154. *Fricke Formula for Quaternian Groups*

By Noburo ISHII

(Comm. by Kenjiro SHODA, M. J. A., Nov. 12, 1974)

For a square free positive integer N, let $\Gamma_0(N)$ be the congruence subgroup of level N, i.e.

$$\Gamma_0(N)=\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in SL_2(\boldsymbol{Z})\,;\, C\equiv 0 \text{ mod. } N\right\} \quad \text{and} \quad \Gamma_0^*(N)$$

be the group generated by $\Gamma_0(N)$ and the element $x=\begin{pmatrix} 0 & -1 \\ N & 0\end{pmatrix}$. Fricke (Die Elliptischen Funktionen und ihre Anwendungen II pp. 357–367) has given a following relation between the genus g of the Riemann surface obtained from $\Gamma_0(N)$ and the genus g^* of that of $\Gamma_0^*(N)$ for $N>4$:

$$2g^*-g=1-\frac{1}{2}\delta_N h(-4N)$$

where $h(-4N)$ is the class number of the order of $\boldsymbol{Q}(\sqrt{-N})$ with discriminant $-4N$ and $\delta_N=2, 4/3, 1$ for $N\equiv 7$, $N\equiv 3$, otherwise, mod. 8, respectively. In this note, we shall give a similar formula for some arithmetic Fuchsian group $\bar{\Gamma}$ obtained from an indefinite quaternion algebra and a certain normalizer $\bar{\Gamma}^*$ of $\bar{\Gamma}$ with $[\bar{\Gamma}^*:\bar{\Gamma}]=2$. To be more precise, let B be a quaternion algebra over a totally real algebraic number field k and let R be an order of square free stufe (cf. [1]). Let v be a finite place of k where the completion R_v is not isomorphic to the total matrix ring with integral coefficients. If the class number of R is one, for such v, there exists an element π_v of B such that π_v is a prime element of R_v and is a unit at any other places. Now we take $\Gamma=$the group of totally positive units in R, and $\Gamma^*=$the group generated by Γ and π_v (or product of such π_v's). Let $\bar{\Gamma}$ (resp. $\bar{\Gamma}^*$) denotes the Fuchsian group corresponding to Γ (resp. Γ^*). Then, denoting by g (resp. g^*) the genus of $\bar{\Gamma}$ (resp. $\bar{\Gamma}^*$), we have the formula (Corollary to Theorem 3.0) of the form;

$2g^*-g=$(*sum of class numbers of certain totally imaginary quadratic extensions of* k).

Our proof depends on the well known *Hurwitz formula* which has the following form under our assumption that $[\bar{\Gamma}^*:\bar{\Gamma}]=2$:

$2g-2=2(2g^*-2)+$(*the number of ramified fixed points of* Γ)

(see, for example, G. Shimura: Introduction to the arithmetic theory of automorphic functions. Iwanami Shoten, 1971, p. 19). Thus our problem amounts to determine the conjugate classes of elliptic points of Γ^* which will be carried out in § 2.

It was suggested by several people that an application of the trace formula of Hecke operators also yields our results. In fact, using the formula of H. Hijikata [2], M. Yamauchi [6] has given a generalization of Fricke formula for $\Gamma_0(N)$ without assuming N to be square free.

Finally, the author wishes to express his hearty gratitude to Professor K. Doi who suggested the problem to him and Dr. H. Saito who read the first draft of this note and gave valuable suggestions.

1.0. Let k be a totally real algebraic number field, and $r(k)$ be the ring of integers of k. For any place v of k, let $k(v)$ denote the completion of k with respect to v. For non-archimedian place v, let $r(v)$ and $p(v)$ denote the ring of integers of $k(v)$ and its maximal ideal. Let p_v be the prime ideal of k corresponding to v. Let m be the degree of k over rational number field $\boldsymbol{Q}$, then k has m archimedian places $v(1),\cdots,v(m)$. Let B be an indefinite quaternion algebra containing k as its center, and n be the number of archimedian places of k where $B\otimes k(v)$ is split. $\{v(1),\cdots,v(n)\}$ will be assumed to be all such archimedian places. Let S be the set of all non-archimedian places of k, where $B\otimes k(v)$ is ramified. The sum $m-n$ and $\sharp(S)$ must be even. ($\sharp(S)$ denote the cardinality of S.) Let S' be the finite set of non-archimedian places, not belonging to S. Let R denote *the order of square free of type SS'*, i.e. (i) R is a subring and is a finitely generated $r(k)$-module in B such that $R\otimes k=B$. (ii) for $v\in S'$, $R_v=R\otimes r(v)$ is isomorphic to $\begin{pmatrix} r(v) & r(v) \\ p(v) & r(v)\end{pmatrix}$. For every non-archimedian places $v\notin S'$, R_v is maximal in $B_v=B\otimes k(v)$. Let N (resp. Tr) be the reduced norm of B (resp. the reduced trace of B). We say that $a\in B$ is *totally positive*, if $N(a)$ is totally positive. For any subring L of B, let $L^\times$ denote the unit group of L. B^+ (resp. k^+) denotes the subgroup generated by all totally positive elements of B (resp. k).

1.1. Put $\Gamma=R^\times\cap B^+$ and $\bar{\Gamma}$ denotes the canonical image of Γ in B^+/k. In a usual manner, $\bar{\Gamma}$ can be considered as a discrete subgroup of the analytic automorphic group of the direct product H^n of n-copies of complex upper half planes. We shall assume the following two conditions for k:

(1)
- (i) All ideals of k are principal.
- (ii) $r(k)^\times$ contains an element of any preassigned signature distribution, i.e. for any $I\subset\{1,\cdots,m\}$, there exists $\varepsilon\in r(k)^\times$ such that $\varepsilon^{(i)}>0$ for $i\in I$ and $\varepsilon^{(i)}<0$ for $i\notin I$ (where $\varepsilon^{(i)}$ denotes the i-th conjugate of ε).

By (1), the class number of R is one and every right R-ideal is generated by a totally positive element of B ([5] p. 174 Lemmas 2.3, 2.4).

For any $v \in S \cup S'$, take π_v of B^+ such that $\pi_v R = R\pi_v$ and $p_v R = (\pi_v R)^2$.

For any subset T of $S \cup S'$, put $X_T = \prod_{v \in T} \pi_v$, $x_T = N(X_T)$. Then $X = X_T$ is a normalizer of R, i.e. $XRX^{-1} = R$. Put Γ^* be the group generated by Γ and ΓX. $\bar{\Gamma}^*$ denotes the canonical image of Γ^* in B^+/k. Then $\bar{\Gamma}$ is a normal subgroup of index 2 of $\bar{\Gamma}^*$.

2.0. We say that $z \in H^n$ is *an elliptic point of* Γ^* *of type* A (resp. *type* B), if (identity transformation on H^n) $\neq \bar{\Gamma}_z^* = \{\gamma \in \bar{\Gamma}^* \mid \gamma(z) = z\} \subset \bar{\Gamma}$ (resp. $\bar{\Gamma}_z^* \bar{\Gamma} = \bar{\Gamma}^*$). Put $C(z) = \{\gamma(z) \mid \gamma \in \bar{\Gamma}\}$ and $\Theta = \{\gamma \in \bar{\Gamma}^* \mid \gamma \notin \bar{\Gamma}\}$, then we can easily establish the following:

(2)
- (i) If $z \in H^n$ is an elliptic point of Γ, then for any $\gamma \in \Theta$, $\gamma(z)$ is so.
- (ii) For $z, z', \in H^n, \gamma, \gamma' \in \Theta$, if $C(z) = C(z')$, then $C(\gamma z) = C(\gamma' z')$.
- (iii) For $z \in H^n$, z is an elliptic point of Γ^* of type B, if and only if there exists $\gamma \in \Theta$ such that $C(\gamma z) = C(z)$.

By (2), the number of Γ^*-equivalent classes of elliptic points of type A equals the half of the number of Γ-equivalent classes of elliptic points of type A. The number of Γ^*-equivalent classes of elliptic points of type B equals the number of Γ-equivalent classes of elliptic points of type B. Let Ω be a set of all subrings $\mathfrak{o}$ of B with the following properties.

1: $K = k(\mathfrak{o})$ is a totally imaginary maximal subfield of B.

2: $\mathfrak{o} = K \cap R$.

3: $\Gamma^*(\mathfrak{o}) = \Gamma^* \cap \mathfrak{o} \neq r(k)^\times$.

Each $\mathfrak{o} \in \Omega$ corresponds to an elliptic point of Γ^* uniquely and vice versa. Let Ω_A (resp. Ω_B) be a subset of all orders corresponding to all elliptic points of type A (resp. type B). We say that $\mathfrak{o}$, $\mathfrak{o}'$ are *Γ-equivalent,* if there exists $\varepsilon \in \Gamma$ such that $\varepsilon \mathfrak{o} \varepsilon^{-1} = \mathfrak{o}'$. We can see easily that each Γ-equivalent class of $\mathfrak{o}$ corresponds to the Γ-equivalent class of an elliptic point of Γ^* and vice versa.

2.1. Lemma. *Let* $\mathfrak{o} \in \Omega$, *then* $\mathfrak{o} \in \Omega_B$ *if and only if there exists an element* X *of* $\mathfrak{o}$ *such that* $N(X) = x_T = x$ *and* $\mathrm{Tr}\,(X)$ *is a multiple of* x.

Proof. 'only if' part is trivial. We shall prove 'if part'. We claim that XR is a two sided R-ideal. If $v \in S$, R_v is an unique maximal order of B_v, hence $XR_vX^{-1} = R_v$, i.e. $XR_v = R_vX$. If $v \in S' \cap T$, we can assume that $R_v = \begin{pmatrix} r(v) & r(v) \\ p(v) & r(v) \end{pmatrix}$, $X = \begin{pmatrix} a & b \\ c\pi & d \end{pmatrix}$, where $a, b, c, d \in r(v)$ and π is a prime element of $k(v)$. $N(X) = a \cdot d - b \cdot c \cdot \pi = \pi\varepsilon$, $\varepsilon \in r(v)^\times$, $\mathrm{Tr}\,(X) = a + d \in p(v)$, so that both a and b must be divided by π. Since $X\begin{pmatrix} 0 & \pi \\ 1 & 0 \end{pmatrix}^{-1}, \begin{pmatrix} 0 & \pi \\ 1 & 0 \end{pmatrix}^{-1} X \in R_v^\times$ and $\begin{pmatrix} 0 & \pi \\ 1 & 0 \end{pmatrix} R_v = R_v \begin{pmatrix} 0 & \pi \\ 1 & 0 \end{pmatrix}$, $XR_v = R_vX$. For any other non-archimedian place v of k, $X \in R_v^\times$ and $XR_v = R_vX$. Thus we have shown $XR = RX$. As is well known, all maximal integral two sided ideals of R with norm $p_v (v \in S \cup S')$ form a basis of the free abelian group generated by all two sided ideals of R.

So that $X=(\prod_{v\in T}\pi_v)\varepsilon$, $(\varepsilon\in\Gamma)$. Hence $\mathfrak{o}\in\Omega_B$. q.e.d.

We can see easily that:

(3) *the number of the elements of* $\mathfrak{o}$ *whose norm are* x *and trace are multiples of* x *equals* $[\Gamma(\mathfrak{o}):r(k)^\times]$, *where* $\Gamma(\mathfrak{o})=\Gamma\cap\mathfrak{o}$.

2.2. Lemma. *For* $\mathfrak{o}\in\Omega_B$.

i) *The conductor* $\mathfrak{f}(\mathfrak{o})$ *of* $\mathfrak{o}$ *is prime to* x.

ii) p_v $(v\in T)$ *is ramified at* $K=k(\mathfrak{o})$.

Proof. i) Let $\mathfrak{f}(\mathfrak{o})r(v)=\mathfrak{f}_v r(v)$ for any non-archimedian places v of k. Of course $f_v\in r(v)$. We have only to show that $f_v\in r(v)^\times$, for any $v\in T$. For $v\in T\cap S$, it is trivial. Let $v\in T\cap S'$ and $\mathfrak{o}_0$ be a maximal order of K. Assume $\mathfrak{o}_0=r(v)\oplus wr(v)$, $\mathfrak{o}=r(v)\oplus f_v wr(v)$, $w=\begin{pmatrix} a & b\\ \pi c & 0\end{pmatrix}$ where $a,b,c\in r(v)$. Take $X\in\mathfrak{o}$ satisfying the properties of Lemma 2.1 and put $X=\alpha+\mathfrak{f}_v\beta w$ $(\alpha,\beta\in r(v))$. Since $N(X)=\alpha^2+\mathfrak{f}_v a\alpha\beta-\pi\mathfrak{f}_v^2 bc\beta^2=\pi\varepsilon$, $\varepsilon\in r(v)^\times$, if we suppose $\mathfrak{f}_v\notin r(v)^\times$, then α is divided by π. Hence ε must be divided by π, which is a contradiction.

ii) Let $Z^2-sZ+x=0$ be a minimal polynomial of X over k. Suppose p_v $(v\in S'\cap T)$ splits in $K=k(\mathfrak{o})$, then $Z^2-sZ+x=0$ must be factorized in $k(v)[Z]$. Let $Z^2-sZ+x=(Z-\alpha)(Z-\beta)$ in $k(v)[Z]$. Then $\alpha\equiv 0 \bmod.\ \pi$, $\beta\in r(v)^\times$ or $\beta\equiv 0 \bmod.\ \pi$, $\alpha\in r(v)^\times$. But in either case we have a contradiction, because s is a multiple of π. q.e.d.

2.3. Lemma. *Let* R_0 *be a maximal order containing* R. *Then, for any* $a_0\in R_0^\times$, *there exists* $a\in R^\times$ *such that* $N(a_0)=N(a)$.

Proof. For $v\in S'$, we can assume $R_{0v}=M_2(r(v))$ and $R_v=\begin{pmatrix} r(v) & r(v)\\ p(v) & r(v)\end{pmatrix}$. For a_0, we can take $u_v\in R_v^\times$ such that $N(u_v)=N(a_0)$ for any $v\in S'$. Since R_0 is dense in $\prod_{v\in S'}R_{0v}$, there exists $b\in R_0$ such that $b\equiv u_v^{-1}a_0$, mod. p_vR_{0v}. Hence $N(b)\equiv 1$ mod. $\prod_{v\in S'}p_v$. By the approximation theory of Eichler, there exists $\tilde{u}\in R_0$ such that $N(\tilde{u})=1$ and $\tilde{u}\equiv b$ mod. $(\prod_{v\in S'}P_v)R_0$. Since $a_0\cdot\tilde{u}^{-1}\equiv u_v$ mod. $p(v)R_{0v}$, we have $a_0\tilde{u}^{-1}\in R_v$ for every $v\in S'$. Put $a=a_0\tilde{u}^{-1}$. q.e.d.

From Lemma 2.3, we know that $N(R^\times)=N(R_0^\times)=\{\varepsilon\in r(k)^\times \mid \varepsilon\equiv 1 \bmod \prod_{i=n+1}^m v(i)\}$ ([4] p. 67). Then by (1), $[R^\times;\Gamma]=2^n$.

2.4. Let $K\subset B$ be a totally imaginary quadratic extension of k with maximal order $\mathfrak{o}_0$ and relative discriminant $\delta_{K/k}$ over k, and X_0 be a fixed element of $\mathfrak{o}_0$. Put $\mathrm{Tr}\,(X_0)=s_0$, $N(X_0)=n_0$. Let $\mathfrak{a}_0$ be an ideal of $r(k)$ such that $(s_0^2-4n_0)=\mathfrak{a}_0^2\delta_{K/k}$. We can determine the form of order of K containing X_0. Such $\mathfrak{o}$ has the following form. Take $a_0\in r(k)$ and let $\mathfrak{f}$ be the ideal dividing $\mathfrak{a}_0$, then $\mathfrak{o}=r(k)\oplus\mathfrak{a}_0^{-1}\mathfrak{f}(X_0-a_0)$ (direct sum). a_0 is uniquely determined modulo $\mathfrak{a}_0$, by the couple (s_0,n_0). $\mathfrak{f}$ is the conductor of $\mathfrak{o}$. In particular $\mathfrak{o}_0=r(k)\oplus\mathfrak{a}_0^{-1}(X_0-a_0)$. If the couple (s_0,n_0) is fixed, then $\mathfrak{f}$ is uniquely determined by the isomorphism class of $\mathfrak{o}$.

Conversely, for any divisor $\mathfrak{f}$ of $\mathfrak{a}_0$, there exists one and only one isomorphism class of an order in B which contains the element with trace s_0, norm n_0, with the conductor $\mathfrak{f}$ (see, for example, Prestel pp. 193–195 [3]).

3.0. Theorem. *The number of Γ^*-equivalent classes among Ω_B equals*;

$$\mathfrak{B}_n=\sum_{s,\mathfrak{f}}\frac{2^{n-1}h(\mathfrak{o}(s,\mathfrak{f}))}{[\mathfrak{o}(s,\mathfrak{f})^\times : r(k)^\times]}\prod_{v\in S-T}\left(1-\left\{\frac{\mathfrak{o}(s,\mathfrak{f})}{p_v}\right\}\right)\prod_{v\in S'-T}\left(1+\left\{\frac{\mathfrak{o}(s,\mathfrak{f})}{p_v}\right\}\right)$$

Where:

s: s runs over all integers of k such that $s\equiv 0$ mod. x and $4x-s^2$ is totally positive.

$\mathfrak{f}$: (for such s) $\mathfrak{f}$ runs over all the divisors of the ideal $\mathfrak{a}$ defined by $\mathfrak{a}^2\delta_{K(s)/k}=4x-s^2$ (where $\delta_{K(s)/k}$ is the discriminant of $K(s)=k\sqrt{(s^2-4x)}$ over k).

$\mathfrak{o}(s,\mathfrak{f})$: the order in $K(s)$ with conductor $\mathfrak{f}$, having an element with trace s and norm x.

$h(\mathfrak{o}(s,\mathfrak{f}))$: the class number of $\mathfrak{o}(s,\mathfrak{f})$

$$\left\{\frac{\mathfrak{o}(s,\mathfrak{f})}{p}\right\}=\begin{cases}1 & \text{if } p \text{ divides } \mathfrak{f}.\\ \left(\dfrac{K(s)/k}{p}\right) & \text{the Artin's symbol, otherwise}\end{cases}$$

Proof. By the same method as Shimizu's pp. 65–68, [4], we can see easily

$$\mathfrak{B}_n=\sum_{\mathfrak{o}\in\tilde{\Omega}_B}\frac{[R^\times : \Gamma]}{2[\mathfrak{o}^\times : \Gamma(\mathfrak{o})]}\prod_{v\in S}\left(1-\left\{\frac{\mathfrak{o}}{p_v}\right\}\right)\prod_{v\in S'}\left(1+\left\{\frac{\mathfrak{o}}{p_v}\right\}\right)$$

where $\tilde{\Omega}_B$ denote the set of all subrings satisfying the following conditions (taken up to isomorphisms.)

i) $\mathfrak{o}$ is an order in a totally imaginary quadratic extension of k.

ii) $\mathfrak{o}$ is optimally embedding into R.

iii) $\mathfrak{o}$ belongs to Ω_B.

In 2.3, $[R^\times ; \Gamma]=2^n$. Using (3) in 2.1, we can easily have the theorem from Lemmas 2.1, 2.2 and 2.4. q.e.d.

If $n=1$, by *the Hurwitz formula*, we have.

Corollary. *Let g^* (g resp.) be the genus of compact Riemann surface $\bar{\Gamma}^*\backslash H$ ($\bar{\Gamma}\backslash H$ resp.), then*

$$2g^*-g=1-\frac{1}{2}\mathfrak{B}_1.$$

3.1. By the result of Shimizu [5], g is given as follows.

$$2g-2=\frac{D_0^{3/2}\zeta_0(2)}{2^{2m-2}\pi^{2m}}\prod_{v\in S}(N(v)-1)\prod_{v\in S'}(N(v)+1)$$
$$-\sum_{s,\mathfrak{f}}\frac{h(\mathfrak{o}(s,\mathfrak{f}))}{[\mathfrak{o}(s,\mathfrak{f})^\times : r(k)^\times]}\prod_{v\in S}\left(1-\left\{\frac{\mathfrak{o}(s,\mathfrak{f})}{p_v}\right\}\right)\prod_{v\in S'}\left(1+\left\{\frac{\mathfrak{o}(s,\mathfrak{f})}{p_v}\right\}\right)$$
$$\times(1-[\Gamma(\mathfrak{o}(s,\mathfrak{f})) : r(k)^\times]^{-1})$$

where $(s,\mathfrak{f})$ runs over the pairs satisfying the conditions obtained by replacing x in the conditions of 3.0 by 1, and the additional conditions $s \neq \pm 2$. The notations in the above formula are almost the same as in 3.0. We shall explain only the new ones.

D_0: the absolute discriminant of k.

$\zeta_0(z)$: the zeta-function of k.

$N(v)$: the index of $p(v)$ in $r(v)$.

Let $\mathfrak{o}_0 = \mathfrak{o}(s, 1)$ be the maximal order of $K(s)$, then we have the relation between the class number of $\mathfrak{o}(s, \mathfrak{f})$ and that of $\mathfrak{o}_0$; [3]

$$\frac{h(\mathfrak{o}(s,\mathfrak{f}))}{h(\mathfrak{o}_0)} = \frac{1}{[\mathfrak{o}_0^\times : \mathfrak{o}(s,\mathfrak{f})^\times]} \prod_{p_v | \mathfrak{f}} \left(N(v) - \left(\frac{K(s)/k}{p_v}\right)\right) \tag{4}$$

Example. Let $k = \boldsymbol{Q}$, then $n = m = 1$, $D_0 = 1$ and $\zeta_0(2) = \pi^2/6$ put $S = \{p_1, p_2, \cdots, p_{2l}\}$. $S' = \{q_1, q_2, \cdots, q_k\}$, and $x = p_1 \cdot p_2 \cdots p_s \cdot q_1 \cdot q_2 \cdots q_t$. $s \leqslant 2l$, $t \leqslant k$. Suppose $x > 3$ and let $h(-D)$ denote the class number of the order with discriminant $-D$ in $\boldsymbol{Q}(\sqrt{-D})$. By (4), $h(-4x) = h(-x)$, $x \not\equiv 3$ mod. 8 and $h(-4x) = 3h(-x)$, $x \equiv 3$ mod. 8.

Hence we have:

$$2g-2 = \frac{1}{6}\prod_{i=1}^{2l}(p_i - 1)\prod_{j=1}^{k}(q_j+1) - \frac{1}{2}\prod_{j=1}^{2l}\left(1 - \left(\frac{-4}{p_i}\right)\right)\prod_{j=1}^{k}\left(1 + \left(\frac{-4}{q_j}\right)\right)$$
$$- \frac{2}{3}\prod_{i=1}^{2l}\left(1 - \left(\frac{-3}{p_i}\right)\right)\prod_{j=1}^{k}\left(1 + \left(\frac{-3}{q_j}\right)\right).$$

$$2g^* - g = 1 - \frac{1}{2}\delta_x h(-4x)\prod_{i>s}\left(1 - \left(\frac{-\sigma_x x}{p_i}\right)\right)\prod_{j>t}\left(1 + \left(\frac{-\sigma_x x}{q_j}\right)\right).$$

Here

$$\delta_x = \begin{cases} \frac{4}{3}, & x \equiv 3 \\ 2, & x \equiv 7 \quad \text{mod. } 8 \\ 1, & \text{otherwise} \end{cases} \qquad \sigma_x = \begin{cases} 4, & x \equiv 3 \text{ mod. } 4 \\ 1, & \text{otherwise} \end{cases}$$

$\left(\frac{*}{p}\right)$: Legendre symbol.

References

[1] M. Eichler: Zur zahlen theorie der Quaternionen-Algebren. J. Reine Angew. Math., **195**, 127–151 (1956).

[2] H. Hijikata: Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$. J. Math. Soc. Japan., **26**, 56–82 (1974).

[3] A. Prestel: Die elliptischen Fixpunkte der Hilbertischen Modulgruppen. Math. Annalen., **177**, 181–209 (1968).

[4] H. Shimizu: On discontinuous groups operating on the product of the upper half planes. Ann. of Math., **77**, 33–71 (1963).

[5] ——: On zeta functions of quaternion algebras. Ann. of Math., **81**, 166–193 (1965).

[6] M. Yamauchi: On the traces of Hecke operators for a normalizer of $\Gamma_0(N)$. J. Math. Kyoto Univ., **13-2**, 403–411 (1973).