifier l'équation

$$t^2 Q_j - \frac{D Q'_j P'_i u^2}{\theta_j^2} = 4, \tag{21}$$

et l'on a

$$\alpha = \frac{t\theta_j - bQ'_j u}{2\theta_j}, \qquad \beta = -\frac{cP'_i u}{\theta_j}, \qquad \gamma = \frac{aP'_i u}{\theta_j}, \qquad \delta = \frac{t\theta_j + bQ'_j u}{2\theta_j}, \tag{22}$$

Réciproquement, si l'on a une solution en nombres entiers de l'équation (21), les valeurs de α, β, γ, δ, calculées par les formules (22), vérifient identiquement l'équation (19) et la relation $\alpha\delta Q_j - \beta\gamma Q'_j = 1$. Pour qu'elles soient entières, il suffit que α et δ ne contiennent pas 2 au dénominateur; or $2\alpha + 2\delta$ ou $2t$ est pair; donc 2α et 2δ sont de même parité. D'ailleurs on a la relation

$$4\alpha\delta Q_j = 4\left(1 - \frac{acP'^2_i Q'_j}{\theta_j^2} u^2\right).$$

Si Q_j n'est pas divisible par 4, $4\alpha\delta$ est pair et 2α, 2δ sont pairs; si Q_j est divisible par 4, on ne peut arriver à la même conclusion, mais on remarque que la parité de α et de δ pour une solution donnée de l'équation (21) forme un caractère constant de toutes les formes équivalentes; si D est négatif et égal à $-\Delta$, l'équation (21) prend la forme

$$t^2 Q_j + \frac{\Delta Q'_j P'_i u^2}{\theta^2} = 4 \tag{23}$$

et n'admet qu'un nombre limité de solutions.

IV.

Dans l'étude des formes attachées à un groupe, la notion des réduites paraît beaucoup plus complexe que dans la théorie ordinaire. On démontre cependant sans difficulté que le nombre des classes de formes pour lesquelles D, ϖ et P_i sont donnés est limité.

Je commence par quelques considérations sur les substitutions linéaires. Les substitutions

$$\begin{pmatrix} \alpha, & \beta L \\ \gamma, & \delta \end{pmatrix}, \tag{A}$$

$$\alpha\delta - \beta\gamma L = 1 \tag{A'}$$

forment un sous-groupe bien connu du groupe des substitutions

$$\begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix}, \tag{B}$$

$$\lambda\rho - \mu\nu = 1. \tag{B'}$$

Étant donnée une quelconque de ces dernières, je me propose de déterminer une substitution (A), telle que le produit de la première par la seconde

$$\begin{pmatrix} \lambda\alpha + \mu\gamma, & \lambda\beta L + \mu\delta \\ \nu\alpha + \rho\gamma, & \nu\beta L + \rho\delta \end{pmatrix} \tag{C}$$

appartienne à un système fini que j'appellerai *système de représentants* du groupe (B) dans le groupe (A).

Je distinguerai deux cas principaux :

1° μ et L sont premiers entre eux. En vertu de (B'), λ est également premier avec μ. Nous pourrons donc trouver des valeurs de β et δ, telles que

$$\lambda\beta L + \mu\delta = -1;$$

on aura

$$\delta = \delta_0 + s\lambda L, \qquad \beta = \beta_0 - s\mu,$$

s étant entier. On en déduit

$$\nu\beta L + \rho\delta = \nu\beta_0 L + \rho\delta_0 + sL;$$

on peut déterminer s de sorte que cette quantité soit comprise entre o et L. Nous prendrons ensuite

$$\alpha = -\mu, \qquad \gamma = \rho.$$

La substitution (C) prend alors la forme

$$\begin{pmatrix} 0, & -1 \\ 1, & r \end{pmatrix},$$

r étant un nombre quelconque compris entre o et L.

2° μ et L ont un plus grand commun diviseur d. On posera

$$\text{(D)} \qquad \lambda\beta L + \mu\delta = -d,$$

$$\delta = \delta_0 + s\frac{\lambda L}{d}, \qquad \beta = \beta_0 - \frac{s\mu}{d}, \qquad \nu\beta L + \rho\delta = \nu\beta_0 L + \rho\delta_0 + s\frac{L}{d}.$$

Supposons d'abord d premier avec $\frac{L}{d}$; on peut satisfaire à la congruence

$$\nu\beta_0 L + \rho\delta_0 + s\frac{L}{d} \equiv 1 \pmod{d},$$

$$s = s_0 + s'd, \qquad \nu\beta L + \rho\delta = \nu\beta_0 L + \rho\delta_0 + s_0\frac{L}{d} + s'L.$$

On pourra déterminer s', de sorte que ce nombre soit compris entre o et L. Nous poserons ensuite

$$\alpha = -\mu t + u\rho, \qquad \gamma = \lambda t - u\nu,$$

on aura

$$\alpha\delta - \beta\gamma L = u(\nu\beta L + \rho\delta) - td = 1.$$

Pour y satisfaire, on réduira la fraction irréductible $\frac{\nu\beta L + \rho\delta}{d}$ en fraction continue, et l'on prendra pour $\frac{t}{u}$ l'avant-dernière réduite; (C) prendra la forme

$$\begin{pmatrix} u, & -d \\ t, & r \end{pmatrix},$$

r étant compris entre o et L, congru à 1 (mod d). A chaque valeur de r est attaché un système t, u.

Supposons que d et $\frac{L}{d}$ aient un plus grand commun diviseur d'. En vertu de (B′), ρ est premier avec μ et, par suite, avec d'; en vertu de (D), δ est premier avec $\frac{L}{d}$ et, par suite, avec d'. Donc $\nu\beta L + \rho\delta$ est toujours premier avec d'.

Pour que $\nu\beta L + \rho\delta$ soit premier avec d, il faut et il suffit que ce nombre ne contienne aucun des facteurs premiers de $\frac{d}{d'}$ qui n'entrent pas dans d'; soit d'' le produit de ces facteurs, on pourra vérifier la congruence

$$\nu\beta_0 L + \rho\delta_0 + s\frac{L}{d} \equiv 1 \qquad (\operatorname{mod} d'')$$

et faire en sorte que le premier membre soit positif et moindre que $\frac{Ld''}{d}$. On achèvera comme dans le cas précédent.

Envisageons maintenant une forme

$$ax^2 + bP_i xy + cLy^2, \qquad b^2 P_i - 4acP'_i = D,$$

et soit

$$Ax^2 + Bxy + Cy^2$$

la forme réduite équivalente dans le sens ordinaire. On aura identiquement

$$\left.\begin{aligned} &ax^2 + bP_i xy + cLy^2 \\ &\quad = A(\lambda x + \mu y)^2 + B(\lambda x + \mu y)(\nu x + \rho y) + C(\nu x + \rho y)^2 \end{aligned}\right\} \quad (\lambda\rho - \mu\nu = 1);$$

il existe une substitution du groupe (A), telle que

$$\begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix}\begin{pmatrix} \alpha, & \beta L \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} \lambda_0, & \mu_0 \\ \nu_0, & \rho_0 \end{pmatrix}$$

soit un *représentant* de (B) dans (A); on aura

$$\begin{pmatrix} \lambda, & \mu \\ \nu, & \rho \end{pmatrix} = \begin{pmatrix} \lambda_0, & \mu_0 \\ \nu_0, & \rho_0 \end{pmatrix}\begin{pmatrix} -\delta, & \beta L \\ \gamma, & -\alpha \end{pmatrix},$$

la forme quadratique considérée peut donc s'obtenir en faisant dans $Ax^2 + Bxy + Cy^2$ la substitution $\begin{pmatrix} \lambda_0, & \mu_0 \\ \nu_0, & \rho_0 \end{pmatrix}$, puis dans la nouvelle forme une substitution du groupe à laquelle la forme donnée est attachée. On obtiendra donc des représentants de toutes les classes de formes pour lesquelles D, P_i et ϖ sont donnés, en formant dans le sens ordinaire toutes les réduites de déterminant DP_i, dont le nombre est fini, en transformant ces réduites par tous les représentants du groupe (B) dans le groupe (A), et en prenant parmi les formes obtenues celles dont le second coefficient est divisible par ϖP_i, et le troisième par L.

Il est possible que l'on obtienne ainsi à la fois plusieurs représentants pour une même classe. Il faut donc avoir un moyen de reconnaître si deux représentants (a, b, c), (a', b', c') sont équivalents ou non. En supposant que l'équivalence ait lieu, on aura

$$a' = a\alpha^2 Q_j + b\alpha\gamma P_i + c\gamma^2 Q'_j, \tag{24}$$

$$b' = 2a\alpha\beta P'_i + b\alpha\delta Q_j + b\beta\gamma Q'_j + 2c\gamma\delta P'_i, \tag{25}$$

$$\alpha\delta Q_j - \beta\gamma Q'_j = 1. \tag{26}$$

On peut remplacer l'équation (24) par la suivante

$$4aa' Q_j = (2a\alpha Q_j + b\gamma P_i)^2 - DP_i\gamma^2, \tag{27}$$

on cherchera des valeurs entières de α et γ satisfaisant à cette équation. Ces valeurs obtenues, on aura

$$\beta = \frac{(b' - b)\alpha Q_j - 2c\gamma P'_i}{2a' P'_i}, \qquad \delta = \frac{2a\alpha P'_i + (b + b')\gamma Q'_j}{2a' P'_i},$$

il faut encore que les valeurs de β et de δ soient entières.

Si D est négatif, l'équation (27) n'admet qu'un nombre limité de solutions. Le nombre des essais à faire pour reconnaître l'équivalence est donc limité.

Si D est positif, on ne peut suivre la même voie. Je m'appuierai alors sur les propriétés de l'équation (21) qui sont analogues à celles de l'équation de Pell. Soient deux solutions de (21) t, u; t', u'.

$$t^2 Q_j - \frac{DQ'_j P'_i}{\theta_j^2} u^2 = 4, \qquad t'^2 Q_h - \frac{DQ'_h P'_i}{\theta_h^2} u'^2 = 4.$$

En multipliant les deux irrationnelles

$$\frac{t\sqrt{Q_j} + u\dfrac{\sqrt{DQ'_j P'_i}}{\theta_j}}{2}, \qquad \frac{t'\sqrt{Q_h} + u'\dfrac{\sqrt{DQ'_h P'_i}}{\theta_h}}{2}, \tag{28}$$

on obtient l'irrationnelle

$$\frac{tt'\sqrt{Q_j Q_h} + uu'\dfrac{DP'_i}{\theta_j\theta_h}\sqrt{Q'_j Q'_h} + ut'\dfrac{\sqrt{DQ'_j P'_i Q_h}}{\theta_j} + u't\dfrac{\sqrt{DQ'_j Q'_h P'_i}}{\theta_h}}{4}.$$

Soient Q_k le produit des modules communs à Q_j et à Q_h et Q_s le produit des modules non communs. La quantité qui précède peut s'écrire

$$\frac{\left(tt'Q_k + uu'\dfrac{DP'_i L}{\theta_j\theta_h Q_k Q_s}\right)\sqrt{Q_s} + \left(ut'\dfrac{Q_h}{Q_k\theta_j} + u't\dfrac{Q_j}{Q_k\theta_h}\right)\sqrt{DQ'_s P'_i}}{4};$$

$\dfrac{DP'_i L}{\theta_j\theta_h Q_k Q_s}$ est un nombre entier : de plus, dans le multiplicateur de $\sqrt{DQ'_s P'_i}$, il ne peut rester en dénominateur que θ_s qui est le plus grand commun diviseur entre $\varpi Q'_s$ et P'_i. On a alors

$$\frac{t''\sqrt{Q_s} + u''\dfrac{\sqrt{DQ'_s P'_i}}{\theta_s}}{2},$$

t'' et u'' ne pouvant contenir que 2 au dénominateur, et satisfaisant à l'équation

$$t''^2 Q_s - \frac{DQ'_s P'_i}{\theta_s^2} u''^2 = 4.$$

Mais, si t, u; t', u' correspondent à des transformations de la forme en elle-même, un calcul facile montre que t'' et u'' correspondent au produit de ces deux transformations et sont, par conséquent, entiers.

Par suite, toutes les irrationnelles (28) qui correspondent à des transformations de la forme en elle-même sont des puissances de l'une d'elles

$$\frac{T\sqrt{Q_J} + U\dfrac{\sqrt{DQ'_J P'_i}}{\theta_J}}{2}.$$

On peut maintenant restreindre à un nombre limité les tâtonnements à faire pour reconnaître si les équations (24), (25), (26) admettent ou non des solutions. On formera une solution réelle quelconque des équations

$$\begin{gathered} a' = a\lambda^2 + bP_i\lambda\nu + cL\nu^2, \\ b'P_i = 2a\lambda\mu + bP_i(\lambda\rho + \mu\nu) + 2cL\nu\rho, \\ \lambda\rho - \mu\nu = 1; \end{gathered}$$

la substitution $\begin{pmatrix}\lambda, \mu\\ \nu, \rho\end{pmatrix}$ transforme (a, bP_i, cL) en $(a', b'P'_i, c'L)$ si $\begin{pmatrix}\alpha\sqrt{Q_j}, & \dfrac{\beta L}{\sqrt{Q_j}}\\ \dfrac{\gamma}{\sqrt{Q_j}}, & \delta\sqrt{Q_j}\end{pmatrix}$ produit le même effet; la substitution

$$\begin{pmatrix}\alpha\sqrt{Q_j}, & \dfrac{\beta L}{\sqrt{Q_j}}\\ \dfrac{\gamma}{\sqrt{Q_j}}, & \delta\sqrt{Q_j}\end{pmatrix}\begin{pmatrix}-\rho, & \mu\\ \nu, & -\lambda\end{pmatrix}=\begin{pmatrix}\lambda', & \mu'\\ \nu', & \rho'\end{pmatrix} \tag{29}$$

laisse (a, bP_i, cL) invariable. Mais l'expression générale des substitutions quelconques qui laissent (a, bP_i, cL) invariable est

$$\frac{2ax_1+(bP_i-\sqrt{DP_i})y_1}{2ax_1+(bP_i+\sqrt{DP_i})y_1}=g\frac{2ax+(bP_i-\sqrt{DP_i})y}{2ax+(bP_i+\sqrt{DP_i})y}, \tag{30}$$

g étant réel; pour que cette substitution appartienne au groupe à déterminants limités, il faut et il suffit que

$$g=\left(\frac{T\sqrt{Q_J}+U\dfrac{\sqrt{DQ'_JP'_i}}{\theta_J}}{2}\right)^n;$$

par suite, toute substitution (30) est le produit d'une substitution du groupe par une substitution (30) dont le g a un logarithme inférieur en valeur absolue à $\log\dfrac{T\sqrt{Q_j}+U\dfrac{\sqrt{DQ_jP'_i}}{\theta_j}}{2}$; on pourra donc poser

$$\begin{pmatrix}\alpha\sqrt{Q_j}, & \dfrac{\beta L}{\sqrt{Q_j}}\\ \dfrac{\gamma}{\sqrt{Q_j}}, & \delta\sqrt{Q_j}\end{pmatrix}\begin{pmatrix}-\rho, & \mu\\ \nu, & -\lambda\end{pmatrix}=\begin{pmatrix}\alpha'\sqrt{Q_h}, & \dfrac{\beta' L}{\sqrt{Q_h}}\\ \dfrac{\gamma'}{\sqrt{Q_h}}, & \delta'\sqrt{Q_h}\end{pmatrix}\begin{pmatrix}\lambda'', & \mu''\\ \nu'', & \rho''\end{pmatrix},$$

où le g de la dernière substitution satisfait à cette condition

$$\begin{pmatrix}-\delta'\sqrt{Q_h}, & \dfrac{\beta' L}{\sqrt{Q_h}}\\ \dfrac{\gamma'}{\sqrt{Q_h}}, & -\alpha'\sqrt{Q_h}\end{pmatrix}\begin{pmatrix}\alpha\sqrt{Q_j}, & \dfrac{\beta L}{\sqrt{Q_j}}\\ \dfrac{\gamma}{\sqrt{Q_j}}, & \delta\sqrt{Q_j}\end{pmatrix}=\begin{pmatrix}\lambda'', & \mu''\\ \nu'', & \rho''\end{pmatrix}\begin{pmatrix}\lambda, & \mu\\ \nu, & \rho\end{pmatrix}.$$

Dans le second membre, la substitution $\begin{pmatrix}\lambda, \mu\\ \nu, \rho\end{pmatrix}$ a été calculée une fois pour toutes, les coefficients de $\begin{pmatrix}\lambda'', & \mu'' \\ \nu'', & \rho''\end{pmatrix}$ ne peuvent varier qu'entre des limites déterminées. Donc les coefficients du premier membre ne peuvent varier qu'entre des limites déterminées. Ce premier membre est une substitution qui transforme (a, b, c) dans (a', b', c'). On n'aura donc à essayer dans (27) qu'un nombre limité de valeurs de α et de γ. Si aucun des essais ne réussit, les deux formes sont de classes différentes.

V.

Les procédés indiqués au paragraphe précédent sont d'une application assez longue, et il peut être utile de connaître le nombre des classes sans être obligé de former des représentants de chaque classe. On y arrive facilement par le même procédé que dans la théorie ordinaire.

Pour éviter des difficultés qu'on lève facilement quand les nombres eux-mêmes sont donnés, je supposerai que $\varpi = 1$, et qu'aucun des modules n'est divisible par 4. Tous nos résultats s'appliqueront immédiatement aux groupes à modules premiers. Je ne considérerai que des formes à déterminants négatifs $D = -\Delta$.

D et P_i étant donnés, formons un système de représentants

$$(a, b, c), \quad (a', b', c'), \quad (a'', b'', c''), \quad \ldots,$$

un pour chaque classe. Envisageons un nombre positif m, premier avec DL. Pour qu'il existe une forme ayant m pour premier coefficient, il faut et il suffit, comme nous savons, que $\frac{DP_i}{\sigma^2}$ soit reste quadratique de $\tau m P'_i$, σ et τ ayant les valeurs suivantes :

P_i étant impair .... $\sigma = 1, \quad \tau = 4;$
P_i étant simplement pair...... $\sigma = 2, \quad \tau = 2.$

Le cas où P_i est doublement pair se trouve forcément écarté; car nous supposons qu'aucun des modules n'est divisible par 4.

D'après nos hypothèses, $\frac{DP_i}{\sigma^2}$ et mP'_i sont premiers entre eux; donc les facteurs communs à $\frac{DP_i}{\sigma^2}$ et à $\tau m P'_i$ divisent τ. Soient

$$\varepsilon = 1, \quad \eta = 1$$

si ces deux nombres sont premiers entre eux;

$$\varepsilon = 1, \quad \eta = 2$$

si $\frac{\mathrm{DP}_i}{\sigma^2}$ est simplement pair;

$$\varepsilon = 2, \qquad \eta = \tau$$

si $\frac{\mathrm{DP}_i}{\sigma^2}$ est doublement pair.

Il faut et il suffit que $\frac{\mathrm{DP}_i}{\sigma^2\varepsilon^2}$ soit reste quadratique de $\frac{\tau m \mathrm{P}'_i}{\eta}$. Ces deux derniers nombres sont premiers entre eux. Aux racines de (18) congrues $(\bmod 2m\mathrm{P}'_i)$ correspondent des racines de

$$(31) \qquad z^2 \equiv \frac{\mathrm{DP}_i}{\sigma^2\varepsilon^2} \qquad \left(\bmod \frac{\tau m \mathrm{P}'_i}{\eta}\right),$$

congrues $\left(\bmod \frac{2m\varepsilon \mathrm{P}'_i}{\eta\eta'}\right)$, où $\eta' = 1$, sauf lorsque $\varepsilon = 2$, $\tau = 2$, alors $\eta' = 2$.

Je distinguerai trois cas :

1° DL est pair; m est donc impair et, par suite, premier avec $\frac{\tau \mathrm{P}'_i}{\eta}$. Le nombre des racines de (18) est $2^{\lambda+\mu}$, λ étant un nombre fixe dépendant de D et de P_i, et μ le nombre des facteurs premiers différents de m.

2° DL est impair. Alors $\sigma = 1$, $\tau = 4$, $\varepsilon = 1$, $\eta = 1$, P'_i est impair. Si DP_i est incongru à 1 (mod 8), m est nécessairement impair. La conclusion est la même que dans le cas précédent.

3° DL est impair, et $\mathrm{DP}_i \equiv 1 \pmod 8$. m peut être pair. Soient $\lambda - 1$ le nombre des facteurs premiers différents de P'_i, μ le nombre des facteurs premiers différents de m, y compris 2. La congruence (18) a $2^{\lambda+\mu}$ racines.

La formule est donc la même dans les trois cas. Soit $\varkappa$ le nombre des transformations d'une forme en elle-même; on aura

$$\sum_{a,b,c}\sum_{x,y} \frac{1}{(ax^2 + b\mathrm{P}_i xy + c\mathrm{L}y^2)^{1+\rho}} = \varkappa 2^\lambda \sum_m \frac{2^\mu}{m^{1+\rho}}.$$

Dans le second membre, m prend toutes les valeurs positives premières à DL et telles que $\frac{\mathrm{DP}_i}{\sigma^2\varepsilon^2}$ soit reste quadratique de m. Dans le premier,

$$x = x_0\sqrt{\mathrm{Q}_j}, \qquad y = \frac{y_0}{\sqrt{\mathrm{Q}_j}},$$

x_0 et y_0 étant premiers entre eux, et tels que $ax^2 + b\mathrm{P}_i xy + c\mathrm{L}y^2$ soit premier à DL. Posons, pour abréger,

$$\frac{\mathrm{DP}_i}{\sigma^2\varepsilon^2} = \mathrm{D}_1,$$

on aura, d'après une transformation connue,

$$\sum \frac{2^\mu}{m^{1+\rho}} = \theta \frac{\sum \frac{1}{n^{1+\rho}} \sum \left(\frac{D_1}{n}\right) \frac{1}{n^{1+\rho}}}{\sum \frac{1}{n^{2+2\rho}}},$$

n étant seulement assujetti à être premier à $2DL$, $\theta = 1$ dans les deux cas où m est nécessairement impair, et $\theta = \frac{2^{\rho+1}+1}{2^{\rho+1}-1}$ dans le dernier. On a, par suite,

$$(17) \qquad \sum_{a,b,c} \sum_{x,y} \sum_{n} \frac{1}{(an^2x^2 + bP_i n^2xy + cLn^2y^2)^{1+\rho}} = \varkappa 2^\lambda \theta \sum \frac{1}{n^{1+\rho}} \sum \left(\frac{D_1}{n}\right) \frac{1}{n^{1+\rho}}.$$

Dans le cas où DL est pair, le complexe des nombres nx et ny est identique au complexe des nombres x', y', tels que la forme

$$ax'^2 + bP_i x'y' + cLy'^2$$

soit première avec DL. Mais, dans le cas où DL est impair, on a

$$\sum_{x',y'} \frac{1}{(ax'^2 + bP_i x'y' + cLy'^2)^{1+\rho}} = \sum_{l} \frac{1}{2^{2l+2l\rho}} \sum_{n;\, x,y} \frac{1}{(an^2x^2 + bP_i n^2xy + cLn^2y^2)^{1+\rho}};$$

d'où

$$(32) \qquad \sum_{a,b,c} \sum_{x',y'} \frac{1}{(ax'^2 + bP_i x'y' + cLy'^2)^{1+\rho}} = \theta\zeta\varkappa 2^\lambda \sum_{n} \frac{1}{n^{1+\rho}} \sum_{n} \left(\frac{D_1}{n}\right) \frac{1}{n^{1+\rho}},$$

$\zeta = 1$, $\frac{2^{2\rho+2}}{2^{2\rho+2}-1}$ suivant que DL est pair ou impair. Je multiplie par ρ les deux membres de l'égalité (32), et je fais tendre ρ vers zéro. La limite de $\theta\zeta$ est 1, $\frac{4}{3}$, 4 suivant le cas.

La limite de $\rho \sum \frac{1}{n^{1+\rho}}$ est $\frac{\varphi(2DL)}{2DL}$. Enfin $\sum_{n} \left(\frac{D_1}{n}\right) \frac{1}{n^{1+\rho}}$ a pour limite

$$\sum \left(\frac{D_1}{n}\right) \frac{1}{n}.$$

Il reste à trouver la limite du premier membre. Pour cela, je vais étudier la formation des nombres x', y'. Avant tout, x'_0 est premier avec Q'_j, et y'_0 avec Q_j.

Remarquons que, dans toutes les formes que nous avons prises comme représentant chaque classe, on peut supposer a premier avec DL. Il suffit de montrer qu'on peut déterminer une substitution $\begin{pmatrix} \alpha\sqrt{Q_j}, & \dfrac{\beta L}{\sqrt{Q_j}} \\ \dfrac{\gamma}{\sqrt{Q_j}}, & \delta\sqrt{Q_j} \end{pmatrix}$, telle que

$$a\alpha^2 Q_j + bP_i\alpha\gamma + c\gamma^2 Q'_j$$

ne soit divisible par aucun facteur premier f de DL. Si f divise a et c, il ne peut diviser bP_i; on prendra donc pour α et γ des nombres non divisibles par f. Si l'un au moins des deux coefficients extrêmes, a, par exemple, n'est pas divisible par f, et que, de plus, f ne divise pas L, on prendra pour γ un multiple de f; si f divise L, on fera entrer dans Q'_j celui des modules qui le contient.

Distinguons maintenant deux cas :

1° D *est premier avec* L. — Alors a et c sont premiers avec P_i.

J'exprime que $aQ_j x'^2_0 + bP_i x'_0 y'_0 + cQ'_j y'^2_0$ est premier.

(A) avec Q_j.

Il suffit évidemment d'exprimer que $bP_i x'_0 + cQ'_j y'_0$ est premier avec Q_j. Soient Q_{j1} le produit des modules communs à P_i et à Q_j, et $Q_j = Q_{j1} Q_{j2}$. c, Q'_j et y'_0 sont premiers avec Q_{j1} ; il en est donc de même de $bP_i x'_0 + cQ'_j y'_0$. Q_{j2} est un diviseur de P'_i et, par suite, premier avec bP_i. Soit R_{j2} un reste quelconque de Q_{j2} premier avec Q_{j2}. La congruence

$$bP_i x'_0 + cQ'_j y'_0 \equiv R_{j2} \pmod{Q_{j2}}$$

donnera pour une valeur quelconque de y'_0 $(\bmod Q_{j2})$ une valeur de x'_0 $(\bmod Q_{j2})$.

(B) avec Q'_j.

Soient Q'_{j1} le produit des modules communs à P_i et à Q'_j, et $Q'_j = Q'_{j1} Q'_{j2}$, R'_{j2} un reste quelconque de Q'_{j2} premier avec Q'_{j2}, on posera

$$aQ_j x'_0 + bP_i y'_0 \equiv R'_{j2} \pmod{Q'_{j2}},$$

ce qui, pour toute valeur de x'_0 $(\bmod Q'_{j2})$ donnera une valeur de y'_0 par rapport au même module.

(C) avec D :

Si D est impair, $4aQ_j$ est premier avec D : il suffit donc d'exprimer que

$$4a^2 Q_j^2 x'^2_0 + 4abP_i Q_j x'_0 y'_0 + 4acL y'^2_0 = (2aQ_j x'_0 + bP_i y'_0)^2 - DP_i y'^2_0,$$

et, par suite, que $2aQ_jx'_0 + bP_iy'_0$ est premier avec D. Soit $\mathcal{R}$ un reste quelconque (mod D) et premier avec D, la congruence

$$2aQ_jx'_0 + bP_iy'_0 \equiv \mathcal{R} \quad (\text{mod } D)$$

fournit pour toute valeur de y'_0 (mod D) une valeur de x'_0 (mod D).

Si D est pair, il est nécessairement divisible par 4; je suppose d'abord $\frac{D}{4}$ impair. Soit $\mathcal{R}$ un reste $\left(\text{mod } \frac{D}{4}\right)$, on aura les deux congruences

$$aQ_jx'_0 + \frac{b}{2}P_iy'_0 \equiv \mathcal{R} \quad \left(\text{mod } \frac{D}{4}\right)$$

et

$$aQ_jx'_0 + \frac{bP_i}{2}y'_0 \equiv y'_0 \quad (\text{mod } 2).$$

Si D est divisible par 8, il suffit de vérifier la congruence

$$aQ_jx'_0 + \frac{b}{2}P_iy'_0 \equiv \mathcal{R} \quad \left(\text{mod } \frac{D}{4}\right).$$

En résumé, les valeurs de x'_0 et de y'_0 forment des progressions arithmétiques ayant pour raisons respectives $\Delta Q'_j Q_{j2}$ et $\Delta Q_j Q'_{j2}$.

Le nombre des systèmes de valeurs de x'_0 et de y'_0 pour lesquels ces quantités sont positives et moindres que les raisons est dans tous les cas $\Delta\,\varphi(\Delta L)\,\varphi(P'_i)$.

Par suite, en appelant N le nombre des modules du groupe et h le nombre des classes,

$$\rho \sum_{a,\,b,\,c} \sum_{x',\,y'} \frac{1}{(ax'^2 + bP_ix'y' + cLy'^2)^{1+\rho}}$$

a pour limite

$$\frac{2^{N+1}\pi\,\varphi(\Delta L)\,\varphi(P'_i)\,h}{\Delta^{\frac{3}{2}} P_i^{\frac{1}{2}} L P'_i}.$$

2° D *n'est pas premier avec* L. — Comme b est premier avec P'_i, tout facteur commun à D et à L divise P_i. a étant premier avec DL, ces facteurs divisent c. Si Q_j contient l'un quelconque des modules qui ne sont pas premiers avec c, la forme ne pourra être première à DL. Soit P_c le produit de ces modules : Q_j sera un diviseur de P'_c; soit $P'_c = Q_jQ''_j$, et l'on aura

$$aQ_jx'^2_0 + bP_ix'_0y'_0 + cP_cQ''_jy'^2_0;$$

nous sommes en présence d'une forme $(a,\ bP_c,\ cP_c)$, dans laquelle le produit des modules est P'_c, et le déterminant DP_c est premier avec P'_c. Nous sommes ramenés au cas précédent. Par suite,

$$\rho \sum_{a,b,c} \sum_{x',y'} \frac{1}{(ax'^2 + bP_i x'y' + cLy'^2)^{1+\rho}}$$

a pour limite

$$\frac{2^{N_1+1}\pi\,\varphi(\Delta L)\,\varphi(P'_i)\,h}{\Delta^{\frac{3}{2}} P_i^{\frac{1}{2}} LP'_i},$$

N_1 désignant le nombre des modules du groupe qui entrent dans P'_c.

Soient $\theta' = \frac{1}{2}$ si DL est impair et $\theta' = 1$ si DL est pair. On a, par suite, D étant premier avec L,

$$(33)\qquad h = \theta\theta'\zeta\varkappa\, 2^{\lambda-N-1} \frac{(\Delta P_i)^{\frac{1}{2}} P'_i}{\pi\,\varphi(P'_i)} \sum_n \left(\frac{D_1}{n}\right)\frac{1}{n}$$

et, D n'étant pas premier avec L,

$$(34)\qquad h = \theta\theta'\zeta\varkappa\, 2^{\lambda-N_1-1} \frac{(\Delta P_i)^{\frac{1}{2}} P'_i}{\pi\,\varphi(P'_i)} \sum_n \left(\frac{D_1}{n}\right)\frac{1}{n}.$$

Dans les séries $\sum\left(\frac{D_1}{n}\right)\frac{1}{n}$, n est assujetti à être premier à $2DL$. Soit δ^2 le plus grand carré contenu dans D_1, et $D_1 = -\delta^2 P$ si D_1 contient une puissance paire de 2, $D_1 = -2\delta^2 P$ si D_1 contient une puissance impaire de 2. $\left(\frac{D_1}{n}\right) = \left(\frac{-P}{n}\right)$ ou $\left(\frac{-2P}{n}\right)$ suivant le cas. Soient $f_i (i = 1, 2, \ldots, k)$ les facteurs premiers impairs de DL qui n'entrent pas dans D_1. Supposons, pour fixer les idées, $-P \equiv 1 \pmod 4$. On a

$$\left(\frac{-P}{n}\right) = \left(\frac{n}{P}\right), \qquad \sum\left(\frac{D_1}{n}\right)\frac{1}{n} = \sum\left(\frac{n}{P}\right)\frac{1}{n},$$

n étant premier avec $2DL$. Désignons par m un nombre quelconque. La somme $\sum_m \left(\frac{m}{P}\right)\frac{1}{m}$ se compose de la somme $\sum_n \left(\frac{n}{P}\right)\frac{1}{n}$, moins la somme étendue aux nombres qui admettent les diviseurs 2 ou f_i; on a, par suite,

$$\sum_n \left(\frac{D_1}{n}\right)\frac{1}{n} = \left[1 - \left(\frac{2}{P}\right)\frac{1}{2}\right] \prod_i \left[1 - \left(\frac{f_i}{P}\right)\frac{1}{f_i}\right] \sum_m \left(\frac{m}{P}\right)\frac{1}{m}.$$

Or on a, $-\mathrm{P}$ étant, par hypothèse, resté quadratique de f_i,

$$\left(\frac{-\mathrm{P}}{f_i}\right)=1 \quad \text{et} \quad \left(\frac{f_i}{\mathrm{P}}\right)=\left(\frac{-\mathrm{P}}{f_i}\right).$$

Donc

$$\sum_n \left(\frac{\mathrm{D}_1}{n}\right)=\left[1-\left(\frac{2}{\mathrm{P}}\right)\frac{1}{2}\right]\prod_i\left(1-\frac{1}{f_i}\right)\sum_m\left(\frac{m}{\mathrm{P}_1}\right)\frac{1}{m}; \tag{35}$$

on est ramené ainsi au calcul d'une série connnue. On a de même

$$\text{Pour } \frac{\mathrm{D}_1}{\delta^2}\equiv 3 \pmod 4 \ldots \quad \sum_n\left(\frac{\mathrm{D}_1}{n}\right)\frac{1}{n}=\prod\left(1-\frac{1}{f_i}\right)\sum_m\left(\frac{m}{\mathrm{P}}\right)(-1)^{\frac{m-1}{2}}\frac{2}{m}$$

$$\text{Pour } \frac{\mathrm{D}_1}{\delta^2}\equiv 2 \pmod 8 \ldots \quad \sum_n\left(\frac{\mathrm{D}_1}{n}\right)\frac{1}{n}=\prod\left(1-\frac{1}{f_i}\right)\sum_m\left(\frac{m}{\mathrm{P}}\right)(-1)^{\frac{m^2-1}{8}}\frac{1}{m}$$

$$\text{Pour } \frac{\mathrm{D}_1}{\delta^2}\equiv 6 \pmod 8 \ldots \quad \sum_n\left(\frac{\mathrm{D}_1}{n}\right)\frac{1}{n}=\prod\left(1-\frac{1}{f_i}\right)\sum_m\left(\frac{m}{\mathrm{P}}\right)(-1)^{\frac{m^2+4m-5}{8}}\frac{1}{m}.$$

Dans ces trois dernières séries, m est un nombre impair quelconque.

VI.

Proposons-nous maintenant la recherche des points singuliers offerts par l'équation fuchsienne qu'engendre un groupe donné par ses modules. Une substitution de période n

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

peut être aussi caractérisée par l'équation de ses points doubles

$$\gamma z^2+(\delta-\alpha)\mathrm{P}_i z-\beta \mathrm{L}=0, \tag{36}$$

car on connaît ainsi γ, β et $\delta-\alpha$ et $(\alpha+\delta)\sqrt{\mathrm{P}_i}=2\cos\frac{\pi}{n}$. Le discriminant de la forme $(\gamma, \delta-\alpha, \beta)$ est $-4\mathrm{P}_i\sin^2\frac{\pi}{n}$. Toutes les substitutions qui correspondent à des formes d'une même classe ont des points doubles homologues les uns des autres dans le groupe donné et, par suite, correspondent à un même point singulier de l'équation fuchsienne.

Réciproquement, étant donnée une forme

$$a x^2+b \mathrm{P}_k \mathrm{P}_i x y+c \mathrm{L} y^2,$$

$$\mathrm{P}_k\left(b^2 \mathrm{P}_k \mathrm{P}_i-4 a c \frac{\mathrm{P}'_i}{\mathrm{P}_k}\right)=-4\sin^2\frac{\pi}{n}, \tag{37}$$

dans laquelle P_i et P_k sont deux produits de modules différents, et où b est premier avec $\frac{P'_i}{P_k}$, si l'on pose

$$\gamma = a, \qquad \delta - \alpha = b P_k, \qquad \beta = - c, \qquad (\alpha + \delta)\sqrt{P_i} = 2 \cos \frac{\pi}{n}, \tag{38}$$

on aura identiquement

$$\alpha\delta P_i - \beta\gamma P'_i = 1;$$

pour que, à la forme donnée corresponde une substitution linéaire de période n, il suffit que α, β, γ, δ fournis par les formules (38) aient des valeurs entières. Cela ne peut avoir lieu que pour $n = \infty$, 2, 3, 4, 6.

1° $n = \infty$. On a

$$(\alpha + \delta)\sqrt{P_i} = 2,$$

donc ou bien

$$\alpha + \delta = 2, \qquad P_i = 1, \tag{A}$$

donc,

$$b^2 P_k - 4ac P'_k = 0;$$

or b est premier avec P'_k, donc

$$P'_k = 1, \qquad P_k = L;$$

bL est nécessairement pair, donc $\delta - \alpha$ fourni par (38) est pair, et les valeurs de α, β, γ, δ sont entières. Il y a donc dans chaque groupe des substitutions paraboliques de cette espèce

$$\alpha + \delta = 1, \qquad P_i = 4, \tag{B}$$

ce qui exige que 4 soit un des modules du groupe; on a ensuite

$$4 b^2 P_k - ac P'_k = 0,$$

$\delta - \alpha$ doit être impair : il en est donc de même de b et de P_k; ainsi P'_k contient le module 4, et l'on aura

$$b^2 P_k - ac \frac{P'_k}{4} = 0.$$

Tout groupe à module 4 contiendra de ces substitutions. Exemple : dans le groupe au module unique 4, $\left(z, \frac{-4}{z+4}\right)$.

2° $n = 2$:

$$\alpha + \delta = 0, \qquad P_k\left(b^2 P_k P_i - 4ac \frac{P'_i}{P_k}\right) = -4.$$

Donc

$$P_k = 1,\ 2,\ 4.$$

$$P_k = 1, \qquad b^2 P_i - 4ac P'_i = -4, \tag{A}$$

$b\mathrm{P}_k = b$ est nécessairement pair; on aura donc

$$\left(\frac{b}{2}\right)^2 \mathrm{P}_i - ac\mathrm{P}'_i = -1.$$

Il faut et il suffit, pour qu'on puisse former ces substitutions, que $-\mathrm{P}_i$ soit reste quadratique de P'_i.

(B) $$\mathrm{P}_k = 2;$$

2 est donc un des modules.

$$b^2\mathrm{P}_i - ac\mathrm{P}'_i = -1;$$

P_i ne contient pas le module 2; par suite, toute solution de cette équation donne un b impair. Il faut que $-\mathrm{P}_i$ soit reste quadratique de $\frac{\mathrm{P}'_i}{2}$. Exemple : dans le groupe à modules 2 et 5, $\left(z, \frac{-3z-10}{z+3}\right)$.

(C) $$\mathrm{P}_k = 4.$$

On a

$$4b^2\mathrm{P}_i - 4ac\frac{\mathrm{P}'_i}{\mathrm{P}_k} = -1,$$

égalité impossible. Il faut donc rejeter cette hypothèse.

3° $n = 3$:

$$\alpha + \delta = \mathrm{P}_i = 1, \qquad \mathrm{P}_k\left(b^2\mathrm{P}_k\mathrm{P}_i - 4ac\frac{\mathrm{P}'_i}{\mathrm{P}_k}\right) = -3, \qquad \mathrm{P}_k = 1,\ 3.$$

(A) $$\mathrm{P}_k = 1, \qquad b^2 - 4ac\mathrm{L} = -3,$$

b doit être premier avec L qui ne contient pas le facteur; -3 doit être reste quadratique de $4\mathrm{L}$; L est donc impair, et ses facteurs premiers sont de la forme $3n+1$. Ces conditions étant réalisées, b est impair, et les valeurs des coefficients sont entières.

(B) $$\mathrm{P}_k = 3, \qquad 3b^2 - 4ac\frac{\mathrm{L}}{3} = -1,$$

un des modules est égal à 3; $\frac{\mathrm{L}}{3}$ ne contient pas 3, et -3 doit être reste quadratique de $4\frac{\mathrm{L}}{3}$, ce qui exige que L soit impair, et que $\frac{\mathrm{L}}{3}$ ne contienne que des facteurs de la forme $3n+1$. Exemple : modules 3 et 7, $\left(z, \frac{-4z-21}{z+5}\right)$.

4° $n = 4$.

$$\alpha + \delta = 1, \qquad \mathrm{P}_i = 2, \qquad \mathrm{P}_k\left(2b^2\mathrm{P}_k - 2ac\frac{\mathrm{L}}{\mathrm{P}_k}\right) = -2;$$

un des modules est égal à 2. On a ensuite

$$P_k = 1 \qquad \text{et} \qquad b^2 - acL = -1.$$

-1 devant être reste quadratique de L, tous ses facteurs premiers impairs seront de la forme $4n+1$.

5° $n = 6$.

$$\alpha + \delta = 1, \qquad P_i = 3, \qquad P_k\left(b^2 P_k P_i - 4ac\frac{P'_i}{P_k}\right) = -1;$$

donc

$$P_k = 1, \qquad 3b^2 - 4ac\frac{L}{3} = -1.$$

Donc L est impair, et, à part, 3 ne contient que des facteurs premiers de la forme $3n+1$.

Quand on aura déterminé les différentes espèces de points singuliers qui peuvent se présenter, il faudra encore chercher le nombre des points singuliers de chaque espèce ou le nombre des classes de formes correspondantes. Une forme pour laquelle $D = 0$ est le carré d'une forme linéaire $cx + dy$, dans laquelle les coefficients de x et de y sont premiers entre eux. La théorie de ces formes linéaires est analogue à celle des formes du second degré. Il suffit de reconnaître combien il y a de fractions $-\frac{d}{c}$ non homologues entre elles par rapport au groupe.

Pour le nombre des autres points singuliers dans chaque espèce, il est donné par les formules du § V.

Exemple. — Dans le groupe à modules 2, 3 et 5, $-15 = -P_i$ est reste quadratique de $\frac{P'_i}{2} = 1$. Il y a donc des substitutions de période 2 avec $P_k = 2$, $P_i = 15$. Pour les formes correspondantes

$$D_1 = -15, \qquad \Delta P_i = 60, \qquad \theta = 1,$$
$$\zeta = 1, \qquad \theta' = 1, \qquad \varkappa = 4, \qquad \lambda = 0, \qquad N_1 = 2, \qquad P_c = 2;$$

donc, d'après (34),

$$h = \frac{2\sqrt{15}}{\pi}\sum\left(\frac{-15}{n}\right)\frac{1}{n} = \sum\left(\frac{\alpha'}{15}\right),$$

α étant l'un quelconque des nombres premiers avec 15 et < 15. D'où

$$h = 2.$$

VII.

La théorie précédente est susceptible de généralisation dans plusieurs sens différents.

1° *Groupes à plusieurs systèmes de modules.* — Imaginons un système de substitutions linéaires à coefficients entiers et à déterminant 1

$$\begin{pmatrix} m^{(1)}, & n^{(1)} \\ p^{(1)}, & q^{(1)} \end{pmatrix}, \quad \begin{pmatrix} m^{(2)}, & n^{(2)} \\ p^{(2)}, & q^{(2)} \end{pmatrix}, \quad \begin{pmatrix} m^{(3)}, & n^{(3)} \\ p^{(3)}, & q^{(3)} \end{pmatrix}, \quad \ldots, \quad \begin{pmatrix} m^{(r)}, & n^{(r)} \\ p^{(r)}, & q^{(r)} \end{pmatrix},$$

et plusieurs systèmes de nombres entiers contenant chacun la même totalité de nombres

$$\begin{array}{ll} a_1^{(1)},\ a_2^{(1)},\ \ldots,\ a_n^{(1)}; & a_1^{(1)} a_2^{(1)} \ldots a_n^{(1)} = \mathrm{L}^{(1)}, \\ a_1^{(2)},\ a_2^{(2)},\ \ldots,\ a_n^{(2)}; & a_1^{(2)} a_2^{(2)} \ldots a_n^{(2)} = \mathrm{L}^{(2)}, \\ \ldots,\ \ldots,\ \ldots,\ \ldots; & \ldots\ \ldots\ldots\ldots\ldots, \\ a_1^{(r)},\ a_2^{(r)},\ \ldots,\ a_n^{(r)}; & a_1^{(r)} a_2^{(r)} \ldots a_n^{(r)} = \mathrm{L}^{(r)}, \end{array}$$

je les nommerai *systèmes de modules*. Les modules d'un même système sont premiers entre eux deux à deux. Je désignerai par $\mathrm{P}_i^1, \mathrm{P}_i^2, \ldots, \mathrm{P}_i^{(r)}$ des produits de modules correspondants, chaque module ne pouvant figurer plus d'une fois dans le produit correspondant. Soient A, B, Γ, Δ des entiers satisfaisant aux conditions suivantes :

$$\mathrm{A}\Delta - \mathrm{B}\Gamma = \mathrm{P}_i^{(1)} \mathrm{P}_i^{(2)} \ldots \mathrm{P}_i^{(r)},$$

$\dfrac{\mathrm{A}+\Delta}{\mathrm{P}_i^1}$ et $\dfrac{2\Gamma m^{(1)} n^{(1)} + (\Delta - \mathrm{A})(n^{(1)} p^{(1)} + m^{(1)} q^{(1)}) - 2\mathrm{B} p^{(1)} q^{(1)}}{\mathrm{P}_i^{(1)}}$ sont entiers et de même parité. $\Gamma n^{(1)2} + (\Delta - \mathrm{A}) n^{(1)} q^{(1)} - \mathrm{B} q^{(1)2}$ est divisible par $\mathrm{L}^{(1)}$. Il en est de même relativement à chaque système de modules. $\dfrac{\mathrm{A}z + \mathrm{B}}{\Gamma z + \Delta}$ sera l'expression générale des substitutions d'un groupe.

Comme exemple, je citerai le groupe formé par les deux espèces de substitutions

$$\left(z, \frac{\alpha z + 3\beta}{2\gamma z + \delta}\right), \quad \left(z, \frac{6\alpha z + 3\beta}{2\gamma z + 6\delta}\right);$$

dans le premier cas, $\alpha\delta - 6\beta\gamma = 1$; dans le second cas, $6\alpha\delta - \beta\gamma = 1$.

2° *Groupes à coefficients irrationnels.* — Je prendrai comme exemple le groupe engendré par les deux substitutions

$$(z,\ z+1),\quad \left(z,\ \frac{-3+\sqrt{5}}{2z}\right).$$

On vérifie que les substitutions peuvent se classer en deux espèces, les uns à déterminant 1, les autres à déterminant $6-2\sqrt{5}$. Mais ces conditions ne suffisent pas, comme lorsque les coefficients sont entiers, à définir le groupe.

3° Nous savons que les nombres de la forme $a+bi$, où a et b sont entiers, jouissent des mêmes propriétés que les nombres entiers au point de vue de la divisibilité. Nous pourrons donc former un système de nombres complexes premiers entre eux deux à deux, qui seront les *modules*. Soient P_i un produit de ces modules et L le produit de tous les modules. Si l'on pose

$$\lambda = \alpha P_i(x+iy)+\beta L,$$
$$\mu = \gamma(x+iy)+\delta P_i,$$

α, β, γ, δ étant quatre nombres complexes satisfaisant à la relation

$$\alpha\delta P_i - \beta\gamma P'_i = 1,$$

les substitutions

$$\begin{pmatrix} x+iy, & \dfrac{\lambda\mu_0+\alpha P_i\gamma_0 z^2}{\mu\mu_0+\alpha\alpha_0 P_i P_{i_0} z^2} \\ z, & \dfrac{z^2}{\mu\mu_0+\alpha\alpha_0 P_i P_{i_0} z^2} \end{pmatrix}$$

forment un groupe discontinu.