Sur un groupe automorphe.

Par

K. Abramowicz.

Dans ma note [1]) insérée dans les Comptes Rendus, t. 187, j'ai étudié les fonctions appartenant au groupe $\{p, q, r\}$ formé des substitutions appelées par M. Fricke de „Haupttypus". En désignant par p_1, q_1, r_1 les diviseurs des nombres positifs p, q, r du corps algébrique $\Omega_k(\theta)$ et posant $p = p_1 p_2$, $q = q_1 q_2$, $r = r_1 r_2$, M. Fricke obtient le groupe plus général des substitutions

$$(1) \qquad \begin{pmatrix} (a\sqrt{p_1 r_1} + b\sqrt{p_2 r_2})\sqrt{q_1}, & (c\sqrt{p_1 r_2} + d\sqrt{p_2 r_1})\sqrt{q_2} \\ -(c\sqrt{p_1 r_2} - d\sqrt{p_2 r_1})\sqrt{q_2}, & (a\sqrt{p_1 r_1} - b\sqrt{p_2 r_2})\sqrt{q_1} \end{pmatrix}$$

au déterminant

$$(2) \qquad a^2 p_1 q_1 r_1 - b^2 p_2 q_1 r_2 + c^2 p_1 q_2 r_2 - d^2 p_2 q_2 r_1 = 1,$$

qu'il appelle [2]) groupe „de type" $[p_1, q_1, r_1]$. Nous nous proposons d'étendre le resultat obtenu dans la note citée aux groupes „ de type" $[p_1, q_1, r_1]$. Nous désignons les substitutions de ce groupe par $[a, b, c, d]$.

Dans ce qui va suivre nous supposerons que le corps algébrique $\Omega_k(\theta)$ de degré k auquel appartiennent les nombres positifs p, q, r est défini par l'équation $F(\theta) = 0$ et que ce corps a la base minimale $(1, \theta, \theta^2, \ldots \theta^{k-1})$. Nous faisons en outre l'hypothèse que le polynome $F(\theta)$ de degré k par rapport à θ est irréductible suivant le module n (supposé premier).

Le corps $\Omega_k(\theta)$ possédera alors les propriétés suivantes [3]) sur lesquelles nous nous appuyerons dans la suite:

---

[1]) Transformation des fonctions automorphes, p. 801.

[2]) Vorlesungen über die Theorie der automorphen Functionen, t. I, p. 538, 588.

[3]) Weber: Lehrbuch der Algebra, II, p. 306.

1) il contient n^k nombres (y compris 0) incongrus suivant le module n,

2) si le produit $a\beta$ de deux nombres a, β du corps est congru à 0, alors l'un de nombres a, β est congru à 0,

3) la congruence $ax \equiv \beta \pmod{n}$ a toujours dans le corps $\Omega_k(\theta)$ une solution et une seule (a n'étant pas $\equiv 0$),

4) on peut diviser ou multiplier les deux membres de la congruence par chaque nombre qui n'est pas $\equiv 0$.

Pour la transformation du n-ème degré du groupe $[p_1, q_1, r_1]$ nous chosirons la substitution V de la forme $V = [K, o, L, o]$ avec le déterminant

$$K^2 q_1 r_1 + L^2 q_2 r_2 = n,$$

où n est un nombre premier et les nombres K et L appartiennent au corps $\Omega_k(\theta)$.

En désignant par $f(z)$ la fonction automorphe appartenant au groupe $[p_1, q_1, r_1]$ nous nous proposons d'étudier la fonction transformée $f(Vz)$ appartenant au groupe $V^{-1}[p_1, q_1, r]V$. Dans le travail actuel nous demontrons que dans le cas où le polygone fondamental du groupe $[p_1, q_1, r_1]$ a un nombre fini de sommets la relation entre les fonctions $f(Vz)$ et $f(z)$ est algébrique de degré $n^k + 1$ en $f(Vz)$.

Pour les substitutions $[a', b', c', d']$ du groupe transformé $V^{-1}[p_1, q_1, r_1]V$ nous obtenons les valeurs:

$$(3) \qquad \begin{aligned} a' &= na, b' = b(K^2 p_1 q_1 r_1 - L^2 p_1 q_2 r_2) - 2\,KLdp_1 q_2 r_1, \\ c' &= nc, d' = d(K^2 p_1 q_1 r_1 - L^2 p_1 q_2 r_2) + 2\,KLbp_1 q_1 r_2. \end{aligned}$$

On voit que les substitutions $[a', b', c', d']$ du groupe transformé $V^{-1}[p_1, q_1, r_1]V$ ont le déterminant n^2; pour que le déterminant de $[a', b', c', d']$ soit égal à 1, les nombres a', b', c', d' doivent être divisibles par n. Après cette remarque on raisonnera de la manière suivante:

1) Dans le sous-groupe g_j commun aux groupes $[p_1, q_1, r_1]$ et $V^{-1}[p_1, q_1, r_1]V$ ne peuvent entrer que les substitutions $[a', b', c', d']$ du groupe $V^{-1}[p_1, q_1, r_1]V$ qui s'obtiennent de substitutions $[a, b, c, d]$ satisfaisant à la congruence

$$Kbq_1 \equiv Ldq_2 \pmod{n}.$$

En effet, dans ce cas seulement les nombres b' et d' sont di-

visibles par n, ce qu'on vérifie immédiatement à l'aide de formules (3), en tenant compte de la congruence [1]):

$$K^2 q_1 r_1 \equiv -L^2 q_2 r_2 .$$

2) Les substitutions $[a', b', c', d]$ qui peuvent entrer dans le groupe g_j doivent remplir la condition

$$Kd' r_1 \equiv Lb' r_2 (\mathrm{mod}\, n).$$

En effet, la resolution des égalités

$$b' = \frac{1}{n}[b(K^2 p_1 q_1 r_1 - L^2 p_1 q_2 r_2) - 2KLdp_1 q_2 r_2],$$

$$d' = \frac{1}{n}[d(K^2 p_1 q_1 r_1 - L^2 p_1 q_2 r_2) + 2KLbp_1 q_1 r_2]$$

par rapport à b et d donne

$$b = \frac{1}{n}\{b'(K^2 p_1 q_1 r_1 - L^2 p_1 q_2 r_2) + 2KLd' p_1 q_2 r_1\},$$

$$d = \frac{1}{n}\{d'(K^2 p_1 q_1 r_2 - L^2 p_1 q_2 r_2) - 2KLb' p_1 q_1 r_2\},$$

et l'on voit que la condition

$$Kd' r_1 \equiv Lb' r_2 (\mathrm{mod}\, n)$$

doit être remplie pour que les nombres b et d soient entiers.

3) On vérifie inversement que chaque substitution $[\alpha, \beta, \gamma, \delta]$ du groupe $[p_1, q_1, r_1]$ qui s'obtient par la transformation V d'une substitution $[a, b, c, d]$ satisfaisant à la congruence $Kbq_1 \equiv Ldq_2$, satisfaira à la conguence

$$K\delta r_1 \equiv L\beta r_2 (\mathrm{mod}\, n).$$

En effet, si l'on transforme la substitution $[a, b, c, d]$ à l'aide de la substitution V et si l'on pose

$$Kbq_1 = Lq_2 d + H \cdot n,$$

où H désigne un nombre entier du corps $\Omega_k(\theta)$, on trouvera (tenant compte de la congruence $K^2 q_1 r_1 \equiv -L^2 q_2 r_2$) les valeurs

---

[1]) Aucun de nombres p, q, r n'est congru à 0.

$$\beta = -b + 2KHp_1r_1,$$
$$\delta = \quad d + 2LKp_1r_2,$$

et l'on aura la congruence

$$Kr_1(d + 2LHp_1r_2) \equiv Lr_2(-b + 2KHpr_1),$$

qui se reduit à

$$Kdr_1 \equiv -Lbr_1 \pmod{n}$$

ou encore $Kbq_1 \equiv Ldq_2$ (en vertu de $K^2q_1r_1 \equiv -L^2q_2r_2$).

4) Le sous-groupe cherché g_j est composé de toutes les substitutions $[\alpha, \beta, \gamma, \delta]$ au déterminant 1 satisfaisant à la congruence

$$K\delta r_1 \equiv L\beta r_2 \pmod{n}. \tag{4}$$

En effet, d'après 3) une telle substitution s'obtient par la transformation V d'une substitution $[a, b, c, d]$ satisfaisant à la congruence $Kbq_1 \equiv Ldq_2$; elle remplit donc la condition 1); d'autre part elle satisfait aussi à la condition 2).

Si l'on fait maintenant l'hypothèse que le polygone fandamentale du groupe discontinu $[p_1, q_1, r_1]$ a un nombre fini de sommets la relation entre les fonctions $f(Vz)$ et $f(z)$ sera algébrique. La fonction $f(Vz)$ satisfaira à une équation de degré égal à l'indice j du sous-groupe g_j par rapport au groupe $[p_1, q_1, r_1]$.

Envisageons le groupe fini G_e auquel se reduit le groupe $[p_1, q_1, r_1]$ par rapport au module n. Le nombre e des substitutions du groupe G_e sera égal à la moitié du nombre de solutions en a, b, c, d de la congruence

$$a^2p_1q_1r_1 - b^2p_2q_1r_2 + c^2p_1q_2r_2 - d^2p_2q_2r_1 \equiv 1 \pmod{n} \tag{5}$$

dans le corps $\Omega_k(\theta)$.

Nous devons distinguer deux cas: 1) les corps $\Omega_k(\theta)$ dans lesquels le nombre -1 est reste quadratique, 2) et les corps $\Omega_k(\theta)$ dans lesquels -1 est non-reste. En désignant par g la racine primitive du nombre n dans le corps $\Omega_k(\theta)$, c'est-à-dire le nombre pour lequel

$$g^{n^k-1} \equiv 1 \pmod{n}$$

on aura la propriété dont nous ferons usage:

Si l'on ajoute 1 aux deux non-résidus

$$g^i, g^{n^k-i-1} \quad (i = 1, 3, \ldots)$$

de la suite

$$g, g^3, \dots g^{n^k-2}$$

alors l'une des sommes

$$1 + g^i, 1 + g^{n^k-i+1}$$

sera résidu, l'autre non-résidu.

En effet, faisant l'hypothèse que $1 + g^i$ est résidu, on a

$$1 + g^i \equiv g^{n^k-1} + g^i \equiv g^i(1 + g^{n^k-i-1})$$

et, comme g^i est non-résidu, la somme $1 + g^{n^k-i-1}$ devra être non-résidu, afin que le produit $g^i(1 + g^{n^k-i-1})$ soit résidu; et inversement.

Nous demontrons maintenant le théorème suivant que nous avons formulé dans la note citée sans demonstration:

Les nombres A et B étant simultanément résidus ou non-résidus (mod n) dans le corps $\Omega_k(\theta)$ les congruences

$$Ax^2 + By^2 \equiv 0, \quad Ax^2 + By^2 \equiv M \not\equiv 0 \pmod{n}$$

ont dans le corps $\Omega_k(\theta)$ respectivement $2n^k - 1$ et $n^k - 1$ solutions, si le nombre -1 est résidu dans le corps $\Omega_k(\theta)$, et respectivement 1 et $n^k + 1$ solutions, si -1 est non-résidu dans le corps $\Omega_k(\theta)$; si l'un de nombres A et B est résidu et l'autre non-résidu les mêmes congruences ont respectivement 1 et $n^k + 1$ solutions dans le premier cas et $2n^k - 1$ et $n^k - 1$ solutions dans le second cas.

Demonstration. 1) Supposons que le nombre -1 est résidu dans le corps $\Omega_k(\theta)$, c'est-à-dire

$$n^k \equiv 1 \pmod 4.$$

Parmi les $(n^k - 1):2$ restes quadratiques

$$1, g^2, g^4, \dots g^{n^k-1}$$

on ne trouvera que les $(n^k - 1):2$ sommes

$$g^{2i} + g^{\frac{k-1}{2}+2i} \equiv 0 \pmod{n}, \quad i = 0, 1, 2, \dots \frac{n^k - 3}{2};$$

de chaque somme on obtiendra 4 solutions de la congruence $x^2 + y^2 \equiv 0$, et en ajoutant la solution $(0, 0)$ on aura $2n^k - 1$ solutions.

Parmi les $(n^k - 1):2$ sommes

$$1 + 1, 1 + g^2, \ldots 1 + g^{n^k-3} \tag{6}$$

on a une égale à 0, et la suite de $(n^k - 1):2$ sommes

$$1 + g, 1 + g^3, \ldots 1 + g^{n^k-2} \tag{7}$$

contiendra (d'après la propriété mentionnée plus haut) $(n^k - 1):4$ résidus et $(n^k - 1):4$ non-résidus. La suite (6) devra donc contenir

$$\frac{n^k - 1}{4} - 1 \text{ résidus}$$

(parceque le deux suites (6) et (7) doivent épuiser tous les résidus). Si l'on joint à la suite (6) la somme $1 + 0$ on aura dans la suite de $(n^k - 1):2 + 1$ sommes

$$1 + 0, 1 + 1, 1 + g^2, \ldots 1 + g^{n^k-3} \tag{8}$$

$(n^k - 1):4$ résidus et $(n^k - 1):4$ non-résidus.

En multipliant les élements de la suite (8) consécutivement par

$$1, g^2, \ldots g^{n^k-3}$$

on obtiendra $(n^k - 1):2$ suites de produits de la forme

$$g^{2i}(1 + g^{2j}); \tag{9}$$

chaque colonne de cet ensemble (9) de produits contiendra ou tous les $(n^k - 1):2$ résidus différents ou tous les $(n^k - 1):2$ non-résidus différents. Chaque résidu ou non-résidu M sera alors de $(n^k - 1):4$ manières representé dans la forme (9). La congruence $x^2 + y^2 \equiv M \pmod{n}$ aura

$$\frac{n^k - 1}{4} \cdot 4 = n^k - 1$$

solutions (parceque chaque somme $g^{2i} + g^{2(i+j)}$ se repète deux fois).

2) Supposons que le nombre -1 est non résidu dans le corps $\Omega_k(\theta)$, c'est-à-dire $n^k = 4s + 3$, où s est un nombre naturel; on n'aura pas ici

$$g^{\frac{n^k-1}{2}} + 1 \equiv 0 \pmod{n}$$

et le nombre $n - 1$ sera non-résidu. Comme précedemment on ajoute 1 à tous les non-résidus

$$g, g^3, \ldots g^{n^k-2}$$

dont le nombre $(n^k - 1):2 = 2s + 1$ est impair; on obtiendra dans la suite

$$1 + g, 1 + g^3, \ldots 1 + g^{n^k-3} \tag{10}$$

une fois 0 et s résidus et s non-résidus (d'après la propriété citée plus haut). Dans la suite de $(n^k - 1):2$ sommes

$$1 + 1, 1 + g^2, \ldots 1 + g^{n^k-3} \tag{11}$$

on aura alors $(n^k - 3):4 + 1$ non résidus (afin qu'on ait dans les deux suites (10) et (11) le nombre total de résidus) et $(n^k - 3):4$ résidus.

La suite de $(n^k + 1):2$ sommes

$$1 + 0, 1 + 1, 1 + g^2, \ldots 1 + g^{n^k-3} \tag{12}$$

contiendra alors $(n^k + 1):4$ résidus et $(n^k + 1):4$ non-résidus.

En multipliant les élements de la suite (12) consécutivement par

$$1, g^2, \ldots g^{n^k-3}$$

on obtiendrra $(n^k - 1):2$ suites de produits de la forme

$$g^{2j}(1 + g^{2j}); \tag{13}$$

chaque colonne de cet ensemble (13) de produits contiendra ou tous les $(n^k - 1):2$ résidus différents ou tous les $(n^k - 1):2$ non résidus différents. Chaque résidu ou non-résidu M sera alors de $(n^k - 1):4$ manières representé dans la forme (13). La congruence $x^2 + y^2 \equiv M$ aura $n^k + 1$ solutions.

Si l'on passe aux congruences $Ax^2 + By^2 \equiv M$, on voit facilement que dans le cas où A et B sont simultanément résidus ou non-résidus les nombres des solutions de congruences $Ax^2 + By^2 \equiv M$ sont les mêmes que des congruences envisagées precédemment.

Si, au contraire, on suppose

$$A \text{ résidu, } B \text{ non-résidu}$$

et si l'on se place dans le premier cas (de -1 résidu) on n'aura jamais

$$g^{2j} + g^{2j+1} \equiv 0,$$

et l'on aura alors une seule solution $(0, 0)$ pour la congruence $Ax^2 + By^2 \equiv 0$. Si l'on prends la suite de $(n^k - 1):2$ sommes

$$1 + g, 1 + g^3, \ldots 1 + g^{n^k-2}$$

dans laquelle on a $(n^k - 1):4$ résidus et $(n^k - 1):4$ non-résidus, et si l'on multiplie les élements de cette suite par

$$g, g^3, \ldots g^{n^k-2}$$

on obtiendra pour chaque nombre $M \not\equiv 0$ $(n^k - 1):4$ représentations dans la forme

$$g^{2i} + g^{2j+1},$$

c'est-à-dire $n^k - 1$ solutions de la congruence $Ax^2 + By^2 \equiv M$; en ajoutant encore *deux* solutions correspondant aux valeurs $x \equiv 0$, si M est non-résidu, et $y \equiv 0$, si M est résidu, on aura définitivement $n^k + 1$ solutions de la congruence $Ax^2 + By^2 \equiv M \pmod n$.

Dans le second cas (de -1 non-résidu, $n^k = 4s + 3$) on aura une congruence

$$g^{2j+1} + 1 \equiv 0 \pmod n$$

et, en la multipliant par les $(n^k - 1):2$ nombres

$$1, g^2, \ldots g^{n^k-3}$$

on aura $(n^k - 1):2 + 1 = 2n^k - 1$ solutions de la congruence $Ax^2 + By^2 \equiv 0$ (après avoir ajouté la solution $(0, 0)$. De même si l'on prends la suite de $(n^k - 1):2$ sommes

$$1 + g, 1 + g^3, \ldots 1 + g^{n^k-2}$$

dans laquelle on a (une de sommes est 0) maintenant

$$(n^k - 3):4 \text{ résidus et } (n^k - 3):4 \text{ non-résidus,}$$

et si l'on la multiplie successivement par $1, g^2, \ldots g^{n^k-3}$ on obtiendra $(n^k - 3):4$ représentations $(\text{mod } n)$ de chaque nombre M dans la forme $g^{2i} + g^{2j+1}$, d'où $n^k - 3$ solutions de la congruence $Ax^2 + By^2 \equiv M$; en ajoutant encore *deux* solutions correspondant à la valeur $x \equiv 0$, si M est non-résidu, et à $y \equiv 0$, si M est résidu, on aura $n^k - 1$ solutions.

Passons maitenant à la détermination du degré du groupe G_e auquel se reduit le groupe $[p_1, q_1, r_1]$ par rapport au module n.

Pour déterminer le nombre de solutions de la congruence (1) en a, b, c, d écrivons cette congruence sous la forme

$$(14) \qquad p_1(a^2q_1r_1 + c^2q_2r_2) - p_2(b^2q_1r_2 + d^2q_2r_1) \equiv 1 \pmod{n}.$$

On posera

$$(15) \qquad \begin{aligned} a^2q_1r_1 + c^2q_2r_2 &= X, \\ b^2q_1r_2 + d^2q_2r_1 &= Y, \end{aligned}$$

et l'on aura alors la congruence

$$p_1X - p_2Y \equiv 1 \pmod{n}:$$

elle a les solutions

$$X \equiv 1 + p_2\xi, \quad Y \equiv p_1\xi,$$

où ξ parcourt l'ensemble de n^k nombres du corps $\Omega_k(\theta)$ incongrus par rapport au module n.

1) Supposons que -1 est résidu dans le corps $\Omega_k(\theta)$. En remarquant que les produits q_1r_1 et q_2r_2 sont simultanément résidus ou non-résidus, on a:

a) pour $\xi = 0$, $X \equiv 1$, $Y \equiv 0$ et les congruences (15) admettront

$$(2n^k - 1)(n^k - 1) \text{ solutions;}$$

b) pour $X \equiv 0$, $Y \equiv \xi_0$ (tel que $1 + p_2\xi_0 \equiv 0$) on aura le même nombre de solutions $(2n^k - 1)(n^k - 1)$,

c) pour les $n^k - 2$ valeurs restantes $Y \equiv \xi$, $X \equiv 1 + p_2\xi$ on aura ensemble

$$(n^k - 2)(n^k - 1)^2$$

solutions En somme on trouve indépendemment de la valeur de produits q_1r_1, q_2r_2 le nombre total $n^k(n^{2k} - 1)$ de solutions; on divisera ce nombre par 2 parceque le changement simultané du signe de coefficients a, b, c, d de la substitution $[a, b, c, d]$ ne donne pas de substitution nouvelle.

2) Supposons que -1 est non-résidu dans le corps $\Omega_k(\theta)$. En remarquant que maintenant l'un de produits q_1r_1 et q_2r_2 est résidu l'autre non-résidu, on aura de la même manière respectivement les nombres

$$1 \cdot (n^k + 1), 1 \cdot (n^k + 1), (n^k - 2)(n^k + 1)^2$$

de solutions; en les additionnant on obtient le même nombre $n^k(n^{2k} - 1)$.

On pourra toujours déterminer un nombre E satisfaisant à la congruence

$$Kr_1E \equiv Lr_2 \pmod{n};$$

on remplacera alors la congruence (4) par $d \equiv Eb$ et, en vertu de l'égalité $K^2q_1r_1 + L^2q_2r_2 = n$, ou aura alors

$$r_1q_2E^2 \equiv -r_2q_1 \pmod{n} \tag{16}$$

On a l'égalité

$$[p_1, q_1, r_1] = \{g_j, S_2g_j, \ldots S_jg_j\},$$

où les S désignent certaines substitutions du groupe $[p_1, q_1, r_1]$ ne vérifiant pas la congruence $d \equiv Eb$. Si nous considerons le groupe fini G_e auquel se reduit le groupe $[p_1, q_1, r_1]$ par rapport au module n, les substitutions du sous-groupe g_j se reduiront à celles de substitutions du groupe G_e qui vérifient la congruence $d \equiv Eb$. Nous sommes donc conduits à chercher l'ordre du groupe de substitutions de G_e satisfaisant à la congruence $d \equiv Eb$. On voit que, grâce à la relation (16), cet ordre sera égal à la moitié du nombre de solutions en a et c de la congruence

$$a^2p_1q_1r_1 + c^2p_1q_2r_2 \equiv 1 \pmod{n} \tag{17}$$

dans le corps $\Omega_k(\theta)$ multiplié par n^k.

1) Si -1 est *résidu* dans le corps $\Omega_k(\theta)$ les produits q_1r_1, q_2r_2 seront simultanément résidus; le nombre de solutions de la congruence (17) est $n^k - 1$;

2) si -1 est *non-résidu* dans le corps $\Omega_k(\theta)$ l'un de produits q_1r_1, q_2r_2 est résidu l'autre non-résidu; mais alors le nombre de solutions de la congruence (17) est aussi $n^k - 1$.

L'ordre du groupe de substitutions $[a, b, c, d]$ satisfaisant (mod n) à la congruence $d \equiv Eb$ est $n^k(n^k - 1):2$. Nous obtenons le théorème suivant:

Si le polygone fondamental du groupe discontinu $[p_1, q_1, r_1]$ défini dans le corps $\Omega_k(\theta)$ de degré k ayant la base minimale $(1, \theta, \ldots \theta^{k-1})$ a un nombre fini de sommets et l'équation $F(\theta) = 0$ définissant le corps $\Omega_k(\theta)$ est irréductible suivant le module n, alors l'équation algébrique à laquelle satisfait la fonction $f(z)$ appartenant au groupe $[p_1, q_1, r_1]$ transformée à l'aide d'une substitution $V = [K, o, L, o]$ de déterminant $K^2q_1r_1 + L^2q_2r_2 = n$ est de degré $n^k + 1$.