COMMENTARII MATHEMATICI UNIVERSITATIS SANCTI PAULI
Vol. 60, No. 1, 2 2011
ed. RIKKYO UNIV/MATH IKEBUKURO TOKYO 171–8501 JAPAN

On Some Problems Concerning Discrete Subgroups

by

Hiroyuki YOSHIDA*

(Received May 3, 2011)

Dedicated to Professor Akio Fujii on the occasion of his retirement

Abstract. We discuss four topics on discrete subgroups: Exceptional zeros of the Selberg zeta function, the construction of noncongruence subgroups of an arithmetic cocompact Fuchsian group, the construction of noncongruence subgroups of the unimodular group and a presentation of a Hilbert modular group.

Introduction

Let Γ be a cocompact Fuchsian group. Selberg ([Sel1]) defined the zeta function $Z_\Gamma(s)$ attached to Γ; concerning the zeros ρ in the critical strip $0 < \Re(\rho) < 1$, he showed that $Z_\Gamma(s)$ satisfies the Riemann hypothesis except for finitely many zeros on the real line. For these exceptional zeros, Selberg ([Sel2]) showed that they actually exist in some cases and conjectured that such phenomena will not take place for congruence subgroups. Later Randol ([R]) gave a simple proof of the existence of exceptional zeros.

In section 1, we will give another conceptually simple proof of the existence of exceptional zeros. The idea is to consider the distribution attached to $Z_\Gamma(s)$ and employ Weil's observation ([W]) that it is of positive type if and only if $Z_\Gamma(s)$ satisfies the Riemann hypothesis. Our example of Γ is given as the kernel Γ_χ of a suitable character χ of Γ_0, where Γ_0 is a cocompact torsion free Fuchsian group. When Γ_0 is arithmetic, Γ_χ should be a noncongruence subgroup in view of the Selberg conjecture. In section 2, we will show that we can actually produce noncongruence subgroups in the form of Γ_χ. The relation of noncongruence property and the existence of exceptional zeros is an interesting problem but we will not touch this topic in this paper. In section 3, we will construct noncongruence subgroups of $SL(2, \mathbf{Z})$ by a different technique. Though the method of section 2 applies for the case $SL(2, \mathbf{Z})$, this new technique has the advantage that we can easily construct examples of modular forms with respect to noncongruence subgroups. We will show an example in section 4. In section 5, we will determine a presentation of the Hilbert modular group for $\mathbf{Q}(\sqrt{5})$.

Some parts of this paper have old origins. I found the proof given in section 1 about twenty years ago when I was preparing my course; section 2 is added on this occasion. I

*The author was supported by Grant-in-Aid for Scientific Research (C) (No. 21540014), Japan Society for Promotion of Science.

found the construction of section 3 when I wrote the paper [Y2]; section 4 is worked out for this paper. Section 5 appeared as an appendix of my paper in Math. Arxiv [Y3].

This paper is written on the occasion of the retirement of Professor Akio Fujii. It is my great pleasure to dedicate this paper to him in gratitude for our long standing friendship since 1973.

NOTATION. For an associative ring A with identity element, $A^\times$ denotes the group of all invertible elements of A. Let R be a commutative ring with identity element. We denote by $M(n, R)$ the ring of all $n \times n$ matrices with entries in R. The unit matrix is denoted by 1_n. We define $\mathrm{GL}(n, R) = M(n, R)^\times$, $\mathrm{SL}(n, R) = \{g \in \mathrm{GL}(n, R) \mid \det g = 1\}$. The quotient group of $\mathrm{SL}(n, R)$ by its center is denoted by $\mathrm{PSL}(n, R)$. For an algebraic number field F, $\mathcal{O}_F$ denotes the ring of integers and $E_F = \mathcal{O}_F^\times$ denotes the group of units of F. We denote by $\mathfrak{H}$ the complex upper half plane. For modular groups and modular forms, we follow the notation of Shimura [Sh2].

§1. Exceptional zeros of the Selberg zeta function

Let Γ be a cocompact Fuchsian group. For simplicity, we assume that $-1_2 \in \Gamma$ and put $\overline{\Gamma} = \Gamma/\{\pm 1_2\}$. Let χ be a character of Γ such that $\chi(-1_2) = 1$. We consider χ as a character of $\overline{\Gamma}$. The Selberg zeta function $Z_\Gamma(s, \chi)$ is defined by

$$Z_\Gamma(s, \chi) = \prod_{\{\gamma\}} \prod_{k=0}^{\infty} (1 - \chi(\gamma)(N(\gamma))^{-s-k})$$

which converges absolutely when $\Re(s) > 1$ and can be continued to an entire function. Here $\{\gamma\}$ extends over all primitive hyperbolic conjugacy classes of $\overline{\Gamma}$ and $N(\gamma)$ denotes the norm of γ. When χ is trivial, we denote $Z_\Gamma(s, \chi)$ by $Z_\Gamma(s)$. We will give a simple proof that there exists Γ for which $Z_\Gamma(s)$ has an exceptional zero.

Let $L^2(\Gamma\backslash\mathfrak{H}, \chi)$ be the Hilbert space consisting of all functions φ on $\mathfrak{H}$ which satisfy $\varphi(\gamma z) = \chi(\gamma)\varphi(z)$ for every $\gamma \in \Gamma$ and $|\varphi| \in L^2(\Gamma\backslash\mathfrak{H})$. We assume that $\overline{\Gamma}$ is torsion free. Then the trace formula reads as follows ([Sel1], p. 74, [H1], p. 32, Theorem 7.5, [GGP], p. 78). For a test function $F \in C_c^\infty(\mathbf{R})$, put

$$\Phi(s) = \int_{-\infty}^{\infty} F(x) e^{(s-1/2)x} dx\,.$$

Then, when F is an even function,

$$\begin{aligned}\sum_\rho \Phi(\rho) =& \frac{\mathrm{vol}(\Gamma\backslash\mathfrak{H})}{2\pi} \int_{-\infty}^{\infty} r \frac{e^{\pi r} - e^{-\pi r}}{e^{\pi r} + e^{-\pi r}} \Phi\left(\frac{1}{2} + ir\right) dr \\ &+ 2 \sum_{\{\gamma\}} \sum_{k=1}^{\infty} \frac{\chi(\gamma)^k \log(N(\gamma))}{N(\gamma)^{k/2} - N(\gamma)^{-k/2}} F(k \log(N(\gamma)))\,.\end{aligned} \tag{1.1}$$

Here for an eigenvalue λ of the non-Euclidean Laplacian $\Delta = -y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right)$ occuring in $L^2(\Gamma\backslash\mathfrak{H}, \chi)$ with multiplicity $m(\lambda)$, we let ρ occur in (1.1) with multiplicity $m(\lambda)$ by the relation $\rho = 1/2 \pm s/2$, $\lambda = (1 - s^2)/4$. (When $\lambda = 1/4$, $s = 0$, we let $\rho = 1/2$ occur with the multiplicity $2m(1/4)$. When $\lambda \neq 1/4$, two ρ's occur.) And $\{\gamma\}$ extends over all primitive hyperbolic conjugacy classes of $\overline{\Gamma}$. The ρ's such that $0 < \Re(\rho) < 1$ coincide with the zeros of $Z_\Gamma(\Gamma, \chi)$ with the multiplicities stated above. Both sides of (1.1) converge absolutely.

We recall the interpretation of (1.1) by representation theory. Let $G = \mathrm{SL}(2, \mathbf{R})$, $K = \mathrm{SO}(2, \mathbf{R})$. Let $L^2(\Gamma\backslash G, \chi)$ be the Hilbert space consisting of all functions φ on G which satisfy $\varphi(\gamma g) = \chi(\gamma)\varphi(g)$ for every $\gamma \in \Gamma$ and $|\varphi| \in L^2(\Gamma\backslash G)$. We put $H_\chi = L^2(\Gamma\backslash G, \chi)$; G acts on H_χ by the right translation. The Hilbert space $L^2(\Gamma\backslash\mathfrak{H}, \chi)$ can be identified with the closed subspace of H_χ consisting of all K-fixed vectors. The unitary representation of G on H_χ decomposes into a discrete direct sum:

$$H_\chi = \oplus_\pi V_\pi$$

where V_π is a closed invariant subspace of H_χ and an irreducible unitary representation π of G is realized on V_π. Then π must satisfy $\pi(-1_2) = \mathrm{id}$; V_π contributes to $L^2(\Gamma\backslash\mathfrak{H}, \chi)$ if and only if π has a (nonzero) K-fixed vector. The classification of such π is given as follows. Let B be the subgroup of G consisting of all upper triangular matrices. For $s \in \mathbf{C}$, we define a quasi-character ω_s of B by

$$\omega_s\left(\begin{pmatrix} t & u \\ 0 & t^{-1} \end{pmatrix}\right) = |t|^{s+1}.$$

Let $PS(\omega_s)$ be the space of smooth functions f on G which satisfy $f(bg) = \omega_s(b)f(g)$ for $b \in B$. Then G acts on $PS(\omega_s)$ by the right translation. When $s \in i\mathbf{R}$, $PS(\omega_s)$ is a pre-Hilbert space with a canonical inner product. Let π_s be the unitary representation of G obtained by completion. It is irreducible and is called a principal series representation. When $-1 < s < 1$, $s \neq 0$, we obtain an irreducible unitary representation π_s by a similar procedure from $PS(\omega_s)$. It is called a complementary series representation. We have $\pi_s \cong \pi_{-s}$. The eigenvalue of Δ for a K-fixed vector of π_s (unique up to constant multiple) is $(1 - s^2)/4$. This finishes the classification besides the trivial representation. A principal series representation π_s corresponds to zeros $1/2 \pm s/2$ on the critical line; a complementary series representation π_s corresponds to zeros $\rho = 1/2 \pm s/2$ on the real line, $0 < \rho < 1$, $\rho \neq 1/2$, i.e. exceptional zeros; the trivial representation contributes $\rho = 0$ and 1 for (1.1).

Now the trivial representation of G occurs in H_χ if and only if $\chi = 1$. Therefore the following observation holds.[1]

(F) The terms $\Phi(0)$ and $\Phi(1)$ appear on the left hand side of (1.1) if and only if $\chi = 1$.

The left-hand side of (1.1) defines a distribution $T_{\Gamma,\chi}$: $T_{\Gamma,\chi}(F) = \sum_\rho \Phi(\rho)$. As is well known (cf. [W]), $T_{\Gamma,\chi}$ is of positive type, i.e., $T_{\Gamma,\chi}(\alpha * \tilde{\alpha}) \geq 0$, $\tilde{\alpha}(x) = \overline{\alpha(-x)}$, for every $\alpha \in C_c^\infty(\mathbf{R})$ if and only if all ρ on the left-hand side of (1.1) lie on the critical line. As a slight refinement of this criterion, I showed that the condition $T_{\Gamma,\chi}(\alpha * \tilde{\alpha}) \geq 0$ for all odd

[1] This fact should not be confused with the existence of trivial zeros of $Z_\Gamma(s, \chi)$.

functions α is sufficient to assure this conclusion ([Y1], Proposition 1)[2]. Then $F = \alpha * \tilde{\alpha}$ is an even function. Now from (F), we see that there exists odd $\alpha \in C_c^\infty(\mathbf{R})$ such that $T_{\Gamma,1}(\alpha * \tilde{\alpha}) < 0$. We fix such an α. Let $g \geq 2$ be the genus of the compact Riemann surface $\Gamma \backslash \mathfrak{H}$. Since $\overline{\Gamma} \cong \pi_1(\Gamma\backslash\mathfrak{H})$, $\overline{\Gamma}$ has $2g$ generators $\sigma_1, \ldots, \sigma_g, \tau_1, \ldots, \tau_g$ whose fundamental relation is

$$(1.2) \qquad (\sigma_1\tau_1\sigma_1^{-1}\tau_1^{-1}) \cdots (\sigma_g\tau_g\sigma_g^{-1}\tau_g^{-1}) = 1 .$$

Choose $s_i \in \mathbf{C}$, $|s_i| = 1$, $t_i \in \mathbf{C}$, $|t_i| = 1$, $1 \leq i \leq g$. In view of (1.2), we can define a character $\overline{\chi}$ of $\overline{\Gamma}$ by

$$\overline{\chi}(\sigma_i) = s_i , \qquad \overline{\chi}(\tau_i) = t_i , \qquad 1 \leq i \leq g .$$

Then we define a character χ of Γ by $\chi = \overline{\chi} \circ p$, where $p : \Gamma \longrightarrow \overline{\Gamma}$ is the canonical homomorphism. If s_i and t_i are sufficiently close to 1, then we see that $T_{\Gamma,\chi}(\alpha*\tilde{\alpha}) < 0$ from the right-hand side of the trace formula (1.1). In view of (F), this implies that $Z_\Gamma(s, \chi)$ has a zero ρ such that $0 < \rho < 1$, $\rho \neq 1/2$ (if $\chi \neq 1$). In particular, choose $s_i = t_i = e^{2\pi i/N}$, $1 \leq i \leq g$ for a positive integer N. Let Γ_χ be the kernel of χ. Then $\Gamma/\Gamma_\chi \cong \mathbf{Z}/N\mathbf{Z}$ and we have[3]

$$Z_{\Gamma_\chi}(s) = \prod_\eta Z_\Gamma(s, \eta)$$

where η extends over all characters of Γ which are trivial on Γ_χ. Therefore, when N is sufficiently large, $Z_{\Gamma_\chi}(s)$ has a zero ρ such that $0 < \rho < 1$, $\rho \neq 1/2$.

A conjecture of Selberg states that $Z_\Gamma(s)$ has no exceptional zeros if Γ is of arithmetic type. In view of this conjecture, the group Γ_χ should be a noncongruence subgroup when Γ is of arithmetic type. We will examine this problem in the next section.

§2. Construction of noncongruence subgroups for cocompact case

We will give a simple proof for the existence of noncongruence subgroups of a cocompact arithmetic Fuchsian group.

Let F be a totally real algebraic number field of degree n. Let $\mathcal{O}_F$ denote the ring of integers of F. Let B be a division quaternion algebra over F such that

$$(2.1) \qquad B \otimes_{\mathbf{Q}} \mathbf{R} \cong M(2, \mathbf{R}) \times \mathbf{H}^{n-1} .$$

Here $\mathbf{H}$ denotes the Hamilton quaternion algebra. Let $*$ denote the main involution and let $N : B \longrightarrow F$ denote the reduced norm. We have $N(x) = xx^*$. We take a maximal order R of B and fix it. For a prime ideal $\mathfrak{p}$ of F, we set

$$B_\mathfrak{p} = B \otimes_F F_\mathfrak{p}, \qquad R_\mathfrak{p} = R \otimes_{\mathcal{O}_F} \mathcal{O}_{F_\mathfrak{p}} ,$$

[2] This proposition is proved for zeros of the Dedekind zeta function. The modification adapted to the present case is easy.

[3] We can prove this equality easily. Instead we can use the obvious fact that the spectra of Δ in $L^2(\Gamma\backslash\mathfrak{H}, \chi)$ are contained in that in $L^2(\Gamma_\chi\backslash\mathfrak{H})$.

where $F_{\mathfrak{p}}$ is the completion of F at $\mathfrak{p}$ and $\mathcal{O}_{F_{\mathfrak{p}}}$ is the ring of integers of $F_{\mathfrak{p}}$. We say that B is ramified at $\mathfrak{p}$ if $B_{\mathfrak{p}}$ is a division algebra and unramified otherwise. In the latter case, $B_{\mathfrak{p}}$ is isomorphic to $M(2, F_{\mathfrak{p}})$ as algebras over $F_{\mathfrak{p}}$.

Put

$$\Gamma = R^1 = \{x \in R \mid N(x) = 1\}\,.$$

By the projection to the first factor in (2.1), we can regard Γ as a subgroup of SL(2, $\mathbf{R}$); Γ is a cocompact Fuchsian group. For an integral ideal $\mathfrak{n}$ of F, we put

$$\Gamma_{\mathfrak{n}} = \{\gamma \in \Gamma \mid \gamma - 1 \in \mathfrak{n}R\}\,.$$

We call $\Gamma_{\mathfrak{n}}$ the principal congruence subgroup of level $\mathfrak{n}$. A subgroup of finite index of Γ is called a noncongruence subgroup if it does not contain $\Gamma_{\mathfrak{n}}$ for any $\mathfrak{n}$. We are going to show that Γ contains noncongruence sugbroups. This case is of particular geometric interest because $\Gamma\backslash\mathfrak{H}$ is (a special case of) the Shimura curve ([Sh1]).

LEMMA 2.1. *There exists an ideal* $\mathfrak{n}$ *such that* $\Gamma_{\mathfrak{n}}$ *is torsion free.*

proof. This is well known. We give a proof for the convenience of the reader. Let $\gamma \in \Gamma$ be an element of order $n \geq 2$. Clearly we can obtain an isomorphism $F(\gamma) \cong F(e^{2\pi i/n})$ by sending γ to $e^{2\pi i/n}$. Since $\gamma^* = \gamma^{-1}$, $\gamma + \gamma^* \in F$, we see that F contains $\cos(2\pi/n)$. Therefore n is bounded. Changing γ to a power of it if necessary, we may assume that $\gamma + \gamma^* = 2\cos(2\pi/n)$. Now suppose that $\gamma \in \Gamma_{\mathfrak{n}}$. Since R is stable under $*$, we see that $2\cos(2\pi/n) \in 2 + \mathfrak{n}R$, which implies $2\cos(2\pi/n) - 2 \equiv 0 \mod \mathfrak{n}$. It suffices to choose $\mathfrak{n}$ so that it does not divide $(2\cos(2\pi/n) - 2)$ for all $n \geq 2$ which can occur as the order of $\gamma \in \Gamma$. This completes the proof.

We take an ideal $\mathfrak{n}$ so that $\Gamma_{\mathfrak{n}}$ is torsion free and put $\Delta = \Gamma_{\mathfrak{n}}$. Let g be the genus of the compact Riemann surface $\Delta\backslash\mathfrak{H}$. As in §1, Δ has $2g$ generators $\sigma_1, \ldots, \sigma_g, \tau_1, \ldots, \tau_g$ whose fundamental relation is (1.2). Let $\mathfrak{p}$ be a prime ideal of F. We put

$$R_{\mathfrak{p}}^1 = \{x \in R_{\mathfrak{p}} \mid N(x) = 1\}\,.$$

For a nonnegative integer f, we put

$$U_{\mathfrak{p},f} = \{u \in R_{\mathfrak{p}}^1 \mid u - 1 \in \mathfrak{p}^f R_{\mathfrak{p}}\}\,.$$

Let S be the finite set of all prime ideals of F at which B is ramified.

THEOREM 2.2. *Let* m *be a positive integer and define a character* χ *of* Δ *by* $\chi(\sigma_i) = \chi(\tau_i) = e^{2\pi i/m}$, $1 \leq i \leq g$. *Let* Γ_χ *be the kernel of* χ. *We assume that* m *has a prime factor* $l \geq 5$ *which satisfies the following three conditions.* (i) l *does not divide the norm of* $\mathfrak{n}$. (ii) l *is relatively prime to every prime ideal* $\mathfrak{p} \in S$. (iii) l *does not divide the order of* $U_{\mathfrak{p},0}/U_{\mathfrak{p},1}$ *for every prime ideal* $\mathfrak{p} \in S$. *Then* Γ_χ *is a noncongruence subgroup of* Γ.

proof. Suppose that Γ_χ contains a principal congruence subgroup of level $\mathfrak{m}$. Then Γ_χ contains $\Gamma_{\mathfrak{n}\mathfrak{m}}$. We may regard χ as a character of $\Delta/\Gamma_{\mathfrak{n}\mathfrak{m}}$. Therefore $\Delta/\Gamma_{\mathfrak{n}\mathfrak{m}}$ has a character of order l. Let

$$\mathfrak{n} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}\,, \qquad \mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{d_{\mathfrak{p}}}$$

be the prime ideal decompositions. By the strong approximation theorem (cf. [Sh3], Corollary 32.13), we have

$$\Gamma_{\mathfrak{n}}/\Gamma_{\mathfrak{nm}} \cong \prod_{\mathfrak{p}} (U_{\mathfrak{p},e_{\mathfrak{p}}}/U_{\mathfrak{p},e_{\mathfrak{p}}+d_{\mathfrak{p}}})\,. \tag{2.2}$$

Hence there exists $\mathfrak{p}$ such that $U_{\mathfrak{p},e_{\mathfrak{p}}}/U_{\mathfrak{p},e_{\mathfrak{p}}+d_{\mathfrak{p}}}$ has a character ψ of order l. We distinguish two cases.

(I) The case where $\mathfrak{p} \notin S$.

Let $p\mathbf{Z} = \mathfrak{p} \cap \mathbf{Z}$. If $e_{\mathfrak{p}} > 0$, then $U_{\mathfrak{p},e_{\mathfrak{p}}}/U_{\mathfrak{p},e_{\mathfrak{p}}+d_{\mathfrak{p}}}$ is a p-group. Since $l \neq p$ by (i), this is a contradiction. Suppose $e_{\mathfrak{p}} = 0$. Since $R_{\mathfrak{p}} \cong M(2, \mathcal{O}_{F_{\mathfrak{p}}})$, we have

$$U_{\mathfrak{p},0}/U_{\mathfrak{p},d_{\mathfrak{p}}} \cong \mathrm{SL}(2, \mathcal{O}_F/\mathfrak{p}^{d_{\mathfrak{p}}}\mathcal{O}_F)\,.$$

If $p \geq 5$, then by Lemma 2.3 given below, the commutator subgroup of $\mathrm{SL}(2, \mathcal{O}_F/\mathfrak{p}^{d_{\mathfrak{p}}}\mathcal{O}_F)$ coincides with itself, which is a contradiction. Suppose that $p = 2$ or 3. Since $l \geq 5$ and $U_{\mathfrak{p},1}/U_{\mathfrak{p},d_{\mathfrak{p}}}$ is a p-group, ψ is trivial on $U_{\mathfrak{p},1}$. Hence ψ can be identified with a character of $\mathrm{SL}(2, \mathcal{O}_F/\mathfrak{p}\mathcal{O}_F)$. We see that ψ is trivial on the subgroups

$$H = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \,\middle|\, u \in \mathcal{O}_F/\mathfrak{p}\mathcal{O}_F \right\}$$

and ${}^tH$. Since H and ${}^tH$ generate $\mathrm{SL}(2, \mathcal{O}_F/\mathfrak{p}\mathcal{O}_F)$, this is a contradiction.

(II) The case where $\mathfrak{p} \in S$.

By (ii) and (iii), we see that l does not divide the order of $U_{\mathfrak{p},e_{\mathfrak{p}}}/U_{\mathfrak{p},e_{\mathfrak{p}}+d_{\mathfrak{p}}}$, which is a contradiction.

To complete the proof of Theorem 2.2, it suffices to prove the next lemma.

LEMMA 2.3. *Let K be a non-archimedean local field, $\mathcal{O}_K$ be the ring of integers, ϖ be a prime element and q be the order of the residue field of K. Take a positive integer n and let $G = \mathrm{SL}(2, \mathcal{O}_K/\varpi^n\mathcal{O}_K)$. If $q > 3$, then the commutator subgroup $[G, G]$ of G coincides with G.*

proof. For $a, b \in G$, we define the commutator by $[a, b] = aba^{-1}b^{-1}$. First we consider the case $n = 1$. Let $\mathbf{F}_q = \mathcal{O}_F/\varpi\mathcal{O}_F$ be the finite field with q elements. It is well known that $\mathrm{PSL}(2, \mathbf{F}_q)$ is a simple group when $q > 3$. Therefore we have $[G, G]\{\pm 1_2\} = G$. Since

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right] = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

we have $-1_2 \in [G, G]$. Hence the assertion holds in this case.

Now assume $n \geq 2$. We put $R = \mathcal{O}_K/\varpi^n\mathcal{O}_K$. Define a subgroup H of G by

$$H = \{ g \in G \mid g \equiv 1_2 \mod \varpi \}\,.$$

Then H is a normal subgroup of G such that $G/H \cong \mathrm{SL}(2, \mathbf{F}_q)$. We have $[G, G]H = G$. For $t \in R^\times$ and $u \in R$, we have

$$\left[\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}, \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & (t^2 - 1)u \\ 0 & 1 \end{pmatrix}.$$

Since $q > 3$, we can choose t so that $t^2 - 1 \in R^\times$. Hence we have $\left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right) \in [G, G]$ for every $u \in R$. Similarly $\left(\begin{smallmatrix} 1 & 0 \\ u & 1 \end{smallmatrix}\right) \in [G, G]$ for every $u \in R$. For $x \in R$, $y \in \varpi\mathcal{O}_K/\varpi^n\mathcal{O}_K$, we have

$$\begin{pmatrix} 1 & 0 \\ -y/(1+xy) & 1 \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}\begin{pmatrix} 1 & -x/(1+xy) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+xy & 0 \\ 0 & 1/(1+xy) \end{pmatrix}.$$

Therefore $\left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) \in [G, G]$ for every $t \in 1 + (\varpi\mathcal{O}_K/\varpi^n\mathcal{O}_K)$. We can check easily that H is generated by such elements together with $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ y & 1 \end{smallmatrix}\right)$, $x, y \in \varpi\mathcal{O}_K/\varpi^n\mathcal{O}_K$. Therefore $[G, G] \supset H$. Combined with $[G, G]H = G$, the assertion follows.

REMARK 2.4. If χ is a character of Δ whose order is divisible by a prime number l satisfying the conditions of Theorem 2.2, then Γ_χ is a noncongruence subgroup of Γ.

PROBLEM 2.5. *Let $\Gamma = R^1$ and let Γ' be a subgroup of Γ of finite index. The Selberg conjecture states that $Z_{\Gamma'}(s)$ does not have an exceptional zero if Γ' is a congruence subgroup. Is the converse true?*

§3. Construction of noncongruence subgroups of SL(2, Z)

We will give a simple construction of noncongruence subgroups of $\mathrm{SL}(2, \mathbf{Z})$. Let

$$\Delta(z) = e^{2\pi iz}\prod_{k=1}^{\infty}(1 - e^{2\pi ikz})^{24}, \qquad z \in \mathfrak{H}$$

be the cusp form of weight 12 with respect to $\mathrm{SL}(2, \mathbf{Z})$. Let n be a positive integer. We define a holomorphic function $\Delta(z)^{1/n}$ so that it takes positive values when z is purely imaginary. We see easily that $\Delta(z)^{1/n}$ has the product expansion

$$(3.1) \qquad \Delta(z)^{1/n} = e^{2\pi iz/n}\prod_{k=1}^{\infty}(1 - e^{2\pi ikz})^{24/n}, \qquad z \in \mathfrak{H}.$$

Here the branch of $(1 - e^{2\pi ikz})^{24/n}$ is taken so that it is positive when z is purely imaginary. Take an integer $m \geq 2$. Put

$$f(z) = \Delta(mz)^{1/n}/\Delta(z)^{1/n}.$$

Then $f(z)^n$ is an automorphic function with respect to $\Gamma_0(m)$, since $\Delta(mz) \in S_{12}(\Gamma_0(m))$. For $\gamma \in \Gamma_0(m)$, put

$$\chi(\gamma) = f(\gamma z)/f(z).$$

Since $\chi(\gamma)^n = 1$, we see that $\chi(\gamma)$ does not depend on z and χ is a character of $\Gamma_0(m)$. From (3.1), we see that

$$\Delta(z+1)^{1/n} = e^{2\pi i/n}\Delta(z)^{1/n}, \qquad \Delta(m(z+1))^{1/n} = e^{2m\pi i/n}\Delta(mz)^{1/n}.$$

Hence we obtain

$$(3.2) \qquad \chi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = e^{2\pi i(m-1)/n}.$$

Let Γ_χ be the kernel of χ. Write $(m-1)/n = p/q$ with relatively prime positive integers p and q. By (3.2), we see that the order of χ divides n and is divisible by q. Hence $[\Gamma_0(m) : \Gamma_\chi]$ divides n and is divisible by q.

THEOREM 3.1. *We assume that q has a prime factor $l \geq 5$ which does not divide m and $t-1$ for every prime factor t of m. Then the group Γ_χ is a noncongruence subgroup.*

proof. Suppose that Γ_χ contains the principal congruence subgroup $\Gamma(N)$ for a positive interger N. Then m divides N and χ factors through the canonical map $\Gamma_0(m) \longrightarrow \Gamma_0(m)/\Gamma(N)$. Hence $\Gamma_0(m)/\Gamma(N)$ posesses a character whose order is divisible by q. Let $N = \prod p^{e_p}$ be the prime factorization. We have

$$\Gamma_0(m)/\Gamma(N) \cong \prod_{p|m} G_p \times \prod_{p\nmid m} \mathrm{SL}(2, \mathbf{Z}/p^{e_p}\mathbf{Z}),$$

where, p^{d_p} being the exact power of p dividing m,

$$G_p = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z}/p^{e_p}\mathbf{Z}) \;\middle|\; c \in p^{d_p}\mathbf{Z}/p^{e_p}\mathbf{Z}) \right\}.$$

Let

$$G = \begin{cases} \prod_{p|m} G_p \times \mathrm{SL}(2, \mathbf{Z}/2^{e_2}\mathbf{Z}) \times \mathrm{SL}(2, \mathbf{Z}/3^{e_3}\mathbf{Z}) & \text{if 6 does not divide } m\,, \\ \prod_{p|m} G_p \times \mathrm{SL}(2, \mathbf{Z}/3^{e_3}\mathbf{Z}) & \text{if 2 divides } m \text{ and 3 does not divide } m, \\ \prod_{p|m} G_p \times \mathrm{SL}(2, \mathbf{Z}/2^{e_2}\mathbf{Z}) & \text{if 3 divides } m \text{ and 2 does not divide } m\,, \\ \prod_{p|m} G_p & \text{if 6 divides } m\,. \end{cases}$$

By Lemma 2.3, the commutator subgroup of $\mathrm{SL}(2, \mathbf{Z}/p^{e_p}\mathbf{Z})$ coincides with itself if $p \geq 5$.[4] Therefore G must have a character whose order is divisible by q. Since the order of G is not divisible by l, this is a contradiction and we complete the proof.

REMARK 3.2. The condition of the theorem is satisfied if $m = 2$ and $n \geq 5$ is a prime number. In the case $m = 2, n = 5$, we obtain a noncongruence subgroup of $\mathrm{SL}(2, \mathbf{Z})$ of index 15.

REMARK 3.3. It is well known that the principal congruence subgroup $\Gamma(p)$ is a free group for a prime number p. Using this fact, we can apply the method of section 2 to produce noncongruence subgroups.

REMARK 3.4. Let D be a hermitian symmetric space. If there exists an everywhere nonvanishing holomorphic automorphic form on D with respect to an arithmetic group Γ, then we can produce noncongruence subgroups of Γ by a similar argument to the above. However the non-existence of such a form is known for a wide class of D.

[4] Another simple proof is given as follows. It is well known that the commutator subgroup of $\mathrm{SL}(2, \mathbf{Z})$ contains $\Gamma(6)$. Take $g \in \mathrm{SL}(2, \mathbf{Z}/p^{e_p}\mathbf{Z})$. Write $g = \gamma \mod p^{e_p}$ with $\gamma \in \Gamma(6)$. We can write γ as the product of commutators of elements of $\mathrm{SL}(2, \mathbf{Z})$. Reduce this expression modulo p^{e_p}. Then we obtain an expression of g as the product of commutators of the elements of $\mathrm{SL}(2, \mathbf{Z}/p^{e_p}\mathbf{Z})$.

§4. An example of modular forms for a noncongruence subgroup

In Theorem 3.1, we assume that m and n are prime numbers such that $n \geq 5$, $n \neq m$ and n does not divide $m-1$. Then Γ_χ is a noncongruence subgroup such that $[\Gamma_0(m) : \Gamma_\chi] = n$. Up to equivalence, $\Gamma_0(m)$ has two cusps ∞ and 0. The equivalence classes of the cusps of Γ_χ lying over ∞ are in one to one correspondence with $\Gamma_\chi \backslash \Gamma_0(m)/\Gamma_0(m)_\infty$ where

$$\Gamma_0(m)_\infty = \{\gamma \in \Gamma_0(m) \mid \gamma\infty = \infty\}.$$

By (3.2), we see easily that $\Gamma_0(m) = \Gamma_\chi \Gamma_0(m)_\infty$. Hence, up to equivalence, there is only one cusp of Γ_χ lying over ∞. We can check easily that

$$\chi\left(\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}\right) = e^{2\pi i(m-1)/n}. \tag{4.1}$$

Then, similarly, we see that there is only one cusp of Γ_χ lying over 0, up to equivalence. The number of equivalence classes of elliptic points of $\Gamma_0(m)$ of order 2 (resp. 3) are ν_2 (resp. ν_3) where (cf. [Sh2], Proposition 1.43)

$$\nu_2 = 1 + \left(\frac{-1}{m}\right), \qquad \nu_3 = 1 + \left(\frac{-3}{m}\right). \tag{4.2}$$

We can show easily that the number of equivalence classes of elliptic points of Γ_χ of order 2 (resp. 3) are $n\nu_2$ (resp. $n\nu_3$).

Let g_χ (resp. g_0) be the genus of the compact Riemann surface $\Gamma_\chi \backslash \mathfrak{H} \cup \{\text{cusps}\}$ (resp. $\Gamma_0(m)\backslash\mathfrak{H} \cup \{\text{cusps}\}$). By Theorem 2.20 of [Sh2], we find

$$g_\chi = n\left[\frac{1}{12}(m+1) - \frac{1}{4}\nu_2 - \frac{1}{3}\nu_3\right], \qquad g_\chi = n g_0. \tag{4.3}$$

Here ν_2 and ν_3 are given by (4.2). By Theorem 2.24 of [Sh2], we have $\dim S_2(\Gamma_\chi) = g_\chi$ and for an even integer $k > 2$, we have

$$\dim S_k(\Gamma_\chi) = (k-1)g_\chi - 1 + n\nu_2\left[\frac{k}{4}\right] + n\nu_3\left[\frac{k}{3}\right]. \tag{4.4}$$

Let

$$f(z) = \Delta(mz)^{1/n}/\Delta(z)^{1/n} \tag{4.5}$$

be the function used in §3. We see that $f(z)$ is an automorphic function with respect to Γ_χ. Let $q = e^{2\pi i z/n}$ (resp. q') be the uniformizing parameter at the cusp ∞ (resp. 0) of Γ_χ. We have

$$\mathrm{ord}_q(f(z)) = m-1, \qquad \mathrm{ord}_{q'}(f(z)) = -(m-1). \tag{4.6}$$

For a function F on $\mathfrak{H}$, $k \in \mathbf{Z}$ and $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbf{R})$, $\det g > 0$, we define a function $(F|_k\, g)(z)$ on $\mathfrak{H}$ by

$$(F|_k\, g)(z) = (\det g)^{k/2} F(gz)(cz+d)^{-k}, \qquad z \in \mathfrak{H}.$$

For $1 \leq i \leq n-1$, we set

$$S_k(\Gamma_0(m), \chi^i) = \{h \in S_k(\Gamma_\chi) \mid h|_k\, \gamma = \chi(\gamma)^i h, \quad \gamma \in \Gamma_0(m)\}.$$

Then we have a decomposition:

$$S_k(\varGamma_\chi) = S_k(\varGamma_0(m)) \oplus (\oplus_{i=1}^{n-1} S_k(\varGamma_0(m), \chi^i)) . \tag{4.7}$$

Let $\omega = \begin{pmatrix} 0 & 1 \\ -m & 0 \end{pmatrix}$. We have

$$\chi(\omega\gamma\omega^{-1}) = \chi(\gamma)^{-1} , \qquad \gamma \in \varGamma_0(m) . \tag{4.8}$$

Hence we see that ω normalizes $\varGamma_\chi$ and that the operator $|_k\,\omega$ gives an isomorphism of $S_k(\varGamma_0(m), \chi^i)$ onto $S_k(\varGamma_0(m), \chi^{-i})$.

Now we take $m = 2$, $n = 5$. We have $\nu_2 = 1$, $\nu_3 = 0$. By (4.3), we have $g_\chi = 0$. By (4.4), we have $\dim S_4(\varGamma_\chi) = 4$. Let

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) e^{2\pi i n z}$$

be the Eisenstein series of weight 4 with respect to SL(2, **Z**). Here $\sigma_3(n) = \sum_{0<d|n} d^3$. Put

$$g(z) = E_4(z) - 2^4 E_4(2z) . \tag{4.9}$$

Then $g(z)$ is a modular form of weight 4 with respect to $\varGamma_0(2)$ and we see that

$$\mathrm{ord}_q(g(z)) = 0 , \qquad \mathrm{ord}_{q'}(g(z)) = n .$$

In view of (4.6), $f(z)^i g(z) \in S_4(\varGamma_0(2), \chi^i) \subset S_4(\varGamma_\chi)$ for $1 \le i \le 4$. By (4.7), they are linearly independent. Therefore a basis of $S_4(\varGamma_\chi)$ is given by

$$\{f(z)g(z), f(z)^2 g(z), f(z)^3 g(z), f(z)^4 g(z)\} . \tag{4.10}$$

REMARK 4.1. We have

$$f(z)^i g(z)|_k\omega = f(z)^{5-i} g(z) , \qquad 1 \le i \le 4 .$$

Put $h(z) = E_4(z) - E_4(2z)$. Then we have

$$\mathrm{ord}_q(h(z)) = n , \qquad \mathrm{ord}_{q'}(h(z)) = 0 .$$

A basis of $S_4(\varGamma_\chi)$ is also given by

$$\{f(z)^{-1}h(z), f(z)^{-2}h(z), f(z)^{-3}h(z), f(z)^{-4}h(z)\} .$$

Using the fact $\dim S_4(\varGamma_0(2), \chi) = 1$, we can prove the relation

$$h(z) = -16 f(z)^5 g(z) .$$

REMARK 4.2. We have $\dim S_6(\varGamma_\chi) = 4$ and a basis of this space can be given similarly. We have $\dim S_8(\varGamma_\chi) = 9$, $\dim S_8(\varGamma_0(2)) = 1$. For $1 \le i \le 4$, a basis of $S_8(\varGamma_0(2), \chi^i)$ is given by $\{f(z)^i g(z)^2, f(z)^i g(z) E_4(z)\}$ and $f(z)^5 g(z)^2$ spans $S_8(\varGamma_0(2))$ (cf. (4.7)).

REMARK 4.3. It would be interesting to examine the example of this section in more detail in view of the Atkin-Swinnerton-Dyer congruences (cf. [AS], [Sc1], [Sc2]).

§5. Generators and relations for a Hilbert modular group

Let F be a real quadratic field and ϵ be the fundamental unit of F. Let $\{1, \omega\}$ be an integral basis of $\mathcal{O}_F$, i.e., $\mathcal{O}_F = \mathbf{Z} \oplus \mathbf{Z}\omega$. We write

$$\epsilon^2 = A + B\omega\,, \qquad \epsilon^2\omega = C + D\omega\,. \tag{5.1}$$

We put $\Gamma = \mathrm{PSL}(2, \mathcal{O}_F)$, $\widetilde{\Gamma} = \mathrm{SL}(2, \mathcal{O}_F)$,

$$\widetilde{P} = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \middle|\, a \in E_F, b \in \mathcal{O}_F \right\}, \qquad P = \widetilde{P}/\{\pm 1_2\}\,.$$

We define elements of $\widetilde{\Gamma}$ by

$$\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mu = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \eta = \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}.$$

Then it is known that σ, μ, τ and η generate $\widetilde{\Gamma}$ (cf. Vaserštein [V]). This fact can be proved in elementary way if $\mathcal{O}_F$ is a Euclidean ring, $F = \mathbf{Q}(\sqrt{5})$ for example. We use same letters σ, μ, τ and η for their classes in Γ, since this will cause no confusion. Now we have relations among them:

(i) $$\sigma^2 = 1\,.$$

(ii) $$(\sigma\tau)^3 = 1\,.$$

(iii) $$(\sigma\mu)^2 = 1\,.$$

(iv) $$\tau\eta = \eta\tau\,.$$

(v) $$\mu\tau\mu^{-1} = \tau^A\eta^B\,.$$

(vi) $$\mu\eta\mu^{-1} = \tau^C\eta^D\,.$$

If we can take $\omega = \epsilon$ and $-\epsilon^{-1} = A' + B'\epsilon$, then we have

(vii) $$\sigma\eta\sigma = \tau^{A'}\eta^{B'}\sigma\eta^{-1}\mu\,.$$

The relations (ii) and (vii) follow from

$$\sigma \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \sigma = \begin{pmatrix} 1 & -t^{-1} \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} -t & 1 \\ 0 & -t^{-1} \end{pmatrix}, \quad t \in E_F\,. \tag{5.2}$$

It is easy to see that μ, τ and η generate P and (iv)~(vi) are their fundamental relations.

The purpose of this section is to prove the following theorem.

THEOREM 5.1. *Let $F = \mathbf{Q}(\sqrt{5})$ and $\Gamma = \mathrm{PSL}(2, \mathcal{O}_F)$. We take $\omega = \epsilon$. The fundamental relations satisfied by the generators σ, μ, τ and η are* (i)~(vii).

We note that if $F = \mathbf{Q}(\sqrt{5})$ then $A = 1$, $B = 1$, $C = 1$, $D = 2$, $A' = 1$, $B' = -1$. The relations (i) to (vi) and (5.2) hold for any real quadratic field. Our theorem states that the minimal relations are enough when $F = \mathbf{Q}(\sqrt{5})$. This minimality will be satisfied by some more real quadratic fields with small discriminants but will not hold in general.

We begin by preliminary considerations on generators and relations of Γ.[5] Since Γ is generated by P and σ, every relation among elements of P and σ takes the form

$$p_1\sigma p_2\sigma \cdots p_m\sigma = 1\,, \qquad p_i \in P\,,\ 1 \le i \le m\,.$$

Using (i) and (iii)~(vi), this relation can be written as

$$\begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & x_2 \\ 0 & 1 \end{pmatrix} \sigma \cdots \begin{pmatrix} 1 & x_m \\ 0 & 1 \end{pmatrix} \sigma = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}, \quad x_i \in \mathcal{O}_F,\ u \in E_F\,.$$

We call a relation of this type an *m terms relation* counting the number of σ involved.

LEMMA 5.2. *Using relations* (i) *and* (iii)~(vi), *every three terms relation can be reduced to* (5.2).

proof. If we have a two terms relation

$$\begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & x_2 \\ 0 & 1 \end{pmatrix} \sigma = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix},$$

we have $x_1 = x_2 = 0$, $u = \pm 1$. Hence the two terms relation reduces to (i) . Let

$$\begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & x_2 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & x_3 \\ 0 & 1 \end{pmatrix} \sigma = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$$

be a three terms relation. Then we see that $x_2 = \pm u \in E_F$. Using (5.2), we have $\sigma \left(\begin{smallmatrix} 1 & x_2 \\ 0 & 1 \end{smallmatrix}\right) \sigma = p_1\sigma p_2$ with some p_1, $p_2 \in P$ and the three terms relation in question reduces to a two terms relation. This completes the proof.

LEMMA 5.3. *Assume that we can take* $\omega = \epsilon$. *The relation* (5.2) *can be reduced to the relations* (i)~(vii). *In other words*, *the relation* (5.2) *for* $t \in E_F$ *can be reduced to the relations* (5.2) *for* $t = 1, \epsilon$ *using relations* (i) *and* (iii)~(vi).

proof. We write the relation (5.2) as $\{t\}$. Using (i), the relation (iii) implies the relation $\left(\begin{smallmatrix} u & 0 \\ 0 & u^{-1} \end{smallmatrix}\right) \sigma = \sigma \left(\begin{smallmatrix} u^{-1} & 0 \\ 0 & u \end{smallmatrix}\right)$ for $u \in E_F$. Then we obtain the relation $\{-t\}$ taking the inverse of the both sides of (5.2), using (i), (iv)~(vi). Taking the conjugate by μ of both sides of (5.2), we obtain the relation $\{\epsilon^{-2}t\}$ using (i), (iii)~(vi). Since E_F is generated by ϵ and ± 1, this completes the proof.

Next we consider the four terms relation.

$$\begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & x_2 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & x_3 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & x_4 \\ 0 & 1 \end{pmatrix} \sigma = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \tag{5.3}$$

We write the relation (5.3) as $\{x_1, x_2, x_3, x_4; u\}$.

LEMMA 5.4. *The four terms relation* (5.3) *reduces to* (i)~(vi) *and* (5.2) *if* $x_i \in E_F$ *for some* i, $1 \le i \le 4$.

---

[5]For this part, we do not assume $F = \mathbf{Q}(\sqrt{5})$.

proof. Suppose that $x_2 \in E_F$. By (5.2), we have $\sigma \begin{pmatrix} 1 & x_2 \\ 0 & 1 \end{pmatrix} \sigma = p_1 \sigma p_2$ with some p_1, $p_2 \in P$. Using this expression, we find that (5.3) reduces to a three terms relation. We write (5.3) as

$$\begin{pmatrix} 1 & x_2 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & x_3 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & x_4 \\ 0 & 1 \end{pmatrix} \sigma = \sigma \begin{pmatrix} 1 & -x_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} .$$

Using (i)∼(vi), the right-hand side can be written as $\begin{pmatrix} u^{-1} & 0 \\ 0 & u \end{pmatrix} \sigma \begin{pmatrix} 1 & -u^{-2}x_1 \\ 0 & 1 \end{pmatrix}$. Hence $\{x_1, x_2, x_3, x_4; u\}$ is equivalent to $\{x_2, x_3, x_4, u^{-2}x_1; u^{-1}\}$ under (i)∼(vi). By this cyclic rotation, any x_i can be brought to the second position at the cost of multiplying by a unit. Hence the assertion follows.

For $u \in E_F$, $x \in \mathcal{O}_F$, we have the relation

$$\begin{aligned} &\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & (1-u)/x \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & -x/u \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & -u(1-u)/x \\ 0 & 1 \end{pmatrix} \sigma \\ &\quad = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \end{aligned} \tag{5.4}$$

if x divides $u - 1$.

LEMMA 5.5. *Under* (i)∼(vi) *and* (5.2), *the four terms relation* (5.3) *can be reduced to* (5.4) *with some x and u.*

proof. We see easily that the four terms relation (5.3) is equivalent to a relation of the form

$$\sigma \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \sigma = \begin{pmatrix} 1 & y_1 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} h & 0 \\ 0 & h^{-1} \end{pmatrix} . \tag{5.3$'$}$$

Here x, $y_i \in \mathcal{O}_F$, $1 \le i \le 3$ and $h \in E_F$. By a direct computation, we get

$$h(y_1 y_2 - 1) = -\omega\,, \qquad h y_2 = \omega x\,, \qquad h^{-1}(y_2 y_3 - 1) = -\omega\,,$$

where $\omega = \pm 1$. Putting $u = \omega h^{-1}$, we have

$$y_2 = ux\,, \qquad y_1 = \frac{1-u}{ux}\,, \qquad y_3 = \frac{1-u^{-1}}{ux}\,.$$

Hence we see that x divides $u - 1$ and that (5.3$'$) is equivalent to

$$\begin{aligned} &\sigma \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \sigma \\ &\quad = \begin{pmatrix} 1 & (1-u)/ux \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & ux \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & (1-u^{-1})/ux \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u^{-1} & 0 \\ 0 & u \end{pmatrix} . \end{aligned} \tag{5.3$''$}$$

On the other hand, under (i)∼(vi), (5.4) is equivalent to

$$\begin{aligned} &\sigma \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \sigma \\ &\quad = \begin{pmatrix} 1 & (1-u)/x \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & -x/u \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & -u(1-u)/x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} . \end{aligned} \tag{5.4$'$}$$

We obtain (5.3″) from (5.4′) by substituting x by $-x$ and u by u^{-1}. This completes the proof.

We denote the four terms relation (5.4) by $\{x, u\}$. We have $\{x, u\} = \{x, (1-u)/x, -x/u, -u(1-u)/x; u\}$. Under (i)∼(vi), the relation of the form (5.3′) is equivalent to $\{x, u\}$ and the relation $\{x_1, x_2, x_3, x_4; u\}$ is equivalent to $\{x_2, x_3, x_4, u^{-2}x_1; u^{-1}\}$ (cf. the proofs of Lemmas 5.4 and 5.5). Therefore $\{x, u\}$ is equivalent to $\{(1-u)/x, u^{-1}\}$ under (i)∼(vi). By Lemma 5.4, $\{x, u\}$ is reducible to (i)∼(vi) and (5.2) if $x \in E_F$ or $(1-u)/x \in E_F$.

LEMMA 5.6. *Assuming* (i)∼(vi) *and* (5.2), *the following assertions hold.*

(1) $\{x, u\}$ *is equivalent to* $\{-x, u^{-1}\}$.
(2) $\{x, u\}$ *is equivalent to* $\{t^2x, u\}$ *for every* $t \in E_F$.
(3) *We assume the four terms relation* $\{x, u\}$. *Then* $\{x, u^e\}$ *is equivalent to* $\{u^e x, u^{1-e}\}$ *for* $e \in \mathbf{Z}$.
(4) $\{x, u\}$ *is equivalent to* $\{(1-u)/x, u^{-1}\}$.
(5) *Suppose that* $(x) = (2)$. *Then* $\{x, u\}$ *is equivalent to* $\{x, -u\}$.

proof. We write $\{-x, u^{-1}\}$ in the form of (5.3″). Taking the inverses of both sides, we obtain (1). We obtain (2) taking the conjugates of both sides by $\begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix}$. To prove (3), we set the right-hand side of (5.3″) is equal for $\{x, u\}$ and for $\{x, u^e\}$. By a simple computation, we find that the resulting equality is

$$\begin{aligned}\sigma \begin{pmatrix} 1 & u^e x \\ 0 & 1 \end{pmatrix} \sigma \\ = \begin{pmatrix} 1 & (u^{e-1}-1)/u^e x \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & ux \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & (u^{-1}-u^{e-2})/x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u^{e-1} & 0 \\ 0 & u^{1-e} \end{pmatrix},\end{aligned}$$

which is $\{u^e x, u^{1-e}\}$. Hence we obtain (3). We noted (4) already in the discussion before Lemma 5.6. To prove (5), we set the right-hand side of (5.3″) is equal for $\{x, u\}$ and for $\{x, -u\}$. The resulting equality is

$$\begin{aligned}\sigma \begin{pmatrix} 1 & ux \\ 0 & 1 \end{pmatrix} \sigma \\ = \begin{pmatrix} 1 & -2/ux \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & -ux \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1 & -2/ux \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\end{aligned}$$

Since $-2/ux \in E_F$, this relation reduces to a three terms relation by Lemma 5.4. In view of Lemma 5.2, this completes the proof.

REMARK 5.7. Suppose that $(1-u)/x \in E_F$. Then, by Lemma 5.4, $\{tx, u\}$ can be reduced to (i)∼(vi) and (5.2) for every $t \in E_F$. By (1) and (3) of Lemma 5.6, we see that $\{x, u^e\}$ can be reduced to (i)∼(vi) and (5.2) for all $e \in \mathbf{Z}$.

The following Lemma is of some interest though it will not be used in this paper.

LEMMA 5.8. *Suppose that there exist sequences of integers* $x_0, x_1, \ldots, x_k \in \mathcal{O}_F$ *and units* $u_0, u_1, \ldots, u_k \in E_F$ *such that*

$$x_{i-1}x_i = 1 - u_i, \quad 1 \le i \le k.$$

We assume that $u_i = u_{i-1}^{m_i}$, $1 \le i \le k$ *with a nonzero integer* m_i. *If* $(1-u_0)/x_0 \in E_F$, *then the four terms relation* $\{x_k, u_k\}$ *reduces to* (i)∼(vi) *and* (5.2).

proof. Using Lemma 5.6, the reducibility of $\{tx_i, u_i^e\}$, $t \in E_F$, $e \in \mathbf{Z}$ can be shown easily by induction on i.

Let G be a group with generators $\sigma_1, \dots, \sigma_m$. Let $\mathcal{F}$ be a free group on the free generators $\widetilde{\sigma}_1, \dots, \widetilde{\sigma}_m$. Then we can define a surjective homomorphism $\pi : \mathcal{F} \longrightarrow G$ by $\pi(\widetilde{\sigma}_i) = \sigma_i$, $1 \le i \le m$. Let R be the kernel of π. Next let S be a finite subset of G which generates G. For $\gamma \in S$, we prepare a symbol $[\gamma]$ and let $\mathcal{F}'$ be the free group on the free generators $[\gamma]$, $\gamma \in S$. We can define a surjective homomorphism $\pi' : \mathcal{F}' \longrightarrow G$ by $\pi'([\gamma]) = \gamma$, $\gamma \in S$. Let R' be the kernel of π'. Clearly $([\gamma_1][\gamma_2])^{-1}[\gamma_1\gamma_2] \in R'$ if $\gamma_1, \gamma_2, \gamma_1\gamma_2 \in S$. We assume that R' is generated by the elements of this form and their conjugates.

Now for every $\gamma \in S$, we take and fix an expression

$$\gamma = \sigma_{i_1}^{\epsilon_1} \cdots \sigma_{i_k}^{\epsilon_k}, \qquad i_j \in [1, m], \quad \epsilon_j = \pm 1$$

and put $\widetilde{\gamma} = \widetilde{\sigma}_{i_1}^{\epsilon_1} \cdots \widetilde{\sigma}_{i_k}^{\epsilon_k}$. (If $\gamma = \sigma_i \in S$, we put $\widetilde{\gamma} = \widetilde{\sigma}_i$.) By the universality of the free group, there exists a homomorphism $\varphi : \mathcal{F}' \longrightarrow \mathcal{F}$ which satisfies $\varphi([\gamma]) = \widetilde{\gamma}$, $\gamma \in S$. Then we have $\pi' = \pi \circ \varphi$. Let R_0 be the normal subgroup of $\mathcal{F}$ generated by $(\widetilde{\gamma}_1\widetilde{\gamma}_2)^{-1}\widetilde{\gamma_1\gamma_2}$, $\gamma_1, \gamma_2, \gamma_1\gamma_2 \in S$ and their conjugates. We have $R_0 \subset R$. Since $\varphi(R') \subset R_0$ by the assumption, φ induces the homomorphism $\bar{\varphi} : \mathcal{F}'/R' \longrightarrow \mathcal{F}/R_0$ which satisfies $\bar{\varphi}(g \mod R') = \varphi(g) \mod R_0$, $g \in \mathcal{F}'$.

LEMMA 5.9. *Let the notation be the same as above. If* $\sigma_i \in S$, $1 \le i \le m$, *then we have* $R_0 = R$.

proof. Define a homomorphism $\pi_0 : \mathcal{F}/R_0 \longrightarrow G$ by $\pi_0(h \mod R_0) = \pi(h)$, $h \in \mathcal{F}$. Since $(\pi_0 \circ \bar{\varphi})(g \mod R') = (\pi \circ \varphi)(g) = \pi'(g)$, $g \in \mathcal{F}'$, $\pi_0 \circ \bar{\varphi}$ is injective. Hence $\pi_0|\bar{\varphi}(\mathcal{F}'/R')$ is injective. We can write $\bar{\varphi}(\mathcal{F}'/R') = H/R_0$ with a subgroup H of $\mathcal{F}$. Now the assumption of the Lemma implies $H = \mathcal{F}$. Therefore π_0 is injective and we obtain $R_0 = R$.

For the proof of Theorem 5.1, we use the following theorem of Macbeath (cf. Theorem 1 of [M] and also Theorem 1.1 of [Sw]).

THEOREM M. *Let* X *be a path connected Hausdorff topological space and* Γ *be a group which acts on* X *as homeomorphisms. We assume that the fundamental group* $\pi_1(X)$ *of* X *is trivial. Let* V *be a path connected open subset of* X *such that* $X = \Gamma V$. *Define a subset* S *of* Γ *by*

$$S = \{\gamma \in \Gamma \mid V \cap \gamma V \neq \emptyset\}.$$

Then S *generates* Γ.[6] *Let* $\mathcal{F}$ *be the free group which has the symbols* $[\sigma]$, $\sigma \in S$ *as free generators. Define a homomorphism* $\pi : \mathcal{F} \longrightarrow \Gamma$ *by* $\pi([\sigma]) = \sigma$. *Let* R *be the kernel of* π. *Then* R *is generated by* $([\sigma][\tau])^{-1}[\sigma\tau]$ *and their conjugates, where* σ *and* τ *are elements of* S *which satisfy*

$$(*) \qquad V \cap \sigma V \cap \sigma\tau V \neq \emptyset.$$

[6] This fact is an old result of Siegel, cf. [Si1].

In other words, Γ has a presentation $\Gamma = \mathcal{F}/R$.

Swan ([Sw]) generalized this theorem to the case where $\pi_1(X) \neq 1$ and obtained generators and relations for $\mathrm{SL}(2, \mathcal{O}_K)$, for several imaginary quadratic fields K with small discriminants.

Let the notation be the same as in Theorem M. For a subset T of X, we put

$$S(T) = \{\gamma \in \Gamma \mid T \cap \gamma T \neq \emptyset\}.$$

Let D be a closed subset of X such that $\Gamma D = X$.

LEMMA 5.10. *Suppose in addition that the topological space X is normal. Then we have*

$$\cap_{U \supset D,\ U \text{ is open}} S(U) = S(D).$$

proof. Clearly the left-hand side contains the right-hand side. Pick an element γ of the left-hand side. Assume that $D \cap \gamma D = \emptyset$. Since X is normal, we can find open subsets U and U' of X so that

$$U \supset D, \qquad U' \supset \gamma D, \qquad U \cap U' = \emptyset.$$

Put $U'' = U \cap \gamma^{-1} U'$. Then we have $U'' \supset D$, $U'' \cap \gamma U'' \subset U \cap U' = \emptyset$. This is a contradiction and we complete the proof.

Next we assume that $S(D)$ is finite and that $S(U)$ is finite for an open set U which contains D. We put

$$S(D) = \{\gamma_1, \ldots, \gamma_m\}, \qquad S(U) = \{\gamma_1, \ldots, \gamma_m, \gamma_{m+1}, \ldots, \gamma_n\}$$

assuming $S(U) \supsetneqq S(D)$. By Lemma 5.10, for every γ_i, $i > m$, there exists an open set $U_i \supset D$ such that $\gamma_i \notin S(U_i)$. Put $V = U \cap (\cap_{i=m+1}^{n} U_i)$. Then we have $\gamma_i \notin S(V)$. Therefore we conclude that $S(D) = S(V)$ for an open set V which contains D. This means that we may replace S to $S(D)$ in Theorem M if such a V is path connected. (Note that in Theorem M, $([\sigma][\tau])^{-1}[\sigma\tau] \in R$ for $\sigma, \tau \in S$ such that $\sigma\tau \in S$. Thus the condition $(*)$ may be dropped. However $(*)$ reduces the number of relations and can be essential for the practical purpose.)

Now let F be a totally real field of degree n. Let us review the fundamental domain of $\Gamma = \mathrm{PSL}(2, \mathcal{O}_F)$ acting on $\mathfrak{H}^n$ (cf. [Si2]). Let $\sigma_1, \ldots, \sigma_n$ be all the isomorphisms of F into $\mathbf{R}$. For $a \in F$, we put $a^{(i)} = a^{\sigma_i}$. Take an integral basis of $\mathcal{O}_F$ so that

$$\mathcal{O}_F = \mathbf{Z}\omega_2 + \mathbf{Z}\omega_2 + \cdots + \mathbf{Z}\omega_n$$

and let $\epsilon_1, \ldots, \epsilon_{n-1}$ be generators of a free part of E_F. For $x = (x_1, \ldots, x_n) \in \mathbf{C}^n$, we put $N(x) = x_1 \cdots x_n$. For simplicity, we assume that the class number of F is one. Take $z = (z_1, \ldots, z_n) \in \mathfrak{H}^n$. Put $z_j = x_j + iy_j$, $x_j, y_j \in \mathbf{R}$. We define the local coordinates of z relative to the cusp ∞ by the formulas (cf. [Si2], p. 249)

$$Y_1 \log|\epsilon_1^{(k)}| + \cdots + Y_{n-1} \log|\epsilon_{n-1}^{(k)}| = \frac{1}{2} \log \frac{y_k}{\sqrt[n]{N(y)}}, \qquad 1 \leq k \leq n-1. \tag{5.5}$$

$$X_1 \omega_1^{(l)} + \cdots + X_n \omega_n^{(l)} = x_l, \qquad 1 \leq l \leq n. \tag{5.6}$$

Here $y = (y_1, \dots, y_n)$. We put

$$D_\infty = \left\{ z \in \mathfrak{H}^n \mid -\frac{1}{2} \le Y_i < \frac{1}{2}\,,\ 1 \le i \le n-1\,, \quad -\frac{1}{2} \le X_j < \frac{1}{2}\,,\ 1 \le j \le n \right\}.$$

Then D_∞ is a fundamental domain of P. (P is the subgroup of Γ consisting of all elements which are represented by upper triangular matrices.) We define

$$D = \{ z \in \overline{D_\infty} \mid N(|cz+d|) \ge 1 \text{ whenever } c \text{ and } d \text{ are relatively prime integers of } \mathcal{O}_F \}\,. \tag{5.7}$$

Here $\overline{D_\infty}$ denote the closure of D_∞ and $|cz+d| = (|c^{(1)}z_1 + d^{(1)}|, \dots, |c^{(n)}z_n + d^{(n)}|)$. Then D satisfies that (cf. [Si2], p. 266–268):

(1) D is a closed subset of $\mathfrak{H}^n$ such that $\Gamma D = \mathfrak{H}^n$.

(2) Two distinct interior points of D cannot be transformed each other by an element of Γ.

(3) There are only finitely many $\gamma \in \Gamma$ such that $D \cap \gamma D \ne \emptyset$. Furthermore D and γD, $\gamma \ne 1$ can intersect only on the boundary of D.

Now we assume that $[F : \mathbf{Q}] = 2$. We may assume that $\omega_1 = 1$, $\omega_2 = \omega$, $\epsilon^{(1)} = \epsilon$. Then we have

$$D = \Bigg\{ z \in \mathfrak{H}^2 \mid \epsilon^{-2} \le \frac{y_2}{y_1} \le \epsilon^2\,, \quad -\frac{1}{2} \le \frac{1}{\omega - \omega'}(\omega' x_1 - \omega x_2) \le \frac{1}{2}\,, \quad -\frac{1}{2} \le \frac{1}{\omega - \omega'}(x_1 - x_2) \le \frac{1}{2}\,, \quad N(|cz+d|) \ge 1 \text{ whenever } c \text{ and } d \text{ are relatively prime integers of } \mathcal{O}_F \Bigg\}\,. \tag{5.8}$$

Here ω' denotes the conjugate of ω.

Hereafter in this section, we assume that $F = \mathbf{Q}(\sqrt{5})$. We take $\omega = \epsilon$. The next lemma is the essential ingredient of the proof of Theorem 5.1.

LEMMA 5.11. *Let $F = \mathbf{Q}(\sqrt{5})$ and take $\omega = \epsilon$. Put $S = \{\gamma \in \Gamma \mid D \cap \gamma D \ne \emptyset\}$. Then S is a finite set and we have $S \subset S_0 \sqcup S_1 \sqcup S_2$, where*

$$S_0 = P\,, \qquad S_1 = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ c \in E_F \right\},$$

$$S_2 = \left\{ \gamma = \begin{pmatrix} \pm\epsilon^3 & b \\ 2\epsilon & \pm\epsilon^3 \end{pmatrix}, \quad \begin{pmatrix} \pm 1 & b \\ 2\epsilon^{-2} & \pm 1 \end{pmatrix} \right\}.$$

Here $\pm$ can be taken arbitrarily and $b \in \mathcal{O}_F$ is chosen so that $\det\gamma = 1$. *(S_2 consists of eight elements.)*

We give a proof of Theorem 5.1 *assuming Lemma* 5.11.

PROOF OF THEOREM 5.1. We consider $\mathfrak{H}^2 \subset \mathbf{C}^2$ and let d denote the Euclidean metric induced by this embedding. For $\delta > 0$, we put

$$D_\delta = \{ z \in \mathfrak{H}^2 \mid d(z, D) < \delta \}\,.$$

We see easily that D is path connected. Let $z \in D_\delta$. Then there exists $z_1 \in D$ such that $d(z, z_1) < \delta$. Hence z is connected by a path to z_1. Therefore D_δ is path connected. By using the argument of Lemma 5.10, we see that $\cap_{\delta>0} S(D_\delta) = S$. Moreover we can show without difficulty that $S(D_\delta)$ is finite when δ is sufficiently small. Therefore $S(D_\delta) = S$ when δ is sufficiently small and Theorem M can be applied with S given in Lemma 5.11.

For $\gamma \in S$, we prepare a symbol $[\gamma]$ and consider the free group $\mathcal{F}'$ on the free generators $[\gamma]$. By Theorem M, it is sufficient to show that $[\gamma_2]^{-1}[\gamma_1]^{-1}[\gamma_1\gamma_2]$, $\gamma_1, \gamma_2, \gamma_1\gamma_2 \in S$ can be reduced to a three term relation. We put $S'_i = S \cap S_i$, $0 \le i \le 2$. We can check easily that $\sigma, \mu, \tau, \eta \in S$. Hence Lemma 5.9 is applicable. Let $\mathcal{F}$ be the free group on the free generators $\widetilde{\sigma}$, $\widetilde{\mu}$, $\widetilde{\tau}$ and $\widetilde{\eta}$. We define a homomorphism $\pi : \mathcal{F} \longrightarrow \Gamma$ by $\pi(\widetilde{\sigma}) = \sigma$, $\pi(\widetilde{\mu}) = \mu$, $\pi(\widetilde{\tau}) = \tau$, $\pi(\widetilde{\eta}) = \eta$. For $\gamma \in S$, we define $\widetilde{\gamma} \in \mathcal{F}$ such that $\pi(\widetilde{\gamma}) = \gamma$ as follows.

If $\gamma \in P$, we write $\gamma = \mu^a\tau^b\eta^c$. Then we define $\widetilde{\gamma} = \widetilde{\mu}^a\widetilde{\tau}^b\widetilde{\eta}^c$. In particular, this rule applies to an element $\gamma \in S'_0$. We have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & c^{-1}a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -c & -d \\ 0 & -c^{-1} \end{pmatrix}, \qquad c \in E_F . \tag{5.9}$$

Hence $\gamma \in S'_1$ can be written as $\gamma = p_1\sigma p_2$, $p_1, p_2 \in P$. We fix such an expression and define $\widetilde{\gamma} = \widetilde{p}_1\widetilde{\sigma}\widetilde{p}_2$. Suppose $\gamma \in S'_2$. We write γ in the form $\gamma = \begin{pmatrix} u & \beta \\ 2\epsilon^m & u^* \end{pmatrix}$, $u, u^* \in E_F$, $\beta \in \mathcal{O}_F$, $m \in \mathbf{Z}$. We have

$$\begin{pmatrix} u & \beta \\ 2\epsilon^m & u^* \end{pmatrix} = \sigma\begin{pmatrix} 1 & -2u^{-1}\epsilon^m \\ 0 & 1 \end{pmatrix}\sigma\begin{pmatrix} -u & -\beta \\ 0 & -u^{-1} \end{pmatrix}. \tag{5.10}$$

We fix this expression $\gamma = \sigma p_1\sigma p_2$, $p_1, p_2 \in P$ and define $\widetilde{\gamma} = \widetilde{\sigma}\widetilde{p}_1\widetilde{\sigma}\widetilde{p}_2$.

By Lemma 5.9, it is sufficient to show that $\widetilde{\gamma}_2^{-1}\widetilde{\gamma}_1^{-1}\widetilde{\gamma_1\gamma_2}$ reduces to a three terms relation (under (i)$\sim$(vi) and (5.2)) when $\gamma_1, \gamma_2, \gamma_1\gamma_2 \in S$. We see that there cannot arise the case where all of $\gamma_1, \gamma_2, \gamma_1\gamma_2$ belong to S'_2, by inspecting the (2, 1)-component of $\gamma_1\gamma_2$. This implies that if two of $\gamma_1, \gamma_2, \gamma_1\gamma_2$ belong to S'_2, then the other one must belong to S'_0. Therefore $\widetilde{\gamma}_2^{-1}\widetilde{\gamma}_1^{-1}\widetilde{\gamma_1\gamma_2}$ defines at most a four terms relation. We may assume that $\widetilde{\gamma}_2^{-1}\widetilde{\gamma}_1^{-1}\widetilde{\gamma_1\gamma_2}$ defines a four terms relation. Then one of $\gamma_1, \gamma_2, \gamma_1\gamma_2$ belongs to S'_2. By (5.10), this relation takes the form (5.3′) with $x \in \mathcal{O}_F$ such that $(x) = (2)$. As shown in the proof of Lemma 5.5, it suffices to consider the four terms relation $\{x, u\}$ for $u \in E_F$ such that x divides $u - 1$. Now the group $E_{(2)} = \{u \in E_F \mid u \equiv 1 \mod 2\}$ is generated by -1 and ϵ^3. By $\epsilon^3 - 1 = 2\epsilon$ and Remark 5.7, we see that $\{x, \epsilon^{3e}\}$ is reducible to (i)$\sim$(vi) and (5.2) for $e \in \mathbf{Z}$. By Lemma 5.6, (5), $\{x, -\epsilon^{3e}\}$ is reducible to (i)$\sim$(vi) and (5.2). This completes the proof.

Now we are going to prove Lemma 5.11. We consider an element $\gamma \in \Gamma$ such that for a point $z \in D$, $\gamma z \in D$ holds, i.e., $D \cap \gamma^{-1}D \neq \emptyset$.[7] We put $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $z' = \gamma z$, $z' = (z'_1, z'_2)$, $z'_j = x'_j + iy'_j$, $j = 1, 2$, $y' = (y'_1, y'_2)$. We have

$$N(y') = \frac{N(y)}{N(|cz + d|)^2}\,.$$

[7]Since S_i, $i = 0, 1, 2$ is stable under $\gamma \mapsto \gamma^{-1}$, it suffices to determine γ which satisfies $D \cap \gamma^{-1}D \neq \emptyset$.

Hence $N(y') \le N(y)$. Changing the roles of z and z', we have $N(y) \le N(y')$. Hence we see that $N(y') = N(y)$ and

$$N(|cz+d|) = 1\,. \tag{5.11}$$

Since we are assuming that $F = \mathbf{Q}(\sqrt{5})$, $\omega = \epsilon$, we have

$$x_1 = X_1 + \frac{1+\sqrt{5}}{2}X_2\,, \quad x_2 = X_1 + \frac{1-\sqrt{5}}{2}X_2\,, \quad -\frac{1}{2} \le X_1 \le \frac{1}{2},\ -\frac{1}{2} \le X_2 \le \frac{1}{2}\,.$$

Then $x_1 x_2 = X_1^2 - X_2^2 + X_1 X_2$ and we see that

$$|x_1 x_2| \le \frac{5}{16}\,, \qquad |x_1| \le \frac{3+\sqrt{5}}{4}\,, \qquad |x_2| \le \frac{1+\sqrt{5}}{4}\,. \tag{5.12}$$

Since $z \in D$, we have

$$N(|z|)^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2) \ge 1\,. \tag{5.13}$$

Put $k = y_1 y_2$. Since $\epsilon^{-2} \le y_1/y_2 \le \epsilon^2$, we have $\epsilon^{-1}\sqrt{k} \le y_1, y_2 \le \epsilon\sqrt{k}$. Then by (5.13), we have

$$k^2 + (x_1^2 + x_2^2)\epsilon^2 k + x_1^2 x_2^2 - 1 \ge 0\,.$$

We consider the equation with respect to t:

$$t^2 + (x_1^2 + x_2^2)\epsilon^2 t + x_1^2 x_2^2 - 1 = 0\,. \tag{5.14}$$

Let ξ be the positive root of (5.14) and let $\kappa^* = \min \xi$. Here the minimum is taken with respect to X_1 and X_2, regarding x_1 and x_2 as the functions of X_1 and X_2; X_1 and X_2 extend over the domain $-1/2 \le X_1, X_2 \le 1/2$. Let κ be the positive root of the equation

$$t^2 + \frac{7(3+\sqrt{5})}{8}t - \frac{15}{16} = 0\,.$$

This is the positive root of (5.14) when $X_1 = X_2 = 1/2$, $x_1 = (3+\sqrt{5})/4$, $x_2 = (3-\sqrt{5})/4$. We have $\kappa = 0.19622\cdots$. By elementary but somewhat tedious calculation, which we omit the details, we can show that $\kappa^* = \kappa$. Hence we have

$$y_1 y_2 \ge \kappa = 0.19622\cdots\,. \tag{5.15}$$

If $c = 0$, then $\gamma \in S_0$. It suffices to show that $\gamma \in S_1 \sqcup S_2$ assuming $c \neq 0$. By (5.11), we have

$$|N(c)| y_1 y_2 \le 1\,. \tag{5.16}$$

By (5.15), we have $|N(c)| \le 1/\kappa$. Therefore $|N(c)| = 1$ or 4 or 5. If $|N(c)| = 1$, then $c \in E_F$ and $\gamma \in S_1$. Hereafter we assume $|N(c)| = 4$ or 5. By (5.15) and (5.16), noting $\epsilon^{-2} \le y_1/y_2 \le \epsilon^2$, we obtain

$$\epsilon^{-1}\sqrt{\kappa} \le y_1, y_2 \le \frac{\epsilon}{\sqrt{|N(c)|}}\,. \tag{5.17}$$

Since $N(|z|) \ge 1$, we have $(x_1^2 + y_1^2)(x_2^2 + y_2^2) \ge 1$. Using $y_1 y_2 \le 1/|N(c)|$, we have

$$x_1^2 y_2^4 - \left(1 - x_1^2 x_2^2 - \frac{1}{N(c)^2}\right) y_2^2 + \frac{x_2^2}{N(c)^2} \ge 0\,. \tag{5.18}$$

If $x_1 = 0$, we obtain

$$y_1^2 x_2^2 \geq 1 - \frac{1}{N(c)^2} \geq 1 - \frac{1}{16}$$

from $N(|z|) \geq 1$ and (5.16). By (5.12), we have

$$y_1 \geq \sqrt{1 - \frac{1}{16}} \cdot \frac{2}{\epsilon} = 1.19681 \cdots .$$

This contradicts (5.17). Hence we have $x_1 \neq 0$.

First we exclude the case $|N(c)| = 5$. To this end, we assume $|N(c)| = 5$ and consider the equation (cf. (5.18))

$$x_1^2 t^2 - \left(1 - x_1^2 x_2^2 - \frac{1}{25}\right) t + \frac{x_2^2}{25} = 0 . \tag{5.19}$$

Let $f(t)$ be the polynomial of t on the left-hand side. For $t_0 = \epsilon^{-2}\kappa$, we have

$$f(t_0) \leq \left(\frac{\epsilon+1}{2}\right)^2 t_0^2 - \left(1 - \frac{25}{256} - \frac{1}{25}\right) t_0 + \frac{1}{25}\left(\frac{\epsilon}{2}\right)^2 = -0.02882 \cdots < 0$$

using (5.12). Let $\eta_1 > \epsilon^{-2}\kappa > \eta_2$ be the roots of the equation (5.19). By (5.17) and (5.18), we must have $y_2 \geq \sqrt{\eta_1}$. We note that (cf. (5.17))

$$y_1, y_2 \leq \frac{\epsilon}{\sqrt{5}} = 0.72360 \cdots . \tag{5.20}$$

We consider η_1 as a function of X_1 and X_2 defined in the domain $-1/2 \leq X_1, X_2 \leq 1/2$. First we consider η_1 on the subdomain defined by the condition $x_1 > 0$. It is not difficult to check that η_1 is monotone decreasing with respect to the both arguments X_1 and X_2. For $X_1 = 1/2$, $X_2 = 0.4985$, we have $\sqrt{\eta_1} = 0.72377 \cdots$. For $X_1 = 0.4985$, $X_2 = 1/2$, we have $\sqrt{\eta_1} = 0.72389 \cdots$. In view of (5.20), we must have $X_1, X_2 > 0.4985$. Similarly, in the subdomain $x_1 < 0$, we must have $X_1, X_2 < -0.4985$.

First we consider the case $X_1, X_2 > 0.4985$. For relatively prime integers $\alpha, \beta \in \mathcal{O}_F$, we have (cf. (5.8)) $N(|\alpha z + \beta|) \geq 1$. Take $\alpha = 2$, $\beta = -\epsilon^2$. We have

$$|2x_1 - \epsilon^2| \leq 0.03(1+\epsilon) , \qquad |2x_2 - \epsilon^{-2}| \leq 0.03(1 + |\epsilon'|) .$$

Here $\epsilon' = (1 - \sqrt{5})/2$ is the conjugate of ϵ. Then we find

$$\begin{aligned} N(|2z - \epsilon^2|)^2 &= \{(2x_1 - \epsilon^2)^2 + 4y_1^2\}\{(2x_2 - \epsilon^{-2})^2 + 4y_2^2\} \\ &= 16 y_1^2 y_2^2 + 4y_1^2(2x_2 - \epsilon^{-2})^2 + 4y_2^2(2x_1 - \epsilon^2)^2 + (2x_1 - \epsilon^2)^2(2x_2 - \epsilon^{-2})^2 \\ &\leq \frac{16}{25} + 4y_1^2\{0.03(1+\epsilon)\}^2 + 4y_2^2\{0.03(1+|\epsilon'|)\}^2 \\ &\quad + \{0.03(1+\epsilon)\}^2\{0.03(1+|\epsilon'|)\}^2 . \end{aligned}$$

Since $y_1, y_2 \leq 0.72360 \cdots$, this contradicts $N(|2z - \epsilon^2|) \geq 1$. When $X_1, X_2 < -0.4985$, we obtain a contradiction similarly by taking $\alpha = 2$, $\beta = \epsilon^2$. Thus we have shown that the case $|N(c)| = 5$ cannot occur.

It remains to show that $\gamma \in S_2$ assuming $|N(c)| = 4$. We can write $c = \pm 2\epsilon^m$ with $m \in \mathbf{Z}$. Changing γ to $-\gamma$ if necessary, we may assume that $c = 2\epsilon^m$. We put

$z' = (z'_1, z'_2) = \gamma z$, $z'_j = x'_j + iy'_j$, $j = 1, 2$. Since $z = \gamma^{-1}z'$, $\gamma^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, the estimate (5.17) holds also for y'_1 and y'_2. We have

$$\epsilon^{-1}\sqrt{\kappa} = 0.27376\cdots \le y_1, y_2, y'_1, y'_2 \le \frac{\epsilon}{\sqrt{|N(c)|}} = 0.80901\cdots . \tag{5.21}$$

We have

$$|c^{(j)}z_j + d^{(j)}|^2 = \frac{y_j}{y'_j}, \qquad j = 1, 2 .$$

Hence we obtain

$$\epsilon^{-2}\sqrt{\kappa}\sqrt{|N(c)|} \le |c^{(j)}z_j + d^{(j)}|^2 \le \frac{\epsilon^2}{\sqrt{\kappa}\sqrt{|N(c)|}}, \qquad j = 1, 2 . \tag{5.22}$$

In particular, we have

$$(c^{(j)})^2 y_j^2 \le \frac{\epsilon^2}{\sqrt{\kappa}\sqrt{|N(c)|}}, \qquad j = 1, 2 .$$

Using (5.21), we obtain

$$|c^{(j)}| \le \epsilon^2\kappa^{-3/4}|N(c)|^{-1/4} = 6.27915\cdots, \qquad j = 1, 2 . \tag{5.23}$$

From (5.23), we obtain $m = 0, \pm 1, \pm 2$.

Next we are going to restrict possibilities of d. A preliminary table of listing all possible d can be obtained by (5.22) and (5.23). By (5.11) and (5.21), we have

$$\{(2\epsilon^m x_1 + d^{(1)})^2 + 4\epsilon^{2m}\cdot\epsilon^{-2}\kappa\}\{(2(\epsilon')^m x_2 + d^{(2)})^2 + 4\epsilon^{-2m}\cdot\epsilon^{-2}\kappa\} \le 1 . \tag{5.24}$$

We consider the equation (cf. (5.18))

$$x_1^2 t^2 - \left(1 - x_1^2 x_2^2 - \frac{1}{16}\right)t + \frac{x_2^2}{16} = 0 . \tag{5.25}$$

Let $g(t)$ be the polynomial of t on the left-hand side. For $t_0 = \epsilon^{-2}\kappa$, we can check $g(t_0) < 0$. Let $\eta_1 > t_0 > \eta_2$ be the roots of $g(t)$. By (5.18) and (5.21), we have $y_2 \ge \sqrt{\eta_1}$. As in the case where $|N(c)| = 5$, we consider η_1 as a function of X_1 and X_2 defined in the domain $-1/2 \le X_1, X_2 \le 1/2$. On the subdomain defined by the condition $x_1 > 0$, we check that η_1 is monotone decreasing with respect to the both arguments X_1 and X_2. For $X_1 = 1/2$, $X_2 = 0.39$, we have $\sqrt{\eta_1} = 0.81291\cdots$. For $X_1 = 0.38$, $X_2 = 1/2$, we have $\sqrt{\eta_1} = 0.81101\cdots$. In view of (5.21), we must have $X_1 > 0.38$, $X_2 > 0.39$. Similarly, in the subdomain $x_1 < 0$, we must have $X_1 < -0.38$, $X_2 < -0.39$. Let V be the closed domain

$$V = \{(X_1, X_2) \mid 0.38 \le |X_1| \le 1/2 ,\ 0.39 \le |X_2| \le 1/2\}$$

and consider the function

$$f(X_1, X_2) = \{(2\epsilon^m x_1 + d^{(1)})^2 + 4\epsilon^{2m-2}\kappa\}\{(2(\epsilon')^m x_2 + d^{(2)})^2 + 4\epsilon^{-2m-2}\kappa\}$$

on V. By (5.24), we see that:

(C1) The minimum of $f(X_1, X_2)$ on V does not exceed 1.

Next let ξ be the positive root of (5.14). Since $y_1 y_2 \geq \xi$, we have $y_1, y_2 \geq \epsilon^{-1}\sqrt{\xi}$. By (5.11), we obtain another inequality:

$$(5.26)\qquad \begin{aligned}&(2\epsilon^m x_1 + d^{(1)})^2(2(\epsilon')^m x_2 + d^{(2)})^2 + 4\epsilon^{-2m-2}\xi(2\epsilon^m x_1 + d^{(1)})^2\\ &\quad + 4\epsilon^{2m-2}\xi(2(\epsilon')^m x_2 + d^{(2)})^2 + 16\xi^2 \leq 1\,.\end{aligned}$$

We regard x_1, x_2 and ξ as the functions of X_1 and X_2 and let $g(X_1, X_2)$ be the function on the left-hand side of (5.26). Then (5.26) implies:

(C2) The minimum of $g(X_1, X_2)$ on V does not exceed 1.

By numerical computations using a computer, we find the following:

For $m = 0$, (C1) leaves possibilities $d = \pm 1, \pm\epsilon, \pm\epsilon^2, \pm\epsilon^{-1}$. If combined with (C2), the only possibility is $d = \pm\epsilon^2$. For $m = 1$, (C1) leaves possibilities $d = \pm 1, \pm\epsilon, \pm\epsilon^2, \pm\epsilon^3$. If combined with (C2), the only possibility is $d = \pm\epsilon^3$. For $m = 2$, (C1) leaves possibilities $d = \pm\epsilon, \pm\epsilon^2, \pm\epsilon^3, \pm\epsilon^4$. If combined with (C2), the only possibility is $d = \pm\epsilon^4$. For $m = -1$, (C1) leaves possibilities $d = \pm 1, \pm\epsilon, \pm\epsilon^{-1}, \pm\epsilon^{-2}$. If combined with (C2), the only possibility is $d = \pm\epsilon$. For $m = -2$, (C1) leaves possibilities $d = \pm 1, \pm\epsilon^{-1}, \pm\epsilon^{-2}, \pm\epsilon^{-3}$. If combined with (C2), the only possibility is $d = \pm 1$.

Thus, in every case where $c = 2\epsilon^m$, we have $d = \pm\epsilon^n$ with n depending only on m. Changing the roles of z and z' and noting that $-\gamma^{-1} = \left(\begin{smallmatrix} -d & b \\ c & -a \end{smallmatrix}\right)$, we see that a must have the same form $a = \pm\epsilon^n$. (Here the $\pm$ sign is arbitrary but n is the same for d and a.) By $\det\gamma = 1$, we have $ad \equiv 1 \mod 2$, which implies $n \equiv 0 \mod 3$. Therefore only the cases $m = 1, -2$ can survive and we see that $\gamma \in S_2$. This completes the proof of Lemma 5.11.

References

[AS] A. O. L. Atkin and H. P. F. Swinnerton-Dyer, Modular forms on noncongruence subgroups, Proc. Symposia Pure Math. **19**, 1971, 1–25.

[GGP] I. M. Gel'fand, M. I. Graev and I. I. Pyatetskii-Shapiro, Representation theory and automorphic functions (English translation), W. B. Saunders Company, 1969.

[H1] D. A. Hejhal, The Selberg trace formula for PSL(2, **R**), Volume 1, Lecture notes in mathematics 548, Springer Verlag, 1976.

[H2] D. A. Hejhal, The Selberg trace formula for PSL(2, **R**), Volume 2, Lecture notes in mathematics 1001, Springer Verlag, 1983.

[M] A. M. Macbeath, Groups of homeomorphisms of a simply connected space, Ann. of Math. **79** (1964), 473–488.

[Ra] B. Randol, Small eigenvalues of the Laplace operator on compact Riemann surfaces, Bull. of Amer. Math. Soc. **80** (1974), 996–1000.

[Re] I. Reiner, Normal subgroups of the unimodular group, Illinois J. Math. **2** (1958), 142–144.

[Sc1] A. J. Scholl, Modular forms and de Rham cohomology; Atkin-Swinnerton-Dyer congruences, Invent. Math. **79** (1985), 49–77.

[Sc2] A. J. Scholl, The ℓ-adic representations attached to a certain noncongruence subgroups, Jour. für reine angew. Math. **392** (1988), 1–15.

[Sel1] A. Selberg, Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series, J. Indian Math. Soc. B. **20** (1956), 47–87 (=Collected papers, 27).

[Sel2] A. Selberg, On the estimation of Fourier coefficients of modular forms, Proc. Sympos. Pure Math. VIII (1965), 1–15 (=Collected papers, 33).

[Ser] J-P. Serre, Le problème des groupes de congruence pour SL_2, Ann. of Math. **92** (1970), 489–527 (=Œuvre II, 86).

[Sh1] G. Shimura, Construction of class fields and zeta functions of algebraic curves, Ann. of Math. **85** (1967), 58–159 (=Collected papers [67b]).

[Sh2] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami Shoten and Princeton University Press, 1971.

[Sh3] G. Shimura, Arithmetic of Quadratic Forms, Springer Monographs in Mathematics, Springer Verlag, 2010.

[Si1] C. L. Siegel, Discontinuous groups, Ann. of Math. **44** (1943), 674–689 (= Gesammelte Abhandlungen III, No. 43).

[Si2] C. L. Siegel, Lectures on advanced analytic number theory, Tata Institute, 1961.

[Su] M. Suzuki, Group Theory I, Grundlehren der mathematischen Wissenshaften 247, Springer Verlag, 1982.

[Sw] R. W. Swan, Generators and relations for certain special linear groups, Advances in Math. **6** (1971), 1–77.

[V] L. N. Vaserštein, On the group SL_2 over Dedekind rings of arithmetic type, Math. USSR Sbornik **18** (1972), 321–332.

[W] A. Weil, Sur les "formules explicites" de la théorie des nombres premiers, Comm. Lund. (1952), 252–267 (=Collected Papers [1952b]).

[Y1] H. Yoshida, On hermitian forms attached to zeta functions, Adv. Stud. in pure math. **21** (1992), 281–325.

[Y2] H. Yoshida, On absolute CM-periods, Proc. Symposia Pure Math. **66**, Part 1, 1999, 221–278.

[Y3] H. Yoshida, Cohomology and L-values, nt/1012.4573.

[Y4] H. Yoshida, Cohomology and L-values, to appear in Kyoto J. Math. (A shortened and partly revised version of [Y3]).

Department of Mathematics
Kyoto University
Kyoto 606–8502, Japan
e-mail: yoshida@math.kyoto-u.ac.jp