Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)
Vol. XVII (2017), 205-230

Certain sets over function fields are polynomial families

NGUYEN NGOC DONG QUAN

Abstract. In 1938, Skolem conjectured that $\mathbf{SL}_n(\mathbb{Z})$ is not a polynomial family for any $n \geq 2$. Carter and Keller disproved Skolem's conjecture for all $n \geq 3$ by proving that $\mathbf{SL}_n(\mathbb{Z})$ is boundedly generated by the elementary matrices, and hence a polynomial family for any $n \geq 3$. Only recently, Vaserstein refuted Skolem's conjecture completely by showing that $\mathbf{SL}_2(\mathbb{Z})$ is a polynomial family. An immediate consequence of Vaserstein's theorem also implies that $\mathbf{SL}_n(\mathbb{Z})$ is a polynomial family for any $n \geq 3$. In this paper, we prove a function field analogue of Vaserstein's theorem: that is, if $\mathbf{A}$ is the ring of polynomials over a finite field of odd characteristic, then $\mathbf{SL}_2(\mathbf{A})$ is a polynomial family in 52 variables. A consequence of our main result also implies that $\mathbf{SL}_n(\mathbf{A})$ is a polynomial family for any $n \geq 3$.

Mathematics Subject Classification (2010): 11D72 (primary); 11R58 (secondary).

1. Introduction

Let $\mathfrak{R}$ be a commutative ring with identity, and let $\mathcal{X}$ be a subset of $\mathfrak{R}^h$. The set $\mathcal{X}$ is said to be a *polynomial family over* $\mathfrak{R}$ *with d parameters* for some positive integer d if there exist polynomials $\mathcal{P}_1, \ldots, \mathcal{P}_h \in \mathfrak{R}[x_1, \ldots, x_d]$ in d variables $x_1, \ldots, x_d$ such that

$$\mathcal{X} = \mathcal{P}(\mathfrak{R}^d),$$

where $\mathcal{P}$ is the polynomial map in d variables $x_1, \ldots, x_d$ of the form

$$\mathcal{P}(x_1, \ldots, x_d) = (\mathcal{P}_1(x_1, \ldots, x_d), \ldots, \mathcal{P}_h(x_1, \ldots, x_d)).$$

We also say that $\mathcal{P}$ is a *polynomial parametrization of* $\mathcal{X}$.

Determining whether a set in $\mathfrak{R}^h$ is a polynomial family has a long history dating back to the 17th century. For example, when $\mathfrak{R} = \mathbb{Z}$, Lagrange's four-square theorem, née Bachet's conjecture, states that every nonnegative integer can be represented as the sum of four integer squares. Equivalently, the theorem says

Received July 9, 2015; accepted in revised form November 3, 2015.
Published online March 2017.

that the set $\mathbb{Z}_{\geq 0}$ of nonnegative integers is a polynomial family with 4 parameters, and the polynomial $\mathcal{P} \in \mathbb{Z}[x_1, x_2, x_3, x_4]$ defined by

$$\mathcal{P}(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

is a polynomial parametrization of $\mathbb{Z}_{\geq 0}$.

In [13, page 23], Skolem conjectured that $\mathbf{SL}_n(\mathbb{Z})$ is not a polynomial family for any $n \geq 2$. Carter and Keller [3] disproved this for all $n \geq 3$ by proving that $\mathbf{SL}_n(\mathbb{Z})$ is *boundedly generated by the elementary matrices* for each $n \geq 3$, and thus is a polynomial family for each $n \geq 3$.

Recall that a group $\mathcal{G}$ is said to be *boundedly generated by a subset* Γ *of* $\mathcal{G}$ if there exists a positive integer ℓ such that every element $g \in \mathcal{G}$ can be written in the form

$$g = \gamma_1 \cdots \gamma_r,$$

where $r \leq \ell$, and the γ_i are elements of $\Gamma \cup \Gamma^{-1}$. We further say that $\mathcal{G}$ is *boundedly generated by the elementary matrices* if Γ is the set of elementary matrices.

When Γ is invariant under the map $\phi : \mathcal{G} \to \mathcal{G}, g \mapsto g^{-1}$ and contains the identity element of $\mathcal{G}$, then $\Gamma \cup \Gamma^{-1} = \Gamma$, and one can write

$$\mathcal{G} = \underbrace{\Gamma \cdot \Gamma \cdots \Gamma}_{r \text{ copies of } \Gamma}.$$

When Γ is a finite union of cyclic groups, the above definition leads to the following: $\mathcal{G}$ *is said to have bounded generation if there exist cyclic subgroups* $\Gamma_1, \ldots, \Gamma_h$ *of* $\mathcal{G}$ *for some integer* $h \geq 1$ *such that* $\mathcal{G} = \Gamma_1 \Gamma_2 \cdots \Gamma_h$.

Fix an integer $n \geq 2$. For any integers i, j with $1 \leq i \neq j \leq n$ and $\alpha \in \mathbb{Z}$, let $\mathcal{E}_{i,j}(\alpha)$ be the matrix in $\mathbf{SL}_n(\mathbb{Z})$ such that all the entries on the diagonal are 1, the (i, j) entry is α, and all other entries are 0. Set

$$\mathcal{E}_{i,j}(\mathbb{Z}) = \{\mathcal{E}_{i,j}(\alpha) \mid \alpha \in \mathbb{Z}\}.$$

It is known that the $\mathcal{E}_{i,j}(\mathbb{Z})$ are cyclic subgroups of $\mathbf{SL}_n(\mathbb{Z})$, and the set of elementary matrices in $\mathbf{SL}_n(\mathbb{Z})$ is a union of the $\mathcal{E}_{i,j}(\mathbb{Z})$. Thus for a fixed integer $n \geq 2$, if $\mathbf{SL}_n(\mathbb{Z})$ is boundedly generated by the elementary matrices, then $\mathbf{SL}_n(\mathbb{Z})$ has bounded generation. For example, Carter–Keller's theorem [3] implies that $\mathbf{SL}_n(\mathbb{Z})$ has bounded generation for all $n \geq 3$.

It is well-known that $\mathbf{SL}_2(\mathbb{Z})$ is finitely generated, but not boundedly generated by the elementary matrices since it has a free subgroup of index 12. Indeed, assume the contrary, *i.e.*, $\mathbf{SL}_2(\mathbb{Z})$ is boundedly generated by the elementary matrices. It then follows from the above discussion that $\mathbf{SL}_2(\mathbb{Z})$ has bounded generation. The next result is well-known, and its proof can be found, for example, in [7, Proposition 1.1].

Proposition 1.1. *Let* $\mathcal{G}$ *be a group, and* $\mathcal{S}$ *be a subgroup of* $\mathcal{G}$ *such that* $[\mathcal{G} : \mathcal{S}]$ *is finite. Then* $\mathcal{G}$ *has bounded generation if and only if* $\mathcal{S}$ *has bounded generation.*

Let $\mathcal{S}$ be the subgroup of $\mathbf{SL}_2(\mathbb{Z})$ that is generated by $\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}$. Sanov's theorem tells us that $\mathcal{S}$ is a free group, and $[\mathbf{SL}_2(\mathbb{Z}) : \mathcal{S}] = 12$. By Proposition 1.1, $\mathcal{S}$ has bounded generation, which is a contradiction since nonabelian free groups do not have bounded generation (see Tavgen' [14]). Thus $\mathbf{SL}_2(\mathbb{Z})$ is not boundedly generated by the elementary matrices. It is worth mentioning here that Tavgen' [14] even proved that if F is either $\mathbb{Q}$ or an imaginary quadratic field over $\mathbb{Q}$, then the elementary matrices do not boundedly generate $\mathbf{SL}_2(\mathcal{O}_F)$, where $\mathcal{O}_F$ is the ring of integers of F.

The above discussion implies that one cannot expect to use the same arguments as Carter and Keller [3] to disprove Skolem's conjecture for $\mathbf{SL}_2(\mathbb{Z})$. In fact, only recently, Vaserstein [16] refuted Skolem's conjecture completely by proving that $\mathbf{SL}_2(\mathbb{Z})$ is a polynomial family with 46 parameters. As an immediate consequence, Vaserstein also showed that $\mathbf{SL}_n(\mathbb{Z})$ with $n \geq 3$ is a polynomial family with less parameters than in the work of Carter and Keller [3]. Following the work of Vaserstein, it is not difficult to show that for a commutative ring $\mathfrak{R}$ satisfying the second Bass stable range condition (see Bass [1] for this definition), if $\mathbf{SL}_2(\mathfrak{R})$ is a polynomial family, then so is $\mathbf{SL}_n(\mathfrak{R})$ for any $n \geq 3$. It is well-known (see Bass [1]) that every Dedekind domain satisfies the second Bass stable range condition, and hence for such a domain $\mathfrak{R}$, it suffices to consider whether $\mathbf{SL}_2(\mathfrak{R})$ is a polynomial family.

Now return to a general setting in which we fix a commutative ring $\mathfrak{R}$ with identity. The question whether $\mathbf{SL}_2(\mathfrak{R})$ is a polynomial family can be rephrased in terms of the solutions of a Diophantine equation as follows. One can realize $\mathbf{SL}_2$ as a hypersurface in $\mathbb{A}^4$ by

$$x_1x_2 - x_3x_4 = 1. \tag{1.1}$$

Then $\mathbf{SL}_2(\mathfrak{R})$ is a polynomial family if and only if all the $\mathfrak{R}$-integral solutions of (1.1) can be obtained from a fixed polynomial parametrization with coefficients in $\mathfrak{R}$ by letting all the variables run through $\mathfrak{R}$. For example, Vaserstein's theorem says that all the integral solutions of (1.1) can be obtained from a fixed polynomial parametrization with $\mathbb{Z}$-coefficients in 46 parameters by letting all the variables run through $\mathbb{Z}$.

It is natural to consider the solutions of a Diophantine equation in a more general ring than the ring $\mathbb{Z}$ of integers. In this direction, it is natural to extend Vaserstein's theorem to a ring of integers in a number field or a function field. Before discussing related results in this direction, let us fix some notation.

For each $h \geq 1$, we denote by $\mathcal{F}_{2h}\big(m^{(1)}, \ldots, m^{(2h)}\big) \in \mathbf{SL}_2\big(\mathbb{Z}\big[m^{(1)}, \ldots, m^{(2h)}\big]\big)$ the polynomial matrix in $2h$ parameters defined by

$$\mathcal{F}_{2h}(m^{(1)}, \ldots, m^{(2h)}) = \begin{pmatrix}1 & m^{(1)}\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ m^{(2)} & 1\end{pmatrix}\cdots\begin{pmatrix}1 & m^{(2h-1)}\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ m^{(2h)} & 1\end{pmatrix}.$$

Similarly, for each integer $h \geq 0$, we denote by $\mathcal{F}_{2h+1}(m^{(1)}, \ldots, m^{(2h+1)}) \in \mathbf{SL}_2(\mathbb{Z}[m^{(1)}, \ldots, m^{(2h+1)}])$ the polynomial matrix in $2h+1$ parameters defined by

$$\begin{aligned}&\mathcal{F}_{2h+1}(m^{(1)}, \ldots, m^{(2h+1)})\\ &= \begin{pmatrix} 1 & m^{(1)} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ m^{(2)} & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & m^{(2h-1)} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ m^{(2h)} & 1 \end{pmatrix} \begin{pmatrix} 1 & m^{(2h+1)} \\ 0 & 1 \end{pmatrix}.\end{aligned}$$

Since the $\mathcal{F}_n$ are defined over the integers, one can view the $\mathcal{F}_n$ as elements in $\mathbf{SL}_2(\mathfrak{R}[m^{(1)}, \ldots, m^{(n)}])$, where $\mathfrak{R}$ is a commutative ring with 1. When $\mathfrak{R}$ is the polynomial ring in one variable with coefficients in the finite field of q elements, the definition of the $\mathcal{F}_n$ agrees with that of the matrix maps, also denoted by $\mathcal{F}_n$, in Subsection 2.1.

In 1996, Zannier [18] proved that conditionally under the truth of the Generalized Riemann Hypothesis, $\mathcal{F}_5$ is surjective over $\mathbb{Z}[\sqrt{2}]$, which implies that $\mathbf{SL}_2(\mathbb{Z}[\sqrt{2}])$ is a polynomial family with 5 parameters. In 2003, Zannier [19] unconditionally showed that $\mathcal{F}_5$ is surjective over $\mathcal{O}_S$, which implies that $\mathbf{SL}_2(\mathcal{O}_S)$ is a polynomial family with 5 parameters. Here $S = \{2, 3, \wp\}$ with $\wp$ being a prime such that $\wp \equiv 1 \pmod 4$, and $\mathcal{O}_S$ is the ring of S-integers in $\mathbb{Q}$ defined by

$$\begin{aligned}\mathcal{O}_S = \big\{q \in \mathbb{Q} \mid &\text{there exist nonnegative integers } \alpha_2, \alpha_3, \alpha_\wp \\ &\text{such that } q 2^{\alpha_2} 3^{\alpha_3} \wp^{\alpha_\wp} \in \mathbb{Z}\big\}.\end{aligned} \tag{1.2}$$

Before discussing the work of Zannier in more detail, let us digress a moment to explain the relation between the maps $\mathcal{F}_n$ and continued fractions.

Let $\lambda_1, \ldots, \lambda_m$ be real numbers such that $\lambda_i \geq 1$ for each $2 \leq i \leq m$. For each integer $1 \leq h \leq m$, the symbol $[\lambda_1, \ldots, \lambda_h]$ is defined recursively by $[\lambda_1] = \lambda_1$, and $[\lambda_1, \lambda_2, \ldots, \lambda_h] = \lambda_1 + \dfrac{1}{[\lambda_2, \ldots, \lambda_h]}$. (Note that $[\lambda_2, \ldots, \lambda_h] > 0$ by the assumption that $\lambda_i \geq 1$ for each $i \geq 2$; so the symbol $[\lambda_1, \ldots, \lambda_h]$ is well-defined.)

Assume now that the λ_i lie in $\mathbb{Z}$. Then the symbol $[\lambda_1, \ldots, \lambda_h]$ is the *h-th convergent of the continued fraction*. It is clear that the h-th convergent is a rational number.

For each $1 \leq h \leq m$, let

$$\frac{P_h}{Q_h} = [\lambda_1, \ldots, \lambda_h],$$

where P_h, Q_h are relatively prime integers. We are only interested in a special case when $m = 2n$ for some positive integer n. If we let $P_0 = Q_{-1} = 1$ and $P_{-1} = Q_0 = 0$, then it is known that $P_h = \lambda_h P_{h-1} + P_{h-2}$ and $Q_h = \lambda_h Q_{h-1} + Q_{h-2}$ for each $h \geq 1$. Since $P_{2n} Q_{2n-1} - P_{2n-1} Q_{2n} = (-1)^{2n} = 1$, there exists an integer μ such that

$$\begin{pmatrix} 1 & 0 \\ -\lambda_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\lambda_2 \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ -\lambda_{2n-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & -\lambda_{2n} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} P_{2n} & Q_{2n} \\ P_{2n-1} & Q_{2n-1} \end{pmatrix} = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix},$$

and thus

$$\begin{pmatrix} P_{2n} & Q_{2n} \\ P_{2n-1} & Q_{2n-1} \end{pmatrix} = \begin{pmatrix} 1 & \lambda_{2n} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \lambda_{2n-1} & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & \lambda_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \lambda_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$$
$$= \mathcal{F}_{2n+1}(\lambda_{2n}, \ldots, \lambda_1, \mu).$$

When $n = 2$, Zannier [18] proved that the Generalized Riemann Hypothesis implies the surjectivity of the matrix map on the left-hand side of the above equation over $\mathbb{Z}[\sqrt{2}]$. Hence $\mathcal{F}_5$ is surjective over $\mathbb{Z}[\sqrt{2}]$ by the above equation. Replaced $\mathbb{Z}[\sqrt{2}]$ by $\mathcal{O}_S$ with $\mathcal{O}_S$ defined by (1.2), Zannier [19] unconditionally obtained the same results.

In 2007, Morris [10] provided details of a proof of the next result that is contained in an unpublished work of Carter, Keller, and Paige [4].

Theorem 1.2 (Carter–Keller–Paige, see [4] and [10, Theorem 1.2]). *Let F be a number field, and let $\mathcal{O}_F$ be the ring of integers of F. Then $\mathbf{SL}_2(\mathcal{O}_F)$ is boundedly generated by the elementary matrices if and only if $\mathcal{O}_F$ has infinitely many units.*

The Carter–Keller–Paige theorem provides a very large class of rings $\mathfrak{R}$ for which $\mathbf{SL}_2(\mathfrak{R})$ is a polynomial family. In fact, the theorem proves that if F is a number field such that $F \neq \mathbb{Q}$ and F is not an imaginary quadratic field over $\mathbb{Q}$, then $\mathbf{SL}_2(\mathcal{O}_F)$ is a polynomial family. Hence, in the number field setting, it remains to consider whether or not $\mathbf{SL}_2(\mathcal{O}_F)$ is a polynomial family when F is an imaginary quadratic field.

Since $\mathbb{Z}[\sqrt{2}]$ contains infinitely many units, Theorem 1.2 also provides a group-theoretic proof of Zannier's result that $\mathbf{SL}_2(\mathbb{Z}[\sqrt{2}])$ is a polynomial family. Although Theorem 1.2 provides an unconditional proof of a corollary of Zannier's result, it does not give an explicit bound for the number of parameters as obtained in the work of Zannier [18].

The bounded number of elementary matrices needed to generate $\mathbf{SL}_2(\mathcal{O}_F)$ in Theorem 1.2 depends on the Compactness Theorem in Model Theory (see [9, Theorem 2.1.4]). Thus Theorem 1.2 does not provide any explicit bound on the number of elementary matrices. It is natural to ask the following questions.

Question 1.3.

(i) Let F be a number field, and let $\mathcal{O}_F$ be the ring of integers of F. Assume that $\mathcal{O}_F$ has infinitely many units. What is an explicit bound for the number of elementary matrices needed to generate $\mathbf{SL}_2(\mathcal{O}_F)$?
(ii) Does there exist a positive integer $\mathcal{U}$ such that for any number field F with the ring of integers $\mathcal{O}_F$ containing infinitely many units, the number of elementary matrices needed to generate $\mathbf{SL}_2(\mathcal{O}_F)$ is less than $\mathcal{U}$?

Let F be a number field, and let $\mathcal{O}_F$ be the ring of integers of F. Let S be a finite set of primes of F that contains all the Archimedean primes. Let $\mathcal{O}_{S,F}$ be the ring of S-integers of F, and let U_S denote the group of units in $\mathcal{O}_{S,F}$. When U_S is infinite,

Cooke and Weinberger [5] proved that the Generalized Riemann Hypothesis implies that $\mathbf{SL}_2(\mathcal{O}_{S,F})$ is a polynomial family with 9 parameters. They further showed that if F admits a real embedding, then 7 parameters are sufficient. The results of Cooke-Weinberger [5] provide a conditional answer to the above questions under the truth of the Generalized Riemann Hypothesis. It is interesting if one can obtain another proof of Theorem 1.2 that does not use the Compactness Theorem in Model Theory. Such a proof should shed some light on the above questions from another viewpoint that may result in an unconditional answer to the above questions.

In Zannier [18, 19], the number of elementary matrices needed to generate $\mathbf{SL}_2(\mathbb{Z}[\sqrt{2}])$ or $\mathbf{SL}_2(\mathcal{O}_S)$ with $\mathcal{O}_S$ defined by (1.2) is 5, which is quite small. It is possible, as remarked in Zannier [19] that 5 should be the smallest number of parameters needed over $\mathbb{Z}[\sqrt{2}]$ or the rings $\mathcal{O}_S$. This motivates the following question.

Question 1.4. If $\mathfrak{R}$ is a ring such that $\mathbf{SL}_2(\mathfrak{R})$ is a polynomial family, what is the smallest number of parameters needed to polynomially parametrize $\mathbf{SL}_2(\mathfrak{R})$?

For each ring $\mathfrak{R}$ with $\mathbf{SL}_2(\mathfrak{R})$ being a polynomial family, denote by $\mathcal{M}(\mathfrak{R})$ the smallest number parameters needed to polynomially parametrize $\mathbf{SL}_2(\mathfrak{R})$. Then Theorem 1 in Zannier [18] shows that $\mathcal{M}(\mathcal{O}_K) \geq 4$ if $\mathcal{O}_K$ is the ring of integers in a number field K. In particular, Vaserstein's theorem [16] combined with Zannier's theorem [18] imply that $4 \leq \mathcal{M}(\mathbb{Z}) \leq 46$. It is certainly interesting if one can find a precise value of $\mathcal{M}(\mathfrak{R})$, where $\mathfrak{R}$ is the ring of integers in a number field or a function field.

Let p be an *odd* prime, and let q be a power of p. Let $\mathbf{A} = \mathbb{F}_q[T]$, where $\mathbb{F}_q$ is the finite field with q elements, and T denotes an indeterminate. The main aim of this paper is to determine an upper bound for $\mathcal{M}(\mathbf{A})$; more precisely, our main goal in this paper is to prove the following.

Theorem 1.5 (See Theorem 3.8). $\mathbf{SL}_2(\mathbf{A})$ *is a polynomial family with* 52 *parameters*.

Despite many strong analogies between $\mathbb{Z}$ and $\mathbf{A}$ (see Goss [6], Rosen [12], Thakur [15], or Weil [17] for these analogies), $\mathbf{SL}_2(\mathbf{A})$ does not always bear a resemblance to $\mathbf{SL}_2(\mathbb{Z})$. For example, Nagao's theorem (see Nagao [11], or Bux and Wortman [2, Section **2**]) says that $\mathbf{SL}_2(\mathbf{A})$ is not finitely generated. The group $\mathbf{SL}_2(\mathbb{Z})$ is however finitely generated as mentioned before. So it is a nontrivial question as to whether there is an analogue of Vaserstein's theorem for $\mathbf{A}$. Theorem 1.5 answers this questions affirmatively by showing that $\mathbf{SL}_2(\mathbf{A})$ is a polynomial family with 52 parameters.

Throughout the work of Vaserstein [16], the polynomial parametrization of $\mathbf{SL}_2(\mathbb{Z})$ is often used to show many interesting sets in $\mathbb{Z}^h$ are polynomial families. Using similar arguments as in Vaserstein [16], one can use Theorem 1.5 to show many sets in $\mathbf{A}^h$ are polynomial families. As an illustration, let us now consider some applications of Theorem 1.5.

Take any commutative ring $\mathfrak{R}$ with identity 1. Recall that a h-tuple $(m_1, \ldots, m_h) \in \mathfrak{R}^h$ is called *unimodular* if there exist elements $\alpha_1, \ldots, \alpha_h \in \mathfrak{R}$

such that $\sum_{i=1}^{h} \alpha_i m_i = 1$. We denote by $\mathbf{UM}_h(\mathfrak{R})$ the set of all unimodular h-tuples in $\mathfrak{R}^h$.

We say that $\mathfrak{R}$ *satisfies the h-th Bass stable range condition* if for any $(h+1)$-tuple $(m_1, \ldots, m_{h+1}) \in \mathbf{UM}_{h+1}(\mathfrak{R})$, there exist elements $\alpha_1, \ldots, \alpha_h \in \mathbf{A}$ such that the h-tuple $(m_1 + \alpha_1 m_{h+1}, \ldots, m_h + \alpha_h m_{h+1})$ belongs to $\mathbf{UM}_h(\mathfrak{R})$. In notation, we write $\mathbf{SR}(\mathfrak{R}) \leq h$.

Now return to our ring $\mathbf{A}$. It is well-known (see [1, page 14]) that $\mathbf{A}$ satisfies the second Bass stable range condition. Hence it follows from Vaserstein [16, pages 994-995] that $\mathbf{UM}_n(\mathbf{A})$ is a polynomial family with $2n$ parameters for all $n \geq 3$. (In fact, Vaserstein proved that the last result also holds if $\mathbf{A}$ is replaced by any commutative ring $\mathfrak{R}$ with $\mathbf{SR}(\mathfrak{R}) \leq 2$.)

Now take any pair $(a, b) \in \mathbf{UM}_2(\mathbf{A})$. Then there exist $c, d \in \mathbf{A}$ such that $ad - bc = 1$. Set

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{A}).$$

By Theorem 1.5, there are polynomials $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_4 \in \mathbf{A}[x_1, \ldots, x_{52}]$ in 52 variables such that

$$\mathbf{SL}_2(\mathbf{A}) = \begin{pmatrix} \mathcal{P}_1(\mathbf{A}^{52}) & \mathcal{P}_2(\mathbf{A}^{52}) \\ \mathcal{P}_3(\mathbf{A}^{52}) & \mathcal{P}_4(\mathbf{A}^{52}) \end{pmatrix}.$$

We deduce that

$$\begin{aligned}(a, b) = (1, 0)\alpha \in (1, 0)\mathbf{SL}_2(\mathbf{A}) &= (1, 0) \begin{pmatrix} \mathcal{P}_1(\mathbf{A}^{52}) & \mathcal{P}_2(\mathbf{A}^{52}) \\ \mathcal{P}_3(\mathbf{A}^{52}) & \mathcal{P}_4(\mathbf{A}^{52}) \end{pmatrix} \\ &= (\mathcal{P}_1(\mathbf{A}^{52}), \mathcal{P}_2(\mathbf{A}^{52})),\end{aligned}$$

which yields the following result.

Corollary 1.6. $\mathbf{UM}_2(\mathbf{A})$ *is a polynomial family with* 52 *parameters*.

Following the same arguments as in Vaserstein [16, page 998] and using Theorem 1.5, the following result is immediate, and can be proved by induction on n.

Corollary 1.7. $\mathbf{SL}_n(\mathbf{A})$ *is a polynomial family with* $45 + n(3n+1)/2$ *parameters for any* $n \geq 2$.

The proof of Theorem 1.5 in Section 3 shows that there exists a surjective matrix map from $\mathbf{A}^{52}$ to $\mathbf{SL}_2(\mathbf{A})$ with *rational integral coefficients*. Hence Theorem 1.5 also implies that $\mathbf{SL}_2(\bar{\mathbb{F}}_q[T])$ is a polynomial family, where $\bar{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$. It is natural to ask the following question.

Question 1.8. Let $\mathfrak{F} : \mathbb{A}^{52} \to \mathbf{SL}_2$ be the morphism defined over $\mathbb{Z}$ that is constructed in the proof of Theorem 1.5 in Section 3. Does there exist a ring $\mathfrak{R}$ such that the matrix map $\mathfrak{F}(\mathfrak{R}) : \mathbb{A}^{52}(\mathfrak{R}) \to \mathbf{SL}_2(\mathfrak{R})$ is not surjective?

One can ask the same question with $\mathfrak{F}$ replaced by the morphism $\mathfrak{V} : \mathbb{A}^{48} \to \mathbf{SL}_2$ from the work of Vaserstein [16]. In fact we do not even know whether or not the matrix map $\mathfrak{V}(\mathbf{A}) : \mathbb{A}^{48}(\mathbf{A}) \to \mathbf{SL}_2(\mathbf{A})$ arising from the Vaserstein morphism is surjective.

1.1. Main ideas of the proof of Theorem 1.5

In this subsection we explain the main ideas of the proof of Theorem 1.5. Our approach is based on that of Vaserstein in [16], but we need to get round to technical difficulties arising from the function field setting.

A simple but important idea is to prove that for a given matrix $\alpha \in \mathbf{SL}_2(\mathbf{A})$, there exist matrices, say L_α, $R_\alpha \in \mathbf{SL}_2(\mathbf{A})$ that can be polynomially parameterized such that $L_\alpha \alpha R_\alpha$ belongs to a subset of $\mathbf{SL}_2(\mathbf{A})$ that can be easily proved to belong to a polynomial family. Note that a product of matrices in $\mathbf{SL}_2(A)$, each of which comes from a polynomial family, also belongs to a polynomial family. With this remark, one can choose L_α, R_α in such a way that each of them is a product of a fixed number of matrices, each of which belongs to a polynomial family.

Let $\mathbf{S}_{\mathrm{PF}}$ be the subset of $\mathbf{SL}_2(\mathbf{A})$ consisting of all matrices $\begin{pmatrix} a & b \\ c & * \end{pmatrix} \in \mathbf{SL}_2(\mathbf{A})$ that satisfy the following conditions:

(i) $a^{e_1} \equiv \epsilon_1 \pmod{b}$ for some unit $\epsilon_1 \in \mathbb{F}_q^\times$ and some $e_1 \in \mathbb{Z}_{>0}$;
(ii) $a^{e_2} \equiv \epsilon_2 \pmod{c}$ for some unit $\epsilon_2 \in \mathbb{F}_q^\times$ and some $e_2 \in \mathbb{Z}_{>0}$; and
(iii) $\gcd(e_1, e_2) = 1$.

As shown in Corollary 3.6, the set $\mathbf{S}_{\mathrm{PF}}$ belongs to a polynomial family, and in fact, the proof of this fact is the most difficult part in the proof of Theorem 1.5.

The structure of the polynomial ring $\mathbf{A}$ plays an important role when one wants to prove that for a given $\alpha \in \mathbf{SL}_2(\mathbf{A})$, there exist elements $u, v \in \mathbf{A}$ such that

$$\begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} \alpha \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in \mathbf{S}_{\mathrm{PF}}.$$

In order to show this, we use the $(q-1)$-th power residue symbol, and a strong function field analogue of Dirichlet's theorem on primes in arithmetic progressions that is not available in the number field context. This function field analogue of the Dirichlet theorem assures that one can choose $u, v \in \mathbf{A}$ such that both $\wp_1 = au + b$ and $\wp_2 = av + c$ are primes in $\mathbf{A}$, and $\mathbf{deg}(\wp_1)$, $\mathbf{deg}(\wp_2)$ are relative prime. The former is necessary for us to use the $(q-1)$-th power residue symbol, and the latter is crucial to transform α into an element in $\mathbf{S}_{\mathrm{PF}}$. This forms a main part of Lemma 3.7.

It remains to show that $\mathbf{S}_{\mathrm{PF}}$ belongs to a polynomial family. For this purpose, the main difficulty is to show that for a given matrix $\alpha = \begin{pmatrix} a & b \\ c & * \end{pmatrix} \in \mathbf{S}_{\mathrm{PF}}$, there exists a matrix β_{PF} that belongs to a polynomial family such that $\alpha^{r_1} = \beta_{\mathrm{PF}}$ for some positive integer r_1. Condition (i) in the definition of $\mathbf{S}_{\mathrm{PF}}$ plays a central role in proving this fact. If this can be done for α, taking the transpose of α and using condition (ii) in the definition of $\mathbf{S}_{\mathrm{PF}}$, one can also show that there exists a matrix γ_{PF} that belongs to a polynomial family such that $(\alpha^T)^{r_2} = \gamma_{\mathrm{PF}}$ for some positive integer r_2. Hence conjugating both sides of the last equation by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, one gets

$\alpha^{-r_2} = \gamma_{\mathrm{PF}}^{\star}$ for another matrix $\gamma_{\mathrm{PF}}^{\star}$ that also belongs to a polynomial family. Using condition (iii), one can further choose $r_1, r_2 \in \mathbb{Z}_{>0}$ such that $r_1 - r_2 = 1$, and hence

$$\alpha = \alpha^{r_1}\alpha^{-r_2} = \beta_{\mathrm{PF}}\gamma_{\mathrm{PF}}^{\star},$$

which proves that $\mathbf{S}_{\mathrm{PF}}$ belongs to a polynomial family. This will be proved in detail in Corollary 3.6.

In order to prove that condition (i) in the definition of $\mathbf{S}_{\mathrm{PF}}$ implies that for each matrix α in $\mathbf{S}_{\mathrm{PF}}$, some power of α belongs to a polynomial family, the key step is to show that for each $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{A})$ and each positive integer r, there exists a matrix γ_{PF} that belongs to a polynomial family such that

$$\alpha^r = \begin{pmatrix} a^r & \epsilon b \\ * & * \end{pmatrix} \gamma_{\mathrm{PF}} \tag{1.3}$$

for some unit $\epsilon \in \mathbb{F}_q^{\times}$. The first part of Lemma 3.2 shows that a simple use of the Caley-Hamilton theorem implies

$$\alpha^r = \begin{pmatrix} au + v & ub \\ * & * \end{pmatrix}$$

for some $u, v \in \mathbf{A}$. One way to get (1.3) from the last equation is to transform the matrix $\begin{pmatrix} a + ub & ub \\ \star & \star \end{pmatrix}$ into the matrix $\begin{pmatrix} au + v & \epsilon b \\ * & * \end{pmatrix}$ for some unit $\epsilon \in \mathbb{F}_q^{\times}$ by multiplying the former matrix by an appropriate matrix β_{PF} that belongs to a polynomial family. This is proved in Lemma 3.1 whose proof also uses a strong function field analogue of the Dirichlet theorem and the $(q-1)$-th power residue symbol. Note that for each $\alpha \in \mathbf{SL}_2(\mathbf{A})$ and each positive integer r, the matrix γ_{PF} in (1.3) is constructed as a product of a fixed number of matrices, each of which belongs to either the set of elementary matrices, the polynomial family $\mathcal{M}_{\Lambda}$, or the polynomial family $\mathcal{M}_{\Lambda}^{T}$. The last two polynomial families will be introduced in Subsection 2.4.

The structure of this paper is as follows. In Section 2 we introduce some basic notation and necessary tools that will be used to prove Theorem 1.5. We will prove Theorem 1.5 in Section 3.

ACKNOWLEDGEMENTS. I am grateful to the referee for an extremely careful reading of this paper, and suggesting insightful remarks and very useful comments on an earlier version of this paper. I thank Leonid Vaserstein for explaining some of his remarks in [16] to me. I would like to thank my parents, Nguyen Ngoc Quang and Phan Thi Thien Huong, for their constant support over the years.

2. Some basic notation and notions

In this section we introduce some basic notation and notions that will be used throughout this paper. Vaserstein [16] used the polynomial matrices $\Phi_5, \Delta_i, \Gamma_i$ (see [16, pages 990, 992] for their definitions) to construct the polynomial matrix in 46 variables that is a polynomial parametrization of $\mathbf{SL}_2(\mathbb{Z})$. We use the same set of polynomial matrices with different notation to obtain a polynomial parametrization of $\mathbf{SL}_2(\mathbf{A})$; more explicitly, $\Lambda, \mathcal{F}_i, \mathcal{G}_i$ in this paper stand for $\Phi_5, \Delta_i, \Gamma_i$ in Vaserstein [16], respectively.

Note that the main aim of this section is to fix notation and notions for the next section. Hence the reader may wish to skip it on the first reading, and return to it later.

2.1. Definitions of $\mathcal{F}_h, \mathcal{G}_h$

For each $m \in \mathbf{A}$, set $m_{\{1,2\}} = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, and let $m_{\{2,1\}} = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$. Both $m_{\{1,2\}}$ and $m_{\{2,1\}}$ of course are in $\mathbf{SL}_2(\mathbf{A})$.

Although the following result is elementary, it is useful in many places of this paper.

Lemma 2.1. *Let $\alpha \in \mathbf{SL}_2(\mathbf{A})$. Then*

$$(\alpha^{-1})^T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}.$$

For each $h \geq 1$, we denote by $\mathcal{F}_{2h}(m^{(1)}, \ldots, m^{(2h)}) \in \mathbf{SL}_2(\mathbf{A}[m^{(1)}, \ldots, m^{(2h)}])$ the polynomial matrix in $2h$ parameters defined by

$$\begin{aligned} \mathcal{F}_{2h}(m^{(1)}, \ldots, m^{(2h)}) &= m^{(1)}_{\{1,2\}} m^{(2)}_{\{2,1\}} \cdots m^{(2h-1)}_{\{1,2\}} m^{(2h)}_{\{2,1\}} \\ &= \begin{pmatrix} 1 & m^{(1)} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ m^{(2)} & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & m^{(2h-1)} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ m^{(2h)} & 1 \end{pmatrix}. \end{aligned}$$

For each $h \geq 0$, we denote by $\mathcal{F}_{2h+1}(m^{(1)}, \ldots, m^{(2h+1)}) \in \mathbf{SL}_2(\mathbf{A}[m^{(1)}, \ldots, m^{(2h+1)}])$ the polynomial matrix in $2h+1$ parameters defined by

$$\begin{aligned} \mathcal{F}_{2h+1}(m^{(1)}, \ldots, m^{(2h+1)}) &= m^{(1)}_{\{1,2\}} m^{(2)}_{\{2,1\}} \cdots m^{(2h)}_{\{2,1\}} m^{(2h+1)}_{\{1,2\}} \\ &= \begin{pmatrix} 1 & m^{(1)} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ m^{(2)} & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ m^{(2h)} & 1 \end{pmatrix} \begin{pmatrix} 1 & m^{(2h+1)} \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Note that since $\mathbf{SL}_2(\mathbf{A})$ is not boundedly generated by the elementary matrices, none of the $\mathcal{F}_h$ is surjective over $\mathbf{A}$.

For each integer $r \geq 1$, set

$$\mathcal{G}_r(m^{(1)}, \ldots, m^{(r)}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \mathcal{F}_r(m^{(1)}, \ldots, m^{(r)}) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}. \tag{2.1}$$

Equivalently, one can write

$$\mathcal{F}_r(m^{(1)},\dots,m^{(r)}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \mathcal{G}_r(m^{(1)},\dots,m^{(r)}) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}. \tag{2.2}$$

The next result follows immediately from Lemma 2.1.

Lemma 2.2.

(i) *For each integer* $h \geq 1$,

$$\begin{aligned} &\mathcal{G}_{2h}(m^{(1)},\dots,m^{(2h)}) \\ =&(-m^{(1)})_{\{2,1\}}(-m^{(2)})_{\{1,2\}}\cdots(-m^{(2h-1)})_{\{2,1\}}(-m^{(2h)})_{\{1,2\}}; \end{aligned}$$

(ii) *for each integer* $h \geq 0$,

$$\begin{aligned} &\mathcal{G}_{2h+1}(m^{(1)},\dots,m^{(2h+1)}) \\ =&(-m^{(1)})_{\{2,1\}}(-m^{(2)})_{\{1,2\}}\cdots(-m^{(2h)})_{\{1,2\}}(-m^{(2h+1)})_{\{2,1\}}. \end{aligned}$$

For each positive integer r, set

$$\mathcal{G}_r(\mathbf{A}^r) = \left\{\mathcal{G}_r(a_1,a_2,\dots,a_r) \mid (a_1,\dots,a_r) \in \mathbf{A}^r\right\}.$$

The next two lemmas are obvious.

Lemma 2.3.

(i) $\mathcal{F}_i(\mathbf{A}^i) \subset \mathcal{F}_j(\mathbf{A}^j)$ *for any* $1 \leq i < j$;
(ii) $\mathcal{F}_{2h}(\mathbf{A}^{2h})\mathcal{F}_r(\mathbf{A}^r) \subset \mathcal{F}_{2h+r}(\mathbf{A}^{2h+r})$ *for each integer* $h \geq 1$ *and each integer* $r \geq 1$;
(iii) $\mathcal{F}_{2h+1}(\mathbf{A}^{2h+1})\mathcal{F}_r(\mathbf{A}^r) \subset \mathcal{F}_{2h+r}(\mathbf{A}^{2h+r})$ *for each integer* $h \geq 0$ *and each integer* $r \geq 1$.

Lemma 2.4.

(i) $\mathcal{G}_i(\mathbf{A}^i) \subset \mathcal{G}_j(\mathbf{A}^j)$ *for any* $1 \leq i < j$;
(ii) $\mathcal{G}_{2h}(\mathbf{A}^{2h})\mathcal{G}_r(\mathbf{A}^r) \subset \mathcal{G}_{2h+r}(\mathbf{A}^{2h+r})$ *for each integer* $h \geq 1$ *and each integer* $r \geq 1$;
(iii) $\mathcal{G}_{2h+1}(\mathbf{A}^{2h+1})\mathcal{G}_r(\mathbf{A}^r) \subset \mathcal{G}_{2h+r}(\mathbf{A}^{2h+r})$ *for each integer* $h \geq 0$ *and each integer* $r \geq 1$.

The matrices $\begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix}$ and $\begin{pmatrix} 0 & -\epsilon \\ \epsilon^{-1} & 0 \end{pmatrix}$ for any $\epsilon \in \mathbb{F}_q^\times$ appear naturally in the proof of our main theorem. The next result shows that these matrices are contained in $\mathcal{G}_4(\mathbf{A}^4) \cap \mathcal{F}_4(\mathbf{A}^4)$ and $\mathcal{G}_3(\mathbf{A}^3) \cap \mathcal{F}_3(\mathbf{A}^3)$, respectively.

Lemma 2.5. *Let $\epsilon \in \mathbb{F}_q^\times$ be a unit in* $\mathbf{A}$. *Then:*

(i)
$$\begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} \in \mathcal{G}_4(\mathbf{A}^4) \cap \mathcal{F}_4(\mathbf{A}^4);$$

(ii)
$$\begin{pmatrix} 0 & -\epsilon \\ \epsilon^{-1} & 0 \end{pmatrix} \in \mathcal{G}_3(\mathbf{A}^3) \cap \mathcal{F}_3(\mathbf{A}^3).$$

Proof. Part (i) follows immediately by noting that

$$\begin{aligned} \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} &= \mathcal{G}_4((\epsilon-1)/\epsilon, -1, 1-\epsilon, 1/\epsilon) \\ &= \mathcal{F}_4(-\epsilon, \epsilon^{-1}-1, 1, \epsilon-1) \in \mathcal{G}_4(\mathbf{A}^4) \cap \mathcal{F}_4(\mathbf{A}^4). \end{aligned}$$

Since

$$\begin{pmatrix} 0 & -\epsilon \\ \epsilon^{-1} & 0 \end{pmatrix} = \mathcal{G}_3(-\epsilon^{-1}, \epsilon, -\epsilon^{-1}) = \mathcal{F}_3(-\epsilon, \epsilon^{-1}, -\epsilon) \in \mathcal{G}_3(\mathbf{A}^3) \cap \mathcal{F}_3(\mathbf{A}^3),$$

we obtain the assertion in part (ii). □

Combining Lemmas 2.3, 2.4, and 2.5, we obtain the following result that we will need in the proof of our main theorem.

Corollary 2.6.

(i) *For any unit $\epsilon \in \mathbb{F}_q^\times$ and any integer $r \geq 1$,*
$$\begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} \mathcal{G}_r(\mathbf{A}^r) \subset \mathcal{G}_{r+4}(\mathbf{A}^{r+4});$$

(ii) *for any unit $\epsilon \in \mathbb{F}_q^\times$ and any integer $r \geq 1$,*
$$\begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} \mathcal{F}_r(\mathbf{A}^r) \subset \mathcal{F}_{r+4}(\mathbf{A}^{r+4}).$$

2.2. Definition of Ψ

In this subsection we recall the notion of the polynomial matrix Φ_3 in Vaserstein [16, page 989] that will be denoted by Ψ in this paper.

Let $\Psi \in \mathbf{SL}_2(\mathbf{A}[m_1, m_2, m_3])$ be the polynomial matrix in three variables m_1, m_2, m_3 defined by

$$\Psi(m_1, m_2, m_3) = \begin{pmatrix} 1 + m_1m_2m_3 & m_1^2m_3 \\ -m_2^2m_3 & 1 - m_1m_2m_3 \end{pmatrix} \in \mathbf{SL}_2(\mathbf{A}[m_1, m_2, m_3]). \quad (2.3)$$

Note that $\Psi(m_1, m_2, m_3)$ is unipotent in $\mathbf{SL}_2(\mathbf{A}[m_1, m_2, m_3])$ since $(1+m_1m_2m_3)+(1-m_1m_2m_3) = 2$.

Remark 2.7. The following remark is due to the referee. Since Ψ has rational integral coefficients, one can view Ψ as a polynomial matrix in $\mathbf{SL}_2(\mathfrak{R}[m_1, m_2, m_3])$ for any commutative ring $\mathfrak{R}$ with 1. When $\mathfrak{R}$ is a principal ideal domain, one can show that every unipotent matrix in $\mathbf{SL}_2(\mathfrak{R})$ lies in the image of Ψ. Indeed, every unipotent matrix $\mathfrak{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathfrak{R})$ satisfies $a + d = 2$ and $ad - bc = 1$. If we let $a = 1 + w$ for some $w \in \mathfrak{R}$, then

$$\mathfrak{M} = \begin{pmatrix} 1 + w & b \\ c & 1 - w \end{pmatrix}.$$

Since $ad - bc = 1$, we know that $w^2 = -bc$. Set $m_3 = \gcd(b, c)$. Then replacing m_3 by ϵm_3 for some unit $\epsilon \in \mathfrak{R}$, if necessary, one can write $w = m_1 m_2 m_3$, $b = m_1^2 m_3$, and $c = -m_2^2 m_3$ for some $m_1, m_2 \in \mathfrak{R}$. Thus

$$\mathfrak{M} = \begin{pmatrix} 1 + m_1 m_2 m_3 & m_1^2 m_3 \\ -m_2^2 m_3 & 1 - m_1 m_2 m_3 \end{pmatrix},$$

which lies in the image of Ψ.

2.3. Definitions of Γ and $\mathcal{M}_\Gamma$

In this subsection we recall the notion of the polynomial matrix Φ_4 in Vaserstein [16, page 989] that will be denoted by Γ in this paper.

Let $\Gamma \in \mathbf{SL}_2(\mathbf{A}[m_1, m_2, m_3, m_4])$ be the polynomial matrix defined by

$$\begin{aligned}&\Gamma(m_1, m_2, m_3, m_4)\\ =&\begin{pmatrix} 1 - m_2 m_4 & m_2^2 \\ -m_4^2 & 1 + m_2 m_4 \end{pmatrix}\begin{pmatrix} 1 - m_1 m_3 & m_1^2 \\ -m_3^2 & 1 + m_1 m_3 \end{pmatrix}\begin{pmatrix} 1 - m_2 m_4 & m_2^2 \\ -m_4^2 & 1 + m_2 m_4 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.\end{aligned}$$

Set

$$\mathcal{M}_\Gamma = \{\alpha\alpha^T \mid \alpha \in \mathbf{SL}_2(\mathbf{A})\} \subset \mathbf{SL}_2(\mathbf{A}).$$

Following the same arguments as in Vaserstein [16, page 989] with $\mathcal{M}_\Gamma$, Γ in the roles of X_4, Φ_4, respectively, one sees that $\mathcal{M}_\Gamma \subset \Gamma(\mathbf{A}^4)$.

2.4. Definitions of Λ, $\mathcal{M}_\Lambda$, and $\mathcal{M}_\Lambda^T$

In this subsection we recall the notions of Φ_5 and X_5 in Vaserstein [16, page 990] that will be denoted by Λ and $\mathcal{M}_\Lambda$, respectively, in this paper. The polynomial matrix Λ will play a central role in a polynomial parametrization of $\mathbf{SL}_2(\mathbf{A})$.

Let $\Lambda \in \mathbf{SL}_2(\mathbf{A}[m_1, m_2, m_3, m_4, m_5])$ be the polynomial matrix in five variables m_1, m_2, m_3, m_4, m_5 defined by

$$\begin{aligned}&\Lambda(m_1, m_2, m_3, m_4, m_5)\\ =&\begin{pmatrix} m_5 & 0 \\ 0 & 1 \end{pmatrix}\Gamma(1 + m_1 m_5, m_2 m_5, m_3 m_5, 1 + m_4 m_5)\begin{pmatrix} m_5 & 0 \\ 0 & 1 \end{pmatrix}^{-1}.\end{aligned}$$

Let $\mathcal{M}_\Lambda$ be the set of matrices defined by

$$\mathcal{M}_\Lambda = \left\{ \begin{pmatrix} 1+ae & be^2 \\ c & 1+de \end{pmatrix} \begin{pmatrix} 1+ae & ce^2 \\ b & 1+de \end{pmatrix} \mid a,b,c,d,e \in \mathbf{A} \right.$$
$$\left. \text{such that } \begin{pmatrix} 1+ae & be^2 \\ c & 1+de \end{pmatrix} \in \mathbf{SL}_2(\mathbf{A}) \right\}$$

Following the same arguments as in Vaserstein [16, page **990**], we get that

$$\mathcal{M}_\Lambda \subset \Lambda(\mathbf{A}^5) \subset \mathbf{SL}_2(\mathbf{A}). \tag{2.4}$$

Set

$$\mathcal{M}_\Lambda^{-1} = \{\alpha^{-1} \mid \alpha \in \mathcal{M}_\Lambda\},$$
$$\mathcal{M}_\Lambda^{T} = \{\alpha^{T} \mid \alpha \in \mathcal{M}_\Lambda\},$$
$$\mathcal{M}_\Lambda^{-1,T} = \{\alpha^{-1} \mid \alpha \in \mathcal{M}_\Lambda^T\}.$$

The next result follows immediately from Lemma 2.1.

Lemma 2.8.

(i) $\mathcal{M}_\Lambda^{-1} = \mathcal{M}_\Lambda$, *and* $\mathcal{M}_\Lambda^{-1,T} = \mathcal{M}_\Lambda^T$;

(ii)
$$\mathcal{M}_\Lambda^T = \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \mid \alpha \in \mathcal{M}_\Lambda \right\}$$
$$= \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \mid \alpha \in \mathcal{M}_\Lambda \right\};$$

(iii)
$$\mathcal{M}_\Lambda = \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \mid \alpha \in \mathcal{M}_\Lambda^T \right\}$$
$$= \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \mid \alpha \in \mathcal{M}_\Lambda^T \right\}.$$

We define the polynomial matrix $\Lambda^T \in \mathbf{SL}_2(\mathbf{A}[m_1, m_2, m_3, m_4, m_5])$ in five variables m_1, m_2, m_3, m_4, m_5 by

$$\Lambda^T(m_1, m_2, m_3, m_4, m_5) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \Lambda(m_1, m_2, m_3, m_4, m_5) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}.$$

Equation (2.4) and Lemma 2.8 (ii) imply that

$$\mathcal{M}_\Lambda^T \subset \Lambda^T(\mathbf{A}^5). \tag{2.5}$$

2.5. The d-th power residue symbol in A

In this subsection we briefly recall the notion of the d-th power residue symbol. We refer the reader to Rosen [12, Chapter 3] for a more complete account.

Let $\wp$ be a prime in $\mathbf{A}$, and let d be a positive divisor of $q-1$. (Recall that q is the number of elements in $\mathbb{F}_q$.) If m is an element in $\mathbf{A}$ such that $\wp$ does not divide m, then it is well-known (see Rosen [12, pages 23-24]) that there exists a unique element of $\mathbb{F}_q^\times$, denoted by $\left(\frac{m}{\wp}\right)_d$, such that

$$m^{\frac{q^{\mathbf{deg}(\wp)}-1}{d}} \equiv \left(\frac{m}{\wp}\right)_d \pmod{\wp}.$$

If m is an element in $\mathbf{A}$ such that $\wp$ divides m, we simply define $\left(\frac{m}{\wp}\right)_d = 0$. We call the symbol $\left(\frac{m}{\wp}\right)_d$ the *d-th power residue symbol*.

3. $\mathbf{SL_2(A)}$ is a polynomial family

In this section we prove Theorem 1.5. Although our proof is based on the work of Vaserstein [16], we need to introduce new ideas to overcome several technical difficulties arising in the function field setting. Vaserstein [16] used Dirichlet's theorem on primes in arithmetic progressions and the quadratic residue symbol in some auxiliary results to obtain a polynomial parametrization for $\mathbf{SL}_2(\mathbb{Z})$. We cannot use these tools in the function field setting. For the proof of Theorem 1.5, we instead exploit the $(q-1)$-th power residue symbol, and an improved version of the function field analogue of Dirichlet's theorem that justifies the existence of many irreducible polynomials of a given degree d in an arithmetic progression in $\mathbf{A}$, provided that d is sufficiently large.

Lemma 3.1. *Let $a, b, u \in \mathbf{A}$, and let $\alpha = \begin{pmatrix} 1+au & bu \\ * & * \end{pmatrix} \in \mathbf{SL}_2(\mathbf{A})$. Then there exist elements $m, n \in \mathbf{A}$, $\epsilon \in \mathbb{F}_q^\times$, and $\beta \in \mathcal{M}_\Lambda$ such that the matrix*

$$\alpha(um)_{\{1,2\}} n_{\{2,1\}} (-\wp u)_{\{1,2\}} \beta (-\epsilon^{-1} un)_{\{1,2\}} (-\epsilon m)_{\{2,1\}} \tag{3.1}$$

is of the form $\begin{pmatrix} * & * \\ \epsilon b & 1+au \end{pmatrix}$, where $\wp = b + m(1+au)$.

Proof. If $1+au = 0$, letting $m = n = 0$, $\wp = b$, and $\epsilon = -u \in \mathbb{F}_q^\times$, we see that Lemma 3.1 follows immediately.

For the rest of the proof, suppose that $1 + au \neq 0$. Since $\det(\alpha) = 1$, we deduce that $1 + au, b$ are relatively prime in $\mathbf{A}$. Set

$$\wp = b + m(1 + au), \tag{3.2}$$

where m will be determined shortly. By Rosen [12, Theorem 4.8], we know that there are infinitely many elements m in $\mathbf{A}$ such that for such an element m, the polynomial $\wp$ is a monic prime whose degree is congruent to $q - 2$ modulo $q - 1$ and greater than $\mathbf{deg}(b)$. Take such a monic prime $\wp$ of degree greater than $\mathbf{deg}(b)$ for some element $m \in \mathbf{A}$. We know that there is some integer r such that

$$\mathbf{deg}(\wp) = q - 2 + (q - 1)r. \tag{3.3}$$

We now prove that there is an element $\epsilon \in \mathbb{F}_q^\times$ such that

$$a \equiv \epsilon a_1^{q-1} \pmod{\wp}, \tag{3.4}$$

where a_1 is an element in $\mathbf{A}$. Indeed, denote by $\left(\frac{\cdot}{\wp}\right)_{q-1}$ the $(q-1)$-th power residue symbol (see Subsection 2.5 for its definition). If $a \equiv 0 \pmod{\wp}$, then one can take $a_1 = 0$, and (3.4) holds trivially.

If $a \not\equiv 0 \pmod{\wp}$, set

$$\epsilon_1 = \left(\frac{a}{\wp}\right)_{q-1} \in \mathbb{F}_q^\times. \tag{3.5}$$

We see from [12, Proposition 3.2] that

$$\left(\frac{a\epsilon_1}{\wp}\right)_{q-1} = \left(\frac{a}{\wp}\right)_{q-1}\left(\frac{\epsilon_1}{\wp}\right)_{q-1} = \epsilon_1 \left(\epsilon_1^{\frac{q-1}{q-1}\mathbf{deg}(\wp)}\right) = \epsilon_1^{(q-1)(r+1)} = 1,$$

and it thus follows from [12, Proposition 3.1] that there exists an element $a_1 \in \mathbf{A}$ such that $a\epsilon_1 \equiv a_1^{q-1} \pmod{\wp}$. Now (3.4) follows immediately by letting $\epsilon = \epsilon_1^{-1}$.

By (3.4), there exists an element $n \in \mathbf{A}$ such that

$$a + n\wp = \epsilon a_1^{q-1}. \tag{3.6}$$

Set

$$\lambda = \alpha(um)_{\{1,2\}} n_{\{2,1\}} (-\wp u)_{\{1,2\}}. \tag{3.7}$$

We see from (3.2) and (3.6) that

$$\begin{aligned}\lambda = \alpha(um)_{\{1,2\}} n_{\{2,1\}} (-\wp u)_{\{1,2\}} &= \begin{pmatrix} 1+au & bu \\ * & * \end{pmatrix} \begin{pmatrix} 1 & mu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} 1 & -\wp u \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1+au & \wp u \\ * & * \end{pmatrix} \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} 1 & -\wp u \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1+u\epsilon a_1^{q-1} & \wp u \\ * & * \end{pmatrix} \begin{pmatrix} 1 & -\wp u \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1+u\epsilon a_1^{q-1} & -\wp u^2 \epsilon a_1^{q-1} \\ c & d \end{pmatrix}, \end{aligned} \tag{3.8}$$

where c, d are some elements in $\mathbf{A}$.

By (3.7), and since $\alpha \in \mathbf{SL}_2(\mathbf{A})$, we know that $\det(\lambda) = 1$, and thus (3.8) tells us that

$$\lambda^{-1} = \begin{pmatrix} d & \wp u^2 \epsilon a_1^{q-1} \\ -c & 1+u\epsilon a_1^{q-1} \end{pmatrix}.$$

Since p is odd (recall that p is the characteristic of $\mathbb{F}_q$), one can write $q-1 = 2q_1$ for some positive integer q_1, and thus $u^2 a_1^{q-1} = (ua_1^{q_1})^2$. Since $\det(\lambda) = \det(\lambda^{-1}) = 1$, we deduce that $d = 1 + d_1 u a_1^{q_1}$ for some $d_1 \in \mathbf{A}$. Hence λ^{-1} can be written in the form

$$\lambda^{-1} = \begin{pmatrix} 1+d_1\left(ua_1^{q_1}\right) & \wp\epsilon\left(ua_1^{q_1}\right)^2 \\ -c & 1+\left(\epsilon a_1^{q_1}\right)\left(ua_1^{q_1}\right) \end{pmatrix}. \tag{3.9}$$

Set

$$\rho = \begin{pmatrix} 1+d_1\left(ua_1^{q_1}\right) & -c\left(ua_1^{q_1}\right)^2 \\ \epsilon\wp & 1+\left(\epsilon a_1^{q_1}\right)\left(ua_1^{q_1}\right) \end{pmatrix}. \tag{3.10}$$

By (3.6), one can write

$$\rho = \begin{pmatrix} * & * \\ \epsilon\wp & 1+(a+n\wp)u \end{pmatrix}.$$

By (3.9) and (3.10), we see that $\lambda^{-1}\rho \in \mathcal{M}_\Lambda$, where $\mathcal{M}_\Lambda$ is defined in Subsection 2.4. Set

$$\beta = \lambda^{-1}\rho \in \mathcal{M}_\Lambda. \tag{3.11}$$

We know that

$$\rho\left(-\epsilon^{-1}un\right)_{\{1,2\}} = \begin{pmatrix} * & * \\ \epsilon\wp & 1+(a+n\wp)u \end{pmatrix} \begin{pmatrix} 1 & -\epsilon^{-1}un \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} * & * \\ \epsilon\wp & 1+au \end{pmatrix},$$

and it thus follows from (3.2) that

$$\rho\left(-\epsilon^{-1}un\right)_{\{1,2\}}(-\epsilon m)_{\{2,1\}} = \begin{pmatrix} * & * \\ \epsilon\wp & 1+au \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -\epsilon m & 1 \end{pmatrix}$$
$$= \begin{pmatrix} * & * \\ \epsilon(\wp - m(1+au)) & 1+au \end{pmatrix}$$
$$= \begin{pmatrix} * & * \\ \epsilon b & 1+au \end{pmatrix}.$$

Lemma 3.1 now follows immediately from (3.7) and (3.11). □

Lemma 3.2. *Let* $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{A})$, *and let* r *be a positive integer. Then there exist* $t^{(1)}, t^{(2)}, \ldots, t^{(10)} \in \mathbf{A}$, $\epsilon \in \mathbb{F}_q^\times$, $\beta \in \mathcal{M}_\Lambda$, *and* $\gamma \in \mathcal{M}_\Lambda^T$ *such that*

$$\alpha^r t^{(1)}_{\{1,2\}} t^{(2)}_{\{2,1\}} t^{(3)}_{\{1,2\}} \beta t^{(4)}_{\{1,2\}} t^{(5)}_{\{2,1\}} t^{(6)}_{\{1,2\}} t^{(7)}_{\{2,1\}} \gamma t^{(8)}_{\{2,1\}} t^{(9)}_{\{1,2\}} t^{(10)}_{\{2,1\}} = \begin{pmatrix} a^r & \epsilon b \\ * & * \end{pmatrix}.$$

Remark 3.3. In the proof of Lemma 3.2 below, we follow the same arguments as that of Vaserstein [16, Lemma 1.2].

Proof. By the Cayley–Hamilton theorem, we know that α satisfies its characteristic equation, that is,

$$\alpha^2 + f\alpha + \mathbf{1}_2 = 0,$$

where $f = -\mathrm{Trace}(\alpha)$, and $\mathbf{1}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. From the above equation, it is not difficult to prove that α^r can be written in the form

$$\alpha^r = u\alpha + v\mathbf{1}_2 = \begin{pmatrix} au+v & ub \\ cu & du+v \end{pmatrix} \tag{3.12}$$

for some elements $u, v \in \mathbf{A}$. We see that $1 = \det(\alpha)^r = \det(\alpha^r) \equiv \det(v\mathbf{1}_2) = v^2 \pmod{u}$, and thus u divides $(v-1)(v+1)$. Therefore there exist $u_1, u_2 \in \mathbf{A}$ such that $v \equiv 1 \pmod{u_1}$, $v \equiv -1 \pmod{u_2}$, and $u = u_1u_2$.

Since $v \equiv 1 \pmod{u_1}$, there exists an element $v_1 \in \mathbf{A}$ such that $v = 1 + u_1v_1$. We see that

$$v + ua = (1 + u_1v_1) + u_1u_2a = 1 + (v_1 + u_2a)u_1,$$

and $ub = (u_2b)u_1$. Applying Lemma 3.1 with α^r, $v_1 + u_2a$, u_2b, u_1 in the roles of α, a, b, u, respectively, we see from (3.12) that there exist $t^{(1)}, t^{(2)}, t^{(3)}, t^{(4)}, w^{(1)} \in \mathbf{A}$, $\epsilon_1 \in \mathbb{F}_q^\times$, and $\beta \in \mathcal{M}_\Lambda$ such that

$$\rho = \alpha^r t^{(1)}_{\{1,2\}} t^{(2)}_{\{2,1\}} t^{(3)}_{\{1,2\}} \beta t^{(4)}_{\{1,2\}} w^{(1)}_{\{2,1\}} = \begin{pmatrix} * & * \\ \epsilon_1 u_2 b & v+ua \end{pmatrix}. \tag{3.13}$$

Set

$$\chi := -\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rho \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} -v - ua & \epsilon_1 u_2 b \\ * & * \end{pmatrix} \in \mathbf{SL}_2(\mathbf{A}). \tag{3.14}$$

Since $v \equiv -1 \pmod{u_2}$, we see that $v = -1 + u_2 v_2$ for some $v_2 \in \mathbf{A}$, and thus

$$-v - ua = 1 - u_2 v_2 - u_1 u_2 a = 1 + (-v_2 - u_1 a) u_2.$$

Applying Lemma 3.1 with $\chi, -v_2 - u_1 a, \epsilon_1 b, u_2$ in the roles of α, a, b, u, we deduce that there exist $w^{(2)}, t^{(6)}, t^{(7)}, t^{(8)}, t^{(9)} \in \mathbf{A}$, $\epsilon_2 \in \mathbb{F}_q^\times$, and $\beta_1 \in \mathcal{M}_\Lambda$ such that

$$\chi w^{(2)}_{\{1,2\}}\left(-t^{(6)}\right)_{\{2,1\}}\left(-t^{(7)}\right)_{\{1,2\}} \beta_1 \left(-t^{(8)}\right)_{\{1,2\}}\left(-t^{(9)}\right)_{\{2,1\}} = \begin{pmatrix} * & * \\ \epsilon_1\epsilon_2 b & -v - ua \end{pmatrix}.$$

Negating both sides of the above equation, and conjugating them by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}$, we get from Lemma 2.1 and (3.14) that

$$\rho\left(-w^{(2)}\right)_{\{2,1\}} t^{(6)}_{\{1,2\}} t^{(7)}_{\{2,1\}} \gamma t^{(8)}_{\{2,1\}} t^{(9)}_{\{1,2\}} = \begin{pmatrix} v + ua & \epsilon b \\ * & * \end{pmatrix}, \tag{3.15}$$

where $\epsilon = \epsilon_1\epsilon_2$, and

$$\gamma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \beta_1 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Note that since $\beta_1 \in \mathcal{M}_\Lambda$, Lemma 2.8 implies that $\gamma \in \mathcal{M}_\Lambda^T$.

We know that

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a & 0 \\ * & * \end{pmatrix} \pmod{b},$$

and it thus follows from (3.12) that

$$\begin{pmatrix} au + v & ub \\ * & * \end{pmatrix} = u\alpha + v\mathbf{1}_2 = \alpha^r \equiv \begin{pmatrix} a^r & 0 \\ * & * \end{pmatrix} \pmod{b}.$$

Therefore $au + v \equiv a^r \pmod{b}$. Since $\epsilon \in \mathbb{F}_q^\times$ is a unit in $\mathbf{A}$, there exists an element $t^{(10)} \in \mathbf{A}$ such that

$$a^r = au + v + t^{(10)}\epsilon b.$$

Hence we deduce from (3.15) that

$$\begin{aligned} \rho\left(-w^{(2)}\right)_{\{2,1\}} t^{(6)}_{\{1,2\}} t^{(7)}_{\{2,1\}} \gamma t^{(8)}_{\{2,1\}} t^{(9)}_{\{1,2\}} t^{(10)}_{\{2,1\}} &= \begin{pmatrix} v + ua & \epsilon b \\ * & * \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t^{(10)} & 1 \end{pmatrix} \\ &= \begin{pmatrix} a^r & \epsilon b \\ * & * \end{pmatrix}. \end{aligned} \tag{3.16}$$

Set

$$t^{(5)} = w^{(1)} - w^{(2)} \in \mathbf{A},$$

and note that

$$\left(t^{(5)}\right)_{\{2,1\}} = \left(w^{(1)}\right)_{\{2,1\}} \left(-w^{(2)}\right)_{\{2,1\}}.$$

Hence Lemma 3.2 follows immediately from (3.13) and (3.16). □

Lemma 3.4. *Let* $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{A})$. *Let* $\epsilon \in \mathbb{F}_q^\times$, *and let* r *be a positive integer. Assume that*

$$a^r \equiv \epsilon \pmod{b}.$$

Then there exist $t^{(1)}, t^{(2)}, \ldots, t^{(12)} \in \mathbf{A}$, $\beta \in \mathcal{M}_\Lambda$, *and* $\gamma \in \mathcal{M}_\Lambda^T$ *such that*

$$\alpha^r t^{(1)}_{\{1,2\}} t^{(2)}_{\{2,1\}} t^{(3)}_{\{1,2\}} \beta t^{(4)}_{\{1,2\}} t^{(5)}_{\{2,1\}} t^{(6)}_{\{1,2\}} t^{(7)}_{\{2,1\}} \gamma t^{(8)}_{\{2,1\}} t^{(9)}_{\{1,2\}} t^{(10)}_{\{2,1\}} t^{(11)}_{\{1,2\}} t^{(12)}_{\{2,1\}} = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix}.$$

Proof. By Lemma 3.2, there exist elements $\epsilon_1 \in \mathbb{F}_q^\times, t^{(1)}, t^{(2)}, \ldots, t^{(9)} \in \mathbf{A}$, $w^{(1)} \in \mathbf{A}$, $\beta \in \mathcal{M}_\Lambda$, and $\gamma \in \mathcal{M}_\Lambda^T$ such that

$$\rho := \alpha^r t^{(1)}_{\{1,2\}} t^{(2)}_{\{2,1\}} t^{(3)}_{\{1,2\}} \beta t^{(4)}_{\{1,2\}} t^{(5)}_{\{2,1\}} t^{(6)}_{\{1,2\}} t^{(7)}_{\{2,1\}} \gamma t^{(8)}_{\{2,1\}} t^{(9)}_{\{1,2\}} w^{(1)}_{\{2,1\}} = \begin{pmatrix} a^r & \epsilon_1 b \\ * & * \end{pmatrix}. \quad (3.17)$$

By assumption, we know that $a^r \equiv \epsilon \pmod{b}$. Since $\epsilon_1 \in \mathbb{F}_q^\times$ is a unit in $\mathbf{A}$, there exists an element $w^{(2)} \in \mathbf{A}$ such that

$$a^r + \epsilon_1 b w^{(2)} = \epsilon,$$

and thus

$$\rho \left(w^{(2)}\right)_{\{2,1\}} = \begin{pmatrix} a^r & \epsilon_1 b \\ * & * \end{pmatrix} \begin{pmatrix} 1 & 0 \\ w^{(2)} & 1 \end{pmatrix} = \begin{pmatrix} a^r + \epsilon_1 b w^{(2)} & \epsilon_1 b \\ * & * \end{pmatrix} = \begin{pmatrix} \epsilon & \epsilon_1 b \\ * & * \end{pmatrix}. \quad (3.18)$$

Set

$$t^{(11)} = -\frac{\epsilon_1 b}{\epsilon}.$$

Since $\epsilon \in \mathbb{F}_q^\times$ is a unit in $\mathbf{A}$, we get that $t^{(11)} \in \mathbf{A}$. We see from (3.18) that

$$\begin{aligned} \rho \left(w^{(2)}\right)_{\{2,1\}} \left(t^{(11)}\right)_{\{1,2\}} &= \begin{pmatrix} \epsilon & \epsilon_1 b \\ * & * \end{pmatrix} t^{(11)}_{\{1,2\}} = \begin{pmatrix} \epsilon & \epsilon_1 b \\ * & * \end{pmatrix} \begin{pmatrix} 1 & t^{(11)} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \epsilon & \epsilon t^{(11)} + \epsilon_1 b \\ * & * \end{pmatrix} = \begin{pmatrix} \epsilon & 0 \\ m & n \end{pmatrix}, \end{aligned} \quad (3.19)$$

where m, n are certain elements in $\mathbf{A}$.

By (3.17), we know that $\det(\rho) = 1$, and thus

$$\epsilon n = \det \begin{pmatrix} \epsilon & 0 \\ m & n \end{pmatrix} = \det \left(\rho w^{(2)}_{\{2,1\}} \right) = 1,$$

and therefore $n = \epsilon^{-1}$. Hence (3.19) implies that

$$\rho w^{(2)}_{\{2,1\}} t^{(11)}_{\{1,2\}} = \begin{pmatrix} \epsilon & 0 \\ m & \epsilon^{-1} \end{pmatrix}. \tag{3.20}$$

Set

$$t^{(12)} = -\epsilon m \in \mathbf{A}.$$

An easy calculation now shows that

$$\rho w^{(2)}_{\{2,1\}} t^{(11)}_{\{1,2\}} t^{(12)}_{\{2,1\}} = \begin{pmatrix} \epsilon & 0 \\ m & \epsilon^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t^{(12)} & 1 \end{pmatrix} = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix}. \tag{3.21}$$

Setting

$$t^{(10)} = w^{(1)} + w^{(2)},$$

we see that Lemma 3.4 follows immediately from (3.17) and (3.21). □

Corollary 3.5. *Let* $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{A})$. *Let* $\epsilon \in \mathbb{F}_q^\times$, *and let* r *be a positive integer. Assume that*

$$a^r \equiv \epsilon \pmod{b}.$$

Then

$$\alpha^r = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} \chi_5 \gamma_\Lambda \chi_4 \beta_\Lambda \chi_3,$$

where $\chi_3 \in \mathcal{F}_3(\mathbf{A}^3)$, $\chi_4 \in \mathcal{G}_4(\mathbf{A}^4)$, $\chi_5 \in \mathcal{G}_5(\mathbf{A}^5)$, $\gamma_\Lambda \in \mathcal{M}_\Lambda^T$, *and* $\beta_\Lambda \in \mathcal{M}_\Lambda$.

Proof. By Lemma 3.4, there exist $t^{(1)}, t^{(2)}, \ldots, t^{(12)} \in \mathbf{A}$, $\beta \in \mathcal{M}_\Lambda$, and $\gamma \in \mathcal{M}_\Lambda^T$ such that

$$\alpha^r t^{(1)}_{\{1,2\}} t^{(2)}_{\{2,1\}} t^{(3)}_{\{1,2\}} \beta t^{(4)}_{\{1,2\}} t^{(5)}_{\{2,1\}} t^{(6)}_{\{1,2\}} t^{(7)}_{\{2,1\}} \gamma t^{(8)}_{\{2,1\}} t^{(9)}_{\{1,2\}} t^{(10)}_{\{2,1\}} t^{(11)}_{\{1,2\}} t^{(12)}_{\{2,1\}} = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix}. \tag{3.22}$$

We see that

$$\begin{aligned} \chi_5 &= \left(t^{(8)}_{\{2,1\}} t^{(9)}_{\{1,2\}} t^{(10)}_{\{2,1\}} t^{(11)}_{\{1,2\}} t^{(12)}_{\{2,1\}} \right)^{-1} \\ &= \left(-t^{(12)}_{\{2,1\}} \right) \left(-t^{(11)} \right)_{\{1,2\}} \left(-t^{(10)} \right)_{\{2,1\}} \left(-t^{(9)} \right)_{\{1,2\}} \left(-t^{(8)} \right)_{\{2,1\}}, \end{aligned}$$

and hence

$$\chi_5 = \mathcal{G}_5 \left(t^{(12)}, t^{(11)}, t^{(10)}, t^{(9)}, t^{(8)} \right) \in \mathcal{G}_5(\mathbf{A}^5). \tag{3.23}$$

Similarly we see that

$$\chi_4 = \left(t^{(4)}_{\{1,2\}} t^{(5)}_{\{2,1\}} t^{(6)}_{\{1,2\}} t^{(7)}_{\{2,1\}}\right)^{-1} \in \mathcal{G}_4(\mathbf{A}^4), \tag{3.24}$$

and

$$\chi_3 = \left(t^{(1)}_{\{1,2\}} t^{(2)}_{\{2,1\}} t^{(3)}_{\{1,2\}}\right)^{-1} \in \mathcal{F}_3(\mathbf{A}^3). \tag{3.25}$$

On the other hand, Lemma 2.8 implies that $\gamma_\Lambda = \gamma^{-1} \in \mathcal{M}_\Lambda^T$, and $\beta_\Lambda = \beta^{-1} \in \mathcal{M}_\Lambda$. It thus follows from (3.22), (3.23), (3.24), and (3.25) that

$$\alpha^r = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} \chi_5 \gamma_\Lambda \chi_4 \beta_\Lambda \chi_3,$$

where $\chi_3 \in \mathcal{F}_3(\mathbf{A}^3)$, $\chi_4 \in \mathcal{G}_4(\mathbf{A}^4)$, $\chi_5 \in \mathcal{G}_5(\mathbf{A}^5)$, $\gamma_\Lambda \in \mathcal{M}_\Lambda^T$, and $\beta_\Lambda \in \mathcal{M}_\Lambda$ as desired. □

Corollary 3.6. *Let* $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{A})$. *Assume that there exist relatively prime integers* $r, s \geq 1$ *such that* $a^r \equiv \epsilon_1 \pmod{b}$ *and* $a^s \equiv \epsilon_2 \pmod{c}$ *for some units* $\epsilon_1, \epsilon_2 \in \mathbb{F}_q^\times$. *Then there exist* $\chi_3 \in \mathcal{F}_3(\mathbf{A}^3)$, $\chi_4 \in \mathcal{G}_4(\mathbf{A}^4)$, $\chi_9 \in \mathcal{G}_9(\mathbf{A}^9)$, $\chi_3^\heartsuit \in \mathcal{G}_3(\mathbf{A}^3)$, $\chi_4^\heartsuit \in \mathcal{F}_4(\mathbf{A}^4)$, $\chi_9^\heartsuit \in \mathcal{F}_9(\mathbf{A}^9)$, $\gamma_\Lambda^\heartsuit, \beta_\Lambda \in \mathcal{M}_\Lambda$, *and* $\gamma_\Lambda, \beta_\Lambda^\heartsuit \in \mathcal{M}_\Lambda^T$ *such that*

$$\alpha = \chi_9 \gamma_\Lambda \chi_4 \beta_\Lambda \chi_3 \chi_9^\heartsuit \gamma_\Lambda^\heartsuit \chi_4^\heartsuit \beta_\Lambda^\heartsuit \chi_3^\heartsuit.$$

Proof. Since r, s are relatively prime, one can find positive integers h_1, h_2 such that $sh_2 = rh_1 - 1$. By replacing r, s by rh_1, sh_2, respectively, one can, without loss of generality, assume that $s = r - 1$.

Applying Corollary 3.5, one can write

$$\alpha^r = \begin{pmatrix} \epsilon_1 & 0 \\ 0 & \epsilon_1^{-1} \end{pmatrix} \chi_5^\# \gamma_\Lambda \chi_4 \beta_\Lambda \chi_3, \tag{3.26}$$

where $\chi_3 \in \mathcal{F}_3(\mathbf{A}^3)$, $\chi_4 \in \mathcal{G}_4(\mathbf{A}^4)$, $\chi_5^\# \in \mathcal{G}_5(\mathbf{A}^5)$, $\gamma_\Lambda \in \mathcal{M}_\Lambda^T$, and $\beta_\Lambda \in \mathcal{M}_\Lambda$.

Applying Corollary 3.5 with α^T in the role of α, one can write

$$(\alpha^T)^s = \begin{pmatrix} \epsilon_2 & 0 \\ 0 & \epsilon_2^{-1} \end{pmatrix} \chi_5^* \gamma_\Lambda^* \chi_4^* \beta_\Lambda^* \chi_3^*, \tag{3.27}$$

where $\chi_3^* \in \mathcal{F}_3(\mathbf{A}^3)$, $\chi_4^* \in \mathcal{G}_4(\mathbf{A}^4)$, $\chi_5^* \in \mathcal{G}_5(\mathbf{A}^5)$, $\gamma_\Lambda^* \in \mathcal{M}_\Lambda^T$, and $\beta_\Lambda^* \in \mathcal{M}_\Lambda$.

Conjugating both sides of (3.27) by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, we deduce from Lemma 2.1 that

$$\alpha^{-s} = \begin{pmatrix} \epsilon_2^{-1} & 0 \\ 0 & \epsilon_2 \end{pmatrix} \chi_5^\diamond \gamma_\Lambda^\heartsuit \chi_4^\heartsuit \beta_\Lambda^\heartsuit \chi_3^\heartsuit, \tag{3.28}$$

where

$$\chi_5^{\diamond} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \chi_5^* \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1},$$
$$\gamma_\Lambda^{\heartsuit} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \gamma_\Lambda^* \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1},$$
$$\chi_4^{\heartsuit} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \chi_4^* \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1},$$
$$\beta_\Lambda^{\heartsuit} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \beta_\Lambda^* \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1},$$
$$\chi_3^{\heartsuit} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \chi_3^* \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}.$$

By Lemma 2.8 and equation (2.2) in Subsection 2.1, one sees immediately that $\chi_3^{\heartsuit} \in \mathcal{G}_3(\mathbf{A}^3)$, $\chi_4^{\heartsuit} \in \mathcal{F}_4(\mathbf{A}^4)$, $\chi_5^{\diamond} \in \mathcal{F}_5(\mathbf{A}^5)$, $\gamma_\Lambda^{\heartsuit} \in \mathcal{M}_\Lambda$, and $\beta_\Lambda^{\heartsuit} \in \mathcal{M}_\Lambda^T$.

By Corollary 2.6,

$$\chi_9^{\heartsuit} := \begin{pmatrix} \epsilon_2^{-1} & 0 \\ 0 & \epsilon_2 \end{pmatrix} \chi_5^{\diamond} \in \mathcal{F}_9(\mathbf{A}^9).$$

Similarly one sees that

$$\chi_9 := \begin{pmatrix} \epsilon_1 & 0 \\ 0 & \epsilon_1^{-1} \end{pmatrix} \chi_5^{\#} \in \mathcal{G}_9(\mathbf{A}^9).$$

From (3.26) and (3.28), we deduce that

$$\alpha = \alpha^r \alpha^{-s} = \chi_9 \gamma_\Lambda \chi_4 \beta_\Lambda \chi_3 \chi_9^{\heartsuit} \gamma_\Lambda^{\heartsuit} \chi_4^{\heartsuit} \beta_\Lambda^{\heartsuit} \chi_3^{\heartsuit},$$

which proves our contention. □

Lemma 3.7. *Every element $\alpha \in \mathbf{SL}_2(\mathbf{A})$ can be represented as*

$$\alpha = \chi_9 \gamma_\Lambda \chi_4 \beta_\Lambda \chi_{11}^{\heartsuit} \gamma_\Lambda^{\heartsuit} \chi_4^{\heartsuit} \beta_\Lambda^{\heartsuit} \chi_4^{\#},$$

where

(i) $\chi_4 \in \mathcal{G}_4(\mathbf{A}^4)$, *and* $\chi_9 \in \mathcal{G}_9(\mathbf{A}^9)$;
(ii) $\chi_4^{\heartsuit} \in \mathcal{F}_4(\mathbf{A}^4)$, *and* $\chi_{11}^{\heartsuit} \in \mathcal{F}_{11}(\mathbf{A}^{11})$;
(iii) $\chi_4^{\#} \in \mathcal{G}_4(\mathbf{A}^4)$;
(iv) $\gamma_\Lambda^{\heartsuit}, \beta_\Lambda \in \mathcal{M}_\Lambda$, *and* $\gamma_\Lambda, \beta_\Lambda^{\heartsuit} \in \mathcal{M}_\Lambda^T$.

Proof. Take any $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{A})$. We consider the following two cases:

$\star$ *Case* 1. $a = 0$

Since $\alpha \in \mathbf{SL}_2(A)$, we see that $b = -\epsilon$ and $c = \epsilon^{-1}$ for some unit $\epsilon \in \mathbb{F}_q^\times$. One can write

$$\alpha = \begin{pmatrix} 0 & -\epsilon \\ \epsilon^{-1} & d \end{pmatrix} = \begin{pmatrix} 0 & -\epsilon \\ \epsilon^{-1} & 0 \end{pmatrix} (\epsilon d)_{\{1,2\}} = \chi_9 \gamma_\Lambda \chi_4 \beta_\Lambda \chi_{11}^\heartsuit \gamma_\Lambda^\heartsuit \chi_4^\heartsuit \beta_\Lambda^\heartsuit \chi_4^\# , \quad (3.29)$$

where

$$\chi_9 = \begin{pmatrix} 0 & -\epsilon \\ \epsilon^{-1} & 0 \end{pmatrix} (\epsilon d)_{\{1,2\}},$$

and

$$\gamma_\Lambda = \chi_4 = \beta_\Lambda = \chi_{11}^\heartsuit = \gamma_\Lambda^\heartsuit = \chi_4^\heartsuit = \beta_\Lambda^\heartsuit = \chi_4^\# = \mathbf{1}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Lemmas 2.5(ii) and 2.2 imply that

$$\chi_9 = \begin{pmatrix} 0 & -\epsilon \\ \epsilon^{-1} & 0 \end{pmatrix} (\epsilon d)_{\{1,2\}} \in \mathcal{G}_4(\mathbf{A}^4),$$

and it thus follows from Lemma 2.4(i) that $\chi_9 \in \mathcal{G}_9(\mathbf{A}^9)$. Lemma 3.7 then follows immediately from (3.29).

$\star$ *Case* 2. $a \neq 0$

By Rosen [12, Theorem 4.8], there exist $u, v \in \mathbf{A}$ such that $au + b$, $av + c$ are primes and $\gcd(\mathbf{deg}(au + b), \mathbf{deg}(av + c)) = 1$. Set

$$\begin{aligned} \wp_1 &= au + b, \\ \wp_2 &= av + c, \\ e_1 &= \frac{q^{\mathbf{deg}(\wp_1)} - 1}{q - 1}, \\ e_2 &= \frac{q^{\mathbf{deg}(\wp_2)} - 1}{q - 1}. \end{aligned}$$

The choice of u, v implies that $\gcd(\mathbf{deg}(\wp_1), \mathbf{deg}(\wp_2)) = 1$.

We see that

$$\gcd\left(q^{\mathbf{deg}(\wp_1)} - 1, q^{\mathbf{deg}(\wp_2)} - 1\right) = q^{\gcd(\mathbf{deg}(\wp_1), \mathbf{deg}(\wp_2))} - 1 = q - 1,$$

and thus

$$\gcd(e_1, e_2) = 1. \quad (3.30)$$

Set

$$\epsilon_1 = \left(\frac{a}{\wp_1}\right)_{q-1} \in \mathbb{F}_q^\times, \epsilon_2 = \left(\frac{a}{\wp_2}\right)_{q-1} \in \mathbb{F}_q^\times,$$

where the $\left(\frac{\cdot}{\wp_i}\right)_{q-1}$ denotes the $(q-1)$-th power residue symbol. It is well-known (see Rosen [12, Chapter 3] or Subsection 2.5) that

$$a^{e_1} \equiv \epsilon_1 \pmod{\wp_1}, \tag{3.31}$$

and

$$a^{e_2} \equiv \epsilon_2 \pmod{\wp_2}. \tag{3.32}$$

We see that

$$v_{\{2,1\}}\alpha u_{\{1,2\}} = \begin{pmatrix} a & au+b \\ av+c & (av+c)u+bv+d \end{pmatrix} = \begin{pmatrix} a & \wp_1 \\ \wp_2 & (av+c)u+bv+d \end{pmatrix}. \tag{3.33}$$

Using (3.30), (3.31), (3.32), and applying Corollary 3.6 with $v_{\{2,1\}}\alpha u_{\{1,2\}}, e_1, e_2$ in the roles of α, r, s, respectively, one can write

$$v_{\{2,1\}}\alpha u_{\{1,2\}} = \chi_9^{\#}\gamma_\Lambda \chi_4 \beta_\Lambda \chi_3 \chi_9^{\heartsuit}\gamma_\Lambda^{\heartsuit}\chi_4^{\heartsuit}\beta_\Lambda^{\heartsuit}\chi_3^{\heartsuit,\#},$$

where $\chi_3 \in \mathcal{F}_3(\mathbf{A}^3)$, $\chi_4 \in \mathcal{G}_4(\mathbf{A}^4)$, $\chi_9^{\#} \in \mathcal{G}_9(\mathbf{A}^9)$, $\chi_3^{\heartsuit,\#} \in \mathcal{G}_3(\mathbf{A}^3)$, $\chi_4^{\heartsuit} \in \mathcal{F}_4(\mathbf{A}^4)$, $\chi_9^{\heartsuit} \in \mathcal{F}_9(\mathbf{A}^9)$, $\gamma_\Lambda^{\heartsuit}, \beta_\Lambda \in \mathcal{M}_\Lambda$, and $\gamma_\Lambda, \beta_\Lambda^{\heartsuit} \in \mathcal{M}_\Lambda^T$. The above equation implies that

$$\alpha = \chi_9\gamma_\Lambda\chi_4\beta_\Lambda\chi_{11}^{\heartsuit}\gamma_\Lambda^{\heartsuit}\chi_4^{\heartsuit}\beta_\Lambda^{\heartsuit}\chi_4^{\#}, \tag{3.34}$$

where

$$\begin{aligned} \chi_9 &= (-v)_{\{2,1\}}\chi_9^{\#}, \\ \chi_{11}^{\heartsuit} &= \chi_3\chi_9^{\heartsuit}, \\ \chi_4^{\#} &= \chi_3^{\heartsuit,\#}(-u)_{\{1,2\}}. \end{aligned}$$

Since $\chi_3^{\heartsuit,\#} \in \mathcal{G}_3(\mathbf{A}^3)$, the definition of $\mathcal{G}_i$ and Lemma 2.2 imply that $\chi_9 \in \mathcal{G}_9(\mathbf{A}^9)$ and $\chi_4^{\#} \in \mathcal{G}_4(\mathbf{A}^4)$. Furthermore Lemma 2.3 implies that $\chi_{11}^{\heartsuit} \in \mathcal{F}_{11}(\mathbf{A}^{11})$. Hence Lemma 3.7 follows from (3.34). □

We now prove our main theorem in this paper.

Theorem 3.8. $\mathbf{SL}_2(\mathbf{A})$ *is a polynomial family with* 52 *variables*.

Proof. Let Ω be the polynomial matrix defined by

$$\Omega = \mathcal{G}_9\Lambda^T\mathcal{G}_4\Lambda\mathcal{F}_{11}\Lambda\mathcal{F}_4\Lambda^T\mathcal{G}_4.$$

We see that Ω has 52 variables. Using Lemma 3.7, and recalling that $\mathcal{M}_\Lambda \subset \Lambda(\mathbf{A}^5)$ and $\mathcal{M}_\Lambda^T \subset \Lambda^T(\mathbf{A}^5)$ (see Subsection 2.4), we deduce that

$$\mathbf{SL}_2(\mathbf{A}) = \Omega(\mathbf{A}^{52}),$$

which proves our assertion. □

References

[1] H. BASS, *K–theory and stable algebra*, Publ. Math. Inst. Hautes Études Sci. **22** (1964), 489–544.

[2] K.-U. BUX and K. WORTMAN, *Finiteness properties of arithmetic groups over function fields*, Invent. Math. **167** (2007), 355–378.

[3] D. CARTER and G. KELLER, *Elementary expressions for unimodular matrices*, Comm. Algebra **12** (1984), 379–389.

[4] D. CARTER, G. KELLER and E. PAIGE, *Bounded expressions in* SL(n, A), unpublished.

[5] G. COOKE and P. J. WEINBERGER, *On the construction of division chains in algebraic number rings, with applications to* $\mathbf{SL}_2$, Comm. Algebra **3** (1975), 481–524.

[6] D. GOSS, "Basic Structures of Function Field Arithmetic", Ergebnisse der Mathematik und ihrer Grenzgebiete 3, Vol. 35, Springer-Verlag, Berlin, 1996.

[7] A. HEALD, "Bounded Generation of Two Families of S-Arithmetic Groups", Ph.D. thesis, University of Virginia, 2013. Available at http://libra.virginia.edu/catalog/libra-oa:3041.

[8] S. LANG, "Algebra", Addison–Wesley Publishing Co., Inc., Reading, Mass., 1965.

[9] D. MARKER, "Model Theory: an Introduction", Graduate Texts in Mathematics, Vol. 217, Springer-Verlag, New York, 2002.

[10] D. W. MORRIS, *Bounded generation of* SL(n, A) *(after D. Carter, G. Keller, and E. Paige)*, New York J. Math. **13** (2007) 383–421. Available at http://nyjm.albany.edu/j/2007/13-17p.pdf.

[11] H. NAGAO, *On GL*(2, $K[x]$), J. Inst. Polytech. Osaka City Univ. Ser. A, **10** (1959), 117–121.

[12] M. ROSEN, "Number Theory in Function Fields", Graduate Texts in Mathematics, Vol. 210, Springer-Verlag, New York, 2002.

[13] T. SKOLEM, "Diophantische Gleichungen", Ergebnisse der Mathematik und ihrer Grenzgebiete, Band V, Heft 4, Springer-Verlag, New York, 1938.

[14] O. I. TAVGEN', *Bounded generability of Chevalley groups over rings of S-integer algebraic numbers (Russian)*, Izv. Akad. Nauk SSSR Ser. Mat. **54** (1990), 97–122, 221–222; translation in Math. USSR-Izv. **36** (1991), 101–128.

[15] D. S. THAKUR, "Function Field Arithmetic", World Scientific Publishing Co., Inc., River Edge, NJ, 2004.

[16] L. VASERSTEIN, *Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups*, Ann. of Math. (2) **171** (2010), 979–1009.

[17] A. WEIL, "Basic Number Theory", Third edition, Die Grundlehren der Mathematischen Wissenschaften, Band 144, Springer-Verlag, New York-Berlin, 1974.

[18] U. ZANNIER, *Remarks on a question of Skolem about the integer solutions of* $x_1x_2 - x_3x_4 = 1$, Acta Arith. **78** (1996), 153–164.

[19] U. ZANNIER, *Parametrizing* $\mathbf{SL}_2(\mathbb{Z})$ *and a question of Skolem*, Acta Arith. **110** (2003), 331–337.

Department of Applied
and Computational Mathematics
and Statistics
University of Notre Dame
153 Hurley Hall
Notre Dame, IN 46556, USA
dongquan.ngoc.nguyen@nd.edu