Sur la transformation du p-ème degré d'une fonction automorphe.

Par

C. Abramowicz.

Dans son mémoire „Sur les fonctions fuchsiennes et l'arithmétique" Poincaré [1]) a envisagé la possibilité de la transformation des fonctions automorphes. Les idées de Poincaré ont été reprises par Fricke qui a consacré des recherches étendues au cas de transformation du 3-ème degré [2]) de la fonction automorphe appartenant au groupe (0, 3; 2, 4, 5). Outre ces recherches de Fricke et deux cas spéciaux conduisant aux groupes G_{60} et G_{168} envisagés par lui [3]), nous ne trouvons pas d'autres résultats dans la théorie de la transformation des fonctions automorphes. Dans le travail actuel nous nous occupons du cas général de transformation de la fonction automorphe appartenant au groupe (0, 3; 2, 4, 5).

Pour énoncer les résultats du travail actuel remarquons qu'on définit le groupe (0, 3; 2, 4, 5) comme l'ensemble de toutes les substitutions de la forme

$$(1) \qquad z' = \frac{(a + b\sqrt{j})\,z + c + d\sqrt{j}}{(-c + d\sqrt{j})\,z + a - b\sqrt{j}}$$

où j désigne la racine positive de l'équation $j^2 + j - 1 = 0$, les nombres a, b, c, d sont des nombres entiers du corps quadratique $K(j)$ et le déterminant $a^2 + c^2 - j(b^2 + d^2)$ des substitutions est égal à 4 ou 2; on a en outre $a \equiv c$, $b \equiv d \pmod 2$.

[1]) Journal de mathématiques, IV, t. 3, p. 405.

[2]) Vorlesungen über die Theorie der automorphen Functionen, t. II, p. 553.

[3]) Acta mathematica, t. 17, p. 345.

La fonction automorphe $\varphi(z)$ appartenant au groupe (0, 3; 2, 4, 5) remplit donc la condition $\varphi(z') = \varphi(z)$.

Si l'on désigne maintenant par $z' = T(z)$ une substitution de la forme (1) au déterminant

$$a^2 + c^2 - j(b^2 + d^2) = p,$$

où p désigne un nombre naturel différent de 4 et 2, on dira avec Poincaré [1]) que la transformation du p-ème degré de la fonction automorphe appartenant au groupe (0, 3; 2, 4, 5) consiste dans la détermination de la relation entre la fonction $\varphi(z)$ et la fonction transformée $\varphi(Tz)$. Cette relation, comme l'a montré Poincaré, ne sera algébrique que dans le cas où le groupe (0, 3; 2, 4, 5) et le groupe $T^{-1}(0, 3; 2, 4, 5)\, T$ sont commensurables.

Il est évident qu'on peut pour la transformation du p-ème degré de la fonction automorphe employer chaque substitution $T(z)$ de la forme (1) ayant le déterminant égal au nombre p. Mais nous faisons la restriction $b = d = 0$ et nous ne regarderons que les substitutions de la forme

$$T(z)\ \frac{Pz + Q}{-Qz + P}$$

au déterminant $P^2 + Q^2 = p$, les nombres P et Q étant entiers dans le corps $K(j)$.

En prenant la substitution $T(z)$ nous obtenons les résultats suivants: 1) nous démontrons la commensurabilité des groupes (0, 3; 2, 4, 5) et $T^{-1}(0, 3; 2, 4, 5)\, T$, 2), nous déterminons l'indice du groupe de substitutions au déterminant 1 contenu dans le groupe (0, 3; 2, 4, 5), 3) en s'appuyant sur ce résultat nous déterminons l'ordre du groupe de Galois de l'équation algébrique à laquelle satisfait la fonction automorphe transformée, 4) nous montrons enfin que le degré de cette équation est égal à $p^2 + 1$; nous appliquons les résultats obtenus à la transformation du 7-ème degré.

§ 1. La commensurabilité des groupes (0, 3; 2, 4, 5) et $T^{-1}(0, 3; 2, 4, 5)\, T$.

Nous désignerons les substitutions (1) du groupe (0, 3; 2, 4, 5) par (a, b, c, d); la substitution $T(z)$ aura alors la forme

$$T = (P, O, Q, O).$$

[1]) Oeuvres, t. II, p. 463.

Calculons les substitutions (A, B, C, D) du groupe transformé $T^{-1}(0.\ 3;\ 2,\ 4,\ 5)\ T$. En appliquant les formules

$$\begin{aligned}
\alpha' &= ms\alpha - nr\delta + rs\beta - mn\gamma,\\
\beta' &= ns(\alpha - \beta) + s^2\beta - n^2\gamma,\\
\gamma' &= mr(\delta - \alpha) - r^2\beta + m^2\gamma,\\
\delta' &= ms\delta - nr\alpha - rs\beta + mn\gamma
\end{aligned}$$

donnant les coefficients α'. β', γ', δ' de la substitution qui s'obtient en transformant la substitution

$$\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \text{ à l'aide de } \begin{pmatrix}m, n\\ r, s\end{pmatrix},$$

nous trouvons pour les coefficients A, B, C, D de la substitution (A, B, C, D) du groupe transformé $T^{-1}(0, 3;\ 2, 4, 5)\ T$ les valeurs

$$\begin{aligned}
A &= pa, \quad B = b(P^2 - Q^2) - 2PQd,\\
C &= pc, \quad D = d(P^2 - Q^2) + 2PQb.
\end{aligned} \tag{2}$$

Pour démontrer la commensurabilité des groupes $(0, 3; 2, 4,)$ et $T^{-1}(0, 3; 2, 4, 5)\ T$ il suffira de montrer l'existence du sous-groupe commun à ces groupes.

Lemme I: Le sous-groupe commun aux groupes $(0, 3; 2, 4, 5)$ et $T^{-1}(0, 3; 2, 4, 5)\ T$ ne pourra contenir d'autres substitutions du groupe $T^{-1}(0, 3; 2, 4, 5)\ T$ que celles qui s'obtiennent de substitutions (a, b, c, d) satisfaisant à la congruence

$$2PQd \equiv (P^2 - Q^2)b\ (mod\, p). \tag{3}$$

En effet, les formules (2) montrent que le déterminant de la substitution (A, B, C, D) est

$$A^2 + C^2 - j(B^2 + D^2) = p^2\{a^2 + c^2 - j(b^2 + d^2)\};$$

afin que cette substitution (A, B, C, D) puisse appartenir au groupe $(0, 3; 2, 4, 5)$ son déterminant devra être égal à 4 ou 2; les nombres A, B, C, D doivent donc être divisibles par p; les quotients

$$\begin{aligned}
a' &= \frac{A}{p} = a, \quad b' = \frac{B}{p} = \frac{1}{p}\left\{b(P^2 - Q^2) - 2PQd\right\},\\
c' &= \frac{C}{p} = c, \quad d' = \frac{D}{p} = \frac{1}{p}\left\{d(P^2 - Q^2) + 2PQb\right\}
\end{aligned} \tag{4}$$

doivent être des nombres entiers du corps $K(j)$. Le nombre b' est entier si la condition (3) est remplie; mais on déduit de (3)

$$2PQd(P^2 - Q^2) = b(P^4 + Q^4 - 2P^2Q^2) = b\{(P^2 + Q^2)^2 - 4P^2Q^2\},$$

d'où, en vertu de l'égalité $P^2 + Q^2 = p$ on a

$$d(P^2 - Q^2) \equiv -2PQb(modp)$$

et la congruence obtenue montre que la valeur pour d'est aussi entière.

Lemme II: Les substitutions (a', b', c', d') du groupe $T^{-1}(0, 3; 2, 4, 5)T$ qui pourront entrer dans le groupe $(0, 3; 2, 4, 5)$ doivent remplir la condition

$$Pd' \equiv Qb'(modp).$$

En effet, le lemme I montre qu'une telle substitution (a', b', c', d') doit s'obtenir par la transformation d'une substitution (a, b, c, d) dont les termes a, b, c, d s'obtiennent en résolvant par rapport à a, b, c, d les congruences (4); ce sont des nombres

$$a = a', \quad b = \frac{1}{p}\left\{(P^2 - Q^2)b' + 2PQd'\right\},$$

$$c = c', \quad d = \frac{1}{p}\left\{(P^2 - Q^2)d' - 2PQb'\right\};$$

mais, afin que les nombres b et d soient entiers il faudra qu'on ait la congruence

$$(P^2 - Q^2)d' \equiv 2PQb'(modp).$$

qui pourra s'écrire

$$(2P^2 - p)d' \equiv 2PQb'(modp)$$

ou encore

$$Pd' \equiv Qb'(modp), \quad c.\,q.\,f.\,d.$$

Après ces remarques nous avons le théorème:

Théorème I: Le plus grand sous-groupe commun aux groupes

$$(0, 3; 2, 4, 5), \quad T^{-1}(0, 3; 2.4.5)T$$

se compose de toutes les substitutions (a, b, c, d) satisfaisant à la condition

$$Pd \equiv Qb(modp). \tag{5}$$

En effet toutes ces substitutions entrent dans le groupe $(0, 3; 2, 4, 5)$; mais, en vertu du lemme II, ce sont en même temps les seules substitutions du groupe transformé $T^{-1}(0, 3; 2, 4, 5)T$ qui peuvent entrer dans le sous-groupe cherché.

Ainsi nous avons démontré l'existence du sous-groupe, défini par la congruence (5). Mais il sera utile pour ce qui va suivre de donner une autre forme à la congruence (5). Nous déterminerons dans ce but un nombre $E + Hj$ du corps $K(j)$ qui satisfasse à la congruence

$$(E + Hj)^2 \equiv -1 \,(mod\, p);$$

alors l'une des deux congruences

$$P(E + Hj) + Q \equiv 0,$$
$$P(E + Hj) - Q \equiv 0$$

sera satisfaite parce que le produit de leurs premiers membres

$$P^2(E + Hj)^2 - Q^2$$

sera, en vertu de l'égalité $P^2 + Q^2 = p$, divisible par p.

Nous pouvons énoncer le théorème suivant:

Théorème II: Si l'on désigne par $E + Hj$ le nombre satisfaisant à la congruence

$$(E + Hj)^2 \equiv -1 \,(mod\, p) \tag{6}$$

et si l'on transforme le groupe $(0, 3; 2, 4, 5)$ à l'aide d'une substitution arbitraire

$$T = \frac{Pz + Q}{-Qz + P}$$

au déterminant $P^2 + Q^2 = p$, le sous-groupe commun aux groupes $(0, 3; 2, 4, 5)$ et $T^{-1}(0, 3; 2, 4, 5)T$ sera déterminé par la congruence

$$\pm d \equiv (E + Hj)b \,(mod\, p).$$

Nous avons supposé l'existence du nombre $E + Hj$ satisfaisant à la congruence (6); cette congrunce est équivalente aux deux suivantes

$$E^2 + H^2 \equiv -1, \quad 2E \equiv H \,(mod\, p)$$

d'où nous obtenons

$$5E^2 + 1 \equiv 0 \,(mod\, p).$$

On voit que le nombre $E + Hj$ n'existe que dans la cas où le nombre premier p remplit la condition

$$\left(\frac{-5}{p}\right) = 1.$$

Nous avons le théorème:

Théorème III: Etant donné un nombre premier p satisfaisant à la condition

$$\left(\frac{-5}{p}\right) = 1,$$

la transformation du p-ème degré de la fonction automorphe $\varphi(z)$ appartenant au groupe $(0, 3; 2, 4, 5)$ conduit à la fonction $\varphi(Tz)$ qui satisfait à une équation algébrique dont le degré est égal à l'indice du sous-groupe, défini par la congruence

$$d \equiv (E + Hj)b \pmod{p}$$

où $E + Hj$ vérifie la congruence $(E + Hj)^2 + 1 \equiv 0 \pmod{p}$.

La détermination de cet indice qui est le but principal de notre travail, s'appuyera sur une propriété du groupe de Galois de l'équation algébrique à laquelle satisfait la fonction transformée $\varphi(Tz)$; nous appelons cette équation l'équation de transformation.

§ 2. Les substitutions du groupe (0, 3; 2, 4, 5) au déterminant 1.

Pour déterminer l'ordre du groupe de Galois de l'équation de transformation, observons que ce groupe sera isomorphe avec le groupe fini G auquel se réduit le groupe $(0, 3; 2, 4, 5)$ suivant le module p. Mais, comme le groupe $(0, 3; 2, 4, 5)$ ne contient que les substitutions aux déterminants égaux à 4 ou à 2, l'ensemble G ne pourra contenir que les substitutions (a, b, c, d) aux déterminants $\equiv \equiv 4$ ou $\equiv 2 \pmod{p}$, les nombres a, b, c, d étant des nombres entiers du corps $K(j)$ incongrus par rapport au module p; le problème consiste à déterminer le nombre de ces substitutions. Mais nous pouvons simplifier les calculs en montrant qu'on peut se borner aux substitutions au déterminant 1 du groupe $(0, 3; 2, 4, 5)$; dans l'en-

semble G ces substitutions auront les déterminants congrus à 1 $(mod\ p)$. Nous démontrons le théorème suivant

Théorème IV: L'ensemble de toutes les substitutions (a, b, c, d) du groupe $(0, 3; 2, 4, 5)$ dont le déterminant $a^2 + c^2 - j(b^2 - d^2)$ est égal à 1 constitue un sous-groupe du groupe $(0, 3; 2, 4, 5)$ avec l'indice 10.

Pour démontrer ce théorème désignons par Γ le groupe considéré de substitutions (a, b, c, d) au déterminant 1 et cherchons le champ fondamental de ce groupe. Nous adjoignons dans ce but au groupe Γ la substitution $z' = -\bar{z}$, où $\bar{z}$ désigne le nombre conjugué avec z; le groupe nouveau $\bar{\Gamma}$ se composera de substitutions (a, b, c, d) et de toutes les substitutions de la forme

$$z' = \frac{(a + b\sqrt{j})\bar{z} - c - d\sqrt{j}}{(-c + d\sqrt{j})\bar{z} - a + b\sqrt{j}}. \tag{7}$$

La frontière du champ fontamental se composera de lignes de symétrie du groupe $\bar{\Gamma}$. Mais les lignes de symétrie sont caractérisées par l'égalité $b = 0$, ce seront donc des cercles

$$(-c + d\sqrt{j})(x^2 + y^2) - 2ax + c + d\sqrt{j} = 0. \tag{8}$$

Nous remarquons en outre que le groupe $\bar{\Gamma}$ ne peut contenir que des substitutions elliptiques à la période égale à 2.

En effet, la substitution (a, b, c, d) étant elliptique, on $a < 1$, mais le nombre $\bar{a}$ conjugué dans le corps $K(j)$ avec a doit aussi remplir la relation $\bar{a} < 1$; il sera donc $a\bar{a} < 1$, autrement dit, la norme du nombre a est plus petite que 1; mais si l'on a $N(a) < 1$, alors $N(a) = 0$ et l'on a $a = 0$; la période de la substitution elliptique est 2.

Il résulte de là que toutes les lignes de symétrie du groupe $\bar{\Gamma}$ se coupent sous des angles droits, autrement dit, les cercles (8) forment sur le plan un réseau de polygones avec les angles droits. Il reste à choisir parmi ces polygones celui qui est le champ fondamental du groupe $\bar{\Gamma}$.

Nous allons procéder de la manière suivante: 1) nous cherchons sur l'axe d'ordonnées le point elliptique du groupe $\bar{\Gamma}$ le plus prochain du point i; sur la ligne de symétrie qui passe par ce point nous cherchons le point elliptique le plus prochain, etc.; en procédant de telle manière nous retournons au point i et nous

obtenons un certain polygone circulaire. Si le groupe Γ contient encore des substitutions transformant ce polygone en lui-même, ces substitutions formeront un certain groupe qui devra être cyclique à une période q, alors la q-ème partie du polygone obtenu sera le champ fondamental du groupe Γ; 2) nous cherchons une telle substitution elliptique V n'appartenant pas au groupe $\bar{\Gamma}$ qui transformerait le groupe $\bar{\Gamma}$ en lui-même; c'est à dire vérifierait la relation $\bar{\Gamma} = V^{-1}\bar{\Gamma}V$.

Déterminons dans le corps du 4-ème degré obtenu par l'adjonction au corps $K(j)$ de la racine quadratique $\sqrt{j}$, une telle unité

$$\varepsilon = \alpha + \beta j + \sqrt{j}(\gamma + \delta j),$$

qu'on ait $\varepsilon\varepsilon = 1$, ε étant égal à $\alpha + \beta j - \sqrt{j}(\gamma + \delta j)$ et que le nombre 2ε soit un carré parfait dans ce corps du 4-ème degré; les calculs montrent qu'on peut prendre pour l'unité ε le nombre

$$\varepsilon = 1 + j + \sqrt{j}(1 + j),$$

et l'on aura

$$2\varepsilon = (1 + j + \sqrt{j})^2 = k^2,$$

où $k = 1 + j + \sqrt{j}$.

Envisageons maintenant la substitution

$$V = \frac{k}{\bar{k}} \cdot \frac{z+1}{-z+1} \tag{9}$$

transformant le point i en $ki : k$, où $\bar{k} = 1 + j - \sqrt{j}$; le déterminant $2k\bar{k}$ de cette substitution est, d'après les calculs précédents, égal à 4.

Cette substitution possède les propriétés suivantes:

1) elle n'entre pas dans le groupe Γ, car son déterminant est égal à 4,

2) elle transforme le groupe Γ en lui-même, ce qu'on vérifie directement en calculant les substitutions $V^{-1}\Gamma V$,

3) elle est une substitution elliptique à la période 5 parce que l'équation donnant la période m de cette substitution est

$$k + \bar{k} = 4\cos\frac{\pi}{m},$$

ce qu'on peut écrire

$$1 + j = 2 \cos \frac{\pi}{m},$$

d'où résulte $m = 5$.

4) ses points fixes z_1 et z_2 sont situés sur le cercle $x^2 + y^2 + 2x = 1$, parce que les valeurs de ces points sont

$$z_1, z_2 = \frac{-\sqrt{j} \pm i\sqrt{2-j}}{1+j-\sqrt{j}}$$

et l'on vérifie cette propriété immédiatement.

D'après ces remarques nous voyons facilement quel effet produit l'application de la substitution V au point fixe i; ce point va du cercle passant par les points fixes z_1 et z_2 sur le cercle passant par ces mêmes points et le coupant sous l'angle $2\pi : 5$; puis il va de ce cercle sur le suivant incliné sous l'angle $2\pi : 5$ etc. En effectuant les constructions nous obtenons un pentagone circulaire dont le centre sera situé sur le cercle

$$x^2 + y^2 + 2x = 1$$

et représentera le nombre

$$\frac{-\sqrt{j} + i\sqrt{2-j}}{1+j-\sqrt{j}}$$

point fixe de la substitution V.

Le pentagone obtenu sera le champ fondamental du groupe Γ.

En effet, ce pentagone se transforme en lui-même à l'aide de substitutions

$$V, V^2, V^3, V^4,$$

mais le déterminant de toutes ces substitutions est égal à 4, elles n'appartiennent donc pas au groupe Γ; ce pentagone se transforme encore en lui-même par l'inversion dans chacune de ses 5 diagonales, mais toutes ces inversions n'appartiennent pas au groupe Γ.

Le pentagone obtenu avec sa réflexion dans l'axe d'ordonnées sera le champ fondamental du groupe Γ.

Pour démontrer maintenant le théorème énoncé nous raisonnerons de la manière suivante. Comme la substitution

$$V = \frac{k}{k} \cdot \frac{z+1}{-z+1}$$

transforme le groupe Γ en lui-même, nous adjoignons au groupe Γ les substitutions V, V^2, V^3, V^4; l'ensemble de substitutions

$$\Gamma,\ \Gamma V^k, \qquad k = 0, 1, 2, 3, 4$$

constituera alors un groupe nouveau que nous désignerons par $\Gamma_{(5)}$; le champ fondamental de ce groupe sera la cinquième partie du champ fondamental du groupe Γ avec le sommet au centre du pentagone. Le pentagone fondamental se transformant en lui-même par l'inversion dans chacune de ses diagonales, nous choisirons une telle inversion, p. e.

$$z' = \frac{-z+1}{\bar{z}+1}$$

et nous l'adjoindrons au groupe $\Gamma_{(5)}$; nous obtenons un groupe nouveau que nous désignerons par $\Gamma_{(10)}$ et dont le champ fondamental sera la moitié du triangle antérieur.

Nous montrerons que

1) le groupe $\Gamma_{(5)}$ se compose exclusivement de substitutions (a, b, c, d) au déterminant $a^2 + c^2 - j(b^2 + d^2) = 4$,

2) le groupe $\Gamma_{(10)}$ se compose exlusivement de substitutions (a, b, c, d) au déterminant $a^2 + c^2 - j(b^2 + d^2) = 4$ ou 2.

De cette manière il sera démontré que le groupe $\Gamma_{(10)}$ ne diffère pas du groupe $(0, 3; 2, 4, 5)$, parce que ce dernier, par définition, se compose exlusivement des substitutions (a, b, c, d) aux déterminants 4 ou 2; il sera en même temps démontré que l'indice du groupe Γ composé des substitutions (a, b, c, d) au déterminant 1 est par rapport au groupe $(0, 3; 2, 4, 5)$ égal à 10, parce que 10 quadrilatères équivalents constituent le champ fondamental du groupe Γ.

1) En effet, il est d'abord évident que le groupe $\Gamma_{(5)}$ ne contient d'autres substitutions que celles au déterminant 4 (y compris les substitutions au déterminant 1); il reste seulement à montrer que le groupe $\Gamma_{(5)}$ épuise toutes les substitutions au déterminant 4. En effet, s'il y avait des substitutions au déterminant 4 qui n'appartiennent pas au groupe $\Gamma_{(5)}$, il y aurait aussi de nouvelles lignes de symétrie n'appartenant pas au groupe $\Gamma_{(5)}$; soit le cercle

$$(-c + d\sqrt{j})(x^2 + y^2) - 2ax + c + d\sqrt{j} = 0$$

une telle ligne de symétrie; de l'égalité $b = 0$ il résulterait alors

$d \equiv 0 \,(mod\ 2)$ et puis, en vertu de l'égalité $a^2 + c^2 - jd^2 = 4$, il résulterait $a^2 + c^2 \equiv 0 \,(mod\ 2)$; mais nous avons de plus $a \equiv c \,(mod\ 2)$, d'où $a \equiv 0 \,(mod\ 2)$; tous les nombres a, c, d seraient divisibles par 2 et la substitution correspondante entrerait dans le groupe $\Gamma_{(5)}$ parce qu'elle entrerait dans le groupe Γ. Il n'y a donc pas de nouvelles lignes de symétrie; le réseau des polygones correspondant au groupe $\Gamma_{(5)}$ et le réseau correspondant à l'ensemble des substitutions (a, b, c, d) au déterminant 4 sont identiques. Le groupe $\Gamma_{(5)}$ contient donc toutes les substitutions (a, c, b, d) au déterminant 4 satisfaisant aux conditions $a \equiv c$, $b \equiv d \,(mod\ 2)$ et n'en contient aucune autre.

2) Pour démontrer que le groupe $\Gamma_{(5)}$ ne contient d'autres substitutions que celles au déterminant $a^2 + c^2 - j(b^2 + d^2) = 4$ ou 2, il suffira de montrer que s désignant une substitution au déterminant 2, S une substitution au déterminant 4 et U la substitution

$$U = \frac{z + 1}{-z + 1}$$

le produit sU sera une substitution au déterminant 4 et le produit $U^{-1}S$ une substitution au déterminant 2.

En effet, nous calculons

$$sU = \begin{pmatrix} a - c + (b - d)\sqrt{j}, & a + c + (b + d)\sqrt{j} \\ -a - c + (b + d)\sqrt{j}, & a - c - (b - d)\sqrt{j} \end{pmatrix}$$

et vérifions immédiatement que, d'après la relation $a^2 + c^2 - j(b^2 + d^2) = 2$, cette substitution a le déterminant 4.

Nous trouvons de même

$$U^{-1}S = \begin{pmatrix} a + c + (b + d)\sqrt{j}. & -a + c + (-b + d)\sqrt{j} \\ a - c + (-b + d)\sqrt{j}, & a + c - (b + d)\sqrt{j} \end{pmatrix}$$

d'où, en vertu des relations $a \equiv c$, $b \equiv d \,(mod\ 2)$, nous constatons que les coefficients de la substitution $U^{-1}S$ sont divisibles par 2; après la réduction de ce facteur nous obtenons la substitution au déterminant 2.

Le théorème énoncé est démontré.

En nous appuyant sur ce théorème nous pouvons dans le calcul de l'ordre du groupe de Galois nous borner aux substitutions au déterminant $\equiv 1$.

§ 3. Détermination de l'ordre du groupe de Galois de l'équation de transformation.

Nous admettons que le nombre p est premier dans le corps $K(j)$; alors la congruence

$$j^2 + j - 1 \equiv 0 \ (mod\ p)$$

n'a pas de racine réelle.

Cela posé, nous déterminons le nombre des solutions de la congruence

$$a^2 + c^2 - j\,(b^2 + d^2) \equiv 1 \ (mod\ p)$$

dans le corps $K(j)$.

Observons d'abord qu'il y a $\frac{1}{2}(p^2 - 1)$ restes quadratiques parmi les $p^2 - 1$ nombres entiers $(mod\ p)$ différents de zéro du corps $K(j)$; ces restes sont des nombres qui peuvent se représenter comme les carrés d'un autre nombre du corps $K(j)$.

Pour représenter ces restes, désignons par g une racine primitive[1]) du nombre p dans le corps $K(j)$, c'est à dire un nombre g satisfaisant à la congruence

$$g^{p^2-1} \equiv 1 \ (mod\ p),$$

alors la suite de $p^2 - 1$ nombres

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

représentera le système des nombres du corps $K(j)$ incongrus par rapport au module p.

Les puissances paires

$$1, g^2, g^4, \ldots g^{p^2-3} \tag{10}$$

seront les restes quadratiques.

Observons aussi la congruence

$$g^{\frac{p^2-1}{2}} \equiv -1 \ (mod\ p). \tag{11}$$

Après ces préliminaires nous avons le théorème:

Théorème V: La congruence

$$x^2 + y^2 \equiv 0 \ (mod\ p)$$

dans le corps $K(j)$ a $2p^2 - 1$ solutions distinctes.

[1]) Serret: Cours d'algèbre supérieure, t. II. p. 175.

En effet, nous pouvons réunir les $\frac{1}{2}(p^2-1)$ restes quadratiques (10) en $\frac{1}{4}(p^2-1)$ paires suivantes

$$\begin{array}{ll} 1, & g^{\frac{p^2-1}{2}} \\ g^2, & g^{\frac{p^2-1}{2}+2} \\ \cdots & \cdots \\ g^{\frac{p^2-1}{2}-2}, & g^{\frac{p^2-1}{2}-2-2}; \end{array}$$

les sommes de chaque paire, en vertu de la congruence (11), sont $\equiv 0 \,(mod\, p)$. Chaque paire nous donnera 8 valeurs pour x et y vérifiant la congruence $x^2+y^2 \equiv 0 \,(mod\, p)$; en définitive, nous avons (y compris 0)

$$\frac{p^2-1}{4}\,8+1=2p^2-1.$$

solutions.

Théorème VI: Si l'on désigne par $\alpha+\beta j$ l'un des p^2-1 nombres entiers différents de zéro du corps $K(j)$, la congruence

$$x^2+y^2 \equiv \alpha+\beta j \,(mod\, p)$$

a dans le corps $K(j)$ précisément p^2-1 solutions distinctes.

En effet, réunissons les restes (10), y compris 0, en $(p^2-1)^2$ paires; nous obtenons des sommes de la forme

$$g^{2r}+g^{2s} \equiv g^{2r}\{1+g^{2(s-r)}\},$$

où $s,r=0,1,2,\ldots\frac{1}{2}(p^2-3)$. Pour chaque valeur donnée arbitrairement de r nous recevrons une moitié des nombres $\alpha+\beta j$; mais il est facile de voir que pour chaque valeur $r+\frac{1}{4}(p^2-1)$ nous recevrons une autre moitié des nombres $\alpha+\beta j$, car autrement il résulterait $g^{\frac{p^2-1}{2}} \equiv 1 \,(mod\, p)$. Chaque nombre $\alpha+\beta j$ sera donc $\frac{1}{4}(p^2-1)$ fois représenté $(mod\, p)$ dans la forme x^2+y^2, ce qui donne p^2-1 solutions distinctes.

Après la démonstration de ces théorèmes, revenons à la détermination du nombre des solutions de la congruence

$$(12) \qquad a^2+c^2-j(b^2+d^2) \equiv 1 \,(mod\, p).$$

Examinons d'abord les valeurs $a \equiv 0$ et $a \equiv 1$; ensuite les autres.

Si $a \equiv 0$ et $c \equiv 0$ nous obtenons la congruence

$$-j(b^2 + d^2) \equiv 1 \pmod{p}$$

qui, en vertu de l'égalité $1 = j(1 + j)$, pourra s'écrire $b^2 + d^2 \equiv -1 - j \pmod{p}$; cette congruence a $\frac{1}{2}(p^2 - 1)$ solutions (théorème VI) parce que les valeurs b et d qui diffèrent par le signe ne donneront pas des substitutions différentes (a, b, c, d); pour les valeurs $a \equiv 0$, $c \equiv 1$ nous obtenons $2p^2 - 1$ solutions (théorème V); chacune des $\frac{1}{2}(p^2 - 1)$ valeurs restantes pour c donnera $p^2 - 1$ solutions; dans le cas $a \equiv 0$ nous obtenons en définitive

$$\frac{p^2 - 1}{2} + 2p^2 - 1 + \frac{p^2 - 3}{2}(p^2 - 1) = \frac{p^2 + 1}{2} p^2$$

solutions.

Pour les valeurs $a \equiv 1$, $c \equiv 0$ nous obtenons $2p^2 - 1$ solutions; chacune des $p^2 - 1$ valeurs restantes pour c donnera $p^2 - 1$ solutions; en somme nous aurons dans le cas $a \equiv 1$

$$2p^2 - 1 + (p^2 - 1)^2 = p^4$$

solutions.

Si nous passons maintenant aux valeurs restantes pour a, nous remarquons qu'il y en a parmi elles certaines qui vérifient la congruence $a^2 + c^2 \equiv 1$ et d'autres qui ne la vérifient pas. Mais, comme cette congruence a $p^2 - 1$ solutions (théorème VI) il y aura $\frac{1}{2}(p^2 - 1) - 2$ valeurs du premier genre, car les valeurs $a \equiv 0$, $a \equiv 1$ étaient déjà envisagées. Pour chacune de ces valeurs il existera deux valeurs c telles que $a^2 + c^2 \equiv 1$, donc chaque fois deux valeurs parmi p^2 valeurs pour c donneront la congruence $b^2 + d^2 \equiv 0$, c'est à dire, d'après le théorème V, $p^2 - 1$ solutions; chacune de $p^2 - 2$ valeurs restantes pour c donnera seulement $p^2 - 1$ solutions. Nous aurons ainsi dans les cas mentionnés

$$\frac{p^2 - 5}{4}\{2(2p^2 - 1) + (p^2 - 2)(p^2 - 1)\} = \frac{p^2 - 5}{4} p^2(p^2 + 1)$$

solutions.

Chacune de $\frac{1}{2}(p^2 - 1)$ valeurs pour a qui ne sont pas racines de la congruence $a^2 + c^2 \equiv 1$ nous donnera $p^2(p^2 - 1)$ solutions; toutes ces valeurs donneront $\frac{1}{2}p^2(p^2 - 1)^2$ solutions.

Nous aurons en définitive la somme

$$p^2\frac{p^2+1}{2}+p^4+\frac{p^2-5}{4}p^2(p^2+1)+\tfrac{1}{4}p^2(p^2-1)^2=\tfrac{1}{2}p^2(p^4-1)$$

exprimant le nombre des solutions de la congruence (12).

Nous pouvons énoncer le théorème:

Théorème VII: Si l'on effectue la transformation T du p-ème degré sur la fonction automorphe $\varphi(z)$ appartenant au groupe $(0, 3; 2, 4, 5)$ le groupe de Galois de l'équation algébrique à laquelle satisfait la fonction transformée $\varphi(Tz)$ est isomorphe avec un groupe d'ordre $\frac{1}{2}p^2(p^4-1)$.

§ 4. Détermination du degré de l'équation de transformation.

Désignons le groupe dont nous avons déterminé le degré par G; notre but principal est de montrer que ce grroupe G contient un sous groupe d'ordre $\frac{1}{2}p^2(p^2-1)$.

Observons en premier lieu le groupe cyclique

$$G_p=(1, 1, 0, E+Hj)^k, \quad k=0, 1, 2, \ldots p-1$$

composé des puissances différentes de la substitution

$$S=(1, 1, 0, E+Hj)$$

ayant la propriété

$$S^p \equiv 1 \ (mod\ p);$$

on vérifie aisément cette propriété en observant que généralement chaque substitution U de la forme $U=(1, b, c, d)$ ayant son premier terme 1, a la période p; on a, en effet les formules

$$\begin{aligned} A &= a\alpha+jb\beta-c\gamma+jd\delta, \\ B &= a\beta+b\alpha+c\delta-\gamma d, \\ C &= a\gamma+jb\delta+c\alpha-jd\beta, \\ D &= a\delta+d\alpha+b\gamma-c\beta \end{aligned} \tag{13}$$

donnant les coefficients A, B, C, D du produit

$$(A, B, C, D)=(a, b, c, d)(\alpha, \beta, \gamma, \delta);$$

ces formules donnent

$$U^2 \equiv (1, 2b, 2c, 2d),$$
$$U^3 \equiv (1, 3b, 3c, 3d),$$
$$\ldots\ldots\ldots\ldots$$
$$U^p \equiv (1, pb, pc, pd) \equiv (1, 0, 0, 0) \equiv 1.$$

Nous démontrons le théorème:

Théorème VIII: L'ensemble de p^2 substitutions de la forme

$$(1, b, 0, (E + Hj)\, b)$$

où b parcourt le système complet des nombres entiers du corps $K(j)$ incongrus par rapport au module p, constitue un groupe G_{p^2} pour lequel le groupe G_p est un diviseur normal.

Déterminons dans ce but toutes les substitutions du groupe G qui transforment le groupe cyclique G_p en lui-même.

Nous aurons la condition

$$(-a, b, c, d)\,(1, 1, 0, E + Hj)\,(a, b, c, d) \equiv (1, 1, 0, E + Hj)$$

parce qu'il est facile de voir que la substitution $(-a, b, c, d)$ est l'inverse de (a, b, c, d).

Si l'on désigne la première partie de cette congruence par (a', b', c', d') on obtient, ayant égard à la congruence

$$a^2 + c^2 - j(b^2 + d^2) \equiv 1 \pmod p, \tag{14}$$

les relations

$$a' \equiv -1,$$
$$b' \equiv -2a^2 + 2jb^2 + 1 + 2(E + Hj)(ca + bdj),$$
$$c' \equiv -2adj + 2j(E + Hj)(dc + ab),$$
$$d' \equiv -2ac + 2jbd + (E + Hj)(1 + 2d^2j - 2a^2),$$

nous aurons donc (après la réduction de 2) les congruences suivantes

$$\begin{aligned} &c^2 - jd^2 + (E + Hj)(ca + bdj) \equiv 0, \\ &ad - (E + Hj)(ab + dc) \equiv 0, \\ &jbd - ac + (E + Hj)(c^2 - b^2j) \equiv 0. \end{aligned} \tag{15}$$

Multipliant la première par b et la troisième par d et les additionnant nous obtenons la relation

$$bc^2 + c[(E + Hj)(ab + dc) - ad] \equiv 0 \pmod p$$

qui, en vertu de la deuxième congruence (15), s'écrira

$$bc^2 \equiv 0 \ (mod\ p);$$

il résulte de là: 1) $b \equiv 0$, ou 2) $c \equiv 0 \ (mod\ p)$.

La condition $b \equiv 0$ est impossible parce que la troisième congruence (15) se changerait alors en

$$c[-a + c(E + Hj)] \equiv 0 \ (mod\ p)$$

et donnerait $a \equiv c(E + Hj)$; la deuxième donnerait alors $-jd^2 \equiv 0$ ou $d \equiv 0$; mais les valeurs

$$b \equiv 0, \ a \equiv c(E + Hj), \ d \equiv 0$$

ne vérifieraient pas la congruence (14).

Reste la condition $c \equiv 0$; alors la troisième congruence (15) se change en

$$jb[d - b(E + Hj)] \equiv 0 \ (mod\ p)$$

ce qui donne

$$d \equiv b(E + Hj) \ (mod\ p).$$

Les congruences (15) se vérifient immédiatement; la relation (14) donne pour a la valeur $\equiv \pm 1$.

Les substitutions (a, b, c, d) transformant le groupe G en lui-même seront donc de la forme

$$(1, b, 0, (E + Hj)b);$$

le nombre b pourra prendre toutes les valeurs entières du corps $K(j)$ incongrues par rapport au module p. Le théorème énoncé est démontré.

Il est facile de montrer l'existence d'au moins $p^2 + 1$ groupes du type G_{p^2}. En effet, le nombre de substitutions (a, b, c, d) avec le premier terme $a \equiv 1$ (la substitution $(1, 0, 0, 0)$ exclue) est, d'après le théorème V, égal à $p^4 - 1$. Si l'on transforme le groupe G_{p^2} à l'aide d'une substitution arbitraire V prise parmi ces $p^4 - 1$ substitutions ayant la période p, on obtiendra un nouveau groupe d'ordre p^2 qui de même sera composé de substitutions à période p. Chaque substitution ayant la période p n'entrera qu'une seule fois dans un groupe déterminé du type G_{p^2}. En effet, si l'on désigne par U_1 et U_2 deux substitutions quelconques du groupe G_{p^2} dont la première U_1 pourrait entrer dans un nou-

veau groupe obtenu de G_{p^2} par la transformation à l'aide d'une substitution S, il serait

$$U_1 \equiv S^{-1} U_2 S,$$

d'où résulterait $SU_1 \equiv U_2 S$, ce qui est impossible. Si donc chaque substitution à période p dont le nombre est $p^4 - 1$ n'entre qu'une seule fois dans un certain groupe déterminé d'ordre p^3 contenant $p^2 - 1$ substitutions différentes de l'unité. le nombre de groupes obtenus sera $(p^4 - 1)\colon (p^2 - 1) = p^2 + 1$.

Après ces remarques montrons que le groupe trouvé G_{p^2} est un diviseur normal avec l'indice $\frac{1}{2}(p^2 - 1)$ d'un certain groupe d'ordre $\frac{1}{2}p^2(p^2 - 1)$.

Nous pouvons énoncer le théorème suivant:

Théorème IX: L'ensemble de $\frac{1}{2}p^2(p^2 - 1)$ substitutions de la forme

$$(a, b, c, (E + Hj)b) \tag{17}$$

dans lesquelles b parcourt le système complet des nombres entiers du corps $K(j)$ incongrus par rapport au module p et les nombres a et c vérifient la congruence

$$a^2 + c^2 \equiv 1 \,(mod\, p),$$

constitue un groupe pour lequel le groupe G_{p^2} est un diviseur normal.

Pour la démonstration adjoignons aux p^3 substitutions du groupe G_{p^2} toutes les substitutions de la forme

$$(a, b, c, (E + Hj)b).$$

Nous aurons $\frac{1}{2}(p^2 - 1)$ systèmes de p^3 substitutions pareilles. car nous avons

$$a^2 + c^2 - jb^2[1 + (E + Hj)^2] \equiv 1 \,(mod\, p).$$

d'où, ayant égard à la congruence

$$(E + Hj)^2 + 1 \equiv 0 \,(mod\, p), \tag{18}$$

nous obtenons $a^2 + c^2 \equiv 1 \,(mod\, p)$ pour déterminer a et c; mais, comme, d'après le théorème VI, la congruence $a^2 + c^2 \equiv 1 \,(mod\, p)$ a $p^2 - 1$ solutions distinctes dans le corps $K(j)$, nous obtenons

$\frac{1}{2}(p^2-1)$ paires (a, c) pour a et c; il sera superflu de prendre d'autres systèmes de la forme

$$(-a, b, -c, (E+Hj)\,b)$$

parce que ces substitutions peuvent s'écrire

$$(a, -b, c, -(E+Hj)\,b)$$

et il est évident qu'elles ne donneront pas des substitutions nouvelles.

Il suffira pour démontrer le théorème énoncé d'écrire le produit

$$(a, b, c, (E+Hj)\,b)\,.\,(a_1, b_1, c_1, (E+Hj)\,b_1)$$

de deux substitutions

$$(a, b, c, (E+Hj)\,b) \text{ et } (a_1, b_1, c_1, (E+Hj)\,b_1)$$

vérifiant les relations

$$a^2+c^2 \equiv 1,\ a_1^2+c_1^2 \equiv 1 \ (mod\ p).$$

En désignant ce produit par (A, B, C, D) nous obtenons

$$\begin{aligned} A &\equiv aa_1 - cc_1, \\ B &\equiv ab_1 + ba_1 + (E+Hj)(cb_1 - c_1 b), \\ C &\equiv ac_1 + ca_1, \\ D &\equiv bc_1 - cb_1 + (E+Hj)(ab_1 + ba_1). \end{aligned}$$

Ayant égard à la congruence (18) nous vérifions immédiatement la relation

$$D \equiv (E+Hj)\,B \ (mod\ p) \tag{19}$$

Nous obtenons ensuite

$$\begin{aligned} A^2+C^2 \equiv a^2a_1^2+c^2c_1^2+a^2c_1^2+c^2a_1^2 &\equiv (a^2+c^2)a_1^2+c^2c_1^2+ \\ &+c_1^2(1-c^2) \equiv a_1^2+c_1^2 \equiv 1, \end{aligned}$$

ce qui montre que l'ensemble des substitutions (17) forme effectivement un groupe.

Pour montrer que le groupe G_{p^2} est un diviseur normal du groupe ci-dessus, observons que ce groupe, d'après la définition, ne peut contenir que p^2 sustitutions avec le premier terme $a \equiv 1$; ce

sont toutes les substitutions du groupe G_{p^2}. Si nous transformons maintenant le groupe G_{p^2} à l'aide d'une substitution arbitraire

$$S = (a', b', c', d')$$

nous calculerons facilement (d'après les formules du § 1) que le premier terme de chaque substitution du groupe $S^{-1}G_{p^2}S$ sera

$$a'^2 + c'^2 - j(b'^2 + d'^2) \equiv 1 \pmod{p},$$

nombre congru à 1 par rapport au module p.

Il sera donc

$$S^{-1}G_{p^2}S \equiv G_{p^2}$$

pour chaque S, c. q. f. d.

L'existence du groupe d'ordre $\frac{1}{2}p^2(p^2-1)$ nous permet de démontrer le théorème suivant:

Théorème X: L'ensemble de toutes les substitutions

$$\frac{(a + b\sqrt{j})z + c + d\sqrt{j}}{(-c + d\sqrt{j})z + a - b\sqrt{j}} \tag{20}$$

du groupe $(0, 3; 2, 4, 5)$ vérifiant la congruence

$$d \equiv (E + Hj)b \pmod{p}, \tag{21}$$

où le nombre $E + Hj$ satisfait à la relation

$$(E + Hj)^2 \equiv -1 \pmod{p},$$

forme un sous-groupe du groupe $(0, 3; 2, 4, 5)$ avec l'indice $p^2 + 1$.

Désignons l'indice de ce sous-groupe par la lettre i, désignons par Γ_i le sous-groupe des substitutions (20) vérifiant la condition (21) et ayant le déterminant $\equiv 1 \pmod{p}$; le groupe Γ, envisagé au § 2, composé de substitutions (20) avec déterminant 1 peut être représenté sous la forme

$$\Gamma \equiv (\Gamma_i, S_2\Gamma_i, S_3\Gamma_i, \ldots S_i\Gamma_i),$$

où les lettres S_k désignent certaines substitutions (20) ne vérifiant pas la congruence (21).

Si nous considérons maintenant le groupe fini G auquel se réduit le groupe Γ par rapport au module p, nous remarquerons que par rapport au module p les substitutions du groupe Γ_i se réduiront à celles des substitutions du groupe G qui vérifient la

congruence (21); autrement dit, le groupe Γ_i se réduira à l'ensemble

$$(a, b, c, (E + Hj)\, b)$$

qui, d'après le théorème IX, constitue un groupe d'ordre $\frac{1}{2}p^2(p^2-1)$

L'indice i sera donc égal au quotient $\frac{1}{2}p^2(p^4-1):\frac{1}{2}p^2(p^2-1) = p^2+1$.

Mais, comme nous l'avons déjà observé auparavant, le degré de l'équation algébrique à laquelle satisfait la fonction transformée $\varphi(Tz)$ doit être égal à l'indice du sous-groupe commun du groupe $(0, 3; 2, 4, 5)$ et du groupe transformé $T^{-1}(0, 3; 2, 4, 5)\,T$, nous avons, en nous appuyant sur le théorème III, le résultat suivant:

Théorème XI: Etant donné un nombre naturel p premier dans le corps $K(j)$ satisfaisant à la condition

$$\left(\frac{-5}{p}\right) = 1,$$

si nous effectuons la transformation

$$T(z) = \frac{Pz + Q}{-Qz + P}$$

du p-ème degré sur la fonction automorphe $\varphi(z)$ appartenant au groupe $(0, 3; 2, 4, 5)$ la fonction transformée $\varphi(Tz)$ satisfait à une équation algébrique du degré p^2+1.

§ 5. Application à la transformation du 7-ème degré.

Les nombres p satisfaisant à la seconde condition du théorème XI sont de la forme

$$20k+1, \quad 20k+3, \quad 20k+7, \quad 20k+9;$$

nous avons donc la suite

$$3, 7, 23, 29, 41, 43, 47, 61, \ldots$$

Après le nombre $p = 3$, envisagé par Fricke, nous avons le nombre [1]) $p = 7$ qui est premier dans le corps $K(j)$; appliquons nos résultats généraux à ce cas.

[1]) Le cas du nombre 5 qui n'est pas premier dans le corps $K(j)$ a fait l'objet du mémoire déjà cité de Fricke dans les Acta Mathematica, 17; il conduit au groupe d'icosaèdre.

Nous voyons d'abord que le nombre de substitutions de la forme

$$z' = \frac{Pz + Q}{-Qz + P}$$

au déterminant $P^2 + Q^2 = p$ ne surpasse pas le nombre $8(p+1)$. En effet, si nous posons

$$P = \alpha + \beta j, \quad Q = \gamma + \delta j,$$

où les nombres $\alpha, \beta, \gamma, \delta$ sont des entiers rationnels, nous voyons facilement que ces nombres doivent satisfaire à l'égalité

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = p,$$

mais, comme on sait, le nombre premier p peut être [1]) de $8(p+1)$ manières décomposé en somme de 4 carrés.

Dans le cas de $p = 7$ nous obtenons

$$2^2 + 1^2 + 1^2 + 1^2 = 7,$$

d'où, ayant égard à la condition

$$2(\alpha\beta + \gamma\delta) = \beta^2 + \delta^2$$

que les nombres $\alpha, \beta, \gamma, \delta$ doivent vérifier, nous n'obtenons que les quatre systèmes suivants des valeurs pour les nombres $\alpha, \beta, \gamma, \delta$:

$$\begin{array}{cccc} 2, & 1, & -1, & 1 \\ 1, & -1, & 2, & 1 \\ 2, & 1, & 1, & -1 \\ -1, & 1, & 2, & 1 \end{array}$$

Nous voyons que, pour la transformation du 7-ème degré de la fonction automorphe $\varphi(z)$ ne peuvent être employés que les quatre substitutions suivantes

$$T_1 = \begin{pmatrix} 2+j, & -1+j \\ 1-j, & 2+j \end{pmatrix}, \quad T_2 = \begin{pmatrix} 1-j, & 2+j \\ -2-j, & 1-j \end{pmatrix}$$

$$T_3 = \begin{pmatrix} 2+j, & 1-j \\ 1+j, & 2+j \end{pmatrix}, \quad T_4 = \begin{pmatrix} 1-j, & -2-j \\ 2+j, & 1-j \end{pmatrix}$$

au déterminant 7.

Il est facile de voir que dans le cas considéré, le nombre $E + Hj$ sera $5 + 3j$ parce qu'on vérifie immédiatement la congruence $(5+3j)^2 + 1 \equiv 0 \pmod 7$.

[1]) Sierpiński: Teorja liczb, 1914, p. 357.

Nous vérifions ensuite que dans le cas des transformations T_1 et T_2 le sous-groupe commun du groupe $(0, 3; 2, 4, 5)$ et du groupe transformé, sera défini par la congruence

$$d \equiv (5 + 3j)\, b \,(mod\, d),$$

dans le cas des substitutions T_3 et T_4 les sous-groupes correspondants seront

$$d \equiv (2 + 4j)\, b \,(mod\, 7).$$

Les substitutions $(1, b, 0, (5 + 3j)b)$, transformant la substitution $(1, 1, 0, 5 + 3j)$ en lui-même, constituent un groupe G_{49} d'ordre 49. Ce groupe est un diviseur normal d'un certain G_{1176} d'ordre 1176. Les fonctions transformées $\varphi(T_1 z)$, $\varphi(T_2 z)$, $\varphi(T_3 z)$, $\varphi(T_4 z)$ seront racines des équations algébriques du degré 50.

Nous pouvons encore remarquer un fait intéressant qui rapproche le cas de transformation du 7 ème degré de la fonction automorphe $\varphi(z)$ avec celui de transformation du 7 ème degré des fonctions modulaires; nous démontrerons le théorème suivant:

Théorème XII: Dans le cas de transformation du 7-ème degré de la fonction automorphe appartenant au groupe $(0, 3; 2, 4, 5)$ le groupe de Galois de l'équation de transformation contient un sous-groupe G_{168} d'ordre 168.

Pour démontrer ce théorème remarquons qu'on a pour chaque substitution

$$S = (a, b, c, d)$$

les formules suivantes $(mod\ 7)$:

$$S^2 \equiv (5a^2 + 1,\ 5ab,\ 5ac,\ 5ad)$$
$$S^3 \equiv (3a^3 + 3a,\ 3a^2 b + b,\ 3a^2 c + c,\ 3a^2 d + d),$$

qui permettent de déterminer les périodes des diverses substitutions du groupe de Galois. Nous savons déjà que pour $a \equiv 1$, la substitution S a la période 7; nous calculons aisément qu'on a pour $a \equiv 0$ la période 2 et pour $a \equiv 3$ la période 3; pour $a \equiv 2$ on a la période 4 et pour $a \equiv 5 + 3j$ la période 6; les valeurs $a \equiv 3j$, $3 + 3j$ donnent la période 5, les valeurs $a \equiv 4 + j$, $1 + 2j$ la période 8, les valeurs $a \equiv 3 + j$, $5 + j$ la période 12, les valeurs $a \equiv 2 + j$, $6 + j$, $1 + 3j$, $2 + 3j$ la période 24 et les valeurs $a \equiv j$, $4 + 2j$, $5 + 2j$, $2j$, $6 + 2j$, $4 + 3j$, $1 + j$, $2 + 2j$, $6 + 3j$, $3 + 2j$ la période 25.

Après ces remarques, prenons la substitution

$$V = (0, b, 1, (5 + 3j)\, b)$$

et déterminons une substitution

$$U = (1, \beta, \gamma, \delta), \quad \gamma^2 - j(\beta^2 + \delta^2) \equiv 0 \pmod 7$$

à période 7, telle que le produit UV ait la période 3.

Observons auparavant qu'on ne peut pas avoir $\gamma = 0$ parce que la substitution U aurait alors la forme $(1, \beta, 0, (5 + 3j)\, \beta)$ et le produit UV n'aurait pas la période 3. En effet, si l'on calcule pour le produit

$$(1, \beta, 0, (5 + 3j)\, \beta) \,.\, (0, b, 1, (5 + 3j)\, b)$$

le premier terme A, on trouve

$$A \equiv j\beta b\,[1 + (5 + 3j)^2] \equiv 0 \pmod 7,$$

ce qui donne la substitution avec période 2.

Prenons donc le produit

$$(1, \beta, \gamma, \delta) \,.\, (0, b, 1, (5 + 3j)\, b);$$

son premier terme A doit vérifier la condition $a \equiv 3$; nous aurons donc

$$A \equiv -\gamma + bj\,[\beta + \delta(5 + 3j)] \equiv 3 \pmod 7.$$

En posant $\gamma \equiv 1$ nous obtenons la congruence

$$bj\,[\beta + \delta(5 + 3j)] \equiv 4 \pmod 7,$$

ou

$$b[(5 + 2j)]\,\delta + j\beta] \equiv 4 \pmod 7 \tag{22}$$

et la condition $j(\beta^2 + \delta^2) \equiv 1$ pour β et δ.

En vertu de l'égalité $1 = j(1 + j)$ la dernière congruence s'écrira

$$\beta^2 + \delta^2 \equiv 1 + j \pmod 7.$$

et nous trouvons les solutions suivantes de cette congruence

$$(1 + j,\ 5 + 3j), \quad (5 + j,\ 6 + 3j), \quad (4 + 3j,\ 2),$$
$$(2 + j,\ 3 + j), \quad (2 + 3j,\ 3j), \quad (3 + 2j,\ 3).$$

Nous vérifions aisément que seulement la solution $(3 + 3j, 3)$ satisfaira à la congruence (22); nous aurons

$$j\beta + \delta(3 + 2j) \equiv j(3 + 2j) + 3(3 + 2j) \equiv 4 \pmod 7.$$

La substitution cherchée U aura donc la forme

$$U = (1,\ 3 + 2j,\ 1,\ 3).$$

La substitution U et la substitution V satisferont aux congruences suivantes

$$U^7 \equiv 1, \quad V^2 \equiv 1, \quad (UV)^3 \equiv 1 \ (mod\ 7). \tag{23}$$

En s'appuyant sur les recherches de Dyck [1]) nous constatons que les substitutions U et V vérifiant les relations (23) conduisent à un groupe G_{168} d'ordre 168; l'existence d'un tel groupe est donc démontrée.

[1]) Gruppentheoretische Studien, Mathem. Annalen, Bd. 20, p. 1.