S-ARITHMETIC GROUPS OF SL$_2$ TYPE

R. SARMA

Abstract. For a number field $K$, we show that any $S$-arithmetic subgroup of $SL_2(K)$ contains a subgroup of finite index generated by three elements if $\text{card}(S) \geq 2$.

1. Introduction and Notation

Let $K$ be a number field and let $S_{\infty}$ 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 so that the cardinality of $S_{\infty}$ is $r_1 + r_2$, then $r_1 + 2r_2 = [K : \mathbb{Q}]$, the extension degree of $K$. Let $S$ be a finite set of primes in $K$ containing $S_{\infty}$. The ring of integers in $K$ is denoted by $\mathcal{O}_K$. For a prime ideal $p$ of $\mathcal{O}_K$, denote by $v_p$ the valuation defined by $p$. The ring $\mathcal{O}_S := \{ x \in K : v_p(x) \geq 0 \text{ for every prime } p \notin S \}$ 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

\begin{equation}
S(F) := \{ p \cap \mathcal{O}_F : p \in S - S_{\infty} \} \cup S_{\infty}(F)
\end{equation}

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

\begin{equation}
\mathcal{O}_{S(F)} := \{ x \in F : v_p(x) \geq 0 \forall p \notin S(F) \}
\end{equation}

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. A subgroup $\Gamma$ of $SL_2(K)$ is called $S$-arithmetic if $\Gamma \asymp SL_2(\mathcal{O}_S)$.

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 $\text{card}(X)$.

1991 Mathematics Subject Classification. Primary 20F05, 11F06; Secondary 22E40

R. Sarma. Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211 019, India. ritumoni@mri.ernet.in.
A number field is called a \textit{totally real} field if all its embeddings are real. A number field is called a \textit{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 \textit{non-CM} field.

For any commutative ring $A$, denote by
\begin{equation}
\begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \quad \text{(resp.} \quad \begin{pmatrix} 1 & 0 \\ A & 1 \end{pmatrix}) \end{equation}
the subgroup of $SL_2(A)$ consisting of matrices of the form
\begin{equation}
\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{(resp.} \quad \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}) \quad \text{for} \quad x \in A.
\end{equation}

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

We use a few well known number theoretic results (for details, see \cite{1,2}): 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 rank$(H)$ denote the rank of $H$ as a $\mathbb{Z}$-module. \textbf{Dirichlet’s unit theorem} asserts that
\begin{equation}
\text{rank}(\mathcal{O}_K^*) = r_1 + r_2 - 1
\end{equation}
where $r_1$ and $r_2$ are defined as above. Also (cf. Lemma \cite{5})
\begin{equation}
\text{rank}(\mathcal{O}_S^*) = \text{card}(S) - 1.
\end{equation}

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 \textbf{ideal class group} of $K$ be denoted by ord$_K(\mathfrak{a})$. It is well known that the class group of a number field is finite. Thus ord$_K(\mathfrak{a})$ is always a \textbf{finite} number.

Now we state the main result of the paper.

\textbf{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 card$(S) \geq 2$. Any $S$-arithmetic subgroup of $SL_2(K)$ is virtually generated by three elements.

We postpone the proof of this theorem to section 3. In \cite{3}, it is shown that the \textbf{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 \textbf{unipotent group}, and if $\Gamma$ is a Zariski dense subgroup of an arithmetic subgroup of $U$, then $\Gamma$ 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 technique
here may indicate how to proceed for other $S$-arithmetic groups. In the next section we prove a number theoretic result which asserts that $\mathcal{O}_S$ is almost generated by some 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 $\text{card}(S) \geq 2$ is equivalent to say that the group $\mathcal{O}^*_S$ is infinite.

2. A Number Theoretic Result

Theorem 2. Let $K$ be a non-CM field and let $S$ be a finite set of primes including the infinite ones with $\text{card}(S) \geq 2$. 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 $n$.

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

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 $\mathcal{O}^*_K$.

Proof. Assume to the contrary that there exists a subfield $F$ of $K$ such that the quotient $\mathcal{O}^*_K/\mathcal{O}^*_F$ is finite. We show that $K$ is a CM field and arrive at a contradiction.

Let $d = [K : F]$ be the degree of exention. Let $A$ (resp. $B$) be the set of all real (resp. nonconjugate complex) embeddings of $F$ over $\mathbb{Q}$. For an embedding $a \in A$, let $x(a)$ (resp. $y(a)$) be the number of real (resp. nonconjugate complex) extensions of $a$ to $K$. Then we have

$$x(a) + 2y(a) = d.$$  

Similarly, we define $x(b), y(b)$ for $b \in B$. Then $x(b) = 0$ and $y(b) = d$. Since $\mathcal{O}^*_K/\mathcal{O}^*_F$ is finite, $\text{rank}(\mathcal{O}^*_F) = \text{rank}(\mathcal{O}^*_K)$. Hence by (1), we have

$$\text{card}(A) + \text{card}(B) - 1 = \sum_{a \in A} x(a) + \left( \sum_{a \in A} y(a) + \sum_{b \in B} y(b) \right) - 1$$

$$= \sum_{a \in A} \left\{ x(a) + y(a) \right\} + \sum_{b \in B} y(b) - 1$$

$$\geq \text{card}(A) + d \text{ card}(B) - 1,$$

as $x(a) + y(a) \geq 1$. Now since $F$ is a proper subfield of $K$, we have $d > 1$. Hence using (7), we see that $\text{card}(B) = 0$. Thus, $F$ is a totally real field. Therefore by inequality (7), we get $\text{card}(A) = \sum_{a \in A} \{ x(a) + y(a) \}$.

Hence for each $a \in A$, we have

$$x(a) + y(a) = 1.$$  

S-ARITHMETIC GROUPS OF SL₂ TYPE
Now, it follows from (9) that $y(a) = d - 1$. Therefore, since $d - 1 \geq 1$, by (3), we have $x(a) = 0$ and $y(a) = 1$. Thus again by (9), we get $d = 2$ so that the field $K$ is an imaginary quadratic extension over the totally real field $F$ which is a contradiction as desired.

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

Proof. Since $\alpha$ 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 $\mathcal{O}_K$. For $0 \leq i \leq (n-1)$, the cosets $\alpha \mathcal{O}_K + i$ are the distinct cosets. Otherwise, $\alpha \mathcal{O}_K + i = \alpha \mathcal{O}_K + j$ for $0 \leq i < j \leq (n-1)$ so that $j - i \in \alpha \mathcal{O}_K$. This implies that $n$ divides $j - i$ which is a contradiction. Therefore, $\mathcal{O}_K$ is the union of these $n$ cosets. Thus, in particular,

$$Z[\alpha] + \alpha \mathcal{O}_K = \mathcal{O}_K.$$  \hfill (9)

On the other hand, $Z[\alpha]$ is of finite index in $\mathcal{O}_K$. By (2), we may assume that the distinct cosets (as an additive subgroup) of $Z[\alpha]$ in $\mathcal{O}_K$ are $Z[\alpha] + \alpha x_i$ with $0 \leq i \leq (m - 1)$. We claim that the representatives of $\mathcal{O}_K[\alpha^{-1}] / Z[\alpha^{-1}]$ in $\mathcal{O}_K[\alpha^{-1}]$ are $\alpha x_i$ (not necessarily distinct). Let $y \in \mathcal{O}_K$. Then, by (3), $y = y_1 + \alpha x_i$, for $y_1 \in Z[\alpha]$ and $0 \leq i_1 \leq (m-1)$. Thus $\alpha^{-1} y = \alpha^{-1} y_1 + x_i$. Again, using (3), we have $x_i = z_i + \alpha x_i$ for $z_i \in Z[\alpha]$ and $0 \leq i_2 \leq (m - 1)$ so that $\alpha^{-1} y = (\alpha^{-1} y_1 + z_i) + \alpha x_i$. Therefore, $Z[\alpha^{-1}] + \alpha^{-1} y = Z[\alpha^{-1}] + \alpha x_i$. Thus inductively, one can show that $Z[\alpha^{-1}] + \alpha^{-r} y = Z[\alpha^{-1}] + \alpha x_i$ 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 $S_\infty$. Assume that $S = S_\infty = \{q_1, \ldots, q_r\}$, $\text{ord}_K(q_i) = a_i$ and that $q_i^{a_i}$ 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 $v_p(z) = 0$ for $p \notin S$ so that, by prime factorization, $z \mathcal{O}_K = \prod_{i=1}^{r} q_i^{n_i}$ with $n_i \geq 0$. Let $m = \prod_{i=1}^{r} a_i$. Since $q_i^{a_i}$ is generated by $\beta_i$, 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 1 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 4, the ring $R[\beta_1^{-1}, \ldots, \beta_r^{-1}]$ is of finite index in $\mathcal{O}_S$. \hfill $\square$
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

\[
V_i := \mathcal{O}_{S_i}^* \otimes \mathbb{Q} \quad \text{and} \quad W_j := (\mathcal{O}_{S(K_j)}^* \cap \mathcal{O}_S^*) \otimes \mathbb{Q}.
\]

Then \( V_i \) (resp. \( W_j \)) is vector space of dimension \( \text{rank}(\mathcal{O}_{S(K_j)}^*) \) (resp. \( \text{rank}(\mathcal{O}_{S(K_j)}^*) \)) over \( \mathbb{Q} \). By Lemma 5, we have \( \mathcal{O}_S^* = \mathcal{O}_K^* \times \mathbb{Z}^r \) where \( r = \text{card}(S) - \text{card}(S_{S\infty}) \).

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

**Proof.** For each \( 1 \leq j \leq s \), we have (see (1) and (2) for definition)

\[
\text{rank}(\mathcal{O}_{S(K_j)}^*) = \text{card}(S(K_j)) - 1 = \{\text{card}(S_{\infty}(K_j)) - 1\} + \text{card}(S(K_j) - S_{\infty}(K_j))
\]

\[
(11) \quad = \text{rank}(\mathcal{O}_{K_j}^*) + \text{card}(S(K_j) - S_{\infty}(K_j)).
\]

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

\[
(12) \quad \text{rank}(\mathcal{O}_{S(K_j)}^* \cap \mathcal{O}_S^*) < \text{rank}(\mathcal{O}_S^*).
\]

Further, \( \text{rank}(\mathcal{O}_{S_i}^*) = \text{card}(S_i) - 1 < \text{rank}(\mathcal{O}_S^*) \). Then by comparing the dimensions, we have \( V_i \subsetneq V \) and \( W_j \subsetneq V \) where \( V := \mathcal{O}_S^* \otimes \mathbb{Q} \) (cf. (12)). 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 \( V - (\bigcup_{i=1}^s V_i) \cup (\bigcup_{j=1}^t W_j) \) is nonempty. Let

\[
(13) \quad X := \{x \in \mathcal{O}_S^* : v_p(x) < 0 \forall p \in S - S_{\infty}\}.
\]

Then \( X \) is Zariski dense in \( V \). Thus the set

\[
Y := X - (\bigcup_{i=1}^s V_i) \cup (\bigcup_{j=1}^t W_j)
\]

is also nonempty. If \( \alpha \in Y \), then \( \alpha^n \in Y \). Thus, \( \alpha \in \mathcal{O}_S^* \) can be chosen such that \( v_p(\alpha) < 0 \) for each \( p \in S - S_{\infty} \). \qed

**Lemma 8.** Let \( \alpha \) 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 \( L \subsetneq K \). Assume for \( p \notin S \) and \( x \in \mathcal{O}_L \) that \( v_p(\mathcal{O}_L(x)) \neq 0 \) so that \( x\mathcal{O}_L \subset p \cap \mathcal{O}_L \). Then, \( x\mathcal{O}_K \subset (p \cap \mathcal{O}_L)\mathcal{O}_K \subset p \) so that \( v_p(x) \neq 0 \). Thus, equivalently, for \( x \in \mathcal{O}_L \), if \( v_p(x) = 0 \) for every \( p \notin S \), we have \( v_p(x) = 0 \) for every \( p \notin S(L) \). Therefore, in particular, \( v_p(\alpha^{-1}) = 0 \forall p \notin S(L) \)

\( \square \)
so that \( \alpha \in \mathcal{O}_{S(L)}^* \cap \mathcal{O}_{S}^* \). This contradicts the choice of \( \alpha \). Hence \( \mathbb{Q}(\alpha) = K \).

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

\[
(14) \quad \alpha^{-1} \mathcal{O}_K = \prod_{i=1}^{l} p_i^{n_i}
\]

where \( n_i \geq 0 \). In fact, by our choice of \( \alpha \), \( n_i > 0 \) for each \( i \). Let \( \text{ord}_K(p_i) = r_i \) and let \( p_i^r = \beta_i \mathcal{O}_K \) for \( \beta_i \in \mathcal{O}_K \). Then, we have

\[
(15) \quad \alpha^m = \prod_{i=1}^{l} \beta_i^{-b_i}
\]

(if necessary absorbing a unit with \( \beta_1 \)) for some integers \( m > 0 \) and \( b_i > 0 \). Since \( \beta_i \in \mathcal{O}_K \), it follows by (15) that \( \beta_i^{-1} \in \mathcal{O}_K[\alpha] \). Now by Lemma \( \square \) the ring \( \mathcal{O}_K[\alpha] = \mathcal{O}_S \). Thus, by Lemma \( \square \) the ring \( \mathbb{Z}[\alpha] \) is of finite index in \( \mathcal{O}_S \). \( \square \)

This completes the proof of Theorem \( \square \)

In fact, we have proved more.

**Corollary 1.** Let \( K \) be any finite extension of \( \mathbb{Q} \) and let \( S \) be as before. If \( \text{rank}(\mathcal{O}_{S(L)}^* \cap \mathcal{O}_S^*) < \text{rank}(\mathcal{O}_S^*) \) 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 \( n \geq 1 \). \( \square \)

The hypothesis of Corollary \( \square \) 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 \( S_\infty \) of infinite primes is singleton. Thus \( \text{card}(S) = 2 \) and hence \( \text{rank}(\mathcal{O}_S^*) = 1 \). Also, \( \mathcal{O}_{S(\mathbb{Q})} = \mathbb{Z}[\frac{1}{2}] \) and so \( \text{rank}(\mathcal{O}_{S(\mathbb{Q})}^* \cap \mathcal{O}_S^*) = 1 \) (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 corollary \( \square \)

(ii) Next 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 \( \text{card}(S) = 3 \) and hence \( \text{rank}(\mathcal{O}_S^*) = 2 \). 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 \( \text{rank}(\mathcal{O}_{S(\mathbb{Q})}^*) = 1 \). This is an example of a set of primes of the CM-field \( K \) which satisfies the hypothesis.

We need Corollary \( \square \) to prove the main theorem of the paper.
3. Proof of the Main Theorem

We imitate the proof of the same result for the case of arithmetic subgroups of $SL_2(K)$ (cf. [3]). Here, we state a result due to Vaserstein which we use in the proof of Theorem 1.

**Theorem 9** (Vaserstein). Let $K$ be a number field and let $S$ be a finite set of primes in $K$ including $S_{\infty}$ such that $\text{card}(S) \geq 2$. Let $a$ be a nonzero ideal of $\mathcal{O}_S$. The group generated by \[
\begin{pmatrix}
1 & a \\
0 & 1
\end{pmatrix}
\quad \text{and} \quad
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
\] is a subgroup of finite index in $SL_2(\mathcal{O}_S)$.

To prove Theorem 1 it suffices to show that any subgroup of finite index in $SL_2(\mathcal{O}_S)$ is virtually generated by three elements. Let $\Gamma$ be a subgroup of finite index in $SL_2(\mathcal{O}_S)$. Without loss of generality we assume that it is a normal subgroup. Let its index in $SL_2(\mathcal{O}_S)$ be $h$.

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

\[
\text{rank}(\mathcal{O}^*_S(L) \cap \mathcal{O}^*_S) < \text{rank}(\mathcal{O}^*_S).
\]

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 $\alpha^h$ by $\alpha$ and assume that $\gamma := \begin{pmatrix}
\alpha & 0 \\
0 & \alpha^{-1}
\end{pmatrix} \in \Gamma$. Define, $\psi_1 := \begin{pmatrix}
1 & 0 \\
0 & h
\end{pmatrix} \in \Gamma$ 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 $\Gamma_0$ is a subgroup of finite index in $SL_2(\mathcal{O}_S)$.

Indeed, $\gamma^{-r} \psi_1^r \gamma^r = \begin{pmatrix} 1 & 0 \\ s\alpha^{2r}h & 1 \end{pmatrix} \in \Gamma_0$ and $\gamma^r \psi_2^r \gamma^{-r} = \begin{pmatrix} 1 & s\alpha^{2r}h \\ 0 & 1 \end{pmatrix} \in \Gamma_0$. One concludes from this that $\Gamma$ contains $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$ with $x, y \in h\mathbb{Z}[\alpha^2]$. By Corollary 1 $h\mathbb{Z}[\alpha^2]$ is of finite index in the additive group $\mathcal{O}_S$. If $m$ is the index then the ideal $a := m\mathcal{O}_S$ is contained in $h\mathbb{Z}[\alpha^2]$. Now it follows from Theorem 9 that the group $\Gamma_0$ is a subgroup of finite index in $SL_2(\mathcal{O}_S)$.

**Case 2:** The pair $(K, S)$ is such that the inequality (16) does not hold for some proper subfield $F$ of $K$. That is, we have

\[
\text{rank}(\mathcal{O}^*_S(F) \cap \mathcal{O}^*_S) = \text{rank}(\mathcal{O}^*_S).
\]
This implies that rank$(\mathcal{O}_F^s) = \text{rank}(\mathcal{O}_K^s)$. 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

\begin{equation}
\mathcal{O}_{S(F)}^s \simeq \mathcal{O}_S^s,
\end{equation}

\begin{equation}
\mathcal{O}_F^s \simeq \mathcal{O}_K^s.
\end{equation}

We prove a number theoretic lemma here.

**Lemma 10.** With the above notation, let (17) hold for a CM field $K = F[\sqrt{-d}]$. There exists $\alpha \in \mathcal{O}_{S(F)}^s \cap \mathcal{O}_S^s$ 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. (11)), does not contain any finite prime which splits completely in $K$. To the contrary, if $S(F)$ contains a split prime $q$ so that $q\mathcal{O}_K = q_1q_2$, then we have two possibilities, namely, $q_1, q_2 \in S$ or $q_1 \in S$ and $q_2 \notin S$. If $q_1, q_2 \in S$, then $\text{card}(S(F)) < \text{card}(S)$ (since $q_1$ and $q_2$ are contracted to the same prime $q$ in $F$) and thus (17) does not hold. This is a contradiction. Next, assume that $q_1 \in S$ and $q_2 \notin S$. Let $\beta$ (resp. $\gamma_1$) be the generator of $q^{\text{ord}_F(q)}$ (resp. $q_1^{\text{ord}_K(q_1)}$). By (13), we have $\mathcal{O}_S \supset \mathcal{O}_{S(F)}$ so that $\beta \in \mathcal{O}_S$. Again (18) and (19) together imply that $\gamma_1^m \in \mathcal{O}_{S(F)}$ for some $m > 0$ so that $\gamma_1^m = u\beta^bx$ for some $b > 0$ and $u \in \mathcal{O}_K^s \cap \mathcal{O}_F^s$ and $x \in \mathcal{O}_{S(F)}^s \cap \mathcal{O}_S^s$ with $v_p(x) = 0$ for $p \notin S(F)$. Then $v_{q_2}(\gamma_1) = 0$ whereas $v_{q_2}(u\beta^bx) = 0$. This is a contradiction. Therefore, we have

\begin{equation}
(q \cap \mathcal{O}_F)\mathcal{O}_K = q \text{ or } q^2.
\end{equation}

Let $\text{ord}_F(q \cap \mathcal{O}_F) = a$. Then, by (20), we see that $(q \cap \mathcal{O}_F)^a\mathcal{O}_K = ((q \cap \mathcal{O}_F)\mathcal{O}_K)^a = q^a$ or $q^{2a}$ is a principal ideal. Thus, $(q \cap \mathcal{O}_F)^a$ and $q^b$ (for $b = a$ or $2a$) are generated by the same element $\beta \in \mathcal{O}_F$.

Let $S - S_\infty = \{p_1, \ldots, p_s\}$. Choose $\beta_i \in \mathcal{O}_F$ such that $(p_i \cap \mathcal{O}_F)^{\text{ord}_F(p_i \cap \mathcal{O}_F)} = \beta_i\mathcal{O}_F$. Then, by Lemma 4, $\mathcal{O}_{S(F)} = \mathcal{O}_F[\beta_1^{-1}, \ldots, \beta_m^{-1}]$ and $\mathcal{O}_S = \mathcal{O}_K[\beta_1^{-1}, \ldots, \beta_m^{-1}]$. Now, since $\mathcal{O}_F[\sqrt{-d}]$ is of finite index in $\mathcal{O}_K$, by Lemma 5, we have $\mathcal{O}_{S(F)}[\sqrt{-d}] = \mathcal{O}_F[\sqrt{-d}]\mathcal{O}_K[\beta_1^{-1}, \ldots, \beta_m^{-1}]$ is of finite index in $\mathcal{O}_S$. Since $F$ is a non-CM field, by Theorem 2 one can choose $\alpha \in \mathcal{O}_{S(F)}^s \cap \mathcal{O}_S^s$ such that $\mathbb{Z}[\alpha^n]$ is of finite index in $\mathcal{O}_{S(F)}$ for every $n \geq 1$. Then $\mathbb{Z}[\alpha^n][\sqrt{-d}]$ is of finite index in $\mathcal{O}_S$. \hfill \Box
Define $\gamma$ and $\psi_1$ as in case 1. We modify the definition of $\psi_2$ 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 $\Gamma_0$ is a subgroup of finite index in $SL_2(\mathcal{O}_S)$.

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

$$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \subset \Gamma_0 \quad \text{and} \quad \begin{pmatrix} 1 & \sqrt{-d}a \\ 0 & 1 \end{pmatrix} \subset \Gamma_0.$$ (21)

Then for $x \in a$, using Bruhat decomposition (see [4, 8.3]) of $\psi_2$, we have

$$\psi_2 \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = u \begin{pmatrix} 1 & h^2dx \\ 0 & 1 \end{pmatrix} \in \Gamma_0 \quad \text{where} \quad u = \begin{pmatrix} 1 & 0 \\ h\sqrt{-d}a & 1 \end{pmatrix}. $$ (22)

Let $b = h^2da$. Then we have

$$u \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \subset \Gamma_0 \quad \text{and} \quad u \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \subset \Gamma_0.$$ (23)

Let $\Gamma_1$ be the subgroup of $SL_2(\mathcal{O}_F)$ generated by $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$. Then, by (23), we have $u\Gamma_1 \subset \Gamma_0$. By Theorem 9, the index of $\Gamma_1$ in $SL_2(\mathcal{O}_F)$ is finite. Thus it follows that there exists an integer $N$ such that

$$\gamma^N \in \Gamma_1 \cap \Gamma_0.$$ (24)

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

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

$$\Gamma_0 \supset \begin{pmatrix} 1 & 0 \\ \sqrt{-d}c & 1 \end{pmatrix}$$ (25)

where $c := (\alpha^{2N} - 1)\mathbb{Z}[\alpha^2] \cap a$. Now $c + \sqrt{-d}c$ is a subgroup of finite index in $\mathcal{O}_{S(F)}[\sqrt{-d}]$ and hence in $\mathcal{O}_S$. Therefore, the group $c + \sqrt{-d}c$ contains a nonzero ideal $q$ of $\mathcal{O}_S$. Since $c \subset a$, by (21) and (25), we have

$$\begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} \subset \Gamma_0.$$ (26)

Again, for $y \in a$, using the Bruhat decomposition of $\psi_1$, we have

$$\psi_1 \begin{pmatrix} 1 & y\sqrt{-d} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ h^2yd & 1 \end{pmatrix} \in \Gamma_0$$ (27)
where \( v = \left( \begin{array}{cc} 1 & \frac{1}{h} \\ 0 & 1 \end{array} \right) \) and \( \varphi = \left( \begin{array}{cc} 1 & 0 \\ 0 & \frac{1}{\sqrt{-d}} \end{array} \right) \). Thus we have

\[
\psi \varphi \left( \begin{array}{cc} 1 & b \\ 0 & 1 \end{array} \right) \subset \Gamma_0, \quad \text{and} \quad \psi \varphi \left( \begin{array}{cc} 1 & 0 \\ b & 1 \end{array} \right) \subset \Gamma_0.
\]

Therefore, \( \psi \varphi \Gamma_1 \subset \Gamma_0 \) and hence \( \psi \varphi \gamma^N \in \Gamma_1 \cap \Gamma_0 \). Thus, using (24) we have

\[
\psi \varphi \gamma^N \gamma^{-N} = \left( \begin{array}{cc} 1 & (1 - \alpha^{2N})\frac{1}{h} \\ 0 & 1 \end{array} \right) \in \Gamma_0.
\]

Again by conjugating this element and its powers by nonnegative powers of \( \gamma \), one shows that

\[
\psi \varphi c^N \psi^{-N} \subset \Gamma_0.
\]

Since \( c \subset a \), by (21) and (30), we have

\[
\psi \varphi q^N \psi^{-N} \subset \Gamma_0.
\]

It follows from (26) and (31), and by Theorem 9, that the group \( \Gamma_0 \) is a subgroup of finite index in \( SL_2(O_S) \). This completes the proof of Theorem 1. \( \Box \)

REFERENCES

[1] D. A. Marcus, *Number fields*, Springer Verlag, 1977.
[2] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, INC 1991.
[3] Ritumoni Sarma, T. N. Venkataramana, *Generators of Arithmetic Groups*, (to appear in Geometriae Dedicata).
[4] T. A. Springer, *Linear Algebraic Groups*, Progress in Math. Vol. 9. Birkhauser, second ed., 1998.
[5] L. N. Vaserstein, *On the Group SL_2 over Dedekind Rings of Arithmetic type*, Math. USSR; Sbornik, 18 (1972), No.2, p. 321-332.

Harish-Chandra Research Institute, Jhunsi, Chhatnag road, Allahabad, India.

E-mail address: ritumoni@mri.ernet.in