Proc. Indian Acad. Sci. (Math. Sci.) (2020) 130:31
https://doi.org/10.1007/s12044-020-0559-8

Computing n-th roots in SL_2 and Fibonacci polynomials

AMIT KULSHRESTHA[1] and ANUPAM SINGH[2,*]

[1]Indian Institute of Science Education and Research Mohali, Knowledge City, Sector 81, Mohali 140 306, India
[2]Indian Institute of Science Education and Research Pune, Dr. Homi Bhabha Road, Pashan, Pune 411 008, India
*Corresponding Author.
E-mail: amitk@iisermohali.ac.in; anupamk18@gmail.com

MS received 13 August 2019; revised 29 November 2019; accepted 17 December 2019

Abstract. Let k be a field of characteristic $\neq 2$. In this paper, we study squares, cubes and their products in split and anisotropic groups of type A_1. In the split case, we show that computing n-th roots is equivalent to finding solutions of certain polynomial equations in at most two variables over the base field k. The description of these polynomials involves generalised Fibonacci polynomials. Using this we obtain asymptotic proportions of n-th powers, and conjugacy classes which are n-th powers, in $\mathrm{SL}_2(\mathbb{F}_q)$ when n is a prime or $n = 4$. We also extend the already known Waring type result for $\mathrm{SL}_2(\mathbb{F}_q)$, that every element of $\mathrm{SL}_2(\mathbb{F}_q)$ is a product of two squares, to $\mathrm{SL}_2(k)$ for an arbitrary k. For anisotropic groups of type A_1, namely $\mathrm{SL}_1(Q)$ where Q is a quaternion division algebra, we prove that when 2 is a square in k, every element of $\mathrm{SL}_1(Q)$ is a product of two squares if and only if -1 is a square in $\mathrm{SL}_1(Q)$.

Keywords. SL_2; n-th roots; Fibonacci polynomials.

Mathematics Subject Classification. 20G15, 37P35, 11P05, 11B39.

1. Introduction

Let k be a field of characteristic $\neq 2$, and let G be a linear algebraic group over k which is a form of SL_2. In this paper, we determine which elements $g \in G(k)$ admit solutions in $G(k)$ of equations of the type $X^n = g$ and $X_1^n X_2^n = g$. The split and anisotropic forms of SL_2 over k give rise to the groups $\mathrm{SL}_2(k)$ and $\mathrm{SL}_1(Q)$ where Q is a quaternion central division algebra over k. When $X^n = g$ admits a solution for a given g, we explicitly determine all of them. We reduce the problem of finding solutions of $X^n = g$ in $\mathrm{SL}_2(k)$ to finding simultaneous solutions of some polynomial equations in at most two variables. The equation $X^n = g$ for $g \in \mathrm{SL}_1(Q)$ can be solved in $\mathrm{SL}_1(Q)$ via embedding of $\mathrm{SL}_1(Q)$ in $\mathrm{SL}_2(K)$ where K is a maximal subfield in Q.

The proportion of n-th powers in a finite group, and an asymptotic formula for the same is of interest in combinatorics. See, for example, [2,13] where the authors have computed this for the symmetric groups. We count the number $c(n, q)$ of conjugacy classes in $\mathrm{SL}_2(\mathbb{F}_q)$ which are n-th powers, and $s(n, q)$, the number of elements in $\mathrm{SL}_2(\mathbb{F}_q)$ which are n-th

Published online: 25 April 2020

powers. This is the content of Theorem 5.1. We compute these directly without requiring character theory. As an application to our counting, an alternate proof of some well known Waring type theorems (see [4,8–10] for more general results) immediately follows in Corollary 5.6.

Since our computation of determining n-th roots works over an arbitrary field, as an application, we prove some Waring type of results for forms of SL_2. When characteristic $\mathrm{char}(k) \neq 2$, we prove that every element of split group $\mathrm{SL}_2(k)$ is a product of two squares. In addition, if 2 is a square in k, we prove in the anisotropic case that every element of $\mathrm{SL}_1(Q)$ is a product of two squares if and only if -1 is a square in $\mathrm{SL}_1(Q)$. This is proved in Theorem 6.1. Additionally, in Theorem 6.1, we also discuss results concerning products of higher powers in $\mathrm{SL}_2(k)$ and $\mathrm{SL}_1(Q)$.

2. The groups of type A_1

Let k be a field of characteristic $\neq 2$. In this section, we set a notation to be followed later. The groups of type A_1 over k are forms of the algebraic group SL_2 over k. The k-forms of SL_2 are in one-to-one correspondence with quaternion algebras over k. In general, the k points of SL_2 are given by SL_Q (the set of reduced norm 1 elements of Q) where Q is a quaternion algebra over k. The k points of split form corresponds to the matrix algebra $M_2(k)$ and is denoted as $\mathrm{SL}_{2,k}$ and that of anisotropic form corresponds to a quaternion division algebra Q denoted as $\mathrm{SL}_{1,Q}$. To set the notation for what follows, we describe each case briefly.

2.1 *The split form* $\mathrm{SL}_{2,k}$

First, we introduce the split form of the algebraic group SL_2 over k. In what follows, we simply write G, B, T to be the k-rational points of SL_2 (simply denoted as $\mathrm{SL}_2(k)$), the upper triangular Borel and the diagonal maximal torus respectively, for convenience of notation. We fix these notations following the theory of Chevalley groups as in [3]. The set $B = \left\{ \begin{pmatrix} a & b \\ & a^{-1} \end{pmatrix} \mid a \in k^*, b \in k \right\}$ consisting of upper triangular matrices is said to be the standard Borel subgroup of $\mathrm{SL}_2(k)$. The set of all diagonals is a maximal torus and is denoted as T. We denote the diagonal matrices as $\mathfrak{h}(a) = \mathrm{diag}(a, a^{-1})$ for $a \in k^*$, and the root generators as $\mathfrak{X}_{12}(t) = \begin{pmatrix} 1 & t \\ & 1 \end{pmatrix}$ and $\mathfrak{X}_{21}(t) = \begin{pmatrix} 1 & \\ t & 1 \end{pmatrix}$ for $t \in k$. Then the group $\mathrm{SL}_2(k)$ (see Lemma 6.1.1 in [3]) is generated by the set of all root generators $\{\mathfrak{X}_{12}(t_1), \mathfrak{X}_{21}(t_2) \mid t_1, t_2 \in k\}$. Define, $\mathfrak{n}(\alpha) := \mathfrak{X}_{12}(\alpha)\mathfrak{X}_{21}(-\alpha^{-1})\mathfrak{X}_{12}(\alpha) = \begin{pmatrix} & \alpha \\ -\alpha^{-1} & \end{pmatrix}$ for $\alpha \neq 0$ and note that $\mathfrak{h}(a) = \mathfrak{n}(a)\mathfrak{n}(-1)$. To simplify the notation, we denote the Weyl group element $\mathfrak{n}(1) = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ simply by n. The Bruhat decomposition is the double coset decomposition of the group $\mathrm{SL}_2(k)$ with respect to the subgroup B, is $\mathrm{SL}_2(k) = B \bigsqcup B\mathfrak{n}B$. The double cosets have group structure induced by the Weyl group. In this case, the Weyl group is simply $\mathbb{Z}/2\mathbb{Z}$. Every element of B can be written uniquely as $\mathfrak{h}(a)\mathfrak{X}_{12}(s)$, where $a \in k^*, s \in k$. And, every element of $B\mathfrak{n}B$ has an unique expression such as $\mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(s)$ for some $t, s \in k$ and $a \in k^*$. For later computations, we need several commuting relations among the elements we have defined earlier. We list them here.

PROPOSITION 2.1

With the notation as above,

(1) $\mathfrak{h}(ab) = \mathfrak{h}(a)\mathfrak{h}(b), \mathfrak{X}_{12}(t_1+t_2) = \mathfrak{X}_{12}(t_1)+\mathfrak{X}_{12}(t_2), \mathfrak{X}_{21}(t_1+t_2) = \mathfrak{X}_{21}(t_1)+\mathfrak{X}_{21}(t_2)$ *and* $\mathfrak{n}(\alpha)\mathfrak{n}(\beta) = -\mathfrak{h}(\alpha\beta^{-1})$,
(2) $\mathfrak{h}(a)\mathfrak{X}_{12}(t) = \mathfrak{X}_{12}(a^2t)\mathfrak{h}(a)$, $\mathfrak{X}_{12}(t)\mathfrak{h}(a) = \mathfrak{h}(a)\mathfrak{X}_{12}(a^{-2}t)$,
$\mathfrak{h}(a)\mathfrak{X}_{21}(t) = \mathfrak{X}_{21}(a^{-2}t)\mathfrak{h}(a)$, $\mathfrak{h}(a)\mathfrak{n}(\alpha) = \mathfrak{n}(a\alpha) = \mathfrak{n}(a^2\alpha)\mathfrak{h}(a)$,
(3) $\mathfrak{n}(\alpha)\mathfrak{X}_{12}(t) = \mathfrak{X}_{21}(-\alpha^{-2}t)\mathfrak{n}(\alpha)$,
(4) $\mathfrak{n}(a)\mathfrak{X}_{12}(t)\mathfrak{n}(a) = \mathfrak{X}_{12}(-a^2t^{-1})\mathfrak{n}(-a^2t^{-1})\mathfrak{X}_{12}(-a^2t^{-1})$.

We will make use of these results freely as and when required. For the convenience of the reader, we note down multiplication relations as well.

PROPOSITION 2.2

With the notation as above,

(1) $\mathfrak{h}(\alpha_1)\mathfrak{X}_{12}(\psi_1)\cdot\mathfrak{h}(\alpha_2)\mathfrak{X}_{12}(\psi_2) = \mathfrak{h}(\alpha_1\alpha_2)\mathfrak{X}_{12}(\alpha_2^{-2}\psi_1+\psi_2)$,
(2) $\mathfrak{h}(\alpha_1)\mathfrak{X}_{12}(\psi_1)\cdot\mathfrak{X}_{12}(\tau_2)\mathfrak{n}(\alpha_2)\mathfrak{X}_{12}(\psi_2) = \mathfrak{X}_{12}(\alpha_1^2(\psi_1+\tau_1))\mathfrak{n}(\alpha_1\alpha_2)\mathfrak{X}_{12}(\psi_2)$,
(3) $\mathfrak{X}_{12}(\tau_1)\mathfrak{n}(\alpha_1)\mathfrak{X}_{12}(\psi_1)\cdot\mathfrak{X}_{12}(\tau_2)\mathfrak{n}(\alpha_2)\mathfrak{X}_{12}(\psi_2)$

$$= \begin{cases} \mathfrak{X}_{12}\left(\tau_1 - \frac{\alpha_1^2}{\psi_1+\tau_2}\right)\mathfrak{n}\left(-\frac{\alpha_1\alpha_2}{\psi_1+\tau_2}\right)\mathfrak{X}_{12}\left(\psi_2 - \frac{\alpha_2^2}{\psi_1+\tau_2}\right) & \text{when } \psi_1+\tau_2 \neq 0, \\ \mathfrak{h}(-\frac{a_1}{a_2})\mathfrak{X}_{12}(\frac{a_2^2}{a_1^2}\tau_1+\psi_2) \text{ when } \psi_1+\tau_2 = 0. \end{cases}$$

We also follow the convention that the scalars which are used for $\mathfrak{n}()$ and $\mathfrak{h}()$ (such as a, α) are invertible in k and the elements which are used for $\mathfrak{X}_{12}()$, such as s, t, τ, ψ are in k.

2.2 *The anisotropic form* $\mathrm{SL}_{1,Q}$

In this paper, we reserve the notation Q to denote a quaternion division algebra. Once again, for convenience of notation, we denote the k points of anisotropic form of SL_2, simply by $\mathrm{SL}_1(Q)$ which is the set of norm 1 elements of Q. We describe the doubling construction here (see [14, §1.5]) and follow this notation in the following sections.

Let K be a degree 2 field extension of k. We write $K = k(\zeta)$, where $\zeta^2 = a \in k^*$. Let $x \to \bar{x}$ be the non-trivial k-automorphism of K induced by $\zeta \mapsto -\zeta$. Let $\lambda \in k^*$ be such that $\lambda \notin N(K^*)$. Here $N : K^* \to k^*$ denotes the norm map for quadratic extension given by $N(x) = x\bar{x}$. Then, the quaternion algebra $Q = K \oplus K$ with multiplication defined by

$$(x_1, y_1).(x_2, y_2) = (x_1x_2 + \lambda y_1\bar{y}_2, x_1y_2 + \bar{x}_2y_1)$$

is a division algebra. This quaternion algebra is denoted by $Q = \left(\frac{a,\lambda}{k}\right)$. The conjugation involution in Q is given by $\overline{(x, y)} = \bar{x} - y$ and the norm is given by the formula $N((x, y)) = N(x) - \lambda N(y)$ (see Proposition 1.5.1 of [14]). We remark that we use the same notation for conjugation and norm in Q as we do over the field K, while the purpose is clear from the context. The group $\{(x, y) \in Q : N((x, y)) = 1\}$ of norm 1 elements in Q is denoted by $\mathrm{SL}_1(Q)$. We embed Q into $M_2(K)$ as follows:

$$(x, y) \mapsto \begin{pmatrix} x & \lambda y \\ \bar{y} & \bar{x} \end{pmatrix}$$

and the quaternion multiplication (trace and norm respectively) becomes matrix multiplication (trace and determinant respectively). We can further think of $\mathrm{SL}_1(Q) = (\mathrm{SL}_1(Q) \cap B) \bigsqcup (\mathrm{SL}_1(Q) \cap B\mathfrak{n}B)$, where B is a Borel in $\mathrm{SL}_2(K)$. This allows us to use computations in split SL_2 to be used in this case as well. Notice that $\begin{pmatrix} x & \lambda y \\ \bar{y} & \bar{x} \end{pmatrix} = \mathfrak{X}_{12}\left(\frac{x}{\bar{y}}\right)\mathfrak{n}\left(\frac{-1}{\bar{y}}\right)\mathfrak{X}_{12}\left(\frac{\bar{x}}{\bar{y}}\right)$ for $y \neq 0$.

2.3 *Conjugacy classes in* $\mathrm{SL}_2(\mathbb{F}_q)$

This can be found in many textbooks on representation theory of finite groups. The size of the group is $q(q^2 - 1)$. In all, there are $q + 4$ conjugacy classes. We list them below according to their types.

Central classes. The two elements ± 1, represented as $\mathfrak{h}(\pm 1)$, are in the centre and form distinct conjugacy classes.

Split regular semisimple classes. These are the diagonal matrices represented by elements $\mathfrak{h}(a)$ with $a \neq \pm 1$. There are $\frac{q-3}{2}$ such conjugacy classes and each conjugacy class is of size $q(q + 1)$.

Non-semisimple classes. There are 4 such conjugacy classes given by $\mathfrak{X}_{12}(1)$, $\mathfrak{h}(-1)\mathfrak{X}_{12}(-1)$, $\mathfrak{X}_{12}(\epsilon)$, $\mathfrak{h}(-1)\mathfrak{X}_{12}(-\epsilon)$ where ϵ is a fixed non-square in $\mathbb{F}_q$. The size of each conjugacy class is $\frac{(q-1)(q+1)}{2}$.

Anisotropic regular semisimple classes. These conjugacy classes are given by the companion matrix of an irreducible polynomial $X^2 - \delta X + 1$ of degree 2. Thus, these classes are represented by the companion matrix $\mathfrak{n}(-1)\mathfrak{X}_{12}(\delta)$ where $\delta \in \mathbb{F}_q$ satisfying $\delta^2 - 4$, a non-square in the field. There are $\frac{q-1}{2}$ such conjugacy classes and each one of them are of size $q(q - 1)$. In Section 5, we present a different perspective to look at these classes which is useful in counting.

3. Generalised Fibonacci polynomials and n-th power

In this section, we define Fibonacci polynomials in two variables which appear in our study later. Denote $u_0(X, Y) = 0$, $u_1(X, Y) = 1$ and define recursively,

$$u_r(X, Y) = Xu_{r-1}(X, Y) + Yu_{r-2}(X, Y).$$

Thus, $u_2(X, Y) = X$, $u_3(X, Y) = X^2 + Y$, $u_4(X, Y) = X^3 + 2XY$ and so on. These polynomials have been studied in literature, for example, see [1,6]. We mention a few interesting properties keeping in mind that these polynomials are in $\mathbb{Z}[X, Y]$.

PROPOSITION 3.1

With the notation as above,

(1) *For* $n \geq 2$, $u_n \mid u_m$ *if and only if* $n \mid m$,
(2) $(u_n, u_m) = u_{(n,m)}$. *This implies*, $(u_n, u_{n+1}) = 1$,

(3) *The polynomials $u_n(X,Y)$ is irreducible over $\mathbb{Q}$ if and only if n is a prime*,
(4) $u_{m+n+1} = u_{m+1}u_{n+1} + Yu_mu_n$.

If we put $\phi(X, Y) = \frac{X+\sqrt{X^2+4Y}}{2}$ and $\psi(X, Y) = \frac{X-\sqrt{X^2+4Y}}{2}$, then

$$u_n = \frac{\phi^n - \psi^n}{\phi - \psi}.$$

In our study, we come across the homogeneous version of these polynomials obtained as follows. Define $f_n(X, Y) = u_{n+1}(X, -Y^2)$. Therefore, $f_{-1}(X, Y) = 0$, $f_0(X, Y) = 1$ and recursively,

$$f_r(X, Y) = Xf_{r-1}(X, Y) - Y^2 f_{r-2}(X, Y).$$

For example, $f_1 = X$, $f_2 = X^2 - Y^2$, $f_3 = X^3 - 2XY^2$, $f_4 = X^4 - 3X^2Y^2 + Y^4$, $f_5 = X^5 - 4X^3Y^2 + 3XY^4$, $f_6 = X^6 - 5X^4Y^2 + 6X^2Y^4 - Y^6$ and so on. Clearly, all these polynomials belong to $\mathbb{Z}[X, Y]$ and are homogeneous of degree r. In this paper, we refer to these polynomials $f_n(X, Y)$ as generalised Fibonacci polynomials.

We compute a formula for x^n when $x \in B\mathfrak{n}B$. This formula is interestingly related to the generalised Fibonacci polynomials $f_n(X, Y)$ defined above. We formulate this as a recursive relation in the generic case when the powers are not in B.

PROPOSITION 3.2

Let $x = \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(s)$ be in $B\mathfrak{n}B$ and suppose x^i belongs to $B\mathfrak{n}B$ for all $1 \le i \le n$. Let us denote $x^i = \mathfrak{X}_{12}(t_i)\mathfrak{n}(a_i)\mathfrak{X}_{12}(s_i)$, where $t_1 = t, a_1 = a$ and $s_1 = s$. Then $x^n = \mathfrak{X}_{12}(t_n)\mathfrak{n}(a_n)\mathfrak{X}_{12}(s_n)$, where

$$t_n = t - \frac{a^2}{t + s_{n-1}}, \quad s_n = s - \frac{a^2}{t + s_{n-1}}, \quad a_n = -\frac{a_{n-1}a}{t + s_{n-1}}.$$

Proof. We compute

$$\begin{aligned}
x^n &= x^{n-1} \cdot x = \mathfrak{X}_{12}(t_{n-1})\mathfrak{n}(a_{n-1})\mathfrak{X}_{12}(s_{n-1}) \cdot \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(s) \\
&= \mathfrak{X}_{12}(t_{n-1}) \cdot \mathfrak{n}(a_{n-1}).\mathfrak{X}_{12}(s_{n-1} + t)\mathfrak{n}(a)\mathfrak{X}_{12}(s) \\
&= \mathfrak{X}_{12}(t_{n-1})\mathfrak{h}\left(\frac{a_{n-1}}{a}\right) \cdot \mathfrak{n}(a)\mathfrak{X}_{12}(s_{n-1} + t)\mathfrak{n}(a).\mathfrak{X}_{12}(s) \\
&= \mathfrak{X}_{12}(t_{n-1})\mathfrak{h}\left(\frac{a_{n-1}}{a}\right) \cdot \mathfrak{X}_{12}\left(-\frac{a^2}{t + s_{n-1}}\right)\mathfrak{n}\left(-\frac{a^2}{t + s_{n-1}}\right) \\
&\quad \mathfrak{X}_{12}\left(-\frac{a^2}{t + s_{n-1}}\right) \cdot \mathfrak{X}_{12}(s) \\
&= \mathfrak{X}_{12}(t_{n-1})\mathfrak{h}\left(\frac{a_{n-1}}{a}\right) \cdot \mathfrak{X}_{12}\left(-\frac{a^2}{t + s_{n-1}}\right)\mathfrak{n}\left(-\frac{a^2}{t + s_{n-1}}\right) \\
&\quad \mathfrak{X}_{12}\left(s - \frac{a^2}{t + s_{n-1}}\right) \\
&= \mathfrak{X}_{12}(t_{n-1})\mathfrak{X}_{12}\left(-\frac{a_{n-1}^2a^2}{a^2(t + s_{n-1})}\right)\mathfrak{h}\left(\frac{a_{n-1}}{a}\right)\mathfrak{n}\left(-\frac{a^2}{t + s_{n-1}}\right)
\end{aligned}$$

$$\mathfrak{X}_{12}\left(s-\frac{a^2}{t+s_{n-1}}\right)$$
$$=\mathfrak{X}_{12}\left(t_{n-1}-\frac{a_{n-1}^2}{t+s_{n-1}}\right)\mathfrak{n}\left(-\frac{a_{n-1}a}{t+s_{n-1}}\right)\mathfrak{X}_{12}\left(s-\frac{a^2}{t+s_{n-1}}\right).$$

The first formula follows by symmetry of computation if we compute $x\cdot x^{n-1}$. □

Now we rewrite these formulae involving generalised Fibonacci polynomials. Appearance of these polynomials in computing powers is well known (for example, see [12]). To begin with, $t+s=f_1(t+s,a)$. Now, note that $t+s_2=t+\left(s-\frac{a^2}{t+s}\right)=\frac{(t+s)^2-a^2}{t+s}$. Thus we get $(t+s)(t+s_2)=(t+s)^2-a^2=f_2(t+s,a)$. More generally, we have the following,

Lemma 3.3. *With the notation as above, for* $r\geq 1$,

$$\prod_{i=1}^{r}(t+s_i)=(t+s)\prod_{i=1}^{r-1}(t+s_i)-a^2\prod_{i=1}^{r-2}(t+s_i)=f_r(t+s,a).$$

Proof. We already noted that $t+s=f_1(t+s,a)$ and $(t+s_1)(t+s_2)=f_2(t+s,a)$. Thus, if we prove the recursive relation we would have established the second identity. We note that, for $r\geq 3$,

$$(t+s)\prod_{i=1}^{r-1}(t+s_i)-a^2\prod_{i=1}^{r-2}(t+s_i)=\left(\prod_{i=1}^{r-1}(t+s_i)\right)\left((t+s)-\frac{a^2}{t+s_{r-1}}\right)$$
$$=\left(\prod_{i=1}^{r-1}(t+s_i)\right)(t+s_r)=\prod_{i=1}^{r}(t+s_i).$$

□

Thus, the formulae in Proposition 3.2 can be re-written as follows:

$$\begin{aligned}t_n&=t-a^2\frac{f_{n-2}(t+s,a)}{f_{n-1}(t+s,a)},\\ s_n&=s-a^2\frac{f_{n-2}(t+s,a)}{f_{n-1}(t+s,a)},\\ a_n&=(-1)^{n-1}\frac{a^n}{f_{n-1}(t+s,a)},\end{aligned}\tag{3.1}$$

where the last equation is obtained inductively as follows:

$$a_n=-\frac{a_{n-1}a}{t+s_{n-1}}=(-1)^2\frac{a_{n-2}a^2}{(t+s_{n-2})(t+s_{n-1})}=\cdots$$
$$=(-1)^{n-1}\frac{a^n}{f_{n-1}(t+s,a)}.$$

Now we deal with the case when $x\in B\mathfrak{n}B$. It can happen that a certain power x^r is in B. We determine this in the following.

PROPOSITION 3.4

Let $x = \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(s) \in B\mathfrak{n}B$. *Then*

(1) $f_1(t+s,a), \ldots, f_{r-2}(t+s,a)$ *are all non-zero and* $f_{r-1}(t+s,a) = 0$ *if and only if* $x, \ldots, x^{r-1} \in B\mathfrak{n}B$ *and* $x^r \in B$.
(2) *Let* r *be the smallest power such that* $x^r \in B$ *(i.e.,* $x^{r-1} \notin B$*). Then,* $x^n \in B$ *if and only if* $r \mid n$.

Proof. First, let us prove Proposition 3.4(1). Clearly if $f_1(t+s,a)$ is not zero, we can compute x^2 by the formula (3.1) and, hence x^2 belongs to $B\mathfrak{n}B$. Thus if $f_1(t+s,a), \ldots, f_{i-1}(t+s,a)$ all are non-zero, we can compute x^i by the formula and hence it belongs to $B\mathfrak{n}B$ not in B. For the converse, let us assume $f_1(t+s,a), \ldots, f_{r-2}(t+s,a)$ are all non-zero and $f_{r-1}(t+s,a) = 0$.

Let us verify this for $r = 2$, i.e., we have $f_1(t+s,a) = t+s = 0$. In this case, $x = \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(-t) = \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(t)^{-1}$ and $x^2 = \mathfrak{X}_{12}(t)\mathfrak{n}(a)^2\mathfrak{X}_{12}(t)^{-1} = -1$. Thus, $x^2 \in B$ and $x^n = (-1)^m$ if $n = 2m$ and $x^n = (-1)^m x$ if $n = 2m+1$. Thus $x^n \in B$ if and only if n is even.

Now to prove the general case, we note that $0 = f_{r-1}(t+s,a) = (t+s)f_{r-2}(t+s,a) - a^2 f_{r-3}(t+s,a)$ (Fibonacci relation) gives $(t+s)f_{r-2}(t+s,a) = a^2 f_{r-3}(t+s,a)$. Thus, x^{r-1} can be computed by the formula (3.1) and $t_{r-1} = t - a^2\frac{f_{r-3}(t+s,a)}{f_{r-2}(t+s,a)} = t - a^2\frac{(t+s)}{a^2} = -s$, similarly, $s_{r-1} = -t$. Thus

$$\begin{aligned} x^r &= x \cdot x^{r-1} = \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(s) \cdot \mathfrak{X}_{12}(t_{r-1})\mathfrak{n}(a_{r-1})\mathfrak{X}_{12}(s_{r-1}) \\ &= \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(s) \cdot \mathfrak{X}_{12}(-s)\mathfrak{n}(a_{r-1})\mathfrak{X}_{12}(-t) \\ &= \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{n}(a_{r-1})\mathfrak{X}_{12}(-t) = \mathfrak{X}_{12}(t)\mathfrak{h}(-aa_{r-1}^{-1})\mathfrak{X}_{12}(-t) \\ &= \mathfrak{h}\left(-\frac{a}{a_{r-1}}\right)\mathfrak{X}_{12}\left(\left(\frac{a_{r-1}^2}{a^2} - 1\right)t\right) \end{aligned} \tag{3.2}$$

which belongs to B.

To prove Proposition 3.4(2), if $r \mid n$, then $x^n = (x^r)^{\frac{n}{r}} \in B$. Now suppose $x^n \in B$. Since r is smallest such that $x^r \in B$ and $x^i \notin B$ for all i, with $1 \le i \le r-1$, $x^i \in B\mathfrak{n}B$. Now we write $n = lr + m$, where $0 \le m \le r-1$ and then $x^n = (x^r)^l x^m$. Thus, $x^n \in B$ if and only if $m = 0$, which happens if and only if $r \mid n$. □

In the next section, we use the above to determine if an element of $\mathrm{SL}_2(k)$ has n- root.

4. n-th root in $\mathrm{SL}_2(k)$

Let g be an element of $\mathrm{SL}_2(k)$, where $\mathrm{char}(k) \neq 2$. We want to solve the equation $X^n = g$ in $\mathrm{SL}_2(k)$. We make two separate cases depending on if g is in B or in $B\mathfrak{n}B$.

4.1 *n-th roots in Borel*

Let $g = \mathfrak{h}(\alpha)\mathfrak{X}_{12}(\psi) \in B$ and let $x \in \mathrm{SL}_2(k)$ be a solution of $X^n = g$. We make two cases separately depending on if x is in B or $B\mathfrak{n}B$. For an element $\alpha \in k$, define

the following polynomials: $S_{2m}(\alpha, X) = (1+\alpha)(1+X^2+X^4+\cdots+X^{2(m-1)})$ and $S_{2m+1}(\alpha, X) = 1+\alpha X+X^2+\alpha X^3+X^4+\cdots+\alpha X^{2m-1}+X^{2m}$. We remark that $S_{2m}(-1, X) = 0$.

PROPOSITION 4.1

Let $g = \mathfrak{h}(\alpha)\mathfrak{X}_{12}(\psi) \in B$. Then

(1) *for $\alpha = \pm 1$, the equation $x^n = g$ has a solution $x \in B$ if and only if the equations $X^n = \alpha$ and $S_n(\alpha, X)Y - \psi X^{2(n-1)} = 0$ have simultaneous solution for X, Y in k,*
(2) *for $\alpha \neq \pm 1$, the equation $x^n = g$ has a solution $x \in B$ if and only if the equation $X^n = \alpha$ has a solution $X \in k$.*

Proof. Let $x = \mathfrak{h}(a)\mathfrak{X}_{12}(t) \in B$ be a root of $X^n = g$. Let us compute using formulae in Proposition 2.1, $x^2 = \mathfrak{h}(a^2)\mathfrak{X}_{12}((1+a^{-2})t)$, $x^3 = \mathfrak{h}(a^3)\mathfrak{X}_{12}((1+a^{-2}+a^{-4})t)$ and inductively, $x^n = \mathfrak{h}(a^n)\mathfrak{X}_{12}((1+a^{-2}+a^{-4}+\cdots+a^{-2(n-1)})t)$. Thus $x^n = g$ gives two equations,

$$a^n = \alpha, \qquad (1+a^{-2}+a^{-4}+\cdots+a^{-2(n-1)})t = \psi.$$

Clearly to show that the solution x exists we need to solve these two equations for a and t.

In the case of Proposition 4.1(1), the equations are $a^n = 1$ and $(1+a^{-2}+a^{-4}+\cdots+a^{-2(n-1)})t = \psi$. By multiplying the second equation with $a^{-2(n-1)}$ we get the required formula.

In the case of Proposition 4.1(2), by multiplying with a^{-2} to the second equation and subtracting with itself, we get $(1-a^{-2n})t = (1-a^{-2})\psi$. Thus to get a we need to solve the equation $X^n = \alpha$ over k and to get t we need to make sure $a^{-2n} \neq 1$, i.e., $\alpha^2 \neq 1$. Conversely, the solution $x = \mathfrak{h}(a)\mathfrak{X}_{12}(t)$ is determined by the root $a^n = \alpha$ provided $a^{2n} \neq 1$ and $t = \left(\frac{1-a^{-2}}{1-a^{-2n}}\right)\psi$. □

Now, we deal with the case if solution x comes from $B\mathfrak{n}B$. First, we deal with some small order cases.

PROPOSITION 4.2

Let $g = \mathfrak{h}(\alpha)\mathfrak{X}_{12}(\psi) \in B$. Then

(1) *the equation $x^2 = g$ has a solution x in $B\mathfrak{n}B$ if and only if $g = -1$. Further, the solutions are of the form $x = \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(-t)$.*
(2) *The equation $x^3 = g$ has a solution x in $B\mathfrak{n}B$ if and only if $g = \pm 1$. Further, the solutions are of the form $x = \mathfrak{X}_{12}(a-s)\mathfrak{n}(a)\mathfrak{X}_{12}(s)$ or $\mathfrak{X}_{12}(-a-s)\mathfrak{n}(a)\mathfrak{X}_{12}(s)$.*
(3) *The equation $x^4 = g$ has a solution x in $B\mathfrak{n}B$ if and only if $g = \pm 1$. The solutions for $g = 1$ come from that of $x^2 = -1$ in $B\mathfrak{n}B$. The equation $x^4 = -1$ has a solution x in $B\mathfrak{n}B$ if and only if $X^2 - 2Y^2 = 0$ has a solution X, Y in k with $Y \neq 0$. Further, the solutions are of the form $\mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(-t+\gamma a)$ where $\gamma^2 = 2$.*

Proof. We begin with proving Proposition 4.2(1). Let $x = \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(s) \in B\mathfrak{n}B$ be such that $x^2 \in B$. For this, it follows from Proposition 3.4 that $f_1(t+s, a) = t+s = 0$. Hence $x = \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(-t) = \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(t)^{-1}$ and $x^2 = -1$.

For proving Proposition 4.2(2), if $x^3 \in B$, we must have $f_1(t+s,a) = t+s \neq 0$ and $f_2(t+s,a) = (t+s)^2 - a^2 = 0$. And $x^3 = \mathfrak{h}\left(-\frac{a}{a_2}\right)\mathfrak{X}_{12}\left(\left(\frac{a_2^2}{a^2}-1\right)t\right) = \mathfrak{h}\left(\frac{t+s}{a}\right)\mathfrak{X}_{12}\left(\left(\frac{a^2}{(t+s)^2}-1\right)t\right) = \mathfrak{h}(\pm 1) = \pm 1$ since $a_2 = -\frac{a^2}{t+s}$.

For proving Proposition 4.2(3), if $x^4 \in B$, we make two cases, first when $x^2 \in B$. From part (1), this happens when $x^2 = -1$ and that would give $x^4 = 1$. These solutions are conjugates of $\mathfrak{n}(a)$. The second case is when $x^2 \notin B$, thus we have $f_1(t+s,a) = t+s \neq 0$, $f_2(t+s,a) = (t+s)^2 - a^2 \neq 0$ and $f_3(t+s,a) = (t+s)^3 - 2(t+s)a^2 = 0$. The last equation gives $(t+s)^2 - 2a^2 = 0$. Now using the formula $a_3 = \frac{a^3}{(t+s)^2-a^2} = \frac{a^3}{2a^2-a^2} = a$, we compute $x^4 = \mathfrak{h}\left(-\frac{a}{a_3}\right)\mathfrak{X}_{12}\left(\left(\frac{a_3^2}{a^2}-1\right)t\right) = \mathfrak{h}(-1) = -1$. Thus the solution exists only if $g = \pm 1$. We also note that, in the case $g = -1$, the solution exists if and only if $f_3 = 0$ which is equivalent to having solutions of $X^2 - 2Y^2 = 0$. □

PROPOSITION 4.3

Let $g = \mathfrak{h}(\alpha)\mathfrak{X}_{12}(\psi) \in B$ and $n \geq 5$.

(1) *When $\alpha \neq \pm 1$, the equation $x^n = g$ has a solution x in $B\mathfrak{n}B$ if and only if the equations $f_{r-3}(X,Y)^d - (-1)^{d(r-1)}\alpha X^d Y^{d(r-4)} = 0$ and $f_{r-1}(X,Y) = 0$ have simultaneous solutions over k with Y non-zero, for some $d < n$ such that $\mathrm{d}r = n$.*

(2) *When $\alpha = \pm 1$, the equation $x^n = g$ has a solution x in $B\mathfrak{n}B$ if and only if $\psi = 0$. In which case, the solutions are of the form $x = \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(\gamma - t)$, where $X = \gamma$ and $Y = a$ are solutions of the equations*

$$f_{r-3}(X,Y)^d - (-1)^{d(r-1)}\alpha X^d Y^{d(r-4)} = 0 \quad \text{and} \quad f_{r-1}(X,Y) = 0$$

with Y non-zero, for some $d < n$ such that $\mathrm{d}r = n$.

Proof. Let $x = \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(s)$ be a solution of $X^n = g$. Then $x^n = g \in B$. Thus from Proposition 3.4, there exists (smallest) r such that $r \mid n$ and $x^r \in B$. Write $n = rd$. Now using the formula in the proof of the same Proposition, we have

$$\begin{aligned} x^n = (x^r)^d &= \left(\mathfrak{h}\left(-\frac{a}{a_{r-1}}\right)\mathfrak{X}_{12}\left(\left(\frac{a_{r-1}^2}{a^2}-1\right)t\right)\right)^d \\ &= \mathfrak{h}\left(\left(-\frac{a}{a_{r-1}}\right)^d\right)\mathfrak{X}_{12}((1+A+A^2+\cdots+A^{d-1})(A-1)t) \\ &= \mathfrak{h}\left(\left(-\frac{a}{a_{r-1}}\right)^d\right)\mathfrak{X}_{12}((A^d-1)t), \end{aligned}$$

where $A = \left(\frac{a_{r-1}}{a}\right)^2$. Equating this with g we get $\left(-\frac{a}{a_{r-1}}\right)^d = \alpha$ and $(A^d-1)t = \psi$. That is, $\alpha^2 = A^{-d}$ and hence $(\alpha^{-2}-1)t = \psi$. Now using the formula for a_{r-1} in terms of Fibonacci polynomials and noting that $f_{r-1} = 0$, we get $\left(-\frac{a}{a_{r-1}}\right) = (-1)^{r-1}\frac{f_{r-3}}{(t+s)a^{r-4}}$. Raising to the power d we get the required equation.

Now, to prove (1), we get the two equations as above. To prove the converse we need to determine t. But this is clear as $\alpha^2 \neq 1$.

To prove (2), we note that $x^n = \mathfrak{h}\left(\left(-\frac{a}{a_{r-1}}\right)^d\right)$ since $\alpha^2 = 1$. The rest of the proof is as stated earlier. □

4.2 n^{th} *roots in* $B\mathfrak{n}B$

Let $g = \mathfrak{X}_{12}(\tau)\mathfrak{n}(\alpha)\mathfrak{X}_{12}(\psi) \in B\mathfrak{n}B$ and let $x \in \mathrm{SL}_2(k)$ be a solution of $X^n = g$. Since B is a subgroup, the solution x can not belong to B. We prove the following,

PROPOSITION 4.4

For $g = \mathfrak{X}_{12}(\tau)\mathfrak{n}(\alpha)\mathfrak{X}_{12}(\psi) \in B\mathfrak{n}B$, the equation $x^n = g$ has a solution x in $\mathrm{SL}_2(k)$ if and only if the following equations have solution X, Y in k:

(1) $2\alpha f_{n-2}(X, Y) + (-1)^{n-2}XY^{n-2} + (-1)^{n-1}(\tau + \psi)Y^{n-2} = 0$, *and*

(2) $\alpha f_{n-1}(X, Y) + (-1)^n Y^n = 0$,

where $f_n(X, Y)$ denotes the generalised Fibonacci polynomials.

Proof. Let $x = \mathfrak{X}_{12}(t)\mathfrak{n}(a)\mathfrak{X}_{12}(s)$ be a solution, i.e., $x^n = g$. Thus we get $t_n = \tau$, $s_n = \psi$ and $a_n = \alpha$. Using the formulae (3.1), we get the following:

$$\begin{aligned}
\tau &= t - a^2\frac{f_{n-2}(t+s, a)}{f_{n-1}(t+s, a)},\\
\psi &= s - a^2\frac{f_{n-2}(t+s, a)}{f_{n-1}(t+s, a)},\\
\alpha &= (-1)^{n-1}\frac{a^n}{f_{n-1}(t+s, a)}.
\end{aligned} \tag{4.1}$$

We add the first two equations and substitute $X = t + s$ and $Y = a$ to get

$$\tau + \psi = X - 2Y^2\frac{f_{n-2}(X, Y)}{f_{n-1}(X, Y)}.$$

The last equation becomes $\alpha f_{n-1}(X, Y) + (-1)^n Y^n = 0$ which is the second required equation in the theorem. Now we substitute this and get

$$\tau + \psi = X - (-1)^{n-1}2Y^2\frac{f_{n-2}(X, Y)\alpha}{Y^n}$$

which is the required first equation.

For the converse, let T and a be a solution to the equations. That is, we know $t + s = T$ and a. We need to show the existence of t, s and a, so that $x^n = g$. Then the second equation gives $f_{n-1}(t + s, a) = (-1)^{n-1}\frac{a^n}{\alpha}$. And the first equation gives $f_{n-2}(t + s, a)$ and hence we can determine t and s separately. □

In general, it is difficult to separate out the variables X and Y from above equations. However, for $n = 2, 3$ and 4, we can do better and reduce these equations to simpler equations. This we discuss in the following sections. Now we apply our results obtained so far to compute powers.

5. Counting powers in $\mathrm{SL}_2(\mathbb{F}_q)$

Let $c(n, q)$ be the number of conjugacy classes in $\mathrm{SL}_2(\mathbb{F}_q)$ which are the n-th power, and $s(n, q)$ be the number of elements in $\mathrm{SL}_2(\mathbb{F}_q)$ which are the n-th power. In this section, we compute this number for $\mathrm{SL}_2(\mathbb{F}_q)$. Clearly, when $n \nmid (q^3 - q) = |\mathrm{SL}_2(\mathbb{F}_q)|$, then $c(n, q) = q + 4$ and $s(n, q) = (q^3 - q)$. Thus, in what follows, we assume $n \mid (q^3 - q)$. We further compute the asymptotic formula for the ratio of conjugacy classes which are the n-th powers, $c(n) = \lim_{q\to\infty} \dfrac{c(n, q)}{q + 4}$ and the ratio of elements which are n-th powers, $s(n) = \lim_{q\to\infty} \dfrac{s(n, q)}{q^3 - q}$. The main theorem is as follows.

Theorem 5.1. *Suppose q is odd. Then*

(1) *For $n = 2$,*

$q \pmod 4$	$c(2, q)$	$s(2, q)$
1	$\frac{q+5}{2}$	$\frac{q^2(q-1)}{2} - q + 1$
3	$\frac{q+5}{2}$	$\frac{q^2(q-1)}{2} + 1$

Thus, $c(2) = s(2) = \frac{1}{2}$.

(2) *For $n = 4$,*

$q \pmod 8$	$c(4, q)$	$s(4, q)$
1	$\frac{3q+21}{8}$	$\frac{3}{8}q^3 - \frac{1}{2}q^2 - \frac{7}{8}q + 1$
3	$\frac{3q+15}{8}$	$\frac{3}{8}(q^3 - q)$
5	$\frac{3q+17}{8}$	$\frac{3}{8}(q^3 - q)$
7	$\frac{3q+11}{8}$	$\frac{3}{8}q^3 - \frac{1}{2}q^2 + \frac{1}{8}q + 1$

Thus, $c(4) = s(4) = \frac{3}{8}$.

(3) *When n is an odd prime, then*

	$c(n, q)$	$s(n, q)$
$n \mid q$	q	$(q - 2)(q^2 - 1)$
$n \mid (q - 1)$	$\frac{(n+1)(q-1)}{2n} + 5$	$\frac{(n+1)(q^3-q)}{2n}$
$n \mid (q + 1)$	$\frac{(n+1)(q-3)+4}{2n} + 5$	$\frac{(n+1)(q^3-q)}{2n}$

Thus, $c(n) = s(n) = \frac{n+1}{2n}$.

The rest of the section is devoted to the proof of this theorem.

Lemma 5.2. *Suppose* $\mathrm{char}(k) \neq 2$. *Then the set of squares in* $\mathrm{SL}_2(k)$ *is the union of following disjoint subsets*:

(1) $\mathcal{S}_1 = \{\mathfrak{h}(a^2)\mathfrak{X}_{12}(t) \mid a \in k^* \text{ with } a^2 + 1 \neq 0, t \in k\}$,

(2) $\mathcal{S}_2 = \{-1\} \cup \{\mathfrak{X}_{12}(s)\mathfrak{n}(b)\mathfrak{X}_{12}\left(-s + b(a^2-2)\right) \mid a, b \in k^*, s \in k\}$.

Proof. The first set, except possibly the element -1, is obtained by squaring elements of B. For $x = \mathfrak{h}(a)\mathfrak{X}_{12}(t) \in B$, we note that $x^2 = \mathfrak{h}(a^2)\mathfrak{X}_{12}((1+a^{-2})t) \in \mathcal{S}_1$ except when $a^2 = -1$. The case when $a^2 = -1$ gives the element -1 which is also obtained by squaring certain elements of $B\mathfrak{n}B$, for example, $\mathfrak{n}$.

Now to get $\mathcal{S}_2$, we square elements of the set $B\mathfrak{n}B$. Thus this gives elements of the form $\mathfrak{X}_{12}(\tau)\mathfrak{n}(\alpha)\mathfrak{X}_{12}(\psi)$ such that $2 - \frac{\tau+\psi}{\alpha} \in k^{*2}$. This gives the required set. □

Proof of Theorem 5.1(1). We count the cardinalities of $\mathcal{S}_1$ and $\mathcal{S}_2$ as in Lemma 5.2. The cardinality of $\mathcal{S}_1$ is $\frac{q(q-1)}{2}$ when $-1 \notin \mathbb{F}_q^{*2}$ and $\frac{q(q-3)}{2}$ when $-1 \in \mathbb{F}_q^{*2}$. The cardinality of $\mathcal{S}_2$ in both the cases is $q(q-1)\left(\frac{q-1}{2}\right) + 1$. Since $\mathcal{S}_1$ and $\mathcal{S}_2$ are disjoint, we get $s(2,q)$ by adding the two.

Now we count conjugacy classes that are squares. The two central classes ± 1 are square. The element -1 is a square of any conjugate of $\mathfrak{n}$. The split regular semisimple classes are of the form $\mathfrak{h}(a)$ with $a \neq \pm 1$. We know that $\mathfrak{h}(a)$ has a square root if and only if $X^2 - a$ has a root in $\mathbb{F}_q$. Thus, the classes which are square are of the form $\mathfrak{h}(a^2)$ with $a^2 \notin \{0, \pm 1\}$. These are $\lfloor \frac{q-3}{4} \rfloor$ classes out of the total $\frac{q-3}{2}$ such classes. The non-semisimple classes are the 4 conjugacy classes represented by $\mathfrak{X}_{12}(1)$, $\mathfrak{h}(-1)\mathfrak{X}_{12}(-1)$, $\mathfrak{X}_{12}(\epsilon)$, $\mathfrak{h}(-1)\mathfrak{X}_{12}(-\epsilon)$, where ϵ is a fixed non-square in $\mathbb{F}_q$. However, only $\mathfrak{X}_{12}(1)$, $\mathfrak{X}_{12}(\epsilon)$ have square roots (note that q is odd). The anisotropic regular semisimple conjugacy classes are of the form $\mathfrak{n}(-1)\mathfrak{X}_{12}(\delta)$ with $\delta^2 - 4$ a non-square. Again from Proposition 4.4, the square root of class $\mathfrak{n}(-1)\mathfrak{X}_{12}(\delta)$ exists if and only if $X^2 = 2 + \delta$ has a solution in $\mathbb{F}_q$. These are $\lfloor \frac{q-1}{4} \rfloor$ classes out of the total $\frac{q-1}{2}$ such classes. Adding all of these, we get the total number of conjugacy classes which are square which equals $2 + \lfloor \frac{q-3}{4} \rfloor + 2 + \lfloor \frac{q-1}{4} \rfloor = \frac{q+5}{2}$. □

The main hindrance in counting higher power is to count the anisotropic regular semisimple classes. Let us look at it from a slightly different perspective. Let $\xi \in \mathbb{F}_{q^2}^*$, then left multiplication l_ξ defines a groups homomorphism $l : \mathbb{F}_{q^2}^* \to GL_2(\mathbb{F}_q)$. The subgroup $\mathbb{F}_{q^2}^1 = \{x \mid N(x) = x^{1+q} = 1\}$ is of the order $q+1$ and is the kernel of the norm map $N : \mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$ given by $x \mapsto x^{1+q}$. Further, the elements $\xi \in \mathbb{F}_{q^2}^1$ under the map l correspond to the elements in $\mathrm{SL}_2(\mathbb{F}_q)$. Note that $\mathbb{F}_{q^2}^1 \bigcap \mathbb{F}_q = \{\pm 1\}$. Under the homomorphism l, the elements of $\mathbb{F}_{q^2}^1 \backslash \mathbb{F}_q = \mathbb{F}_{q^2}^1 \backslash \{\pm 1\}$ correspond to the anisotropic regular semisimple conjugacy classes of $\mathrm{SL}_2(\mathbb{F}_q)$. Notice that two elements correspond to the same conjugacy class and hence the number of conjugacy classes is $\frac{q+1-2}{2} = \frac{q-1}{2}$. Let $g = l_\xi$ be a representative of an anisotropic regular semisimple class and we wish to solve the equation $X^n = l_\xi$. First, observe that if a solution x to this equation exists in $\mathrm{SL}_2(\mathbb{F}_q)$, it must be in $B\mathfrak{n}B$ and correspond to an anisotropic regular semisimple class, say represented by ζ, that is, we would have $y l_\zeta^n y^{-1} = l_\xi$. This amounts to finding the solution of $X^n = \xi$ in $\mathbb{F}_{q^2}^1 \backslash \{\pm 1\}$. Hence we have as follows.

Lemma 5.3. *With the notation as above and q odd, the number of anisotropic regular semisimple classes in* $\mathrm{SL}_2(\mathbb{F}_q)$ *which are n-th power is as follows*:

$$\begin{cases} \frac{q-1}{2}, & \text{if } (n, q+1) = 1, \\ \frac{1}{2}\left(\frac{q+1}{d} - 1\right), & \text{if } (n, q+1) > 1 \text{ and } -1 \notin (\mathbb{F}_{q^2}^1)^n, \\ \frac{1}{2}\left(\frac{q+1}{d} - 2\right), & \text{if } (n, q+1) > 1 \text{ and } -1 \in (\mathbb{F}_{q^2}^1)^n, \end{cases}$$

where d is the size of the kernel of the map $\mathbb{F}_{q^2}^1 \to \mathbb{F}_{q^2}^1$ given by $x \mapsto x^n$.

COROLLARY 5.4

When $n \geq 3$, a prime, the number of anisotropic regular semisimple conjugacy classes in $\mathrm{SL}_2(\mathbb{F}_q)$ which are the n-th power is

$$\begin{cases} \frac{q-1}{2}, & \text{if } n \nmid q+1, \\ \frac{q+1}{2n} - 1, & \text{if } n \mid q+1. \end{cases}$$

Proof. Since n is an odd prime, ± 1 both are n-th power. The rest follows from the above lemma. □

COROLLARY 5.5

When $n = 4$, the total number of anisotropic regular semisimple classes in $\mathrm{SL}_2(\mathbb{F}_q)$ which are fourth power is

$$\begin{cases} \frac{q-1}{4}, & \text{if } q \equiv 1 \pmod 4, \\ \frac{q-3}{8}, & \text{if } q \equiv 3 \pmod 8, \\ \frac{q-7}{8}, & \text{if } q \equiv 7 \pmod 8. \end{cases}$$

Proof. Since q is odd, 4 is never co-prime to $q+1$. We note that the size of the kernel of the map $\mu_4 \colon \mathbb{F}_{q^2}^1 \to \mathbb{F}_{q^2}^1$ is given by $x \mapsto x^4$ which is the 4-th root of unity, and hence

$$d = \begin{cases} 2 & \text{if } q \equiv 1 \pmod 4, \\ 4 & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Now we need to determine when -1 is in the image of μ_4. We know that -1 is a fourth power in the field $\mathbb{F}_{q^2}$ if and only if $q^2 \equiv 1 \pmod 8$ if and only if $q \equiv \pm 1 \pmod 8$. In the case $q \equiv 1 \pmod 8$, the elements -1 has fourth root in the base field $\mathbb{F}_q$ itself and hence it is not in the image of $\mathbb{F}_{q^2}^1$ under the norm map (only ± 1 in $\mathbb{F}_q$ have this property). Thus, if -1 has fourth root in $\mathbb{F}_{q^2}$ and the root is a norm 1 element, it happens if and only if $q \equiv 7 \pmod 8$. We get the counting using the lemma above. □

Proof of Theorem 5.1(2). Now, we explicitly count the number of conjugacy classes as well as elements that are fourth powers in $\mathrm{SL}_2(\mathbb{F}_q)$. We analyse each conjugacy class one by one. The element 1 is a fourth power of itself. However the fourth root of -1 need not exist in $\mathrm{SL}_2(\mathbb{F}_q)$ always, this happens if and only if $q \equiv \pm 1 \pmod 8$. Thus both of these classes are fourth power if and only if $q \equiv \pm 1 \pmod 8$. The split regular semisimple

classes are represented by elements $\mathfrak{h}(a)$ with $a \neq \pm 1$. Clearly $\mathfrak{h}(a)$ has a fourth root if and only if $X^4 - a = 0$ has a solution in $\mathbb{F}_q$. Hence the total number is $\frac{q-1}{2d} - 1$ if $q \equiv 1 \pmod 8$, else it is $\frac{q-1}{2d} - \frac{1}{2}$, where $d = (q-1, 4)$ which we tabulate below:

$q \pmod 8$	Total number
1	$\frac{q-9}{8}$
3	$\frac{q-3}{4}$
5	$\frac{q-5}{8}$
7	$\frac{q-3}{4}$

The non-semisimple classes are 4 conjugacy classes of this kind given by $\mathfrak{X}_{12}(1)$, $\mathfrak{h}(-1)\mathfrak{X}_{12}(-1)$, $\mathfrak{X}_{12}(\epsilon)$, $\mathfrak{h}(-1)\mathfrak{X}_{12}(-\epsilon)$, where ϵ is a fixed non-square in $\mathbb{F}_q$. The representatives of all these classes are of the form $\pm\mathfrak{X}_{12}(\psi)$ with $\psi \neq 0$. Out of these, only $\mathfrak{X}_{12}(1)$ and $\mathfrak{X}_{12}(\epsilon)$ are fourth power. The anisotropic regular semisimple conjugacy classes are $\mathfrak{n}(-1)\mathfrak{X}_{12}(\delta)$ such that $X^2 - \delta X + 1$ is irreducible over $\mathbb{F}_q$. Using Corollary 5.5, we get the total number of these classes which are fourth power as in the following table:

$q \pmod 8$	Total number
1	$\frac{q-1}{4}$
3	$\frac{q-3}{8}$
5	$\frac{q-1}{4}$
7	$\frac{q-7}{8}$

Thus, we get the total number of conjugacy classes which are fourth power and get the required result. Now we count the number of elements. We do this by counting case by case, as follows:

(1) When $q \equiv 1 \pmod 8$, the total number of elements which are fourth power is

$$\begin{aligned} &2 \cdot 1 + \frac{q-9}{8} \cdot q(q+1) + 2 \cdot \frac{q^2-1}{2} + \frac{q-1}{4} \cdot q(q-1) \\ &= \frac{3}{8}q^3 - \frac{1}{2}q^2 - \frac{7}{8}q + 1. \end{aligned}$$

(2) When $q \equiv 3 \pmod 8$, the total number of elements which are fourth power is

$$1 \cdot 1 + \frac{q-3}{4} \cdot q(q+1) + 2 \cdot \frac{q^2-1}{2} + \frac{q-3}{8} \cdot q(q-1) = \frac{3}{8}(q^3 - q).$$

(3) When $q \equiv 5 \pmod 8$, the total number of elements which are fourth power is

$$1 \cdot 1 + \frac{q-5}{8} \cdot q(q+1) + 2 \cdot \frac{q^2-1}{2} + \frac{q-1}{4} \cdot q(q-1) = \frac{3}{8}(q^3 - q).$$

(4) When $q \equiv 7 \pmod 8$, the total number of elements which are fourth power is

$$\begin{aligned} &2 \cdot 1 + \frac{q-3}{4} \cdot q(q+1) + 2 \cdot \frac{q^2-1}{2} + \frac{q-7}{8} \cdot q(q-1) \\ &= \frac{3}{8}q^3 - \frac{1}{2}q^2 + \frac{1}{8}q + 1. \end{aligned}$$

□

Proof of Theorem 5.1(3). The proof is similar to the earlier cases. Since n divides the order of group, n divides exactly one of $q-1, q, q+1$.

(1) When $n \mid q$, it also means $n \nmid (q-1)(q+1)$ and hence

$$c(n,q) = 2 + \frac{q-3}{2} + 0 + \frac{q-1}{2} = q$$

and

$$\begin{aligned} s(n,q) &= 2 \cdot 1 + \frac{q-3}{2} \cdot q(q+1) + 0 \cdot \frac{q^2-1}{2} + \frac{q-1}{2} \cdot q(q-1) \\ &= (q-2)(q^2-1). \end{aligned}$$

(2) When $n \mid (q-1)$, it also implies $n \nmid q(q+1)$ and hence

$$c(n,q) = 2 + \left(\frac{q-1}{2n} - 1\right) + 4 + \frac{q-1}{2} = \frac{(n+1)(q-1)}{2n} + 5$$

and

$$\begin{aligned} s(n,q) &= 2 \cdot 1 + \left(\frac{q-1}{2n} - 1\right) \cdot q(q+1) + 4 \cdot \frac{q^2-1}{2} \\ &\quad + \frac{q-1}{2} \cdot q(q-1) \\ &= \frac{(n+1)(q^3-q)}{2n}. \end{aligned}$$

(3) Similarly, when $n \mid (q+1)$ gives $n \nmid (q-1)q$,

$$c(n,q) = 2 + \frac{q-3}{2} + 4 + \left(\frac{q+1}{2n} - 1\right) = \frac{(n+1)(q-3)+4}{2n} + 5$$

and

$$\begin{aligned} s(n,q) &= 2 \cdot 1 + \frac{q-3}{2} \cdot q(q+1) + 4 \cdot \frac{q^2-1}{2} \\ &\quad + \left(\frac{q+1}{2n} - 1\right) \cdot q(q-1) \\ &= \frac{(n+1)(q^3-q)}{2n}. \end{aligned}$$

□

As a consequence to our counting above, we give an alternate proof to a well known Waring type result (see [5,10,11] for more general results) for the groups $\mathrm{SL}_2(\mathbb{F}_q)$.

COROLLARY 5.6

Let $n > 2$ be a prime and q odd. Then the word map $X_1^n X_2^n$ is surjective on $\mathrm{SL}_2(\mathbb{F}_q)$ except when $n = 3 = q$.

Proof. If n does not divide the order of the group, the word map X^n itself is surjective. Thus we need to look at the case when n divides the order of the group. If $n \nmid q$, then from Theorem 5.1, it is clear that the number of n-th powers is $\frac{n+1}{2n} > \frac{1}{2}$. Hence, the product of two such elements will cover the whole of the group.

Now, we are left with the case $n \mid q$. The proportion of elements which are n-th powers in $\mathrm{SL}_2(\mathbb{F}_q)$ is $\frac{q-2}{q}$ which is $> \frac{1}{2}$ if $q \geq 5$, and we are done. This leaves us with the case when $q = 3$ and $n = 3$. In this case, non-semisimple classes are not cubes nor product of cubes, as discussed in the following paragraph. Thus the proof concludes. □

We now discuss the exception case $n = 3 = q$ of the above theorem. In the group $\mathrm{SL}_2(\mathbb{F}_3)$, the word map $X_1^3 X_2^3$ is not surjective. The group $\mathrm{SL}_2(\mathbb{F}_3)$ has 7 conjugacy classes. Of these, 2 conjugacy classes are central, 4 are non-semisimple and 1 is anisotropic regular semisimple corresponding to the irreducible polynomial $X^2 + 1$ over $\mathbb{F}_3$. The non-semisimple conjugacy classes are not cube but the others are cubes. Hence the number of conjugacy classes which are cubes is 3 and the number of elements in $\mathrm{SL}_2(\mathbb{F}_3)$ which are cubes is $2.1 + 1.3(3 - 1) = 8$. These are the following elements:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix},$$
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}.$$

These 8 elements form a subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$, isomorphic to the quaternion group. Thus, we conclude that in $\mathrm{SL}_2(\mathbb{F}_3)$ product of cubes is again a cube. Therefore, non-cubes in this group, which are 16 in count, can never be products of any number of cubes. In particular, the word map $X_1^3 X_2^3 \ldots X_l^3$ on $\mathrm{SL}_2(\mathbb{F}_3)$ is not surjective for any $l \geq 1$.

6. Product of powers in groups of type A_1

As an application of our methods, we discuss products of powers in the forms of SL_2 over the base field k when $\mathrm{char}(k) \neq 2$. We recall that groups G of type A_1 are the following:

I. Split case. $G = \mathrm{SL}_2(k)$.
II. Anisotropic case. $G = \mathrm{SL}_1(Q)$, where Q is a quaternion division algebra over k.

When $k = \mathbb{F}_q$, the results are known for a larger class of groups (see [5,10,11]). The results for the anisotropic case, and for the split case with arbitrary k are new.

Theorem 6.1. *Let k be a field with $\mathrm{char}(k) \neq 2$. Let G be a group of type A_1 over k.*

(1) *If G is split, then the word map $X_1^n X_2^n$ is surjective on G if $n = 2$ or $n = 3$ and $\mathrm{char}(k) \neq 3$.*
(2) *If G is anisotropic and $2 \in (k^*)^2$, then the word map $X_1^2 X_2^2$ is surjective on G if and only if -1 is a square in G.*

(3) *If G is anisotropic and $n \geq 3$ is odd, then the word map $X_1^n X_2^n$ is surjective if -1 is a square in G.*

We prove this theorem in the rest of this section.

Proof of Theorem 6.1(1). We use the description of squares in $\mathrm{SL}_2(k)$ obtained in Lemma 5.2, along with the notation $\mathcal{S}_1$ and $\mathcal{S}_2$ therein. We first prove that all elements of $B\mathfrak{n}B$ are products of two squares. For this, we take $x_1^2 \in \mathcal{S}_1$ and $x_2^2 \in B\mathfrak{n}B$. The product is $x_1^2x_2^2 = \mathfrak{h}(a_1^2)\mathfrak{X}_{12}(t_1) \cdot \mathfrak{X}_{12}(t_2)\mathfrak{n}(a_2)\ \mathfrak{X}_{12}(-t_2 + a_2(s_2^2 - 2)) = \mathfrak{X}_{12}(a_1^4(t_1 + t_2))\mathfrak{n}(a_1^2a_2)$ $\mathfrak{X}_{12}(-t_2 + a_2(s_2^2 - 2))$. By taking $a_1 = 1$, we see that we get all the elements of $B\mathfrak{n}B$. Now, to get all the elements of B, we take products from $\mathcal{S}_2$ as follows: $x_1^2x_2^2 = \mathfrak{X}_{12}(t_1)\mathfrak{n}(a_1)\mathfrak{X}_{12}(-t_1 + a_1(s_1^2 - 2)) \cdot \mathfrak{X}_{12}(t_1 - a_1(s_1^2 - 2))\mathfrak{n}(a_2)\mathfrak{X}_{12}(-t_1 + a_1(s_1^2 - 2) + a_2(s_2^2 - 2)) = \mathfrak{h}(-a_1a_2^{-1})\ \mathfrak{X}_{12}(-t_1 + a_1(s_1^2 - 2) + a_2(s_2^2 - 2) + a_1^{-2}a_2^2t_1)$. This covers all the elements of B except when $a_1 = \pm 1$. Thus the elements which are left out so far are $\pm\mathfrak{X}_{12}(t)$. These are obtained by multiplying elements of $\mathcal{S}_1$ together with -1 from $\mathcal{S}_2$. This completes the case of the product of two squares.

For the case of product of two cubes, we note that the elements of the form $\pm\mathfrak{X}_{12}(\psi)$ are always cube. Other elements $\mathfrak{h}(a)\mathfrak{X}_{12}(s)$ of B are cubes if $a \in (k^*)^3$. More importantly, $\mathfrak{X}_{12}(\tau)\mathfrak{n}(\alpha)\mathfrak{X}_{12}(\psi)$ with $\tau + \psi = 2\alpha$ are certainly cubes. Let us consider product of cubes of the form $\mathfrak{X}_{12}(\tau)\mathfrak{n}(\alpha)\mathfrak{X}_{12}(2\alpha - \tau)$ which are in $B\mathfrak{n}B$. Take the product when the last term of x_1^3 is the same as the inverse of the first term of x_2^3. We get as follows:

$$\begin{aligned} x_1^3x_2^3 &= \mathfrak{X}_{12}(\tau_1)\mathfrak{n}(\alpha_1)\mathfrak{X}_{12}(2\alpha_1 - \tau_1) \\ &\quad \cdot\mathfrak{X}_{12}(-2\alpha_1 + \tau_1)\mathfrak{n}(\alpha_2)\mathfrak{X}_{12}(2\alpha_2 + 2\alpha_1 - \tau_1) \\ &= \mathfrak{X}_{12}(\tau_1)\mathfrak{h}\left(-\frac{\alpha_1}{\alpha_2}\right)\mathfrak{X}_{12}(2\alpha_2 + 2\alpha_1 - \tau_1) \\ &= \mathfrak{h}\left(-\frac{\alpha_1}{\alpha_2}\right)\mathfrak{X}_{12}\left(\left(\frac{\alpha_2^2}{\alpha_1^2} - 1\right)\tau_1 + 2(\alpha_1 + \alpha_2)\right). \end{aligned}$$

Combined with the fact that $\pm\mathfrak{X}_{12}(\psi)$ are already a cube, all elements of B are a product of two cubes. Now, let us compute the product when $x_1^3 = \mathfrak{X}_{12}(\psi)$ and x_2^3 is in $B\mathfrak{n}B$ of the above kind. We get

$$\begin{aligned} x_1^3x_2^3 &= \mathfrak{X}_{12}(\tau_1).\mathfrak{X}_{12}(\tau_2)\mathfrak{n}(\alpha_2)\mathfrak{X}_{12}(2\alpha_2 - \tau_2) \\ &= \mathfrak{X}_{12}(\tau_1 + \tau_2)\mathfrak{n}(\alpha_2)\mathfrak{X}_{12}(2\alpha_2 - \tau_2). \end{aligned}$$

This shows that all elements of $B\mathfrak{n}B$ are also a product of two cubes. This completes the proof of 6.1(1). □

To prove Theorems 6.1(2) and 6.1(3), we set up some lemmas. Let k be a field of characteristic $\neq 2$ and $Q = \left(\frac{a,\lambda}{k}\right)$ be a quaternion division algebra over k. We recall that every element ψ of Q satisfies the quadratic equation $\psi^2 - Tr(\psi)\psi + N(\psi) = 0$.

Lemma 6.2. *Let $(\alpha, \beta) \in \mathrm{SL}_1(Q)$ with $\beta \neq 0$. Thus $X^2 = (\alpha, \beta)$ has a solution in $\mathrm{SL}_1(Q)$ if and only if $\mathrm{Tr}(\alpha) + 2 \in (k^*)^2$.*

Proof. Let us first assume $\mathrm{Tr}(\alpha)+2 \in (k^*)^2$. Let $(x, y) \in Q$ be a solution of $X^2 = (\alpha, \beta)$. Then, $(x, y)^2 = \mathrm{Tr}(x)(x, y) - 1$ gives the equations $\mathrm{Tr}(x)x - 1 = \alpha$ and $\mathrm{Tr}(x)y = \beta$. For simplicity of further calculation, let us write $x = l + m\zeta$ and $\alpha = \alpha_1 + \alpha_2\zeta$ where $\alpha_1, \alpha_2, l, m \in k$. In case $\mathrm{Tr}(\alpha) = 2\alpha_1 \neq -2$, i.e., $\alpha_1 \neq -1$, the equation $2l^2 - 1 = \alpha_1$ give $l \neq 0$ and $y = \frac{\beta}{2l}$. Hence $l^2 = \frac{\mathrm{Tr}(\alpha)+2}{4}$ and $x = \frac{\alpha+1}{2l}$ gives the solution. In the case $\alpha_1 = -1$, we get $l = 0$, i.e., $\mathrm{Tr}(x) = 0$. Thus $\alpha = -1$ and $\beta = 0$ which is not the case.

Now, suppose $X^2 = (\alpha, \beta)$ has a solution, say (x, y). Then, the equation $\mathrm{Tr}(x)x = \alpha+1$, after taking trace, gives that $\mathrm{Tr}(x)^2 = \mathrm{Tr}(\alpha) + 2$. Clearly $\mathrm{Tr}(x) \neq 0$ else $\beta = 0$. □

Lemma 6.3. *Let $\phi = (\alpha, \beta) \in \mathrm{SL}_1(Q)$ with $\mathrm{Tr} + (\alpha) = 0$ and $\beta \neq 0$. Then, for any n odd, the equation $X^n = \phi$ has a solution in $\mathrm{SL}_1(Q)$.*

Proof. We have $\phi^2 = -1$. Hence, $\phi^n = \phi$ if $n \equiv 1 \pmod 4$ and $\phi^n = -\phi$ when $n \equiv 3 \pmod 4$. Hence, all such $\phi \in Q$ have n-th root which is either ϕ or $-\phi$. □

Proofs of Theorems 6.1(2) and 6.1(3). Let us prove Theorem 6.1(2) first. Let -1 be a square in $\mathrm{SL}_1(Q)$. Consider the set $\mathcal{H} = \{(\alpha, \beta) \mid N(\alpha, \beta) = 1, \mathrm{Tr}(\alpha) = 0\}$. The set $\mathcal{H}$ consists of a square-root of -1 in $\mathrm{SL}_1(Q)$ and is non-empty. Further, it is contained in squares (Lemma 6.2). We consider (α_1, β_1) and (α_2, β_2) in $\mathcal{H}$ and

$$(\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1\alpha_2 + \lambda\beta_1\bar{\beta}_2, \alpha_1\beta_2 + \bar{\alpha}_2\beta_1).$$

Thus, when $\alpha_1\beta_2 + \bar{\alpha}_2\beta_1 \neq 0$, say γ, then the product becomes $(\frac{\gamma\alpha_2-\beta_1}{\beta_2}, \gamma)$. This covers all elements $(x, y) \in \mathrm{SL}_1(Q)$ with $y \neq 0$. Now we need to produce elements of the kind $(x, 0)$ as a product of two squares. We note that when $\alpha_1\beta_2+\bar{\alpha}_2\beta_1 = 0$, $(\alpha_1, \beta_1)(\alpha_2, \beta_2) = \left(-\frac{\bar{\beta}_2}{\bar{\beta}_1}, 0\right) = \left(-\frac{\alpha_2}{\bar{\alpha}_1}, 0\right)$. Thus it reduces to prove that every element of K is a product of two elements from the set $S = \{\alpha \in K \mid \mathrm{Tr}(\alpha) + 2 \in (k^*)^2\}$ which is easy to verify.

Now to prove the converse, we begin with $-1 = (\alpha_1, \beta_1)(\alpha_2, \beta_2)$, where $(\alpha_1, \beta_1) = (x_1, y_1)^2 = (x_1^2 + \lambda N(y_1), \mathrm{Tr}(x_1)y_1)$ and $(\alpha_2, \beta_2) = (x_2, y_2)^2$. We may assume that $\mathrm{Tr}(x_1)$ and $\mathrm{Tr}(x_2)$ are both not 0 else we get -1 as a square. If $y_1 = 0$, then $-1 = x_1^2(x_2^2 + \lambda N(y_2), \mathrm{Tr}(x_2)y_2)$ hence $\mathrm{Tr}(x_2)y_2 = 0$. If $y_2 = 0$, we get $-1 = x_1^2x_2^2$ and if $\mathrm{Tr}(x_2) = 0$ we would have $(x_2, y_2)^2 = -1$. Similarly we can prove this when $y_2 = 0$, thus we may assume β_1 and β_2 both are non-zero. Now we use $\mathrm{SL}_2(K)$ notation and we have

$$-1 = \mathfrak{X}_{12}\left(\frac{\alpha_1}{\bar{\beta}_1}\right)\mathfrak{n}\left(\frac{-1}{\bar{\beta}_1}\right)\mathfrak{X}_{12}\left(\frac{\bar{\alpha}_1}{\bar{\beta}_1}\right)\mathfrak{X}_{12}\left(\frac{\alpha_2}{\bar{\beta}_2}\right)\mathfrak{n}\left(\frac{-1}{\bar{\beta}_2}\right)\mathfrak{X}_{12}\left(\frac{\bar{\alpha}_2}{\bar{\beta}_2}\right)$$

in $\mathrm{SL}_2(K)$. From Proposition 2.2(3), we must have $\frac{\bar{\alpha}_1}{\bar{\beta}_1} = -\frac{\alpha_2}{\bar{\beta}_2}$. Write $\frac{\bar{\alpha}_1}{\alpha_2} = -\frac{\bar{\beta}_1}{\bar{\beta}_2} = \theta$ and get $(\alpha_1, \beta_1) = \bar{\theta}(\alpha_2, -\beta_2)$. This gives $\theta = -1$ and thus the equation becomes $-1 = (-\bar{\alpha}_2, \beta_2)(\alpha_2, \beta_2)$. Write $\alpha_2 = r + \zeta s$, and we get $\mathrm{Tr}(-\bar{\alpha}_2) + 2 = -2r + 2 \in (k^*)^2$ and $\mathrm{Tr}(\alpha_2) + 2 = 2r + 2 \in (k^*)^2$. Thus $1 - r^2 \in (k^*)^2$. Now $1 = N(\alpha_2, \beta_2) = r^2 - as^2 - \lambda N(\beta_2)$ implies that the quadratic form $\langle 1, a, \lambda, -a\lambda\rangle$ is isotropic which is equivalent to -1 being a square (see [7], Chapter III, Exercise 5). In fact, it gives $\left(\frac{s\zeta}{r'}, \frac{\beta_2}{r'}\right)$, where $1 - r^2 = r'^2$, of which square is -1.

For the proof of Theorem 6.1(3), we consider the set $\mathcal{H} = \{(\alpha, \beta) \in \mathrm{SL}_1(Q) \mid \mathrm{Tr}(\alpha) = 0, \beta \neq 0\}$ contained in n-th powers. For the set $\mathcal{H}$ to be non-empty, we require -1 to be a square. The rest of the proof is similar to as above. □

We end this section with some examples.

Example 6.4. Let $k = \mathbb{Q}$ and $g = \begin{pmatrix} & 1 \\ -1 & -a \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Q})$, where $a \neq 0$. Clearly, $g = \mathfrak{n}\mathfrak{X}_{12}(a)$. From Lemma 5.2, it follows that $x^2 = g$ has a solution in $\mathrm{SL}_2(k)$ if and only if $8 - 2a^2 \in \mathbb{Q}^2$. Thus, if $a \geq 5$, then g does not have a square root in $\mathrm{SL}_2(\mathbb{Q})$. Similarly, we can produce elements which are not n-th power in $\mathrm{SL}_2(\mathbb{F}_q)$ using the discussion preceding Lemma 5.3.

Example 6.5. Consider $k = \mathbb{R}$ and $Q = \mathbb{H}$, the Hamilton's quaternion. Consider an element $(\alpha, \beta) \in \mathrm{SL}_1(\mathbb{H})$ with $\beta \neq 0$. Any such element with $\mathrm{Tr}(\alpha) \leq -3$ is not a square, using Lemma 6.2.

Acknowledgements

The authors would like to thank B. Sury, Indian Statistical Institute, Bangalore for his encouragement during this work. They would also like to thank the referees for helpful comments which improved the readability of this article. This work was supported by DST, India through Indo-Russian research Grant INT/RUS/RFBR/P-288. The first-named author also acknowledges SERB Grant EMR/2016/001516 for supporting this work.

References

[1] Amdeberhan T, Chen Xi, Moll V H and Sagan B E, Generalized Fibonacci polynomials and Fibonomial coefficients, *Ann. Comb*. **18(4)** (2014) 541–562
[2] Blum J, Enumeration of the square permutations in S_n, *J. Combinatorial Theory Ser. A* **17** (1974) 156–161
[3] Carter R W, Simple groups of Lie type, Pure and Applied Mathematics (1972) (London–New York–Sydney: John Wiley & Sons) vol. 28
[4] Guralnick R, Liebeck M, Eamon O'Brien, Shalev A and Tiep P-H, Surjective word maps and Burnsides $p^a q^b$ theorem, *Invent. Math*. **213(2)** (2018) 589–695
[5] Guralnick R and Malle G, Products of conjugacy classes and fixed point spaces, *J. Amer. Math. Soc*. **25(1)** (2012) 77–121
[6] Hoggatt V E Jr, and Long C T, Divisibility properties of generalized Fibonacci polynomials, *Fibonacci Quart*. **12** (1974) 113–120
[7] Lam T Y, Introduction to quadratic forms over fields, Graduate Studies in Mathematics 67, American Mathematical Society, Providence, RI (2005) xxii+550 pp.
[8] Larsen M, Shalev A and Tiep P-H, The Waring problem for finite simple groups, *Ann. Math. (2)* **174(3)** (2011) 1885–1950
[9] Larsen M and Shalev A and Tiep P-H, Waring problem for finite quasisimple groups, *Int. Math. Res. Not. IMRN* **2013(10)** 2323–2348
[10] Liebeck M W, O'Brien E A, Shalev A and Tiep P-H, Products of squares in finite simple groups, *Proc. Amer. Math. Soc*. **140(1)** (2012) 21–33
[11] Lubotzky A, Images of word maps in finite simple groups, *Glasg. Math. J*. **56(2)** (2014) 465–469
[12] McLaughlin J and Sury B, Powers of a matrix and combinatorial identities, *Integers* **5(1)** (2005) A13, 9 pp.
[13] Pouyanne N, On the number of permutations admitting an m-th root, *Electron. J. Combin*. **9(1)** (2002) Research Paper 3, 12 pp.

[14] Springer T A and Veldkamp F D, Octonions, Jordan algebras and exceptional groups, Springer Monographs in Mathematics (2000) (Berlin: Springer-Verlag) viii+208 pp.

COMMUNICATING EDITOR: B Sury