Asian J. Math.
Vol. 10, No. 4, pp. 749–756, December 2006
© 2006 International Press
006

ON VIRTUAL 3-GENERATION OF S-ARITHMETIC SUBGROUPS OF SL_2*

RITUMONI SARMA†

Abstract. For a number field K, we show that any S-arithmetic subgroup of $\mathrm{SL}_2(K)$ contains a subgroup of finite index generated by three elements if $\mathrm{card}(S) \geq 2$.

Key words. S-integers, S-arithmetic, CM field, subgroup of finite index, virtual generators.

AMS subject classifications. Primary 20F05, 11F06; Secondary 22E40.

1. Introduction and Notation. Let K be a number field and let S_∞ be the set of all nonconjugate embeddings of K into $\mathbb{C}$. We refer to these embeddings as *infinite primes* of K. If r_1 (resp. r_2) is the number of distinct real (resp. nonconjugate complex) embeddings, then the cardinality of S_∞ is $r_1 + r_2$ and $r_1 + 2r_2 = [K : \mathbb{Q}]$, the extension degree of K. The ring of integers in K is denoted by $\mathcal{O}_K$. The nonzero prime ideals of $\mathcal{O}_K$ are called *finite primes* of K. Let S be a finite set of primes in K containing S_∞. For a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, denote by $v_\mathfrak{p}$ the valuation defined by $\mathfrak{p}$. The ring $\mathcal{O}_S := \{x \in K : v_\mathfrak{p}(x) \geq 0 \text{ for every prime } \mathfrak{p} \notin S\}$ is called the ring of *S-integers* of K. Then $\mathcal{O}_{S_\infty} = \mathcal{O}_K$. If F is a subfield of K, then set

$$S(F) := \{\mathfrak{p} \cap \mathcal{O}_F : \mathfrak{p} \in S - S_\infty\} \sqcup S_\infty(F) \tag{1}$$

where $S_\infty(F)$ denotes the infinite primes of F. We write

$$\mathcal{O}_{S(F)} := \{x \in F : v_\mathfrak{p}(x) \geq 0 \;\forall\, \mathfrak{p} \notin S(F)\} \tag{2}$$

the ring of $S(F)$-integers in F.

For two subgroups H_1 and H_2 in a group, if $H_1 \cap H_2$ is a subgroup of finite index both in H_1 and H_2, then we say that H_1 and H_2 are *commensurable* and we write $H_1 \asymp H_2$. In particular, a group is commensurable with its subgroups of finite index. Let G be a linear algebraic group defined over K. A subgroup Γ of G is called an *S-arithmetic* subgroup of G if $\Gamma \asymp G(\mathcal{O}_S)$. The algebraic groups which we would like to deal with are $\mathrm{SL}_2(K)$ where K is a number field.

A subset X of a group G is called a set of *virtual* generators of G if the group generated by X is a subgroup of finite index in G and the group G is said to be generated *virtually* by X.

Let the cardinality of any set X be denoted by $\mathrm{card}(X)$.

A number field is called a *totally real* field if all its embeddings are real. A number field is called a *CM field* if it is an imaginary quadratic extension of a totally real field. If a number field is not CM then we refer to it as a *non-CM* field.

For any commutative ring A, denote by

$$\begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \quad \left(\text{ resp. } \begin{pmatrix} 1 & 0 \\ A & 1 \end{pmatrix}\right) \tag{3}$$

*Received September 2, 2005; accepted for publication February 4, 2006.
†Harish-Chandra Research Institute, Chhatnag road, Jhunsi, Allahabad 211 019, India (ritumoni @mri.ernet.in).

the subgroup of $\mathrm{SL}_2(A)$ consisting of matrices of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad (\text{ resp. } \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}) \qquad \text{for } x \in A.$$

Let G be any group and let $a, b \in G$. Denote by ${}^a b$ the element aba^{-1} in G.

We use, without proof, a few well known results from number theory (for details, see [2],[3]): The ring $\mathcal{O}_K$ of integers in K is a **Dedekind domain**. An ideal of $\mathcal{O}_K$ has a unique **factorization into prime ideals** of $\mathcal{O}_K$. For a finitely generated abelian group H, let $\mathrm{rank}(H)$ denote the **rank** of H as a $\mathbb{Z}$-module. **Dirichlet's unit theorem** asserts that

$$\mathrm{rank}(\mathcal{O}_K^*) = r_1 + r_2 - 1 \tag{4}$$

where r_1 and r_2 are defined as above. Also (cf. Lemma 5)

$$\mathrm{rank}(\mathcal{O}_S^*) = \mathrm{card}(S) - 1. \tag{5}$$

The group of units of a ring A is denoted by A^*. For an ideal $\mathfrak{a}$ of $\mathcal{O}_K$, let the **order** of the class of $\mathfrak{a}$ in the **ideal class group** of K be denoted by $\mathrm{ord}_K(\mathfrak{a})$. It is well known that the class group of a number field is finite. Thus $\mathrm{ord}_K(\mathfrak{a})$ is always a **finite** number.

Now we state the main result of the paper.

THEOREM 1. *Let K be a number field and let S be a finite set of primes in K containing the infinite ones such that* $\mathrm{card}(S) \geq 2$*. Any S-arithmetic subgroup of* $\mathrm{SL}_2(K)$ *is virtually generated by three elements.*

We postpone the proof of this theorem to section 3. It follows immediately from [6] that an S-arithmetic subgroup of $\mathrm{SL}_2(K)$ is virtually generated by d (≥ 3) elements where d depends up on K and S. Theorem 1 shows that d requires to be at most 3; in particular, it is independent of K and S. It is still an open question whether an S-arithmetic subgroup of $\mathrm{SL}_2(K)$ can virtually be generated by just two elements.

In [4], it is shown that the **higher rank arithmetic groups** are virtually generated by three elements. The tools used to prove this do not seem to work for the case of S-arithmetic groups. For instance, if U is a **unipotent group**, and if Γ is a **Zariski dense** subgroup of an arithmetic subgroup of U, then Γ is also arithmetic. This fact plays a crucial role in the case of higher rank arithmetic groups. The analogous statement does not hold in the case of S-arithmetic subgroups. So it needs a separate treatment. The case of SL_2 is the first case that one would like to deal with because this is the simplest possible case. The techniques here may indicate how to proceed for other S-arithmetic groups. However, the most of the techniques here are extentions of those applied in the case of arithmetic subgroups of SL_2.

In the next section we prove a number theoretic result which asserts that $\mathcal{O}_S$ is **almost** generated by a **suitably chosen** unit (in fact, by any positive power of that unit) in $\mathcal{O}_S$. Then our main result follows from a theorem due to Vaserstein. The condition that $\mathrm{card}(S) \geq 2$ is equivalent to saying that the group $\mathcal{O}_S^*$ is infinite.

2. Existence of a unit generator of $\mathcal{O}_S$.

THEOREM 2. *Let K be a non-CM field and let S be a finite set of primes including the infinite ones with* $\mathrm{card}(S) \geq 2$*. Then there exists $\alpha \in \mathcal{O}_S^*$ such that the ring $\mathbb{Z}[\alpha^n]$ is a subgroup of finite index in the ring $\mathcal{O}_S$ of S-integers for every positive integer n.*

Proof. The proof of Theorem 2 is divided into a few lemmata.

LEMMA 3 ([4], Lemma 3). *If K is a non-CM field and if F is a proper subfield of K, then $\mathcal{O}_F^*$ is a subgroup of infinite index in $\mathcal{O}_K^*$.*

LEMMA 4. *Let $K = \mathbb{Q}(\alpha)$ and let α be integral. Then $\mathbb{Z}[\alpha^{-1}]$ is of finite index in $\mathcal{O}_K[\alpha^{-1}]$.*

Proof. Since α is an integral element, we have $\mathbb{Z}[\alpha] \subset \mathbb{Z}[\alpha^{-1}]$. Let n be the index of $\alpha\mathcal{O}_K$ in $\mathcal{O}_K$. We claim that for $0 \leq i \leq (n-1)$, the cosets $\alpha\mathcal{O}_K + i$ are the distinct cosets. Indeed, if $\alpha\mathcal{O}_K + i = \alpha\mathcal{O}_K + j$ for $0 \leq i < j \leq (n-1)$ then $j - i \in \alpha\mathcal{O}_K$. This implies that n divides $j - i$ which is a contradiction. Thus, $\mathcal{O}_K$ is the union of these n cosets. In particular,

$$\mathbb{Z}[\alpha] + \alpha\mathcal{O}_K = \mathcal{O}_K. \tag{6}$$

On the other hand, $\mathbb{Z}[\alpha]$ is of finite index in $\mathcal{O}_K$. Let the index be m. By (6), we may assume that the distinct cosets (as an additive subgroup) of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$ are $\mathbb{Z}[\alpha] + \alpha x_i$ for $x_i \in \mathcal{O}_K$, $0 \leq i \leq (m-1)$. We claim that the representatives of $\mathcal{O}_K[\alpha^{-1}]/\mathbb{Z}[\alpha^{-1}]$ in $\mathcal{O}_K[\alpha^{-1}]$ are αx_i (not necessarily distinct). Let $y \in \mathcal{O}_K$. Then, by (6), $y = y_1 + \alpha x_{i_1}$ for $y_1 \in \mathbb{Z}[\alpha]$ and $0 \leq i_1 \leq (m-1)$. Thus $\alpha^{-1}y = \alpha^{-1}y_1 + x_{i_1}$. Again, using (6), we have $x_{i_1} = z_1 + \alpha x_{i_2}$ for $z_1 \in \mathbb{Z}[\alpha]$ and $0 \leq i_2 \leq (m-1)$ so that $\alpha^{-1}y = (\alpha^{-1}y_1 + z_1) + \alpha x_{i_2}$. Therefore, $\mathbb{Z}[\alpha^{-1}] + \alpha^{-1}y = \mathbb{Z}[\alpha^{-1}] + \alpha x_{i_2}$. Thus inductively one can show that $\mathbb{Z}[\alpha^{-1}] + \alpha^{-r}y = \mathbb{Z}[\alpha^{-1}] + \alpha x_i$ for some $0 \leq i \leq (m-1)$. □

LEMMA 5. *Let K be a number field and let S be a finite set of primes in K containing S_∞. Assume that $S - S_\infty = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$, $\mathrm{ord}_K(\mathfrak{q}_i) = a_i$ and that $\mathfrak{q}_i^{a_i}$ is generated by $\beta_i \in \mathcal{O}_K$ $\forall i$. Then $\mathcal{O}_S = \mathcal{O}_K[\beta_1^{-1}, \ldots, \beta_r^{-1}]$.*

Proof. Obviously, $\mathcal{O}_S \supset \mathcal{O}_K[\beta_1^{-1}, \ldots, \beta_r^{-1}]$. To see the other containment, let $x \in \mathcal{O}_S$. Then $x = yz^{-1}$ for $y, z \in \mathcal{O}_K$ and $v_\mathfrak{p}(z) = 0$ for $\mathfrak{p} \notin S$ so that, by prime factorization, $z\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{q}_i^{n_i}$ with $n_i \geq 0$. Let $m = \prod_{i=1}^{r} a_i$. Since $\mathfrak{q}_i^{a_i}$ is generated by β_i, we have $z^{-m} = u\prod_{i=1}^{r} \beta_i^{-n_i'}$ for some $u \in \mathcal{O}_K^*$ and $n_i' \geq 0$ so that $z^{-m} \in \mathcal{O}_K[\beta_1^{-1}, \ldots, \beta_r^{-1}]$. Further, $z^{-1} = z^{m-1}z^{-m}$ and $z^{m-1} \in \mathcal{O}_K$. Therefore, $z^{-1} \in \mathcal{O}_K[\beta_1^{-1}, \ldots, \beta_r^{-1}]$ and hence $x = yz^{-1} \in \mathcal{O}_K[\beta_1^{-1}, \ldots, \beta_r^{-1}]$. □

Now by Lemma 4 and Lemma 5, we have the following lemma.

LEMMA 6. *Suppose that R is a subring of finite index in $\mathcal{O}_K$. Then with the notation as in Lemma 5, the ring $R[\beta_1^{-1}, \ldots, \beta_r^{-1}]$ is of finite index in $\mathcal{O}_S$.* □

Let $\{S_i : 1 \leq i \leq s\}$ be the set of **all the proper subsets** of S and let $\{K_j : 1 \leq j \leq t\}$ be the set of **all the proper subfields** of K. Define

$$V_i := \mathcal{O}_{S_i}^* \otimes_\mathbb{Z} \mathbb{Q} \tag{7}$$

$$W_j := (\mathcal{O}_{S(K_j)}^* \cap \mathcal{O}_S^*) \otimes_\mathbb{Z} \mathbb{Q} \tag{8}$$

$$V := \mathcal{O}_S^* \otimes_\mathbb{Z} \mathbb{Q}. \tag{9}$$

Then V_i (resp. W_j) is a vector subspace of V and its dimension is $\mathrm{rank}(\mathcal{O}_{S_i}^*)$ (resp. $\mathrm{rank}(\mathcal{O}_{S(K_j)}^*)$) over $\mathbb{Q}$. By Lemma 5, we have $\mathcal{O}_S^* \cong \mathcal{O}_K^* \times \mathbb{Z}^r$ where $r = \mathrm{card}(S) - \mathrm{card}(S_\infty)$. Let this **identification** be θ. Denote again by $\mathcal{O}_S^*$, the image of $\mathcal{O}_S^*$ in V.

Two elements $a, b \in \mathcal{O}_S^*$ are identified in V if and only if $a = ub$ for a root of unity $u \in \mathcal{O}_S^*$.

LEMMA 7. *With the above notation, if K is a non-CM field, there exists $\alpha \in \mathcal{O}_S^* - (\overset{s}{\underset{i=1}{\cup}} V_i) \cup (\overset{t}{\underset{j=1}{\cup}} W_j)$ such that $v_{\mathfrak{p}}(\alpha) < 0$ for all $\mathfrak{p} \in S - S_\infty$.*

Proof. For each $1 \leq j \leq s$, we have

$$\begin{aligned} \operatorname{rank}(\mathcal{O}_{S(K_j)}^*) &= \operatorname{card}(S(K_j)) - 1 \\ &= \{\operatorname{card}(S_\infty(K_j)) - 1\} + \operatorname{card}(S(K_j) - S_\infty(K_j)) \\ &= \operatorname{rank}(\mathcal{O}_{K_j}^*) + \operatorname{card}(S(K_j) - S_\infty(K_j)). \end{aligned} \tag{10}$$

Since K is a non-CM field, by Lemma 3, $\operatorname{rank}(\mathcal{O}_{K_j}^*) < \operatorname{rank}(\mathcal{O}_K^*)$. Moreover, $\operatorname{card}(S(K_j) - S_\infty(K_j)) \leq \operatorname{card}(S - S_\infty)$. Therefore, we get

$$\operatorname{rank}(\mathcal{O}_{S(K_j)}^* \cap \mathcal{O}_S^*) < \operatorname{rank}(\mathcal{O}_S^*). \tag{11}$$

Further, $\operatorname{rank}(\mathcal{O}_{S_i}^*) = \operatorname{card}(S_i) - 1 < \operatorname{rank}(\mathcal{O}_S^*)$. Hence by comparing the dimensions, we have $V_i \subsetneqq V$ and $W_j \subsetneqq V$ (cf. (7),(8), (9)). Since a finite union of proper subspaces of a vector space over an infinite field is a proper subset of the vector space, we have $V - (\overset{s}{\underset{i=1}{\cup}} V_i) \cup (\overset{t}{\underset{j=1}{\cup}} W_j)$ is **nonempty**. Let

$$X := \{x \in \mathcal{O}_S^* : \; v_{\mathfrak{p}}(x) \; < 0 \, \forall \mathfrak{p} \in S - S_\infty\}. \tag{12}$$

Under the identification θ we have $X \cong \mathcal{O}_K^* \times \mathbb{Z}_{<o}^r \subset \mathcal{O}_K^* \times \mathbb{Z}^r$ where $\mathbb{Z}_{<0}$ denotes the set of negative integers. Hence the image of X is Zariski dense in V. Thus, if we denote the image of X in V again by X, the set

$$Y := X - (\overset{s}{\underset{i=1}{\cup}} V_i) \cup (\overset{t}{\underset{j=1}{\cup}} W_j)$$

is also nonempty. If $\alpha \in Y$, then $\alpha^n \in Y$. Thus, $\alpha \in \mathcal{O}_S^*$ can be chosen with the desired property. ∎

LEMMA 8. *Assume that K is a non-CM field. With the notations as above, let α be chosen as in Lemma 7. Then the ring $\mathbb{Z}[\alpha^n]$ is a subgroup of finite index in $\mathcal{O}_S$ for every positive integer n.*

Proof. We claim $\mathbb{Q}(\alpha) = K$. If not, then let $\mathbb{Q}(\alpha) = L$ such that $L \subsetneqq K$. Assume for $\mathfrak{p} \notin S$ and $x \in \mathcal{O}_L$ that $v_{\mathfrak{p} \cap \mathcal{O}_L}(x) \neq 0$ so that $x\mathcal{O}_L \subset \mathfrak{p} \cap \mathcal{O}_L$. Then, $x\mathcal{O}_K \subset (\mathfrak{p} \cap \mathcal{O}_L)\mathcal{O}_K \subset \mathfrak{p}$. Hence $v_{\mathfrak{p}}(x) \neq 0$. Equivalently, for $x \in \mathcal{O}_L$, if $v_{\mathfrak{p}}(x) = 0$ for every $\mathfrak{p} \notin S$, we have $v_{\mathfrak{p}}(x) = 0$ for every $\mathfrak{p} \notin S(L)$. Therefore, in particular, $v_p(\alpha^{-1}) = 0 \, \forall \mathfrak{p} \notin S(L)$ so that $\alpha \in \mathcal{O}_{S(L)}^* \cap \mathcal{O}_S^*$. This contradicts the choice of α. Hence $\mathbb{Q}(\alpha) = K$.

Since $K = \mathbb{Q}(\alpha)$, we also have $K = \mathbb{Q}(\alpha^{-1})$ and since α^{-1} is integral in K, the ring $\mathbb{Z}[\alpha^{-1}]$ is a subgroup of finite index in $\mathcal{O}_K$. Let $S - S_\infty = \{\mathfrak{p}_i : 1 \leq i \leq l\}$. Consider the prime factorization

$$\alpha^{-1}\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{p}_i^{n_i} \tag{13}$$

where $n_i > 0$ because of our **choice** of α. Let $\mathrm{ord}_K(\mathfrak{p}_i) = r_i$ and let $\mathfrak{p}_i^{r_i} = \beta_i \mathcal{O}_K$ for $\beta_i \in \mathcal{O}_K$. Then, we have

$$\alpha^m = u \prod_{i=1}^{l} \beta_i^{-b_i} \tag{14}$$

for some integers $m > 0$, $b_i > 0$ and $u \in \mathcal{O}_K^*$. Since $\beta_i \in \mathcal{O}_K$, it follows by (14) that $\beta_i^{-1} \in \mathcal{O}_K[\alpha]$. Now by Lemma 5, the ring $\mathcal{O}_K[\alpha] = \mathcal{O}_S$. Thus, by Lemma 4, the ring $\mathbb{Z}[\alpha]$ is of finite index in $\mathcal{O}_S$. □

This completes the proof of Theorem 2. □

In fact, we have proved more.

COROLLARY 1. *Let K be any finite extension of $\mathbb{Q}$ and let S be as before. If* $\mathrm{rank}(\mathcal{O}_{S(L)}^* \cap \mathcal{O}_S^*) < \mathrm{rank}(\mathcal{O}_S^*)$ **for every proper subfield** *L of K, then there exists $\alpha \in \mathcal{O}_S^*$ such that the ring $\mathbb{Z}[\alpha^n]$ is a subgroup of finite index in $\mathcal{O}_S$* **for every** *$n \geq 1$.* □

The hypothesis of Corollary 1 **may hold sometimes even for a CM field**. Here we see two examples:

EXAMPLE. (i) The field $K = \mathbb{Q}(\sqrt{-1})$ is a CM field and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$. The prime ideal $2\mathbb{Z}$ of $\mathbb{Q}$ is totally ramified in K. In fact, $2\mathcal{O}_K = \mathfrak{p}^2$ where $\mathfrak{p} = \langle 1 + \sqrt{-1} \rangle$. Let $S - S_\infty = \{\mathfrak{p}\}$. For K, the set S_∞ of infinite primes is singleton. Thus $\mathrm{card}(S) = 2$ and hence $\mathrm{rank}(\mathcal{O}_S^*) = 1$. Also, $\mathcal{O}_{S(\mathbb{Q})} = \mathbb{Z}[\frac{1}{2}]$ and so $\mathrm{rank}(\mathcal{O}_{S(\mathbb{Q})}^* \cap \mathcal{O}_S^*) = 1$ (observe that $\mathcal{O}_S = \mathbb{Z}[\sqrt{-1}][\frac{1}{1+\sqrt{-1}}]$ includes $\mathcal{O}_{S(\mathbb{Q})}$). This is an example which does not satisfy the hypothesis of corollary 1.
(ii) Let K be as in (i). Consider the ideal $5\mathbb{Z}$ of $\mathbb{Q}$ which splits completely in K: $5\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1 = \langle 5, 2 + \sqrt{-1} \rangle$ and $\mathfrak{p}_2 = \langle 5, 2 - \sqrt{-1} \rangle$. Let $S - S_\infty = \{\mathfrak{p}_1, \mathfrak{p}_2\}$. Then $\mathrm{card}(S) = 3$ and hence $\mathrm{rank}(\mathcal{O}_S^*) = 2$. The contraction of the primes of $S - S_\infty$ to $\mathbb{Q}$ are $5\mathbb{Z}$ each. Therefore, $\mathcal{O}_{S(\mathbb{Q})} = \mathbb{Z}[\frac{1}{5}]$ and hence $\mathrm{rank}(\mathcal{O}_{S(\mathbb{Q})}^*) = 1$. This is an example of a set of primes of the CM-field K which satisfies the hypothesis.

We need Corollary 1 to prove the main theorem of the paper.

3. Proof of the Main Theorem. We imitate the proof for the case of arithmetic subgroups of $\mathrm{SL}_2(K)$ (cf. [4]). Here, we state a result due to Vaserstein which we use in the proof of Theorem 1.

THEOREM 9 ([1],[6]). *Let K be a number field and let S be a finite set of primes in K including S_∞ such that* $\mathrm{card}(S) \geq 2$. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_S$. The group generated by $\begin{pmatrix} 1 & \mathfrak{a} \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ \mathfrak{a} & 1 \end{pmatrix}$ is a subgroup of finite index in* $\mathrm{SL}_2(\mathcal{O}_S)$.

To prove Theorem 1, it suffices to show that any subgroup of finite index in $\mathrm{SL}_2(\mathcal{O}_S)$ is virtually generated by three elements. Let Γ be a subgroup of finite index in $\mathrm{SL}_2(\mathcal{O}_S)$. Without loss of generality we assume that Γ is a normal subgroup. Let its index in $\mathrm{SL}_2(\mathcal{O}_S)$ be h.

Proof of Theorem 1.
Case 1: The pair (K, S) is such that for **every proper subfield** L of K, we have

$$\mathrm{rank}(\mathcal{O}_{S(L)}^* \cap \mathcal{O}_S^*) < \mathrm{rank}(\mathcal{O}_S^*). \tag{15}$$

Choose $\alpha \in \mathcal{O}_S^*$ **as in Corollary 1**. Obviously, $\begin{pmatrix} \alpha^h & 0 \\ 0 & \alpha^{-h} \end{pmatrix} \in \Gamma$. Since $\mathbb{Z}[\alpha^h]$ is a subring of finite index in $\mathcal{O}_S$, we replace α^h by α and assume that $\gamma := \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \in \Gamma$. Define, $\psi_1 := \begin{pmatrix} 1 & 0 \\ h & 1 \end{pmatrix} \in \Gamma$ and $\psi_2 := \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma$. Let $\Gamma_0 = \langle \gamma, \psi_1, \psi_2 \rangle$. We claim that Γ_0 is a subgroup of finite index in $\mathrm{SL}_2(\mathcal{O}_S)$.

Indeed, $\gamma^{-r}\psi_1^s\gamma^r = \begin{pmatrix} 1 & 0 \\ s\alpha^{2r}h & 1 \end{pmatrix} \in \Gamma_0$ and $\gamma^r\psi_2^s\gamma^{-r} = \begin{pmatrix} 1 & s\alpha^{2r}h \\ 0 & 1 \end{pmatrix} \in \Gamma_0$. One concludes from this that Γ contains $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$ for $x, y \in h\mathbb{Z}[\alpha^2]$. By Corollary 1, the additive subgroup $h\mathbb{Z}[\alpha^2]$ is of finite index in $\mathcal{O}_S$. If m is the index then the ideal $\mathfrak{a} := m\mathcal{O}_S$ is contained in $h\mathbb{Z}[\alpha^2]$. Now it follows from Theorem 9 that the group Γ_0 is a subgroup of finite index in $\mathrm{SL}_2(\mathcal{O}_S)$.

Case 2: The pair (K, S) is such that the inequality (15) **does not hold for some proper subfield** F of K. That is, we have

$$\mathrm{rank}(\mathcal{O}_{S(F)}^* \cap \mathcal{O}_S^*) = \mathrm{rank}(\mathcal{O}_S^*). \tag{16}$$

Now, (16) implies that $\mathrm{rank}(\mathcal{O}_F^*) = \mathrm{rank}(\mathcal{O}_K^*)$. Thus, by Lemma 3, K is a CM field and in fact $K = F(\sqrt{-d})$ so that F is a totally real field and d a totally positive integer in F. Thus, we have

$$\mathcal{O}_{S(F)}^* \asymp \mathcal{O}_S^*, \tag{17}$$

$$\mathcal{O}_F^* \asymp \mathcal{O}_K^*. \tag{18}$$

We prove a number theoretic lemma here.

Lemma 10. *With the above notation, let* (16) *hold for a CM filed* $K = F[\sqrt{-d}]$. *There exists* $\alpha \in \mathcal{O}_{S(F)}^* \cap \mathcal{O}_S^*$ *such that the ring* $\mathbb{Z}[\alpha^n][\sqrt{-d}]$ *is of finite index in* $\mathcal{O}_S$ *for any integer* n.

Proof. In the case of a quadratic extension, a prime ideal of the base field is either inert or totally ramified or split completely (into two distinct primes). We claim that the set $S(F)$ (cf. definition (1)), does not contain any finite prime which splits completely in K. To the contrary, if $S(F)$ contains a split prime $\mathfrak{q}$ so that $\mathfrak{q}\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$, then we have two possibilities, namely, $\mathfrak{q}_1, \mathfrak{q}_2 \in S$ or $\mathfrak{q}_1 \in S$ and $\mathfrak{q}_2 \notin S$. If $\mathfrak{q}_1, \mathfrak{q}_2 \in S$, then $\mathrm{card}(S(F)) < \mathrm{card}(S)$ (since $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are contracted to the same prime $\mathfrak{q}$ in F) and thus (16) does not hold and we get a contradiction. Next, assume that $\mathfrak{q}_1 \in S$ and $\mathfrak{q}_2 \notin S$. Let β (resp. γ_1) be the generator of $\mathfrak{q}^{\mathrm{ord}_F(\mathfrak{q})}$ (resp. $\mathfrak{q}_1^{\mathrm{ord}_K(\mathfrak{q}_1)}$). By (17), we have $\mathcal{O}_S \supset \mathcal{O}_{S(F)}$ so that $\beta \in \mathcal{O}_S$. Again (17) and (18) together imply that $\gamma_1^m \in \mathcal{O}_{S(F)}$ for some $m > 0$ so that $\gamma_1^m = u\beta^b x$ for some $b > 0$ and $u \in \mathcal{O}_K^* \cap \mathcal{O}_F^*$ and $x \in \mathcal{O}_{S(F)}^* \cap \mathcal{O}_S^*$ with $v_{\mathfrak{p}}(x) = 0$ for $\mathfrak{p} \notin S(F)$. Then $v_{\mathfrak{q}_2}(\gamma_1) = 0$ whereas $v_{\mathfrak{q}_2}(u\beta^b x) > 0$ and we again get a contradiction. Therefore, we have

$$(\mathfrak{q} \cap \mathcal{O}_F)\mathcal{O}_K = \mathfrak{q} \text{ or } \mathfrak{q}^2. \tag{19}$$

Let $\mathrm{ord}_F(\mathfrak{q} \cap \mathcal{O}_F) = a$. Then, by (19), we see that $(\mathfrak{q} \cap \mathcal{O}_F)^a\mathcal{O}_K = ((\mathfrak{q} \cap \mathcal{O}_F)\mathcal{O}_K)^a = \mathfrak{q}^a$ or $\mathfrak{q}^{2a}$ is a principal ideal. Thus, $(\mathfrak{q} \cap \mathcal{O}_F)^a$ and $\mathfrak{q}^b$ (for $b = a$ or $2a$) are generated by the same element $\beta \in \mathcal{O}_F$.

Let $S - S_\infty = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Choose $\beta_i \in \mathcal{O}_F$ such that $(\mathfrak{p}_i \cap \mathcal{O}_F)^{\mathrm{ord}_F(\mathfrak{p}_i \cap \mathcal{O}_F)} = \beta_i \mathcal{O}_F$. Then, by Lemma 5, $\mathcal{O}_{S(F)} = \mathcal{O}_F[\beta_1^{-1}, \ldots, \beta_m^{-1}]$. Moreover, by the conclusion of the above paragraph and by Lemma 5, we have $\mathcal{O}_S = \mathcal{O}_K[\beta_1^{-1}, \ldots, \beta_m^{-1}]$. Now, since $\mathcal{O}_F[\sqrt{-d}]$ is of finite index in $\mathcal{O}_K$, by Lemma 6, we have $\mathcal{O}_{S(F)}[\sqrt{-d}] = \mathcal{O}_F[\sqrt{-d}][\beta_1^{-1}, \ldots, \beta_m^{-1}]$ is of finite index in $\mathcal{O}_S$. Since F is a non-CM field, by Theorem 2, one can choose $\alpha \in \mathcal{O}_{S(F)}^* \cap \mathcal{O}_S^*$ such that $\mathbb{Z}[\alpha^n]$ is of finite index in $\mathcal{O}_{S(F)}$ for every $n \geq 1$. Hence $\mathbb{Z}[\alpha^n][\sqrt{-d}]$ is of finite index in $\mathcal{O}_S$. □

Choose α as in Lemma 10 and define γ and ψ_1 as in **case 1**. We define ψ_2 by $\psi_2 := \begin{pmatrix} 1 & h\sqrt{-d} \\ 0 & 1 \end{pmatrix} \in \Gamma$. Let $\Gamma_0 := \langle \gamma, \psi_1, \psi_2 \rangle$. We show that Γ_0 is a subgroup of finite index in $\mathrm{SL}_2(\mathcal{O}_S)$.

Since F is a non-CM field, by an argument similar to case 1, one shows that there is an ideal $\mathfrak{a}$ of $\mathcal{O}_{S(F)}$ such that

$$\begin{pmatrix} 1 & 0 \\ \mathfrak{a} & 1 \end{pmatrix} \subset \Gamma_0 \quad \text{and} \quad \begin{pmatrix} 1 & \sqrt{-d}\mathfrak{a} \\ 0 & 1 \end{pmatrix} \subset \Gamma_0. \tag{20}$$

Then for $x \in \mathfrak{a}$, using Bruhat decomposition (see [5, 8.3]) of ψ_2, we have

$$^{\psi_2}\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = {}^{u}\begin{pmatrix} 1 & h^2dx \\ 0 & 1 \end{pmatrix} \in \Gamma_0 \text{ where } u = \begin{pmatrix} 1 & 0 \\ \frac{1}{h\sqrt{-d}} & 1 \end{pmatrix}. \tag{21}$$

Let $\mathfrak{b} = h^2 d\mathfrak{a}$. Then we have

$$^{u}\begin{pmatrix} 1 & \mathfrak{b} \\ 0 & 1 \end{pmatrix} \subset \Gamma_0 \quad \text{and} \quad {}^{u}\begin{pmatrix} 1 & 0 \\ \mathfrak{b} & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \mathfrak{b} & 1 \end{pmatrix} \subset \Gamma_0. \tag{22}$$

Let Γ_1 be the subgroup of $\mathrm{SL}_2(\mathcal{O}_F)$ generated by $\begin{pmatrix} 1 & \mathfrak{b} \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ \mathfrak{b} & 1 \end{pmatrix}$. Then, by (22), we have ${}^{u}\Gamma_1 \subset \Gamma_0$. By Theorem 9, the index of Γ_1 in $\mathrm{SL}_2(\mathcal{O}_F)$ is finite. Thus it follows that there exists an integer N such that

$$\gamma^N \in \Gamma_1 \cap \Gamma_0. \tag{23}$$

Since ${}^{u}\Gamma_1 \subset \Gamma_0$, we have ${}^{u}\gamma^N \in \Gamma_0$.

Therefore, ${}^{u}\gamma^{-N}\gamma^N = \begin{pmatrix} 1 & 0 \\ (\alpha^{2N} - 1)\frac{\sqrt{-d}}{hd} & 1 \end{pmatrix} \in \Gamma_0$. Now by conjugating this element and its powers by negative powers of γ, one shows that

$$\Gamma_0 \supset \begin{pmatrix} 1 & 0 \\ \sqrt{-d}\mathfrak{c} & 1 \end{pmatrix} \tag{24}$$

where $\mathfrak{c} := (\alpha^{2N} - 1)\mathbb{Z}[\alpha^2] \cap \mathfrak{a}$. Now $\mathfrak{c} + \sqrt{-d}\mathfrak{c}$ is a subgroup of finite index in $\mathcal{O}_{S(F)}[\sqrt{-d}]$ and hence in $\mathcal{O}_S$. Therefore, the group $\mathfrak{c} + \sqrt{-d}\mathfrak{c}$ contains a nonzero ideal $\mathfrak{q}$ of $\mathcal{O}_S$. Since $\mathfrak{c} \subset \mathfrak{a}$, by (20) and (24), we have

$$\begin{pmatrix} 1 & 0 \\ \mathfrak{q} & 1 \end{pmatrix} \subset \Gamma_0. \tag{25}$$

Again, for $y \in \mathfrak{a}$, using the Bruhat decomposition of ψ_1, we have

$$^{\psi_1}\begin{pmatrix} 1 & y\sqrt{-d} \\ 0 & 1 \end{pmatrix} = {}^{v\varphi}\begin{pmatrix} 1 & 0 \\ h^2yd & 1 \end{pmatrix} \in \Gamma_0 \tag{26}$$

where $v = \begin{pmatrix} 1 & \frac{1}{h} \\ 0 & 1 \end{pmatrix}$ and $\varphi = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{-d}} \end{pmatrix}$. Thus we have

$$^{v\varphi}\begin{pmatrix} 1 & \mathfrak{b} \\ 0 & 1 \end{pmatrix} \subset \Gamma_0, \qquad \text{and} \; ^{v\varphi}\begin{pmatrix} 1 & 0 \\ \mathfrak{b} & 1 \end{pmatrix} \subset \Gamma_0. \tag{27}$$

Therefore, $^{v\varphi}\Gamma_1 \subset \Gamma_0$ and hence $^{v\varphi}\gamma^N \in \Gamma_1 \cap \Gamma_0$. Thus, using (23) we have

$$^{v\varphi}\gamma^N \gamma^{-N} = \begin{pmatrix} 1 & (1-\alpha^{2N})\frac{1}{h} \\ 0 & 1 \end{pmatrix} \in \Gamma_0. \tag{28}$$

Again by conjugating this element and its powers by nonnegative powers of γ, one shows that

$$\begin{pmatrix} 1 & \mathfrak{c} \\ 0 & 1 \end{pmatrix} \subset \Gamma_0. \tag{29}$$

Since $\mathfrak{c} \subset \mathfrak{a}$, by (20) and (29), we have

$$\begin{pmatrix} 1 & \mathfrak{q} \\ 0 & 1 \end{pmatrix} \subset \Gamma_0. \tag{30}$$

It follows from (25) and (30), and by Theorem 9, that the group Γ_0 is a subgroup of finite index in $\mathrm{SL}_2(\mathcal{O}_S)$. This completes the proof of Theorem 1. □

Acknowledgment. A part of this work was carried out when I was visiting School of Mathematics, TIFR, Mumbai. I thankfully acknowledge their support. I thank Amala for going through the manuscript and her useful comments. I also thank the referee for her/his valuable suggestions and remarks.

REFERENCES

[1] B. Liehl, *On the Group* SL_2 *over orders of arithmetic type*, J. Reine Angew. Math., 323 (1981), pp. 153–171.
[2] D. A. Marcus, *Number fields*, Springer Verlag, 1977.
[3] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, INC 1991.
[4] R. Sarma, T. N. Venkataramana, *Generators of Arithmetic Groups*, Geometriae Dedicata, 114:1 (2005), pp. 103–146.
[5] T. A. Springer, *Linear Algebraic Groups*, Progress in Math. Vol. 9. Birkhauser, second ed., 1998.
[6] L. N. Vaserstein, *On the Group* SL_2 *over Dedekind Rings of Arithmetic type*, Math. USSR; Sbornik, 18:2 (1972), pp. 321–332.