Width of $\text{SL}(n, \mathcal{O}_S, I)$

Pavel Gvozdevsky
Chebyshev Laboratory, St. Petersburg State University, Saint Petersburg, Russia

ABSTRACT
We give an estimate for the width of the congruence subgroup $\text{SL}(n, \mathcal{O}_S, I)$ in Tits–Vaserstein generators, where $\mathcal{O}_S$ is a localization of the ring of integers in a number field $K$. We assume that either $K$ has a real embedding, or the ideal $I$ is prime to the number of roots of unity in $K$.

1. Introduction
Given a group $G$ with generating set $X$, the width of $G$ in generators from $X$ is a minimal number $N$ such that any element of $G$ is a product of at most $N$ elements from $X$. When the width is finite, we say that $G$ admits bounded generation with respect to $X$.

For special linear group, or more generally for Chevalley groups bounded generation with respect to the elementary generators is known for certain classes of rings. For example this holds for Dedekind domains of arithmetic type, see [4–7, 9, 11, 12, 20, 21, 23–28]. These results are of great value, for example they are connected to the congruence subgroup property, see [10, 13]; to Margulis–Zimmer conjecture, see [16]; and have applications in logic, see, for example, [1, 2].

In [17], it was proven that the principal congruence subgroup $G(\Phi, \mathcal{O}_S, I)$ of a classical Chevalley group with $\text{rk} \Phi \geq 2$ over a Dedekind domain $\mathcal{O}_S$ of arithmetic type has finite width in Tits–Vaserstein generators, provided the fraction field of $\mathcal{O}_S$ has a real embedding. Also this result can be deduced from [23]. However, either way the proof relies on results from [22], which on its turn are not constructive and do not allow to obtain an explicit estimate of the width in question. In Section 5, we show how one can obtain such a proof directly from the result of [4].

In the main part of the present paper we prove an effective version of the result from [17] for special linear group, i.e. the width of $\text{SL}(n, \mathcal{O}_S, I)$ will be estimated explicitly.

First we consider the double $\mathcal{O}$ of the ring $\mathcal{O}$ with respect to the ideal $I$, where $\mathcal{O}$ is the ring of integers in a number field, and adopt the technique from [4] in order to give an estimate for how many elementary transvections from $\text{SL}(3, \mathcal{O})$ is enough to present any matrix from $\text{SL}(2, \mathcal{O})$ (Theorem 3.1). Then we generalize this result to a localization $\mathcal{O}_S$ of the ring $\mathcal{O}$ (Corollary 3.2). After that we use these results to estimate the width of $\text{SL}(n, \mathcal{O}_S, I)$ in Tits–Vaserstein generators (Corollary 3.5). Finally, considering two ideals $A,B \subseteq \mathcal{O}_S$, we use the proof of Lemma 7 in [30] in order to estimate the width of $\text{SL}(n, \mathcal{O}_S, AB)$ in generators $[t_{i,j}(a), t_{h,k}(b)]$, where $1 \leq i \neq j \leq n$, $1 \leq h \neq k \leq n$, $a \in A$ and $b \in B$. 

CONTACT Pavel Gvozdevsky gvozdevskiy96@gmail.com Chebyshev Laboratory, St. Petersburg State University, 14th Line V.O., 298, Saint Petersburg 199178, Russia.
This article has been corrected with minor changes. These changes do not impact the academic content of the article.
© 2022 Taylor & Francis Group, LLC
The paper is organized as follows. In Section 2 we give the necessary preliminaries and introduce basic notation. In Section 3 we formulate Theorem 3.1 and prove its corollaries as described above. In Section 4 we give the proof of Theorem 3.1. In Section 5 we give some final remarks.

I am grateful to Nikolai Vavilov for optimizing the proof of Corollary 3.4.

2. Preliminaries and notation

2.1. Special linear group

For a commutative ring \( R \) we denote by \( \text{SL}(n, R) \) the group of \( n \times n \) matrices over \( R \) with determinant one. By \( t_{i,j}(ξ) \), where \( 1 \leq i \neq j \leq n \) and \( ξ \in R \), we denote an elementary transvection, i.e. the matrix that has 1 in all the diagonal positions, \( ξ \) in the position \( (i,j) \) and 0 in all the remaining positions. By \( E(n, R) \) we denote the elementary group, i.e. the subgroup of \( \text{SL}(n, R) \) generated by all the elementary transvections.

2.2. Congruence subgroups

For an ideal \( I \trianglelefteq R \), we denote the principal congruence subgroup, i.e. the normal closure of \( \{ t_{i,j}(ξ) : ξ ∈ I \} \), where \( E \) denotes the elementary congruence subgroup, i.e. the normal closure of \( E(n, I) \) in \( E(n, R) \).

As a group \( E(n, R, I) \) is generated by Tits–Vaserstein generators
\[
\{ t_{i,j}(ξ) t_{i,j}(ζ) : ξ ∈ I, ζ ∈ \mathcal{O}_S \},
\]
see, for example, Theorem 2 in [29].

In the present paper, we consider the localization \( \mathcal{O}_S \) of the ring \( \mathcal{O} \) of integers in a number field \( K \). We assume that either \( K \) has a real embedding, or the ideal \( I \) is prime to \( m \), where \( m \) be the number of roots of unity in \( K \). Under these assumptions it follows from [3] that \( E(n, \mathcal{O}_S, I) = \text{SL}(n, \mathcal{O}_S, I) \). Corollary 3.5 of the present paper gives an estimate for the width of \( \text{SL}(n, \mathcal{O}_S, I) \) in Tits–Vaserstein generators.

2.3. Double of a ring

Let \( R \) be a commutative ring, and \( I \trianglelefteq R \) be an ideal. The double of the ring \( R \) with respect to the ideal \( I \) is a subring of \( R \times R \) that consists of pairs with elements congruent to each other modulo \( I \):
\[
\tilde{R} = \{ (a, b) ∈ R × R : a ≡ b \mod I \}.
\]

We will use the following lemma.

**Lemma 2.1.** Let \( b = (b', b'') ∈ \tilde{R} \) be such that \( b' \) (and hence \( b'' \)) is prime to \( I \). Then the natural map
\[
\tilde{R}/b\tilde{R} \to R/b'R × R/b''R
\]
is an isomorphism.

**Proof.** It is easy to see that \( \text{Ker}(\tilde{R} \to R/b'R) = b\tilde{R} + (0, I) \) and \( \text{Ker}(\tilde{R} \to R/b''R) = b\tilde{R} + (I, 0) \). These two ideals are comaximal, because \( \tilde{R}/(I, I) = R/I \) and by assumption the image of \( b \) in \( R/I \) is invertible. Hence we have
\[
b\tilde{R} ≤ (b\tilde{R} + (0, I)) ∩ (b\tilde{R} + (I, 0)) = (b\tilde{R} + (0, I))(b\tilde{R} + (I, 0)) ≤ b\tilde{R}.
\]
So we have
\[
b\tilde{R} + (0, I)) ∩ (b\tilde{R} + (I, 0)) = b\tilde{R}.
\]
The statement of the lemma now follows from the Chinese remainder theorem. □
3. Statement of the main theorem and proofs of corollaries.

Let $O$ be the ring of integers in an algebraic number field $K$. Let $D$ be the discriminant of $K$ and $Cl(K)$ be its class group. Let $m$ be the number of roots of unity in $K$. For any rational prime $p$ set $e_p = \text{ord}_p(m)$, i.e. $m = \prod_{|p| > 0} p^{e_p}$. Further for any rational prime $p$ we denote by $L_p$ the extension of $K$ obtained by adjoining a primitive $p^{e_p+1}$-th root of unity. Now set

$$S_{\text{bad}} = \{ p \in \mathbb{P} : p \mid D \text{ and } \gcd([L_p : K], [Cl(K)]) > 1 \},$$

where $\mathbb{P}$ denotes the set of rational primes. Finally, set

$$\Delta = \max_{\delta_1 + \delta_2 + \delta_3 = |S_{\text{bad}}|} \left( \sum_{i=1}^{3} \max(1, \lceil \ln(\delta_i + 1)/\ln 2 \rceil) \right),$$

where maximum is taken over all triples of nonnegative integers $\delta_1, \delta_2, \delta_3$ with $\delta_1 + \delta_2 + \delta_3 = |S_{\text{bad}}|$.

The main result of the present paper is the following theorem.

**Theorem 3.1.** In the notation above, let $I$ be a non zero ideal in $O$. Suppose that either $K$ has a real embedding, or $I$ is prime to $m$. Let $\tilde{O}$ be the double of the ring $O$ with respect to the ideal $I$. Then for any matrix $(a/b, c/d) \in SL(2, \tilde{O})$ the matrix

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL(3, \tilde{O})$$

is a product of at most $68\Delta + 4$ elementary transvections.

We prove this theorem in Section 4. Now we deduce the corollary for localizations of the ring $O$.

**Corollary 3.2.** In the notation above, let $S$ be a multiplicative system in $O$, let $O_S = O[S^{-1}]$, and $I_S$ be a non zero ideal in $O_S$. Suppose that either $K$ has a real embedding, or $I_S$ is prime to $m$. Let $\tilde{O}_S$ be the double of the ring $O_S$ with respect to the ideal $I_S$. Then for any matrix $(a/b, c/d) \in SL(2, \tilde{O}_S)$ the matrix

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL(3, \tilde{O}_S)$$

is a product of at most $68\Delta + 8$ elementary transvections.

**Proof.** Let $I$ be the preimage of $I_S$ in $O$. Note that any element $s \in S$ is prime to $I$. Indeed, let $I = \prod p_i^{k_i}$ be the decomposition of $I$ into a product of primes, and assume that $s$ belongs to one of the $p_i$, say $p_1$. Then the localization homomorphism maps $\prod_{i \neq 1} p_i^{k_i}$ to $I_S$, hence $\prod_{i \neq 1} p_i^{k_i} \leq I$, which is a contradiction.

It follows that, if $I_S$ is prime to $m$ in $O_S$, then $I$ is prime to $m$ in $O$. Indeed, in this case the ideal $mO + I$ must contain an element $s \in S$; and since $mO + I$ also contains $I$, it follows that $mO + I = O$.

Therefore, Theorem 3.1 can be applied to the ring $O$ and the ideal $I$. It is easy to see that $O_S = \tilde{O}[S^{-1}]$, where $S$ is embeded into $O_S$ diagonally; and $\tilde{O}$ maps to $\tilde{O}_S$ injectively. So it remains to prove that any matrix $(a_1/b_1, c_1/d_1) \in SL(2, \tilde{O}_S)$ can be transformed to a matrix from $SL(2, \tilde{O})$ by 4 elementary transformations.

We perform these transformations as follows. At the first step, we multiply our matrix on the right by a suitable transvection, so that in the new matrix $(a_2/b_2, c_2/d_2)$ the entry $a_2$ became prime to $(I_S, I_S)$. This is possible because the ring $\tilde{O}_S/(I_S, I_S) \simeq O/I$ is semilocal.

Now let $a_2 = (a'_2, a''_2)$ and $b_1 = (b'_1, b''_1)$. Both $a'_2$ and $a''_2$ are prime to $I_S$, so in particular, they are non zero; hence $O \to \tilde{O}_S/a'_2 \tilde{O}_S$ is surjective. Hence we can choose $b'_2 \in O$ such that $b'_2 \equiv b'_1 \pmod{a'_2 \tilde{O}_S}$. Moreover, since $a'_2$ is prime to $I_S$ and every element of $S$ is prime to $I$ in $O$, it follows that the numerator
of \( a' \) is prime to \( I \) in \( \mathcal{O} \); hence changing \( b' \) by a multiple of that numerator, we may assume that \( b' = 1 \) mod \( I \). Similarly, we choose \( b'' \in \mathcal{O} \) so that \( b'' = b_1' \) mod \( a'' \mathcal{O}_S \) and \( b'' = 1 \) mod \( I \). By construction, we have \( b_1 = (b_1', b''_1) \in \mathcal{O} \). Since \( b_1 = b_1' \) mod \( a'' \mathcal{O}_S \), \( b''_1 \) mod \( a'' \mathcal{O}_S \), and \( a''_1 \) is prime to \( I \), it follows by Lemma 2.1 that \( b_1 = 1 \) mod \( a'' \mathcal{O}_S \). Therefore, at the second step, we can multiply our matrix from the right by a suitable transvection to transform it into the matrix \((a''_2 b''_2)\).

Now we factor \( b' \mathcal{O} = b'_1 b'_2 \), such that no prime divisors of \( b'_1 \) meet \( S \) and such that all prime divisors of \( b'_2 \) meet \( S \). Similarly, we factor \( b'' \mathcal{O} = b''_1 b''_2 \). Further, choose \( v', v'' \in \mathcal{O} \) such that \( v' \equiv a''_1 \) mod \( b''_1 \mathcal{O}_S \) and \( v'' \equiv a''_1 \) mod \( b''_1 \mathcal{O}_S \). By the Chinese remainder theorem we may now choose \( a'_3, a''_3 \in \mathcal{O} \) such that

\[
\begin{align*}
a'_3 &\equiv v' \mod b'_1 \mathcal{O}, & a'_3 &\equiv 1 \mod b'_1 I, \\
a''_3 &\equiv v'' \mod b''_1 \mathcal{O}, & a''_3 &\equiv 1 \mod b''_1 I.
\end{align*}
\]

By construction, we have \( a_3 = (a'_3, a''_3) \in \mathcal{O} \). Since \( a'_3 \equiv a'_2 \) mod \( b''_2 \mathcal{O}_S \), \( a''_3 \equiv a''_2 \) mod \( b''_2 \mathcal{O}_S \), and \( b'_2 \) is prime to \( I \), it follows by Lemma 2.1 that \( a_3 \equiv a_2 \) mod \( b_2 \mathcal{O}_S \). Therefore, at the third step, we can multiply our matrix from the right by a suitable transvection to transform it into the matrix \((a''_3 b''_3)\).

In addition, by construction, we have \( a'_3 \mathcal{O} + b'_2 \mathcal{O} = a''_3 \mathcal{O} + b''_2 \mathcal{O} = \mathcal{O} \). Thus \( a'_3 \) is invertible modulo \( b'_2 \mathcal{O} \) and \( a''_3 \) is invertible modulo \( b''_2 \mathcal{O} \). It follows then by Lemma 2.1 that \( a_3 \) is invertible modulo \( b_2 \mathcal{O} \), i.e. \( a_3 \mathcal{O} + b_2 \mathcal{O} = \mathcal{O} \). Therefore, at the fourth step, we can multiply our matrix from the left by a suitable transvection to transform it into the matrix from \( SL(2, \mathcal{O}) \).

Now we show that the results above allow to estimate the width of the congruence subgroup \( SL(n, \mathcal{O}_S, I) \). First we consider matrices from the image of the embedding \( SL(2, \mathcal{O}_S, I) \to SL(3, \mathcal{O}_S, I) \).

**Corollary 3.3.** In the notation above, let \( S \) be a multiplicative system in \( \mathcal{O} \), let \( \mathcal{O}_S = \mathcal{O}[S^{-1}] \), and \( I \) be a non zero ideal in \( \mathcal{O}_S \). Suppose that either \( K \) has a real embedding, or \( I \) is prime to \( m \). Then for any matrix \((a b c d) \in SL(2, \mathcal{O}_S, I)\) the matrix

\[
g = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL(3, \mathcal{O}_S, I)
\]

is a product of at most \( 68\Delta + 8 \) elements of type \( t_{i,j}(\xi)^h \), where \( \xi \in I \) and \( h \in SL(3, \mathcal{O}_S) \).

**Proof.** Set \( N = 68\Delta + 8 \). Consider the matrix

\[
\begin{pmatrix} (a, 1) & (b, 0) & (0, 0) \\ (c, 0) & (d, 1) & (0, 0) \\ (0, 0) & (0, 0) & (1, 1) \end{pmatrix} \in SL(3, \mathcal{O}_S).
\]

By Corollary 3.2, this matrix is a product of \( N \) elementary transvections. Thus there exist elements \( \xi_1', \ldots, \xi_N', \xi_1''', \ldots, \xi_N''' \in \mathcal{O}_S \) such that

- \( \xi_k' \equiv \xi_k'' \mod I \) for all \( 1 \leq k \leq N \),
- \( \prod_{k=1}^{N} t_{i_k j_k} (\xi_k') = g \),
- \( \prod_{k=1}^{N} t_{i_k j_k} (\xi_k'') = e \),

for some indices \( i_k, j_k \).

Set \( \xi_k = \xi_k' - \xi_k'' \in I \). Then we have

\[
g = \prod_{k=1}^{N} t_{i_k j_k} (\xi_k') t_{i_k j_k} (\xi_k) = \left( \prod_{k=1}^{N} t_{i_k j_k} (\xi_k') \right) \left( \prod_{k=1}^{N} t_{i_k j_k} (\xi_k'')^{h_k} \right) = \prod_{k=1}^{N} t_{i_k j_k} (\xi_k)^{h_k},
\]

where \( h_k = \prod_{l=k+2}^{N} t_{i_l j_l} (\xi_l'') \).

\( \square \)
Corollary 3.4. Under the conditions of Corollary 3.3, the matrix \( g \) is a product of at most \( 24 \cdot (68\Delta + 8) = 1632\Delta + 192 \) Tits–Vaserstein generators, i.e. elements of type \( t_{i,j}(\xi)^h \), where \( \xi \in I, \zeta \in O_S \).

Proof. Due to Corollary 3.3, it is enough to prove that any element of type \( t_{i,j}(\xi)^h \) is a product of at most 24 elements of type \( t_{i,j}(\xi)^{h'} \).

So let \( g = t_{i,j}(\xi)^h \). Without loss of generality, we assume that \( i = 1, j = 2 \).

We use the technique from [19]. Let

\[
\begin{pmatrix}
    h_1,1 & h_1,2 & h_1,3 \\
    h_2,1 & h_2,2 & h_2,3 \\
    h_3,1 & h_3,2 & h_3,3
\end{pmatrix}
\]

Then we have

\[
t_{1,2}(\xi) = \prod_{k=1}^{3} t_{1,2}(h_{k,3}'(\xi)h_{3,k})t_{1,3}(-h_{k,3}'(\xi)h_{2,k}).
\]

Thus it is enough to express \( (t_{1,2}(h_{k,3}'(\xi)h_{3,k})t_{1,3}(-h_{k,3}'(\xi)h_{2,k}))^h \) as a product of 8 Tits–Vaserstein generators. It follows from [19] that

\[
(t_{1,2}(h_{k,3}'(\xi)h_{3,k})t_{1,3}(-h_{k,3}'(\xi)h_{2,k}))^h = [t_{i,k}(\xi_1)t_{j,k}(\xi_2), t_{k,i}(\xi_1)t_{k,j}(\xi_2)]t_{k,i}(\xi_3)t_{k,j}(\xi_4),
\]

where \( \{i, j, k\} = \{1, 2, 3\} \), \( \xi_1 = h_{k,3}'(\xi)h_{j,1}' \), \( \xi_2 = -h_{k,3}'(\xi)h_{j,1}' \), \( \xi_4 = h_{k,1}'(\xi_1) \), \( \xi_5 = h_{k,1}'(\xi_2) \), \( \xi_3 = h_{k,1}'(\xi_1) \), \( \xi_2 = h_{j,1}' \).

Now we have

\[
(t_{1,2}(h_{k,3}'(\xi)h_{3,k})t_{1,3}(-h_{k,3}'(\xi)h_{2,k}))^h = (t_{k,i}(\xi_1)t_{k,j}(\xi_2))^{t_{i,j}(-\zeta_1)t_{j,k}(-\zeta_2)}t_{k,i}(\xi_3)t_{k,j}(\xi_4),
\]

Thus it remains to express \( (t_{k,i}(\xi_1)t_{k,j}(\xi_2))^{t_{i,j}(-\zeta_1)t_{j,k}(-\zeta_2)} \) as a product of 6 Tits–Vaserstein generators. We have

\[
(t_{k,i}(\xi_1)t_{k,j}(\xi_2))^{t_{i,j}(-\zeta_1)t_{j,k}(-\zeta_2)} = t_{k,i}(\xi_1)^{t_{i,j}(-\zeta_1)t_{j,k}(-\zeta_2)}t_{k,j}(\xi_2)^{t_{i,j}(-\zeta_1)t_{j,k}(-\zeta_2)},
\]

where

\[
t_{k,i}(\xi_1)^{t_{i,j}(-\zeta_1)t_{j,k}(-\zeta_2)} = (t_{j,i}(\xi_1\xi_2)t_{k,i}(\xi_1))^{t_{i,j}(-\zeta_1)} = t_{j,i}(\xi_1\xi_2)t_{j,k}(-\xi_1\xi_1\xi_2)(t_{k,i}(\xi_1))^{t_{i,j}(-\zeta_1)},
\]

and similarly

\[
t_{k,j}(\xi_2)^{t_{i,j}(-\zeta_1)t_{j,k}(-\zeta_2)} = t_{i,j}(\xi_2\xi_1)t_{i,k}(-\xi_2\xi_1\xi_2)(t_{k,j}(\xi_2))^{t_{i,j}(-\zeta_2)}.
\]

That finishes the proof.

Now we estimate the width of \( \text{SL}(n, O_S, I) \) for arbitrary \( n \geq 3 \).

Corollary 3.5. In the notation above, let \( S \) be a multiplicative system in \( O \), let \( O_S = O[S^{-1}] \), and \( I \) be a non zero ideal in \( O_S \). Suppose that either \( K \) has a real embedding, or \( I \) is prime to \( n \). Let \( n \geq 3 \). Then the width of \( \text{SL}(n, O_S, I) \) in Tits–Vaserstein generators \( \{t_{i,j}(\xi)^{h} : \xi \in I, \zeta \in O_S\} \) is at most \( 3n(n - 1)/2 + 2n + 1632\Delta + 185 \).

Proof. By Corollary 4.8 in [17], every element of \( \text{SL}(n, O_S, I) \) can be decomposed into a product of one element of \( \text{SL}(2, O_S, I) \) and at most \( 3n(n - 1)/2 + 2n - 7 \) Tits–Vaserstein generators. It remains to apply Corollary 3.4 to that one element of \( \text{SL}(2, O_S, I) \).

Remark 3.6. Similarly one can give an estimate for the width of a congruence subgroup of the split spinor group. Unfortunately, at the time of this writing there are no proven analog of Corollary 4.8 in [17] for
Chevalley groups of type E; however, one can still give an estimate for the width of a corresponding congruence subgroup as follows. Since the double $\mathcal{O}_S$ of the ring $\mathcal{O}_S$ with respect to the ideal $I$ has Krull dimension equal to one, the proofs of the surjective $K_1$-stability as presented in [8, 14, 15, 18] together with Corollary 3.2 allow to estimate the width of the Chevalley group over $\mathcal{O}_S$ in elementary generators. This gives an estimate for the width of a congruence subgroup in conjugates of elementary generators. After that it is theoretically possible to estimate how many Tits-Vaserstein generators one needs to express such a conjugate in a manner similar to the proof of Corollary 3.4.

**Corollary 3.7.** In the notation above, let $S$ be a multiplicative system in $\mathcal{O}$, let $\mathcal{O}_S = \mathcal{O}[S^{-1}]$, let $A$ and $B$ be non zero ideals in $\mathcal{O}_S$. Suppose that either $K$ has a real embedding, or $AB$ is prime to $m$. Let $n \geq 3$. Then the group $\text{SL}(n, \mathcal{O}_S, AB)$ is generated by commutators $[t_i(a), t_{n,k}(b)]$, where $1 \leq i \neq j \leq n$, $1 \leq k \leq n$, $a \in A$ and $b \in B$; and the width of $\text{SL}(n, \mathcal{O}_S, AB)$ in these generators is at most $12 \cdot (3n(n - 1)/2 + 2n + 1632\Delta + 185) = 18n^2 + 6n + 19584\Delta + 2220$.

**Proof.** Due to Corollary 3.5 it is enough to prove that any Tits–Vaserstein generator for $\text{SL}(n, \mathcal{O}_S, AB)$ is a product of at most 12 such commutators; and that follows from the proof of Lemma 7 in [30].

**Remark 3.8.** Similarly, if one calculates an estimate for the width of congruence subgroup in the spinor group or the Chevalley group of type E in Tits–Vaserstein generators, then multiplying this number by 12 one gets an estimate of the width in elementary commutators similar to those above.

**4. The proof of the main theorem**

For a commutative ring $R$ and an ideal $J \subseteq R$ we denote by $\varepsilon_R(J)$ the exponent of the multiplicative group $(R/J)^*$ with the convention $\varepsilon_R(J) = 0$ if this exponent is infinite. In other words, $\varepsilon_R(J)$ is the smallest positive integer such that for any element $a \in R$ prime to $J$ we have $a^{\varepsilon_R(J)} \equiv 1 \mod J$, or zero if such a positive integer does not exists. For any $b \in R$ we set $\varepsilon_R(b) = \varepsilon_R(bR)$. Also we will omit the ring in the index if it is clear from the context.

The proof of the next proposition is the same as the proof of the main theorem in [4], so we omit it here.

**Proposition 4.1.** Let $R$ be a commutative ring; let $k$, $\Delta$ and $m$ be positive integers; and let $\Omega \subseteq R^2$. Suppose that the two following conditions hold true.

1. Any row $(a_1, b_1)$, where $a_1, b_1 \in R$ and $a_1 R + b_1 R = R$, can be transformed to a row $(a^m, b)$, where $(a, b) \in \Omega$, by $k$ elementary transvections from $\text{SL}(2, R)$.
2. For any $(a, b) \in \Omega$ there exist $c_1, \ldots, c_{\Delta_0} \in R$ and $\gamma_1, \ldots, \gamma_{\Delta_0} \in \mathbb{Z}_{\geq 0}$, where $\Delta_0 \leq \Delta$, such that $\gcd(\gamma_1, \ldots, \gamma_{\Delta_0}) = 1$, and for any $1 \leq i \leq \Delta_0$ we have $c_i b \equiv -1 \mod aR$ and $\gcd(\varepsilon(b), \varepsilon(c_i)) = my_i$.

Then for any matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, R)$ the matrix

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \text{SL}(3, R)$$

is a product of at most $68\Delta + k$ elementary transvections.

In order to prove Theorem 3.1, we apply Proposition 4.1 to the case where $R = \widehat{\mathcal{O}}$, $k = 4$, $\Delta$ is as above, $m$ is the number of roots of unity in $K$, and $\Omega$ be the set of all pairs $(a, b) = ((a', a''), (b', b'')) \in \widehat{\mathcal{O}}^2$ such that the following conditions hold true.
1. $\tilde{a} \tilde{O} + b \tilde{O} = \tilde{O}$;
2. Each of the elements $a',a'',b',b''$ is prime to $I$;
3. $b'\tilde{O}$ and $b''\tilde{O}$ are prime ideals of $\tilde{O}$ with residue characteristic prime to $m$;
4. The residue characteristic of $b'\tilde{O}$ does not divide $\varepsilon_{\tilde{O}}(b'')$, and vice versa.

Therefore it remains to verify conditions (1), (2) of Proposition 4.1 in this setting. The following lemma verifies condition (1).

**Lemma 4.2.** Under the conditions of Theorem 3.1 any row $(a_1, b_1)$, where $a_1, b_1 \in \tilde{O}$ and $a_1 \tilde{O} + b_1 \tilde{O} = \tilde{O}$, can be transformed to a row $(a^m, b)$, where $(a, b) \in \Omega$, by 4 elementary transvections from $SL(2, \tilde{O})$.

**Proof. Step 1.** By one transvection, we transform the row $(a_1, b_1)$ into a row $(a_1, b_2)$, where $b_2$ is prime to the ideal $(mI, mI) \subseteq \tilde{O}$. Equivalently, $b_2 = (b'_2, b''_2)$, where both $b'_2$ and $b''_2$ are prime to $mI$.

Clearly, such a transformation is possible, because $\tilde{O}/(mI, mI)$ is a semilocal ring.

We shall make use of power norm residue symbols and the $m$-th power reciprocity law as described in [3], appendix on number theory. Let $p_1, \ldots, p_r$ be all the rational primes dividing $m$. Fix a positive integer $N$ that is so large that, firstly, for any $K$-prime $p$ lying over one of the $p_i$ any integer element of the completion $K_p$ that is congruent to 1 modulo $p^N$ has an $m$-th root in $K_p$; and secondly, powers in the decomposition of $I$ into $K$-primes do not exceed $N$. Further for any $p_i$ fix a $K$-prime $p_i$ lying over $p_i$.

Then we fix $p_i$-local units $u_i, w_i$ such that

$$\zeta = \prod_{i=1}^r \left( \frac{u_i}{p_i} \right)_m$$

is a primitive $m$-th root of unity. Existence of such $u_i$ and $w_i$ follows from [3] proposition A.17 and the standard properties of power norm residue symbols.

**Step 2.** By one transvection, we transform the row $(a_1, b_2)$ into a row $(a_2, b_2) = ((a'_2, a''_2), (b'_2, b''_2))$, where

- $a'_2 \equiv a' \mod b'_2 \tilde{O}$ and $a''_2 \equiv a'' \mod b''_2 \tilde{O}$;
- $a'_2 \tilde{O}$ and $a''_2 \tilde{O}$ are prime ideals;
- $a'_{i} \equiv a'_{i} \equiv w_i \mod p^N_i$ for $i = 1, \ldots, r$;
- $a'_2 \equiv a''_2 \equiv 1 \mod p_q^N$ for any prime $q$ such that $mI \subseteq q$, $q \neq p_i$ for $i = 1, \ldots, r$;
- $a''_2$ is positive in every real embedding of $K$;
- If $K$ has a real embedding, then $a''_2$ is negative in one such embedding and positive in all remaining real embeddings.

Existence of such $a'_2$ and $a''_2$ follows from the Chinese remainder theorem and the generalized Dirichlet theorem on primes in arithmetic progressions, see A.11 in [3]. By conditions on $a'_2$ and $a''_2$, we have $a'_2 \equiv a''_2 \mod I$, i.e. $a_2 = (a'_2, a''_2) \in \tilde{O}$. Since $b'_2$ is prime to $I$, it follows by Lemma 2.1 that $a_2 \equiv a_1 \mod b_2 \tilde{O}$.

**Step 3.** By one transvection, we transform the row $(a_2, b_2)$ into a row $(a_3, b) = ((a'_3, a''_3), (b', b''))$, where

- $b' \equiv b'_2 \mod a'_2 \tilde{O}$ and $b'' \equiv b''_2 \mod a''_2 \tilde{O}$;
- $b' \equiv b'_2 \mod I$;
- $b' \tilde{O}$ and $b'' \tilde{O}$ are prime ideals;
- $b'$ and $b''$ are prime to $mI$;
- The residue characteristic of $b' \tilde{O}$ does not divide $\varepsilon_{\tilde{O}}(b'')$, and the residue characteristic of $b'' \tilde{O}$ does not divide $\varepsilon_{\tilde{O}}(b')$;
- $a'_3$ is an $m$-th power modulo $b' \tilde{O}$, and $a''_3$ is an $m$-th power modulo $b'' \tilde{O}$.

It is enough to prove that such $b'$ and $b''$ exist; then it would follow by Lemma 2.1 that $b \equiv b_2 \mod a_2 \tilde{O}$. 
It follows from the proof of Lemma 3 of [4] that there exists an element \( v'' \in O \) prime to \( m \) such that the congruence \( b'' \equiv v'' \mod m^N O \) guarantees that \( a''_2 \) is an \( m \)-th power modulo \( b'' O \), provided \( b'' O \) is a prime ideal and \( b'' \equiv b''_2 \mod a''_2 O \). Since it is only residue of \( v'' \) modulo \( m^N \) that matters, we may assume that \( v'' \equiv 1 \mod q \) for any prime \( q \) such that \( I \subseteq q \) but \( m \notin q \). Also we may assume that \( v'' \equiv b''_2 \mod a''_2 O \).

Further let \( \mathfrak{A} = a''_2 m^N I \) and \( H_\mathfrak{A} \) denote the ray class group of \( K \) that correspond to the ideal \( \mathfrak{A} \). By the existence theorem of class field theory there is a finite abelian extension \( K_\mathfrak{A} / K \) for which the Artin reciprocity map gives an isomorphism \( H_\mathfrak{A} \approx \mathrm{Gal}(K_\mathfrak{A} / K) \).

Now we choose \( b' \) such that
\[
\begin{align*}
\bullet & \ b' \equiv b'_2 \mod a'_2 O; \\
\bullet & \ b' \equiv v'' \mod I; \\
\bullet & \ b' O \text{ is a prime ideal}; \\
\bullet & \ \text{The extension } K_\mathfrak{A} / K \text{ is unramified in } b'O, \text{i.e. } b' \text{ is prime to } \mathfrak{A}; \\
\bullet & \ b' \text{ is prime to } mI; \\
\bullet & \ a'_2 \text{ is an } m \text{-th power modulo } b'O;
\end{align*}
\]

Let us prove that such \( b' \) exists. Here we use the conditions of Theorem 3.1, and consider two cases.

**Case 1.** The field \( K \) has no real embeddings and the ideal \( I \) is prime to \( m \).

Similarly to \( v'' \) we can find \( v' \in O \) prime to \( m \) such that the congruence \( b' \equiv v' \mod m^N O \) guarantees that \( a'_2 \) is an \( m \)-th power modulo \( b'O \), provided \( b'O \) is a prime ideal and \( b' \equiv b'_2 \mod a'_2 O \). Since \( mO, a'_2 O \) and \( I \) are pairwise coprime there exist infinitely many prime elements \( b' \) such that
\[
\begin{align*}
b' & \equiv b'_2 \mod a'_2 O, \\
b' & \equiv v'' \mod I, \\
b' & \equiv v' \mod m^N O.
\end{align*}
\]

We choose one avoiding the primes that ramify in \( K_\mathfrak{A} \).

**Case 2.** The field \( K \) has a real embedding.

In this case we have \( m = 2 \). We search for a suitable \( b' \) among prime elements such that
\[
\begin{align*}
b' & \equiv b'_2 \mod a'_2 O, \\
b' & \equiv v'' \mod m^N I.
\end{align*}
\]

The only terms in the quadratic reciprocity law for \( a'_2 \) and \( b' \) that have not been fixed yet are the one corresponding to the ideal \( b'O \) and the one corresponding to the real embedding that makes \( a'_2 \) negative. Therefore, we can guarantee that \( a'_2 \) is a square modulo \( b'O \) by prescribing certain sign for \( b' \) in this embedding. That still leaves infinitely many prime elements. We choose one avoiding the primes that ramify in \( K_\mathfrak{A} \).

Now let \( p \) be the rational prime lying under \( b'O \). Since \( K_\mathfrak{A} / K \) is unramified in \( b'O \) and \( L_p \) is totally ramified in \( b'O \) it follows that \( K_\mathfrak{A} \cap L_p = K \); hence \( \mathrm{Gal}(L_pK_\mathfrak{A} / K) = \mathrm{Gal}(L_p / K) \times \mathrm{Gal}(K_\mathfrak{A} / K) \). We choose an element \( \sigma \in \mathrm{Gal}(L_pK_\mathfrak{A} / K) \) such that \( \mathrm{res}_{K_\mathfrak{A}}(\sigma) = (v''O, K_\mathfrak{A} / K) \), where \( (v''O, K_\mathfrak{A} / K) \) is an Artin symbol, and \( \mathrm{res}_{L_p}(\sigma) \) is nontrivial.

By the Tchebotarev density theorem, there exist infinitely many primes \( p \) such that \( (p, L_pK_\mathfrak{A} / K) = \sigma \). Choose one avoiding the ramified primes and the divisors of \( \varepsilon(b')mI \).

Since \( (p, K_\mathfrak{A} / K) = (v''O, K_\mathfrak{A} / K) \) and since the isomorphism \( H_\mathfrak{A} \approx \mathrm{Gal}(K_\mathfrak{A} / K) \) is given by Artin symbols, it follows that \( p \) and \( v''O \) represent the same element of the ray class group \( H_\mathfrak{A} \). Therefore, there exists \( \lambda \in K \) such that it is multiplicatively congruent to \( 1 \mod \mathfrak{A} \) (i.e. \( \lambda = \lambda_1 / \lambda_2 \), where \( \lambda, \lambda_1, \lambda_2 \in O \) and \( \lambda_1 \equiv \lambda_2 \equiv 1 \mod \mathfrak{A} \)) and \( \lambda v''O = p \). Set \( b'' = \lambda v'' \). Then \( b'' \equiv v'' \mod \mathfrak{A} \) and \( b''O = p \). Since \( (b''O, L_p / K) \) is nontrivial, it follows that \( \varepsilon(b'') \) is not divisible by \( p \), c.f. A.8 of [3].

**Step 4.** By one transvection, we transform the row \((a_2, b)\) into a row \((a^n, b) = ((a', a'')^m, (b', b''))\), where \((a, b) \in \Omega\).
By the previous step, there exist \(a'\) and \(a''\) such that \((a')^m \equiv a'_1 \mod b'O\) and \((a'')^m \equiv a''_2 \mod b''O\). Since \(b'\) and \(b''\) are prime to \(I\), we may assume that \(a' \equiv a''_2 \equiv 1 \mod I\); hence \((a, b) = ((a', a''), (b', b'')) \in \Omega\). Finally, by Lemma 2.1 we have \(a''_1 \equiv a_2 \mod b'O\).

\[\square\]

In order to verify condition (2) of Proposition 4.1, we need the following lemma.

**Lemma 4.3.** In the setting of Theorem 3.1, let \(A\) be a nonzero ideal of \(O\), let \(b \in O\) be a nonzero element such that

i. \(bO\) is a prime ideal with residue characteristic prime to \(m\);

ii. \(bO\) and \(A\) are comaximal.

Let \(S \subseteq \mathbb{P}\) be a finite set of rational primes such that it does not contain the residue characteristic of \(bO\) and one of the following conditions holds: either the Artin symbol \((bO, L_p/K)\) is non trivial for all \(p \in S\); or the Artin symbol \((bO, L_p/K)\) is trivial for all \(p \in S\), but there exists \(\bar{\sigma}_1 \in \text{Gal}(L/K)\), where \(L\) is a composite \(L = \prod_{p \in S} L_p\), such that \(\text{res}_{L_p}(\bar{\sigma}_1)\) is nontrivial for all \(p \in S\).

Then there exists \(c \in O\) such that \(bc \equiv -1 \mod A\) and \(\varepsilon(c) = my\), where none of the primes from \(S\) divide \(\gamma\).

**Proof.** Let \(H_{\mathfrak{A}}\) denote the ray class group of \(K\) that correspond to the ideal \(\mathfrak{A}\). By the existence theorem of class field theory there is a finite abelian extension \(K_{\mathfrak{A}}/K\) for which the Artin reciprocity map gives an isomorphism \(H_{\mathfrak{A}} \simeq \text{Gal}(K_{\mathfrak{A}}/K)\). Consider the composite \(L_{\mathfrak{A}} = LK_{\mathfrak{A}}\).

Now we consider two cases described in the assumptions.

**Case 1** The Artin symbol \((bO, L_p/K)\) is non trivial for all \(p \in S\).

Applying the Tchebotarev density theorem to the extension \(L_{\mathfrak{A}}/K\), we conclude that there are infinitely many \(K\)-primes \(p\) such that \((p, L_{\mathfrak{A}}/K) = (bO, L_{\mathfrak{A}}/K)^{-1}\). Choose one avoiding the ramified primes and the divisors of \(m\mathfrak{A}\).

Let \(c_0\) be any element of \(\mathfrak{O}\) such that \(bc_0 \equiv -1 \mod \mathfrak{A}\). Then \((bO, K_{\mathfrak{A}}/K)^{-1} = (c_0, K_{\mathfrak{A}}/K)\) and hence \((p, K_{\mathfrak{A}}/K) = (c_0, K_{\mathfrak{A}}/K)\). By Artin reciprocity it follows that there exists \(\lambda\) in \(K\) such that it is multiplicatively congruent to \(1 \mod \mathfrak{A}\) and \(\lambda c_0 \mathfrak{O} = p\). Set \(c = \lambda c_0\). Then \(bc \equiv -1 \mod \mathfrak{A}\); and since \((cO, L_{\mathfrak{A}}/K) = (bO, L_{\mathfrak{A}}/K)^{-1}\) has nontrivial restrictions to all the \(L_p\) for \(p \in S\), it follows that \(\text{ord}_p(\varepsilon(c)) = \text{ord}_p(|R/p| - 1) = \text{ord}_p(m)\) for all \(p \in S\). Therefore, \(\varepsilon(c) = my\), where none of the primes from \(S\) divide \(\gamma\).

**Case 2** The Artin symbol \((bO, L_p/K)\) is trivial for all \(p \in S\), but there exists \(\bar{\sigma}_1 \in \text{Gal}(L/K)\) such that \(\text{res}_{L_p}(\bar{\sigma}_1)\) is nontrivial for all \(p \in S\).

Choose \(\sigma_1 \in \text{Gal}(L_{\mathfrak{A}}/K)\) such that \(\text{res}_{L}(\sigma_1) = \bar{\sigma}_1\). Then set \(\sigma_2 = (bO, L_{\mathfrak{A}}/K)\sigma_1^{-1}\).

Applying the Tchebotarev density theorem to the extension \(L_{\mathfrak{A}}/K\), we conclude that there are infinitely many \(K\)-primes \(p_1, p_2\) such that \(\sigma_1^{-1} = (p_i, L_{\mathfrak{A}}/K)\), for \(i = 1, 2\). Choose any two distinct such primes, avoiding the ramified primes and the divisors of \(m\mathfrak{A}\).

Similarly to the previous case, we obtain that the ideal \(p_1p_2\) is principal with the generator \(c\) such that \(bc \equiv -1 \mod \mathfrak{A}\). Since both \(\sigma_1\) and \(\sigma_2\) have nontrivial restrictions to all the \(L_p\) for \(p \in S\), it follows that \(\text{ord}_p(|R/p_1| - 1) = \text{ord}_p(|R/p_2| - 1) = \text{ord}_p(m)\) for all \(p \in S\). Hence \(\varepsilon(c) = \text{lcm}(|R/p_1| - 1, |R/p_2| - 1) = my\), where none of the primes from \(S\) divide \(\gamma\).

\[\square\]

Now we finish the proof of the main theorem. Recall that it remains to verify condition (2) of Proposition 4.1 in the setting above.

So let \((a, b) = ((a', a''), (b', b'')) \in \Omega\). Since \(b'\) is prime to \(I\), it follows from Lemma 2.1 that

\[\varepsilon_{\mathfrak{O}}(b) = \text{lcm}(\varepsilon_{\mathfrak{O}}(b'), \varepsilon_{\mathfrak{O}}(b'')).\]

Recall that \( e_p = \text{ord}_p(m) \). Set

\[
S_0 = \{ p \in \mathbb{P} : \text{ord}_p(\varepsilon(b)) > e_p \}.
\]

Note that \( S_0 \) does not contain residue characteristics of \( b' \) and \( b'' \). Indeed, all the primes from \( S_0 \) are either divisors of \( \varepsilon(b') \) or of \( \varepsilon(b'') \). A divisor of \( \varepsilon(b') \) cannot be the residue characteristic of \( b'' \) by the definition of \( \Omega \) and it cannot be the residue characteristic of \( b' \), because \( |\mathcal{O}/b'| = \varepsilon(b') + 1 \). Similarly, a divisor of \( \varepsilon(b'') \) also cannot coincide with these residue characteristics. Therefore, for \( p \in S_0 \) the extension \( L_p/K \) is unramified in \( b'O \) and \( b'' \), and we can consider the Artin symbols \( (b'/\mathcal{O}, L_p/K) \) and \( (b''/\mathcal{O}, L_p/K) \in \text{Gal}(L_p/K) \).

By the definition of \( S_0 \) for any \( p \in S_0 \) we have either \( \text{ord}_p(\varepsilon(b')) > e_p \) or \( \text{ord}_p(\varepsilon(b'')) > e_p \). In the first case \( (b'/\mathcal{O}, L_p/K) \) is trivial, and in the second case \( (b''/\mathcal{O}, L_p/K) \) is trivial. Therefore, we have

\[
S_0 = S_1 \sqcup S_2 \sqcup S_3,
\]

where

\[
S_1 = \{ p \in S_0 : (b'/\mathcal{O}, L_p/K) = 1 \text{ and } (b''/\mathcal{O}, L_p/K) \neq 1 \},
\]

\[
S_2 = \{ p \in S_0 : (b'/\mathcal{O}, L_p/K) = (b''/\mathcal{O}, L_p/K) = 1 \},
\]

\[
S_3 = \{ p \in S_0 : (b'/\mathcal{O}, L_p/K) \neq 1 \text{ and } (b''/\mathcal{O}, L_p/K) = 1 \}.
\]

Now for \( i = 1, 2, 3 \) set \( \delta_i = |S_i \cap S_{\text{bad}}| \), and \( \Delta_i = \max(1, \ln(\delta_i + 1)/\ln 2) \). Finally, set \( \Delta_0 = \Delta_1 + \Delta_2 + \Delta_3 \). Clearly, \( \Delta_0 \leq \Delta \).

Let us prove that for any \( i \in \{1, 2, 3\} \) we can present \( S_i \) as such a union

\[
S_i = \bigcup_{j=1}^{\Delta_i} S_i^{(j)}
\]

that for any \( 1 \leq j \leq \Delta_i \) there exists an element \( \sigma \in \text{Gal}(L/K) \) with \( \text{res}_{L_p}(\sigma) \) being nontrivial for all \( p \in S_i^{(j)} \), where \( L = \prod_{p \in S_i} L_p \).

Similarly to the proof of Lemma 4 of [4], we obtain that

\[
\text{Gal}(L/K) = \text{Gal}(L_{\text{bad}}/K) \times \prod_{p \in S_i \setminus S_{\text{bad}}} \text{Gal}(L_p/K),
\]

where \( L_{\text{bad}} = \prod_{p \in S_i \cap S_{\text{bad}}} L_p \).

If \( \delta_i = 0 \), then \( \Delta_i = 1 \) and, clearly, we can set \( S_i^{(1)} = S_i \). So assume that \( \delta_i > 0 \). Then by Referee’s Addendum to the paper [4], there exist elements \( \sigma_1, \ldots, \sigma_{\Delta_i} \in \text{Gal}(L_{\text{bad}}/K) \) such that for any \( p \in S_i \cap S_{\text{bad}} \) at least one of the \( \sigma_j \) does not belong to the kernel of the restriction map \( \text{Gal}(L_{\text{bad}}/K) \rightarrow \text{Gal}(L_p/K) \).

Therefore we can set

\[
S_i^{(j)} = (S_i \setminus S_{\text{bad}}) \cup \{ p \in S_i \cap S_{\text{bad}} : \text{res}_{L_p}(\sigma_j) \neq 1 \}.
\]

Now by Lemma 4.3 for any \( 1 \leq i \leq 3 \) and \( 1 \leq j \leq \Delta_i \) there exist elements \( c_{ij}, c_{ij}' \in \mathcal{O} \) such that

\[
b'c_{ij} = -1 \mod a'I,
\]

\[
b''c_{ij}' = -1 \mod a''I,
\]

\[
\varepsilon(c_{ij}) = m\gamma_{ij}',
\]

\[
\varepsilon(c_{ij}') = m\gamma_{ij}'',
\]

where none of the primes from \( S_i^{(j)} \) divides \( \gamma_{ij}' \) or \( \gamma_{ij}'' \).

Here we applied Lemma 4.3 for \( \mathfrak{A} = a'I \) resp. \( \mathfrak{A} = a''I \); and we used that \( b'O \) and \( a'I \) are comaximal, because \( b'O \) and \( a'O \) are comaximal and \( b'O \) and \( I \) are comaximal; similarly \( b''O \) and \( a''I \) are comaximal.
Since the residue characteristics of $b'O$ and $b''O$ are prime to $m$, it follows that both $\varepsilon(b')$ and $\varepsilon(b'')$ are divisible by $m$. Let

$$\varepsilon_{\tilde{O}}(b) = \text{lcm}(\varepsilon(b'), \varepsilon(b'')) = m\gamma.$$ 

Now we set $c_{ij} = (c'_{ij}, c''_{ij})$ and $\gamma_{ij} = \gcd(\varepsilon_{\tilde{O}}(c'_{ij}), \varepsilon_{\tilde{O}}(c''_{ij}))$. Let us verify that these elements satisfy the requirements in condition (2) of Proposition 4.1.

- Since for all $ij$ we have $b'c'_{ij} \equiv b''c''_{ij} \equiv -1$ mod $I$, it follows that $c_{ij} \in \tilde{O}$.
- All the primes dividing $\gamma_{ij}$ also divide $\gamma$ and thus by definition of $S_0$ they belong to $S_0$. But the primes from $S_i^{(j)}$ do not divide $\gamma'_{ij}$ and $\gamma''_{ij}$; hence they do not divide $\text{lcm}(\gamma'_{ij}, \gamma''_{ij})$; hence they do not divide $\gamma_{ij}$. Since $S_0 = \bigcup_{ij} S_i^{(j)}$, it follows that $\gcd_{ij}(\gamma_{ij}) = 1$.
- Since $b'c'_{ij} \equiv -1$ mod $a'O$, $b''c''_{ij} \equiv -1$ mod $a''O$ and $a'$ is prime to $I$, it follows by Lemma 2.1 that $bc_{ij} \equiv -1$ mod $a\tilde{O}$.
- Finally, since $c'_{ij}$ is prime to $I$, it follows by Lemma 2.1 that $\varepsilon_{\tilde{O}}(c_{ij}) = \text{lcm}(\varepsilon_{\tilde{O}}(c'_{ij}), \varepsilon_{\tilde{O}}(c''_{ij}))$.

Therefore,

$$\gcd(\varepsilon_{\tilde{O}}(b), \varepsilon_{\tilde{O}}(c_{ij})) = \gcd(m\gamma, \text{lcm}(m\gamma'_{ij}, m\gamma''_{ij})) = m \gcd(\gamma, \text{lcm}(\gamma'_{ij}, \gamma''_{ij})) = m\gamma_{ij}.$$ 

That finishes the proof of Theorem 3.1.

5. Final remarks

Now we give a quick proof that $E(n, \mathcal{O}_S, I)$ has finite width in Tits–Vaserstein generators without any assumptions on $K$ and $I$ that relies only on the result of [4]. This proof is similar to the one given in [22] for $E(\Phi, I)$; and we will see why this proof does not allow to obtain any explicit estimate.

Proposition 5.1. In the previous notation, let $I$ be a non zero ideal in $\mathcal{O}_S$, and let $n \geq 3$. Then the group $E(n, \mathcal{O}_S, I)$ has finite width in Tits–Vaserstein generators.

Proof. For $g \in E(n, \mathcal{O}_S, I)$ let $l(g)$ be the smallest integer such that $g$ can be expressed as a product of $l(g)$ Tits–Vaserstein generators.

Note that $\mathcal{O}_S/I$ is a finite set, so let $\xi_1, \ldots, \xi_r$ be representatives of all the classes in $\mathcal{O}_S/I$. By [4] any element $g \in E(n, \mathcal{O}_S, I) \leq E(n, \mathcal{O}_S)$ is a product of at most $N$ transvections. We can write it as

$$g = \prod_{u=1}^{N} t_{i_u j_u} (\xi_{k_u} + \xi_u),$$

where $\xi_u \in I$. Then we have

$$g = \prod_{u=1}^{N} t_{i_u j_u} (\xi_u)^{h_u} \cdot \prod_{u=1}^{N} t_{i_u j_u} (\xi_{k_u}),$$

where $h_u = \prod_{v=1}^{u} t_{i_v j_v} (-\xi_{k_v})$. The number $l(t_{i_u j_u} (\xi_u)^{h_u})$ can be estimated in a manner similar to the proof of Corollary 3.4 with some constant $C$. Now let $\Theta$ be the set of all elements of the form

$$\prod_{u=1}^{N} t_{i_u j_u} (\xi_{k_u}),$$

then $\Theta$ is a finite set. Therefore we have

$$l(g) \leq CN + \max_{h \in \Theta \cap E(n, \mathcal{O}_S, I)} l(h).$$

\[\square\]
As we can see this estimate is not explicit because we do not know the bound for \( l(h) \), where \( h \in \Theta \cap E(n, O_S, I) \). We just know that some way to express such \( h \) as a product of Tits–Vaserstein generators exists.

However, we believe that it is possible to generalize the results of the present paper to the arbitrary ideals in \( O_S \), replacing \( SL(n, O_S, I) \) by \( E(n, O_S, I) \). The only problem is the compatibility of certain congruences in step 3 of the proof of Lemma 4.2. Our conjecture is that those congruences will be compatible automatically if the matrix we start with belongs to \( E(3, O_S) \).

**Funding**

Research is supported by Russian Science Foundation grant (project No:22-21-00257).

**References**

1. Avni, N., Lubotzky, A., Meiri, C. (2019). First order rigidity of non-uniform higher rank arithmetic groups. *Invent. Math.* 217:219–240.
2. Avni, N., Meiri, C. (2020). On the model theory of higher rank arithmetic groups. to be completed. Preprint. https://arxiv.org/abs/2004.05039.
3. Bass, H., Milnor, J., Serre, J. P. (1967). Solution of the congruence subgroup problem for \( SL_n \) \((n \geq 3)\) and \( Sp_{2n} \) \((n \geq 2)\). *Publ. Math. Inst. Hautes Études Sci.* 33:59–137.
4. Carter, D., Keller, G. E. (1983). Bounded elementary generation of \( SL_n(\mathcal{O}) \). *Amer. J. Math.* 105:673–687.
5. Carter, D., Keller, G. E. (1984). Elementary expressions for unimodular matrices. *Commun. Algebra* 12:379–389.
6. Erovenko, I. V., Rapinchuk, A. S. (2001). Bounded generation of some \( S \)-arithmetic orthogonal groups. *C. R. Acad. Sci., Paris, Sér. A* 333(5):395–398.
7. Erovenko, I. V., Rapinchuk, A. S. (2006). Bounded generation of \( S \)-arithmetic subgroups of isotropic orthogonal groups over number fields. *J. Number Theory* 119(1):28–48.
8. Gvozdevsky, P. (2020). Improved \( K_1 \)-stability for the embedding \( D_3 \) into \( E_6 \). *Commun. Algebra*, 48(11):4922–4931.
9. Kunyavskii, B., Plotkin, E., Vavilov, N. (2022). Bounded generation and commutator width of chevalley groups: function case. Preprint. https://arxiv.org/abs/2204.10951.
10. Lubotzky, A. (1995). Subgroup growth and congruence subgroups. *Invent. Math.* 119:267–295.
11. Morgan A. V., Rapinchuk A. S., Sury B. (2017). Bounded generation of \( SL_2 \) over rings of \( S \)-integers with infinitely many units. *Algebra Number Theory* 13:383–421.
12. Morris, D. W. (2007). Bounded generation of \( SL(n, A) \) (after D. Carter, G. Keller, and E. Paige). *N. Y. J. Math.* 13:383–421.
13. Platonov, V., Rapinchuk, A. (1992). Abstract properties of \( S \)-arithmetic groups and the congruence subgroup problem. *Izv. Ross. Akad. Nauk, Ser. Mat* 56:483–508.
14. Plotkin, E. B. (1993). Surjective stabilization for \( K_1 \)-functor for some exceptional Chevalley groups. *J. Soviet Math.* 64:751–767.
15. Plotkin, E. B. (1998). On the stability of the \( K_1 \)-functor for Chevalley groups of type \( E_7 \). *J. Algebra* 210:67–85.
16. Shalom, Y., Willis, G. (2013). Commensurated subgroups of arithmetic groups, totally disconnected groups and adelic rigidity. *Geom. Funct. Anal.* 23(5):1631–1683.
17. Sinchuk, S., Smolensky, A. (2018). Decompositions of congruence subgroups of Chevalley groups. *Int. J. Algebra Comput.* 28(6):935–958.
18. Stein, M. R. (1978). Stability theorems for \( K_1 \), \( K_2 \) and related functors modeled on Chevalley groups. *Japan J. Math.* 4:77–108.
19. Stepanov, A. V., Vavilov, N. A. (2000). Decomposition of transvections: theme with variations. *K-Theory* 19(2):109–153.
20. Tavgen, O. I. (1991). Bounded generation of Chevalley groups over rings of algebraic \( S \)-integers. *Math. USSR. Izvestija* 36(1):101–128.
21. Tavgen, O. I. (1992). Bounded generation of normal and twisted Chevalley groups over the rings of \( S \)-integers. *Contemp. Math.* 131(1):409–421.
22. Tavgen, O. I. (1993). *Combinatorial Methods in the Theory of Linear and Arithmetic Groups*. Habilitation thesis, Institute of Mathematics of Belarus Academy of Science.
23. Trost, A. (2019). Finite index subgroups in Chevalley groups are bounded: an addendum to “On bi-invariant word metrics”. Preprint. https://arxiv.org/abs/1808.06376.
24. Trost, A. (2020). Strong boundedness of simply connected split Chevalley groups defined over rings. Preprint. https://arxiv.org/abs/2004.05039.
25. Trost, A. (2021a). Bounded generation by root elements for chevalley groups defined over rings of integers of function fields with an application in strong boundedness. Preprint. https://arxiv.org/abs/2108.12254.
[26] Trost, A. (2021b). Bounded generation for congruence subgroups of Sp_4(R). Preprint. https://arxiv.org/abs/2101.02301.

[27] Trost, A. (2021c). Strong boundedness of SL_2(R) for rings of S-algebraic integers with infinitely many units. Preprint. https://arxiv.org/abs/2105.10972.

[28] Trost, A. (2022). Explicit strong boundedness for higher rank symplectic groups. J. Algebra 604:694–726.

[29] Vaserstein, L. N. (1986). On normal subgroups of Chevalley groups over commutative rings. Tohoku Math. J. 38:219–230.

[30] Vavilov, N. A., Zhang, Z. (2021). Commutators of elementary subgroups: curiouser and curiouser. Transformation Groups. DOI: 10.1007/s00031-021-09662-z.