CERTAIN SETS OVER FUNCTION FIELDS ARE POLYNOMIAL FAMILIES

NGUYEN NGOC DONG QUAN

CONTENTS
1. Introduction ............................................. 1
2. Some basic notation and notions .................. 3
   2.1. Definitions of $F_h, G_h$ .................. 3
   2.2. Definition of $\Psi$ ...................... 5
   2.3. Definitions of $\Gamma$ and $M_\Gamma$ ...... 5
   2.4. Definitions of $\Lambda, M_\Lambda$, and $M^T_\Lambda$ ....... 6
   2.5. The $d$-th power residue symbol in $A$ .... 6
3. $\text{SL}_2(A)$ is a polynomial family ............. 7
Acknowledgements ..................................... 14
References ............................................. 15

Abstract. In 1938, Skolem conjectured that $\text{SL}_n(\mathbb{Z})$ 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 $\text{SL}_n(\mathbb{Z})$ 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 $\text{SL}_2(\mathbb{Z})$ is a polynomial family. An immediate consequence of Vaserstein’s theorem also implies that $\text{SL}_n(\mathbb{Z})$ 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 $A$ is the ring of polynomials over a finite field of odd characteristic, then $\text{SL}_2(A)$ is a polynomial family in 52 variables. A consequence of our main result also implies that $\text{SL}_n(A)$ is a polynomial family for any $n \geq 3$.

1. INTRODUCTION

Let $R$ be a commutative ring with identity, and let $\mathcal{X}$ be a subset of $R^h$. The set $\mathcal{X}$ is said to be a polynomial family over $R$ with $d$ parameters for some positive integer $d$ if there exist polynomials $P_1, \ldots, P_h \in R[x_1, \ldots, x_d]$ in $d$ variables $x_1, \ldots, x_d$ such that

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

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

$$\mathcal{P}(x_1, \ldots, x_d) = (P_1(x_1, \ldots, x_d), \ldots, P_h(x_1, \ldots, x_d)).$$

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

Determining whether a set in $R^h$ is a polynomial family has a long history dating back to the 17th century. For example, when $R = \mathbb{Z}$, 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 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 [8, page 23], Skolem conjectured that $\text{SL}_n(\mathbb{Z})$ is not a polynomial family for any $n \geq 2$. Carter and Keller [3] disproved this for all $n \geq 3$ by proving that $\text{SL}_n(\mathbb{Z})$ is boundedly generated by the elementary matrices for each $n \geq 3$, and thus is a polynomial family for each $n \geq 3$.

Date: May 4, 2015.
Recall that a group $G$ is said to be \textit{boundedly generated by a subset $\Gamma$ of $G$} if there exists a positive integer $\ell$ such that every element $g \in G$ can be written in the form

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

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

It is well-known that $\text{SL}_2(\mathbb{Z})$ is finitely generated, but not boundedly generated since it has a free subgroup of index 12. So one cannot expect to use the same arguments as Carter and Keller \cite{Carter1977} to disprove Skolem’s conjecture for $\text{SL}_2(\mathbb{Z})$. In fact, only recently, Vaserstein \cite{Vaserstein1997} refuted Skolem’s conjecture completely by proving that $\text{SL}_2(\mathbb{Z})$ is a polynomial family with 46 parameters. As an immediate consequence, Vaserstein also showed that $\text{SL}_n(\mathbb{Z})$ with $n \geq 3$ is a polynomial family with less parameters than in the work of Carter and Keller \cite{Carter1977}. Following the work of Vaserstein, it is not difficult to show that for a commutative ring $\mathcal{R}$ satisfying the second Bass stable range condition (see Bass \cite{Bass1967} for this definition), if $\text{SL}_2(\mathcal{R})$ is a polynomial family, then so is $\text{SL}_n(\mathcal{R})$ for any $n \geq 3$. It is well-known (see Bass \cite{Bass1967}) that every Dedekind domain satisfies the second Bass stable range condition, and hence for such a domain $\mathcal{R}$, it suffices to consider whether $\text{SL}_2(\mathcal{R})$ is a polynomial family.

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

$$x_1 x_2 - x_3 x_4 = 1.$$  \hfill (1)

Then $\text{SL}_2(\mathcal{R})$ is a polynomial family if and only if all the $\mathcal{R}$-integral solutions of (1) can be obtained from a fixed polynomial parametrization with coefficients in $\mathcal{R}$ by letting all the variables run through $\mathcal{R}$. For example, Vaserstein’s theorem says that all the integral solutions of (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 global field. Only a few of such rings in number fields are known. Zannier \cite{Zannier2001} proved that $\text{SL}_2(\mathbb{Z}[\sqrt{2}])$ is a polynomial family with 5 parameters conditionally under the truth of the Generalized Riemann Hypothesis. Zannier \cite{Zannier2002} unconditionally showed that $\text{SL}_2(\mathcal{O}_S)$ is a polynomial family with 5 parameters, where $S = \{2, 3, \mathfrak{p}\}$ with $\mathfrak{p}$ being a prime such that $\mathfrak{p} \equiv 1 \pmod{4}$, and $\mathcal{O}_S$ is the ring of $S$-integers in $\mathbb{Q}$ defined by

$$\mathcal{O}_S = \{q \in \mathbb{Q} \mid \text{there exist nonnegative integers } \alpha_2, \alpha_3, \alpha_\mathfrak{p}, \text{ such that } q 2^{\alpha_2} 3^{\alpha_3} \mathfrak{p}^{\alpha_\mathfrak{p}} \in \mathbb{Z}\}.$$  

The work of Zannier \cite{Zannier2001} \cite{Zannier2002} begs a question: For a ring $\mathcal{R}$, what is the smallest number of parameters needed to polynomially parametrize $\text{SL}_2(\mathcal{R})$? For each ring $\mathcal{R}$, denote by $\mathcal{M}(\mathcal{R})$ the smallest number of parameters needed to polynomially parametrize $\text{SL}_2(\mathcal{R})$. Then Theorem 1 in Zannier \cite{Zannier2001} shows that $\mathcal{M}(O_K) \geq 4$ if $O_K$ is the ring of integers in a number field $K$. In particular, Vaserstein’s theorem \cite{Vaserstein1997} implies that $4 \leq \mathcal{M}(\mathbb{Z}) \leq 46$. For an extension of $\mathbb{Z}$, Zannier’s theorem \cite{Zannier2001} shows that $4 \leq \mathcal{M}(\mathbb{Z}[\sqrt{2}]) \leq 5$ conditionally under the truth of the Generalized Riemann Hypothesis. It is certainly interesting if one can find a precise value of $\mathcal{M}(\mathcal{R})$, where $\mathcal{R}$ 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 $\mathbb{A} = \mathbb{F}_q[T]$, 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 $\mathcal{M}(\mathbb{A})$; more precisely, our main goal in this paper is to prove the following.

**Theorem 1.1.** $\text{SL}_2(\mathbb{A})$ is a polynomial family with 52 parameters.

Despite many strong analogies between $\mathbb{Z}$ and $\mathbb{A}$ (see Goss \cite{Goss1996}, Rosen \cite{Rosen1998}, or Thakur \cite{Thakur1996} for these analogies), $\text{SL}_2(\mathbb{A})$ does not always bear a resemblance to $\text{SL}_2(\mathbb{Z})$. For example, Nagao’s theorem (see Nagao \cite{Nagao1985}, or Bux and Wortman \cite{Bux2006, Section 2}) says that $\text{SL}_2(\mathbb{A})$ is not finitely generated. The group $\text{SL}_2(\mathbb{Z})$ 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 $\mathbb{A}$. Theorem 1.1 answers this questions affirmatively by showing that $\text{SL}_2(\mathbb{A})$ is a polynomial family with 52 parameters.
Throughout the work of Vaserstein [10], the polynomial parametrization of $\text{SL}_2(\mathbb{Z})$ is often used to show many interesting sets in $\mathbb{Z}^h$ are polynomial families. Using similar arguments as in Vaserstein [10], one can use Theorem 1.1 to show many sets in $\mathbb{A}^h$ are polynomial families. As an illustration, let us now consider some applications of Theorem 1.1.

Take any commutative ring $\mathcal{R}$ with identity 1. Recall that a $h$-tuple $(m_1, \ldots, m_h) \in \mathcal{R}^h$ is called \textit{unimodular} if there exist elements $\alpha_1, \ldots, \alpha_h \in \mathcal{R}$ such that $\sum_{i=1}^h \alpha_i m_i = 1$. We denote by $\text{UM}_h(\mathcal{R})$ the set of all unimodular $h$-tuples in $\mathcal{R}^d$.

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

Now return to our ring $\mathcal{A}$. It is well-known (see [1, page 14]) that $\mathcal{A}$ satisfies the second Bass stable range condition. Hence it follows from Vaserstein [10, pages 994 and 995] that $\text{UM}_n(\mathcal{A})$ is a polynomial family with $2n$ parameters for all $n \geq 3$. (In fact, Vaserstein proved that the last result also holds if $\mathcal{A}$ is replaced by any commutative ring $\mathcal{R}$ with $\text{SR}(\mathcal{R}) \leq 2$.)

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

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

By Theorem 1.1, there are polynomials $p_1, p_2, p_3, p_4 \in \mathcal{A}[x_1, \ldots, x_{52}]$ in 52 variables such that

$$\text{SL}_2(\mathcal{A}) = \begin{pmatrix} p_1(\mathcal{A}^{52}) & p_2(\mathcal{A}^{52}) \\ p_3(\mathcal{A}^{52}) & p_4(\mathcal{A}^{52}) \end{pmatrix}.$$

We deduce that

$$(a, b) = (1, 0)\alpha \in (1, 0)\text{SL}_2(\mathcal{A}) = (1, 0)\begin{pmatrix} p_1(\mathcal{A}^{52}) & p_2(\mathcal{A}^{52}) \\ p_3(\mathcal{A}^{52}) & p_4(\mathcal{A}^{52}) \end{pmatrix} = (p_1(\mathcal{A}^{52}), p_2(\mathcal{A}^{52})),$$

which yields the following result.

\textbf{Corollary 1.2.} $\text{UM}_2(\mathcal{A})$ is a polynomial family with 52 parameters.

Following the same arguments as in Vaserstein [10, page 998] and using Theorem 1.1, the following result is immediate, and can be proved by induction on $n$.

\textbf{Corollary 1.3.} $\text{SL}_n(\mathcal{A})$ is a polynomial family with $45 + n(3n + 1)/2$ parameters for any $n \geq 2$.

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 1.1. We will prove Theorem 1.1 in Section 3.

\section{Some Basic Notation and Notions}

In this section, we introduce some basic notation and notions that will be used throughout this paper. Vaserstein [10] used the polynomial matrices $\Phi_2, \Delta_1, \Gamma_1$ (see [10, pages 990, 992] for their definitions) to construct the polynomial matrix in 46 variables that is a polynomial parametrization of $\text{SL}_2(\mathbb{Z})$. We use the same set of polynomial matrices with different notation to obtain a polynomial parametrization of $\text{SL}_2(\mathcal{A})$; more explicitly, $\Lambda, \mathcal{F}_1, \mathcal{G}_1$ in this paper stand for $\Phi_2, \Delta_1, \Gamma_1$ in Vaserstein [10], 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.

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

For each $m \in \mathcal{A}$, 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 $\text{SL}_2(\mathcal{A})$.

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

\textbf{Lemma 2.1.} Let $\alpha \in \text{SL}_2(\mathcal{A})$. 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 $\mathcal{F}_{2h}(m^{(1)}, \ldots, m^{(2h)}) \in \text{SL}_2(\mathbb{A}[m^{(1)}, \ldots, m^{(2h)}])$ the polynomial matrix in $2h$ parameters defined by

$$
\mathcal{F}_{2h}(m^{(1)}, \ldots, m^{(2h)}) = m^{(1)}_{(1,2)}m^{(2)}_{(2,1)} \cdots m^{(2h-1)}_{(1,2)}m^{(2h)}_{(2,1)} = \prod_{i=0}^{h-1} m^{(2i+1)}_{(1,2)} \prod_{j=1}^{h} m^{(2j)}_{(2,1)}.
$$

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

$$
\mathcal{F}_{2h+1}(m^{(1)}, \ldots, m^{(2h+1)}) = m^{(1)}_{(1,2)}m^{(2)}_{(2,1)} \cdots m^{(2h)}_{(1,2)}m^{(2h+1)}_{(2,1)} = \prod_{i=0}^{h} m^{(2i+1)}_{(1,2)} \prod_{j=1}^{h} m^{(2j)}_{(2,1)}.
$$

For each integer $r \geq 1$, set

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

Equivalently, one can write

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

The next result follows immediately from Lemma 2.1.

**Lemma 2.2.**

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

$$
G_{2h}(m^{(1)}, \ldots, m^{(2h)}) = (-m^{(1)})_{(2,1)}(-m^{(2)})_{(1,2)} \cdots (-m^{(2h-1)})_{(1,2)}(-m^{(2h)})_{(2,1)}.
$$

(ii) For each integer $h \geq 0$,

$$
G_{2h+1}(m^{(1)}, \ldots, m^{(2h+1)}) = (-m^{(1)})_{(2,1)}(-m^{(2)})_{(1,2)} \cdots (-m^{(2h)})_{(1,2)}(-m^{(2h+1)})_{(2,1)}.
$$

For each positive integer $r$, set

$$
G_r(\mathbb{A}^r) = \{ G_r(a_1, a_2, \ldots, a_r) \mid (a_1, \ldots, a_r) \in \mathbb{A}^r \}.
$$

The next two lemmas are obvious.

**Lemma 2.3.**

(i) $\mathcal{F}_i(\mathbb{A}^i) \subset \mathcal{F}_j(\mathbb{A}^j)$ for any $1 \leq i < j$.

(ii) $\mathcal{F}_{2h}(\mathbb{A}^{2h}) \mathcal{F}_r(\mathbb{A}^r) \subset \mathcal{F}_{2h+r}(\mathbb{A}^{2h+r})$ for each integer $h \geq 1$ and each integer $r \geq 1$.

(iii) $\mathcal{F}_{2h+1}(\mathbb{A}^{2h+1}) \mathcal{F}_r(\mathbb{A}^r) \subset \mathcal{F}_{2h+r}(\mathbb{A}^{2h+r})$ for each integer $h \geq 0$ and each integer $r \geq 1$.

**Lemma 2.4.**

(i) $G_i(\mathbb{A}^i) \subset G_j(\mathbb{A}^j)$ for any $1 \leq i < j$.

(ii) $G_{2h}(\mathbb{A}^{2h}) G_r(\mathbb{A}^r) \subset G_{2h+r}(\mathbb{A}^{2h+r})$ for each integer $h \geq 1$ and each integer $r \geq 1$.

(iii) $G_{2h+1}(\mathbb{A}^{2h+1}) G_r(\mathbb{A}^r) \subset G_{2h+r}(\mathbb{A}^{2h+r})$ 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 $G_4(\mathbb{A}^4) \cap \mathcal{F}_4(\mathbb{A}^4)$ and $G_3(\mathbb{A}^3) \cap \mathcal{F}_3(\mathbb{A}^3)$, respectively.

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

(i) $\begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} \in G_4(\mathbb{A}^4) \cap \mathcal{F}_4(\mathbb{A}^4)$.
(ii) \[
\begin{pmatrix}
0 & -\epsilon \\
\epsilon^{-1} & 0
\end{pmatrix} \in G_3(A^3) \cap F_3(A^3).
\]

**Proof.** Part (i) follows immediately by noting that
\[
\begin{pmatrix}
\epsilon & 0 \\
0 & \epsilon^{-1}
\end{pmatrix} = G_4((\epsilon - 1)/\epsilon, -1, 1 - \epsilon, 1/\epsilon) = F_4(-\epsilon, \epsilon^{-1} - 1, 1, \epsilon - 1) \in G_4(A^4) \cap F_4(A^4).
\]

Since
\[
\begin{pmatrix}
0 & -\epsilon \\
\epsilon^{-1} & 0
\end{pmatrix} = G_3(-\epsilon^{-1}, \epsilon, -\epsilon^{-1}) = F_3(-\epsilon, -\epsilon^{-1}, -\epsilon) \in G_3(A^3) \cap F_3(A^3),
\]
we obtain the assertion in part (ii).

\[\square\]

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 \( \epsilon \in F_q^* \) and any integer \( r \geq 1 \),
\[
\begin{pmatrix}
\epsilon & 0 \\
0 & \epsilon^{-1}
\end{pmatrix} G_r(A^r) \subset G_{r+4}(A^{r+4}).
\]

(ii) For any unit \( \epsilon \in F_q^* \) and any integer \( r \geq 1 \),
\[
\begin{pmatrix}
\epsilon & 0 \\
0 & \epsilon^{-1}
\end{pmatrix} F_r(A^r) \subset F_{r+4}(A^{r+4}).
\]

2.2. **Definition of \( \Psi \).** In this subsection, we recall the notion of the polynomial matrix \( \Phi_3 \) in Vaserstein [10, page 989] that will be denoted by \( \Psi \) in this paper.

Let \( \Psi \in SL_2(A[m_1, m_2, m_3]) \) be the polynomial matrix in three variables \( m_1, m_2, m_3 \) defined by
\[
(4) \quad \Psi(m_1, m_2, m_3) = \begin{pmatrix}
m_1^2m_3 & m_1m_2m_3 \\
m_2m_3 & 1 - m_1m_2m_3
\end{pmatrix} \in SL_2(A[m_1, m_2, m_3]).
\]

The next lemma shows that every conjugate of \( m_1 \{1, 2 \} \) or \( m_2 \{1, 2 \} \) in \( SL_2(A) \) is contained in the image of \( \Psi \) for all \( m \in A \).

**Lemma 2.7.**

(i) \( \Psi(-a, c, m) = am_1 \{1, 2 \} \alpha^{-1} \) for every \( \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(A) \) and every \( m \in A \).

(ii) \( \Psi(b, -d, -m) = am_1 \{2, 1 \} \alpha^{-1} \) for every \( \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(A) \) and every \( m \in A \).

2.3. **Definitions of \( \Gamma \) and \( \mathcal{M}_\Gamma \).** In this subsection, we recall the notion of the polynomial matrix \( \Phi_4 \) in Vaserstein [10, page 989] that will be denoted by \( \Gamma \) in this paper.

Let \( \Gamma \in SL_2(A[m_1, m_2, m_3, m_4]) \) be the polynomial matrix defined by
\[
\Gamma(m_1, m_2, m_3, m_4) = \begin{pmatrix}
1 - m_2m_4 & m_2^2 \\
-m_2^2 & 1 + m_2m_4
\end{pmatrix} \begin{pmatrix}
1 - m_1m_3 & m_1^2 \\
-m_1^2 & 1 + m_1m_3
\end{pmatrix} \begin{pmatrix}
1 & m_2m_4 \\
-m_2m_4 & 1
\end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.
\]

Set
\[
\mathcal{M}_\Gamma = \{ \alpha \alpha^T \mid \alpha \in SL_2(A) \} \subset SL_2(A).
\]

Following the same arguments as in Vaserstein [10, page 989] with \( \mathcal{M}_\Gamma, \Gamma \) in the roles of \( X_4, \Phi_4 \), respectively, one sees that \( \mathcal{M}_\Gamma \subset \Gamma(A^4) \).
2.4. Definitions of $\Lambda$, $\mathcal{M}_\Lambda$, and $\mathcal{M}_\Lambda^T$. In this subsection, we recall the notions of $\Phi_5$ and $\chi_5$ in Vaserstein [10, page 990] that will be denoted by $\Lambda$ and $\mathcal{M}_\Lambda$, respectively in this paper. The polynomial matrix $\Lambda$ will play a central role in a polynomial parametrization of $\text{SL}_2(\mathbb{A})$.

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

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

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

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

Following the same arguments as in Vaserstein [10, page 990], we get that

\begin{equation}
\mathcal{M}_\Lambda \subset \Lambda(\mathbb{A}^5) \subset \text{SL}_2(\mathbb{A}).
\end{equation}

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

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

We define the polynomial matrix $\Lambda^T \in \text{SL}_2(\mathbb{A}[m_1, m_2, m_3, m_4, m_5])$ 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 (5) and Lemma 2.8(ii) imply that

\begin{equation}
\mathcal{M}_\Lambda^T \subset \Lambda^T(\mathbb{A}^5).
\end{equation}

2.5. The $d$-th power residue symbol in $\mathbb{A}$. In this subsection, we briefly recall the notion of the $d$-th power residue symbol. We refer the reader to Rosen [7, Chapter 3] for a more complete account.

Let $\varphi$ be a prime in $\mathbb{A}$, 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 $\mathbb{A}$ such that $\varphi$ does not divide $m$, then it is well-known (see Rosen [7, pages 23, 24]) that there exists a unique element of $\mathbb{F}_q^\times$, denoted by $\left(\frac{m}{\varphi}\right)_d$, such that

$$\frac{q^{\deg(\varphi)} - 1}{m} \equiv \left(\frac{m}{\varphi}\right)_d \pmod{\varphi}.$$
If \( m \) is an element in \( A \) such that \( \varphi \) divides \( m \), we simply define \( \left( \frac{m}{\varphi} \right)_d = 0 \). We call the symbol \( \left( \frac{m}{\varphi} \right)_d \) the \( d \)-th power residue symbol.

3. \( SL_2(A) \) Is a Polynomial Family

In this section, we prove Theorem 1.1. Although our proof is based on the work of Vaserstein [10], we need to introduce new ideas to overcome several technical difficulties arising in the function field setting. Vaserstein [10] used Dirichlet’s theorem on primes in arithmetic progressions and the quadratic residue symbol in some auxiliary results to obtain a polynomial parametrization for \( SL_2(\mathbb{Z}) \). We cannot use these tools in the function field setting. For the proof of Theorem 1.1, 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 \( A \), provided that \( d \) is sufficiently large.

Lemma 3.1. Let \( a, b, u \in A \), and let \( \alpha = \begin{pmatrix} 1 + au & bu \\ \ast & * \end{pmatrix} \in SL_2(A) \). Then there exist elements \( m, n \in A \), \( \epsilon \in \mathbb{F}_q^\times \), and \( \beta \in M_A \) such that the matrix

\[
\alpha(mn)_{\{1,2\}}(\varphi u)_{\{1,2\}}(\varphi^{-1}mn)_{\{1,2\}}(\varphi^{-1}m)_{\{1,2\}}
\]

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

Proof. If \( 1 + au = 0 \), letting \( m = n = 0 \), \( \varphi = b \), 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 \( A \). Set

\[
\varphi = b + m(1 + au),
\]

where \( m \) will be determined shortly. By Rosen [7, Theorem 4.8], we know that there are infinitely many elements \( m \) in \( A \) such that for such an element \( m \), the polynomial \( \varphi \) is a monic prime whose degree is congruent to \( q - 2 \) modulo \( q - 1 \) and greater than \( \deg(b) \). Take such a monic prime \( \varphi \) of degree greater than \( \deg(b) \) for some element \( m \in A \). We know that there is some integer \( r \) such that

\[
\deg(\varphi) = q - 2 + (q - 1)r.
\]

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

\[
\alpha = \epsilon a_1^{q-1} \pmod{\varphi},
\]

where \( a_1 \) is an element in \( A \). Indeed, denote by \( \left( \frac{\cdot}{\varphi} \right)_{q-1} \) the \((q-1)\)-th power residue symbol (see Subsection 2.5 for its definition). If \( a \equiv 0 \pmod{\varphi} \), then one can take \( a_1 = 0 \), and (10) holds trivially.

If \( a \not\equiv 0 \pmod{\varphi} \), set

\[
\epsilon_1 = \left( \frac{a}{\varphi} \right)_{q-1} \in \mathbb{F}_q^\times.
\]

We see from [7, Proposition 3.2] that

\[
\left( \frac{ae_1}{\varphi} \right)_{q-1} = \left( \frac{a}{\varphi} \right)_{q-1} \left( \frac{\epsilon_1}{\varphi} \right)_{q-1} = \epsilon_1 \left( \frac{q - 1}{\epsilon_1} \right)^{\deg(\varphi)} = \epsilon_1^{(q-1)(r+1)} = 1,
\]

and it thus follows from [7, Proposition 3.1] that there exists an element \( a_1 \in A \) such that \( a \epsilon_1 \equiv a_1^{q-1} \pmod{\varphi} \). Now (10) follows immediately by letting \( \epsilon = \epsilon_1^{-1} \).
By (10), there exists an element \( n \in A \) such that
\[
a + n \varphi = ea_1^{q-1}.
\]
Set
\[
\lambda = \alpha(um)\{1,2\} n\{2,1\} (-\varphi u)\{1,2\}.
\]
We see from (8) and (12) that
\[
\lambda = \alpha(um)\{1,2\} n\{2,1\} (-\varphi u)\{1,2\} = \left(\begin{array}{cc}
1 + au & bu \\
* & *
\end{array}\right) \begin{pmatrix} 1 & mu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} 1 & -\varphi u \\ 0 & 1 \end{pmatrix} \\
= \left(\begin{array}{cc}
1 + au & \varphi u \\
* & *
\end{array}\right) \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} 1 & -\varphi u \\ 0 & 1 \end{pmatrix} \\
= \left(\begin{array}{cc}
1 + u e a_1^{q-1} & \varphi u \\
* & *
\end{array}\right) \begin{pmatrix} 1 & -\varphi u \\ 0 & 1 \end{pmatrix} \\
= \left(\begin{array}{cc}
1 + u e a_1^{q-1} & -\varphi u^2 e a_1^{q-1} \\
c & d
\end{array}\right),
\]
where \( c, d \) are some elements in \( A \).
By (13), and since \( \alpha \in SL_2(A) \), we know that \( \det(\lambda) = 1 \), and thus (14) tells us that
\[
\lambda^{-1} = \left(\begin{array}{cc}
d & \varphi u^2 e a_1^{q-1} \\
-c & 1 + u e a_1^{q-1}
\end{array}\right).
\]

Since \( p \) is odd (recall that \( p \) is the characteristic of \( F_q \)), 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 \( d_1 \in A \). Hence \( \lambda^{-1} \) can be written in the form
\[
\lambda^{-1} = \left(\begin{array}{cc}
1 + d_1 (ua_1^{q_1}) & \varphi c (ua_1^{q_1}) \\
-c & 1 + (e a_1^{q_1})(ua_1^{q_1})
\end{array}\right).
\]
Set
\[
\rho = \left(\begin{array}{cc}
1 + d_1 (ua_1^{q_1}) & -c (ua_1^{q_1}) \\
\eps \varphi & 1 + (e a_1^{q_1})(ua_1^{q_1})
\end{array}\right).
\]
By (12), one can write
\[
\rho = \left(\begin{array}{cc}
* & * \\
\eps \varphi & 1 + (a + n \varphi)u
\end{array}\right).
\]
By (15) and (16), we see that \( \lambda^{-1} \rho \in M_\Lambda \), where \( M_\Lambda \) is defined in Subsection 2.4. Set
\[
\beta = \lambda^{-1} \rho \in M_\Lambda.
\]
We know that
\[
\rho(-\epsilon^{-1} un)\{1,2\} = \left(\begin{array}{cc}
* & * \\
\eps \varphi & 1 + (a + n \varphi)u
\end{array}\right) \begin{pmatrix} 1 & -\epsilon^{-1} u n \\ 0 & 1 \end{pmatrix} = \left(\begin{array}{cc}
* & * \\
\eps \varphi & 1 + au
\end{array}\right),
\]
and it thus follows from (8) that
\[
\rho(-\epsilon^{-1} un)\{1,2\} (-\epsilon m)\{2,1\} = \left(\begin{array}{cc}
* & * \\
\eps \varphi & 1 + au
\end{array}\right) \begin{pmatrix} 1 & 0 \\ -\epsilon m & 1 \end{pmatrix} = \left(\begin{array}{cc}
* & * \\
\eps (\varphi - m(1 + au)) & 1 + au
\end{array}\right) = \left(\begin{array}{cc}
* & * \\
\epsilon b & 1 + au
\end{array}\right).
\]
Lemma 3.1 now follows immediately from (13) and (17).
Lemma 3.2. Let \( \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathcal{A}) \), and let \( r \) be a positive integer. Then there exist \( t^{(1)}, t^{(2)}, \ldots, t^{(10)} \in \mathcal{A} \), \( \epsilon \in \mathbb{F}_q^x \), \( \beta \in \mathcal{M}_\Lambda \), and \( \gamma \in \mathcal{M}_\Lambda^T \) such that
\[
\alpha^{r} t^{(1)}_{(1,2)} t^{(2)}_{(2,1)} t^{(3)}_{(1,2)} t^{(4)}_{(1,2)} t^{(5)}_{(2,1)} t^{(6)}_{(2,1)} t^{(7)}_{(2,1)} t^{(8)}_{(1,2)} t^{(9)}_{(1,2)} t^{(10)}_{(2,1)} = \begin{pmatrix} \alpha^r & \epsilon b \\ * & * \end{pmatrix}.
\]

Remark 3.3. In the proof of Lemma 3.2 below, we follow the same arguments as that of Vaserstein [10, Lemma 1.2].

Proof. By the Cayley–Hamilton theorem, we know that \( \alpha \) satisfies its characteristic equation, that is,
\[
\alpha^2 + f(\alpha) + 1_2 = 0,
\]
where \( f = -\text{Trace}(\alpha) \), and \( 1_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \). From the above equation, it is not difficult to prove that \( \alpha^r \) can be written in the form
\[
\alpha^r = u\alpha + v1_2 = \begin{pmatrix} au + v & ub \\ cu & du + v \end{pmatrix}
\]
for some elements \( u, v \in \mathcal{A} \). We see that \( 1 = \det(\alpha^r) = \det(\alpha^r) = \det(v1_2) = v^2 \) (mod \( u \)), and thus \( u \) divides \( (v - 1)(v + 1) \). Therefore there exist \( u_1, u_2 \in \mathcal{A} \) such that \( u \equiv 1 \) (mod \( u_1 \)), \( v \equiv -1 \) (mod \( u_2 \)), and \( u = u_1u_2 \).

Since \( v \equiv 1 \) (mod \( u_1 \)), there exists an element \( v_1 \in \mathcal{A} \) 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 \( \alpha^r, v_1 + u_2a, u_2b, u_1 \) in the roles of \( \alpha, a, b, u \), respectively, we see from (18) that there exist \( t^{(1)}, t^{(2)}, t^{(3)}, t^{(4)} \in \mathcal{A} \), \( \epsilon_1 \in \mathbb{F}_q^x \), and \( \beta \in \mathcal{M}_\Lambda \) such that
\[
\rho = \alpha^{r} t^{(1)}_{(1,2)} t^{(2)}_{(2,1)} t^{(3)}_{(1,2)} t^{(4)}_{(1,2)} = \begin{pmatrix} \epsilon_1u_2b & v + ua \\ * & * \end{pmatrix}.
\]

Set
\[
\chi := -\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rho \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} -v - ua & \epsilon_1u_2b \\ * & * \end{pmatrix} \in \text{SL}_2(\mathcal{A}).
\]
Since \( v \equiv -1 \) (mod \( u_2 \)), we see that \( v = -1 + u_2v_2 \) for some \( v_2 \in \mathcal{A} \), and thus
\[
-v - ua = 1 - u_2v_2 = v_2 - u_1a = 1 - (v_2 - u_1a)u_2.
\]
Applying Lemma 3.1 with \( \chi, v_2 - u_1a, \epsilon_1b, u_2b \) in the roles of \( \alpha, a, b, u \), we deduce that there exist \( w^{(2)}, t^{(6)}, t^{(7)}, t^{(8)}, t^{(9)} \in \mathcal{A}, \epsilon_2 \in \mathbb{F}_q^x \), and \( \beta_1 \in \mathcal{M}_\Lambda \) such that
\[
\chi^{w^{(2)}_{(1,2)}(-t^{(6)})_{(2,1)}(-t^{(7)})_{(1,2)}(-t^{(8)})_{(1,2)}(-t^{(9)})_{(2,1)}} = \begin{pmatrix} v + ua & \epsilon_1\epsilon_2b \\ * & * \end{pmatrix}.
\]

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 (20) that
\[
\rho(-w^{(2)}_{(1,2)}(-t^{(6)})_{(2,1)}(-t^{(7)})_{(1,2)}(-t^{(8)})_{(1,2)}(-t^{(9)})_{(2,1)}) = \begin{pmatrix} v + ua & \epsilon b \\ * & * \end{pmatrix},
\]
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 (18) that
\[
\begin{pmatrix}
a u + v & u b \\ * & *
\end{pmatrix} = u \alpha + v 1_2 = \alpha^r \equiv \begin{pmatrix} a^r \\ * \\ * 
\end{pmatrix} \pmod{b}.
\]
Therefore \(a u + v \equiv a^r \pmod{b} \). Since \(\epsilon \in \mathbb{F}_q^\times\) is a unit in \(A\), there exists an element \(t^{(10)} \in A\) such that
\[
a^r = a u + v + t^{(10)} e b.
\]
Hence we deduce from (21) that
\[
\rho(-w^{(2)}) \in \{1, 2\} t^{(6)} \{1, 2\} t^{(7)} \gamma t^{(9)} t^{(9)} t^{(10)} t^{(11)} t^{(12)} = \left(\begin{array}{cc} v + u a & e b \\ * & * \end{array}\right) \left(\begin{array}{c} 1 \\ t^{(10)} \end{array}\right) = \begin{pmatrix} a^r & e b \\ * & * 
\end{pmatrix}.
\]
Set
\[
t^{(5)} = w^{(1)} - w^{(2)} \in A,
\]
and note that
\[
(t^{(5)}) \{1, 2\} = (w^{(1)}) \{1, 2\} (-w^{(2)}) \{1, 2\}.
\]
Hence Lemma 3.2 follows immediately from (19) and (22).

Lemma 3.4. Let \(\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(A)\). 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 \(t^{(1)}, t^{(2)}, \ldots, t^{(12)} \in A\), \(\beta \in \mathcal{M}_\Lambda\), and \(\gamma \in \mathcal{M}_\Lambda^T\) such that
\[
\alpha^r t^{(1)}(1, 2) t^{(1)}(1, 2) t^{(3)}(1, 2) t^{(8)}(1, 2) t^{(7)}(1, 2) t^{(10)}(1, 2) t^{(11)}(1, 2) t^{(12)}(1, 2) = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix}.
\]

Proof. By Lemma 3.2, there exist elements \(\epsilon_1 \in \mathbb{F}_q^\times\), \(t^{(1)}, t^{(2)}, \ldots, t^{(9)} \in A\), \(w^{(1)} \in A\), \(\beta \in \mathcal{M}_\Lambda\), and \(\gamma \in \mathcal{M}_\Lambda^T\) such that
\[
\rho := \alpha^r t^{(1)}(1, 2) t^{(1)}(1, 2) t^{(3)}(1, 2) t^{(8)}(1, 2) t^{(7)}(1, 2) t^{(10)}(1, 2) t^{(11)}(1, 2) t^{(12)}(1, 2) w^{(1)} = \begin{pmatrix} a^r & \epsilon_1 b \\ * & * \end{pmatrix}.
\]

By assumption, we know that \(a^r \equiv \epsilon \pmod{b}\). Since \(\epsilon_1 \in \mathbb{F}_q^\times\) is a unit in \(A\), there exists an element \(w^{(2)} \in A\) such that
\[
a^r + \epsilon_1 bw^{(2)} = \epsilon,
\]
and thus
\[
\rho(w^{(2)}) \{1, 2\} = \begin{pmatrix} a^r & \epsilon_1 b \\ * & * \end{pmatrix} \left(\begin{array}{c} 1 \\ w^{(2)} \end{array}\right) = \begin{pmatrix} a^r + \epsilon_1 bw^{(2)} \\ * \end{array} \begin{array}{c} \epsilon_1 b \\ * \end{array} = \begin{pmatrix} \epsilon & \epsilon_1 b \\ * & * \end{array}.
\]

Set
\[
t^{(11)} = -\frac{\epsilon_1 b}{\epsilon}.
\]
Since \(\epsilon \in \mathbb{F}_q^\times\) is a unit in \(A\), we get that \(t^{(11)} \in A\). We see from (24) that
\[
\rho(w^{(2)}) \{1, 2\} = \begin{pmatrix} \epsilon & \epsilon_1 b \\ * & * \end{pmatrix} t^{(11)} \{1, 2\} = \begin{pmatrix} \epsilon & \epsilon_1 b \\ * & * \end{pmatrix} \left(\begin{array}{c} 1 \\ t^{(11)} \end{array}\right) = \begin{pmatrix} \epsilon & \epsilon t^{(11)} + \epsilon_1 b \\ * & * \end{array} = \begin{pmatrix} \epsilon & 0 \\ m & n \end{array},
\]
where \(m, n\) are certain elements in \(A\).

By (23), we know that \(\det(\rho) = 1\), and thus
\[
\epsilon n = \det \begin{pmatrix} \epsilon & 0 \\ m & n \end{pmatrix} = \det(\rho w^{(2)} \{1, 2\}) = 1,
\]
and therefore $n = \epsilon^{-1}$. Hence (25) implies that

\begin{equation}
\rho_{t^{(2)}}(\{2,1\}) = \begin{pmatrix} \epsilon & 0 \\ m & \epsilon^{-1} \end{pmatrix}.
\end{equation}

Set

\[ t^{(12)} = -\epsilon m \in A. \]

An easy calculation now shows that

\begin{equation}
\rho_{t^{(2)}}(\{2,1\}) t^{(11)}(2,1) = \begin{pmatrix} \epsilon & 0 \\ m & \epsilon^{-1} \end{pmatrix} \begin{pmatrix} 1 \\ t^{(12)} \end{pmatrix} = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix}.
\end{equation}

Setting

\[ t^{(10)} = w^{(1)} + w^{(2)}, \]

we see that Lemma 3.4 follows immediately from (23) and (27).

\[ \square \]

**Corollary 3.5.** Let $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(A)$. 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 $\chi_3 \in \mathcal{F}_3(A^3), \chi_4 \in \mathcal{G}_4(A^4), \chi_5 \in \mathcal{G}_5(A^5), \gamma \Lambda \in \mathcal{M}_A^T$, and $\beta \Lambda \in \mathcal{M}_A$.

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

\begin{equation}
\alpha^r = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} \chi_5 \gamma \Lambda \chi_4 \beta \Lambda \chi_3,
\end{equation}

where $\chi_3 \in \mathcal{F}_3(A^3), \chi_4 \in \mathcal{G}_4(A^4), \chi_5 \in \mathcal{G}_5(A^5), \gamma \Lambda \in \mathcal{M}_A^T$, and $\beta \Lambda \in \mathcal{M}_A$.

\[ \square \]
Corollary 3.6. Let $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{A})$. Assume that there exist relatively prime integers $r, s \geq 1$ such that $a^r \equiv e_1 \pmod{b}$ and $a^s \equiv e_2 \pmod{c}$ for some units $e_1, e_2 \in \mathbb{F}_q^\times$. Then there exist $\chi_3 \in \mathcal{F}_3(\mathbb{A}^3)$, $\chi_4 \in \mathcal{G}_4(\mathbb{A}^4)$, $\chi_9 \in \mathcal{G}_9(\mathbb{A}^9)$, $\chi_3^\circ \in \mathcal{G}_3(\mathbb{A}^3)$, $\chi_4^\circ \in \mathcal{F}_4(\mathbb{A}^4)$, $\chi_9^\circ \in \mathcal{F}_9(\mathbb{A}^9)$, $\gamma_\Lambda^\circ, \beta_\Lambda \in \mathcal{M}_\Lambda$, and $\gamma_\Lambda, \beta_\Lambda \in \mathcal{M}_\Lambda^T$ such that

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

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

$$\alpha^r = \begin{pmatrix} e_1 & 0 \\ 0 & e_1^{-1} \end{pmatrix} \chi_3^\circ \gamma_\Lambda \chi_4 \beta_\Lambda \chi_3,$$

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

Applying Corollary 3.5 with $\alpha^T$ in the role of $\alpha$, one can write

$$\left(\alpha^T\right)^s = \begin{pmatrix} e_2 & 0 \\ 0 & e_2^{-1} \end{pmatrix} \chi_3^\circ \gamma_\Lambda \chi_4 \beta_\Lambda \chi_3,$$

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

Conjugating both sides of (33) by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, we deduce from Lemma 2.1 that

$$\alpha^{-s} = \begin{pmatrix} e_2^{-1} & 0 \\ 0 & e_2 \end{pmatrix} \chi_3^\circ \gamma_\Lambda \chi_4 \beta_\Lambda \chi_3,$$

where

$$\chi_3^\circ = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \chi_5 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1},$$

$$\gamma_\Lambda^* = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \gamma_\Lambda \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1},$$

$$\chi_4^* = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \chi_4 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1},$$

$$\beta_\Lambda^* = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \beta_\Lambda \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1},$$

$$\chi_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \chi_3 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}.$$  

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

By Corollary 2.6,

$$\chi_9^\circ := \begin{pmatrix} e_2^{-1} & 0 \\ 0 & e_2 \end{pmatrix} \chi_5 \in \mathcal{F}_9(\mathbb{A}^9).$$

Similarly one sees that

$$\chi_9 := \begin{pmatrix} e_1 & 0 \\ 0 & e_1^{-1} \end{pmatrix} \chi_5^\# \in \mathcal{G}_9(\mathbb{A}^9).$$

From (32) and (34), we deduce that

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

which proves our contention. □
Lemma 3.7. Every element $\alpha \in \text{SL}_2(A)$ can be represented as
\[ \alpha = \chi_9 \gamma \Lambda \chi_4 \beta \Lambda \gamma \Lambda \chi_4 \beta \Lambda \chi_4, \]
where
(i) $\chi_4 \in G_4(A^4)$, and $\chi_9 \in G_9(A^9)$;
(ii) $\chi_4 \in F_4(A^4)$, and $\chi_{11} \in F_{11}(A^{11})$;
(iii) $\gamma \Lambda \in G_4(A^4)$;
(iv) $\gamma \Lambda, \beta \Lambda \in M_\Lambda$, and $\gamma \Lambda, \beta \Lambda \in M_\Lambda^T$.

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

* Case 1. $a = 0$.
  Since $\alpha \in \text{SL}_2(A)$, we see that $b = -\epsilon$ and $c = \epsilon^{-1}$ for some unit $\epsilon \in \mathbb{F}_q^\times$. One can write
  \[ \alpha = \begin{pmatrix} 0 & -\epsilon \\ \epsilon^{-1} & d \end{pmatrix} = \begin{pmatrix} 0 & -\epsilon \\ \epsilon^{-1} & 0 \end{pmatrix} (ed)_{\{1, 2\}} = \chi_9 \gamma \Lambda \chi_4 \beta \Lambda \gamma \Lambda \chi_4 \beta \Lambda \chi_4, \]
  where
  \[ \chi_9 = \begin{pmatrix} 0 & -\epsilon \\ \epsilon^{-1} & 0 \end{pmatrix} (ed)_{\{1, 2\}}, \]
  and
  \[ \gamma \Lambda = \chi_4 = \beta \Lambda = \chi_{11} = \gamma \Lambda = \chi_4 = \beta \Lambda = \chi_4 = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \]

  Lemmas 2.5(ii) and 2.2 imply that
  \[ \chi_9 = \begin{pmatrix} 0 & -\epsilon \\ \epsilon^{-1} & 0 \end{pmatrix} (ed)_{\{1, 2\}} \in G_4(A^4), \]
  and it thus follows from Lemma 2.4(i) that $\chi_9 \in G_9(A^9)$. Lemma 3.7 then follows immediately from (35).

* Case 1. $a \neq 0$.
  By Rosen [7, Theorem 4.8], there exist $u, v \in A$ such that $au + b, av + c$ are primes and $\text{gcd}(\deg(au + b), \deg(av + c)) = 1$. Set
  \[ \varphi_1 = au + b, \]
  \[ \varphi_2 = av + c, \]
  \[ \epsilon_1 = \frac{q^{\deg(\varphi_1)} - 1}{q - 1}, \]
  \[ \epsilon_2 = \frac{q^{\deg(\varphi_2)} - 1}{q - 1}. \]
  The choice of $u, v$ implies that $\text{gcd}(\deg(\varphi_1), \deg(\varphi_2)) = 1$.

  We see that
  \[ \text{gcd}(q^{\deg(\varphi_1)} - 1, q^{\deg(\varphi_2)} - 1) = q^{\text{gcd}(\deg(\varphi_1), \deg(\varphi_2))} - 1 = q - 1, \]
  and thus
  \[ \text{gcd}(\epsilon_1, \epsilon_2) = 1. \]
  \[ \text{gcd}(\epsilon_1, \epsilon_2) = 1. \]
  Set
  \[ \epsilon_1 = \left( \frac{a}{\varphi_1} \right)_{q - 1} \in \mathbb{F}_q^\times, \]
  \[ \epsilon_2 = \left( \frac{a}{\varphi_2} \right)_{q - 1} \in \mathbb{F}_q^\times. \]
where the \( \left( \frac{-1}{\wp_i} \right) \) denotes the \((q-1)\)-th power residue symbol. It is well-known (see Rosen [7, Chapter 3] or Subsection 2.5) that

\[(37) \quad a^{e_1} \equiv e_1 \pmod{\varphi_1},\]

and

\[(38) \quad a^{e_2} \equiv e_2 \pmod{\varphi_2}.\]

We see that

\[(39) \quad v\{2,1\} \alpha u\{1,2\} = \left( \begin{array}{c} a \\ \varphi_1 \\ b \end{array} \right) = \left( \begin{array}{c} au \\ (av + c)u + bv + d \end{array} \right). \]

Using (36), (37), (38), and applying Corollary 3.6 with \(v\{2,1\} \alpha u\{1,2\}, e_1, e_2\) in the roles of \(\alpha, r, s\), respectively, one can write

\[(40) \quad \alpha = \chi\gamma_3\chi_4^\triangledown,\]

where

\[\chi_3 \in \mathcal{F}_3(A^3), \quad \chi_4 \in \mathcal{G}_4(A^4), \quad \chi_3^\triangledown \in \mathcal{G}_3(A^3), \quad \chi_4^\triangledown \in \mathcal{F}_4(A^4), \quad \chi_9 \in \mathcal{F}_9(A^9), \quad \chi_3^\triangledown \in \mathcal{F}_3(A^3), \quad \chi_4^\triangledown \in \mathcal{F}_4(A^4), \quad \chi_9 \in \mathcal{F}_9(A^9), \quad \gamma_\Lambda, \beta_\Lambda \in \mathcal{M}_\Lambda, \quad \gamma_\triangledown, \beta_\triangledown \in \mathcal{T}_\Lambda. \]

The above equation implies that

\[\alpha = \chi_9 \gamma_\Lambda \chi_4^\triangledown \chi_3^\triangledown \chi_4^\triangledown,\]

where

\[\chi_9 = (-v)_{\{2,1\}} \chi_9^\#, \]

\[\chi_3^\triangledown = \chi_3 \chi_9^\triangledown, \]

\[\chi_4^\triangledown = \chi_3^\triangledown \chi_4^\triangledown (-u)_{\{1,2\}}. \]

Since \(\chi_3^\triangledown \in \mathcal{G}_3(A^3)\), the definition of \(\mathcal{G}_i\) and Lemma 2.2 imply that \(\chi_9 \in \mathcal{G}_9(A^9)\) and \(\chi_4^\triangledown \in \mathcal{G}_4(A^4)\). Furthermore Lemma 2.3 implies that \(\chi_1 \in \mathcal{F}_1(A^1)\). Hence Lemma 3.7 follows from (40).

We now prove our main theorem in this paper.

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

**Proof.** Let \(\Omega\) be the polynomial matrix defined by

\[\Omega = \mathcal{G}_9 \mathcal{A}^T \mathcal{G}_4 \mathcal{A} \mathcal{F}_{11}^T \mathcal{A} \mathcal{F}_4 \mathcal{T} \mathcal{G}_4. \]

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

\[\text{SL}_2(A) = \Omega(A^{52}),\]

which proves our contention.

\(\square\)

**Acknowledgements**

I would like to thank Umberto Zannier for pointing out some relevant references, and for many useful discussions. I also thank Leonid Vaserstein for explaining some of his remarks in [10] to me.
REFERENCES

[1] H. Bass, K–theory and stable algebra, Inst. Hautes Études Sci. Publ. Math. (1964), 5–60.
[2] K.-U. Bux and K. Wortman, Finiteness properties of arithmetic groups over function fields, Invent. Math. 167 (2007), no. 2, 355–378.
[3] D. Carter and G. Keller, Elementary expressions for unimodular matrices, Comm. Algebra 12 (1984), 379–389.
[4] D. Goss, Basic structures of function field arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 35, Springer-Verlag, Berlin, (1996).
[5] S. Lang, Algebra, Addison–Wesley Publishing Co., Inc., Reading, Mass. (1965).
[6] H. Nagao, On GL(2, K[x]), J. Inst. Polytech. Osaka City Univ. Ser. A 10 (1959), 117–121.
[7] M. Rosen, Number theory in function fields, Graduate Texts in Mathematics, 210. Springer-Verlag, New York (2002).
[8] T. Skolem, Diophantische Gleichungen, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band V, Heft 4, Springer-Verlag, New York, (1938).
[9] D.S. Thakur, Function Field Arithmetic, World Scientific Publishing Co., Inc., River Edge, NJ, (2004).
[10] L. Vaserstein, Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups, Ann. of Math. (2) 171 (2010), no. 2, 979–1009.
[11] 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.
[12] U. Zannier, Parametrizing $SL_2(\mathbb{Z})$ and a question of Skolem, Acta Arith. 110 (2003), no. 4, 331–337.

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF TEXAS AT AUSTIN, AUSTIN, TX 78712, USA
E-mail address: dongquanngocnguyen@gmail.com