M. Larsen and D. Q. N. Nguyen (2021) "Polynomial Parametrization for SL_2 over Quadratic Number Rings," International Mathematics Research Notices, Vol. 2021, No. 9, pp. 6993–7003
Advance Access Publication March 13, 2019
doi:10.1093/imrn/rnz046

Polynomial Parametrization for SL_2 over Quadratic Number Rings

Michael Larsen[1] **and Dong Quan Ngoc Nguyen**[2,*]

[1]Department of Mathematics, Indiana University, Bloomington, Indiana 47405, USA and [2]Department of Applied and Computational Mathematics and Statistics, University of Notre Dame, Notre Dame, Indiana 46556, USA

*Correspondence to be sent to: e-mail: dongquan.ngoc.nguyen@nd.edu

If R is the ring of integers of a number field, then there exists a *polynomial parametrization* of the set $\mathrm{SL}_2(R)$, that is, an element $A \in \mathrm{SL}_2(\mathbb{Z}[x_1, \ldots, x_n])$ such that every element of $\mathrm{SL}_2(R)$ is obtained by specializing A via some homomorphism $\mathbb{Z}[x_1, \ldots, x_n] \to R$.

Let R be a commutative ring. We say a subset $S \subset \mathrm{SL}_N(R)$ is *bounded* if there exists an element $A(x_1, \ldots, x_n) \in \mathrm{SL}_N(\mathbb{Z}[x_1, \ldots, x_n])$ such that

$$S \subseteq \{A(r_1, \ldots, r_n) \mid r_i \in R\},$$

and $A(x_1, \ldots, x_n) = I$ has a solution in R^n, where I denotes the identity matrix. It is clear that if S and T are bounded subsets of $\mathrm{SL}_N(R)$, then every subset of S is bounded, and likewise, $S \cup \{I\}$, S^{-1}, and ST are bounded. Thus, $S \cup T \subset (S \cup \{I\})(T \cup \{I\})$ is also bounded. When $\mathrm{SL}_N(R)$ itself is bounded, we say it is *polynomially parametrized*.

For $1 \leq i \neq j \leq N$, the set of elementary matrices $\{e_{ij}^r \mid r \in R\}$, with entry r in position (i, j), is bounded. Therefore, the set of all elementary matrices (i.e., the union of these sets over pairs (i, j)) is again bounded, so for any fixed k, the set of products of k elementary matrices is bounded. Carter and Keller [1] proved that if $N \geq 3$ and R is the ring of integers in any number field, then every element of $\mathrm{SL}_N(R)$ can be written

Received August 23, 2018; Revised January 23, 2019; Accepted January 28, 2019

as a product of k elementary matrices, for k depending on N and R. Thus, $\mathrm{SL}_N(R)$ is polynomially parametrized. This leaves the question as to whether $\mathrm{SL}_2(R)$ is likewise always polynomially parametrized.

When $R^\times$ is infinite, this is known to have an affirmative answer. Vaserstein [6] proved that in this case $\mathrm{SL}_2(R)$ is generated by elementary matrices, and Carter *et al.* [5] proved that this implies that $\mathrm{SL}_2(R)$ is indeed polynomially parametrized (see also recent work by Morgan *et al.* [4] for another proof of this fact). Vaserstein [7] also proved that $\mathrm{SL}_2(\mathbb{Z})$ is polynomially parametrized. This leaves the case of rings of integers in imaginary quadratic fields. The point of this note is to show that the methods of Carter and Keller in [1] and Vaserstein in [7] extend to cover this case as well.

We say $Z \subseteq \mathrm{SL}_2(R)^2$ is *bounded* if there exist bounded sets S and T in $\mathrm{SL}_2(R)$ such that for all pairs $(M,N) \in Z$ there exist $X \in S$ and $Y \in T$ such that

$$N = XMY.$$

In particular, $\{(I,X) \mid X \in S\}$ is bounded if and only if S is bounded in $\mathrm{SL}_2(R)$.

Lemma 1.1. We have the following boundedness statements for $\mathrm{SL}_2(R)^2$:

1. The set $\{(M,M) \mid M \in \mathrm{SL}_2(R)\}$ is bounded.
2. If $Z \subseteq \mathrm{SL}_2(R)^2$ is bounded, then $\{(M,N) \mid (N,M) \in Z\}$ is bounded.
3. If $Z, W \subseteq \mathrm{SL}_2(R)^2$ are bounded, then the set of pairs $(M,P) \in \mathrm{SL}_2(R)^2$ such that there exists N with $(M,N) \in Z$ and $(N,P) \in W$ is bounded.
4. The set of pairs $\{(M,XMY) \mid M \in \mathrm{SL}_2(R),\ X,Y \in \mathrm{SL}_2(\mathbb{Z})\}$ is bounded.
5. The set $\{(M^{-1},M^T) \mid M \in \mathrm{SL}_2(R)\}$ is bounded.

Proof. Part (1) is trivial. Part (2) follows from the fact that if $S \subseteq \mathrm{SL}_2(R)$ is bounded, then S^{-1} is bounded. Part (3) follows from the fact that if $S,T \subseteq \mathrm{SL}_2(R)$ are bounded, then ST is bounded. Part (4) follows from the boundedness of $\mathrm{SL}_2(\mathbb{Z})$. Part (5) follows from (4), together with the identity

$$M^T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} M^{-1} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

■

All ordered pairs of elements of $\mathrm{SL}_2(R)$ whose 1st rows coincide forms a bounded family. This follows from the boundedness of the set of elementary matrices in $\mathrm{SL}_2(R)$.

An ordered pair (a,b) is *primitive* if and only if the elements a and b generate the unit ideal or, equivalently, if and only if there exists an element of $\mathrm{SL}_2(R)$ whose 1st row is $\begin{pmatrix} a & b \end{pmatrix}$. We say a set of ordered pairs $((a,b),(a',b'))$ of primitive pairs is *bounded* if the set of pairs (M,M'), where M and M' have 1st rows $\begin{pmatrix} a & b \end{pmatrix}$ and $\begin{pmatrix} a' & b' \end{pmatrix}$, respectively, is bounded. We indicate this boundedness condition informally by writing $(a,b) \sim (a',b')$ for pairs in the set.

Given a fixed ring R, for polynomials $P_1, Q_1, P_2, Q_2 \in \mathbb{Z}[t_1,\dots,t_k]$ the relation $(P_1,Q_1) \sim (P_2,Q_2)$ we mean the following. First, for any $\vec{a} := (a_1,\dots,a_k) \in R^k$, the pair $(P_1(\vec{a}), Q_1(\vec{a}))$ is primitive if and only if the pair $(P_2(\vec{a}), Q_2(\vec{a}))$ is primitive. Second, the set of pairs $(X_1,X_2) \in \mathrm{SL}_2(R)^2$ such that for some $\vec{a} \in R^k$, the first row of X_i is

$$\begin{pmatrix} P_i(\vec{a}) & Q_i(\vec{a}) \end{pmatrix},$$

for $i = 1,2$, is bounded. By Lemma 1.1, this makes $\sim$ an equivalence relation on $\mathbb{Z}[x_1,\dots,x_k]^2$.

Lemma 1.2. For every ring R, we have

$$(t_1,t_2) \sim (t_1, t_2 + t_1 t_3)$$

and

$$(t_1,t_2) \sim (t_1 + t_2 t_3, t_2).$$

Proof. For $a_1,a_2,a_3 \in R$, (a_1,a_2) is primitive if and only if $(a_1, a_2 + a_1 a_3)$ is primitive, and likewise for $(a_1 + a_2 a_3, a_2)$. The boundedness condition follows immediately from the boundedness of the set of elementary matrices in $\mathrm{SL}_2(R)$. ■

The following argument is due to Vaserstein [7].

Proposition 1.3. For any ring R, we have

$$(1 + t_1 t_2, t_2^2 t_3) \sim (1 + t_1 t_2, t_3).$$

Proof. Let t_1,t_2,t_3 map to $a,b,c \in R$, respectively. It is clear that $(1+ab, b^2c)$ primitive implies $(1+ab,c)$ primitive. Conversely, if $1+ab, b^2c \in J$ for some ideal $J \subsetneq R$, then for any maximal ideal $\mathfrak{m}$ containing J, we have $1+ab \in \mathfrak{m}$, hence $b \notin \mathfrak{m}$, so $c \in \mathfrak{m}$, which implies $(1+ab,c)$ is not primitive.

Let

$$A := \mathbb{Z}[x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4]/(x_1y_4 - x_3y_2 - 1,\ y_1x_4 - y_3x_2 - 1).$$

For $\begin{pmatrix} x_1 & y_2 \\ x_3 & y_4 \end{pmatrix}, \begin{pmatrix} y_1 & x_2 \\ y_3 & x_4 \end{pmatrix} \in \mathrm{SL}_2(A)$, setting

$$M := \begin{pmatrix} x_1 & y_2 \\ x_3 & y_4 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x_1 & y_2 \\ x_3 & y_4 \end{pmatrix}^{-1},\ N := \begin{pmatrix} y_1 & x_2 \\ y_3 & x_4 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} y_1 & x_2 \\ y_3 & x_4 \end{pmatrix}^{-1},$$

we see that M and N lie, respectively, in the image of $\mathrm{SL}_2(\mathbb{Z}[x_1, x_3])$ and of $\mathrm{SL}_2(\mathbb{Z}[x_2, x_4])$ in $\mathrm{SL}_2(A)$; namely,

$$M = \begin{pmatrix} 1 - x_1x_3 & x_1^2 \\ -x_3^2 & 1 + x_1x_3 \end{pmatrix},\ N = \begin{pmatrix} 1 - x_2x_4 & x_2^2 \\ -x_4^2 & 1 + x_2x_4 \end{pmatrix}.$$

Writing

$$NMN\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} P(x_1, x_2, x_3, x_4) & Q(x_1, x_2, x_3, x_4) \\ R(x_1, x_2, x_3, x_4) & S(x_1, x_2, x_3, x_4) \end{pmatrix}, \tag{1}$$

the relation

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = I$$

implies that $P - 1$, Q, R, and $S - 1$ vanish at $(1, 0, 0, 1)$. Substituting

$$\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = I + z_5\begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix},$$

we see that Q and R are divisible by z_5, so

$$\begin{pmatrix} z_5 & 0 \\ 0 & 1 \end{pmatrix} NMN \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} z_5 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \in \mathrm{SL}_2(\mathbb{Z}[z_1, \ldots, z_5]). \tag{2}$$

For each $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathrm{SL}_2(R)$, the polynomials $x_1y_4 - x_3y_2 - 1$ and $y_1x_4 - y_3x_2 - 1$ both vanish at

$$(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4) = (a_1, a_2, a_3, a_4, a_1, a_2, a_3, a_4),$$

so there exists a unique homomorphism $A \to R$ sending $x_i \mapsto a_i$ and $y_i \mapsto a_i$ for $i = 1, 2, 3, 4$. Specializing (1), we have

$$\begin{aligned} NMN\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} &= A\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}A^{-1}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ &= A\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}A^{-1}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = AA^T, \end{aligned}$$

so

$$\left\{AA^T \,\middle|\, A \in \mathrm{SL}_2(R)\right\}$$

is bounded. Further specializing to the case $A = I + z_5\begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix} \in \mathrm{SL}_2(R)$, (2) implies the boundedness of

$$\left\{\begin{pmatrix} 1+z_5z_1 & z_5^2z_2 \\ z_3 & 1+z_5z_4 \end{pmatrix}\begin{pmatrix} 1+z_5z_1 & z_5^2z_3 \\ z_2 & 1+z_5z_4 \end{pmatrix} \,\middle|\, z_1 + z_4 + z_5(z_1z_4 - z_2z_3) = 0\right\}.$$

The family of pairs

$$\left\{\left(\begin{pmatrix} 1+z_5z_1 & z_5^2z_2 \\ z_3 & 1+z_5z_4 \end{pmatrix}, \begin{pmatrix} 1+z_5z_1 & z_5^2z_3 \\ z_2 & 1+z_5z_4 \end{pmatrix}^{-1}\right)\right\}$$

subject to the condition

$$z_1 + z_4 + z_5(z_1z_4 - z_2z_3) = 0 \tag{3}$$

is therefore bounded, so by part (5) of Lemma 1.1, the same is true for the family of pairs

$$\left\{\left(\begin{pmatrix} 1+z_5z_1 & z_5^2z_2 \\ z_3 & 1+z_5z_4 \end{pmatrix}, \begin{pmatrix} 1+z_5z_1 & z_5^2z_3 \\ z_2 & 1+z_5z_4 \end{pmatrix}^{T}\right)\right\}$$

satisfying (3). If $(1+ab, b^2c)$ is primitive, then substituting $z_1 = a$, $z_2 = c$, $z_5 = b$, we can solve (3) for z_3 and z_4 in R, which proves the proposition. ■

Henceforth, we assume R is the ring of integers in an imaginary quadratic field K.

Proposition 1.4. For R as above,

$$(1 + t_1t_2, t_2t_3) \sim (1 + t_1t_2, t_3).$$

Proof. By Lemma 1.2, for all $d \in R$

$$(1 + ab, bc) \sim (1 + ab, bc + (1 + ab)bd) = (1 + ab, b(c + (1 + ab)d))$$

and

$$(1 + ab, c) \sim (1 + ab, c + (1 + ab)d)),$$

so we may replace c by any element in the same residue class (mod $1+ab$). Since $(c, 1+ab)$ is primitive, by Hasse's theorem (see [3, Satz 13, p. 32]) there exist infinitely many choices $d \in R$, such that $c + (1 + ab)d$ generates a prime ideal in R. In particular, replacing c by this element, we may assume c is relatively prime to $2a$.

We also have for all $e \in R$,

$$(1 + ab, bc) \sim (1 + ab + bce, bc) = (1 + (a + ce)b, bc)$$

and

$$(1 + ab, c) \sim (1 + (a + ce)b, c).$$

Applying Hasse's theorem again, there exist infinitely many $e \in R$ such that $a + ce$ is divisible by 4, and $q := \frac{a+ce}{4}$ generates a prime ideal of R. We may therefore assume $a = 4q$ where q generates a prime ideal not dividing (2). Finally, applying Hasse's theorem a 3rd time, we may choose $p := c + (1 + ab)f$ such that (p) is a prime ideal, and $p \equiv 1 \pmod{8q}$. Using the same argument as above, we may replace c by p.

For every place v of K, let $[-q, p]_v$ denote the Hilbert symbol (which is 1 if and only if $-qx^2 + py^2 = 1$ has a solution in K_v and is -1 otherwise). By Hilbert reciprocity,

$$\prod_v [-q, p]_v = 1.$$

We can restrict the product to finite places of K since the only infinite place is complex. By Hensel's lemma, if v does not lie over 2, $-qx^2+py^2 = 1$ has a solution in K_v if and only if the reduced equation $-\vec{a}rqx^2 + \vec{a}rpy^2 = 1$ has a solution in the residue field k_v. This holds automatically as long as $\vec{a}rq$ and $\vec{a}rp$ are non-zero in k_v, hence over all odd v other than those corresponding to the prime ideals q and p. As $p \equiv 1 \pmod 8$, $\{1-py^2 \mid y \in K_v\}$ contains a neighborhood of 0 if v lies over 2, and it follows that $-qx^2 + py^2 = 1$ has a solution in K_v. As $p \equiv 1 \pmod q$, $-qx^2+py^2 = 1$ has a solution in the completion of K at q. We conclude that $[-q, p]_v = 1$ when v is the place corresponding to p, so the image of $a = 4q$ is congruent (mod p) to an element of the form $-r^2$, for some $r \in R$. Thus, $a \equiv -r^2 \pmod c$.

As $ab \equiv -r^2b \pmod{bc}$,

$$(1 + ab, bc) \sim (1 - r^2b, bc) \sim (1 - r^2b, bc - (1 - r^2b)bc) = (1 - r^2b, r^2b^2c).$$

Applying Proposition 1.3, this is boundedly equivalent to

$$(1 - r^2b, c) \sim (1 + ab, c),$$

and the proposition holds. ■

For n a non-negative integer and $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(R)$, we write

$$\alpha^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}.$$

Thus, for each n, a_n, b_n, c_n, and d_n can be regarded as polynomials in a, b, c, and d with integer coefficients.

Proposition 1.5. For all n and α, we have $(a^n, b) \sim (a_n, b_n)$.

Proof. We define a sequence of polynomials in t as follows:

$$Q_{-1} = -1,\ Q_0 = 0,\ Q_{i+1} = tQ_i - Q_{i-1}\ \forall\, i \geq 0.$$

For $n \geq -1$, we set $u_i := Q_i(\mathrm{Tr}(\alpha))$. By induction on i, we have

$$Q_{i+1}(t)Q_{i-1}(t) = Q_i(t)^2 - 1$$

for $i \geq 0$, so $u_i u_{i-2} = (u_{i-1}+1)(u_{i-1}-1)$ for all $i \geq 1$. In particular, we can write $u_n = v_n w_n$, where v_n divides $u_{n-1}-1$ and w_n divides $u_{n-1}+1$.

By the Cayley–Hamilton theorem, $\alpha^2 = \mathrm{Tr}(\alpha)\alpha - I$, so for all $i \geq 1$,

$$\alpha^i = u_i\alpha - u_{i-1}I.$$

In particular,

$$a_n = au_n - u_{n-1},\ b_n = bu_n = bv_n w_n,$$

so $a_n \equiv 1 \pmod{w_n}$ and $a_n \equiv -1 \pmod{v_n}$. By Proposition 1.4 and part (4) of Lemma 1.1,

$$(a_n, b_n) \sim (a_n, bv_n) \sim (-a_n, -bv_n) \sim (-a_n, -b) \sim (a_n, b).$$

As α is upper triangular $\pmod{b}$, we have $a_n \equiv a^n \pmod{b}$, and the proposition follows. ■

We recall the following result of Carter and Keller.

Lemma 1.6. (Carter–Keller, see [1, Lemma 4, p. 680])

Let F be a number field, $\mathcal{O}$ its ring of integers, and m the number of roots of unity in F. Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}$, and let b be a non-zero element of $\mathcal{O}$ such that

(i) $b\mathcal{O}$ is a prime ideal with residue characteristic prime to m, that is, $b\mathcal{O}$ is a prime ideal, and $\#(\mathcal{O}/b\mathcal{O})$ and m are relatively prime integers.

(ii) $\mathfrak{a}$ and $b\mathcal{O}$ are comaximal, that is, $\mathfrak{a} + b\mathcal{O} = \mathcal{O}$.

Then for every unit $u \in \mathcal{O}^\times$, there exists an element $c \in \mathcal{O}$ such that $bc \equiv u \pmod{\mathfrak{a}}$ and such that the greatest common divisor of $\epsilon(b)$ and $\epsilon(c)$ is $m\gamma$, where γ is a positive integer all of whose rational prime divisors ramify in $F/\mathbb{Q}$ (that is, they divide the discriminant of K). Furthermore, c may be chosen such that γ avoids any single rational prime that ramifies in $F/\mathbb{Q}$. Finally if the class number of K is 1, c may be chosen such that $\gamma = 1$.

Remark 1.7. The above lemma is in [1,Lemma 4, p. 680]. In [1,Lemma 4], Carter and Keller made an additional assumption that $\mathfrak{a}$ is a *prime principal* ideal whereas in the above lemma, we do not impose such condition on $\mathfrak{a}$. In fact the proof of Lemma 4 in [1] given in pages 680–682 does not need such assumption, and thus the proof of the above lemma follows the same lines as that of Lemma 4 in [1]. Note that in the last paragraph of page 683, Carter and Keller applied Lemma 4 to a non-zero ideal $\mathfrak{a}$ that is not necessarily prime; so it seems that the assumption in Lemma 4 that $\mathfrak{a}$ is prime and principal is a typo in [1].

Proposition 1.8. Let $m = |R^\times|$. If $ab \neq 0$ and (a, b) is primitive, then $(a^m, b) \sim (1, 0)$.

Proof. For $k \in R \setminus \{0\}$, let $\epsilon(k)$ denote the exponent of the finite group $(R/kR)^\times$.

Let $p_1, \ldots, p_\ell$ be the distinct prime divisors of the discriminant of $K/\mathbb{Q}$. For each $1 \leq i \leq \ell$, applying Lemma 1.6 for the ideal $a\mathcal{O}$ and the element $b \in \mathcal{O}$ with $u = -1$, one obtains an element $c_i \in \mathcal{O}$ such that the following are satisfied:

(i) $bc_i \equiv -1 \pmod{a\mathcal{O}}$; and

(ii) the greatest common divisor of $\epsilon(b)$ and $\epsilon(c_i)$ is $m\gamma_i$, where γ_i is not divisible by the prime p_i and all prime divisors of γ_i divide the discriminant of $K/\mathbb{Q}$.

By (ii), note that $\gcd(\gamma_1, \ldots, \gamma_\ell) = 1$, and thus there are integers $h_1, \ldots, h_\ell$ such that

$$h_1\gamma_1 + \cdots + h_\ell\gamma_\ell = 1.$$

For each $1 \leq i \leq \ell$, choose $d_i \in \mathcal{O}$ so that

$$N_i = \begin{pmatrix} a & b \\ c_i & d_i \end{pmatrix}.$$

Choose $x, y \in R$ so that

$$M = \begin{pmatrix} a & b \\ x & y \end{pmatrix} \in \mathrm{SL}_2(R).$$

Then

$$M^m = M^{mh_1\gamma_1} \cdots M^{mh_\ell\gamma_\ell}.$$

We claim that $M^{mh_i\gamma_i}$ belongs to a bounded subset of $\mathrm{SL}_2(R)$ for all $1 \leq i \leq \ell$, and thus the same is true of M^m. This implies the proposition.

To prove the claim, take an integer $1 \leq i \leq \ell$. By Proposition 1.5, there exist bounded sets U_1, V_1 in $\mathrm{SL}_2(R)$ such that there exist $X_1 \in U_1$ and $Y_1 \in V_1$ for which

$$X_1 M^{m|h_i\gamma_i|} Y_1 = \begin{pmatrix} a^{m|h_i\gamma_i|} & b \\ x_1 & y_1 \end{pmatrix},$$

for some $x_1, y_1 \in R$. Using the same argument, there exist bounded sets U_2, V_2 in $\mathrm{SL}_2(R)$ such that there exist $X_2 \in U_2$, $Y_2 \in V_2$ for which

$$X_2 \begin{pmatrix} a^{m|h_i\gamma_i|} & b \\ x_1 & y_1 \end{pmatrix} Y_2 = N_i^{m|h_i\gamma_i|}.$$

Let s, t be positive integers such that $t - s = m\gamma_i$, s is divisible by $\epsilon(c_i)$, and t is divisible by $\epsilon(b)$. Then

$$(1,0) \sim (a^t, b) \sim (a_t, b_t),$$

so N_i^t belongs to a bounded subset of $\mathrm{SL}_2(R)$, which does not depend on (a, b). Likewise,

$$(1,0) \sim (a^s, c) \sim (a_s, c_s),$$

so $(N_i^T)^s$ belongs to a bounded subset of $\mathrm{SL}_2(R)$. By part (5) of Lemma 1.1, N_i^{-s} belongs to a bounded subset of $\mathrm{SL}_2(R)$, so the same is true of $N_i^{m\gamma_i} = N_i^{t-s}$. Thus, $N_i^{m|h_i\gamma_i|}$ belongs to a bounded subset of $\mathrm{SL}_2(R)$, so the same is true of $M^{m|h_i\gamma_i|}$. Therefore, $M^{mh_i\gamma_i}$ belongs to a bounded subset of $\mathrm{SL}_2(R)$ for all $1 \leq i \leq \ell$, which proves our claim. ■

Theorem 1.9. If R is the ring of integers in an imaginary quadratic field, then $\mathrm{SL}_2(R)$ is polynomially parametrized.

Proof. It suffices to prove that if $(s, t) \in R^2$ is primitive, then $(1, 0) \sim (s, t)$. By [1, Lemma 3], there exists $a, b \in R$ such that $(s, t) \sim (a^m, d)$, where $m = |R^\times|$. Proposition 1.8 implies that $(a^m, d) \sim (1, 0)$. ■

Remark 1.10. If A is a commutative ring such that $\mathrm{SL}_2(A)$ is polynomially parametrized, it is natural to ask what is *the smallest number of parameters needed to polynomially parametrize* $\mathrm{SL}_2(A)$. We do not attempt to answer this question in this paper. With a detailed analysis of the proof of Theorem 1.8, one could in principle find an *explicit* upper bound for the smallest number of parameters needed for $\mathrm{SL}_2(R)$, where R is the ring of integers of an imaginary quadratic number field.

There are several explicit results of this kind in the literature. Vaserstein [7] gives an upper bound of 46 for $\mathrm{SL}_2(\mathbb{Z})$. Morgan *et al.* [4] show that if $\mathcal{O}$ is a ring of S-integers in a number field K such that the group of units $\mathcal{O}^\times$ is infinite, then 18 is an upper bound for $\mathrm{SL}_2(\mathcal{O})$. (This bound was originally given by Cooke and Weinberger [2], assuming the Generalized Riemann Hypothesis.) If $\mathcal{O}$ is the ring of integers in a number field, Zannier [8] proves that a lower bound for the number of parameters needed for $SL_2(\mathcal{O})$ is 4. It is a natural question as to whether there exists a uniform upper bound for the number of parameters needed for $SL_2(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers of an arbitrary number field.

Funding

ML was partially supported by NSF Grant DMS-1702152 and DQNN was partially supported by DARPA grant N66001-17-1-4041.

Acknowledgments

The 2nd-named author thanks Andrei Rapinchuk for useful correspondence regarding Remark 1.7. We would both like to thank the referee for pointing out an error in the proof of Proposition 1.3 in an earlier draft of this paper.

References

[1] Carter, D. and G. Keller. “Bounded elementary generation of SL_n ($\mathcal{O}$).” *Amer. J. Math.* 105, no. 3 (1983): 673–687.

[2] Cooke, G. and P. J. Weinberger. “On the construction of division chains in algebraic number rings, with applications to SL_2.” *Commun. Algebra* 3, no. 6 (1975): 481–524.

[3] Hasse, H. “Bericht über neuere Unterschungen und Probleme aus der Theorie der algebraischen Zahlkörper.” *Jahresber. Deutsch. Math.-Verein.* 35 (1926): 1–55.

[4] Morgan, A. V., A. S. Rapinchuk, and B. Sury. “Bounded generation of SL_2 over rings of S-integers with infinitely many units.” *Algebra Number Theory* 12, no. 8 (2018): 1949–74 .

[5] Morris, D. W. “Bounded generation of SL (n, A) (after D. Carter, G. Keller, and E. Paige).” *New York J. Math.* 13 (2007): 383–421.

[6] Vaserstein, L. “The group SL_2 over Dedekind rings of arithmetic type.” *Mat. Sb. (N. S.)* 89(131) (1972): 313–22, 351. [In Russian].

[7] Vaserstein, L. “Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups.” *Ann. of Math. (2)* 171, no. 2 (2010): 979–1009.

[8] Zannier, U. “Remarks on a question of Skolem about the integer solutions of $x_1x_2 - x_3x_4 = 1$.” *Acta Arith.* 78 (1996), no. 2, 153–64.