
SUR

CERTAINS GROUPES FUCHSIENS

FORMÉS AVEC LES RACINES D'ÉQUATIONS BINOMES,

PAR M. X. STOUFF,

Maître de Conférences à la Faculté des Sciences de Montpellier.

I.

Le présent travail a pour objet d'indiquer une nouvelle méthode pour obtenir des groupes fuchsien dont une partie sont, il est vrai, des transformés de groupes fuchsien à coefficients entiers ⁽¹⁾, mais dont une infinité ne peuvent, par aucune transformation, acquérir de pareils coefficients.

Soit j une racine primitive de l'équation

$$x^p = 1,$$

où le nombre entier p est premier. Je considère la substitution

$$S_j \left(z, \frac{a_j z + b_j}{c_j z + d_j} \right),$$

dont les coefficients sont formés comme il suit

$$(1) \quad \left\{ \begin{array}{l} a_j = \sum_{h=1}^{\frac{p-1}{2}} \alpha_h (j^h + j^{-h}), \\ b_j = \sum_{h=1}^{\frac{p-1}{2}} \beta_h (j^h + j^{-h}), \\ c_j = \sum_{h=1}^{\frac{p-1}{2}} \gamma_h (j^h + j^{-h}), \\ d_j = \sum_{h=1}^{\frac{p-1}{2}} \delta_h (j^h + j^{-h}); \end{array} \right.$$

⁽¹⁾ Voir, sur les groupes fuchsien à coefficients entiers, *Les fonctions fuchsiennes et l'Arithmétique*, par M. Poincaré (*Journal de Liouville*; 1887).

les $\alpha_h, \beta_h, \gamma_h, \delta_h$ sont des nombres entiers tels que

$$(2) \quad a_j d_j - b_j c_j = 1.$$

Les substitutions S_j forment un groupe. Mais, même en tenant compte de la condition (2), les coefficients de S_j contiennent encore trop d'entiers variant indépendamment les uns des autres pour que ce groupe soit discontinu : il faut établir entre eux de nouvelles relations.

Je considère une substitution

$$\Sigma_j \left(z, \frac{m_j z + n_j}{p_j z + q_j} \right),$$

$$m_j q_j - n_j p_j = \Delta_j,$$

où

$$(3) \quad \left\{ \begin{array}{l} m_j = \sum_{h=1}^{\frac{p-1}{2}} \mu_h (j^h + j^{-h}), \\ n_j = \sum_{h=1}^{\frac{p-1}{2}} \nu_h (j^h + j^{-h}), \\ p_j = \sum_{h=1}^{\frac{p-1}{2}} \pi_h (j^h + j^{-h}), \\ q_j = \sum_{h=1}^{\frac{p-1}{2}} \gamma_h (j^h + j^{-h}), \end{array} \right.$$

où les $\mu_h, \nu_h, \pi_h, \gamma_h$ sont des entiers. Désignons par ρ une racine primitive au sens arithmétique du nombre p , et par S_{j^x}, Σ_{j^x} ce que deviennent S_j et Σ_j quand on y remplace j par j^x . Je suppose de plus que Σ_j soit telle que, en multipliant Σ_j par Σ_{j^2} , puis le produit par Σ_{j^4} , et ainsi de suite, la dernière substitution employée comme facteur étant $\Sigma_{j^{\frac{p-3}{2}}}$, on obtienne la substitution unité et on l'obtienne pour la première fois

$$(4) \quad \prod_{h=0}^{k=\frac{p-3}{2}} \Sigma_{j^{\rho^h}} = 1;$$

ceci posé, la substitution Σ_j restant fixe, j'impose aux substitutions S_j la

condition

$$(5) \quad \mathbf{S}_{j^{\rho}} = \Sigma_j^{-1} \mathbf{S}_j \Sigma_j.$$

Les substitutions qui satisfont à la condition (5) forment un groupe, car il est évident que, si deux substitutions satisfont à cette condition, leur produit y satisfait aussi. L'équation (5) entraîne toutes celles que l'on en peut déduire en remplaçant la racine j par une racine primitive d'indice p de l'unité, à cause de l'irréductibilité de l'équation qui fournit ces racines. On aura donc

$$(6) \quad \mathbf{S}_{j^{\rho^k}} = \Sigma_{j^{\rho^{k-1}}}^{-1} \mathbf{S}_{j^{\rho^{k-1}}} \Sigma_{j^{\rho^{k-1}}}, \quad k = 0, 1, \dots, \frac{\rho-3}{2};$$

en appliquant les formules qui donnent les coefficients de la transformée d'une substitution par une autre substitution, les équations (6) donnent

$$(7) \quad \begin{cases} a_{j^{\rho}} = (a_j m_j q_j + b_j p_j q_j - c_j m_j n_j - d_j n_j p_j) \sigma_j, \\ b_{j^{\rho}} = (a_j n_j q_j + b_j q_j^2 - c_j n_j^2 - d_j n_j q_j) \sigma_j, \\ c_{j^{\rho}} = (-a_j m_j p_j - b_j p_j^2 + c_j m_j^2 + d_j m_j p_j) \sigma_j, \\ d_{j^{\rho}} = (-a_j n_j p_j - b_j p_j q_j + c_j m_j n_j + d_j m_j q_j) \sigma_j. \end{cases}$$

On déduit de (2) et de (7)

$$a_{j^{\rho}} d_{j^{\rho}} - b_{j^{\rho}} c_{j^{\rho}} = 1$$

et

$$a_{j^{\rho}} d_{j^{\rho}} - b_{j^{\rho}} c_{j^{\rho}} = (a_j d_j - b_j c_j) \Delta_j^3 \sigma_j^2;$$

donc

$$\sigma_j = \pm \frac{1}{\Delta_j} = \frac{\varepsilon}{\Delta_j}, \quad \varepsilon = \pm 1,$$

Les équations complexes (7) équivalent à $2p - 2$ équations rationnelles entre les $2p - 2$ entiers $\alpha_h, \beta_h, \gamma_h, \delta_h$. Mais on peut choisir ε de telle sorte que $2p - 6$ seulement de ces équations soient distinctes. Il suffit de montrer que quatre combinaisons de ces $2p - 2$ équations rationnelles sont identiques. En effet, les équations obtenues en remplaçant dans (7) $j^{\frac{p-3}{2}}$ fois successivement par j^{ρ} sont toutes des combinaisons de ces $2p - 2$ équations rationnelles et permettront, par des substitutions successives, d'exprimer $a_j^{\rho^{\frac{p-1}{2}}}, b_j^{\rho^{\frac{p-1}{2}}}, c_j^{\rho^{\frac{p-1}{2}}}, d_j^{\rho^{\frac{p-1}{2}}}$ en a_j, b_j, c_j, d_j . Les équations résultantes ne sont autres que celles que l'on obtiendrait en exprimant l'égalité

$$\mathbf{S}_{j^{\rho^{\frac{p-1}{2}}}} = \left(\prod_{k=0}^{\frac{p-3}{2}} \Sigma_{j^{\rho^k}} \right)^{-1} \mathbf{S}_j \left(\prod_{k=0}^{\frac{p-3}{2}} \Sigma_{j^{\rho^k}} \right)$$

et, en tenant compte de l'équation (4) et en remarquant que

$$S_j \rho^{\frac{p-1}{2}} = S_j,$$

il vient pour ces équations

$$a_j = \varepsilon^{\frac{p-1}{2}} a_j, \quad b_j = \varepsilon^{\frac{p-1}{2}} b_j, \quad c_j = \varepsilon^{\frac{p-1}{2}} c_j.$$

Pour que ces quatre équations soient vérifiées par des valeurs de a_j, b_j, c_j, d_j qui ne soient pas toutes nulles, ce qui est nécessaire pour notre problème, il faut que

$$(8) \quad \frac{p-1}{\varepsilon^2} = 1;$$

donc il faut prendre $\varepsilon = 1$, si p est de la forme $4n + 3$. On pourra prendre $\varepsilon = \pm 1$, si p est de la forme $4n + 1$. On voit facilement que la valeur de ε relative au produit de deux substitutions est le produit des ε relatifs à ces substitutions. Lorsque p est de la forme $4n + 3$, il n'y a donc qu'une seule espèce de substitutions; mais, lorsque p est de la forme $4n + 1$, il y en a deux espèces, les substitutions correspondant à $\varepsilon = +1$, que nous pourrions appeler *substitutions paires*, et les substitutions correspondant à $\varepsilon = -1$, que nous nommerons *substitutions impaires*. Les substitutions paires forment un sous-groupe; le produit de deux substitutions impaires est une substitution paire; le produit d'une substitution impaire par une substitution paire est une substitution impaire.

Les $\alpha_h, \beta_h, \gamma_h, \delta_h$ devant être des nombres entiers, les équations (7) donnent lieu, non seulement, comme nous l'avons vu, à $2p - 2$ équations, mais aussi à $2p - 2$ congruences par rapport à la norme de Δ_j considérée comme module. La théorie de ces congruences est parallèle à celle des équations.

L'équation (8) étant satisfaite, il n'en reste que $2p - 6$ de distinctes.

Les équations (7) étant satisfaites, des $2p - 2$ entiers $\alpha_h, \beta_h, \gamma_h, \delta_h$, il n'en reste plus que quatre arbitraires. Remarquons que le déterminant $a_j d_j - b_j c_j$ est alors réel; car il ne change pas, lorsqu'on remplace j par j^p . En écrivant l'équation (2), nous n'établissons donc plus qu'une seule relation nouvelle entre ces entiers. Nos groupes contiennent donc trois entiers indépendants. Pour démontrer qu'ils sont discontinus, j'emploierai une

méthode qui a servi à M. Hurwitz pour démontrer la discontinuité du groupe arithmétique (1).

J'envisage d'une manière générale un groupe à coefficients réels

$$\left(z, \frac{az + b}{cz + d} \right), \quad ad - bc = 1,$$

pour reconnaître s'il est continu ou discontinu; je considère pour plus de commodité le groupe isomorphe de substitutions linéaires homogènes à deux variables imaginaires $x + iy$, $u + iv$ dont z est le quotient

$$(9) \quad \begin{cases} \rho(x' + iy') = a(x + iy) + b(u + iv), \\ \rho(u' + iv') = c(x + iy) + d(u + iv). \end{cases}$$

Je désigne, suivant l'usage, par N_0 le conjugué d'un nombre complexe N , et je considère une valeur de z telle que le déterminant

$$D = \begin{vmatrix} x + iy & u + iv \\ x - iy & u - iv \end{vmatrix}$$

ne soit pas nul, ou, ce qui revient au même, une valeur de z qui n'est pas réelle. Je puis décrire autour du point correspondant M un cercle de rayon fini C qui ne coupe, ni ne touche l'axe réel. Je dis qu'il n'existe qu'un nombre fini de substitutions d'un de nos groupes qui transforme le point M en un point intérieur à ce cercle. En effet, soit $\frac{x' + iy'}{u' + iv'}$ un point intérieur à C . Si c'est un transformé de z , on a les équations (9).

Je multiplie le déterminant D par le déterminant

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

et, en tenant compte des équations (9), j'ai

$$D = \rho \rho_0 D' \quad \text{ou} \quad D' = \begin{vmatrix} x' + iy' & u' + iv' \\ x' - iy' & u' + iv' \end{vmatrix},$$

et, en remplaçant ρ et ρ_0 par leurs valeurs tirées de la première des équations

(1) *Mathematische Annalen*, t. XVIII, p. 535.

tions (9), on déduit de

$$\rho\rho_0 = \frac{D}{D'},$$

$$(10) \quad (ax + bu)^2 + (ay + bv)^2 = (x'^2 + y'^2) \frac{D}{D'};$$

mais, si le point $\frac{x' + iy'}{u' + iv'}$ est intérieur au cercle C, la valeur absolue de $\frac{D'}{x'^2 + y'^2}$ reste supérieure à un certain nombre ; le premier membre de (10) étant une somme de deux carrés, il en résulte que la valeur absolue de chacune des deux quantités

$$ax + bu, \quad ay + bv$$

ne peut dépasser un certain nombre : comme le déterminant

$$\begin{vmatrix} x & y \\ u & v \end{vmatrix}$$

n'est autre que le déterminant D à un facteur près et, par suite, n'est pas nul, il en résulte une limitation analogue pour les valeurs absolues de a et de b . On arriverait de même à prouver que les valeurs absolues des coefficients c et d sont limitées.

a, b, c, d sont dans nos groupes des fonctions linéaires et homogènes des quatre entiers que les $2p - 2$ équations (7) laissent seuls indépendants. En résolvant ces formules par rapport à ces quatre entiers, on verra que leurs valeurs absolues sont limitées, et, comme elles sont entières, il n'y aura qu'un nombre fini de substitutions qui puissent transformer M en un point intérieur au cercle C. Donc nos groupes sont discontinus (1).

Remarquons que, si l'on veut que la substitution Σ_j soit rationnelle, auquel cas elle est indépendante de j , p ne peut prendre que les valeurs 5, 7, 13, parce que les seules périodes que puisse posséder une substitution à coefficients entiers sont 2, 3, 4 et 6.

(1) Une marche toute semblable peut servir à prouver qu'un groupe de substitutions linéaires homogènes entières de déterminant 1 à n variables est discontinu par rapport à $n - 1$ systèmes de valeurs de ces variables.

II.

J'applique la théorie précédente à quelques exemples :

1° Soit

$$p = 5, \quad \Sigma_j = \left(z, \frac{-1}{z} \right).$$

Posons

$$(11) \quad \begin{cases} S_j = \left\{ z, \frac{[\alpha_1(j+j^4) + \alpha_2(j^2+j^3)]z + \beta_1(j+j^4) + \beta_2(j^2+j^3)}{[\gamma_1(j+j^4) + \gamma_2(j^2+j^3)]z + \delta_1(j+j^4) + \delta_2(j^2+j^3)} \right\}, \\ S_{j^2} = \left\{ z, \frac{[\alpha_1(j^2+j^3) + \alpha_2(j+j^4)]z + \beta_1(j^2+j^3) + \beta_2(j+j^4)}{[\gamma_1(j^2+j^3) + \gamma_2(j+j^4)]z + \delta_1(j^2+j^3) + \delta_2(j^2+j^4)} \right\}. \end{cases}$$

D'ailleurs la transformée de la substitution S_j par Σ s'exprime par la relation

$$\frac{-1}{z^j} = \frac{[\alpha_1(j+j^4) + \alpha_2(j^2+j^3)] \left(\frac{-1}{z} \right) + \beta_1(j+j^4) + \beta_2(j^2+j^3)}{[\gamma_1(j+j^4) + \gamma_2(j^2+j^3)] \left(\frac{-1}{z} \right) + \delta_1(j+j^4) + \delta_2(j^2+j^3)}$$

ou

$$\Sigma^{-1} S_j \Sigma = \left\{ z, \frac{[\delta_1(j+j^4) + \delta_2(j^2+j^3)]z - \gamma_1(j+j^4) - \gamma_2(j^2+j^3)}{-[\beta_1(j+j^4) + \beta_2(j^2+j^3)]z + \alpha_1(j+j^4) + \alpha_2(j^2+j^3)} \right\}$$

et, en identifiant S_j et $\Sigma^{-1} S_j \Sigma$,

$$\delta_1 = \varepsilon \alpha_2, \quad \delta_2 = \varepsilon \alpha_1, \quad \gamma_2 = -\varepsilon \beta_1, \quad \gamma_1 = -\varepsilon \beta_2,$$

on déduit de ces relations

$$\varepsilon^2 = 1, \quad \varepsilon = \pm 1;$$

de là les deux espèces de substitutions du groupe :

Substitutions impaires

$$\left\{ z, \frac{[\alpha_1(j+j^4) + \alpha_2(j^2+j^3)]z + \beta_1(j+j^4) + \beta_2(j^2+j^3)}{[\beta_1(j^2+j^3) + \beta_2(j+j^4)]z - \alpha_1(j^2+j^3) - \alpha_2(j+j^4)} \right\},$$

avec la relation

$$(12) \quad \alpha_1^2 + \alpha_2^2 - 3\alpha_1\alpha_2 + \beta_1^2 + \beta_2^2 - 3\beta_1\beta_2 = 1.$$

Nous représenterons cette substitution par

$$(\alpha_1, \alpha_2, \beta_1, \beta_2).$$

Substitutions paires

$$\left\{ z, \frac{[\alpha_1(j+j^4) + \alpha_2(j^2+j^3)]z + \beta_1(j+j^4) + \beta_2(j^2+j^3)}{-[\beta_1(j^2+j^3) + \beta_2(j+j^4)]z + \alpha_1(j^2+j^3) + \alpha_2(j+j^4)} \right\}.$$

Nous représenterons cette substitution par

$$[\alpha_1, \alpha_2, \beta_1, \beta_2],$$

on a la relation

$$(13) \quad \alpha_1^2 + \alpha_2^2 - 3\alpha_1\alpha_2 + \beta_1^2 + \beta_2^2 - 3\beta_1\beta_2 = -1.$$

Je désignerai par G_3 ce groupe, que nous étudierons de plus près dans la suite.

2° Soit

$$p = 5, \quad \Sigma_j = \left(z, \frac{z+4}{-z-1} \right),$$

de déterminant 3.

En prenant une substitution S_j sous la forme (11), on a

$$(14) \quad \begin{cases} \alpha_2 = \pm \frac{1}{3}(-\alpha_1 + \beta_1 - 4\gamma_1 + 4\delta_1), \\ \beta_2 = \pm \frac{1}{3}(-4\alpha_1 + \beta_1 - 16\gamma_1 + 4\delta_1), \\ \gamma_2 = \pm \frac{1}{3}(\alpha_1 + \beta_1 + \gamma_1 - \delta_1), \\ \delta_2 = \pm \frac{1}{3}(4\alpha_1 + \beta_1 + 4\gamma_1 - \delta_1), \end{cases}$$

les signes correspondants devant être pris ensemble; pour que $\alpha_2, \beta_2, \gamma_2, \delta_2$ soient entiers, il faut et il suffit que $\alpha_1, \beta_1, \gamma_1, \delta_1$ satisfassent à la congruence unique

$$\alpha_1 - \beta_1 + \gamma_1 - \delta_1 \equiv 0 \pmod{3},$$

et l'on a la relation

$$(15) \quad \begin{cases} 3(\alpha_1\delta_1 - \beta_1\gamma_1) - \frac{1}{3}(4\alpha_1^2 + \beta_1^2 + 16\gamma_1^2 + 4\delta_1^2 - 2\alpha_1\beta_1 + 8\alpha_1\gamma_1 \\ - 2\alpha_1\delta_1 - 2\beta_1\gamma_1 + 2\beta_1\delta_1 - 8\gamma_1\delta_1) = 1. \end{cases}$$

Nous nommerons ce groupe G'_3 .

3° Soit

$$p = 7, \quad \Sigma_j = \left(z, \frac{-1}{z+1} \right),$$

$$S_j \left\{ z, \frac{[\alpha_1(j+j^6) + \alpha_2(j^2+j^5) + \alpha_3(j^3+j^4)]z + \beta_1(j+j^6) + \beta_2(j^2+j^5) + \beta_3(j^3+j^4)}{[\gamma_1(j+j^6) + \gamma_2(j^2+j^5) + \gamma_3(j^3+j^4)]z + \delta_1(j+j^6) + \delta_2(j^2+j^5) + \delta_3(j^3+j^4)} \right\},$$

on a

$$\begin{aligned} \alpha_2 &= -\gamma_1 + \delta_1, & \alpha_3 &= \beta_1 + \delta_1, \\ \beta_2 &= -\gamma_1, & \beta_3 &= -\alpha_1 + \beta_1 - \gamma_1 + \delta_1, \\ \gamma_2 &= \alpha_1 - \beta_1 + \gamma_1 - \delta_1, & \gamma_3 &= -\beta_1, \\ \delta_2 &= \alpha_1 + \gamma_1, & \delta_3 &= \alpha_1 - \beta_1, \end{aligned}$$

et, en exprimant que le déterminant de la substitution est égal à 1, on a la relation

$$(16) \quad 5(\alpha_1\delta_1 - \beta_1\gamma_1) - 2(\alpha_1^2 + \beta_1^2 + \gamma_1^2 + \delta_1^2 - \alpha_1\beta_1 + \alpha_1\gamma_1 - \beta_1\gamma_1 + \beta_1\delta_1 - \gamma_1\delta_1) = 1.$$

Nous désignerons ce groupe par G_7 et nous l'étudierons d'une manière approfondie.

4° Soit

$$p = 13; \quad \Sigma_j \left(z, \frac{6z+3}{-7z-3} \right) \quad (G_{13}),$$

$$S_j \left(z, \frac{z \sum_{h=1}^6 \alpha_h (j^h + j^{-h}) + \sum_{h=1}^6 \beta_h (j^h + j^{-h})}{z \sum_{h=1}^6 \gamma_h (j^h + j^{-h}) + \sum_{h=1}^6 \delta_h (j^h + j^{-h})} \right);$$

on voit immédiatement que β_h doit être divisible par 3; posons

$$\beta_h = 3\beta'_h,$$

on a les relations

$$\begin{aligned} \pm \alpha_6 &= -6\alpha_1 + 21\beta'_1 - 6\gamma_1 + 7\delta_1, \\ \pm \beta_6 &= -\alpha_1 + 3\beta'_1 - \gamma_1 + \delta_1, \\ \pm \gamma_6 &= 14\alpha_1 - 49\beta'_1 + 12\gamma_1 - 14\delta_1, \\ \pm \delta_6 &= 7\alpha_1 - 21\beta'_1 + 6\gamma_1 - 6\delta_1; \end{aligned}$$

$$\begin{aligned} \alpha_3 &= -20\alpha_1 + 84\beta'_1 - 15\gamma_1 + 21\delta_1, \\ \beta_3 &= -4\alpha_1 + 16\beta'_1 - 3\gamma_1 + 4\delta_1, \\ \gamma_3 &= 35\alpha_1 - 147\beta'_1 + 25\gamma_1 - 35\delta_1, \\ \delta_3 &= 21\alpha_1 - 84\beta'_1 + 15\gamma_1 - 20\delta_1; \end{aligned}$$

$$\begin{aligned} \pm \alpha_5 &= -27\alpha_1 + 126\beta'_1 - 18\gamma_1 + 28\delta_1, \\ \pm \beta_5 &= -6\alpha_1 + 27\beta'_1 - 4\gamma_1 + 6\delta_1, \\ \pm \gamma_5 &= 42\alpha_1 - 196\beta'_1 + 27\gamma_1 - 42\delta_1, \\ \pm \delta_5 &= 28\alpha_1 - 126\beta'_1 + 18\gamma_1 - 27\delta_1; \end{aligned}$$

$$\begin{aligned}
\alpha_4 &= -20\alpha_1 + 105\beta'_1 - 12\gamma_1 + 21\delta_1, \\
\beta'_4 &= -5\alpha_1 + 25\beta'_1 - 3\gamma_1 + 5\delta_1, \\
\gamma_4 &= 28\alpha_1 - 147\beta'_1 + 16\gamma_1 - 28\delta_1, \\
\delta_4 &= 21\alpha_1 - 105\beta'_1 + 12\gamma_1 - 20\delta_1; \\
\pm\alpha_2 &= -6\alpha_1 + 42\beta'_1 - 3\gamma_1 + 7\delta_1, \\
\pm\beta'_2 &= -2\alpha_1 + 12\beta'_1 - \gamma_1 + 2\delta_1, \\
\pm\gamma_2 &= 7\alpha_1 - 49\beta'_1 + 3\gamma_1 - 7\delta_1, \\
\pm\delta_2 &= 7\alpha_1 - 42\beta'_1 + 3\gamma_1 - 6\delta_1.
\end{aligned}$$

5° Supposons le nombre premier p quelconque; soient j et j^r deux racines primitives distinctes de l'équation binôme, M_j et M_{j^r} deux nombres complexes réels formés de la même façon, l'un avec la racine j , l'autre avec la racine j^r .

On pourra prendre pour Σ_j

$$\left(z, \frac{M_j}{M_{j^r}} z \right),$$

car il est clair qu'alors la relation (4) est satisfaite.

Par exemple, pour $p = 17$, on pourra utiliser la substitution

$$\left[z, \frac{(j + j^{-1})z}{j^2 + j^{-2}} \right]$$

en prenant $\varphi = 3$.

III.

L'intérêt de nos groupes serait beaucoup diminué s'ils pouvaient se ramener à des groupes à coefficients entiers. Je vais faire voir qu'ils ne s'y ramènent que partiellement.

THÉORÈME I. — *Si les coefficients d'un groupe G et ceux de son transformé G , par une substitution Σ ne contiennent que certaines irrationalités (R, R', R'', \dots), on peut toujours ramener la substitution Σ à ne contenir que ces irrationalités.*

Nous pouvons supposer que le groupe G contient au moins deux substitutions qui ne sont pas de période 2 et qui ne sont pas puissances l'une de l'autre. En effet, cette circonstance se présente dans tous les groupes fuchsien qui offrent quelque intérêt. Soient

$$S \left(z, \frac{az + b}{cz + d} \right), \quad S' \left(z, \frac{a'z + b'}{c'z + d'} \right), \quad \Sigma \left(z, \frac{mz + n}{pz + q} \right)$$

ces substitutions, et

$$S_1 \left(z, \frac{a_1 z + b_1}{c_1 z + d_1} \right), \quad S'_1 \left(z, \frac{a'_1 z + b'_1}{c'_1 z + d'_1} \right)$$

leurs transformées par la substitution Σ , qui appartient à G_1 . On a

$$(17) \quad \begin{cases} amq + bpq - cmn - dpn = \lambda a_1, \\ bq^2 + (a-d) nq - cn^2 = \lambda b_1, \\ cm^2 + (d-a) mp - bp^2 = \lambda c_1, \\ cmn + dmq - anp - bpq = \lambda d_1, \end{cases}$$

et quatre autres équations analogues exprimant la relation qui existe entre S' et S'_1 . De la première et de la quatrième des équations (17), en tenant compte de la troisième de ces équations, je tire

$$\begin{aligned} n &= m \frac{ad_1 - da_1}{(a+d)c_1} + p \frac{b(a_1 + d_1)}{(a+d)c_1}, \\ q &= m \frac{c(a_1 + d_1)}{(a+d)c_1} + p \frac{dd_1 - aa_1}{(a+d)c_1}; \end{aligned}$$

mais l'on aurait de même, en considérant S et S'_1 ,

$$(18) \quad \begin{cases} n = m \frac{a'd'_1 - d'a'_1}{(a'+d')c'_1} + p \frac{b'(a'_1 + d'_1)}{(a'+d')c'_1}, \\ q = m \frac{c'(a'_1 + d'_1)}{(a'+d')c'_1} + p \frac{d'd'_1 - a'a'_1}{(a'+d')c'_1}. \end{cases}$$

On déduit de ces quatre équations homogènes des quantités proportionnelles à m, n, p, q et fonctions rationnelles des coefficients des quatre substitutions S, S_1, S', S'_1 .

On peut prendre ces quantités elles-mêmes pour m, n, p, q , car m, n, p, q ne sont évidemment déterminées qu'à un facteur près, ce qui démontre le théorème.

En particulier, si l'un des groupes est à coefficients entiers, et si l'autre contient seulement les irrationalités $j^h + j^{-h}$, il existera une substitution transformante dont les coefficients ne contiendront que ces irrationalités.

THÉORÈME II. — *Pour qu'un groupe formé avec une racine $p^{\text{ième}}$ de l'unité (d'après le procédé indiqué dans le § I) et une substitution Σ_j puisse être transformé en un groupe à coefficients entiers, il faut et il*

suffit qu'il existe une substitution U_j ne contenant que les irrationalités $j^h + j^{-h}$ et telle que

$$(19) \quad U_{j^2} = U_j \Sigma_j;$$

la condition est nécessaire : supposons qu'un de nos groupes soit le transformé d'un groupe à coefficients entiers par une substitution; cette substitution ne contiendra, d'après le théorème précédent, que les irrationalités $j^h + j^{-h}$; représentons-la par U_j , S_j désignant une quelconque des substitutions de notre groupe, T la substitution correspondante du groupe à coefficients entiers, nous aurons

$$S_j = U_j^{-1} T U_j,$$

d'où

$$S_{j^2} = U_{j^2}^{-1} T U_{j^2};$$

mais

$$S_{j^2} = \Sigma_j^{-1} S_j \Sigma_j = \Sigma_j^{-1} U_j^{-1} T U_j \Sigma_j;$$

donc

$$\Sigma_j^{-1} U_j^{-1} T U_j \Sigma_j = U_{j^2}^{-1} T U_{j^2},$$

$$U_{j^2} \Sigma_j^{-1} U_j^{-1} T U_j \Sigma_j U_{j^2}^{-1} = T.$$

Ainsi la substitution $U_j \Sigma_j U_{j^2}^{-1}$ ne devrait altérer, en la transformant, aucune des substitutions du groupe à coefficients entiers : c'est donc la substitution identique.

La condition est suffisante; je suppose qu'il existe une substitution U_j satisfaisant à la relation (19). Je considère la substitution $T_j = U_j S_j U_j^{-1}$; si l'on y change j en j^2 , elle devient

$$T_{j^2} = U_{j^2} S_{j^2} U_{j^2}^{-1},$$

ou, d'après les relations (5) et (19),

$$T_{j^2} = U_j \Sigma_j \cdot \Sigma_j^{-1} S_j \Sigma_j \cdot \Sigma_j^{-1} U_j^{-1} = U_j S_j U_{j^{-1}};$$

donc la substitution T_j ne change pas quand on change dans ses coefficients j en j^2 ; donc elle a ses coefficients entiers, ou du moins on peut les rendre entiers en les multipliant par un facteur convenable.

THÉORÈME III. — Soit

$$\Sigma \left(z, \frac{mz + n}{pz + q} \right)$$

une substitution à coefficients entiers et à déterminant positif Δ , dont la période est paire et égale à $2n$; et si l'on considère la substitution homogène correspondante à deux variables

$$\Sigma' \begin{pmatrix} x, mx + ny \\ y, px + qy \end{pmatrix},$$

l'application de la substitution Σ' , répétée $2n$ fois, au système x, y donne la substitution

$$\Sigma'^{2n} \begin{pmatrix} x, -\Delta^n x \\ y, -\Delta^n y \end{pmatrix},$$

où le multiplicateur de x et de y est négatif.

Faisons d'abord une remarque essentielle.

Étant donnée une substitution Σ de période m , il est clair que la substitution homogène Σ' correspondante répétée m fois reproduira x et y affectés d'un certain multiplicateur K égal en valeur absolue à $\Delta^{\frac{m}{2}}$, puissance de Δ dont l'exposant est entier si m est pair, et fractionnaire si m est impair. La substitution Σ ne détermine pas complètement la substitution Σ' ; car on peut, sans changer Σ , multiplier tous ses termes par un même nombre positif ou négatif, ce qui altère Σ' . Voici en quoi consiste notre observation : le *signe* du multiplicateur K est une *propriété de la substitution fractionnaire* Σ , si m est pair, et n'en est pas une, si m est impair. En effet, dans le premier cas, le multiplicateur K contient les coefficients de Σ à une puissance paire, et, par suite, conserve le même signe quand on multiplie tous ces coefficients par un même nombre de signe quelconque; dans le second cas, il les contient à une puissance impaire et change de signe lorsque ce nombre est négatif. Notre théorème a précisément pour objet de déterminer le signe de K lorsque ce signe est invariable. On étudie la périodicité des substitutions par le procédé suivant, qui est classique. Cherchons une forme linéaire en x et y , $\lambda x + \mu y$ telle que la substitution Σ' la reproduise multipliée par un facteur

$$\omega(\lambda x + \mu y) = (\lambda m + \mu p)x + (\lambda n + \mu q)y,$$

d'où

$$\begin{aligned} (m - \omega)\lambda + \mu p &= 0, \\ n\lambda + \mu(q - \omega) &= 0, \\ \omega^2 - (m + q)\omega + \Delta &= 0. \end{aligned}$$

Cette équation a en général deux racines distinctes, $\omega, \omega' = \frac{\Delta}{\omega}$, qui fournissent deux formes linéaires $\lambda x + \mu y = u, \lambda' x + \mu' y = u'$. On peut prendre ces formes pour nouvelles variables et remplacer la substitution Σ' par la substitution

$$\begin{pmatrix} u, u\omega \\ v, v\omega' \end{pmatrix}.$$

Pour que la substitution fractionnaire Σ qui correspond à Σ' ait pour période $2n$, il faut que la puissance $2n$ de $\frac{\omega}{\omega'}$ soit égale à 1 et que ce soit la plus petite puissance de cette quantité qui soit égale à 1

$$\left(\frac{\omega}{\omega'}\right)^{2n} = \left(\frac{\omega^2}{\Delta}\right)^{2n} = 1, \quad \omega^{4n} = \Delta^{2n} :$$

donc, α désignant une racine *primitive* de l'équation binôme

$$(20) \quad \begin{aligned} x^{4n} &= 1, \\ \omega &= \pm\sqrt{\Delta}\alpha, \quad \omega' = \pm\sqrt{\Delta}\alpha^{-1}, \end{aligned}$$

la $2n^{\text{ième}}$ puissance de Σ' multiplierà u et v et, par suite, x et y par ω^{2n} et par ω'^{2n} . Mais les racines primitives de l'équation (20) et, en particulier, α et α^{-1} sont racines de l'équation

$$x^{2n} + 1 = 0;$$

donc

$$\omega^{2n} = \omega'^{2n} = -\Delta^{2n},$$

ce qui démontre le théorème.

Il ne paraît pas exister de théorème *général* analogue quand on prend pour Σ_j une substitution irrationnelle.

THÉORÈME IV. — *Les groupes fuchsien formés d'après le procédé du § I, en prenant pour Σ_j une substitution à coefficients entiers à déterminant positif, peuvent être transformés en groupes à coefficients entiers quand p est de la forme $4n + 3$, et ne peuvent pas l'être quand p est de la forme $4n + 1$.*

Soit

$$\Sigma \left(z, \frac{mz + n}{pz + q} \right),$$

de période $\frac{p-1}{2}$ et de déterminant Δ ; il faut chercher si l'on peut déterminer une substitution

$$U_j \left(z, \frac{r_j z + s_j}{t_j z + u_j} \right),$$

ne contenant que les irrationalités $j^h + j^{-h}$, et telle que

$$U_{j^p} = U_j \Sigma.$$

On a ainsi

$$(21) \quad \begin{cases} r_{j^p} = K_j(mr_j + ps_j), \\ s_{j^p} = K_j(nr_j + qs_j), \\ t_{j^p} = K_j(mt_j + pu_j), \\ u_{j^p} = K_j(nt_j + qu_j); \end{cases}$$

chacune des équations (21) équivaut à $\frac{p-1}{2}$ équations rationnelles; on a donc en tout $2p - 2$ équations, autant que les coefficients de la substitution U_j contiennent d'entiers inconnus. En changeant dans les équations (21) j en j^p , $\frac{p-3}{2}$ fois, puis en éliminant $r_{j^{pk}}, s_{j^{pk}}, t_{j^{pk}}, u_{j^{pk}}$,

$$\left(k = 1, 2, \dots, \frac{p-3}{2} \right)$$

entre ces équations, nous trouverons pour $p = 4n + 3$, et en prenant K rationnel,

$$\begin{aligned} r_j &= \pm K^{2n+1} \Delta^{\frac{2n+1}{2}} r_j, \\ s_j &= \pm K^{2n+1} \Delta^{\frac{2n+1}{2}} s_j, \\ t_j &= \pm K^{2n+1} \Delta^{\frac{2n+1}{2}} t_j, \\ u_j &= \pm K^{2n+1} \Delta^{\frac{2n+1}{2}} u_j. \end{aligned}$$

Ces équations ne contiennent pas d'autres irrationnelles que $j^h + j^{-h}$, car on voit facilement que Δ doit être carré parfait: donc on pourra toujours trouver une valeur de K rationnelle et telle que

$$(22) \quad \pm K^{2n+1} \Delta^{\frac{2n+1}{2}} = 1,$$

et alors ces quatre équations deviennent identiques. Les $2p - 2$ équations rationnelles contenues dans les équations complexes (21) se réduisent seulement à $2p - 6$ distinctes. On voit donc qu'il existe une infinité des substitutions U_j cherchées; ces substitutions contiendront quatre entiers

Errata. — A la page précédente, 4^e ligne en remontant, au lieu de *ne peuvent pas l'être*, lire : *ne peuvent pas toujours l'être*.

arbitraires, ceux-ci une fois choisis, les autres seront déterminés par les équations (21).

Soit $p = 4n + 1$: les parenthèses qui figurent dans les seconds membres des équations (21) ne sont autres que les résultats obtenus en appliquant la substitution homogène

$$\begin{pmatrix} x, mx + py \\ y, nx + qy \end{pmatrix},$$

au système $x = r_j, y = s_j$ et au système $x = t_j, y = u_j$. Donc d'après le théorème II, nous aurons

$$\begin{aligned} r_j &= -\Delta^n r_j \Pi K_j^k, \\ s_j &= -\Delta^n s_j \Pi K_j^k, \\ t_j &= -\Delta^n t_j \Pi K_j^k, \\ u_j &= -\Delta^n u_j \Pi K_j^k; \end{aligned}$$

en prenant K_j rationnel, on serait conduit à poser

$$(23) \quad \begin{aligned} K^{-2n} \Delta^n &= 1, \\ K &= \frac{i}{\sqrt{\Delta}}; \end{aligned}$$

cette valeur de K contenant une nouvelle irrationnalité ne convient pas. En prenant K_j irrationnel, il faut que Δ^{-n} puisse être représenté par la norme d'un nombre abélien K_j .

Corollaires. — 1° Le groupe G_7 est le transformé d'un groupe à coefficients entiers.

2° Les groupes formés avec une racine 5^{ième} de l'unité et une substitution transformante rationnelle Σ ne sont réductibles à des coefficients entiers que si le déterminant de Σ est de la forme $x^2 - 3xy + y^2$.

Remarque I. — Si l'on prend dans le cas de $p = 4n + 3$ pour K un quelconque des nombres irrationnels satisfaisant à l'équation (22) et dans le cas de $p = 4n + 3$ un nombre irrationnel satisfaisant à (23), on pourra en déduire des substitutions U_j telles que, à la vérité, le groupe transformé du primitif par U_j^{-1} contienne encore l'irrationnalité de K , mais ne contienne plus les irrationnalités de l'équation binôme de degré p (1).

Remarque II. — Une marche analogue permet de reconnaître si ceux de nos groupes qui ne se ramènent pas à des groupes à coefficients entiers

(1) Ceci montre le rapport entre les groupes dont il est question ici et ceux découverts par M. Bianchi : *Geometrische Darstellung der Gruppen linearer Substitutionen mit ganzen complexen Coefficienten* (*Mathematische Annalen*, 1891), que j'ai pu utiliser en achevant ce Mémoire. M. Bianchi prend pour point de départ la théorie des groupes kleinéens.

sont des transformés les uns des autres ou ont des sous-groupes qui soient les transformés les uns des autres.

Je vais, par exemple, comparer les groupes G_3 et G'_3 . Il faut voir si une substitution S_j du premier est une transformée d'une substitution T_j du second par une substitution U_j . Cette substitution peut être ramenée à ne contenir que les irrationalités des deux groupes, c'est-à-dire $j + j'$ et $j^2 + j'^2$. Soient

$$\Sigma = \left(z, -\frac{1}{z} \right), \quad Z = \left(z, \frac{z+4}{-z-1} \right),$$

on aurait

$$(24) \quad S_j = U_j^{-1} T_j U_j,$$

d'où

$$S_{j^2} = U_{j^2}^{-1} T_{j^2} U_{j^2};$$

or

$$S_{j^2} = \Sigma^{-1} S_j \Sigma, \quad T_{j^2} = Z^{-1} T_j Z,$$

et, en tenant compte de (24),

$$\Sigma^{-1} U_j^{-1} T_j U_j \Sigma = U_{j^2}^{-1} Z^{-1} T_j Z U_{j^2},$$

d'où l'on déduit

$$U_{j^2} = Z^{-1} U_j \Sigma.$$

On voit facilement que la transformation est impossible parce que, pour la réaliser, on serait conduit à introduire dans les coefficients de U_j l'irrationalité $\sqrt{3}$.

IV.

Je me propose d'étudier plus particulièrement le groupe G_5 . Les substitutions impaires de ce groupe ont pour invariant $(\alpha_1 - \alpha_2)\sqrt{5}$. Il n'y en a donc pas de paraboliques et elles ne peuvent présenter que la période 2. Les substitutions paires ont pour invariant $-(\alpha_1 + \alpha_2)$. Or l'équation (13) peut s'écrire

$$(\alpha_1 + \alpha_2)^2 + (\beta_1 + \beta_2)^2 = -1 + 5\alpha_1\alpha_2 + 5\beta_1\beta_2,$$

d'où

$$(\beta_1 + \beta_2)^2 \equiv -(\alpha_1 + \alpha_2)^2 - 1 \pmod{5}.$$

On pourra donner à $\alpha_1 + \alpha_2$ les valeurs 0 et 2, car le second membre prend alors les valeurs -1 et -5 qui sont restes quadratiques de 5; mais $\alpha_1 + \alpha_2$

ne pourra pas prendre la valeur 1, car alors le second membre devient égal à -2. Or -2 n'est pas reste quadratique de 5. Ainsi G_5 ne contient pas de substitutions de période 3.

La formation de substitutions de G_5 revient à la recherche de nombres entiers satisfaisant aux équations (12) et (13). Voici un Tableau contenant quelques-unes de ces substitutions et qui pourra être utile dans les calculs relatifs à G_5 :

$$\begin{aligned} & [0, 0, 1, 1], (0, 0, 1, 0), (1, 3, 0, 0), \\ & [0, 0, 1, 2], [0, 0, 2, 5], (0, 0, 3, 8), \\ & (1, -1, 2, 4), [2, 6, 2, 3], (2, 4, 1, -1), \\ & (3, -3, 6, 8), (2, -2, 4, 5), \dots \end{aligned}$$

Pour la composition des substitutions, on se servira des formules

$$\begin{aligned} & (\alpha_1, \alpha_2, \beta_1, \beta_2)(\alpha'_1, \alpha'_2, \beta'_1, \beta'_2) \\ & = [-(\alpha_1 - \alpha_2)(\alpha'_1 - \alpha'_2) + (\beta_1 - \beta_2)(\beta'_1 - \beta'_2) - \alpha_1\alpha'_1 - \beta_1\beta'_2, \\ & \quad -(\alpha_1 - \alpha_2)(\alpha'_1 - \alpha'_2) + (\beta_1 - \beta_2)(\beta'_1 - \beta'_2) - \alpha_2\alpha'_2 - \beta_2\beta'_1, \\ & \quad -(\alpha_1 - \alpha_2)(\beta'_1 - \beta'_2) - (\beta_1 - \beta_2)(\alpha'_1 - \alpha'_2) - \alpha_1\beta'_1 - \beta_2\alpha'_2, \\ & \quad -(\alpha_1 - \alpha_2)(\beta'_1 - \beta'_2) - (\beta_1 - \beta_2)(\alpha'_1 - \alpha'_2) - \alpha_2\beta'_2 + \beta_2\alpha'_1]; \end{aligned}$$

$$\begin{aligned} & (\alpha_1, \alpha_2, \beta_1, \beta_2)[\alpha'_1, \alpha'_2, \beta'_1, \beta'_2] \\ & = (-(\alpha_1 - \alpha_2)(\alpha'_1 - \alpha'_2) - (\beta_1 - \beta_2)(\beta'_1 - \beta'_2) - \alpha_1\alpha'_1 + \beta_1\beta'_2, \\ & \quad -(\alpha_1 - \alpha_2)(\alpha'_1 - \alpha'_2) - (\beta_1 - \beta_2)(\beta'_1 - \beta'_2) - \alpha_2\alpha'_2 + \beta_2\beta'_1, \\ & \quad (\alpha_1 - \alpha_2)(\beta'_1 - \beta'_2) + (\beta_1 - \beta_2)(\alpha'_1 - \alpha'_2) - \alpha'_1\beta_2 - \beta_1\alpha'_2, \\ & \quad (\alpha_1 - \alpha_2)(\beta'_1 - \beta'_2) + (\beta_1 - \beta_2)(\alpha'_1 - \alpha'_2) - \alpha_2\beta'_1 + \beta_2\alpha'_1); \end{aligned}$$

$$\begin{aligned} & [\alpha_1, \alpha_2, \beta_1, \beta_2](\alpha'_1, \alpha'_2, \beta'_1, \beta'_2) \\ & = [-(\alpha_1 - \alpha_2)(\alpha'_1 - \alpha'_2) - (\beta_1 - \beta_2)(\beta'_1 - \beta'_2) - \alpha_1\alpha'_1 + \beta_2\beta'_1, \\ & \quad -(\alpha_1 - \alpha_2)(\alpha'_1 - \alpha'_2) - (\beta_1 - \beta_2)(\beta'_1 - \beta'_2) - \alpha_2\alpha'_2 + \beta_1\beta'_2, \\ & \quad -(\alpha_1 - \alpha_2)(\beta'_1 - \beta'_2) - (\beta_1 - \beta_2)(\alpha'_1 - \alpha'_2) - \alpha_1\beta'_1 + \beta_1\alpha'_2, \\ & \quad -(\alpha_1 - \alpha_2)(\beta'_1 - \beta'_2) - (\beta_1 - \beta_2)(\alpha'_1 - \alpha'_2) - \alpha_2\beta'_2 + \beta_2\alpha'_1]; \end{aligned}$$

$$\begin{aligned} & [\alpha_1, \alpha_2, \beta_1, \beta_2][\alpha'_1, \alpha'_2, \beta'_1, \beta'_2] \\ & = [-(\alpha_1 - \alpha_2)(\alpha'_1 - \alpha'_2) - (\beta_1 - \beta_2)(\beta'_1 - \beta'_2) - \alpha_1\alpha'_1 + \beta_1\beta'_2, \\ & \quad -(\alpha_1 - \alpha_2)(\alpha'_1 - \alpha'_2) - (\beta_1 - \beta_2)(\beta'_1 - \beta'_2) + \beta_2\beta'_1 - \alpha_2\alpha'_2, \\ & \quad (\beta_1 - \beta_2)(\alpha'_1 - \alpha'_2) - (\alpha_1 - \alpha_2)(\beta'_1 - \beta'_2) - \alpha_2\beta'_2 - \beta_2\alpha'_1, \\ & \quad (\beta_1 - \beta_2)(\alpha'_1 - \alpha'_2) - (\alpha_1 - \alpha_2)(\beta'_1 - \beta'_2) - \beta_1\alpha'_2 - \alpha_2\beta'_1] \end{aligned}$$

Considérons les trois substitutions de période 2

$$\begin{aligned} A[0, 0, 1, 1], & \left(z, -\frac{1}{z}\right), \\ B(0, 0, 1, 0), & \left[z, \frac{j+j^4}{(j^2+j^3)z}\right]; \\ C(-2, -2, -1, 1), & \left[z, \frac{2z+1+2j^2+2j^3}{(1+2j+2j^4)z-2}\right]. \end{aligned}$$

On trouve que

$$CBA = [2, 0, 2, 3], \quad \left[z, \frac{2(j+j^4)z-2+j^2+j^3}{(2-j-j^4)z+2j^2+2j^3}\right]$$

est une substitution parabolique. Les trois substitutions A, B, C définissent un polygone fuchsien. Le polygone sera un triangle ayant ses trois angles nuls et dont les demi-côtés sont conjugués par les substitutions A, B, C. Les sommets du triangle sont les points

$$-(j^2+j^3), \quad j+j^4, \quad -(j+j^4),$$

ou en posant

$$j = e^{\frac{2i\pi}{5}},$$

$$\frac{\sqrt{5}+1}{2}, \quad \frac{\sqrt{5}-1}{2}, \quad -\frac{\sqrt{5}+1}{2},$$

les milieux des côtés sont les points

$$i, \quad i(j+j^4), \quad \frac{-(2+i)(1+2j+2j^3)}{5}$$

ou

$$i, \quad i\frac{\sqrt{5}-1}{2}, \quad \frac{(2+i)\sqrt{5}}{5}.$$

Les procédés ordinaires pour reconnaître si un polygone fuchsien peut être décomposé en polygones plus petits permettent de reconnaître que ce polygone ne peut être décomposé en d'autres ne contenant que des cycles de période 2 ou ∞ . C'est donc un polygone générateur de G_5 , et l'on pourra prendre A, B, C comme système de substitutions fondamentales.

D'après la remarque I (§ III), on peut donner au groupe G_5 une forme fort utile. Nous cherchons une substitution U_j telle que

$$U_j^2 = U_j \Sigma, \quad \Sigma = \left(z, -\frac{1}{z}\right).$$

En posant

$$U_j = \left\{ z, \frac{[\rho_1(j+j^*) + \rho_2(j^2+j^3)]z + \sigma_1(j+j^*) + \sigma_2(j^2+j^3)}{[\tau_1(j+j^*) + \tau_2(j^2+j^3)]z + \nu_1(j+j^*) + \nu_2(j^2+j^3)} \right\},$$

on trouve les relations

$$\begin{aligned} \sigma_1 &= k\rho_2, & \sigma_2 &= k\rho_1, & \rho_1 &= -k\sigma_2, & \rho_2 &= -k\sigma_1, \\ \nu_1 &= k\tau_2, & \nu_2 &= k\tau_1, & \tau_1 &= -k\nu_2, & \tau_2 &= -k\nu_1. \end{aligned}$$

On en déduit

$$k^2 = -1, \quad k = \pm i,$$

et, en prenant $k = +i$,

$$U_j = \left\{ z, \frac{[\rho_1(j+j^*) + \rho_2(j^2+j^3)]z + i[\rho_2(j+j^*) + \rho_1(j^2+j^3)]}{[\tau_1(j+j^*) + \tau_2(j^2+j^3)]z + i[\tau_2(j+j^*) + \tau_1(j^2+j^3)]} \right\},$$

le déterminant de U_j est

$$i(\rho_1\tau_2 - \rho_2\tau_1)(j^3 + j^3 - j - j^*) = -i\sqrt{5}(\rho_1\tau_2 - \rho_2\tau_1).$$

Nous aurons la plus simple des substitutions U_j en prenant

$$\rho_1 = 1, \quad \rho_2 = 0, \quad \tau_1 = 0, \quad \tau_2 = 1,$$

soit

$$\left[z, \frac{(j+j^*)z + i(j^2+j^3)}{(j^2+j^3)z + i(j+j^*)} \right].$$

On trouve, pour la transformée de la substitution

$$\begin{aligned} &(\alpha_1, \alpha_2, \beta_1, \beta_2), \\ &\left\{ z, \frac{-z[\beta_1 + \beta_2 + i(4\alpha_1 - \alpha_2)] + \beta_2 - 4\beta_1 - i(\alpha_1 + \alpha_2)}{z[-\beta_1 + 4\beta_2 + i(\alpha_1 + \alpha_2)] + \beta_1 + \beta_2 + i(4\alpha_2 - \alpha_1)} \right\}, \end{aligned}$$

dont le déterminant est -5 ; et, pour la transformée de

$$\begin{aligned} &(\alpha_1, \alpha_2, \beta_1, \beta_2), \\ &\left\{ z, \frac{[\beta_1 - \beta_2 + i(2\alpha_1 - \alpha_2)]z + 2\beta_1 - \beta_2 - i(\alpha_2 - \alpha_1)}{[2\beta_2 - \beta_1 + i(\alpha_2 - \alpha_1)]z + \beta_2 - \beta_1 + i(2\alpha_2 - \alpha_1)} \right\}, \end{aligned}$$

dont le déterminant est -1 . Le nouveau cercle fondamental est le cercle dans lequel la substitution U_j^{-1} transforme l'axe réel. En effet, en désignant par C_0 l'axe réel, nous avons

$$C_0 S_j = C_0,$$

d'où évidemment

$$C_0 U_j^{-1} \cdot U_j S_j U_j^{-1} = C_0 U_j^{-1}.$$

Pour avoir l'équation du nouveau cercle fondamental, on posera

$$z' = \frac{(j + j^4)z + i(j^2 + j^3)}{(j^2 + j^3)z + i(j + j^4)}, \quad z_0' = \frac{(j + j^4)z - i(j^2 + j^3)}{(j^2 + j^3)z - i(j + j^4)},$$

et l'on éliminera z entre ces deux équations, ce qui donne

$$2z'z_0 + 3(z' + z_0') + 2 = 0,$$

ou, en revenant aux coordonnées cartésiennes,

$$x'^2 + y'^2 + 3x' + 1 = 0.$$

Remarquons que le groupe sous sa nouvelle forme est permutable avec la substitution (z, z_0) . L'équation fuchsienne correspondante peut donc être ramenée à avoir des coefficients réels.

Le groupe G_5 et les groupes analogues partagent avec le groupe arithmétique une propriété très remarquable et très importante : ils sont commensurables avec une infinité de leurs transformés ⁽¹⁾. En effet, formons une substitution

$$(\alpha_1, \alpha_2, \beta_1, \beta_2) \quad \text{ou} \quad [\alpha_1, \alpha_2, \beta_1, \beta_2],$$

où les $\alpha_1, \alpha_2, \beta_1, \beta_2$ seront des entiers, mais que nous n'assujettirons pas aux équations (12), respectivement (13). Une pareille substitution transformera G_5 en un groupe du même cercle fondamental, dont les substitutions auront, en général, pour déterminant le carré du déterminant de la substitution transformante et, à cela près, présenteront le même aspect que les substitutions de G_5 . Moyennant certaines congruences, on pourra rendre les coefficients de ces substitutions divisibles par le déterminant de la transformante, et l'on obtiendra un sous-groupe commun à G_5 et à son transformé d'indice fini dans les deux groupes.

V.

Une substitution du groupe G_7 est déterminée par les valeurs des quatre entiers $\alpha_1, \beta_1, \gamma_1, \delta_1$. Nous la représenterons par

$$S : (\alpha_1, \beta_1, \gamma_1, \delta_1).$$

⁽¹⁾ Voir, sur la notion des groupes commensurables entre eux, *Les fonctions fuchsiennes et l'Arithmétique*.

Soit une autre substitution S' de ce groupe

$$S' : (\alpha', \beta', \gamma', \delta').$$

La substitution SS' est donnée par la formule

$$\begin{aligned} SS' : & [\alpha_1(-3\alpha'_1 - 2\gamma'_1 + 2\delta'_1) \\ & + \beta_1(2\alpha'_1 - 2\beta'_1 - \gamma'_1 - 2\delta'_1) + \gamma_1(-2\beta'_1 - 2\gamma'_1) + \delta_1(2\alpha'_1 + 2\gamma'_1 - 2\delta'_1), \\ & \alpha_1(-3\beta'_1 - 2\gamma'_1) \\ & + \beta_1(2\alpha'_1 + 2\gamma'_1 - 3\delta'_1) + \gamma_1(2\alpha'_1 - 2\beta'_1 - 2\delta'_1) + \delta_1(2\beta'_1 + 2\gamma'_1), \\ & \alpha_1(2\beta'_1 + 2\gamma'_1) \\ & + \beta_1(-2\alpha'_1 - 2\gamma'_1 + 2\delta'_1) + \gamma'_1(-3\alpha'_1 + 2\beta'_1 + 2\delta'_1) + \delta_1(-2\beta'_1 - 3\gamma'_1), \\ & \alpha_1(-2\alpha'_1 + 2\beta'_1 + 2\delta'_1) \\ & + \beta_1(-2\beta'_1 - 2\gamma'_1) + \gamma_1(-2\alpha'_1 - \beta'_1 - 2\gamma'_1 + 2\delta'_1) + \delta_1(2\alpha'_1 - 2\beta'_1 - 3\delta'_1)]. \end{aligned}$$

L'invariant de ces substitutions étant entier et le déterminant étant égal à 1, ces substitutions ne peuvent présenter que les périodes 2, 3, ∞ .

Substitutions de période 2. — En posant $\alpha_1 + \delta_1 = 0$ dans la relation (16), on obtient l'équation

$$9\alpha_1^2 + 4\alpha_1(\gamma_1 - \beta_1) + 2(\beta_1^2 + \gamma_1^2) + 3\beta_1\gamma_1 + 1 = 0,$$

et, en tirant la valeur de α_1 ,

$$\alpha_1 = \frac{-2(\gamma_1 - \beta_1) \pm \sqrt{-9 - 7(\beta_1 + 2\gamma_1)(\gamma_1 + 2\beta_1)}}{9};$$

or, quelles que soient les valeurs que l'on mette à la place de β_1 et de γ_1 , α_1 n'est jamais rationnel, parce que -9 n'est pas reste quadratique de 7. Donc le groupe ne contient pas de substitutions de période 2.

Substitutions de période 3. — La relation (16) donne, pour $\delta_1 = 1 - \alpha_1$,

$$\alpha_1 = \frac{9 + 4\beta_1 - 4\gamma_1 \pm \sqrt{-27 - 28(\beta_1 + 2\gamma_1)(\gamma_1 + 2\beta_1)}}{18}.$$

Lorsque la quantité placée sous le radical sera carré parfait, ce sera le carré d'un multiple de 7 ± 1 . En s'appuyant sur cette remarque pour chercher des substitutions de période 3, on trouve, par exemple,

$$(0, -1, 1, 1), \quad (3, 5, -3, -2).$$

Substitutions paraboliques. — On a

$$\alpha_1 = \frac{9 + 2\beta_1 - 2\gamma_1 \pm \sqrt{-7(\beta_1 + 2\gamma_1)(\gamma_1 + 2\beta_1)}}{9},$$

on posera

$$\beta_1 + 2\gamma_1 = u, \quad \gamma_1 + 2\beta_1 = v, \quad u \equiv 2v \pmod{3},$$

et on aura

$$\alpha_1 = 1 + \frac{2v - 2u \pm \sqrt{7uv}}{9}.$$

On trouve ainsi facilement des substitutions paraboliques. Exemples :

$$(3, 6, -3, -1), \quad (-1, -6, -3, 3), \\ (2, 3, -5, 0), \quad (-1, -10, 6, 3).$$

Polygone générateur du groupe. — Le calcul montre que le produit de substitutions

$$(0, -1, 1, 1), \quad (0, -3, 3, 1), \quad (0, 3, -5, -2),$$

dont les deux premières sont de période 3 et la troisième est parabolique, est une substitution parabolique $(3, 3, -6, -1)$. Ces trois substitutions conjuguent les côtés d'un polygone fuchsien de genre 0 et ayant six côtés, deux conjugués par $(0, -1, 1, 1)$, deux par $(0, -3, 3, 1)$, deux par $(0, 3, -5, -2$; trois des sommets forment chacun un cycle. Ce polygone est le polygone générateur du groupe, car il est impossible de le décomposer en polygones générateurs plus petits, en tenant compte de ce que le groupe ne contient pas de substitutions de période 2, et que les deux substitutions paraboliques $(0, 3, -5, -2)$, $(3, 3, -6, -1)$ ne sont les carrés d'aucune substitution. Il a pour aire non euclidienne $\frac{8\pi}{3}$. Les trois substitutions ci-dessus forment donc un système de substitutions génératrices.

Forme rationnelle de G_7 . — En cherchant une substitution U_j satisfaisant à la relation (19), pour $\rho = 2$, on trouve

$$U_j = \left\{ \begin{array}{l} \left\{ \begin{array}{l} [\lambda_1(j+j^4) + (\mu_1 - \lambda_1)(j^2 + j^5) - \mu_1(j^3 + j^4)]z \\ + \mu_1(j + j^6) - \lambda_1(j^2 + j^5) - (\mu_1 - \lambda_1)(j^3 + j^3) \end{array} \right\} \\ \left\{ \begin{array}{l} [\nu_1(j + j^6) + (\rho_1 - \nu_1)(j^2 + j^5) - \rho_1(j^3 + j^3)]z \\ + \rho_1(j + j^6) - \nu_1(j^2 + j^5) - (\rho_1 - \nu_1)(j^3 + j^3) \end{array} \right\} \end{array} \right\};$$

le déterminant de U_j est

$$7(\lambda_1 \rho_1 - \mu_1 \nu_1).$$

Nous choisirons la plus simple possible des substitutions U_j en posant

$$\lambda_1 = \rho_1 = 1, \quad \mu_1 = \nu_1 = 0.$$

Après avoir transformé par U_j^{-1} la substitution générale du groupe G_7 (§ II), on trouve, après avoir divisé par 7 tous les coefficients,

$$U_j S_j U_j^{-1} = \left[z, \frac{-(2\beta_1 + \gamma_1 + \delta_1)z + 2\alpha_1 - 2\beta_1 + \gamma_1 - 2\delta_1}{(\alpha_1 + \beta_1 + \gamma_1 - \delta_1)z - \alpha_1 + 2\beta_1 + \gamma_1} \right],$$

dont le déterminant est 1. Notre groupe $U_j G_7 U_j^{-1}$ est donc un sous-groupe du groupe arithmétique. Soit

$$\left(z, \frac{mz + n}{pz + q} \right), \quad mq - np = 1$$

une substitution de ce dernier groupe: nous allons chercher à quelles conditions de congruence doivent satisfaire m, n, p, q pour que, en identifiant les deux substitutions, on trouve pour $\alpha_1, \beta_1, \gamma_1, \delta_1$ des valeurs entières.

On a

$$\begin{aligned} \alpha_1 &= \frac{-2m - n + 4p - 5q}{7}, \\ \beta_1 &= \frac{m - 3n + 5p - q}{7}, \\ \gamma_1 &= \frac{-4m + 5n - 6p + 4q}{7}, \\ \delta_1 &= \frac{-5m + n - 4p - 2q}{7}. \end{aligned}$$

Les numérateurs ne sont autres (mod 7) que la forme linéaire

$$m - 3n + 5p - q$$

multipliée (mod 7) par $-2, -4, -5$. Il faut donc et il suffit que cette forme linéaire soit congrue à 0 (mod 7). Ainsi notre groupe $U_j G_7 U_j^{-1}$ est le groupe

$$(A) \quad \left(z, \frac{mz + n}{pz + q} \right), \quad \begin{aligned} m - 3n + 5p - q &\equiv 0 \pmod{7}, \\ mp - nq &= 1. \end{aligned}$$

Cherchons combien on obtiendra de groupes différents en transformant

$U_j G_7 U_j^{-1}$ par les substitutions du groupe arithmétique. Il y en aura autant que des substitutions $\frac{\mu z + \nu}{\rho z + \pi}$, $\mu\pi - \nu\rho = 1$, donnant, par une transformation de $(z, \frac{mz + n}{pz + q})$, des congruences résultant de (A) et distinctes. Or A devient

$$\begin{aligned} m(\mu\pi - 3\nu\pi - 5\mu\nu + \nu\rho) + n(-3\rho^2 + 2\pi\rho - 5\pi^2) \\ + p(3\nu^2 - 2\mu\nu + 5\mu^2) \\ + q(-\nu\rho + 3\nu\pi + 5\mu\nu - \nu\pi) \equiv 0 \pmod{7}. \end{aligned}$$

Les multiplicateurs de m, n, p, q ne sont autres que les coefficients d'une transformée de la substitution

$$\frac{z + 3}{-5z - 1} \pmod{7}.$$

Il y aura donc autant de groupes que de transformées distinctes de cette substitution (mod 7). Or elle est de période 2 et a pour déterminant 7. Elle est donc caractérisée complètement par l'équation de ses points doubles

$$(5z + 1)^2 \equiv 0 \pmod{7},$$

et donnera lieu à autant de transformées distinctes (mod 7) qu'il y a de formes linéaires distinctes (mod 7). Or on sait qu'il y en a 8 qui s'annulent pour 0, ± 1 , ± 2 , ± 3 , ∞ , $l'\infty$ étant l'imaginaire de Galois (1).

(1) Comparer KLEIN, *Gleichungen siebenten und achten Grades* (*Mathematische Annalen*, t. XV, p. 269 et suivantes). — KLEIN, *Zur Theorie der elliptischen Modulfunctionen* (*Mathematische Annalen*, t. XVII). Le groupe G_7 est un groupe à congruences de septième rang.

