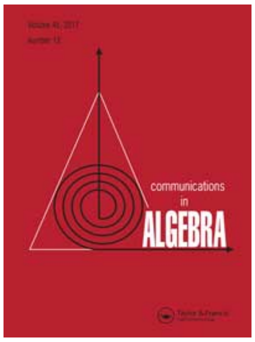

Communications in Algebra

ISSN: 0092-7872 (Print) 1532-4125 (Online) Journal homepage: http://www.tandfonline.com/loi/lagb20

Isomorphy classes of finite order automorphisms of $SL(2,k)$

Robert W. Benim, Mark Hunnell & Amanda K. Sutherland

COMMUNICATIONS IN ALGEBRA®
2017, VOL. 45, NO. 12, 5145–5157
http://dx.doi.org/10.1080/00927872.2017.1298770

Isomorphy classes of finite order automorphisms of SL$(2, k)$

Robert W. Benim[a], Mark Hunnell[b], and Amanda K. Sutherland[c]

[a]Department of Mathematics, University of Georgia, Athens, Georgia, USA; [b]Department of Mathematics, Winston-Salem State University, Winston-Salem, North Carolina, USA; [c]Department of Mathematical Sciences, Shenandoah University, Winchester, Virginia, USA

ABSTRACT

In this paper, we consider the order m k-automorphisms of SL$(2, k)$. We first characterize the forms that order m k-automorphisms of SL$(2, k)$ take and then we find simple conditions on matrices A and B, involving eigenvalues and the field that the entries of A and B lie in, that are equivalent to isomorphy between the order m k-automorphisms Inn_A and Inn_B. We examine the number of isomorphy classes and conclude with examples for selected fields.

ARTICLE HISTORY
Received 3 June 2015
Revised 10 February 2017
Communicated by K. Misra

KEYWORDS
Automorphism; special linear group; symmetric k-varieties

2010 MATHEMATICS SUBJECT CLASSIFICATION
20G15; 14M27; 20E36

1. Introduction

Let k be a field of characteristic not two, and let G be a connected reductive algebraic group defined over k. We denote the k-rational points of G as G_k. A k-involution of G is a k-automorphism of G which is of order 2. Let θ be a k-involution of G, and let H be a k-open subgroup of the fixed-point group of θ. We similarly denote the k-rational points of H as H_k. The variety G_k/H_k is called a symmetric k-variety. To understand symmetric k-varieties, we need to first understand the corresponding k-involutions. The isomorphism classes of these k-involutions were first considered in [5].

There has been much more work done regarding k-involutions. In [6], a full characterization of the isomorphism classes of k-involutions was given in the case that $G = \mathrm{SL}(2, k)$ which does not depend on any of the results in [5]. Similarly, this is done for $\mathrm{SL}(n, k)$ in [7]. Using this characterization, the possible isomorphism classes of involutions for algebraically closed fields, the real numbers, the p-adic numbers, and the finite fields were classified. Analogous results for isomorphism classes of involutions of connected reductive algebraic groups can be found in [9], [8], [10], and [11] for the exceptional groups, in [14] for $\mathrm{SL}(n, k)$ where k is of characteristic 2, in [2] for symplectic groups, and in [1] for orthogonal groups.

These concepts can be generalized by considering order m k-automorphisms of G instead of k-involutions. This problem has been considered previously. In [16], isomorphy classes of inner k-automorphisms of complex Lie groups are considered. This is done by considering the eigenvalues of the matrix A for some inner k-automorphism Inn_A. Taken together, the eigenvalues of the matrix A are sometimes referred to as the Kac coordinates. This is similar to the approach that will be taken in this paper, but we will consider the group $\mathrm{SL}(2, k)$ for all fields k of characteristic not 2. In [12], and its updated version on the arXiv, inner k-automorphisms were again considered, but a much different approach was used. Here, inner k-automorphisms are constructed using the Weyl group. That is, inner k-automorphisms are of the form Inn_{n_w} where $n_w \in N_{G_k}(T)$ and $w = n_wT \in W$ is an element of order m. Here, T is a torus of the group $\mathrm{SL}(2, k)$ which is maximally stable under the involution and whose Lie algebra contains a Cartan subspace, W is the associated Weyl group, and $N_{G_k}(T)$ is the normalizer of T over $\mathrm{SL}(2, k)$. This is similar to the approaches taken in [15], [4], and [5] when considering k-involutions.

CONTACT Robert W. Benim robert.benim@uga.edu Department of Mathematics, University of Georgia, Athens, GA 30602, USA.

In this paper, we consider the order m k-automorphisms of $\mathrm{SL}(2,k)$ and characterize the isomorphy classes of these automorphisms. We take an approach similar to that of [6], [7], [8], [2], and [1]. Throughout this paper, we assume $m \geq 2$ and $\mathrm{char}(k) \neq 2$. Since we include the case where $m = 2$, we will verify the main results of [6]. In Section 2, we define some of the basic terminology that will be used and state previous results on k-involutions of $\mathrm{SL}(2,k)$. In Section 3, we characterize the form that k-automorphisms of $\mathrm{SL}(2,k)$ take. In Section 4, we find simple conditions on matrices A and B, involving eigenvalues and the field that the entries of A and B lie in, that are equivalent to isomorphy between k-automorphisms Inn_A and Inn_B. In Section 5, we examine the occurrence of m-valid eigenpairs, which indicate an order m k-automorphism. In Section 6, we consider the number of isomorphy classes for a given field k and order m. We conclude in Section 7 by examining the cases when $k = \bar{k}$, $\mathbb{R}$, $\mathbb{Q}$, or $\mathbb{F}_p$.

2. Preliminaries

We begin by defining some basic notation. Let k be a field of characteristic not two and $\bar{k}$ be the algebraic closure of k. Let k^* denote the multiplicative group of nonzero elements of k and $(k^*)^2 = \{a^2 \mid a \in k^*\}$ denote the set of squares in k. We also define the following:

$$\mathrm{GL}(2,k) = \{A \in k^{2\times 2} \mid \det(A) \neq 0\},$$
$$\mathrm{PGL}(2,k) = \mathrm{GL}(2,k)/\{\alpha I \mid \alpha \in k^*\},$$

and

$$\mathrm{SL}(2,k) = \{A \in \mathrm{GL}(2,k) \mid \det(A) = 1\}$$

where $I \in \mathrm{GL}(2,k)$ denotes the identity matrix.

Let G be an algebraic group defined over a field k. Let G_k be the k-rational points of G. We make use of this notation in the following definitions.

Definition 2.1. Let $\mathrm{Aut}(G, G_k)$ denote the the set of k-automorphisms of G_k. That is, $\mathrm{Aut}(G, G_k)$ is the set of automorphisms of G which leave G_k invariant. We say $\theta \in \mathrm{Aut}(G, G_k)$ is a *k-involution* if $\theta^2 = \mathrm{id}$ but $\theta \neq \mathrm{id}$. Thus, a k-involution is a k-automorphism of order 2.

Definition 2.2. For $A \in G_k$, the map $\mathrm{Inn}_A(X) = A^{-1}XA$ is called an *inner k-automorphism of G_k*. We denote the set of such k-automorphisms by $\mathrm{Inn}(G_k)$. If $\mathrm{Inn}_A \in \mathrm{Inn}(G_k)$ is a k-involution, then we say that Inn_A is an *inner k-involution of G_k*.

Definition 2.3. Assume L is an algebraic group defined over k which contains G. Let L_k be the k-rational points of L. For $A \in L$, if the map $\mathrm{Inn}_A(X) = A^{-1}XA$ is such that $\mathrm{Inn}_A \in \mathrm{Aut}(G, G_k)$, then Inn_A is an *inner k-automorphism of G_k over L*. We denote the set of such k-automorphisms by $\mathrm{Inn}(L, G_k)$. If $\mathrm{Inn}_A \in \mathrm{Inn}(L, G_k)$ is a k-involution, then we say that Inn_A is an *inner k-involution of G_k over L*.

Definition 2.4. Suppose $\theta, \tau \in \mathrm{Aut}(G, G_K)$. Then θ is *isomorphic* to τ *over L_k* if there is ϕ in $\mathrm{Inn}(L_k)$ such that $\tau = \phi^{-1}\theta\phi$. Equivalently, we say that τ and θ are in the same *isomorphy class over L_k*.

For simplicity, we will refer to k-automorphisms simply as automorphisms for the remainder of this paper.

Definition 2.5. For a field k, we will refer to $k^*/(k^*)^2$ as the *square classes* of k.

For example, if $k = \bar{k}$, then $|k^*/(k^*)^2| = 1$ where 1 is a representative of this single square class. Further, $|\mathbb{R}^*/(\mathbb{R}^*)^2| = 2$ with representatives ± 1; the set $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is infinite with representatives ± 1

and all the prime numbers. For finite fields $k = \mathbb{F}_q$ where $q = p^r$ for prime $p \neq 2$, it is always the case that $|\mathbb{F}_q^*/(\mathbb{F}_q^*)^2| = 2$. In particular, the representatives are ± 1 if and only if $p \equiv 1 \mod 4$.

The following is the main result of [6].

Theorem 2.6. *Let k be a field of characteristic not two. Then $\mathrm{SL}(2,k)$ has exactly $|k^*/(k^*)^2|$ isomorphy classes of involutions.*

We will confirm this result in this paper, and see that the number of isomorphy classes of order m automorphisms where $m > 2$ does not depend on $|k^*/(k^*)^2|$.

3. Inner Automorphisms of SL(2, *k*)

Since the Dynkin diagram of $\mathrm{SL}(2,k)$ has a trivial automorphism group, it follows from a proposition on page 190 of [3] that all automorphisms of $\mathrm{SL}(2,k)$ are of the form Inn_B for some $B \in \mathrm{GL}(2,\overline{k})$. We improve upon this and Lemma 4 in [6] in the following lemma.

Lemma 3.1. *If ϕ is an automorphism of $\mathrm{SL}(2,k)$, then $\phi = \mathrm{Inn}_A$ for some $A \in \mathrm{SL}(2,k[\sqrt{\alpha}])$ where $\alpha \in k$ and each entry of A is a k-multiple of $\sqrt{\alpha}$.*

Proof. Let ϕ be an automorphism of $\mathrm{SL}(2,k)$. We can write $\phi = \mathrm{Inn}_B$ for some $B \in \mathrm{GL}(2,\overline{k})$. It follows from Lemma 4 of [6] that we can assume that $B \in \mathrm{GL}(2,k)$. Let $A = (\det(B))^{-\frac{1}{2}}B$ and $\alpha = \det(B)$. Note that $\alpha \in k$. By construction, we see that $\det(A) = 1$ and that the entries of A are k-multiples of $\sqrt{\alpha}$. $\square$

We now consider a lemma which characterizes matrices in $\mathrm{SL}(2,\overline{k})$.

Lemma 3.2. *Suppose $A \in \mathrm{SL}(2,\overline{k})$. Let $m_A(x)$ be the minimal polynomial of A and λ_1 and λ_2 be the eigenvalues of A where $\lambda_2 = \lambda_1^{-1}$. Then A is of the form*

$$A = \begin{pmatrix} a & b \\ -\frac{m_A(a)}{b} & -a+\lambda_1+\lambda_2 \end{pmatrix}$$

where $a, b \in \overline{k}$, $b \neq 0$, and $m_A(a) = a^2 - a(\lambda_1+\lambda_2)+1$, or A is of the form

$$A = \begin{pmatrix} \lambda_1 & 0 \\ c & \lambda_2 \end{pmatrix}$$

where $c \in \overline{k}$.

Proof. If A is diagonal, then A is in the latter form where $c = 0$. So, we proceed by assuming that A is not diagonal and write $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. We first assume that b is nonzero. We need only show that $c = -\frac{m_A(a)}{b}$ and $d = -a+\lambda_1+\lambda_2$. The latter is clear since the the trace of A is $a+d = \lambda_1+\lambda_2$. So we are only concerned with c.

Note that $m_A(x) = x^2 - \mathrm{trace}(A)x + \det(A) = x^2 - (\lambda_1+\lambda_2)x + 1$ since A is a 2×2 matrix. Now, to find the value of c, recall that $ad - bc = 1$. Thus,

$$1 = a(-a+\lambda_1+\lambda_2) - bc,$$

which implies that

$$bc = -a^2 + (\lambda_1+\lambda_2)a - 1.$$

Since b is nonzero, we have that $c = -\frac{m_A(a)}{b}$.

We now suppose $b = 0$, then A is lower triangular and its diagonal entries must be its eigenvalues. Thus, $A = \begin{pmatrix} \lambda_1 & 0 \\ c & \lambda_2 \end{pmatrix}$. □

We can summarize the previous two lemmas into a characterization of the matrices $A \in \mathrm{SL}(2, k[\sqrt{\alpha}])$ that define automorphisms of $\mathrm{SL}(2, k)$.

Theorem 3.3. *Suppose* Inn_A *is an automorphism of* $\mathrm{SL}(2, k)$ *where* $A \in \mathrm{SL}(2, k[\sqrt{\alpha}])$, $\alpha \in k$, *and each entry of A is a k-multiple of* $\sqrt{\alpha}$. *Then A is of the form*

$$A = \begin{pmatrix} a & b \\ -\frac{m_A(a)}{b} & -a + \lambda_1 + \lambda_2 \end{pmatrix}$$

where $a, b \in \bar{k}$, $b \neq 0$, *and* $m_A(a) = a^2 - a(\lambda_1 + \lambda_2) + 1$, *or*

$$A = \begin{pmatrix} \lambda_1 & 0 \\ c & \lambda_2 \end{pmatrix}$$

where $c \in \bar{k}$.

Alternatively, we could have characterized the automorphisms of $\mathrm{SL}(2, k)$ as Inn_A for some $A \in \mathrm{GL}(2, k)$. But, we will find it useful in the later sections to know that $\lambda_1\lambda_2 = 1$.

4. Isomorphy conditions of automorphisms

In this section, we find conditions on the matrices A and B that determine whether or not Inn_A and Inn_B are isomorphic over $\mathrm{GL}(2, k)$. We begin with a lemma that translates the isomorphy conditions from one about mappings to one about matrices.

Lemma 4.1. *Assume* Inn_A *and* Inn_B *are automorphisms of* $\mathrm{SL}(2, k)$. *Further, suppose A lies in* $\mathrm{SL}(2, k[\sqrt{\alpha}])$ *where each entry of A is a k-multiple of* $\sqrt{\alpha}$, *B lies in* $\mathrm{SL}(2, k[\sqrt{\gamma}])$ *where each entry of B is a k-multiple of* $\sqrt{\gamma}$, *and where* $\alpha, \gamma \in k$. *Then* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{GL}(2, k)$ *if and only if there exists* $Q \in \mathrm{GL}(2, k)$ *such that* $Q^{-1}AQ = B$ *or* $-B$.

Proof. First assume there exists $Q \in \mathrm{GL}(2, k)$ such that $Q^{-1}AQ = B$ or $-B$. Then for all $U \in \mathrm{SL}(2, k)$, we have

$$\begin{aligned} \mathrm{Inn}_Q\mathrm{Inn}_A\mathrm{Inn}_{Q^{-1}}(U) &= Q^{-1}A^{-1}QUQ^{-1}AQ \\ &= (Q^{-1}AQ)^{-1}U(Q^{-1}AQ) \\ &= (\pm B)^{-1}U(\pm B) \\ &= B^{-1}UB \\ &= \mathrm{Inn}_B(U). \end{aligned}$$

So, $\mathrm{Inn}_Q\mathrm{Inn}_A\mathrm{Inn}_{Q^{-1}} = \mathrm{Inn}_B$ and Inn_A and Inn_B are isomorphic over $\mathrm{GL}(2, k)$.

To prove the converse, we now assume that Inn_A and Inn_B are isomorphic over $\mathrm{GL}(2, k)$. Then there exists $Q \in \mathrm{GL}(2, k)$ such that $\mathrm{Inn}_Q\mathrm{Inn}_A\mathrm{Inn}_{Q^{-1}} = \mathrm{Inn}_B$. We note that Inn_A and Inn_B are also automorphisms of $\mathrm{SL}(2, \bar{k})$. For all $U \in \mathrm{SL}(2, \bar{k})$, we have

$$Q^{-1}A^{-1}QUQ^{-1}AQ = B^{-1}UB,$$

which implies

$$BQ^{-1}A^{-1}QUQ^{-1}AQB^{-1} = U.$$

So, $Q^{-1}AQB^{-1}$ commutes with all elements of $\mathrm{SL}(2,\bar{k})$. We note that $Q^{-1}AQB^{-1} \in \mathrm{SL}(2,\bar{k})$, so $Q^{-1}AQB^{-1}$ must lie in the center of $\mathrm{SL}(2,\bar{k})$, which is $\{I,-I\}$. Thus $Q^{-1}AQ = B$ or $-B$. □

An alternative approach would have been to consider the inner automorphisms Inn_A where A is a representative of an element of $\mathrm{PGL}(2,k)$. This approach would have simplified the previous lemma since $-B$ would not have to be considered but would make most of the work in this paper more tedious since it would require frequent transitioning between $\mathrm{SL}(2,k)$ and $\mathrm{PGL}(2,k)$.

Note that Inn_A and Inn_B will be isomorphic only if A and B have entries in the same quadratic extension of k.

Lemma 4.2. *Assume* Inn_A *and* Inn_B *are automorphisms of* $\mathrm{SL}(2,k)$*,* A *lies in* $\mathrm{SL}(2,k[\sqrt{\alpha}])$ *where each entry of* A *is a* k*-multiple of* $\sqrt{\alpha}$*,* B *lies in* $\mathrm{SL}(2,k[\sqrt{\gamma}])$ *where each entry of* B *is a* k*-multiple of* $\sqrt{\gamma}$*, and* $\alpha,\gamma \in k$*. If* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{GL}(2,k)$*, then* $\gamma = c\alpha$*. That is,* α *and* γ *lie in the same square class of* k*, and all of the entries of* B *are* k*-multiples of* $\sqrt{\alpha}$*.*

Proof. By Lemma 4.1, there exists $Q \in \mathrm{GL}(2,k)$ such that $Q^{-1}AQ = B$ or $-B$ and the result follows. □

Using the previous theorem and lemmas, we can now characterize isomorphy classes of automorphisms of $\mathrm{SL}(2,k)$.

Theorem 4.3. *Suppose* Inn_A *and* Inn_B *are automorphisms of* $\mathrm{SL}(2,k)$ *where* $A, B \in \mathrm{SL}(2,k[\sqrt{\alpha}])$ *for some* $\alpha \in k$ *and where each entry of* A *and* B *is a* k*-multiple of* $\sqrt{\alpha}$*.*

(a) *If* A *and* B *have the same eigenvalues,* λ_1 *and* λ_2*, then* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{GL}(2,k)$*.*
(b) *If* A *has eigenvalues* λ_1 *and* λ_2 *and* B *has eigenvalues* $-\lambda_1$ *and* $-\lambda_2$*, then* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{GL}(2,k)$*.*
(c) *If* Inn_A *is isomorphic to* Inn_B *over* $\mathrm{GL}(2,k)$*, then* A *has the same eigenvalues as* B *or* $-B$*.*

Proof.
(a) We consider three cases based on if λ_1 and λ_2 are k-multiples of $\sqrt{\alpha}$.

Case 1: Suppose λ_1 and λ_2 are not k-multiples of $\sqrt{\alpha}$. Then both A and B must not be lower triangular. We can assume

$$A = \begin{pmatrix} a & b \\ -\frac{m_A(a)}{b} & -a+\lambda_1+\lambda_2 \end{pmatrix}$$

and

$$B = \begin{pmatrix} c & d \\ -\frac{m_A(c)}{d} & -c+\lambda_1+\lambda_2 \end{pmatrix}.$$

Then for

$$Q_A = \begin{pmatrix} b & b \\ \lambda_1 - a & \lambda_2 - a \end{pmatrix} \in \mathrm{GL}(2,\bar{k}),$$

we have

$$Q_A^{-1}AQ_A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

Likewise, if we let

$$Q_B = \begin{pmatrix} d & d \\ \lambda_1 - c & \lambda_2 - c \end{pmatrix} \in \mathrm{GL}(2,\bar{k}),$$

it follows that

$$Q_B^{-1}BQ_B = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

Let

$$Q = Q_AQ_B^{-1} = \begin{pmatrix} \frac{b}{d} & 0 \\ \frac{c-a}{d} & 1 \end{pmatrix}.$$

Then $Q^{-1}AQ = B$ and $Q \in \mathrm{GL}(2,k)$. Using the result of Lemma 4.1, we have shown that Inn_A and Inn_B are isomorphic over $\mathrm{GL}(2,k)$.

Case 2: Now suppose λ_1 and λ_2 are k-multiples of $\sqrt{\alpha}$ and define $D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$. In this case, it is possible but not necessary that A and B are lower triangular. If neither are lower triangular, then the argument from Case 1 shows that Inn_A and Inn_B are isomorphic over $\mathrm{GL}(2,k)$, as desired.

Subcase 2.1: Assume that A and B are lower triangular. We write

$$A = \begin{pmatrix} \lambda_1 & 0 \\ c & \lambda_2 \end{pmatrix}.$$

From Lemma 3.1, we know that λ_1, λ_2, and c are k-multiples of $\sqrt{\alpha}$. Let

$$Q_A = \begin{pmatrix} \frac{\lambda_1-\lambda_2}{c} & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}(2,k)$$

then

$$Q_A^{-1}AQ_A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = D.$$

We have shown that Inn_D is isomorphic over $\mathrm{GL}(2,k)$ to Inn_A by Lemma 4.1.

Since B is lower triangular as well, then we can similarly show that Inn_B is isomorphic to Inn_D. By transitivity of isomorphy, Inn_A is isomorphic to Inn_B over $\mathrm{GL}(2,k)$.

Subcase 2.2: The only case left to consider is when one matrix is lower triangular but the other is not. Without loss of generality, assume that A is not lower triangular, but B is lower triangular. It suffices to show that Inn_A is isomorphic over $\mathrm{GL}(2,k)$ to Inn_D where $D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, since we have already shown Inn_B is isomorphic to Inn_D whenever B is lower triangular. We consider

$$A = \begin{pmatrix} a & b \\ -\frac{m_A(a)}{b} & -a+\lambda_1+\lambda_2 \end{pmatrix} \in \mathrm{SL}(2,k[\sqrt{\alpha}])$$

and

$$Q_A = \begin{pmatrix} b & b \\ \lambda_1 - a & \lambda_2 - a \end{pmatrix} \in \mathrm{GL}(2,\bar{k}).$$

Then

$$Q_A^{-1}AQ_A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = D.$$

Let $Q_2 = \sqrt{\alpha}Q_A$. Since all of the entries of Q_A are k-multiples of $\sqrt{\alpha}$, it follows that $Q_2 \in \mathrm{GL}(2,k)$. We can see that $Q_2^{-1}AQ_2 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = D$, and Inn_A is isomorphic to Inn_D by Lemma 4.1. Thus, by transitivity of isomorphy, Inn_A is isomophic to Inn_B.

(b) Suppose A has eigenvalues λ_1 and λ_2 and B has eigenvalues $-\lambda_1$ and $-\lambda_2$. Observe that A and $-B$ have the same eigenvalues. From the proof of (a), we know that Inn_A is isomorphic to Inn_{-B}. Since $\mathrm{Inn}_B = \mathrm{Inn}_{-B}$, we are done.
(c) Suppose Inn_A is isomorphic to Inn_B over $\mathrm{GL}(2, k)$. By Lemma 4.1, there exists $Q \in \mathrm{GL}(2, k)$ such that $Q^{-1}AQ = B$ or $-B$. □

We summarize the results of this theorem in the following corollary.

Corollary 4.4. *Suppose* Inn_A *and* Inn_B *are automorphisms of* $\mathrm{SL}(2, k)$ *where* A *and* $B \in \mathrm{SL}(2, k[\sqrt{\alpha}])$ *for some* $\alpha \in k$ *and each entry of* A *and* B *is a* k*-multiple of* $\sqrt{\alpha}$*. Then* Inn_A *is isomorphic to* Inn_B *over* $\mathrm{GL}(2, k)$ *if and only if* A *has the same eigenvalues as* B *or* $-B$*.*

5. *m*-valid eigenpairs

In the previous section, we reduced the problem of isomorphy of automorphisms of $\mathrm{SL}(2, k)$ to a problem of eigenvalues and quadratic extensions. In this section, we consider the valid pairs of eigenvalues of a matrix A that could induce an automorphism of order m. In the following two lemmas we characterize the matrices B where Inn_B acts as the identity on $\mathrm{SL}(2, k)$.

Lemma 5.1. *Suppose* Inn_B *for* $B \in \mathrm{GL}(n, \bar{k})$ *acts as the identity on* $\mathrm{SL}(2, k)$*. Then* $B = cI$ *for some* $c \in \bar{k}$*.*

Proof. See Lemma 2 of [6]. □

We can improve upon this result since we can assume $B \in \mathrm{SL}(2, \bar{k})$. We can use this idea to characterize the matrices that induce order m automorphisms on $\mathrm{SL}(2, k)$.

Lemma 5.2.
(a) *Suppose* Inn_B *for* $B \in \mathrm{SL}(2, \bar{k})$ *acts as the identity on* $\mathrm{SL}(2, k)$*. Then* $B = I$ *or* $B = -I$*.*
(b) Inn_A *is an order* m *automorphism of* $\mathrm{SL}(2, k)$ *if and only if* m *is the smallest integer such that* $A^m = \pm I$*.*

Proof.
(a) From Lemma 5.1, we have that $B = cI$ for some $c \in \bar{k}$. Since $B \in \mathrm{SL}(2, \bar{k})$, $\det(B) = 1 = c^2$, which means $c = \pm 1$.
(b) If m is the smallest integer such that $A^m = I$ or $A^m = -I$, then m is the smallest integer such that $\mathrm{Inn}_{A^m} = (\mathrm{Inn}_A)^m$ acts as the identity on $\mathrm{SL}(2, k)$, which means Inn_A is an order m automorphism of $\mathrm{SL}(2, k)$.
If Inn_A is an order m automorphism of $\mathrm{SL}(2, k)$, then Inn_{A^m} acts as the identity on $\mathrm{SL}(2, k)$. Then (a) implies that $A^m = I$ or $A^m = -I$. If there exists r such that $0 \leq r < m$ where $A^r = I$ or $A^r = -I$, then Inn_A is at most an order r automorphism of $\mathrm{SL}(2, k)$, which is a contradiction. Thus, m is the smallest integer such that $A^m = I$ or $A^m = -I$.

□

Definition 5.3. We call the pair $\lambda_1, \lambda_2 \in \bar{k}$ an *m-valid eigenpair* of $\mathrm{SL}(2, \bar{k})$ if $A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \in \mathrm{SL}(2, \bar{k})$ and Inn_A is an order m automorphism of $\mathrm{SL}(2, \bar{k})$.

In the following theorem, we characterize the m-valid eigenpairs.

Theorem 5.4. *The pair* λ_1 *and* λ_2 *is an* m*-valid eigenpair of* $\mathrm{SL}(2, \bar{k})$ *if and only if*
(a) λ_1 *is a primitive* $2m$*-th root of unity and* $\lambda_2 = \lambda_1^{2m-1}$*, or*
(b) m *is odd,* λ_1 *is a primitive* m*-th root of unity, and* $\lambda_2 = \lambda_1^{m-1}$

Proof. We begin by assuming that λ_1 and λ_2 is an m-valid eigenpair for $\mathrm{SL}(2,\overline{k})$, and we will show that (a) or (b) must follow. Let $A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$. Note that $A \in \mathrm{SL}(2,\overline{k})$. We know that Inn_A is an order m automorphism of $\mathrm{SL}(2,\overline{k})$. By Lemma 5.2 (b), we know that m is the smallest integer such that $A^m = I$ or $A^m = -I$. There are two cases to consider.

First assume that m is the smallest integer that $A^m = -I$ and that $A^r \neq I$ when $0 \leq r \leq m$. It follows that $\lambda_1^m = -1 = \lambda_2^m$, but that $\lambda_1^r \neq 1 \neq \lambda_2^r$ and $\lambda_1^r \neq -1 \neq \lambda_2^r$ for $0 \leq r < m$. Thus λ_1 is a $2m$-th root of unity. Since $\det(A) = 1$, $\lambda_2 = \lambda_1^{2m-1}$.

Now assume that m is the smallest integer such that $A^m = I$ and that $A^r \neq -I$ when $0 \leq r \leq m$. It follows that $\lambda_1^m = 1 = \lambda_2^m$, but that $\lambda_1^r \neq 1 \neq \lambda_2^r$ and $\lambda_1^r \neq -1 \neq \lambda_2^r$ for $0 \leq r < m$. Note that m must be odd. Further, λ_1 is an m-th root of unity. Since $\det(A) = 1$, then $\lambda_2 = \lambda_1^{m-1}$.

Now we prove the converse. In either case, $A \in \mathrm{SL}(2,\overline{k})$ follows from the construction of A. Let's first assume (a). Then m is the smallest positive integer such that $\lambda_1^m = -1 = \lambda_2^m$, and $2m$ is the smallest integer such that $\lambda_1^{2m} = 1 = \lambda_2^{2m}$. Thus, m is the smallest integer such that $A^m = -I$ and $2m$ is the smallest integer such that $A^{2m} = I$. By Lemma 5.2 (b), Inn_A is an order m automorphism of $\mathrm{SL}(2,\overline{k})$.

Now assume the conditions of (b). Then m is the smallest integer such that $\lambda_1^m = 1 = \lambda_2^m$, and $\lambda_1^r \neq 1 \neq \lambda_2^r$ for every integer r where $0 \leq r < m$. We know that $\lambda_1^r \neq -1$, so m is the smallest integer such that $A^m = I$, and Lemma 5.2 (b) tells us that Inn_A is an order m automorphism of $\mathrm{SL}(2,\overline{k})$. □

Let ϕ denote Euler's ϕ-function. That is, for any positive integer m, $\phi(m)$ is the number of integers l such that $1 \leq l < m$ and $\gcd(l, m) = 1$.

Corollary 5.5. *For any field k of characteristic not 2, there are $\phi(m)$ m-valid eigenpairs of* $\mathrm{SL}(2,\overline{k})$.

Proof. We consider separately the cases where m is odd and even. First, assume m is even. Write $m = 2^s t$ where s and t are integers and t is odd. If we include ordering, then there are $\phi(2m)$ such pairs. This double counts the m-valid eigenpairs of $\mathrm{SL}(2,\overline{k})$. Thus, the number of distinct m-valid eigenpairs for $\mathrm{SL}(2,\overline{k})$ is

$$\begin{aligned}\frac{\phi(2m)}{2} &= \frac{\phi(2^{s+1}t)}{2}\\ &= \frac{\phi(2^{s+1})\phi(t)}{2}\\ &= \frac{2^s\phi(t)}{2}\\ &= 2^{s-1}\phi(t)\\ &= \phi(2^s)\phi(t)\\ &= \phi(2^s t)\\ &= \phi(m).\end{aligned}$$

Now suppose m is odd. By Theorem 5.4 the eigenvalues may be primitive m-th or $2m$-th roots of unity. If we include ordering, there are $\phi(m) + \phi(2m)$ such pairs. Again, this double counts the m-valid eigenpairs of $\mathrm{SL}(2,\overline{k})$. The number of distinct m-valid eigenpairs of $\mathrm{SL}(2,\overline{k})$ when m is odd is

$$\begin{aligned}\frac{\phi(m)+\phi(2m)}{2} &= \frac{\phi(m)+\phi(m)}{2}\\ &= \phi(m).\end{aligned}$$

Therefore, regardless of the parity of m, there are always $\phi(m)$ m-valid eigenpairs of $\mathrm{SL}(2,\overline{k})$. □

6. Number of Isomorphy Classes

Given a field k not of characteristic 2 which is not necessarily algebraically closed, we would like to know the number of the isomorphy classes of order m automorphisms of $\mathrm{SL}(2,k)$.

Definition 6.1. Let $C(m,k)$ denote the number of isomorphy classes of order m automorphisms of $\mathrm{SL}(2,k)$ over $\mathrm{GL}(2,k)$ for a field of characteristic not 2.

Theorem 6.2. *When* $\mathrm{char}(k) \neq 2$, $C(m,k) = \frac{1}{2}\phi(m)$ *or* 0 *for* $m > 2$ *and* $C(2,k) = |k^*/(k^*)^2|$.

Proof. From Corollary 2 in [6], we know that $C(2,k) = |k^*/(k^*)^2|$. This is also clear from our results, since there is exactly one 2-valid eigenpair for $\mathrm{SL}(2,\bar{k})$, consisting of the two roots of -1. Thus, a matrix of the form

$$\begin{aligned}\begin{pmatrix} a & b \\ -\frac{m_A(a)}{b} & -a+\lambda+\lambda^{-1}\end{pmatrix} &= \begin{pmatrix} a & b \\ -\frac{m_A(a)}{b} & -a+i+(-i)\end{pmatrix} \\ &= \begin{pmatrix} a & b \\ -\frac{m_A(a)}{b} & -a\end{pmatrix}\end{aligned}$$

can have entries that are k-multiples of $\sqrt{\alpha}$ for any $\alpha \in k$.

Now assume $m > 2$. We claim that each m-valid eigenpair of $\mathrm{SL}(2,\bar{k})$ induces either one or zero isomorphy classes of order m automorphisms of $\mathrm{SL}(2,k)$. Recall that if Inn_A is an order m automorphism, then by Theorem 3.3 we know that

$$A = \begin{pmatrix} a & b \\ -\frac{m_A(a)}{b} & -a+\lambda+\lambda^{-1}\end{pmatrix}$$

or

$$A = \begin{pmatrix} \lambda & 0 \\ c & \lambda^{-1}\end{pmatrix},$$

where $\det(A) = 1$ and the entries of A are in k or are k-multiples of $\sqrt{\alpha}$ for some $\alpha \in k$. Also, by Theorem 5.4 we may assume that λ is an m-th or $2m$-th primitive root of unity. If $\lambda+\lambda^{-1}$ is nonzero, then $\lambda+\lambda^{-1}$ can lie in at most one square class of k since the square classes form a partition of the field k. To see that this is the case, we need only show that $\lambda+\lambda^{-1} \neq 0$ when $m > 2$. But, if $\lambda+\lambda^{-1} = 0$, then we can rearrange this equation to get $\lambda^2 = -1$ which is the case only when $m = 2$. Since $m \neq 2$, then it is clear that $\lambda+\lambda^{-1} \neq 0$.

So, $C(m,k)$ is at most $\phi(m)$. We need only consider the possibility that there are distinct m-valid eigenpairs that induce the same isomorphy class. But, we know from Corollary 4.4 that if Inn_A and Inn_B are isomorphic where $A, B \in \mathrm{SL}(2,k[\sqrt{\alpha}])$, then A has the same eigenvalues as B or $-B$. So, if A has eigenvalues λ_1 and λ_2, then B has the same eigenvalues, or eigenvalues $-\lambda_1$ and $-\lambda_2$. So, $C(m,k) \geq \frac{\phi(m)}{2}$. But, if λ_1 and λ_2 is an m-valid eigenpair of $\mathrm{SL}(2,\bar{k})$, then $-\lambda_1$ and $-\lambda_2$ is also an m-valid eigenpair of $\mathrm{SL}(2,\bar{k})$. Thus, $C(m,k) = \frac{\phi(m)}{2}$. □

For the remainder of this section, we consider how many quadratic extensions of k can induce an order m automorphism of $\mathrm{SL}(2,k)$, specifically when $m > 2$.

Lemma 6.3. *Let k be a field and $\alpha \in k$, and suppose λ is an lth primitive root of unity.*

(a) *If λ is a k-multiple of $\sqrt{\alpha}$, then λ^r is a k-multiple of $\sqrt{\alpha}$ for all odd integers r, and $\lambda^r \in k$ for all even integers r.*

(b) *If $\lambda+\lambda^{-1}$ is a k-multiple of $\sqrt{\alpha}$, then $\lambda^r+\lambda^{-r}$ is a k-multiple of $\sqrt{\alpha}$ for all odd integers r and $\lambda^r+\lambda^{-r} \in k$ for all even integers r.*

Proof. The proof of (a) is clear. We probe (b) by induction. Let $r > 1$ be even and suppose $\lambda + \lambda^{-1}$ and $\lambda^{r-1} + \lambda^{-(r-1)}$ are k-multiples of $\sqrt{\alpha}$, and that $\lambda^{r-2} + \lambda^{-(r-2)} \in k$. Then

$$(\lambda + \lambda^{-1})(\lambda^{r-1} + \lambda^{-(r-1)}) = (\lambda^r + \lambda^{-r}) + (\lambda^{r-2} + \lambda^{-(r-2)}) \in k.$$

Thus, $\lambda^r + \lambda^{-r} \in k$.

Let $r > 1$ be odd and suppose $\lambda + \lambda^{-1}$ and $\lambda^{r-2} + \lambda^{-(r-2)}$ are k-multiples of $\sqrt{\alpha}$, and that $\lambda^{r-1} + \lambda^{-(r-1)} \in k$. Then an argument similar to the above shows that $\lambda^r + \lambda^{-r}$ is a k-multiple of $\sqrt{\alpha}$. □

From Theorem 6.2, if $m > 2$, then each m-valid eigenpair of $\mathrm{SL}(2, \bar{k})$ can induce at most one isomorphy class of order m automorphisms of $\mathrm{SL}(2, k)$. Paired with Lemma 6.3, if $\mathrm{SL}(2, k)$ has an order m automorphism Inn_A, then the entries of matrices A that induce these automorphisms will have entries in k, or a single quadratic extension of k. This gives the following result.

Corollary 6.4. *Let k be a field of characteristic not 2. If $m > 2$ and $A, B \in \mathrm{SL}(2, k)$, then it is not possible for Inn_A and Inn_B to be order m automorphisms of $\mathrm{SL}(2, k)$ and for A and B to have entries in distinct quadratic extensions of k.*

7. Examples

We now look at a few examples over different fields k. Recall Definition 2.5, the definition of the square classes of a field k, and the examples of square classes for a collection of fields which followed.

Example 7.1 ($k = \bar{k}$). Since all roots of unity will lie in k when k is algebraically closed, then every m-valid eigenpair of $\mathrm{SL}(2, \bar{k})$, λ_1 and λ_2, will induce an order m automorphism of $\mathrm{SL}(2, k)$ of the form Inn_A where $A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$.

Recall Definition 6.1, the definition of $C(m, k)$. The following is a direct result of Theorem 6.2:

Theorem 7.2. *If $\mathrm{char}(\bar{k}) \neq 2$, then $C(2, \bar{k}) = 1$ and $C(m, \bar{k}) = \frac{1}{2}\phi(m)$ when $m > 2$.*

Example 7.3 ($k = \mathbb{R}$). Let i denote the square root of -1 and λ be an lth primitive root of unity where we assume $l = 2m$ and m can be odd or even, or $l = m$ and m is odd. We know that λ and λ^{l-1} form an l-valid eigenpair of $\mathrm{SL}(2, \bar{k})$ by Theorem 5.4. For this eigenpair to induce an automorphism on $\mathrm{SL}(2, \mathbb{R})$ we need one of the following to be the case:
(a) $\lambda \in \mathbb{R}$;
(b) $\lambda = \gamma i$, for $\gamma \in \mathbb{R}$;
(c) $\lambda + \lambda^{l-1} \in \mathbb{R}$; or
(d) $\lambda + \lambda^{l-1} = \gamma i$, for $\gamma \in \mathbb{R}$.

These conditions follow since the entries of A must lie in $\mathbb{R}$ or be $\mathbb{R}$-multiples of i. Cases (a) and (b) correspond to $A = \begin{pmatrix} \lambda & 0 \\ c & \lambda^{l-1} \end{pmatrix}$ inducing the automorphism Inn_A, and cases (c) and (d) correspond to $A = \begin{pmatrix} a & b \\ -\frac{m_A(a)}{b} & -a+\lambda+\lambda^{l-1} \end{pmatrix}$ inducing the automorphism Inn_A. Further, (a) and (c) correspond to the entries of A falling in $\mathbb{R}$, and (b) and (d) correspond to the entries of A being $\mathbb{R}$-multiples of i. Using De Moivre's formula, we can write

$$\lambda = \cos\left(\frac{2\pi r}{l}\right) + i \sin\left(\frac{2\pi r}{l}\right)$$

and

$$\lambda^{l-1} = \cos\left(\frac{2\pi r}{l}\right) - i \sin\left(\frac{2\pi r}{l}\right)$$

for some integer r where $0 < r < l$ and r is coprime to l. By Lemma 6.3, if one such value of r yields an m-valid eigenpair for $\mathrm{SL}(2, \bar{k})$, then all such values of r will yield m-valid eigenpairs. So, without loss of generality we assume that $r = 1$.

We can easily check to see when we have each of the four cases listed above.

(a) When is $\lambda \in \mathbb{R}$? If $\lambda \in \mathbb{R}$, then $\sin\left(\frac{2\pi}{l}\right) = 0$, which means $l = 1$ or 2. If $l = 1$, then $\lambda = \cos\left(\frac{2\pi}{l}\right) = 1$. If $l = 2$, then $\lambda = \cos\left(\frac{2\pi}{l}\right) = -1$. In either case, we have $m = 1$. We are not concerned with 1-valid eigenpairs so we may ignore this case.

(b) When is $\lambda = \gamma i$, for $\gamma \in \mathbb{R}$? Similar to the previous case, we know that $\cos\left(\frac{2\pi}{l}\right) = 0$, which means $l = 4$ or $\frac{4}{3}$. Since l must be a positive integer we may assume $l = 4$. Thus, $\lambda = i$, which means $m = 2$. There is one 2-valid eigenpair of $\mathrm{SL}(2, \bar{k})$, which is formed by i and $-i$.

(c) When is $\lambda + \lambda^{l-1} \in \mathbb{R}$? Using De Moivre's formula, we see that

$$\begin{aligned}\lambda + \lambda^{l-1} &= \left(\cos\left(\frac{2\pi}{l}\right) + i\sin\left(\frac{2\pi}{l}\right)\right) + \left(\cos\left(\frac{2\pi}{l}\right) - i\sin\left(\frac{2\pi}{l}\right)\right)\\ &= 2\cos\left(\frac{2\pi}{l}\right) \in \mathbb{R}.\end{aligned}$$

This is always the case.

(d) Based on the previous case, we see that $\lambda + \lambda^{l-1} = \gamma i$ for $\gamma \in \mathbb{R}$ is never the case.

If $m = 2$, then $l = 4$. There are two isomorphy classes of order 2 automorphisms: one where the matrix takes entries in $\mathbb{R}$ from (c), and one where the matrix has entries that are $\mathbb{R}$-multiples of i from case (b). Thus, $C(2, \mathbb{R}) = 2$, which agrees with the results in [6] and Theorem 6.2.

Suppose $m > 2$. Case (c) applies here. It follows that there are always mth and $2m$th primitive roots of unity. Based on what has just been shown and Theorem 6.2, we have the following result.

Theorem 7.4. *If $m = 2$, then $C(2, \mathbb{R}) = 2$; if $m > 2$, then $C(m, \mathbb{R}) = \frac{1}{2}\phi(m)$.*

Example 7.5 ($k = \mathbb{Q}$). We know that $C(2, \mathbb{Q})$ is infinite. Consider the case where $m > 2$. Let λ be an lth root of unity where $l = 2m$ and m can be odd or even, or $l = m$ and m is odd. As noted in the case where $k = \mathbb{R}$, $\lambda + \lambda^{l-1} = 2\cos\left(\frac{2\pi r}{l}\right)$. The group $\mathrm{SL}(2, \mathbb{Q})$ will have order m automorphisms if and only if $\cos\left(\frac{2\pi r}{l}\right)$ lies in $\mathbb{Q}$ or is a $\mathbb{Q}$ multiple of $\sqrt{n}$ for some positive integer n. Similar to the real case above, we can use Lemma 6.3 and assume without loss of generality that $r = 1$.

We first examine the case when $\cos\left(\frac{2\pi}{l}\right)$ lies in $\mathbb{Q}$. By Niven's Theorem, Corollary 3.12 of [13], $\cos x$ and $\frac{x}{\pi}$ are simultaneously rational only when $\cos x = 0, \pm\frac{1}{2}$, or ± 1. Then $\cos\left(\frac{2\pi}{l}\right)$ is rational if and only if $l = 6, 4, 3, 2, \frac{3}{2}, \frac{4}{3}$, or $\frac{6}{5}$. Since l must be an integer, we need only consider $l = 6, 4, 3$, or 2. Since $m > 2$ we can further restrict our considerations to $l = 3$ or 6. Both of these correspond to order 3 automorphisms. There is $\frac{\phi(3)}{2} = 1$ isomorphy class of order 3 automorphisms of $\mathrm{SL}(2, \mathbb{Q})$. If we let $l = 6$ and choose $a = b = 1$, then

$$A = \begin{pmatrix} a & b \\ -\frac{m_A(a)}{b} & -a + \lambda + \lambda^{l-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

is a matrix that will induce an order 3 automorphism.

We now consider the case when $2\cos\left(\frac{2\pi}{l}\right)$ is a $\mathbb{Q}$ multiple of $\sqrt{n}$ for some positive integer n. We note the following lemma which is a part of Theorem 3.9 in [13].

Lemma 7.6. *Let l be a positive integer. Then $2\cos\left(\frac{2\pi}{l}\right)$ is an algebraic integer which satisfies a minimal polynomial of degree $\frac{\phi(l)}{2}$.*

Since we are interested in knowing when $2\cos\left(\frac{2\pi r}{l}\right) = \mu\sqrt{n}$ for some $\mu \in \mathbb{Q}$ and positive integer n, we need $2\cos\left(\frac{2\pi r}{l}\right)$ to satisfy a polynomial of the form $x^2 - \mu^2 n = 0$. By the lemma, a necessary condition for such l is that $\frac{\phi(l)}{2} = 2$, or $\phi(l) = 4$.

If $l = p^m$ for some prime p, then

$$4 = \phi(p^m) = p^{m-1}(p-1).$$

Note that p and $p-1$ cannot both be even, so it must be the case that $p^{m-1} = 4$ and $p-1 = 1$, which means $l = 8$, or $p^{m-1} = 1$ and $p-1 = 4$, which means $l = 5$.

If $l = p^m q^t$ for some distinct primes p and q, then

$$4 = \phi(p^m q^t) = (p^m - p^{m-1})(q^t - q^{t-1}).$$

If $p^m - p^{m-1} = 2 = q^t - q^{t-1}$, then without loss of generality $p^m = 4$ and $q^t = 3$ which means $l = 12$. (Other primes and/or larger powers would not yield $\phi(p^m) = 2$.) If $p^m - p^{m-1} = 4$ and $q^t - q^{t-1} = 1$, then $p^m = 8$ or 5, and $q^t = 2$. Since p and q are distinct, we have $l = 10$.

If l is a product of three or more distinct primes, then $\phi(l) > 4$. So, the only l for which $\phi(l) = 4$ are $l = 5, 8, 10$ and 12. For these values of l, we have the following values for $\lambda + \lambda^{l-1}$:

$$2\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{2},$$
$$2\cos\left(\frac{2\pi}{8}\right) = \sqrt{2},$$
$$2\cos\left(\frac{2\pi}{10}\right) = \frac{1+\sqrt{5}}{2},$$

and

$$2\cos\left(\frac{2\pi}{12}\right) = \sqrt{3}.$$

When $l = 8$ or 12, $2\cos\left(\frac{2\pi r}{l}\right)$ satisfies a polynomial of the form $x^2 - \mu^2 n = 0$, but no linear polynomial and for no other values of l. Thus, $\mathrm{SL}(2,\mathbb{Q})$ also has automorphisms of order 4 and 6.

Theorem 7.7. $\mathrm{SL}(2,\mathbb{Q})$ *only has finite order automorphisms of orders 1, 2, 3, 4, and 6. Further,* $C(2,\mathbb{Q})$ *is infinite, and* $C(3,\mathbb{Q}) = C(4,\mathbb{Q}) = C(6,\mathbb{Q}) = 1$.

Example 7.8 **($k = \mathbb{F}_q, q = p^r, p \neq 2$).** If $m = 2$, then $C(2,\mathbb{F}_q) = 2$. Again, assume $m > 2$. We need only determine when m-th and $2m$-th primitive roots of unity lie in $\mathbb{F}_q$ or are an $\mathbb{F}_q$-muliple of $\sqrt{\alpha}$ for some $\alpha \in \mathbb{F}_q$. We first consider the primitive roots of unity which lie in $\mathbb{F}_q$. It is known that $\mathbb{F}_q^*$ is a cyclic multiplicative group of order $q-1$, so it contains elements of orders $q-1$, and all of $(q-1)$'s divisors. Thus, $\mathbb{F}_q$ will contain all of the primitive roots of unity of orders $q-1$, and its divisors.

We now consider the primitive roots of unity which are $\mathbb{F}_q$ multiples of $\sqrt{\alpha}$ for some $\alpha \in \mathbb{F}_q$. Suppose $\lambda = \mu\sqrt{\alpha}$ where $\mu, \alpha \in \mathbb{F}_q$. Note that

$$\lambda^{q-1} = \mu^{q-1}\alpha^{\frac{q-1}{2}} = \alpha^{\frac{q-1}{2}}.$$

It follows that $\lambda^{2(q-1)} = 1$. The maximal possible value l such that an lth primitive root of unity is an $\mathbb{F}_q$ multiple of $\sqrt{\alpha}$ for $\alpha \in \mathbb{F}_q$ is $2(q-1)$. To see that this maximal order of primitive roots of unity will always occur, suppose $\alpha \in \mathbb{F}_q$ is a $(q-1)$th primitive root of unity. Then $\sqrt{\alpha}$ is a $2(q-1)$-th primitive root of unity. This, along with Theorem 6.2, proves the following result.

Theorem 7.9.

(a) *If* $m = 2$*, then* $C(2,\mathbb{F}_q) = 2$.

(b) *If* $m > 2$ *is even and* $2m$ *divides* $2(q-1)$ *or if* $m > 2$ *is odd and both* m *and* $2m$ *divide* $q-1$ *then* $C(m,\mathbb{F}_q) = \frac{\phi(m)}{2}$.

(c) *In any other case,* $C(m,\mathbb{F}_q) = 0$.

References

[1] Benim, R.-W., Dometrius, C., Helminck, A. G., Wu, L. (2016). Isomorphy classes of k-involutions of $\mathrm{SO}(n, k, \beta)$, $n > 2$. *Journal of Lie Theory* 26:383–438.
[2] Benim, R.-W., Helminck, A. G., Jackson Ward, F. (2015). Isomorphy classes of involutions of $\mathrm{SP}(2n, k)$, $n > 2$. *Journal of Lie Theory* 25:903–947.
[3] Borel, A. (1991). *Linear Algebraic Groups*. Graduate Texts in Mathematics, Vol. 126. 2nd enlarged edition. New York: Springer Verlag.
[4] Helminck, A. G. (1988). Algebraic groups with a commuting pair of involutions and semisimple symmetric spaces. *Adv. Math.* 71:21–91.
[5] Helminck, A. G. (2000). On the Classification of k-involutions I. *Adv. Math.* 153(1):1–117.
[6] Helminck, A. G., Wu, L. (2002). Classification of involutions of $\mathrm{SL}(2, k)$. *Commun. Algebra* 30(1):193–203.
[7] Helminck, A. G., Wu, L., Dometrius, C. (2006). Involutions of $\mathrm{SL}(n, k)$, $(n > 2)$. *Acta Appl. Math.* 90:91–119.
[8] Hutchens, J. (2014). Isomorphy classes of k-involutions of G_2. *J. Algebra Appl.* 13(7):1–16.
[9] Hutchens, J. (2015). Isomorphism classes of k-involutions of algebraic groups of type F_4. *J. Lie Theory* 25:1003–1022.
[10] Hutchens, J. (2016). Isomorphism classes of k-involutions of algebraic groups of type E_6. *Beiträge zur Algebra und Geometrie/Contributions to Algebra and Geometry* 57:525–552.
[11] Hutchens, J., Schwartz, N. Involutions of type G_2 over a field of characteristic 2. 1–30.
[12] Levy, P. (2009). Vinberg's θ-groups in positive characteristic and Kostant-Weierstrass slices. *Transformation Groups* 14(2).
[13] Niven, I. (1956). *Irrational Numbers*. Buffalo Mathematical Association of America; New York: J. Wiley.
[14] Schwartz, N. k-involutions of $\mathrm{SL}(n, k)$ over fields of characteristic 2. 1–19.
[15] Springer, T. A. (1987). The classification of involutions of simple algebraic groups. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 34(3):655–670.
[16] Vinberg, È. B. (1976). The Weyl Group of a graded Lie algebra. *Mathematics of the USSR-Izvestiya* 10(3).