Sur une équation de transformation.

Par

M. K. Abramowicz à Poznań.

Dans ma note: „Transformation des fonctions automorphes“, insérée dans les Comptes Rendus, t. 187, j'ai determinée le degré de l'équation de transformation de la fonction automorphe appartenant [1]) au groupe (p, q, r) de Fricke, défini dans le corps algébrique $R_m(j)$ de dégre m. Dans l'article actuel nous nous proposons d'envisager les cas où le degré de cet équation pourra s'abaisser.

Nous faisons l'hypothèse que 1) le corps algébrique $R_m(j)$ de degré m, défini par l'équation $F(j) = 0$, a la base minimale $(1, j, j^2, \ldots j^{m-1})$, 2) que le polynome $F(j)$ est irréductible suivant le module n, 3) que le module n (degré de transformation) est un nombre naturel premier dans le corps $R_m(j)$, 4) que le polygone fondamental du groupe (p, q, r) a un nombre fini de sommets. En conservant les notations de la note citée, nous désignons par (p, q, r) le groupe discontinu de substitutions linéaires de la forme

$$\frac{(a + b\sqrt{pq})z + (c\sqrt{r} + d\sqrt{p})\sqrt{q}}{(-c\sqrt{r} + d\sqrt{p})\sqrt{q}\,z + a - b\sqrt{pq}}, \tag{1}$$

où p, q, r sont trois nombres donnés du corps $R_m(j)$ et les nombres a, b, c, d du corps $R_m(j)$ sont liés par la relation

$$a^2 + c^2qr - p(b^2q + d^2r) = 1.$$

Nous désignons encore par G_e le groupe fini de toutes les substitutions (mod n)

---

[1]) Fricke, Vorlesungen über die Theorie d. automorphen Funktionen, Bd. I, p. 588.

$$\begin{pmatrix} a+b\sqrt{pq}, & (c\sqrt{r}+d\sqrt{p})\sqrt{q} \\ (-c\sqrt{r}+d\sqrt{p})\sqrt{q}, & a-b\sqrt{pq} \end{pmatrix}$$

dont les coefficients a, b, c, d satisfaisant à la congruence

$$(2) \qquad a^2+c^2qr-p(b^2q+d^2r) \equiv 1 \pmod{n}$$

parcourrent le système complet de restes du corps $R_m(j)$ incongrus par rapport au module n; nous désignons par G_{e_1} le groupe fini auquel se reduit le groupe (p, q, r) par rapport au module n. Si les groupes G_e et G_{e_1} ne sont pas identiques le groupe G_{e_1} sera un sous-groupe du groupe G_e et l'on aura la relation $e = ke_1$, où le nombre k désigne l'indice du groupe G_{e_1} par rapport au groupe G_e. Nous étudierons les groupes G_e et G_{e_1} et nous allons voir que le cas $k > 1$ pourra conduire à l'abaissement [1]) du degré de l'équation de transformation. Envisageons en premier lieu le groupe G_{e_1} auquel se reduit le groupe (p, q, r) suivant le module n.

§ 1. En désignant par $(*a, *b, *c, *d)$ les substitutions du groupe G_{e_1} nous appellons équivalentes à $(*a, *b, *c, *d)$ les substitutions (a, b, c, d) du groupe (p, q, r) qui se reduisent (mod n) à la substitution $(*a, *b, *c, *d)$; chaque substitutions $(*a, *b, *c, *d)$ du groupe G_{e_1} *aura* ses équivalentes dans le groupe (p, q, r), parce que le groupe $(p, q\ r)$ se reduit (mod n) au groupe G_{e_1}. Mais cela n'aura pas lieu par rapport au groupe G_e; dans le cas, où l'indice k est plus grande que 1, le groupe G_e contiendra des substitutions qui *n'auront pas* d'équivalentes dans le groupe (p, q, r). Observons encore que l'ensemble de toutes les substitutions du groupe (p, q, r) équivalentes à une substitutions $(*a, *b, *c, *d)$ du groupe G_{e_1} (différente de l'unité) ne formera pas, en général, un groupe.

Nous envisageons en premier lieu l'ensemble infini de substitutions $(a, b\ c, d)$ du groupe (p, q, r) *équivalentes* à 1; appellons cet ensemble Γ. L'ensemble Γ formera évidemment un groupe. En effet, si l'on a deux substitutions (a, b, c, d) et (a', b', c', d') équivalentes à 1, on a

$$a \equiv 1, \quad b \equiv c \equiv d \equiv 0 \pmod{n},$$
$$a' \equiv 1, \quad b' \equiv c' \equiv d' \equiv 0 \pmod{n};$$

le produit (a'', b'', c'', d'') de ces substitutions est donné par les formules:

[1]) Dans la note citée nous avons envisagés le cas $k = 1$.

$$a'' = aa' + bb'pr - cc'qr + dd'pq,$$
$$b'' = ab' + ba' + cd'q - dc'q,$$
$$c'' = ac' + bd'p + ca' - db'p,$$
$$d'' = ad' + bc'r - cb'r + da,$$

d'où l'on déduit immédiatement les congruences

$$a'' \equiv 1, \quad b'' \equiv c'' \equiv d'' \equiv 0 \pmod{n}.$$

Nous demontrons le théorème suivant:

Théorème I. *L'indice du groupe Γ par rapport au groupe (p, q, r) est égale á e_1, où e_1 est le degré du groupe fini auquel se reduit* (mod n) *le groupe (p, q, r).*

Soient

$$1, V_2, V_3, \ldots \tag{4}$$

les substitutions du groupe Γ, c'est-à-dire les substitutions équivalentes à la substitution $(1, 0, 0, 0)$. Prenons une substitution $(^*a, ^*b, ^*c, ^*d)$ du groupe G_{e_1}; il existera toujours dans le groupe (p, q, r) une substitution (a, b, c, d) équivalente à la substitution $(^*a, ^*b, ^*c, ^*d)$; nous formons les produits

$$(a, b, c, d), \quad (a,b,c,d)V_2, \quad (a, b, c, d)V_3, \ldots \tag{5}$$

Nous montrons que l'ensemble obtenu épuise toutes les substitutions du groupe $(p. q, r)$ *équivalentes* à la substitution $(^*a, ^*b, ^*c, ^*d)$; il suffira dans ce but de montrer qu'en général, chaque substitution (a, b, c, d) du groupe (p, q, r) équivalente à $(^*a, ^*b, ^*c, ^*d)$ *peut être* representée (d'une seule manière) comme le produit de la substitution (a, b, c, d) et d'une certaine substitution V_i équivalente à l'unité; cette substitution (a, b, c, d) devra alors se trouver dans la suite (5), parce que la suite (4) épuise toutes les substitutions $\equiv 1 \pmod{n}$ du groupe (p, q, r).

En effet, chaque substitution du groupe (p, q, r) équivalente à 1 a la forme

$$(n\alpha + 1, n\beta, n\gamma, n\delta),$$

où $\alpha, \beta, \gamma, \delta$ sont des nombres entiers du corps $R_m(j)$; chaque substitution du groupe (p, q, r) équivalente à $(^*a, ^*b, ^*c, ^*d)$ a la forme

$$(^*a + nA, ^*b + nB, ^*c + nC, ^*d + nD),$$

où A, B, C, D sont des nombres entiers du corps $R_m(j)$; il reste pour notre but à montrer qu'étant donnés quatre nombres A, B, C, D

du corps algébrique $R_m(j)$ on peut déterminer les nombres entiers $\alpha, \beta, \gamma, \delta$ du corps $R_m(j)$ satisfaisant à l'égalité

$$(a, b, c, d)(n\alpha + 1, n\beta, n\gamma, n\delta) = (^*a + nA, ^*b + nB, ^*c + nC, ^*d + nD).$$

D'après les formules (3) donnant les coefficients du produit de deux substitutions (a, b, c, d) on obtiendra les équations:

$$\begin{aligned} A' &= a\alpha + b\beta pr - cqr\gamma + dpq\delta, \\ B' &= b\alpha + a\beta - dq\gamma + cq\delta, \\ C' &= c\alpha - dp\beta + a\gamma + bp\delta, \\ D' &= d\alpha - cr\beta + br\gamma + a\delta, \end{aligned}$$

où A', B', C', D' sont certains nombres entiers du corps $R_m(j)$ (il faut se rappeller que le coefficient a ne diffère de $^*a$ que par un multiple de n; le même se rapporte aux nombres b, c, d).

On demontre facilement que le determinant

$$\begin{vmatrix} a, & bpr, & -cqr, & dpq \\ b, & -a, & -dq, & aq \\ c, & -pd, & a, & bp \\ d, & -cr, & br, & a \end{vmatrix}$$

de ce système de quatre équations (par rapport à $\alpha, \beta, \gamma, \delta$) est égal au carré du determinant

$$a^2 + c^2qr - p(b^2r + d^2q)$$

qui est égal à l'unité; on voit que les nombres $\alpha, \beta, \gamma, \delta$ seront entiers. Cela suffit pour montrer que chaque substitution (a, b, c, d) du groupe (p, q, r) équivalente à $(^*a, ^*b, ^*c, ^*d)$ peut être representée comme le produit de la substitution (a, b, c, d) et d'une certaine substitution équivalente à 1.

Prenons maintenant une substitution (a_1, b_1, c_1, d_1) du groupe (p, q, r) équivalente à une autre substitution $(^*a_1, ^*b_1, ^*c_1, ^*d_1)$ du groupe G_{e_1}; nous obtenons la suite

$$(6) \qquad (a_1, b_1, c_1, d_1), \quad (a_1, b_1, c_1, d_1)V_2, \quad (a_1, b_1, c_2, d_1)V_2, \ldots$$

qui, comme la précédente, *épuisera* toutes les substitutions du groupe (p, q, r) équivalentes à la substitution $(^*a_1, ^*b_1, ^*c_1, ^*d_1)$; on voit aisément que les suites (5) et (6) ne contiendront pas da substitutions égales; en effet, si l'on avait

$$(a, b, c, d)V_i = (a_1, b_1, c_1, d_1)V_j,$$

on aurait

$$(a_1, b_1, c_1, d_1) = (a, b, c, d)V_j V_i^{-1};$$

le produit $V_j V_i^{-1}$ étant équivalente à l'unité, on voit que la substitution (a_1, b_1, c_1, d_1) devrait alors se trouver dans la suite (5), ce qui est impossible, parce que la suite (5) est composée exclusivement de substitutions équivalentes à $(*a, *b, *c, *d)$.

En prenant successivement toutes les substitutions du groupe G_{e_1} on obtiendra d'une manière semblable e_1 suites telle que (5) ou (6) et l'on demontrera, par la méthode connue, que le groupe Γ de substitutions équivalentes (mod n) à 1 a par rapport au groupe (p, q, r) l'indice égale à e_1.

§ 2. Nous passons maintenant à l'égalité [1])

$$(7) \qquad (p, q, r) = (g_j, S_2 g_j, \ldots, S_j g_j),$$

où g_j désigne le sous-groupe du groupe (p, q, r) composé de substitutions (a, b, c, d) satisfaisant à la congruence

$$d \equiv \omega b \pmod{n},$$

où $q\omega^2 \equiv -r \pmod{n}$, L'indice j du groupe g_j par rapport au groupe (p, q, r) est égale au degré de l'équation de transformation de la fonction automorphe appartenant au groupe (p, q, r).

Nous démontrons le théorème suivant:

Théorème II: *L'indice du sous-groupe g_j par rapport au groupe (p, q, r) est égale au quotient du degré e_1 du groupe G_{e_1} par le degré du groupe fini $*g_j$ auquel se reduit le groupe g_j par rapport au module n.*

En effet, la première partie de l'égalité (7) se reduit (mod n) au groupe G_{e_1}. Le groupe g_j qui figure dans cette égalité se reduit à l'ensemble de substitutions du groupe G_{e_1} qui satisfont à la congruence

$$(8) \qquad *d \equiv \omega *b \pmod{n}.$$

Inversement, chaque substitution $(*a, *b, *c, *d)$ du groupe G_{e_1} satisfaisant à la congruence (8) *aura* dans le groupe (p, q, r) des substitutions équivalentes (a, b, c, d) satisfaisant à la congruence

$$d \equiv \omega b \pmod{n},$$

[1]) Cf. la note citée: Transformation des fonctions automorphes.

parce que le groupe G_{e_1} contient toutes les substitutions auxquelles se reguit le groupe (p, q, r)

Envisageons les substitutions $S_2, S_3, \ldots S_j$. Désignons par $(a_2, {}^*b_2, {}^*c_2, {}^*d_2)$ la substitution du groupe G_{e_1} à laquelle se reduit la substitution $S_2 = (a_2, b_2, c_2, d_2)$; cette substitution (a_2, b_2, c_2, d_2) n'entrera pas dans le groupe reduit ${}^*g_j$ parce que autrement la substitution (a_2, b_2, c_2, d_2) devrait se trouver dans le groupe g_j, ce qui n'a pas lieu; la ligne $S_2 g_j$ se reduira à l'ensemble

$$(9) \qquad ({}^*a_2, {}^*b_2, {}^*c_2, {}^*d_2) {}^*g_j.$$

L'ensemble (9) n'aura pas de substitutions communes avec le groupe ${}^*g_j$, car désignant par U et U' deux substitutions du groupe ${}^*g_j$ on aurait alors

$$({}^*a_2, {}^*b_2, {}^*c_2, {}^*d_2) U = U',$$

d'où

$$({}^*a_2, {}^*b_2, {}^*c_2, {}^*d) = U' U^{-1}$$

et la substitution $({}^*a_2, {}^*b_2, {}^*c_2, {}^*d_2)$ devrait faire partie du groupe ${}^*g_j$.

La substitution $(a_3, b_3, c_3, d_3) = S_3$ se reduira à la substitution $({}^*a_3, {}^*b_3, {}^*c_3, {}^*d_3)$ qui n'entrera ni dans le groure ${}^*g_j$ ni dans la ligne (9). Nous demontrons cela de la manière suivante: le groupe g_j contient toutes les substitutions

$$1, V_2, V_3 \ldots.$$

équivalentes (mod n) à 1 dont il était question plus haut (parce qu'elles vérifient la conquence $d \equiv \omega b$); la ligne $S_2 g_j$ *épuisera* par suite toutes les substitutions *équivalentes* à la substitution $({}^*a_2, {}^*b_2, {}^*c_2, {}^*d_2)$, parce qu'elle contiendra toutes les substitutions de la forme $(a_2, b_2, c_2, d_2) V_i$; la substitution (a_3, b_3, c_3, d_3) devra donc être équivalente à une substitution autre que $({}^*a_2, {}^*b_2, {}^*c_2, {}^*d_2)$. Mais la substitution (a_3, b_3, c_3, d_3) ne pourra aussi être équivalente à aucune substitution

$$({}^*a_2, {}^*b_2, {}^*c_2, {}^*d_2) U$$

de la ligne ${}^*S_2 {}^*g_j$, parce que la ligne $S_2 g_j$ *épuise toutes* les substitutions équivalentes à la substitution $({}^*a_2, {}^*b_2, {}^*c_2, {}^*d_2) U$; en effet, pour obtenir *toutes* les substitutions équivalentes à la substitution $({}^*a_2, {}^*b_2, {}^*c_2, {}^*d_2) U$ il suffira, d'après ce qui a été dit plu haut (p. 3), de multiplier la substitution $(a_2, b_2, c_2, d_2) U$ par les substitutions $V_2 \; V_3 \ldots$ équivalente à 1; mais les substitutions ainsi obtenues

$$(a_2, b_2, c_2, d_2)\, UV_i$$

entrent dans la ligne $S_2 g_j$, parce qua la substitution UV_i se trouve dans le groupe g_j. On voit qu'aucune substitution équivalente à $(*a_2, *b_2, *c_2, *d_2)\, U$ ne se trouvera hors de la ligne $S_2 g_j$. La substitution reduite $(*a_3, *b_3, *c_3, *d_3)$ n'entrera donc pas ni dans le groupe $*g_j$ ni dans la ligne $*S_2 *g_j$.

La ligne $S_3 g_j$ se reduira ainsi (mod n) à l'ensemble

$$(*a_3, *b_3, *c_3, *d_3) *g_j \tag{10}$$

dont *toutes les substitutions seront différentes de celles du groupe* $*g_j$ *et de la ligne* (9).

D'une manière semblable on obtiendra de nouvelles lignes

$$*S_i *g_j \qquad (i = 2, 3, \ldots, j)$$

dont aucune ne contiendra d'élements communs avec les précédentes. On aura la décomposition de Lagrange du groupe G_{e_1} en j lignes suivant le groupe reduit $*g_j$. Cela montre que le nombre j dont il était question est égal à l'indice du groupe $*g_j$ de substitutions $(*a, *b, *c, *d)$ satisfaisant à la congruence $*d \equiv \omega *b$, par rapport au groupe reduit G_{e_1}.

§ 3. Après ces remarques désignons par g l'ensemble de substitutions du groupe G_e satisfaisant à la congruence

$$*d \equiv \omega *b \pmod{n}. \tag{11}$$

Cet ensemble pourra être representé de la manière suivante:

$$g = (*g_j, T_1, T_2, \ldots, T_p), \tag{12}$$

où T_i désignent les substitutions du groupe G_e qui vérifient la congruence (11), mais qui n'entrent pas dans le groupe $*g_j$ auquel se reduisent les substitutions du groupe (p, q, r) satisfaisant à la congruence $d \equiv \omega b \pmod{n}$; on a $p \geqslant 0$.

Nous avons désigné dejà l'indice du groupe

$*g_j$ par rapport à G_{e_1} par j,
G_{e_1} „ „ G_e „ k,

nous désignons maintenant les indices du groupe

$*g_j$ par rapport à g par k_1,
g „ „ G_e „ j_1.

On aura $kj = k, j_1$, parce qu'en désignant par m le degré du groupe $^*g_j$ on a les égalités

$$e = mk_1 j_1 = mkj.$$

Envisageons en premier lieu le cas:

$$k_1 \leqslant k, \quad j_1 \geqslant j.$$

Nous démontrons le propriété suivante:

Théorème III: *Si l'indice k_1 du groupe $^*g_j$ par rapport au groupe g est inférieure à l'indice k du groupe G_{e_1} par rapport a G_e, on a la relation*

$$j_1 - j = \frac{e}{M} \frac{k - k_1}{k},$$

où M désigne le degré du groupe g.

Prenons la substitution $S_2 = (a_2, b_2, c_2, d_2)$ qui figure dans la formule (7); elle se reduit (mod n) à la substitution $^*S_2 = (^*a_2, ^*b_2, ^*c_2, ^*d_2)$ qui ne se trouvera pas parmi les substitutions

$$T_1, T_2, \ldots, T_p$$

de la formule (12), parce que la substitution S_2 ne satisfait pas à la congruence

$$d_2 \equiv \omega b_2 \pmod{n}.$$

Nous obtenons l'ensemble

$$^*S_2\, ^*g_j, ^*S_2\, T_1, \ldots, ^*S_2\, T_p \tag{13}$$

composé de substitutions du groupe G_e.

Cet ensemble possédera les propriétés suivantes:

1) l'égalité $^*S_2\, T_j = T_i$ $(i, j = 1, 2, \ldots, p)$ sera impossible, car on aurait alors

$$^*S_2 = T_i T_j^{-1},$$

et la substitution S_2 devrait vérifier la congruence $d_2 \equiv \omega b_2 \pmod{n}$,

2) la substitution $S_2\, T_i$ n'entrera pas dans le groupe $^*g_j$, parce qu'en désignant par U une substitution du groupe $^*g_j$ on aurait

$$^*S_2\, T_i = U, \quad \text{d'où} \quad ^*S_2 = UT_i^{-1};$$

mais la substitution S_2 ne satisfait pas à la congruence $d_2 \equiv \omega b_2 \pmod{n}$,

3) aucune substitution T n'entre dans l'ensemble $^*S_2\,^*g_j$, parce qu'on aurait alors

$$^*S_2\,U = T, \quad \text{où} \quad ^*S_2 = TU^{-1},$$

où U désigne une substitution du groupe $^*g_j$, mais la substitution $^*S_2$ ne satisfait pas à la congruence $d_2 \equiv \omega b_2$,

4) l'ensemble $^*S_2\,^*g_j$ n'a pas de substitutions communes avec le groupe $^*g_j$ (d'après le théorème II).

La substitution $^*S_3 = (^*a_3, ^*b_3, ^*c_3, ^*d_3)$ à laquelle se reduit la substitution S_3 figurant dans la formule (7), ne se trouvera pas parmi les substitutions T_i et $^*S_2\,T_i$ parce que les substitutions T_i et $^*S_2\,T_i$ sont du nombre de celles auxquelles ne se reduisent pas (mod n) les substitutions du groupe (p, q, r). Nous obtenons la suite.

$$^*S_3\,^*g_j, ^*S_3\,T_1, ^*S_3\,T_2, \ldots, ^*S_3\,T_p \tag{14}$$

qui n'aura pas des substitutions égales. La suite obtenue possèdera les propriétés suivantes:

1) l'égalité

$$^*S_3\,T_i = ^*S_2\,T_j$$

n'aura pas lieu, parce qu'on aurait alors

$$^*S_2^{-1}\,^*S_3 = T_j\,T_i^{-1}$$

et la substitution $^*S_2^{-1}\,^*S_3 =$ devrait vérifier la congruence $d \equiv \omega b$ (mod n); cette substitution devrait donc: a) ou se trouver parmi les substitutions T_i ou b) entrer dans le groupe $^*g_j$. Mais la substitution $^*S_2^{-1}\,^*S_3$ ne peut être égale à T_i, parce que le produit $^*S_2^{-1}\,^*S_3$ doit être en chaque cas une substitution de nombre de celles, auquelles se reduit le groupe (p, q, r); de même on ne peut pas avoir (en désignant par U une substitution du groupe $^*g_j$)

$$^*S_2^{-1}\,^*S_3 = U,$$

parce qu'il serait alors $^*S_3 = ^*S_2\,U$ et la substtttution $^*S_3$ se trouverait dans la ligne (9) de la décomposition du groupe G_{e_1} (p. 6),

2) la substitution $^*S_3\,T_i$ n'entrera pas dans la ligne $^*S^*g_j$, parce qu'on aurait alors

$$^*S_3\,T_i = ^*S_2\,U,$$

d'où

$$T_i = ^*S_3^{-1}\,^*S_2\,U,$$

et la substitution T_i devrait se trouver dans le groupe G_{e_1}, ce qui est contraire à l'hypothèse que la substitution T_i appartient au

nombre de substitutions auxquelles ne se reduit pas le groupe (p, q, r),

3) la substitution $*S_2\,T$ n'entre pas dans la ligne $*S_3\,*g_j$, parce qu'on aurait alors

$$*S\,T = *S_3\,U,$$

ce qui est impossible (comme plus haut),

4) les ensembles $*S_3*g_j$ et $*S_2*g_j$ n'ont pas de substitutions communes, car on aurait alors (en désignant par U_1 et U_2 deux substitutions du groupe $*g_j$)

$$*S_3\,U_1 = *S_2\,U_2,$$

d'où $*S_3 = *S_2\,U_2\,U_1^{-1} = *S_2\,U$, où l'on a posé $U = U_2\,U_1^{-1}$; la substitution S_3 devrait donc entrer dans la ligne (13).

Nous obtenons le tableau suivant

$$\begin{array}{cccccc} *g_j, & T_1, & T_2, \ldots, & T_p, \\ *S_2\,*g_j, & *S_2\,T_1, & *S_2\,T_2, \ldots, & *S_2\,T_p, \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ *S_j*g_j, & *S_j\,T_1, & *S_j\,T_2, \ldots, & *S_j\,T_p, \end{array}$$

composé de substitutions du groupe G_e *toutes différentes.*

Si ce tableau n'épuise pas toutes les substitutions du groupe G_e, nous obtiendrons encore $j_1 - j$ lignes; il sera

$$j_1 = \frac{e}{M};$$

où M désigne le degré du groupe g.

Observons maintenant qu'en vertu du théorème II, le degré e_1 du groupe G_{e_1} est égal au produit de l'indice j et du degré du groupe de substitutions reduites $(*a, *b, *c, *d)$ satisfaisant à la congruence $*d \equiv \omega *b \pmod n$ et faisant partie du groupe G_{e_1}. Mais le degré de ce groupe est $M : k_1$, on a donc

$$e_1 = j\,\frac{M}{k_1};$$

on a $e = e_1\,k$, parce que l'indice du groupe G_{e_1} par rapport à G_e est k, on a donc:

$$\frac{e}{k} = j\,\frac{M}{k_1},$$

d'où

$$j_1 - j = \frac{e}{M} \cdot \frac{k - k_1}{k}.$$

§ 4. Passons maintenant au second cas $k_1 > k$. Nous avons le théorème suivant:

Théorème IV: *L'indice k_1 du groupe $*g_j$ par rapport à g, ne peut pas surpasser l'indice du groupe G_{e_1} par rapport à G_e.*

En effet; représentons le groupe G_{e_1} dans le tableau suivant

$$\begin{array}{c} *g_j, \\ *S_2 *g_j, \\ \vdots \\ \vdots \\ *S_j *g_j, \end{array}$$

et envisageons le groupe

$$g = (*g_j, T_1, T_2 \ldots, T_p),$$

où T_i sont des substitutions du groupe G_e qui vérifient la congruence $*d \equiv \omega *b \pmod{n}$, mais n'entrent pas dans le groupe $*g_j$.

Prenons une des substitutions T, par exemple T_2: alors dans le tableau

$$\begin{array}{c} *g_j T_2, \\ *S_2 *g_j T_2, \\ \vdots \\ \vdots \\ *S_j *g_j T_2 \end{array}$$

l'ensemble $*g_j T_2$ sera composé exclusivement de substitutions T différentes entre elles. Les ensembles

$$(15) \qquad *S_2 *g_j T_2, \ldots, *S_j *g_j T_2$$

et les ensembles

$$(16) \qquad *S_2 *g_j, \ldots, *S_j *g_j$$

ne contiendront pas de substitutions communes. En effet, en désignant par U une substitution du groupe $*g_j$ on aurait:

$$*S_m U = *S_n U_1 T_2, \qquad (m, n = 2, 3, \ldots, j)$$

d'où

$$T_2 = U_1^{-1} *S_n *S_m U;$$

mais les substitutions $*S$ et $*U$, étant reduites du groupe (p, q, r) entrent dans le groupe G_{e_1}, donc la substitution T_2 devrait alors entrer dans le groupe G_{e_1}, ce qui est contraire à l'hypothèse faite sur les substitutions T. L'ensemble (16) n'aura donc pas de substitutions communes avec l'ensemble (15).

En prenant successivement une substitution T_3 qui n'entre pas dans l'ensemble $*g_j T_2$, une autre T_4 qui n'entre pas dans les ensembles $*g_j T_2$, $*g_j T_3$ et ainsi de suite, on obtiendra le tableau

$$(17)\qquad \begin{array}{c} *g_j, \quad *g_j T_2, \ldots, \quad *g_j T_k, \\ *S_2 *g_j, *S_2 *g_j T_2, \ldots, *S_2 *g_j T_k, \\ \cdots\cdots\cdots\cdots\cdots \\ *S_j *g_j, *S_j *g_j T_2, \ldots, *S_j *g_j T_k, \end{array}$$

dans lequel aucune de deux colonnes ne contiendra d'élements communes. En effet, il suffira démontrer dans ce but l'impossibilité de 5 égalités suivantes

$$\begin{aligned} S_r U_j' T_s &= S_i U_j T_l, \\ S_r U_j &= S_i U_j T_l, \\ U_j' &= S_i U_j T_l, \\ S_r U_j' T_s &= U_j T_l, \\ S_r U_j' &= U_j T_l, \end{aligned}$$

où l'on a posé: $r, i = 2, 3, \ldots, j$; $l, s = 2, 3, \ldots, k$ et les U désignent les substitutions du groupe $*g_j$.

Il suffira de démontrer l'impossibilité de la première égalité. En effet, si nous avions

$$S_r U_j' T_s = S_i U_j T_l,$$

on aurait alors

$$T_l T_s^{-1} = U_j^{-1} S_i^{-1} S_r U_j'$$

et le produit

$$(18)\qquad U_j^{-1} S_i^{-1} S_r U_j'$$

étant égal à $T_l T_s^{-1}$, devrait vérifier la congruence

$$d \equiv \omega b \pmod{n};$$

il devrait donc: a) ou être une de substitutions T ou b) appartenir au groupe $*g_j$. La première hypothèse est impossible, parce que les T sont les substitutions du groupe G_e auxquelles ne se reduisent

pas (mod n) les substitutions du groupe (p, q, r) et les substitutions S et U appartiennent au groupe G_{e_1}. La seconde hypothèse que le produit (18) appartienne au groupe $^*g_j$ conduit à l'égalité

$$U_q = U_j^{-1} S_i^{-1} S_r U_j',$$

où U_q désigne une substitution du groupe $^*g_j$. Mais on aurait alors

$$S_r U_j' = S_i U_j U_q$$

ce qui dans le cas $r \neq i$ est en contradiction avec la decomposition

$$G_{e_1} = (^*g_j, S_2\, ^*g_j, \ldots)$$

du groupe G_{e_1} par rapport à $^*g_j$; dans le cas $r = i$ on aurait

$$U' T_s = U T_l,$$

d'où $T_l = U^{-1} U' T_s$ ce qui est impossible.

Le tableau contient donc

$$mkj$$

substitutions différentes du groupe G_{e_1}; ce tableau répresente donc le groupe G_e entier et l'on ne peut pas avoir $k_1 > k$.

§ 5. Revenons maintenant au cas $k_1 \leqslant k$ envisagé auparavant; nous avons trouvé l'expression

$$j = \frac{e}{M} \cdot \frac{k_1}{k}$$

qui donnera dans notre cas le degré de l'équation de transformation pour la fonction automorphe appartenant au groupe (p, q, r). Le degré e du groupe G_e qui est égal au nombre de solutions de la congruence

$$a^2 + c^2 qr - p(b^2 q + d^2 r) \equiv 1 \pmod{n},$$

est, d'après la note citée, égal au nombre $n^m(n^{2m} - 1) : 2$: le degré M du groupe $^*g_j$ que est égal au nombre de solutions dans le corps $R_m(j)$ de la congruence $a^2 + c^2 qr \equiv 1 \pmod{n}$, est donné par la formule $n^m(n^m - 1) : 2$. On obtient le resultat suivant:

Théorème V: *Si l'indice k_1 du groupe $^*g_j$ par rapport au groupe g est inférieure à l'indice k du groupe G_{e_1}, par rapport à G_e le degré de l'équation de transformation de la fonction automorphe appartenant au groupe (p, q, r) défini dans le corps $R_m(j)$ a l'expression $(n^m + 1) k_1 : k$.*