ABSTRACT

SCHWARTZ, NATHANIEL JACOB. On the Classification of k-involutions of $\mathrm{SL}(n,k)$ and $\mathrm{O}(n,k)$ over Fields of Characteristic 2. (Under the direction of Aloysius G. Helminck.)

The characterization and classification of k-involutions of algebraic groups enables one to determine much of the structure of the related symmetric k-varieties. Helminck characterized k-involutions of connected, reductive algebraic groups over algebraically closed fields of characteristic not 2 in [20]. More recently, Benim, Dometrius, and Wu completely classified k-involutions of $\mathrm{SL}(n,k)$ and $\mathrm{SO}(2n+1,k)$ over perfect fields of characteristic not 2. In this present work, we proceed with a similar theme, but k is any field of characteristic 2. We classify k-involutions of $\mathrm{SL}(2,k)$ as a preliminary step, then, using similar techniques, we classify involutions of $\mathrm{SL}(n,k)$. Finally, we initiate a similar classification for $\mathrm{O}(n,k)$ and note partial results.

On the Classification of k-involutions of $\mathrm{SL}(n,k)$ and $\mathrm{O}(n,k)$ over Fields of Characteristic 2

by
Nathaniel Jacob Schwartz

A dissertation submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Mathematics

Raleigh, North Carolina

2013

APPROVED BY:

Ernest L. Stitzinger	Thomas P. Lada
Naihuan Jing	Aloysius G. Helminck Chair of Advisory Committee

BIOGRAPHY

Nathaniel is the youngest of four sons of Connie and Leonidas Schwartz. He was home-schooled while growing up on a farm in Virginia. At age 16 he began working full-time for a local land surveyor; he continued working for various land surveying and engineering firms until he was 23. To further his education and career, he entered community college at Piedmont Virginia Community College in Charlottesville, Virginia. He graduated from PVCC in 2005 with an Associate's degree in engineering, and immediately enrolled at Virginia Commonwealth University in Richmond, Virginia. Here he studied mathematics and computer science, and he graduated in 2008 with a double major. In 2008 he entered graduate school at North Carolina State University. At NCSU he studied theoretical mathematics under the guidance of Aloysius Helminck. At the same time he taught classes and attended to his responsibilities as a graduate teaching assistant. Nathaniel will graduate in December of 2013, earning a Ph.D. in mathematics.

ACKNOWLEDGEMENTS

I wish to extend my most sincere thanks and gratitude to the following people.

For helping me with my research and graduation: My advisor, Loek Helminck, for his patience, kindness, understanding and guidance. The members of my committee: Dr. Naihuan Jing, Dr. Ernest Stitzinger, and Dr. Thomas Lada. My graduate school representatives, Dr. Jason Swarts, and Dr. Nagui Rouphail. Maggie Rahmoeller, for patiently proof-reading everything except these acknowledgements.

For inspiring, teaching and helping me to stay excited about math: My mentors and professors from PVCC, VCU, and NCSU, including (but not limited to) Jon Hexter, Dewey Taylor, Richard Hammack, John Fogelgren, Robert Martin, Ernest Stitzinger, Mohan Putcha, Kailash Misra, and Molly Fenn.

For non-mathematical advice and support in all things: Denise Seabrooks, Charlene Wallace, Carolyn Gunton, Di Bucklad, Julia Reynolds, John Griggs, Matt Haught, and all the support staff at NCSU. Tara Hudson for a great PTP peer mentoring experience.

For making graduate school a bit more awesome: Mitch's Tavern for the *real* Cuban. Global Village for the coffee, and Justin Wright for convincing me to try coffee. Tyler's Taproom for the excellent brews. And the one raccoon that just had to cross the road at the wrong time.

For their love and life support: Grace, for her unwavering support and love. My parents and my brothers, Connie, Leonidas, Benjamin, Baron and Aedin, for constant support and love.

For camaraderie, all my fellow graduate student friends: Justin Wright, Emma Norbrothen, Zack Kenz, John Hutchens, Tom & Mami Wentworth, Maggie Rahmoeller, Stephen Adams, Abby Bishop, Matthew Comer, SAS 4121 (Nicole Panza, Mandy Smith, Justin Wright, Greg Dempsey, Stephen Adams), SAS 3213 (Karen Bobinyec, Maggie Rahmoeller), "The Epsilon Ballers", and all the people who are important, but not quite important enough to list here (who should all feel slighted, but probably won't read this anyway).

For the word "manywhere": Michael Artin.

Finally, I want to acknowledge the people who have helped me succeed personally.

TABLE OF CONTENTS

LIST OF TABLES

Chapter 1

Introduction

This work follows and extends the work of Aloysius Helminck, his collaborators, and several of his current and former graduate students. Recent works by Wu, Dometrius, and Benim have provided significant insight for the present work (see [39], [14], and [5]). Their examples and techniques have been helpful in classifying k-involutions and symmetric k-varieties for linear algebraic groups defined over fields of characteristic 2. Beyond the standard references by Helgason [18], Borel [6], etc., the several publications of Helminck (see [21], [19], and [20]) provide most of the direct background for the present work.

1.1 Symmetric Spaces

Symmetric spaces have been studied since the late 19th century. Recent advances in the subject brought about several useful connections between symmetric spaces and a variety of applications. They have also been extended in several ways from symmetric spaces of Lie groups over the real and complex numbers. Our present concern is with symmetric k-varieties of algebraic groups over arbitrary fields k. In the most general sense, symmetric spaces can be defined for any group, in which case they are called generalized symmetric spaces.

Let G be any group, and let θ be an automorphism of G such that $\theta^2 = \mathrm{Id}$. We say that θ is an *involution* since it has order exactly 2. A *generalized symmetric space* of G is the set

$$Q = \{x\theta(x)^{-1} \mid x \in G\}.$$

The fixed point group of the involution θ is particularly useful in studying symmetric spaces, especially when it is compact. We define the *fixed point group* of θ as

$$H = G^\theta = \{g \in G \mid \theta(g) = g\}.$$

Define a map $\tau : G \to Q$ by $\tau(g) = g\theta(g)^{-1}$; τ is surjective and the fiber of $\tau(g)$ is gH; hence $Q \simeq G/H$. This illustrates the relationship between symmetric spaces and the fixed point groups of the corresponding involutions. Viewing symmetric spaces in this way yields a great deal of information about their structure.

Example 1.1. Any group G is a symmetric space. Consider the group $g = G \times G$. The map $\theta : g \to g$ defined by $\theta(x, y) = (y, x)$ is an involution, and the fixed point group H of θ is isomorphic to G; it consists of elements of the form (x, x). Moreover,

$$H = \{(x, x) | x \in G\} \qquad \text{and} \qquad Q = \{(x, x^{-1}) | x \in G\} \cong G.$$

□

Historically, the first symmetric spaces studied were those associated with the real reductive Lie groups whose involutions have compact fixed point groups. When H is compact and G is a real reductive Lie group, the involution is called the *Cartan involution*. The Cartan involution plays a significant role in the representation theory of semisimple Lie algebras and Lie groups. These symmetric spaces were called *Riemannian symmetric spaces* and they were studied by Cartan in the late 1800's through the 1920's (see [7] and [8]). Riemannian symmetric spaces can also be defined via differential geometry, but we prefer the more algebraic definition as it is more easily extensible and falls within the realm of Lie theory. The two approaches are equivalent for Riemannian symmetric spaces.

Example 1.2. Symmetric spaces were originally named for the symmetry of their elements. Historically, the first symmetric space that was studied illustrates this phenomenon elegantly. We begin with a finite dimensional vector space V over $\mathbb{R}$. Let B be a bilinear form on V. For this example, we will let B be the standard dot product on V, for the sake of illustration. For any linear operator A on V, we define its *adjoint* to be the operator A' that satisfies

$$B(Ax, y) = B(x, A'y)$$

for all $x, y \in V$. The adjoint depends on B. Since B is the dot product, the adjoint of A is the transpose of A. Thus, if A is *self-adjoint* (i.e., $A = A'$), then A is symmetric, since $A = A^T$.

The set of all self-adjoint operators of V with respect to B is a subspace, which we denote $\mathfrak{p}(V, B)$. Every $A \in \mathfrak{p}(V, B)$ has real eigenvalues; if these eigenvalues are positive we say A is a *positive* operator. We denote by $P(V, B)$ the set of positive, self-adjoint operators. Also, note that $\exp(\mathfrak{p}) = P \subset \mathrm{GL}(V)$.

An operator A is *orthogonal* with respect to B if $B(Ax, Ay) = B(x, y)$ for all $x, y \in V$. This condition is equivalent to the condition that $A'A = \mathrm{Id}$. When B is the dot product $A' = A^T$,

and A is orthogonal in the usual sense. With respect to B, the orthogonal operators on V form a compact subgroup of $\mathrm{GL}(V)$, which we denote $\mathrm{O}(V, B)$.

Let $\theta : \mathrm{GL}(V) \to \mathrm{GL}(V)$ by $\theta(A) = (A')^{-1}$. If B is the dot product, this is the same as $A \mapsto (A^T)^{-1}$. Then θ is an automorphism of $\mathrm{GL}(V)$, and $\theta^2 = \mathrm{Id}$. Moreover, the fixed point group of θ is $\mathrm{O}(V, B)$.

The symmetric space Q consists of elements $A\theta(A)^{-1} = A\big((A')^{-1}\big)^{-1} = AA' = AA^T$. Since, for any $A \in \mathrm{GL}(V)$, AA^T is a positive operator, it follows that $Q \subset P(V, B)$. Moreover, every positive operator A has a unique, positive square root T in $P(V, B)$. To see this, notice that $P(V, B)$ consists of semisimple elements A with positive real eigenvalues. For each A, there exists a diagonal matrix Λ and an orthogonal matrix S so that $A = S\Lambda S^{-1}$. Moreover, $T = S\sqrt{\Lambda}S^{-1}$, $T^2 = A$, and $T \in P(V, B)$.

Every element X of $\mathrm{GL}(V)$ can be uniquely decomposed as a product of an orthogonal operator O and a self-adjoint operator A, i.e., $X = O{\cdot}A$. Since the fixed points are the orthogonal operators, the map $\theta : \mathrm{GL}(V) \to \mathrm{GL}(V)$ has image $P(V, B)$ and hence $\mathrm{GL}(V)/\mathrm{O}(V, B) \cong P(V, B)$. If B is the dot product, it consists of symmetric operators which can be viewed as symmetric matrices.

In summary, $Q = P(V, B)$, and when B is the dot product, Q consists of symmetric matrices. □

Affine symmetric spaces, or *real reductive symmetric spaces*, are essentially the same as Riemannian symmetric spaces, except that the involution does not have a compact fixed point group. Equivalently, the involution is not the Cartan involution.

Symmetric varieties are defined as the spherical homogeneous spaces G/H where the field k is algebraically closed and G is a reductive algebraic group with H the fixed point of an involution.

Symmetric k-varieties are a generalization to both affine symmetric spaces and symmetric varieties. They are defined as the homogeneous spaces $Q_k = G_k/H_k$ where G is a reductive algebraic group defined over k, and H is the fixed point group of a k-involution of G. Here H_k and G_k denote the k-rational points of H and G, respectively.

In Example 1.2, H is compact, θ is the Cartan involution, and the elements of Q are orthogonally diagonalizable. In the more general setting, the elements of Q_k are semisimple if k has characteristic 0 and H is *k-anisotropic* (i.e., there are no non-trivial k-split tori in H). H being k-anisotropic is somewhat analogous to H being compact. Consequently, one theme is to determine which (if any) fixed point groups are k-anisotropic.

Beginning in the 1980's, symmetric k-varieties became important in a variety of areas of mathematics. Some examples are found in the study of arithmetic subgroups (see [35]), character sheaves (see [28, 15]), geometry (see [10, 11] and [1]), singularity theory (see [29] and [25]), and

the study of Harish-Chandra modules (see [4] and [36, 37]). They are most well-known for their role in representation theory. This prompted a detailed study of these symmetric k-varieties and their applications. The first major results were obtained by Helminck and Wang [22]. They showed that symmetric k-varieties are isomorphic if and only if their corresponding k-involutions are isomorphic. After this ground-breaking work, many results followed.

A classification of symmetric k-varieties turned out to be much more complicated than in the case of classical (affine) symmetric spaces. It was not until the late 90's that Helminck [21] characterized the symmetric k-varieties defined over perfect fields of characteristic not 2.

All previous studies of symmetric k-varieties and their applications exclude the case that k has characteristic 2. This is due to of a variety of complications that arise. The building blocks of symmetric spaces come from algebraic groups and not all of it applies to characteristic 2 fields. At some point, all of the dependent assumptions must be verified for characteristic 2 fields.

Example 1.3. One example that arises which is distinct to characteristic 2 is that k-involutions can correspond to conjugation by matrices that are not semisimple. For other fields, inner k-involutions always correspond to conjugation by a semisimple matrix. One such k-involution of $G = \mathrm{GL}(2, k)$ conjugation by $X = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. Since k has characteristic 2, X is not semisimple. □

A consequence of these differences is that there are many open questions about the classification and characterization of symmetric k-varieties over fields of characteristic 2. In this dissertation, we initiate the study of symmetric k-varieties over fields of characteristic two, beginning with a classification of k-involutions.

1.2 Summary of Results

In this dissertation, we classify k-involutions of $\mathrm{SL}(2, k)$ and $\mathrm{SL}(n, k)$ when k is a field of characteristic 2. We determine the fixed point groups of each k-involution.

For $\mathrm{O}(n, k)$ we indicate some preliminary results in the effort to classify the involutions. We also list several conjectures. We verified some of these conjectures in the case that n is small and with small finite fields.

In order to summarize the involutions of $\mathrm{SL}(n, k)$, we need the following notation. Let

$\theta : \mathrm{SL}(n,k) \to \mathrm{SL}(n,k)$ by $\theta(x) = (x^T)^{-1}$. We also use the following special matrices.

$$L_p = \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix}$$

$$L_{\frac{n}{2},p} = \begin{bmatrix} \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix} & & \\ & \ddots & \\ & & \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix} \end{bmatrix}$$

$$L_{m,c^2,c} = \begin{bmatrix} \begin{bmatrix} 0 & 1 \\ c^2 & 0 \end{bmatrix} & & & & & \\ & \ddots & & & & \\ & & \begin{bmatrix} 0 & 1 \\ c^2 & 0 \end{bmatrix} & & & \\ & & & c & & \\ & & & & \ddots & \\ & & & & & c \end{bmatrix}$$

For $\mathrm{SL}(2,k)$, the k-involutions are:

1. $\mathrm{Inn}(L_p)$ where $p \in k$.

For $\mathrm{SL}(n,k)$, the k-involutions are:

1. For $k = \mathbb{F}_q$ or $k = \overline{k}$, one of
   (a) $\mathrm{Inn}(L_{m,c^2,c})$ for some $c \in k$.
   (b) θ.
2. For $k = \mathbb{F}_q(x)$, or any field k which is neither finite nor algebraically closed, the k-involutions are as follows:
   (a) $\mathrm{Inn}(L_{m,c^2,c})$ for some $c \in k$.
   (b) $\mathrm{Inn}(L_{\frac{n}{2},p})$ for some $p \in k$.
   (c) $\theta\,\mathrm{Inn}(A)$ where A is $\mathrm{Diag}(1,\ldots,1,N_{p_1},\ldots,N_{p_r})$ where N_{p_i} are (not necessarily unique) non-squares in k, and $0 \le r \le n$.

For $\mathrm{O}(2n+1,k)$, the k-involutions satisfy:

1. $\mathrm{Inn}(A)$ where $A^2 \in \mathrm{St}(2n+1,\overline{k})$ and $A^T A \in \mathrm{St}(2n+1,\overline{k})$.

Chapter 2

Background & Related Results

The main goal of this dissertation is to understand involutions, so we begin with a definition:

Definition 2.0.1. Let G be a group and $\varphi : G \to G$ be an automorphism of order exactly 2. Then φ is called an *involution* of G.

This dissertation concerns classifying and characterizing k-involutions of linear algebraic groups. In particular, these groups are defined over fields of characteristic 2, most of which are finite fields, so the groups can be very different from Lie groups. For example, the notions of compactness and connectedness do not apply. Linear algebraic groups are groups of matrices, so one expects to use standard linear algebra results; however, in characteristic 2, some of the matrix theory does not apply. Because the field is not ordered, there are no norms in the traditional sense; this complicates the process of finding orthonormal bases of eigenvectors, for instance. Many properties which are true for real or complex matrices are false. Another significant difference is that many of the standard facts about bilinear and quadratic forms no longer hold, further complicating matters for the orthogonal groups. We will address the main concerns and differences in this chapter, comparing and contrasting with the real and complex cases in the process.

This project is a small part of a large, collected effort to classify and characterize symmetric spaces and their several generalizations. Much work has already been completed, leading to many useful results, especially for the 'nice' fields. The final section of this chapter contains an outline of some closely related results. In the subsequent chapters, we will refer to the related results, draw comparisons, and highlight contrasting differences in the characteristic 2 case. Some directly related work has been completed by the joint efforts of Ling Wu, Christopher Dometrius, and Robert Benim (summarized and expanded upon in [5]); they are current or former Ph.D. students of Aloysius Helminck. The general background and theory has been developed over the past century by many mathematicians, and Helminck has made important

contributions to the area. This work is a natural extension of Helminck's work.

Our basic references for Lie groups is Brian Hall [17], and for algebraic groups Borel [6] and Humphreys [27]. When possible, we follow their terminology and notation. For groups defined over finite fields, we make frequent reference to Wilson [38] and Dieudonné [12]. For bilinear and quadratic forms and the orthogonal groups, Wilson [38] is again helpful, as well as books by Sharlau [32] and Dieudonné. Basic linear algebra facts may be found in the excellent book by Hoffman and Kunze [26]; slightly more advanced explanations may be found in the book by Roman [31]. Most of the general abstract algebra notation is consistent with that used by Artin in [3]; his book contains useful and relevant examples manywhere.

2.1 Lie Groups

For this entire section, let $k = \mathbb{R}$ or $\mathbb{C}$.

Definition 2.1.1. A *matrix Lie group* G is any closed subgroup of $\mathrm{GL}(n, k)$.

By *closed*, we mean a convergent sequence of matrices $A_n \to A$, $A_n \in G$ implies that $A \in G$ or else A has no inverse. It is clear that this property holds for the general linear groups $\mathrm{GL}(n, k)$. It is basically a technicality that we require a subgroup of $\mathrm{GL}(n, k)$ be closed; most of the interesting subgroups of $\mathrm{GL}(n, k)$ are closed anyway.

The special linear groups $\mathrm{SL}(n, k)$ are the groups of $n \times n$ invertible matrices with determinant 1. Since the determinant is a continuous function, and any sequence A_n of matrices with determinant 1 converges to a matrix with determinant 1, the special linear groups are also Lie groups.

Before we define the orthogonal groups $\mathrm{O}(n, k)$, we will need some additional terminology and definitions pertaining to bilinear forms.

Definition 2.1.2. Let V be a vector space over k. A *bilinear form* B is a mapping

$$B : V \times V \to k$$

that is linear in each coordinate. That is, for scalars α and β,

$$B(\alpha u + \beta v, w) = \alpha B(u, w) + \beta B(v, w)$$
$$B(w, \alpha u + \beta v) = \alpha B(w, u) + \beta B(w, v).$$

A bilinear form B is called *symmetric* if $B(u, v) = B(v, u)$ for all $u, v \in V$, *skew-symmetric* if $B(u, v) = -B(v, u)$ for all $u, v \in V$, and *alternating* if $B(u, u) = 0$ for all $u \in V$.

Definition 2.1.3. A matrix A is *orthogonal* if $A^TA = \mathrm{Id}$. A more general way to describe orthogonal matrices is that they are the matrices which preserve the form B in the sense that $B(Ax, Ay) = B(x, y)$ for all $x, y \in V$. This is equivalent to saying that the columns of A are orthonormal, i.e., $B(A_i, A_j) = \delta_{i,j}$ for all columns A_i and A_j of A.

Given a particular basis $\mathcal{B}$ of V, the bilinear form B can be uniquely represented by a matrix M so that $B(u, v) = u^TMv$. If $\mathcal{B} = \{v_1, \ldots, v_n\}$, then $M_{i,j} = B(v_i, v_j)$. Orthogonality is independent of the choice of basis.

Example 2.1. The standard dot product on k^n is a bilinear form with $B(u, v) = u^Tv$. So $M = \mathrm{Id}$, and the dot product is non-degenerate. A matrix A is orthogonal with respect to the dot product if and only if $A^TA = \mathrm{Id}$. □

Definition 2.1.4. A bilinear form B is said to be *non-degenerate* if, whenever $B(u, v) = 0$ for all $v \in V$, then $u = 0$.

Consequently, the matrix M of B is non-singular exactly when B is non-degenerate. When B is symmetric, skew-symmetric, or alternating, the pair (V, B) is called an *inner product space*. When B is symmetric M is a symmetric matrix, when B is skew-symmetric M is skew-symmetric, and when B is alternating M is skew-symmetric with zero diagonal. The dot product is a symmetric bilinear form, since $M = \mathrm{Id}$ in this case.

Definition 2.1.5. We say a vector u is *perpendicular* to a vector v (and we write $u \perp v$) if $B(u, v) = 0$. The *radical* of V, denoted $\mathrm{rad}(B)$ or $V^\perp$, is the set $\{v \in V \mid v \perp w,\ \forall\ w \in V\}$.

Two matrices represent the same bilinear form (with respect to different bases of V) if they are congruent, i.e., $B_1 \cong B_2$ if and only if $M_1 = P^TM_2P$, where P is some invertible matrix.

Definition 2.1.6. Let V and W be vector spaces. An *isometry* is a bijective linear map $\varphi : V \to W$ such that $B\big(\varphi(u), \varphi(v)\big) = B(u, v)$.

We are ready to define the orthogonal groups when k is not a field of characteristic 2.

Definition 2.1.7. If $\varphi : V \to V$ is an isometry of (V, B) then φ is called an *orthogonal transformation*. The set, $\mathrm{O}(V, B)$, of orthogonal transformations on V is a group under composition; it is called the *orthogonal group* of V with respect to B.

Definition 2.1.8. The group of orthogonal transformations all have determinant 1 or -1. Those having determinant 1 form a subgroup of $\mathrm{O}(V, B)$ called the *special orthogonal group*, denoted $\mathrm{SO}(V, B)$.

In the Lie group case, $k = \mathbb{R}$ or $k = \mathbb{C}$ and $V = k^n$, we write $\mathrm{O}(n, k)$ and $\mathrm{SO}(n, k)$. If B happens to be an alternating bilinear form, then φ is a *symplectic* transformation. The group of all symplectic transformations on V is called the *symplectic group* of V, and we denote it by $\mathrm{Sp}(V)$.

The properties of the underlying field determine relationships between symmetric, skew-symmetric, and alternating bilinear forms. In particular, if the field k has characteristic not 2, alternating forms are also skew-symmetric forms.

As we saw above, the definition of the orthogonal groups depends on the symmetric bilinear form. Thus, to classify orthogonal groups in general, a classification of symmetric bilinear forms is needed. This classification may be found in the book by Roman (see [31], Chapter 11). There are a couple of relevant facts. First, as we have noted, symmetric bilinear forms have symmetric matrices. Second, symmetric matrices are congruent to diagonal matrices. Third, diagonal matrices are congruent to diagonal matrices whose entries are either 1, -1, or at most a single non-square entry. These facts can be combined to give a general classification of non-degenerate, symmetric bilinear forms, in terms of their matrices:

1. For algebraically closed fields ($\mathbb{C}$, eg.) we have

$$M_B = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}.$$

2. For $k = \mathbb{R}$ we have

$$M_B = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & -1 & & \\ & & & & \ddots & \\ & & & & & -1 \end{bmatrix},$$

where there are i ones and j negative ones on the diagonal such that $i + j = n$. The number j of negative ones is called the *signature* of the form.

3. For k a finite field (not of characteristic 2) we have

$$M_B = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & d \end{bmatrix}$$

where d is either a non-square and has no square factors, or else $d = 1$.

As mentioned above, two symmetric bilinear forms are equivalent (up to a change of basis) if and only if their matrices are congruent. This is analogous to linear operators being equivalent if and only if their matrices are conjugate. Hence the classification of symmetric bilinear forms essentially classifies the orthogonal groups, except in the case that k has characteristic 2. Since our main groups of interest are $\mathrm{GL}(n, k)$, $\mathrm{SL}(n, k)$ and $\mathrm{O}(n, k)$, we are almost ready to proceed to a discussion of these groups over fields of characteristic 2. But first we give a short treatment of finite fields and also of general properties of fields of characteristic 2.

2.2 Finite Fields

Richard Dedekind was allegedly the first to call the real numbers and complex numbers a "field." In French, the word used for "field" is "corps," which means "body"; in German the word for body is "Körper," which may be why the symbol k is often used to denote an arbitrary field. In some of the literature, there are references made to "sfields" or a "skew fields." The modern terminology is "division ring." *Division rings* are essentially fields in which multiplication is non-commutative. We do not need to consider division rings in this dissertation.

Throughout this section, unless otherwise specified, we will assume k is an arbitrary field of characteristic 2, K is an extension field of k, and $\overline{k}$ is the algebraic closure of k. Finite fields are not the only fields of characteristic 2, but they are (in some ways) the easiest to work with. Most of the examples in this dissertation are of linear algebraic groups defined over finite fields. This section is a summary of the important facts about finite fields. We also explain how finite fields are extended to larger fields, and how to construct fields of fractions of finite fields.

Definition 2.2.1. The integers modulo a prime p is a field, called a *prime field*.

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, 3, \ldots, (p-1)\}.$$

All fields with p elements are identical (up to isomorphism). We denote the prime fields by $\mathbb{F}_p$ and the non-zero elements of $\mathbb{F}_p$ by $\mathbb{F}_p^*$.

Lemma 2.2.2 (Artin [3]). *There are $p-1$ non-zero elements of $\mathbb{F}_p$ that form a cyclic group under multiplication.*

Prime fields can be extended to fields whose order is a power of p. This is accomplished by adjoining the roots of an irreducible polynomial $f(x)$ whose coefficients are in the prime field $\mathbb{F}_p$. Let $r \in \mathbb{N}$ and $q = p^r$. The new field $\mathbb{F}_q$ consists of $\mathbb{F}_p$, the *prime subfield* of $\mathbb{F}_q$, and all linear combinations of the roots of f. All finite fields have the form $\mathbb{F}_q$, and whenever q is a prime power there is a field of order q that is isomorphic to $\mathbb{F}_q$. As in Lemma 2.2.2, the non-zero elements form a cyclic group of order $q-1$.

Definition 2.2.3. When $p = 2$, the finite fields $\mathbb{F}_q$ are called fields of even characteristic, binary fields, or *fields of characteristic 2.*

The finite field $\mathbb{F}_2 = \{0, 1\}$ is the smallest of all finite fields. Extension fields of $\mathbb{F}_2$ are straightforward. The polynomial $f(x) = x^r + x + 1$ is always irreducible over $\mathbb{F}_2$; the roots of $f(x)$ generate $\mathbb{F}_{2^r}$. Following are several useful facts about fields of characteristic 2.

Lemma 2.2.4 (J-P. Serre, [33]). *Let $k = \mathbb{F}_{2^r}$. Let k^* denote the set of nonzero elements of k. Every element of k^* is a square. Hence $|k^*/(k^*)^2| = 1$.*

Proof. Consider the Frobenius homomorphism $\varphi : k \to k$ given by $x \mapsto x^2$. This is a ring homomorphism since $(x+y)^n = x^n + y^n$ (all the other binomial coefficients are zero in the expansion) and $(xy)^n = x^n y^n$. Moreover, φ is surjective since $1 \in \mathrm{Im}(\varphi)$, which is an ideal of k. Therefore, $\ker \varphi = \{0\}$ and φ is an automorphism of k. ■

The *algebraic closure* of a field k is the smallest field $\overline{k}$ which contains k and the roots of all polynomials whose coefficients are in k. The algebraic closure of the finite field $\mathbb{F}_{p^r}$ is an infinite field constructed by taking the union of all fields $\mathbb{F}_{p^n}$ for any $n \in \mathbb{N}$. That is

$$\overline{\mathbb{F}_p} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}.$$

Lemma 2.2.4 holds for the algebraic closure of $\mathbb{F}_q$, since every element of the algebraic closure is also an element of a finite field.

Another extension of finite fields is the quotient field $\mathbb{F}_p[x]/(f)$ where f is an irreducible polynomial. Since $f(x)$ is irreducible over $\mathbb{F}_p$, (f) is a maximal ideal. Therefore $\mathbb{F}_p[x]/(f)$ is a field.

Lemma 2.2.5. *Every nonzero element of a finite field k of characteristic 2 has a unique square root.*

Proof. Let $x = p^2$ and $x = q^2$. Then $p^2 = q^2$ and hence $(p+q)(p+q) = 0$. Since k is a field, it is a unique factorization domain and there are no zero divisors. Thus $p = q$. ■

Lemma 2.2.6. *When k has characteristic 2, the equation $(x+y)^n = x^n + y^n$ is always true.*

Occasionally we will need to differentiate between results that hold for perfect fields only. The fields of rational functions $k(x)$ are imperfect fields when the characteristic of the field is positive. Otherwise, all fields encountered in this dissertation are perfect.

We now turn our discussion towards the groups $\mathrm{GL}(n,k)$, $\mathrm{SL}(n,k)$, and $\mathrm{O}(n,k)$ over fields of characteristic 2.

2.3 Algebraic Groups in Characteristic 2

In terms of definitions, the general linear group $\mathrm{GL}(n,k)$ and the special linear group $\mathrm{SL}(n,k)$ are essentially the same as over fields characteristic 2. The classification of involutions of symplectic groups will be the object of some future work. But, the even dimensional symplectic groups turn out to be useful in classifying automorphisms of orthogonal groups when k has characteristic 2. The following theorem gives the order of general and special linear groups when k is finite and of characteristic 2.

Theorem 2.3.1 (Robinson [30], 3.2.7)**.** *Let $q = 2^r$ for some $r \in \mathbb{N}$. Then*

1. $|\mathrm{GL}(n,\mathbb{F}_q)| = \prod_{i=1}^{n} \left(q^n - q^{i-1}\right).$
2. $|\mathrm{SL}(n,\mathbb{F}_q)| = \dfrac{|\mathrm{GL}(n,\mathbb{F}_q)|}{(q-1)}.$

Proof.

1. An invertible, $n \times n$ matrix can be constructed as follows. For entries in the first row, we may choose any combination except all zeros. There are $q^n - 1$ ways to do this. For the second row, we may choose any combination of elements except for scalar multiples of the first row. There are $q^n - q$ ways to do this. For the i-th row, we may choose any combination of elements provided that the result is not a linear combination of the first $i-1$ rows. There are $q^n - q^{i-1}$ ways to do this.

2. The determinant function $\det(X) \mapsto \mathbb{F}_q$ is a surjective homomorphism whose kernel is $\mathrm{SL}(n,\mathbb{F}_q)$. The formula follows directly from the first isomorphism theorem and the counting formula (see [3], p.58 and p.68).

■

The differences between orthogonal groups over characteristic 2 begin with the definition of the group. We must use quadratic forms instead of symmetric bilinear forms to construct

the orthogonal groups. Moreover, all determinants are $+1$, so $\mathrm{O}(n,k) = \mathrm{SO}(n,k)$. Our basic references for this section will be Wilson [38], Scharlau [32], Dieudonné [12], and Grove [16]. After more than 50 years, Dieudonné's book still seems to be the go-to reference for information on automorphisms of the classical groups. It's not as helpful for fields of characteristic 2 in the orthogonal case, but it does give us some information in the odd dimensional case because $\mathrm{O}(2n+1,k) \cong \mathrm{Sp}(2n,k)$ when k is a perfect field. Scharlau's book should probably be considered the bible of quadratic forms, and he gives a lot of details, though not always presented with the same terminology as more modern sources. Wilson gives a fairly complete account of the properties of finite simple groups in general, and classical groups in particular, though he omits certain details. Grove's account of classical groups over arbitrary fields is also quite useful.

For a field whose characteristic is not 2, symmetric bilinear forms are in a one-to-one correspondence with quadratic forms, and it is simple to determine one form if given the other. Thus a classification of symmetric bilinear forms is equivalent to a classification of quadratic forms, which classifies the orthogonal groups. In characteristic 2, quadratic forms and bilinear forms are not in $1-1$ correspondence. Thus, it is impossible to recover the quadratic form from a given symmetric bilinear form. Moreover, the definition of symmetric bilinear form does not "capture the interesting geometrical (and group theoretical) phenomena" [38]. Thus, in order to classify orthogonal groups over fields of characteristic 2, a classification of quadratic forms is needed.

Orthogonal groups are different according to the parity of the dimension. Over characteristic 2, $\mathrm{O}(2n+1,k) \cong \mathrm{Sp}(2n,k)$, if k is a perfect field (see [16], Theorem 14.2, p. 129). This applies to all finite fields of characteristic 2, as well as their algebraic closure, but it does not include the function fields $k(x)$, where k is a field of characteristic 2 and x is an indeterminant (or a vector of indeterminants). So the automorphisms in the odd dimensional case are the same as those of the even dimensional symplectic group. A description of these automorphisms can be found in Dieudonné [12], as summarized below.

Definition 2.3.2. A *semi-linear transformation* is a function $T : V \to V$ such that

1. $T(u+v) = T(u) + T(v)$
2. $T(au) = a^{\sigma} T(u)$

where σ is an automorphism of the field k, and a^{σ} denotes the image of a under σ.

Theorem 2.3.3 (Dieudonné [12], Theorem 9, p. 31)**.** *Every automorphism of* $\mathrm{Sp}(2m,k)$ *($m \geq 2$ and $m \neq 2$ if k has only two elements) is of the form $X \mapsto TXT^{-1}$, where T is a $1-1$ semi-linear transformation of V onto itself relative to an automorphism σ of k, and such that $\big(T(X), T(Y)\big) = \lambda(X,Y)^{\sigma}$ for all $X, Y \in V$ and for some $\lambda \in k$.*

Wilson provides the following formula for the order of the odd-dimensional orthogonal groups over finite fields of characteristic 2 (see [38], p. 60, (3.22)). Grove also proves the same formula (see [16] Theorem 3.12, p.27).

Theorem 2.3.4.

$$|\mathrm{O}(2n+1, \mathbb{F}_q)| = q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)$$

The symplectic group $\mathrm{Sp}(2m, k)$ is generated by symplectic transvections, as asserted by Wilson, and given an isomorphism between $\mathrm{Sp}(2m, k)$ and $\mathrm{O}(2n+1, k)$ we obtain information about the odd-dimensional orthogonal groups.

Definition 2.3.5 (Wilson [38], p. 61)**.** A *symplectic transvection* is a linear map

$$T_v(\lambda) : x \mapsto x + \lambda B(x, v)v,$$

where B is a fixed symplectic (i.e. non-singular alternating bilinear) form on V and $v \neq 0$ and $\lambda \neq 0$.

We proceed to the even-dimensional case. In what follows, we collect the necessary facts about quadratic forms from relevant sections of Wilson's book on finite groups (see [38]) and Scharlau's book on quadratic and hermitian forms (see [32]). There are only two forms when $k = \mathbb{F}_{2^r}$; thus there are two orthogonal groups in even dimension. So we begin with a classification of quadratic forms over fields of characteristic 2.

Definition 2.3.6. A *quadratic form* is a map $q : V \to k$ such that

$$q(au + v) = a^2 q(u) + aB_q(u, v) + q(v)$$

where B_q is a symmetric bilinear form called the *associated form*.

The associated form B_q can be recovered from q when the characteristic of k is not 2 by $q(v) = \frac{1}{2}B_q(v, v)$. When k has characteristic 2, the reverse correspondence does not hold; that is, the quadratic form cannot be recovered from the bilinear form. Moreover, in characteristic 2, the associated form B_q is alternating since

$$0 = q(2v) = q(v + v) = q(v) + B_q(v, v) + q(v) = B_q(v, v).$$

Definition 2.3.7. A non-zero vector u is said to be *isotropic* if it is perpendicular to itself; that is, if $B(u, u) = 0$. A space is said to be *totally isotropic* if it consists entirely of isotropic vectors. Analogously, and with respect to a quadratic form, we say that a vector is *isotropic* if $q(u) = 0$.

When k has characteristic different from 2, the notion of isotropic is the same regardless of whether the form is quadratic or symmetric bilinear. However, this is not true for characteristic 2.

Definition 2.3.8. The *radical* of q is the set $\operatorname{rad}(q) = \{v \in \operatorname{rad}(f) \mid q(v) = 0\}$.

In analogy with bilinear forms, q is called *non-singular* if $\operatorname{rad} q = \{0\}$ and *non-degenerate* or *non-defective* if $\operatorname{rad} f = \{0\}$.

There are two main methods used to classify quadratic forms over fields of characteristic 2. The method used by Scharlau [32] is called the *Arf invariant*. There exists a *symplectic basis* $e_1, e_2, \ldots, e_m, f_1, f_2, \ldots, f_m$ of V with respect to q (see [32], Chapter 7.8, eg.). In other words, $b_q(e_i, f_i) = 1$ and all other pairs are orthogonal (with respect to b_q). Collectively, this means we can write the matrix $Q = (q_{i,j})$ of q where

$$q_{ij} = \begin{cases} q(e_i) & \text{if } i = j \\ b_q(e_i, e_j) & \text{if } i < j \\ 0 & \text{if } i > j \end{cases}$$

and Q has the form

$$Q = \begin{bmatrix} \begin{bmatrix} \alpha_1 & 1 \\ 0 & \beta_1 \end{bmatrix} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \begin{bmatrix} \alpha_m & 1 \\ 0 & \beta_m \end{bmatrix} \end{bmatrix},$$

where $\alpha_i = q(e_i)$ and $\beta_i = q(f_i)$.

We also have the following theorem due to Arf [2]. For a proof, see Scharlau [32], (Theorem 9.4.2, p. 340).

Theorem 2.3.9 (Arf)**.** *Let q be a non-degenerate quadratic form on a vector space V with dimension $n = 2m$ with symplectic basis as above. Set $\mathcal{P}(k) = \{\gamma^2 + \gamma \mid \gamma \in k\}$. Then the class Δ of $q(e_1)q(f_1) + \cdots + q(e_m)q(f_m)$ in $k/\mathcal{P}(k)$ is independent of the choice of symplectic basis.*

Definition 2.3.10. The element $\Delta(V, q) = \sum_{i=1}^{m} q(e_i)q(f_i)$ is called the *Arf invariant* of V with respect to q.

With the previous definition in hand, we are able to characterize quadratic spaces in the following theorem.

Theorem 2.3.11 (Scharlau, 9.4.5)**.** *For perfect fields k of characteristic 2, quadratic spaces are classified by dimension and Arf invariant.*

Definition 2.3.12. A *reflection* is a map

$$r_v : x \mapsto x - 2\frac{B(x,v)}{B(v,v)}v$$

which fixes all vectors orthogonal to v and maps $\langle v \rangle$ to $-\langle v \rangle$. Obviously r_v is undefined for characteristic 2. Instead we replace it by an *orthogonal transvection*, which is a map

$$t_v : x \mapsto x + \frac{B_q(x,v)}{q(v)}v,$$

where v is not isotropic. Orthogonal transvections are often called reflections in the literature.

Now, according to Scharlau, if k is finite of characteristic 2, then $\mathrm{O}(n,k)$ is a subset of $\mathrm{Sp}(n,k)$. We use the *Dickson invariant* as a replacement for the determinant. Letting $\sigma \in \mathrm{O}(n,k)$, this is defined as

$$\Delta : \mathrm{O}(n,k) \to \{0,1\},$$

with $\Delta(\sigma) = 0$ or 1 depending on whether or not σ can be written as a product of an even or odd number of orthogonal transvections. Except for the case that $k = \mathbb{F}_2$ and $n = 4$, (with k assumed finite, characteristic 2), $\mathrm{O}(n,k)$ is generated by orthogonal transvections ([32], Theorem 9.4.12, p.345).

For finite fields of characteristic 2, and the dimension of V is $n = 2m$, there are two non-singular, quadratic forms. They are distinguished by *plus type* and *minus type* depending on the value of the Dixon invariant.

In summary, if k is finite and of characteristic 2, there are two orthogonal groups in even dimension. Furthermore, excepting the case that $k = \mathbb{F}_2$ and $n = 4$, the orthogonal groups are all generated by orthogonal transvections. The even-dimensional orthogonal groups are $\mathrm{O}^+(2m, \mathbb{F}_{2^r})$ and $\mathrm{O}^-(2m, \mathbb{F}_{2^r})$, and their orders are

$$|\,\mathrm{O}^+(2m, \mathbb{F}_{2^r})| = 2q^{m(m-1)}(q^2-1)(q^4-1)\cdots(q^{2m-2}-1)(q^m-1)$$

$$|\,\mathrm{O}^-(2m, \mathbb{F}_{2^r})| = 2q^{m(m-1)}(q^2-1)(q^4-1)\cdots(q^{2m-2}-1)(q^m+1).$$

For details, see Wilson [38], (3.39) on p. 77 or Grove [16], Theorem 14.48, p. 149. Moreover, if we know how to write an element as a product of orthogonal transvections, we know which group contains the element. The literature does not appear to provide hints on how to decompose elements as products of reflections.

2.4 Summary of Related Results

Let k be algebraically closed, finite or $\mathfrak{p}$-adic. We summarize the following results from papers by Wu (see [39]), Dometrius (see [14]) and Benim (see [5]). Let

$$I_{s,t} = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & -1 & & & \\ & & & & \ddots & & \\ & & & & & -1 & \end{bmatrix}$$

where there are s plus ones and t minus ones such that $s + t = n$. Also, let

$$L_{n,q} = \begin{bmatrix} \begin{bmatrix} 0 & 1 \\ q & 0 \end{bmatrix} & & & \\ & \ddots & & \\ & & \begin{bmatrix} 0 & 1 \\ q & 0 \end{bmatrix} & \end{bmatrix}$$

be a block diagonal matrix of dimension $2n \times 2n$. When $q = -1$ we write

$$J_n = \begin{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} & & & \\ & \ddots & & \\ & & \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} & \end{bmatrix}.$$

Finally, we have the $n \times n$ diagonal matrix

$$K_{n,x,y,z} = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & x & & \\ & & & & y & \\ & & & & & z \end{bmatrix}$$

where there are $n-3$ ones. We will also write $M_{n,x}$ for $K_{n,1,1,x}$ and $N_{n,x,y}$ for $K_{n,1,x,y}$.

2.4.1 k-involutions of $\mathrm{SL}(2,k)$

All k-involutions are inner, and representatives of isomorphism classes are $\left[\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right]$, where p is a non-square in k. The fixed point groups of these k-involutions are

$$H^q = \left\{ \begin{bmatrix} x & y \\ ay & x \end{bmatrix} \middle| x^2 - qy^2 = 1 \right\}$$

2.4.2 k-involutions of $\mathrm{SL}(n,k)$, $n > 2$

Here we have both inner and outer automorphisms of $G = \mathrm{SL}(n,k)$. Since $|\operatorname{Aut}(G)/\operatorname{Inn}(G)| = 2$ and $\theta : G \to G$ by $\theta(X) = (X^{-1})^T$ is always in $\operatorname{Aut}(G)$, representatives of $\operatorname{Aut}(G)$ are of the form $\theta \operatorname{Inn}(A)$ where $\operatorname{Inn}(A) \in \operatorname{Inn}(G)$. The k-involutions belong to the following cases:

1. k is algebraically closed.

   - If n is odd, there are $\frac{n+1}{2}$ isomorphism classes of k-involutions. Representatives are $\operatorname{Inn}(I_{n-i,i})$ and θ, $i = 1, 2, \ldots, \frac{n-1}{2}$.
   - If n is even, there are $\frac{n}{2} + 2$ isomorphism classes of k-involutions. Representatives are $\operatorname{Inn}(I_{n-i,i})$ with $i = 1, 2, \ldots, \frac{n}{2}$, θ and $\theta \operatorname{Inn}(J_n)$.

2. k is the real numbers $\mathbb{R}$.

   - If n is odd, there are n isomorphism classes of k-involutions. Representatives are θ, $\operatorname{Inn}(I_{n-i,i})$ for $i = 1, 2, \ldots, \frac{n-1}{2}$, and $\theta \operatorname{Inn}(I_{n-i,i})$.
   - If n is even, there are $n+3$ isomorphism classes of k-involutions. Representatives are $\operatorname{Inn}(J_n)$, θ, $\theta \operatorname{Inn}(J_n)$, $\operatorname{Inn}(I_{n-i,i})$ and $\theta \operatorname{Inn}(I_{n-i,i})$ with $i = 1, 2, \ldots, \frac{n}{2}$.

3. k is a finite field, $\mathbb{F}_p$, $p \neq 2$. Let N_p be a non-trivial representative of $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$.

   - If n is odd, there are $\frac{n-1}{2} + 2$ isomorphism classes of k-involutions. Representatives are θ, $\operatorname{Inn}(I_{n-i,i})$, $\theta \operatorname{Inn}(M_{n,N_p})$, where $i = 1, 2, \ldots, \frac{n-1}{2}$.
   - If n is even, there are $\frac{n}{2} + 4$ isomorphism classes of k-involutions. Representatives are $\operatorname{Inn}(I_{n-i,i})$, $\operatorname{Inn}(L_{n,N_p})$, $\theta \operatorname{Inn}(J_n)$ and $\theta \operatorname{Inn}(M_{n,N_p})$, $i = 1, 2, \ldots, \frac{n}{2}$.

4. k is the $\mathfrak{p}$-adic numbers. If $p \neq 2$ then we take 1, p, N_p, and pN_p as representatives of $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. If $p = 2$, we take the representatives $1, -1, 2, -2, 3, -3, 6, -6$ instead.

   - If n is even, there are $\frac{n}{2} + 9$ isomorphism classes of involutions for $p \neq 2$ and $\frac{n}{2} + 17$ for $p = 2$. Representatives are

– For $p \neq 2$, $\mathrm{Inn}(I_{n-i,i})$, $\mathrm{Inn}(B)$, θ, $\theta\,\mathrm{Inn}(C)$, and $\theta\,\mathrm{Inn}(D)$. Here we have $i = 1, 2, \ldots, \frac{n}{2}$, B is $L_{n,x}$, and C is $M_{n,x}$ where $x = N_p$, p or pN_p. For D, it is slightly more complex:

$$D = \begin{cases} K_{n,p,N_p,pN_p} & \text{if } -1 \in \mathbb{Q}_p^2 \\ N_{n,p,p} & \text{if } -1 \notin \mathbb{Q}_p^2 \text{ and } n = 4k \\ N_{n,p,p,N_p} & \text{if } -1 \notin \mathbb{Q}_p^2 \text{ and } n = 4k+2 \end{cases}.$$

– For $p = 2$, we have the same as above, but x is now chosen from 1, -1, 2, -2, 3, -3, 6, or -6 instead. Also D is again slightly more complex:

$$D = \begin{cases} I_{n-2,2} & \text{if } n = 4k \\ K_{n,2,3,-6} & \text{if } n = 4k+2 \end{cases}.$$

- If $n = 4k+1$ there are $\frac{n-1}{2} + 2$ isomorphism classes of k-involutions if $-1 \in \mathbb{Q}_p^2$; otherwise there are $\frac{n-1}{2} + 1$. Representatives are $\mathrm{Inn}(I_{n-i,i})$, θ, and possibly $\mathrm{Inn}(D)$ if $-1 \in \mathbb{Q}_p^2$. Here D is K_{n,p,N_p,pN_p}, and $i = 1, 2, \ldots, \frac{n-1}{2}$.
- If $n = 4k+3$, there are $\frac{n-1}{2}+2$ isomorphism classes of k-involutions. Representatives are $\mathrm{Inn}(I_{n-i,i})$, θ, and $\theta\,\mathrm{Inn}(D)$ where $i = 1, 2, \ldots, \frac{n-1}{2}$ and D is again complicated:

$$D = \begin{cases} K_{n,p,N_p,pN_p} & \text{if } -1 \in \mathbb{Q}_p^2 \\ N_{n,p,p} & \text{if } -1 \notin \mathbb{Q}_p^2 \\ I_{n-2,2} & \text{if } p = 2 \end{cases}.$$

2.4.3 k-involutions of $\mathrm{SO}(n,k)$

We now summarize the results on the special orthogonal groups $\mathrm{SO}(n,\beta,k)$ that were obtained by the combined efforts of Wu, Dometrius, Benim, and Helminck; the results are collected in [5]. The authors determined four possible types of inner k-involutions. The k-involutions corresponding different types are not isomorphic. As with the case of $G = \mathrm{SL}(2,k)$, all k-involutions of $\mathrm{SO}(n,\beta,k)$ are inner. This follows from a proposition due to Borel [6].

Fix a bilinear form β with matrix M. If $A \in \mathrm{GL}(n,k)$ is a matrix such that $M^{-1}A^TMA = \alpha\,\mathrm{Id}$, then we call A α-orthogonal. Note that orthogonal matrices are 1-orthogonal.

The inner k-involutions of $\mathrm{SO}(n,k)$ come from conjugation by a matrix A which is in either $\mathrm{O}(n,k,\beta)$ or $\mathrm{O}(n,k[\sqrt{\alpha}],\beta)\setminus \mathrm{O}(n,k,\beta)$. A has the additional property that $A^2 = \pm 1$, so this gives four cases, as shown in Figure 2.1.

The type that is of most interest to us (and most relevant) is Type 1 since we are interested in the odd-dimensional orthogonal groups, and since we will never have $A^2 = -\,\mathrm{Id}$ over charac-

	$A \in \mathrm{O}(n,k,\beta)$	$A \in \mathrm{O}(n,k[\sqrt{\alpha}],\beta) \setminus \mathrm{O}(n,k,\beta)$
$A^2 = \mathrm{Id}$	Type I	Type 2
$A^2 = -\mathrm{Id}$	Type 3	Type 4

Table 2.1: List of Types of Inner k-involutions

teristic 2 fields. The inner k-involutions of Type 1 come from conjugation by a matrix A such that $A^2 = \mathrm{Id}$,

$$A = XI_{s,t}X^{-1},$$

where $X \in \mathrm{GL}(n,k)$ and X has columns of orthogonal eigenvectors of A, and

$$I_{s,t} = \begin{bmatrix} -\mathrm{Id}_s & 0 \\ 0 & \mathrm{Id}_t \end{bmatrix},$$

where $s + t = n$ and $s \leq t$. If the matrix of β is M, then $X^T MX$ is diagonal. The following theorem classifies the isomorphism classes of Type 1 inner k-involutions.

Theorem 2.4.4 ([5], Theorem 4.3)**.** *Suppose ϑ and φ are two Type 1 k-involutions of $\mathrm{SO}(n,k,\beta)$ where $\vartheta = \mathrm{Inn}(A)$ and $\varphi = \mathrm{Inn}(B)$. Then, $A = XI_{m_A,n-m_A}X^{-1}$ and $B = YI_{m_B,n-m_B}Y^{-1}$ where X and $Y \in \mathrm{GL}(n,k)$ with columns that are orthogonal eigenvectors of A and B, respectively. We also have the diagonal matrices*

$$X^T MX = \begin{bmatrix} X_1 & 0 \\ 0 & X_2 \end{bmatrix}$$

and

$$Y^T MY = \begin{bmatrix} Y_1 & 0 \\ 0 & Y_2 \end{bmatrix}.$$

The following are equivalent:

1. *ϑ is congruent to φ over $\mathrm{SO}(n,k,\beta)$*
2. *A is conjugate to B over $\mathrm{SO}(n,k,\beta)$*
3. *X_1 and Y_1 are both $m \times m$ matrices, X_1 is congruent to Y_1 over $\mathrm{GL}(m,k)$ and X_2 is congruent to Y_2 over $\mathrm{GL}(n-m,k)$*
4. *If $k = \mathbb{Q}_p$, there exists some $\gamma \in \mathbb{Q}_p$ such that $\det(X_1) = \gamma^2 \det(Y_1)$, $\det(X_2) = \gamma^2 \det(Y_2)$, $c_p(X_1) = c_p(Y_1)$ and $c_p(X_2) = c_p(Y_2)$*

where $c_p(M)$ denotes the Hasse symbol of the matrix M.

Chapter 3

k-involutions of $\mathrm{SL}(2,k)$

In this chapter let k be a field of characteristic 2, let $K \supset k$ be an extension field of k, and let $\overline{k}$ be the algebraic closure of k; thus $k \subset K \subseteq \overline{k}$. Let $G = \mathrm{SL}(2,\overline{k})$, $G_k = \mathrm{SL}(2,k)$, and $G_K = \mathrm{SL}(2,K)$. We first characterize the k-involutions of G_k, and then use the characterization to classify k-involutions of G_k.

In his Ph.D. dissertation [39] Wu characterized and classified k-involutions of G_k for perfect fields k of characteristic not 2. In this dissertation, we find several similarities and differences in the classification as compared to the classification in [39]. Because $2 = 0$ and $1 = -1$, we also find differences in many proofs of analogous results.

In order to determine the k-involutions of G_k, we first determine which automorphisms of G_K fix G_k point-wise. Next, we establish which automorphisms of G_K fix G_k as a group. Finally, we choose the automorphisms of G_K that fix G_k such that the square of the automorphism fixes G_k point-wise; these are the k-involutions of G_k.

3.1 Automorphisms of $\mathrm{SL}(2,k)$

The process of conjugating elements of a group by some fixed group element is a group automorphism. That is, for some $g \in G$, the map $\mathrm{Inn}(g)(x) = gxg^{-1}$ is an automorphism of G that is called an *inner automorphism*. It is possible, in the case that $G = \mathrm{SL}(n,k)$, that conjugation by a matrix in $\mathrm{GL}(n,k)$ or $\mathrm{GL}(n,K)$ is an automorphism of G, so we also need to consider these automorphisms. Let $\mathrm{Aut}(G_k)$ denote the set of automorphisms of G_k such that conjugation is by elements in $\mathrm{GL}(n,k)$; then $\mathrm{Aut}(G,G_k)$ denotes the group of automorphisms in $\mathrm{Aut}(G)$ that fix G_k; these are called *k-automorphisms*. Similar notation applies to inner automorphisms.

Beyond determining k-involutions of G_k, we are also interested in characterizing the ways in which k-involutions act equivalently in some sense. In the context of this dissertation, the most useful measure of equivalence is conjugacy. We say that two conjugate automorphisms are

isomorphic. Thus our goal is to determine the conjugacy or *isomorphism* classes of k-involutions of G_k.

Definition 3.1.1. Let θ and $\varphi \in \mathrm{Aut}(G, G_k)$. If $\sigma\theta\sigma^{-1} = \varphi$ and

- $\sigma \in \mathrm{Aut}(G, G_k)$, then θ and φ are $\mathrm{Aut}(G, G_k)$-isomorphic.
- $\sigma \in \mathrm{Inn}(G, G_k)$, then θ and φ are $\mathrm{Inn}(G, G_k)$-isomorphic.

We want to determine which k-involutions are $\mathrm{Inn}(G, G_k)$-isomorphic. To begin, we note the following lemma which is consequence of a proposition of Borel [6, Proposition 14.9].

Lemma 3.1.2. *Let $G = \mathrm{SL}(n, \overline{k})$ as above. Then $\mathrm{Aut}(G) = \mathrm{Inn}(G)$.*

In other words, every automorphism of G_k can be written as conjugation by some element of $\mathrm{GL}(2, K)$. Specifically, given an automorphism φ of G_k, there is a matrix $A \in \mathrm{GL}(2, K)$ such that $\varphi = \mathrm{Inn}(A)|_{G_k}$. Notice that the entries of A may be in some (smaller) extension field, K, rather than $\overline{k}$; we choose A to be as generic as possible.

Lemma 3.1.3. *Suppose $A \in \mathrm{GL}(2, K)$. If $\mathrm{Inn}(A)|_{G_k} = \mathrm{Id}$, then $A = p\,\mathrm{Id}$, for some $p \in K$.*

Proof. Let $A = (a_{ij})$ with $i, j \in \{1, 2\}$ and $a_{ij} \in K$. Since $\mathrm{Inn}(A)|_{G_k} = \mathrm{Id}$, then for all $X = (x_{ij}) \in G_k$, $\mathrm{Inn}(A)(X) = AXA^{-1} = X$, so $AX = XA$. In other words, A commutes with all elements of G_k. In terms of matrices, $XA = AX$ is

$$\begin{bmatrix} a_{11}x_{11} + a_{12}x_{21} & a_{11}x_{12} + a_{12}x_{22} \\ a_{21}x_{11} + a_{22}x_{21} & a_{21}x_{12} + a_{22}x_{22} \end{bmatrix} = \begin{bmatrix} a_{11}x_{11} + a_{21}x_{12} & a_{12}x_{11} + a_{22}x_{12} \\ a_{11}x_{21} + a_{21}x_{22} & a_{12}x_{21} + a_{22}x_{22} \end{bmatrix}.$$

In particular, this holds for $X = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$, and the above relations reduce to

$$\begin{bmatrix} a_{11} + a_{12} & a_{12} \\ a_{21} + a_{22} & a_{22} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{11} + a_{21} & a_{12} + a_{22} \end{bmatrix}.$$

This forces the following relations $a_{11} = a_{22} = p$ and $a_{12} = 0$. Similarly, by setting $X = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$, we force the relations $a_{21} = 0$. Thus $A = p\,\mathrm{Id}$. ∎

Lemma 3.1.4. *$\mathrm{Inn}(A) \in \mathrm{Aut}(G, G_K)$ acts invariantly on G_k if and only if $A = pB$, for some $p \in K$ and $B \in \mathrm{GL}(2, k)$.*

Proof. Write $A \in \mathrm{GL}(2, K)$ as

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}.$$

Then

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} a_{22} & a_{12} \\ a_{21} & a_{11} \end{bmatrix}.$$

For each $X = (x_{ij}) \in G_k$, set $\mathrm{Inn}(A)(X) = AXA^{-1} = B$. The entries of B are

$$b_{11} = \frac{a_{22}a_{11}x_{11} + a_{12}a_{22}x_{21} + a_{11}a_{21}x_{12} + a_{21}a_{12}x_{22}}{a_{11}a_{22} + a_{12}a_{21}}, \tag{3.1.4.1}$$

$$b_{12} = \frac{a_{12}a_{11}x_{11} + a_{12}^2x_{21} + a_{11}^2x_{12} + a_{11}a_{12}x_{22}}{a_{11}a_{22} + a_{12}a_{21}}, \tag{3.1.4.2}$$

$$b_{21} = \frac{a_{22}a_{21}x_{11} + a_{22}^2x_{21} + a_{21}^2x_{12} + a_{21}a_{22}x_{22}}{a_{11}a_{22} + a_{12}a_{21}}, \tag{3.1.4.3}$$

$$b_{22} = \frac{a_{12}a_{21}x_{11} + a_{12}a_{22}x_{21} + a_{11}a_{21}x_{12} + a_{11}a_{22}x_{22}}{a_{11}a_{22} + a_{12}a_{21}}. \tag{3.1.4.4}$$

Since X can vary over all G_k, we may choose particular elements X_{ij}, the matrix whose ij-th entry is zero and all other entries are one, and X'_{ij}, the matrix which has zeros on the diagonal which contains the ij-th element and ones on the other diagonal. Adding

$$AX_{ij}A^{-1} + AX'_{ij}A^{-1},$$

for each i and j, and using all of the combinations of $X_{i,j}$, we get

$$\frac{a_{ij}a_{k\ell}}{a_{11}a_{22} + a_{12}a_{21}} \in k$$

for all i, j, k and ℓ.

What we have shown is that $\mathrm{Inn}(A)(X) \in G_k$ if and only if

$$\frac{a_{ij}a_{k\ell}}{a_{11}a_{22} + a_{12}a_{21}} \in k.$$

Now choose i and j so that $a_{ij} \neq 0$, and let

$$r = \frac{a_{ij}a_{k\ell}}{a_{11}a_{22} + a_{12}a_{21}}$$

and

$$s = \left(\frac{a_{ij}a_{ij}}{a_{11}a_{22} + a_{12}a_{21}}\right)^{-1}.$$

Since $r \cdot s \in k$, then $\frac{a_{k\ell}}{a_{ij}} \in k$ for all k and ℓ. Therefore,

$$A = a_{ij} \begin{bmatrix} \frac{a_{11}}{a_{ij}} & \frac{a_{12}}{a_{ij}} \\ \frac{a_{21}}{a_{ij}} & \frac{a_{22}}{a_{ij}} \end{bmatrix},$$

where $a_{ij} \in K$. That is, $A = pB$ with $B \in G_k$ and $p \in K$. ■

Corollary 3.1.5. *Every automorphism of G_k can be written as $\mathrm{Inn}(A)$ for some $A \in \mathrm{GL}(2,k)$.*

Proof. By Lemma 3.1.2, $\mathrm{Aut}(G_K) = \mathrm{Inn}(G_K)$, and Lemma 3.1.4 states that if $\mathrm{Inn}(A) \in \mathrm{Aut}(G, G_k)$, then $\mathrm{Inn}(A) = \mathrm{Inn}(pB)$ where $B \in \mathrm{GL}(2,k)$. But, $pBX(pB)^{-1} = BXB^{-1}$. Thus $\mathrm{Inn}(pB) = \mathrm{Inn}(B)$. ■

3.2 k-involutions of $\mathrm{SL}(2,k)$

Since every automorphism of G_k is inner, every involution of G_k is inner. Suppose $\theta \in \mathrm{Aut}(G_k)$ is an involution. Then, as a consequence of Lemma 3.1.2 and Corollary 3.1.5, there is a matrix $A \in \mathrm{GL}(2,k)$ such that $\theta = \mathrm{Inn}(A)|_{G_k}$. Since $A \in \mathrm{GL}(2,k)$, by Lemma 3.1.3, $A^2 = p\,\mathrm{Id}$, where $p \in k$ since $A \in \mathrm{GL}(2,k)$. This is slightly more general than what Lemma 3.1.3 implies.

Lemma 3.2.1. *Suppose $\theta \in \mathrm{Aut}(G_k)$ is an involution. There exists some $p \in k$ and a matrix $A \in \mathrm{GL}(2,k)$ such that $\theta = \mathrm{Inn}(A)|_{G_k}$ and A is conjugate to $\begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix}$.*

Proof. θ is an involution, so there exists some $A \in \mathrm{GL}(2,k)$ such that $\mathrm{Inn}(A)^2 = \mathrm{Id}$. That is, $\mathrm{Inn}(A^2) = \mathrm{Id}$. Let $a, b, c, d \in k$ and

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Then

$$A^2 = \begin{bmatrix} a^2 + bc & (a+c)b \\ (a+d)c & d^2 + bc \end{bmatrix}.$$

By Lemma 3.1.3, $A^2 = p\,\mathrm{Id}$ for some $p \in k$. This forces the relations

$$a^2 + bc = d^2 + bc \tag{3.2.1.1}$$

$$(a+d)c = (a+d)b = 0. \tag{3.2.1.2}$$

Thus $a = d$. There are no restrictions on b and c. Since A is invertible, $a^2 + bc \neq 0$ and

$$A = \begin{bmatrix} a & b \\ c & a \end{bmatrix}.$$

The characteristic polynomial of A is

$$C_A(x) = x^2 + \mathrm{Tr}(A)x + \det(A) \tag{3.2.1.3}$$

$$= x^2 + 2ax + a^2 + bc \tag{3.2.1.4}$$

$$= x^2 + a^2 + bc. \tag{3.2.1.5}$$

If the minimal polynomial of A is $M_A(x) = x + \beta$, for some $\beta \in k$, then $A = \beta\,\mathrm{Id}$ for some $\beta \in k$, and $\mathrm{Inn}(A)$ is not an involution. If $M_A(x) = C_A(x)$ then A is conjugate to the matrix (in rational canonical form)

$$B = \begin{bmatrix} 0 & a^2 + bc \\ 1 & 0 \end{bmatrix}.$$

To demonstrate the rational canonical form explicitly, we find a cyclic vector α of A. Because $C_A(x) = M_A(x)$, A has a cyclic vector. Next, we construct the basis $\{\alpha, A(\alpha)\}$ by which A can be represented as B. We can assume, without loss of generality, that c is non-zero. Let $\alpha = e_1$. Then

$$P = \begin{bmatrix} 1 & a \\ 0 & c \end{bmatrix},$$

and $B = P^{-1}AP$.

In general, we write

$$B = \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix},$$

where $p = (bc + a^2)^{-1} \in k$. ■

Example 3.1. In the case that $k = \mathbb{F}_2$, there are three involutions. The two involutions $\mathrm{Inn}(A)$ and $\mathrm{Inn}(B)$, which correspond to the matrices

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

are both conjugate to the matrix $\mathrm{Inn}(Y)$, where

$$Y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

by letting

$$P_A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \qquad P_A^{-1} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

and

$$P_B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad P_B^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

□

Corollary 3.2.2. *Each isomorphism class of k-involutions of G_k can be represented by* $\mathrm{Inn}(A)$,

where $A \in \mathrm{GL}(2,k)$ *is of the form*

$$A = \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix}.$$

Remark 3.2.3. Since the characteristic and minimal polynomials of $A = \left[\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right]$ are different, A is never a semisimple element. However A is a unipotent element, as we showed in Example 3.1.

Lemma 3.2.4. *Let*

$$A = \begin{bmatrix} 0 & 1 \\ r & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ s & 0 \end{bmatrix}.$$

Then $\mathrm{Inn}(A)$ *is isomorphic to* $\mathrm{Inn}(B)$ *if and only if there is a matrix* $C \in \mathrm{GL}(2,k)$ *and a constant* $p \in k$ *such that* $CAC^{-1} = pB$.

Proof. By definition, $\mathrm{Inn}(A)$ is isomorphic to $\mathrm{Inn}(B)$ if and only if there is a matrix $C \in \mathrm{GL}(2,k)$ such that $\mathrm{Inn}(C)\,\mathrm{Inn}(A)\,\mathrm{Inn}(C)^{-1} = \mathrm{Inn}(B)$. For any $X \in G$, then $CAC^{-1}XCA^{-1}C^{-1} = BXB^{-1}$ which we can rearrange to

$$(B^{-1}CAC^{-1})X(CA^{-1}C^{-1}B) = X.$$

That is, when $\mathrm{Inn}(B^{-1}CAC^{-1}) = \mathrm{Id}$. By Lemma 3.1.3, $B^{-1}CAC^{-1} = p\,\mathrm{Id}$ for some $p \in k$. Thus

$$CAC^{-1} = pB \tag{3.2.4.1}$$

■

Let k^* denote the non-zero elements of k and let $(k^*)^2$ denote the set of elements of k which have square roots in k.

Theorem 3.2.5. *If* $\mathrm{Inn}(A)$ *and* $\mathrm{Inn}(B) \in \mathrm{Aut}(G, G_k)$ *are* k*-involutions corresponding to*

$$A = \begin{bmatrix} 0 & 1 \\ r & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 \\ s & 0 \end{bmatrix},$$

then $\mathrm{Inn}(A)$ *is isomorphic to* $\mathrm{Inn}(B)$ *if and only if* $r/s \in (k^*)^2$.

Proof. From Lemma 3.2.4, take the determinant of both sides of (3.2.4.1), which leads to the

following equivalent statements:

$$\begin{aligned}
\det(CAC^{-1}) &= \det(pB) \\
\det(C)\det(A)\det(C^{-1}) &= p^2\det(B) \\
\det(C)\det(A)\det(C)^{-1} &= p^2\det(B) \\
\det(A) &= p^2\det(B) \\
r &= p^2 s.
\end{aligned}$$

Thus $r/s = p^2$, so $r/s \in (k^*)^2$. Conversely, let $r/s = p^2$ for some $p \in k$, and let

$$C = \begin{bmatrix} 0 & 1 \\ ps & 0 \end{bmatrix}.$$

Then

$$\begin{aligned}
CAC^{-1} &= \begin{bmatrix} 0 & 1 \\ ps & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ r & 0 \end{bmatrix} \begin{bmatrix} 0 & \frac{1}{ps} \\ 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} 0 & \frac{r}{ps} \\ ps & 0 \end{bmatrix} \\
&= p \begin{bmatrix} 0 & 1 \\ s & 0 \end{bmatrix} \\
&= pB.
\end{aligned}$$

By Lemma 3.2.4, $\mathrm{Inn}(A)$ is isomorphic to $\mathrm{Inn}(B)$. ■

Corollary 3.2.6. *The number of isomorphism classes of k-involutions of G_k is the same as the number of square classes of k^*.*

3.3 Isomorphism Classes of k-involutions of $\mathrm{SL}(2,k)$

The isomorphism classes of k-involutions of G_k depend on the elements in $(k^*)^2$. By Lemma 2.2.4, every non-zero element of the finite field $\mathbb{F}_q$ is a square. Therefore, we have the following corollary to Theorem 3.2.5:

Corollary 3.3.1. *Let k be a finite field, or any algebraically closed field. Then there is one isomorphism class of k-involutions of $\mathrm{SL}(2,k)$.*

For any algebraically closed field k, with $a \in k$, the equation $x^2 + a = 0$ has a unique solution. By Theorem 3.2.5 and Corollary 3.3.1, there is exactly one isomorphism class of k-involutions

of $\mathrm{SL}(2,\overline{k})$.

Let k be any infinite field which is not algebraically closed. There are infinitely many non-squares in k. For example, if $k = \mathbb{F}_q(x)$, where x is a vector of indeterminates, there are non-squares x, x^3, x^5, etc. In these cases, k is not a perfect field.

Corollary 3.3.2. *Let k be any infinite field which is not algebraically closed. There are infinitely many isomorphism classes of k-involutions of $\mathrm{SL}(2,k)$.*

3.4 Fixed Point Groups

The fixed point group H_k of a k-involution of G_k plays an important role in determining the structure of the corresponding symmetric k-variety. Since $Q_k \cong G_k/H_k$, it is important to characterize H_k. Recall $H_k = \{x \in G_k \mid \theta(x) = x\}$ and $Q_k = \{g\theta(g)^{-1} \mid g \in G_k\}$. If $k = \mathbb{F}_q$, where $q = 2^r$ (or if k is the algebraic closure of $\mathbb{F}_q$), then there is only one representative of $k^*/(k^*)^2$. In general we have

$$\begin{aligned}
H_k &= \left\{ \begin{bmatrix} x & y \\ z & w \end{bmatrix} \;\middle|\; \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} 0 & p^{-1} \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}, wx + yz = 1 \right\} \\
&= \left\{ \begin{bmatrix} x & y \\ z & w \end{bmatrix} \;\middle|\; \begin{bmatrix} w & p^{-1}z \\ py & x \end{bmatrix} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}, wx + yz = 1 \right\} \\
&= \left\{ \begin{bmatrix} x & y \\ z & w \end{bmatrix} \;\middle|\; w = x, py = z, wx + yz = 1 \right\} \\
&= \left\{ \begin{bmatrix} x & y \\ py & x \end{bmatrix} \;\middle|\; x^2 + py^2 = 1 \right\}.
\end{aligned}$$

The following lemma asserts that isomorphic k-involutions have isomorphic fixed point groups.

Lemma 3.4.1. *If θ_1 and θ_2 are isomorphic k-involutions of G_k, then their fixed point groups H_1 and H_2, respectively, are isomorphic.*

Proof. Suppose $\psi\theta_1\psi^{-1} = \theta_2$. By definition, ψ is an automorphism of G_k. So $\psi : H_1 \to H_2$ is the desired isomorphism of the fixed point groups. To see this, suppose $X \in H_1$. Then $\theta_1(X) = X$ which means that $\psi(\theta_1(X)) = \psi(X) = \theta_2(\psi(X))$ which shows that $\psi(X) \in H_2$. Since ψ is already an isomorphism of G_k, it is also an isomorphism of subgroups of G_k. ■

Remark 3.4.2. The converse of Lemma 3.4.1 is not true in general, though it does hold in general for algebraic groups. That is, two fixed point groups H_1 and H_2 may be isomorphic, but their

related involutions may not be isomorphic. In a paper describing the generalized symmetric spaces of the dihedral groups [9], Helminck et al. give an example illustrating this fact.

We state without proof, in the following lemma, that semisimple fixed point groups are conjugate to semisimple fixed point groups.

Lemma 3.4.3. *Let θ_1 and θ_2 be isomorphic k-involutions of G_k, and let $\varphi\theta_1\varphi^{-1} = \theta_2$. Suppose H_1 and H_2 are the fixed point groups of θ_1 and θ_2, respectively. If $X \in H_1$ is diagonalizable with $PXP^{-1} = D$ for some invertible P and diagonal D, then $\varphi(X)$ is diagonalizable.*

Remark 3.4.4. Suppose $\mathrm{Inn}(A) \in \mathrm{Aut}(G, G_k)$ is a k-involution such that $A = \left[\begin{smallmatrix} 0 & 1 \\ a & 0 \end{smallmatrix}\right]$. For some $Y \in H_k$, the characteristic polynomial of Y is $C_Y(t) = t^2 + x^2 + ay^2$. Since $x^2 + ay^2 = 1$, then $C_Y(t) = t^2 + 1 = (t+1)^2$. Thus Y is diagonalizable if and only if $Y = \mathrm{Id}$. This means that H_k consists of non-semisimple elements unless $k = \mathbb{F}_2$. Moreover, we will soon show the fixed point groups consist of unipotent elements.

Example 3.2. The fixed point groups of k-involutions have different properties when k does not have characteristic 2. The inner k-involution corresponding to $A = \left[\begin{smallmatrix} 0 & 1 \\ a & 0 \end{smallmatrix}\right]$ is an element of $\mathrm{Aut}(G, G_k)$ with fixed point group

$$H^a = \left\{ \begin{bmatrix} x & y \\ ay & x \end{bmatrix} \middle| x^2 - ay^2 = 1 \right\}.$$

For $k = \mathbb{R}$, there are two possibilities for a, $a = 1$, and $a = -1$. For $k = \mathbb{C}$, the only possibility is that $a = 1$. This gives two fixed point groups. Wu [39] showed that H^a is k-split if and only if a is a square in k^*, and otherwise H^a is k-anisotropic. Thus H^a is k-anisotropic if $k = \mathbb{R}$, and H^a is non-compact if $k = \mathbb{C}$. The fixed point groups of k-involutions corresponding to semisimple matrices are reductive. □

For any k-involution $\varphi \in \mathrm{Aut}(G, G_k)$, $\varphi = \mathrm{Inn}(A)$ and A is conjugate to some $\left[\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right]$. Since $\mathrm{Inn}(pA) = \mathrm{Inn}(A)$, and since

$$\begin{bmatrix} 1 & 0 \\ \sqrt{p} & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \sqrt{p} & 1 \end{bmatrix} = \begin{bmatrix} \sqrt{p} & 1 \\ 0 & \sqrt{p} \end{bmatrix},$$

if $p \in (k^*)^2$, then φ is isomorphic to $\mathrm{Inn}(B)$ where

$$B = \begin{bmatrix} 1 & \sqrt{p}^{-1} \\ 0 & 1 \end{bmatrix}.$$

To summarize, we have proved the following

Theorem 3.4.5. *Every k-involution of G_k is conjugate to a k-involution of the form* $\mathrm{Inn}(B)$ *where*

$$B = S \begin{bmatrix} 1 & \sqrt{p}^{-1} \\ 0 & 1 \end{bmatrix} S^{-1},$$

for some $S \in \mathrm{GL}(n, K)$. Moreover, $\mathrm{Inn}(B)$ *has fixed point group SHS^{-1}, where H is the unipotent subgroup*

$$H = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \,\middle|\, x \in k \right\}.$$

So every k-involution of G_k has a unipotent fixed point group.

3.5 The Structure of Q_k

Since every k-involution of G_k is conjugation by an element of the form $A = \left[\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right]$, for some $p \in k$, the elements of $Q_k \cong G_k/H_k$ have the following form:

$$\begin{aligned}
Q_k &= \left\{ X\theta(X)^{-1} \mid X \in G \right\} \\
&= \left\{ X \left[\mathrm{Inn}(A)(X)\right]^{-1} \mid X \in G \right\} \\
&= \left\{ X \left[AXA^{-1}\right]^{-1} \mid X \in G \right\} \\
&= \left\{ XAX^{-1}A^{-1} \mid X \in G \right\} \\
&= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix} \begin{bmatrix} d & b \\ c & a \end{bmatrix} \begin{bmatrix} 0 & \frac{1}{p} \\ 1 & 0 \end{bmatrix} \,\middle|\, ad + bc = 1 \right\} \\
&= \left\{ \begin{bmatrix} pb^2 + a^2 & \frac{1}{p}(pbd + ac) \\ pbd + ac & \frac{1}{p}(pd^2 + c^2) \end{bmatrix} \,\middle|\, ad + bc = 1 \right\}
\end{aligned}$$

The minimal polynomial of any element $X \in Q_k$ has the form

$$M_X(t) = t^2 + t\left(a^2 + d^2 + pb^2 + \frac{c^2}{p}\right) + \frac{1}{p}\left(pdb + ac\right)^2$$

which can be factored into distinct linear factors if and only if $a^2 + d^2 + pb^2 + \frac{c^2}{p} = 0$. That means that $X \in Q_k$ is semisimple exactly when $a^2 + d^2 + pb^2 + \frac{c^2}{p} \neq 0$.

Chapter 4

k-involutions of $\mathrm{SL}(n,k)$ for $n > 2$

In this chapter, we build upon the results from Chapter 3. As before, let k be a field of characteristic 2, K an extension field of k, $G = \mathrm{SL}(n,\overline{k})$, $G_K = \mathrm{SL}(n,K)$, and $G_k = \mathrm{SL}(n,k)$.

The automorphisms of the classical groups were (mostly) characterized in the mid 1900's. Dieudonné [12] completed most of the work for $n \geq 3$. Usually, the case $n = 2$ must be treated separately, as must the case that k has characteristic 2. In a supplement to Dieudonné's results, L. K. Hua directly computed the automorphisms for some of the remaining low-dimension cases. Dieudonné also published these and other results in 1955 [13]. This is a very useful reference, though it is written in French. Unfortunately, the case that k has characteristic 2 was not included for the orthogonal groups, but that is the subject of the next chapter.

Proposition 4.0.1 (Dieudonné)**.**

1. *Every automorphism of* $\mathrm{GL}(n,k)$ *($n \geq 2$) takes one of the two forms* $u \to \chi(u)gug^{-1}$ *or* $u \to \chi(u)h\breve{u}h^{-1}$*, where* $u \to \chi(u)$ *is a representation of* $\mathrm{GL}(n,k)$ *in the multiplicative group of the center of* k*,* g *is a semi-linear transformation of* V *onto* V*;* h *is a semi-linear transformation of* V *onto* V^* *and* $\breve{u}$ *denotes the transformation contragredient to* u*. Every automorphism of* $PGL(n,k)$ *($n \geq 2$) is induced by an automorphism of* $\mathrm{GL}(n,k)$*.*

2. *Every automorphism of* $\mathrm{SL}(n,k)$ *($n \geq 2$) is the restriction of an automorphism of* $\mathrm{GL}(n,k)$*, with the possible exception of the cases* $n = 2$ *or* 4 *when* k *is non-commutative, has characteristic different from 2 and is such that* -1 *is not in the commutator subgroup of* k^**. Every automorphism of* $PSL(n,k)$ *(same restrictions as above) is induced by an automorphism of* $\mathrm{SL}(n,k)$*.*

Now that $n > 2$, there are both inner and outer automorphisms of G_k, and we must deal with each case separately.

4.1 Inner Automorphisms of $\mathrm{SL}(n,k)$

Any automorphism in $\mathrm{Inn}(G, G_k)$ is defined by conjugation by a matrix in $\mathrm{GL}(n,K)$. As before, we want to determine which of these automorphisms fix G_k as a group and which fix G_k pointwise. The general plan of attack is very similar to that of Chapter 3, at least for the inner automorphisms and involutions. We begin by proving several similar statements.

Lemma 4.1.1. *Suppose $A \in \mathrm{GL}(n,K)$. If $\mathrm{Inn}(A)|_{G_k} = \mathrm{Id}$, then $A = p\,\mathrm{Id}$, for some $p \in K$.*

Proof. Let $A \in \mathrm{GL}(n,K)$. Since $\mathrm{Inn}(A)(X) = X$, then $AX = XA$ for any $X \in G_k$. Equating corresponding entries of AX and XA, we get the relations

$$\sum_{k=1}^{n} a_{ik}x_{kj} = \sum_{\ell=1}^{n} x_{i\ell}a_{\ell j} \tag{4.1.1.1}$$

for $\ell, k \in \{1, 2, \ldots n\}$. When X is the matrix $E_{r,s} + \mathrm{Id}$, $i = r$, and $j = s$, we get

$$a_{r,s}x_{s,s} + a_{r,r}x_{r,s} = x_{r,s}a_{s,s} + x_{r,r}a_{r,s}$$

which gives $a_{r,r} = a_{s,s}$ ($x_{s,s} = x_{r,s} = x_{r,r} = 1$). Since X can vary over all $E_{r,s}$ with $r \neq s$, it follows that the diagonal entries are equal.

To show that $a_{r,s} = 0$ when $r \neq s$, there are many suitable choices for X. For example, let $X = E_{s,q} + \mathrm{Id}$ for $s \neq q$. Setting $i = r$ and $j = q$ in (4.1.1.1) gives

$$a_{r,s}x_{s,q} + a_{r,q}x_{q,q} = x_{r,r}a_{r,q}.$$

This equation reduces to $a_{r,s} = 0$, as desired, since $x_{s,q} = 1 = x_{q,q} = x_{r,r}$. ∎

Lemma 4.1.2. *Let $A \in \mathrm{GL}(n,K)$. Then $\mathrm{Inn}(A)|_{G_k} \in \mathrm{Aut}(G_k)$ if and only if $A = pB$, for some $p \in K$ and $B \in \mathrm{GL}(n,k)$.*

Proof. We want to show that if $\mathrm{Inn}(A)(X) \in G_k$ then $A = pB$. We do this by choosing $X \in G_k$ so that it forces certain relationships between the entries of A. Then we factor out a constant.

Let $X \in G_k$. By definition,

$$\mathrm{Inn}_A(X) = AXA^{-1} = \frac{1}{\det(A)}AXA', \tag{4.1.2.1}$$

where A' is the transpose of the adjugate matrix of A. That is, A' is the matrix whose (i,j) entry is $A_{j,i}$, the determinant of the (j,i)-th minor of A. Then the (i,j) entry of (4.1.2.1) is

$$\frac{1}{\det A}\left(\sum_{m=1}^{n}\sum_{\ell=1}^{n} a_{i,m}x_{m,\ell}A_{j,\ell}\right), \tag{4.1.2.2}$$

which must be an element of k since $\mathrm{Inn}(A)$ fixes G_k point-wise.

Let $X = \mathrm{Id}$. Then (4.1.2.2) becomes

$$\frac{1}{\det A}\left(a_{i,1}A_{j,1} + \cdots + a_{i,n}A_{j,n}\right). \tag{4.1.2.3}$$

Also, let $X = \mathrm{Id} + E_{pq}$, where $p \neq q$. Then (4.1.2.2) is

$$\frac{1}{\det A}\left(a_{i,1}A_{j,1} + \cdots + a_{i,n}A_{j,n} + a_{i,p}A_{q,j}\right). \tag{4.1.2.4}$$

By adding these two we get

$$\frac{a_{i,p}A_{q,j}}{\det(A)} \in k. \tag{4.1.2.5}$$

This holds for any $p \neq q$.

Next, let X be the permutation matrix with rows p and q switched. Then (4.1.2.1) is

$$\frac{1}{\det(A)}\left(a_{i,q}A_{p,j} + a_{i,p}A_{q,j} + \sum_{\substack{\ell=1 \\ \ell\neq p,q}}^{n} a_{i,\ell}A_{j,\ell}\right). \tag{4.1.2.6}$$

Finally, let X be as above with $x_{q,q} = 1$ instead of 0. Then (4.1.2.1) is

$$\frac{1}{\det(A)}\left(a_{i,q}A_{p,j} + (a_{i,p} + a_{i,q})A_{q,j} + \sum_{\substack{\ell=1 \\ \ell\neq p,q}}^{n} a_{i,\ell}A_{j,\ell}\right). \tag{4.1.2.7}$$

Adding these last two expressions, we get

$$\frac{a_{i,q}A_{q,j}}{\det(A)} \in k. \tag{4.1.2.8}$$

By dividing 4.1.2.5 by 4.1.2.8 and re-labeling indices as needed, we have

$$\frac{\dfrac{a_{i,j}A_{m,\ell}}{\det(A)}}{\dfrac{a_{m,n}A_{m,\ell}}{\det(A)}} = \frac{a_{i,j}}{a_{m,n}} \in k$$

for any $m, n, i, j \in \{1, 2, \ldots n\}$, provided that $a_{m,n} \neq 0$. Now, by factoring $a_{m,n}$ from A, we get $A = a_{m,n}B = pB$ where $b_{i,j} = \frac{a_{i,j}}{a_{m,n}}$. Since $\mathrm{Inn}(pB) = \mathrm{Inn}(B)$, we have proved the claim. ■

Corollary 4.1.3. *Any inner automorphism of G_k can be written as conjugation by a matrix in $\mathrm{GL}(n, k)$, since $\mathrm{Inn}(pA) = \mathrm{Inn}(A)$.*

Lemma 4.1.4. *The inner automorphisms* $\mathrm{Inn}(A)$ *and* $\mathrm{Inn}(B)$ *are isomorphic if and only if* A *is conjugate to* cB *for some* $c \in k$.

Proof. Since $\mathrm{Inn}(A)$ is isomorphic to $\mathrm{Inn}(B)$, by definition, there is a matrix $C \in \mathrm{GL}(n, K)$ with $\mathrm{Inn}(C) \in \mathrm{Aut}(G, G_k)$ such that

$$\mathrm{Inn}(C)\,\mathrm{Inn}(A)\,\mathrm{Inn}(C)^{-1} = \mathrm{Inn}(B).$$

By the Corollary 4.1.3, we can take $C \in \mathrm{GL}(n, k)$, so that $\mathrm{Inn}(C) \in \mathrm{Aut}(G_k)$. This implies that $\mathrm{Inn}(C)\,\mathrm{Inn}(A)\,\mathrm{Inn}(C)^{-1}(X) = \mathrm{Inn}(B)(X)$ for every $X \in G_k$. Moreover,

$$\mathrm{Inn}(B^{-1}CAC^{-1}) = \mathrm{Id},$$

and, by Lemma 4.1.1, it follows that

$$B^{-1}CAC^{-1} = c\,\mathrm{Id}$$

for some $c \in k$. Thus $CAC^{-1} = cB$. ■

4.2 Inner k-involutions of $\mathrm{SL}(n, k)$

By Lemma 4.1.1, if $\mathrm{Inn}(A) \in \mathrm{Aut}(G, G_k)$ fixes G_k point-wise, then $A = p\,\mathrm{Id}$ for some $p \in K$. By Lemma 4.1.2, we may take $p \in k$. Since $\mathrm{Inn}(A)^2 = \mathrm{Inn}(A^2)$, it makes sense to determine which properties of A lead to $A^2 = p\,\mathrm{Id}$. We begin by noting the following lemma:

Lemma 4.2.1. *Suppose* $A \in \mathrm{GL}(n, k)$ *with* $A^2 = p\,\mathrm{Id}$.

1. *If* $A = c\,\mathrm{Id}$ *where* $c^2 = p$ *and* $c \in k$, *then* $\mathrm{Inn}(A)$ *is not a* k*-involution.*
2. *If* $A^2 + c^2\,\mathrm{Id} = 0$, *where* $c \in k$, *but* $A \neq c\,\mathrm{Id}$, *then* A *is conjugate to a matrix with* m *copies of* L_{c^2} *and* $n - 2m$ *copies of* c *on the diagonal, as in*

$$L_{m,c^2,c} = \begin{bmatrix} \begin{bmatrix} 0 & 1 \\ c^2 & 0 \end{bmatrix} & & & & & & \\ & \ddots & & & & & \\ & & \begin{bmatrix} 0 & 1 \\ c^2 & 0 \end{bmatrix} & & & & \\ & & & c & & & \\ & & & & \ddots & & \\ & & & & & c & \end{bmatrix}. \tag{4.2.1.1}$$

3. *If* $A^2 + p\,\mathrm{Id} = 0$, *where* $p \notin (k^*)^2$, *then* A *is conjugate to a matrix with* $\frac{n}{2}$ *copies of* $L_p = \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix}$ *on the diagonal, as in*

$$L_{\frac{n}{2},p} = \begin{bmatrix} \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix} & & \\ & \ddots & \\ & & \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix} \end{bmatrix}. \tag{4.2.1.2}$$

Proof.

1. Since $\mathrm{Inn}(A)$ has order 1, it is not an involution.

2. Since the minimal polynomial of A is $M_A(x) = x^2 + c^2 = (x + c)^2$, and the invariant factors of A must divide $M_A(x)$, we know some of the structure of the rational canonical form of A. Without knowing A explicitly we can not determine the multiplicities of the invariant factors, so there may be any combination of invariant factors of the form $(x+c)^2$ or $(x+c)$. The only constraint is that the sum of the degrees of the invariant factors equals n, and that there is at least one factor of $(x + c)^2$. Therefore $A = L_{m,c^2,c}$, where m varies from 1 to $n/2$.

3. The minimal polynomial is $M_A(x) = x^2 + p$, where p is not a square. The characteristic polynomial is $C_A(x) = (x^2 + p)^{n/2}$, and here, the invariant factors are all $M_A(x)$, since they are forced to divide $M_A(x)$. Since the sum of the degrees of all the invariant factors must equal the degree of $C_A(x) = n$, the dimension of A is even. Therefore, A is a direct sum of $\frac{n}{2}$ blocks of L_p, as in $L_{\frac{n}{2},p}$.

In both (2) and (3), we use the fact that $\mathrm{Inn}(pA) = \mathrm{Inn}(A)$ in order to obtain L_p, since it is not always possible to write the blocks in the form L_p by only using conjugation. Notice that (3) does not occur when $k = \overline{k}$ or when k is finite. ■

Example 4.1. Let

$$A = \begin{bmatrix} 0 & a & 0 \\ a & 0 & 0 \\ 0 & 0 & a \end{bmatrix}.$$

Then $A^2 = a^2\,\mathrm{Id}$, but $A \neq a\,\mathrm{Id}$. Square roots of matrices are not unique, in general, and there exist non-diagonal matrices that square to $p\,\mathrm{Id}$. Here, the minimal polynomial is $M_A(x) = (x + a)^2$, and the characteristic polynomial is $C_A(x) = (x + a)^3$. The invariant factors are

$(x+a)^2$ and $(x+a)$, and hence

$$A \cong \begin{bmatrix} 0 & a^2 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & a \end{bmatrix} = a^2 \begin{bmatrix} 0 & 1 & 0 \\ a^{-2} & 0 & 0 \\ 0 & 0 & a^{-1} \end{bmatrix}.$$

Since $\mathrm{Inn}(pA) = \mathrm{Inn}(A)$, we can write the corresponding inner automorphism as conjugation by

$$A = \begin{bmatrix} 0 & 1 & 0 \\ p & 0 & 0 \\ 0 & 0 & c \end{bmatrix}$$

for some $c \in k$ such that $c^2 = p$.

Notice that any matrix is diagonalizable if and only if the minimal polynomial is a product of *distinct* linear factors. Since $M_A(x) = (x+a)^2$, A is *not* diagonalizable. However, if the field is $\mathbb{R}$, then $M_A(x) = (x+a)(x-a)$ which implies A is diagonalizable. (See Hoffman & Kunze [26], Theorem 6.6, p. 204.) □

Example 4.2. Let A be as in Example 4.1, but now let $k = \mathbb{R}$. In this case, A can be diagonalized as follows:

$$A = \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} -a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix} \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}.$$

The difference between this example and Example 4.1 is that the minimal polynomial here is $M_A(x) = (x+a)(x-a) = x^2 - a^2$, and hence A is diagonalizable. Ling Wu considered this situation in his doctoral dissertation (See [39], Lemma 15, p.26 or [24]). In this case, $\mathrm{Inn}(A)$ is a k-involution since $A \ncong p\,\mathrm{Id}$. □

Example 4.3. Let

$$A = \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix}.$$

Whenever p is a square in k, which always occurs when k is finite, A is conjugate to a symmetric matrix. The transition matrix is

$$P = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{p}} \end{bmatrix}.$$

So we have

$$PAP^{-1} = \begin{bmatrix} 0 & \sqrt{p} \\ \sqrt{p} & 0 \end{bmatrix}.$$

□

Corollary 4.2.2. *Suppose $\varphi \in \mathrm{Aut}(G_k)$ is a k-inner involution. Then there is a matrix $A \in \mathrm{GL}(n,k)$ such that $\varphi = \mathrm{Inn}(A)$ where A is conjugate to one of the following matrices:*

1. *$L_{m,c^2,c}$ for $c \in k^*$ (See 4.2.1.1).*
2. *$L_{\frac{n}{2},p}$ for some $p \in k^*/(k^*)^2$ (See 4.2.1.2).*

Proof. By Corollary 4.1.3, there is a matrix $A \in \mathrm{GL}(n,k)$ so that $\varphi = \mathrm{Inn}(A)$. Since φ is an involution, we have $\varphi^2 = \mathrm{Inn}(A^2) = \mathrm{Id}$. Moreover, by Lemma 4.1.1, $A^2 = p\,\mathrm{Id}$ for some $p \in k$. It follows from Lemma 4.2.1 that A is conjugate to either $L_{\frac{n}{2},p}$ or $L_{m,c^2,c}$. ■

Notice the special case when 4.2.1.1 and 4.2.1.2 appear to be the same matrix; this happens when there are $n/2$ blocks of L_{c^2} as in $L_{\frac{n}{2},c^2,c}$, for n even. The subtle difference in 4.2.1.2 is that $p \notin (k^*)^2$, whereas in 4.2.1.1, $c^2 \in (k^*)^2$ which implies that $c \in k$. This is an important distinction that we will later use to determine isomorphism classes of k-involutions.

Also note that $L_{m,c^2,c}$ and $L_{\frac{n}{2},p}$ have different minimal and characteristic polynomials and different invariant factors, so they are not conjugate. Moreover, whenever $m_1 \neq m_2$, by the same argument $L_{m_1,c^2,c} \ncong L_{m_2,c^2,c}$. This is because the number of blocks of L_{c^2} is different, which means they have different numbers of invariant factors.

We do need to determine when $L_{m,c^2,c}$ and $L_{m,d^2,d}$ correspond to isomorphic k-involutions and when $L_{\frac{n}{2},p}$ and $L_{\frac{n}{2},q}$ correspond to isomorphic k-involutions.

Lemma 4.2.3. *$\mathrm{Inn}(L_{\frac{n}{2},p})$ is isomorphic to $\mathrm{Inn}(L_{\frac{n}{2},q})$ if and only if $p/q \in (k^*)^2$.*

Proof. By (4.2.1.2), $p, q \in k^*/(k^*)^2$, and by Lemma 4.1.4, $\mathrm{Inn}(L_{\frac{n}{2},p})$ is isomorphic to $\mathrm{Inn}(L_{\frac{n}{2},q})$ if and only if $A = L_{\frac{n}{2},p}$ is conjugate to $cB = cL_{\frac{n}{2},q}$ for some $c \in k$. The minimal polynomials are $M_A(x) = x^2 + p$ and $M_{cB}(x) = x^2 + c^2q$, and the characteristic polynomials are $C_A(x) = (x^2+p)^{n/2}$ and $C_B(x) = (x^2+c^2q)^{n/2}$, respectively. This means that A and cB are conjugate if and only if $c^2q = p$, since the invariant factors are fixed by the minimal polynomials. But this implies that $c^2 = p/q$. Thus $p/q \in (k^*)^2$. ■

Lemma 4.2.4. *Let $b, c \in k^*$. Then $\mathrm{Inn}(L_{m,b^2,b})$ is isomorphic to $\mathrm{Inn}(L_{m,c^2,c})$.*

Proof. By Lemma 4.1.4, $\mathrm{Inn}(L_{m,b^2,b})$ is isomorphic to $\mathrm{Inn}(L_{m,c^2,c})$ if and only if $A = L_{m,b^2,b} \cong tB = tL_{m,c^2,c}$ for some $t \in k$. By Lemma 4.1.1, the minimal polynomials are $M_A(x) = (x^2 + b^2)(x+b)$ and $M_{tB}(x) = (x^2 + t^2c^2)(x+tc)$. If A and tB are conjugate, they must have the same invariant factors and characteristic and minimal polynomials. Thus they are conjugate if and only if $tc = b$ and $t^2c^2 = b^2$; these two conditions are equivalent to $t = b/c$. It is always possible to pick t so that $t = b/c$. Therefore, $\mathrm{Inn}(L_{m,b^2,b})$ is isomorphic to $\mathrm{Inn}(L_{m,c^2,c})$. ■

Theorem 4.2.5. *Suppose $\varphi \in \mathrm{Aut}(G_k)$ is an inner k-involution. Then, up to isomorphism, φ is of the form*

1. $\mathrm{Inn}(A)$ *where* $A = L_{\frac{n}{2},p}$ *for some* $p \in k^*/(k^*)^2$.

2. $\mathrm{Inn}(A)$ *where* $A = L_{m,c^2,c}$ *for some* $c \in k^*$.

Proof. The claim follows directly from Lemmas 4.2.3 and 4.2.4 and Corollary 4.2.2. ■

As in the Chapter 3, the isomorphism classes of k-involutions of $\mathrm{SL}(n,k)$ depend on the number of square classes in k^*. All inner k-involutions of G_k correspond to matrices which are not semisimple, because the minimal polynomials are not products of distinct linear terms. However, there exist unipotent elements which correspond to inner k-involutions, as in the $\mathrm{SL}(2,k)$ case.

Example 4.4. Conjugation by

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

corresponds to a unipotent inner k-involution since $A^2 = \mathrm{Id}$ and $A \neq \mathrm{Id}$. Since the characteristic polynomial of A is $C_A(x) = x^3+1$, and the minimal polynomial is $M_A(x) = x^2+1$, the invariant factors are x^2+1 and $x+1$. Thus A is conjugate to the block diagonal matrix B where the blocks are the companion matrices of the invariant factors.

$$A \cong B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

which is $L_{1,1,1}$. □

When k does not have characteristic 2, there are several differences as compared to the characteristic not 2 case. First, the matrices $I_{n-i,i}$ (see Chapter 2.4) are diagonal matrices which correspond to k-involutions, so there are semisimple elements which correspond to k-involutions whenever k is perfect with characteristic not 2. In fact, there are several different types of semisimple elements, all of which are listed in Chapter 2.4.

The k-involution $\mathrm{Inn}(L_{m,c^2,c})$ is unique to fields of characteristic 2. By Theorem 4.2.5, whenever k is algebraically closed or finite (and all field elements have unique squares), the k-involutions may be represented by either $\mathrm{Inn}(L_{\frac{n}{2},1})$ or $\mathrm{Inn}(L_{m,1,1})$. In summary, we have the following corollary to Theorem 4.2.5, analogous to the corollary in Chapter 3.

Corollary 4.2.6.

1. *Let k be a finite field or any algebraically closed field. Then there is one isomorphism class of k-involutions of $\mathrm{SL}(n,k)$ corresponding to $L_{\frac{n}{2},p}$ and there are $\frac{n}{2}-1$ classes corresponding to $L_{m,c^2,c}$.*

2. *Let k be any field which is not a union of finite fields. Then there are infinitely many isomorphism classes of k-involutions of $\mathrm{SL}(2,k)$, corresponding to $L_{\frac{n}{2},p}$, and there are $\frac{n}{2}-1$ classes corresponding to $L_{m,c^2,c}$.*

4.3 Outer Automorphisms of $\mathrm{SL}(n,k)$

For $n>2$, there are k-automorphisms of G_k which are not inner. For example, $\theta: G_k \to G_k$ by $\theta(X) = (X^{-1})^T$ is not an inner automorphism. When $n=2$, we can represent θ by conjugation by $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. We will call θ the *duality automorphism*. In some situations, over fields not considered in this work, θ is actually a Cartan involution.

Lemma 4.3.1. *If k is an algebraically closed field and $n>2$, then*

$$\frac{|\operatorname{Aut}(G)|}{|\operatorname{Inn}(G)|} = 2.$$

Proof. This is a consequence of Lemma 3.1.2. ■

Our plan is simpler than when determined the inner k-involutions of G_k. To begin, we note the following characterization of outer k-involutions in terms of inner k-involutions.

Lemma 4.3.2. *Let θ be a fixed outer automorphism of G. Since $|\operatorname{Aut}(G)/\operatorname{Inn}(G)| = 2$, we can write any outer automorphism of G as $\theta\operatorname{Inn}(A)$ for some matrix $A \in \mathrm{GL}(n,k)$.*

For convenience, we choose θ to be the duality automorphism. Note that θ is already an involution of G_k, and hence an automorphism of G_k. Thus $\theta\operatorname{Inn}(A)$ is always an automorphism of G_k. Throughout the rest of this chapter, θ will always refer to the duality automorphism. The next step is simply to determine which automorphisms $\theta\operatorname{Inn}(A)$ square to the identity.

4.4 Outer Involutions of $\mathrm{SL}(n,k)$

From Section 4.3, we know that every outer automorphism of G can be represented as $\theta\operatorname{Inn}(A)$ for some $A \in \mathrm{GL}(n,k)$ where θ is the duality automorphism. Recall that $\theta(X) = (X^{-1})^T$. The next lemma describes outer k-involutions in terms of the duality automorphism.

Lemma 4.4.1. *Let θ be the duality automorphism. Then $\theta\operatorname{Inn}(A)$ is an involution if and only if A is symmetric.*

Proof. We break the proof into two steps. First we show $\theta\,\mathrm{Inn}(A)$ is an involution if and only if $\theta(A)A \in Z(G_k)$, and then we show that $\theta(A)A \in Z(G_k)$ if and only if $A^T = A$. We use the fact that $\theta\,\mathrm{Inn}(A)\theta = \mathrm{Inn}\big(\theta(A)\big)$; this equation is a consequence of the fact that $\theta = \theta^{-1}$.

Let $Z(G_k)$ denote the center of G_k, and let $X \in G_k$.

1. Assume $\theta\,\mathrm{Inn}(A)$ is an involution; then $\theta\,\mathrm{Inn}(A)\theta\,\mathrm{Inn}(A)(X) = X$ for any $X \in G_k$. This also holds for $X = \theta(X)$. We want to show that $\theta(A)A \in Z(G_k)$. Then

$$\begin{aligned}
\theta\,\mathrm{Inn}(A)\theta\,\mathrm{Inn}(A)\big(\theta(X)\big) &= \theta(X)\\
\mathrm{Inn}\big(\theta(A)\big)\,\mathrm{Inn}(A)\big(\theta(X)\big) &= \theta(X)\\
\mathrm{Inn}\big(A\theta(A)\big)\big(\theta(X)\big) &= \theta(X)\\
\theta^{-1}(A)A^{-1}\theta(X)A\theta(A) &= \theta(X)\\
\theta(X)A\theta(A) &= A\theta(A)\theta(X)\\
\big(X^{-1}\big)^T A\big(A^{-1}\big)^T &= A\big(A^{-1}\big)^T\big(X^{-1}\big)^T\\
X\theta(A)A &= \theta(A)AX.
\end{aligned}$$

   Each pair of statements is a double implication.

2. Since $\big(A^{-1}\big)^T A \in Z_{\mathrm{GL}(n,k)}(G_k)$, we re-label it as z^{-1}. Then $A^T = zA$. $Z_{\mathrm{GL}(n,k)}(G_k)$ consists of all scalar multiples $s\,\mathrm{Id}$ of the identity matrix such that $s^n = 1$, since $\det(s\,\mathrm{Id}) = 1$. Hence we can write $z = s$ and we have $A^T = sA$. But $A = A^{TT} = (sA)^T = s^T A^T = s(sA) = s^2 A \implies s = 1$. So $A = A^T$.

■

Example 4.5. The matrix $L_p = \begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix}$ is conjugate to a symmetric matrix. So $\mathrm{Inn}(L_{\frac{n}{2},p})$ is isomorphic as an automorphism to $\mathrm{Inn}(A)$ which meets the requirements of Lemma 4.4.1. However, as we will see, this does *not* mean that $\theta\,\mathrm{Inn}(L_{\frac{n}{2},p})$ is isomorphic as an outer involution to $\theta\,\mathrm{Inn}(A)$. The notion of isomorphic outer involutions is discussed next. □

Now that we know more about the shape of A when $\theta\,\mathrm{Inn}(A)$ is a k-involution, we need to determine which k-involutions are isomorphic.

Lemma 4.4.2. *$\theta\,\mathrm{Inn}(A)$ is isomorphic to $\theta\,\mathrm{Inn}(B)$ if and only if A is congruent to pB, for some $p \in k$.*

Proof. Since A is congruent to pB, there is a matrix $Q \in \mathrm{GL}(n,k)$ such that $Q^T AQ = pB$. For

$C^{-1} \in \mathrm{GL}(n,k)$,

$$\begin{aligned}\mathrm{Inn}(C^{-1})\theta\,\mathrm{Inn}(A)\,\mathrm{Inn}((C^{-1})^{-1}) &= \theta\theta\,\mathrm{Inn}(C^{-1})\theta\,\mathrm{Inn}(A)\,\mathrm{Inn}((C^{-1})^{-1}) \\ &= \theta\,\mathrm{Inn}(\theta(C^{-1})AC) \\ &= \theta\,\mathrm{Inn}(C^{T}AC).\end{aligned}$$

So $\mathrm{Inn}(B) = \mathrm{Inn}(C^{T}AC)$. By Lemma 4.1.4, this forces $C^{T}AC = pB$, for some $p \in k$. ■

Remark 4.4.3. By Lemma 4.4.1, if $\theta\,\mathrm{Inn}(A)$ is an involution, then A is symmetric. We use the relations $\theta\,\mathrm{Inn}\big(\theta(A)\big) = \mathrm{Inn}(A)\theta$ and $\theta\,\mathrm{Inn}(A) = \mathrm{Inn}\big(\theta(A)\big)\theta$ to show that A^{-1} is congruent to pB if $\theta\,\mathrm{Inn}(A) \cong \theta\,\mathrm{Inn}(B)$.

$$\begin{aligned}\Big[\theta\,\mathrm{Inn}(C)\Big]\Big[\theta\,\mathrm{Inn}(A)\Big]\Big[\theta\,\mathrm{Inn}(C)\Big]^{-1} &= \theta\,\mathrm{Inn}(C)\theta\,\mathrm{Inn}(A)\,\mathrm{Inn}\big(C^{-1}\big)\theta \\ &= \theta\,\mathrm{Inn}(C)\theta\,\mathrm{Inn}\big(AC^{-1}\big)\theta \\ &= \mathrm{Inn}\big(\theta(C)\big)\,\mathrm{Inn}\big(AC^{-1}\big)\theta \\ &= \mathrm{Inn}\Big(\big(C^{-1}\big)AC^{-1}\Big)\theta \\ &= \theta\,\mathrm{Inn}\Big[\theta\Big(\big(C^{-1}\big)^{T}AC^{-1}\Big)\Big] \\ &= \theta\,\mathrm{Inn}\big(C(A^{-1})^{T}C^{T}\big) \\ &= \theta\,\mathrm{Inn}\big(CA^{-1}C^{T}\big)\end{aligned}$$

By Lemma 4.1.4, $\theta\,\mathrm{Inn}(A) \cong \theta\,\mathrm{Inn}(B)$ if A^{-1} is congruent to pB for some $p \in k$. This condition is equivalent to the condition in Lemma 4.1.4, and it shows that if two outer k-involutions are $\mathrm{Inn}(G, G_k)$-isomorphic, then they are also $\mathrm{Aut}(G, G_k)$-isomorphic.

Lemma 4.4.4.

1. *Symmetric (non-singular) matrices are congruent to diagonal matrices.*
2. *If* $b_1, \ldots, b_n \in k^*$, *then* $A = \mathrm{Diag}(a_1, \ldots, a_n) \equiv \mathrm{Diag}(b_1^2 a_1, \ldots, b_n^2 a_n) = B$.

Proof.

1. Let A be a symmetric matrix. The claim holds for $n = 1$, trivially. Assume the claim

holds for some $n = k - 1$ where $k \in \mathbb{N}$. We want to show the claim holds for $n = k$. Let

$$A = \begin{bmatrix} a_1 & a_{11} & a_{12} & \dots & a_{1k} \\ a_{11} & a_2 & a_{22} & \dots & a_{2k} \\ a_{12} & a_{22} & a_3 & \dots & a_{3k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{1k} & a_{2k} & a_{3k} & \dots & a_k \end{bmatrix}.$$

Suppose that $a_1 \neq 0$. Let

$$Q = \begin{bmatrix} 1 & -\frac{a_{11}}{a_1} & \dots & -\frac{a_{1k}}{a_1} \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

Then

$$Q^T A Q = \begin{bmatrix} a_1 & 0 \\ 0 & A_k \end{bmatrix},$$

where A_k is symmetric, since for any symmetric matrix A, $P^T A P$ is also symmetric. The induction hypothesis shows that $Q^T A Q$ is a diagonal matrix. If $a_1 = 0$ then there is a non-zero entry in the first column, say $a_{1,i} \neq 0$. For $T = I_n + E_{1,i}$, $T^T A T$ is symmetric with the $(1,1)$ entry non-zero. Then we apply the procedure as above.

2. Choose $Q = \mathrm{Diag}(b_1, \dots, b_n)$. Then $Q^T A Q = B$.

■

Let θ be an outer automorphism of G_k and $\mathrm{Inn}(A)$ be an inner automorphism of G_k. By Lemma 4.4.1, $\theta\,\mathrm{Inn}(A)$ is an involution if and only if A is symmetric. By Lemma 4.4.2, if $\theta\,\mathrm{Inn}(A)$ is congruent to $\theta\,\mathrm{Inn}(B)$, then A is congruent to pB for some $p \in k$. Also, by Lemma 4.4.4, A is congruent to a diagonal matrix. To summarize the situation, the outer involutions are always of the form $\theta\,\mathrm{Inn}(A)$ where A is a diagonal matrix. Moreover, we can write A as $\mathrm{Diag}(1, \dots, 1, N_{p_1}, \dots, N_{p_r})$ where N_{p_i} are (not necessarily unique) non-squares in k. If k is closed or if all elements of k^* are squares, then $A = \mathrm{Id}$.

Theorem 4.4.5. *Let $\theta\,\mathrm{Inn}(A)$ be a k-involution, where θ is the duality automorphism.*

(1) If $k = \mathbb{F}_q$ where $q = 2^r$, then there is one isomorphism class of k-involutions of outer type.

(2) If $k = \overline{\mathbb{F}_q}$, the algebraic closure of $\mathbb{F}_q$, there is one isomorphism class of k-involutions of outer type.

(3) If $k = \mathbb{F}_q(x)$, the field of fractions, then there are infinitely many classes of k-involutions of outer type.

Proof. For the first two cases, there is exactly one square class, so conjugation by a matrix A is equivalent to conjugation by the identity matrix. In other words, A is congruent to the identity matrix. For the last case, there are infinitely many square classes in the field. It is possible to reorder the diagonal elements by congruence with a permutation matrix, so by convention we order the diagonal elements as stated in the previous comments. ■

The outer k-involutions of $\mathrm{SL}(n,k)$ always correspond to $\theta\,\mathrm{Inn}(A)$ where A is semisimple. In fact, if k is a finite field or an algebraically closed field, then A is the identity matrix. If k is infinite and not algebraically closed, e.g. $k = \mathbb{F}_q(x)$, then $A \neq \mathrm{Id}$.

The situation is somewhat simpler than it is for fields k of characteristic not 2. When $k = \mathbb{F}_p$ and $p \neq 2$, there are k-involutions of the form $\theta\,\mathrm{Inn}(J_n)$, and J_n is not semisimple. In all the remaining cases, the outer k-involutions correspond to semisimple matrices.

When k is a field of characteristic 2, the following corollary summarizes the number of isomorphism classes of outer k-involutions of $\mathrm{SL}(n,k)$.

Corollary 4.4.6.

1. *Let k be a finite field, or any algebraically closed field. There is one isomorphism class of outer k-involutions of* $\mathrm{SL}(n,k)$.

2. *Let k be any finite, not algebraically closed field. There are infinitely many isomorphism classes of outer k-involutions of* $\mathrm{SL}(2,k)$.

4.5 Fixed Point Groups and Symmetric k-Varieties

When G_k is an algebraic group, the fixed point groups of isomorphic involutions are isomorphic groups (recall Lemma 3.4.1). This is important in classifying fixed point groups. We need to determine explicitly the fixed point groups for each of the involutions of G_k. We begin with the inner involutions.

Lemma 4.5.1.

1. *The fixed point group of the involution* $\mathrm{Inn}(L_{m,c^2,c})$ *consists of matrices in* G_k *of the form*

$$\begin{bmatrix} \begin{bmatrix} a_{1,1} & b_{1,1} \\ c^2 b_{1,1} & a_{1,1} \end{bmatrix} & \cdots & \begin{bmatrix} a_{1,2m-1} & b_{1,2m-1} \\ c^2 b_{1,2m-1} & a_{1,2m-1} \end{bmatrix} & h_{1,2m} & \cdots & h_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ \begin{bmatrix} a_{2m,1} & b_{2m,1} \\ c^2 b_{2m-1,1} & a_{2m-1,1} \end{bmatrix} & \cdots & \begin{bmatrix} a_{2m-1,2m-1} & b_{2m-1,2m-1} \\ c^2 b_{2m-1,2m-1} & a_{2m-1,2m-1} \end{bmatrix} & h_{2m,2m} & \cdots & h_{2m,n} \\ g_{2m,1} \quad cg_{2m,1} & & g_{2m,2m-1} \quad cg_{2m,2m-1} & s_{2m,2m} & \cdots & s_{2m,n} \\ \vdots \quad \vdots & \cdots & \vdots \quad \vdots & \vdots & & \vdots \\ g_{n,1} \quad cg_{n,1} & & g_{n,2m-1} \quad cg_{n,2m-1} & s_{n,2m} & \cdots & s_{n,n} \end{bmatrix}.$$

This matrix has m 2×2 *blocks in the upper left-hand corner. The upper right-hand corner has the property that the even rows are* c*-multiples of the preceding odd rows. Analogously, the bottom left-hand corner has the property that the even columns are* c*-multiples of the preceding odd columns. Finally, in the bottom right-hand corner, there are no relations.*

2. *The fixed point group of the involution* $\mathrm{Inn}(L_{\frac{n}{2},p})$ *consists of the block matrices*

$$\begin{bmatrix} \begin{bmatrix} a_{1,1} & b_{1,1} \\ pb_{1,1} & a_{1,1} \end{bmatrix} & \cdots & \begin{bmatrix} a_{1,n-1} & b_{1,n-1} \\ pb_{1,n-1} & a_{1,n-1} \end{bmatrix} \\ \vdots & & \vdots \\ \begin{bmatrix} a_{n-1,1} & b_{n-1,1} \\ pb_{n-1,1} & a_{n-1,1} \end{bmatrix} & \cdots & \begin{bmatrix} a_{n-1,n-1} & b_{n-1,n-1} \\ pb_{n-1,n-1} & a_{n-1,n-1} \end{bmatrix} \end{bmatrix}.$$

This matrix consists of 2×2 *blocks, and is basically the same as in case (1) above, in the upper left-hand corner.*

Proof.

1. The matrix $L_{m,c^2,c}$ acts on a matrix A when multiplying on the left and on the right. Let R_i denote the ith row of A, and C_i denote the ith column of A. Multiplication on the left by $L_{m,c^2,c}$ changes A as follows:

   - Replace R_i by $c^2 R_{i-1}$ when i is even and $1 < i \leq 2m$.
   - Replace R_j by R_{j+1} when j is odd and $1 \leq j < 2m$.
   - Replace R_k by cR_k for $k > 2m$.

   Multiplication on the right by $L^{-1}_{m,c^2,c}$ changes A as follows:

- Replace C_i by $\frac{1}{c^2}C_{i-1}$ when i is even and $1 < i \leq 2m$.
- Replace C_j by C_{j+1} when j is odd and $1 \leq j < 2m$.
- Replace C_k by $\frac{1}{c}C_k$ for $k > 2m$.

Now equate entries to get the desired relations.

2. This is simpler than case 1, and the result corresponds to the upper left-hand corner of the matrix in case 1.

■

Example 4.6. Here we explicitly compute the fixed point group of $\mathrm{Inn}(L_{1,c^2,c})$:

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ c^2 & 0 & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & c \end{bmatrix} \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix} \begin{bmatrix} 0 & c^{-2} & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & c^{-1} & 0 \\ 0 & 0 & 0 & c^{-1} \end{bmatrix} = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix}$$

$$\begin{bmatrix} a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ c^2a_{1,1} & c^2a_{1,2} & c^2a_{1,3} & c^2a_{1,4} \\ ca_{3,1} & ca_{3,2} & ca_{3,3} & ca_{3,4} \\ ca_{4,1} & ca_{4,2} & ca_{4,3} & ca_{4,4} \end{bmatrix} \begin{bmatrix} 0 & c^{-2} & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & c^{-1} & 0 \\ 0 & 0 & 0 & c^{-1} \end{bmatrix} = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix}$$

$$\begin{bmatrix} a_{2,2} & c^{-2}a_{2,1} & c^{-1}a_{2,3} & c^{-1}a_{2,4} \\ c^2a_{1,2} & a_{1,1} & ca_{1,3} & ca_{1,4} \\ ca_{3,2} & c^{-1}a_{3,1} & a_{3,3} & a_{3,4} \\ ca_{4,2} & c^{-1}a_{4,1} & a_{4,3} & a_{4,4} \end{bmatrix} = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix}$$

Now we can see that $a_{1,1} = a_{2,2}$, $c^2a_{1,2} = a_{2,1}$, $ca_{4,2} = a_{4,1}$, etc. Thus the fixed points are the matrices with unit determinant of the form

$$\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ c^2a_{1,2} & a_{1,1} & ca_{1,3} & ca_{1,4} \\ a_{3,1} & ca_{3,1} & a_{3,3} & a_{3,4} \\ a_{4,1} & ca_{4,1} & a_{4,3} & a_{4,4} \end{bmatrix}.$$

□

The matrix $L_{m,c^2,c}$ is conjugate to a constant times a unipotent matrix. Let

$$U_c = \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix}$$

and let

$$U_{m,c} = \begin{bmatrix} \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} & & & & & \\ & \ddots & & & & \\ & & \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix}.$$

Then $U_{m,c}L_{m,c^2,c}U_{m,c} = cB$ where

$$B = \begin{bmatrix} 1 & c^{-1} & & & & \\ & \ddots & \ddots & & & \\ & & 1 & c^{-1} & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix}. \tag{4.5.1.1}$$

By a similar method, $L_{\frac{n}{2},p}$ is conjugate (over G_K) to a matrix of the form $\sqrt{p}B$ where

$$B = \begin{bmatrix} 1 & \sqrt{p}^{-1} & & \\ & \ddots & \ddots & \\ & & \ddots & \sqrt{p}^{-1} \\ & & & 1 \end{bmatrix}. \tag{4.5.1.2}$$

So, in both cases, φ is conjugate to some involution of the form $\mathrm{Inn}(B)$, where B is one of 4.5.1.1 or 4.5.1.2, both of which are unipotent matrices. Over fields of characteristic not 2, inner involutions are always semi simple.

Lemma 4.5.2. *Let $k = \mathbb{F}_q$ or $\overline{\mathbb{F}_q}$. Then the fixed point group of the outer automorphism $\theta\,\mathrm{Inn}(A)$ consists of orthogonal matrices with determinant 1. That is, $G_k^{\theta\,\mathrm{Inn}(A)} = \mathrm{O}(n,k)$.*

Proof. By Lemma 4.4.4, A is diagonal. By congruence, we can reduce any squares on the diagonal of A to ones. By Lemma 2.2.4, every non-zero element is a square in k, so A is congruent to the identity matrix. Thus, if X is a fixed point, then $\theta\,\mathrm{Inn}(A)(X) = (X^{-1})^T = X$ and so $X \in \mathrm{O}(n,k)$. Recall that $\mathrm{SO}(n,k) = \mathrm{O}(n,k)$ when k has characteristic 2. ■

Lemma 4.5.3. *Let $k = \mathbb{F}_q(x)$. The fixed point group of $\theta\,\mathrm{Inn}(A)$ is the matrices $X \in G_k$ such that $AX^{-1} = X^TA$, where $A \in \mathrm{GL}(n,k)$ and A is diagonal.*

Proof. Since $\theta \operatorname{Inn}(A)(X) = X$, then $\theta(AXA^{-1}) = X$. So $X = A^{-1}(X^{-1})^T A$, and $AX^{-1} = X^T A$. ■

4.5.4 The Structure of Q_k

For the involutions $\operatorname{Inn}(L_{m,c^2,c})$ and $\operatorname{Inn}(L_{\frac{n}{2},p})$, Q_k has the following structure:

$$\begin{aligned} Q_k &= \left\{ X\big(\operatorname{Inn}(A)(X)\big)^{-1} \mid X \in G_k \right\} \\ &= \left\{ X(A^T)^{-1}X^T A^T \mid X \in G_k \right\}. \end{aligned}$$

In the case that the involutions are outer, we have

$$\begin{aligned} Q_k &= \left\{ X\big(\theta \operatorname{Inn}(A)(X)\big)^{-1} \mid X \in G_k \right\} \\ &= \left\{ X\theta(AXA^{-1})^{-1} \mid X \in G_k \right\} \\ &= \left\{ X\big((A^T)^{-1}(X^T)^{-1}A^T\big)^{-1} \mid X \in G_k \right\} \\ &= \left\{ XA^T X^T (A^T)^{-1} \mid X \in G_k \right\}. \end{aligned}$$

If $A = \mathrm{Id}$, then Q_k consists of symmetric matrices.

Chapter 5

Involutions of $\mathrm{O}(2n+1,k)$

Our goal again is to determine the involutions of $G_k = \mathrm{O}(n,k)$. We will proceed as we did with the $\mathrm{SL}(n,k)$ case. However, we quickly encounter some difficulties. For now, we note some initial findings and state conjectures that we have verified for small field sizes and low dimensional groups. Most of the work in this chapter applies to both even and odd dimensional orthogonal groups over fields k of characteristic 2, though the primary goal is to determine involutions in the odd case. By a similar statement as in Chapter 3, all automorphisms of $\mathrm{O}(2n+1,k)$ are inner automorphisms.

Before considering automorphisms, we introduce some notation and record several pertinent facts. All of this will be used in Section 5.2.

5.1 Strictly Symmetric Matrices

Definition 5.1.1. We will call the matrix $A_n \in \mathrm{GL}(n,k)$ *strictly symmetric* if it is a constant matrix plus a scalar times the identity matrix. That is, if it has the form

$$A_n = \begin{bmatrix} a & b & \dots & b \\ b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \dots & b & a \end{bmatrix}. \tag{5.1.1.1}$$

We will frequently refer to a strictly symmetric matrix as A_n or (5.1.1.1). This matrix is fundamental in determining the inner automorphisms of $\mathrm{O}(n,k)$. With this in mind, we record the following facts for later use.

Lemma 5.1.2. *Let A_n be strictly symmetric, as in (5.1.1.1).*

1. *If n is odd, then* $\det(A_n) = a(a+b)^{n-1}$.

2. *If n is even, then* $\det(A_n) = (a+b)^n$.

Proof. We proceed by complete induction. For the first few values of n, the calculations are straightforward. Assume the claim holds for all n up to and including $n = k$. Let

$$\overline{A_{k-1}} = \begin{bmatrix} b & & \mathbf{b} & \\ & \begin{bmatrix} a & b & \dots & b \\ b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \dots & b & a \end{bmatrix} & & \\ \mathbf{b} & & & \end{bmatrix}, \tag{5.1.2.1}$$

which is the form (up to permutation of rows) of every $(k-1)\times(k-1)$ minor of A_k, except for the (1,1) minor which is simply A_{k-1}. Notice that $\overline{A_{k-1}}$ has a nested copy of A_{k-2} in the bottom right corner. In the following two cases, we use cofactor expansion to find the determinants.
Case I: Assume k is odd. Then $k+1$ is even, so we want to show $\det(A_{k+1}) = (a+b)^{k+1}$. Notice that $k \equiv 1 \pmod 2$ and $k-1 \equiv 0 \pmod 2$. We have

$$\begin{aligned} \det(A_{k+1}) &= a \cdot \det(A_k) + b \cdot k \cdot \det(\overline{A_k}) \\ &= a\big[a(a+b)^{k-1}\big] + b \cdot k\Big[b \cdot \det(A_{k-1}) + (k-1) \cdot b \cdot \det\left(\overline{A_{k-1}}\right)\Big] \\ &= a^2(a+b)^{k-1} + b \cdot 1 \cdot \Big[b \cdot \det(A_{k-1}) + 0 \cdot b \cdot \det\left(\overline{A_{k-1}}\right)\Big] \\ &= a^2(a+b)^{k-1} + b^2 \cdot (a+b)^{k-1} \\ &= (a^2+b^2)(a+b)^{k-1} \\ &= (a+b)^{k+1}, \end{aligned}$$

which is what we wanted to show. Notice that $a^2 + b^2 = (a+b)^2$ if k has characteristic 2.
Case II: Assume k is even. Then $k+1$ is odd. We want to show $\det(A_{k+1}) = a(a+b)^k$. We have

$$\begin{aligned} \det(A_{k+1}) &= a \cdot \det(A_k) + b \cdot k \cdot \det(\overline{A_k}) \\ &= a \cdot (a+b)^k + b \cdot 0 \cdot \det(\overline{A_k}) \\ &= a(a+b)^k, \end{aligned}$$

which is what we wanted to show. ∎

Corollary 5.1.3. *The strictly symmetric matrix A_n in (5.1.1.1) is singular if and only if*

1. *$a = 0$ or $a = b$ when n is odd*
2. *$a = b$ when n is even.*

Lemma 5.1.4. *The inverse of the strictly symmetric matrix A_n in (5.1.1.1) is*

$$A_n^{-1} = \frac{1}{\det(A_n)} \operatorname{Adj}(A_n)^T$$

where $\operatorname{Adj}(A_n)$ *denotes the adjugate matrix of* A_n*, (the matrix of cofactors of* A_n*). Since* A_n *is symmetric,* $\operatorname{Adj}(A_n)^T = \operatorname{Adj}(A_n)$*. The matrix* A_n^{-1} *has the form*

$$A_n^{-1} = \frac{1}{a(a+b)^{n-1}} \begin{bmatrix} (a+b)^{n-1} & b(a+b)^{n-2} & \dots & b(a+b)^{n-2} \\ b(a+b)^{n-2} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b(a+b)^{n-2} \\ b(a+b)^{n-2} & \dots & b(a+b)^{n-2} & (a+b)^{n-1} \end{bmatrix} \tag{5.1.4.1}$$

if n *is odd, and*

$$A_n^{-1} = \frac{1}{(a+b)^n} \begin{bmatrix} a(a+b)^{n-2} & b(a+b)^{n-2} & \dots & b(a+b)^{n-2} \\ b(a+b)^{n-2} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b(a+b)^{n-2} \\ b(a+b)^{n-2} & \dots & b(a+b)^{n-2} & a(a+b)^{n-2} \end{bmatrix} \tag{5.1.4.2}$$

if n *is even.*

Proof. Case I: Suppose n is odd. Then $(i,j)^{th}$ cofactor of A_n, $[A_n]_{i,j}$, is

- $[A_n]_{i,j} = \det\left(\overline{A_{n-1}}\right)$ if $i \neq j$, (see matrix 5.1.2.1)
- $[A_n]_{i,j} = \det(A_{n-1})$ if $i = j$. (see matrix 5.1.1.1)

The diagonal entries of $\operatorname{Adj}(A_n)$ are

$$[A_n]_{i,i} = (a+b)^{n-1}$$

since $n-1$ is even. The off-diagonal entries are slightly more complex:

$$\begin{aligned}
[A_n]_{i,j} &= \det\left(\overline{A_{n-1}}\right) \\
&= b \cdot \det(A_{n-2}) + b \cdot (n-2) \det\left(\overline{A_{n-2}}\right) \\
&= b \cdot \left[a(a+b)^{n-3}\right] + b \cdot \det\left(\overline{A_{n-2}}\right) \\
&= ab(a+b)^{n-3} + b \cdot \left[b \cdot \det(A_{n-3}) + b \cdot (n-3) \det\left(\overline{A_{n-3}}\right)\right] \\
&= ab(a+b)^{n-3} + b \cdot \left[b \cdot (a+b)^{n-3} + 0\right] \\
&= ab(a+b)^{n-3} + b^2 \cdot (a+b)^{n-3} \\
&= (ab+b^2)(a+b)^{n-3} \\
&= b(a+b)^{n-2}
\end{aligned}$$

Case II: Suppose n is even. Then

$$[A_n]_{i,i} = a(a+b)^{n-2}$$

since $n-1$ is odd. The off diagonal entries are

$$\begin{aligned}
[A_n]_{i,j} &= \det\left(\overline{A_{n-1}}\right) \\
&= b \cdot \det(A_{n-2}) + (n-2) \cdot b \cdot \det\left(\overline{A_{n-2}}\right) \\
&= b \cdot (a+b)^{n-2} + 0 \\
&= b \cdot (a+b)^{n-2}
\end{aligned}$$

■

Factoring A_n^{-1} in (5.1.4.1 and 5.1.4.2) leads to nice forms:

$$A_n^{-1} = \frac{1}{a(a+b)} \begin{bmatrix} a+b & b & \dots & b \\ b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \dots & b & a+b \end{bmatrix} \qquad \text{(if } n \text{ is odd)} \qquad (5.1.4.3)$$

$$A_n^{-1} = \frac{1}{(a+b)^2} \begin{bmatrix} a & b & \dots & b \\ b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \dots & b & a \end{bmatrix} \qquad \text{(if } n \text{ is even).} \qquad (5.1.4.4)$$

In particular, it is clear that the inverse of a strictly symmetric matrix (5.1.1.1) is also strictly symmetric. The identity matrix is strictly symmetric, and these two facts together establish the following corollary:

Corollary 5.1.5. *If k has characteristic 2, the strictly symmetric matrices form a subgroup of* $\mathrm{GL}(n,k)$*, which we denote* $\mathrm{St}(n,k)$*.*

Lemma 5.1.6. *Let k be the finite field with $q = 2^r$ elements, where $r \in \mathbb{N}$. Then* $\mathrm{St}(n,k)$ *has $q(q-1)$ elements if n is even, and $(q-1)^2$ elements if n is odd.*

Proof. Suppose n is even. Then there are q choices for a and $q-1$ choices for $b \neq a$, when n is even. The only restriction from the $\det(A_n) = 1$ is that $a \neq b$. When n is odd, the $\det(A_n) = 0$ when $a = 0$ or $a = b$, so there are $q-1$ choices for a and $q-1$ choices for b. In this last case we may choose $b = 0$. ■

Lemma 5.1.7. *Let A_n be a strictly symmetric matrix as in (5.1.1.1). If n is odd, A_n is diagonalizable.*

Proof. By Lemma 5.1.2, the characteristic polynomial for A_n is

$$C_{A_n}(x) = \det(x\,\mathrm{Id} + A_n) = (a+x)\Big((a+x)+b\Big)^{n-1}.$$

From this it is clear that the eigenvalues are $\lambda_1 = a$ and $\lambda_2 = a+b$. The minimal polynomial for A_n is

$$M_{A_n}(x) = (x+a)(x+a+b).$$

If $b = 0$, then $M_{A_n}(x)$ has a repeated linear factor, but in that case A_n is already diagonal. It is simple to verify the minimal polynomial of A_n by a direct calculation.

$$M_{A_n}(A_n) = \begin{bmatrix} 0 & b & \dots & b \\ b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \dots & b & 0 \end{bmatrix} \begin{bmatrix} b & b & \dots & b \\ b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \dots & b & b \end{bmatrix} = \mathbf{0}$$

Note that each entry of the product is $(n-1)\cdot b^2 = 0$, and n is odd; hence $n - 1 \equiv 0 \pmod 2$. Finally, by a standard result from linear algebra (e.g. [26], Theorem 6 on p. 204), any matrix over a field is diagonalizable if and only if the minimal polynomial is a product of distinct linear factors. ■

Example 5.1. Let $n = 3$. Then A_3 has eigenvalues $\lambda_1 = a$ and $\lambda_2 = a + b$. The basis of E_{λ_1} is the basis of the nullspace of $A_3 + \lambda_1 I$; i.e., the nullspace of the matrix

$$\begin{bmatrix} 0 & b & b \\ b & 0 & b \\ b & b & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

The basis is

$$\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\}.$$

Similarly, the basis of E_{λ_2} is

$$\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \right\}.$$

We form the transition matrix

$$P = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

for which $PAP^{-1} = D$, where

$$D = \begin{bmatrix} a & 0 & 0 \\ 0 & a+b & 0 \\ 0 & 0 & a+b \end{bmatrix}.$$

□

The method used in the last example is extensible to dimension $2n + 1$, as in the following lemma.

Lemma 5.1.8. *If n is odd, then A_n (5.1.1.1) is diagonalizable via the transition matrix*

$$P = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 0 & \dots & 0 \\ 1 & 0 & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & 0 & \dots & 0 & 1 \end{bmatrix}.$$

Proof.

$$
\begin{aligned}
PA_nP^{-1} &= \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 0 & \dots & 0 \\ 1 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 1 & 0 & \dots & 0 & 1 \end{bmatrix} \begin{bmatrix} a & b & \dots & b \\ b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \dots & b & a \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ 1 & 1 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 \\ 1 & 1 & \dots & 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} a & a & a & \dots & a \\ a+b & a+b & 0 & \dots & 0 \\ a+b & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a+b & 0 & \dots & 0 & a+b \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ 1 & 1 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 \\ 1 & 1 & \dots & 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} a & 0 & 0 & \dots & 0 \\ 0 & a+b & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & a+b \end{bmatrix}.
\end{aligned}
$$

■

When n is even, the strictly symmetric matrix A_n (5.1.1.1) is not diagonalizable. The best possible form is block diagonal.

Lemma 5.1.9. *If n is even, the strictly symmetric matrix A_n (5.1.1.1) is conjugate to $L_{\frac{n}{2},a^2+b^2}$. That is, a direct sum of $\frac{n}{2}$ blocks of the matrix*

$$
\begin{bmatrix} 0 & a^2+b^2 \\ 1 & 0 \end{bmatrix}
$$

Proof. The characteristic polynomial of A_n is

$$
C_{A_n}(x) = \Big(x + (a+b)\Big)^n,
$$

which follows directly from Lemma 5.1.2. The minimal polynomial of A_n is

$$
M_{A_n}(x) = \Big(x + (a+b)\Big)^2.
$$

This can be verified by calculation:

$$M_{A_n}(A_n) = \begin{bmatrix} b & b & \dots & b \\ b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \dots & b & b \end{bmatrix}^2 = \mathbf{0}$$

since each entry is $n \cdot b^2 = 0$.

The invariant factors of A_n are multiples of $\Big(x + (a+b)\Big)^2 = x^2 + \big(a^2 + b^2\big)$, but that is not enough to determine the rational canonical form of A_n. However, if we can show the maximum dimension of any cyclic subspace is 2, then the invariant factors each have degree 2. This will prove that the invariant factors are $x^2 + (a^2 + b^2)$.

Let $e = (c_1, \dots, c_n)^T$. Then

$$A_n e = \left[\left(ac_1 + b\sum_{k=2}^{n} c_k \right), \dots, \left(ac_i + b\sum_{k=1, k\neq i}^{n} c_k \right), \dots, \left(ac_n + b\sum_{k=1}^{n-1} c_k \right) \right]^T.$$

The kth entry of $(A_n)^2 e$ is

$$a^2 c_k + ab \sum_{\substack{i\neq k \\ i\in[n]}} c_i + ab \sum_{\substack{i\neq k \\ i\in[n]}} c_i + b^2 \sum_{\substack{j\neq k \\ j\in[n]}} \sum_{\substack{i\neq j \\ i\in[n]}} c_i.$$

The first two sums are the same, so they cancel. The double sum contains c_k in an odd number of terms and, for $\ell \neq k$, c_ℓ in an even number of terms. The only surviving terms are $a^2 c_k$ and $b^2 c_k$. So

$$a^2 c_k + ab \sum_{\substack{i\neq k \\ i\in[n]}} c_i + ab \sum_{\substack{i\neq k \\ i\in[n]}} c_i + b^2 \sum_{\substack{j\neq k \\ j\in[n]}} \sum_{\substack{i\neq j \\ i\in[n]}} c_i = c_k\Big(a^2 + b^2\Big).$$

This implies that $A_n^2 e$ is a scalar multiple of e; hence the maximum dimension of any cyclic subspace is 2. It is possible to pick e to be a characteristic vector, but the minimal polynomials for the cyclic subspaces (i.e. the invariant factors) must be divisible by the minimal polynomial of A_n. This forces each invariant factor to have degree 2 or more, and since the degree of the invariant factor is the degree of the cyclic subspace, it can be no more than 2.

So each cyclic subspace in the cyclic decomposition of A_n has dimension 2, and the invariant factors are $(x^2 + (a^2 + b^2))$. There are $\frac{n}{2}$ subspaces in the decomposition.

To put things in the same form as in the $\mathrm{SL}(n, k)$ case, we note that the matrix $\begin{bmatrix} 0 & a^2+b^2 \\ 1 & 0 \end{bmatrix}$ is congruent to $\begin{bmatrix} 0 & 1 \\ a^2+b^2 & 0 \end{bmatrix}$ via the transition matrix $\begin{bmatrix} 0 & a^2+b^2 \\ a^2+b^2 & 0 \end{bmatrix}$. So A_n is congruent to the

matrix in the statement, $L_{\frac{n}{2},a^2+b^2}$. ■

Over the complex numbers, A_n is diagonalizable if n is even, since the minimal polynomial factors as $\Big(x+(a+b)\Big)^2 = (x+a+b)(x-a-b)$ which is a product of distinct linear factors.

5.2 Automorphisms of $\mathrm{O}(n,k)$

Now that we have set up the basic notation, we are ready to proceed with determining some properties of automorphisms of $G_k = \mathrm{O}(n,k)$. Most of these apply to arbitrary n, but at some point we will split the discussion between even and odd cases. Similar to previous chapters, we let $G = \mathrm{O}(n,\overline{k})$ and $G_K = \mathrm{O}(n,K)$ where $k \subset K \subseteq \overline{k}$ are fields of characteristic 2.

Lemma 5.2.1. *Let k be a field of characteristic 2. If $A \in \mathrm{GL}(n,K)$ and $\mathrm{Inn}(A)|_{G_k} = \mathrm{Id}$, then A is strictly symmetric.*

Proof. Let $I_{i,j}$ denote the (i,j) permutation matrix (i.e. the i-th and j-th rows or columns are swapped). Note that $I_{i,j} \in \mathrm{O}(2n+1,k)$. If $\mathrm{Inn}(A)(X) = X$ for every $X \in G_k$, then $AI_{i,j} = I_{i,j}A$. Note that $AI_{i,j}$ is the same as A, except with the i and j columns permuted, and $I_{i,j}A$ is the same as A, but with the i and j rows permuted. For i,j,k,ℓ distinct, the equation forces the following relations:

$$a_{i,k} = a_{j,k} \tag{5.2.1.1}$$

$$a_{\ell,i} = a_{\ell,j} \tag{5.2.1.2}$$

$$a_{i,i} = a_{j,j} \tag{5.2.1.3}$$

$$a_{i,j} = a_{j,i}. \tag{5.2.1.4}$$

More concisely, $a_{ij} = a_{ji}$ for all $i \neq j$, and $a_{ii} = a_{jj}$ for all i and j, where $i,j \in [2n+1]$. ■

Over fields with characteristic not 2, the elements which induce automorphisms that act as the identity on $\mathrm{SO}(n,k)$ are at least diagonal matrices. For most orthogonal groups, these matrices are scalar multiples of the identity matrix; hence they are in the center of $\mathrm{GL}(n,k)$. Over characteristic 2 fields, many more matrices potentially induce inner involutions on G.

Lemma 5.2.2. *The center of $\mathrm{O}(n,k)$ is trivial.*

Proof. Suppose $A \in \mathrm{O}(n,k)$ is in the center of $\mathrm{O}(n,k)$. Then $XA = AX$ for any $X \in \mathrm{O}(n,k)$. This means that $\mathrm{Inn}(A) = \mathrm{Id}$ on $\mathrm{O}(n,k)$. By Lemma 5.2.1, A is strictly symmetric. Since $A \in \mathrm{O}(n,k)$, we know that $A^TA = \mathrm{Id}$, which means that $A^2 = \mathrm{Id}$. We must use a different argument depending on the parity of the dimension of the group.

1. The square of an odd dimensional strictly symmetric matrix is the same as the element-wise square, i.e., if A is strictly symmetric of the form (5.1.1.1), then

$$A^2 = \begin{bmatrix} a^2 & b^2 & \dots & b^2 \\ b^2 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b^2 \\ b^2 & \dots & b^2 & a^2 \end{bmatrix}.$$

   Thus $a^2 = 1$ which means $a = 1$. Also, $b^2 = 0$ which means $b = 0$. (See Lemma 2.2.5.)

2. The square of an even-dimensional strictly symmetric of the form (5.1.1.1) is

$$A^2 = \begin{bmatrix} a^2 + b^2 & & \\ & \ddots & \\ & & a^2 + b^2 \end{bmatrix}.$$

   Thus $a^2 + b^2 = (a + b)^2 = 1$, so $a + b$ must be an element of order 2. This cannot happen when k is finite, since $p^r = q$ is even, and hence $q - 1$ is odd. This implies that the multiplicative group has odd order, so no element can have multiplicative order 2. For $\mathbb{F}_q(x)$, the only possible elements of order 2 must belong to the finite subfield, so the same argument applies. All elements of $\mathbb{F}_q(x)$ that do not belong to the subfield $\mathbb{F}_q$ have infinite order. Since $a + b$ does not have order 2, and since $(a + b)^2 = 2$, then $a + b = 1$.

■

Lemma 5.2.3. *Suppose* $\mathrm{Inn}(A)$ *fixes* $G = \mathrm{O}(n, k)$. *Then* $A^T A$ *is strictly symmetric.*

Proof. Let $A \in \mathrm{GL}(n, k_1)$. If $\mathrm{Inn}(A)$ fixes G, then $\mathrm{Inn}(A)(X) \in G$. That means

$$\big[\mathrm{Inn}(A)(X)\big]^T \big[\mathrm{Inn}(A)(X)\big] = \mathrm{Id}\,.$$

From this we see that

$$\big[AXA^{-1}\big]^T \big[AXA^{-1}\big] = \big(A^{-1}\big)^T X^T A^T A X A^{-1} = \mathrm{Id}$$

which implies that $\mathrm{Inn}(A^T A)(X) = X$ for all $X \in G$. So $\mathrm{Inn}(A^T A) = \mathrm{Id}$, and by Lemma 5.2.1, $A^T A$ is strictly symmetric. ■

Lemma 5.2.4. *Strictly symmetric matrices of odd dimension have a unique strictly symmetric square root.*

Proof. Beginning with the matrix A_n in (5.1.1.1), set

$$\sqrt{A_n} = \begin{bmatrix} \sqrt{a} & \sqrt{b} & \dots & \sqrt{b} \\ \sqrt{b} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \sqrt{b} \\ \sqrt{b} & \dots & \sqrt{b} & \sqrt{a} \end{bmatrix}.$$

The matrix $\sqrt{A_n}$ is the square root of A_n, and clearly $\sqrt{A_n} \in \mathrm{St}(n, \overline{k})$. This fact relies on the property that the square of a strictly symmetric matrix (for odd n) is the element-wise square. Since the square of any field element is unique, the matrix $\sqrt{A_n}$ is unique. ■

Lemma 5.2.5. *Let $A \in \mathrm{St}(2n+1, k)$. Let S be the unique, strictly symmetric square root of A. Let O be symmetric in $\mathrm{O}(2n+1, k)$. Then $\mathrm{Inn}(SO)$ is always an involution corresponding to the strictly symmetric matrix A. That is, $(SO)^2 = A$.*

Proof. Since O is orthogonal, $O^T O = \mathrm{Id}$. Also, note that S commutes with $\mathrm{O}(2n+1, k)$ since $Z_{\mathrm{GL}(n,k)}(G_k) = \mathrm{St}(n, k)$. This means that $(OS)^2 = OSOS = OOSS = O^T OS^2 = \mathrm{Id} \cdot A = A$. ■

Lemma 5.2.6. *The eigenvalues of A are the same as the eigenvalues of A^T.*

Proof.

$$\begin{aligned} &\det(A^T) = \det(A) \\ \implies &0 = \det(A - \lambda \,\mathrm{Id}) = \det(A^T - \lambda \,\mathrm{Id}) = 0 \end{aligned}$$

■

Example 5.2. Symmetric matrices do not have unique square roots. Consider

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

This matrix squares to the identity, which is symmetric. Also notice that another symmetric square root of the identity matrix is the identity matrix itself. There are many more simple examples. □

Example 5.3. Symmetric matrices defined over finite fields do not necessarily have eigenvalues in the field. For example, let

$$A = \begin{bmatrix} \beta^2+1 & 1 & 1 \\ 1 & 0 & \beta^2+\beta+1 \\ 1 & \beta^2+\beta+1 & \beta^2+1 \end{bmatrix},$$

where $A \in \mathrm{GL}(3, \mathbb{F}_8)$. This matrix has characteristic polynomial $C_A(x) = x\beta^2 + x^3 + 1$. None of the roots of $C_A(x)$ are in $\mathbb{F}_8$. □

5.2.7 Conjectures & Computed Results

In the absence of a complete characterization of the involutions of $\mathrm{O}(n, k)$, we close with some conjectures and a summary of results of direct computations. The computations have been instrumental in forming conjectures and guiding the work to this point.

Conjecture 5.2.8. *Let $A \in \mathrm{GL}(n, \overline{k})$ so that $\mathrm{Inn}(A)^2 = \mathrm{Id}$ and $\mathrm{Inn}(A)$ keeps G_k invariant.*

1. *There exist matrices $B \in \mathrm{St}(n, k)$ and $C \in \mathrm{O}(n, \overline{k})$ so that $A = BC$.*
2. *If $X \in G$ and $\mathrm{Inn}(X)\big(G_k\big) = G_k$, then there exists some $Y \in G_k$ so that $\mathrm{Inn}(X)|_{G_k} = \mathrm{Inn}(Y)$.*

Conjecture 5.2.9. *Let n be odd, and let k be a finite field of order $q = 2^r$. Then the fixed point group of an involution $\mathrm{Inn}(A) \in \mathrm{Aut}(G_k)$ has q (symmetric) elements. If $A \in \mathrm{St}(n, k)$ the fixed point group is all of G_k.*

Conjecture 5.2.10. *If A^2 and A^TA are both strictly symmetric, then $A^2 = A^TA$.*

Conjecture 5.2.11. *If $\mathrm{Inn}(A)$ is an involution on $\mathrm{O}(2n+1, k)$, then A is symmetric.*

Proof. If Conjecture 5.2.10 is true, this is also true. By Lemma 5.2.1, since $\mathrm{Inn}(A)$ is an involution, $\mathrm{Inn}(A)^2 = \mathrm{Id}$, and hence A^2 is strictly symmetric. Also, by Lemma 5.2.3, since $\mathrm{Inn}(A)$ fixes G, A^TA is strictly symmetric. By Conjecture 5.2.10, $A^2 = A^TA$. Multiplying by A^{-1} on the right on both sides finishes the proof. ■

By brute force calculations, the involutions of $\mathrm{O}(3, \mathbb{F}_4)$ and $\mathrm{O}(3, \mathbb{F}_8)$ match Lemma 5.2.5; that is, these are the *only* involutions. There are more involutions which come from fields which contain $\mathbb{F}_4$, for example $\mathbb{F}_{16}$ induces more involutions. The following example illustrates this last point.

There are 16 symmetric matrices in $\mathrm{O}(3, \mathbb{F}_4)$ and 9 matrices in $\mathrm{St}(3, \mathbb{F}_4)$ which results in 144 involutions. For $\mathrm{O}(3, \mathbb{F}_8)$, there are 64 symmetric matrices in $\mathrm{O}(3, \mathbb{F}_8)$ and 49 strictly symmetric matrices, for a total of $64 \cdot 49 = 3136$ involutions.

Example 5.4. Let

$$k = \mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$$

where α is a solution of $x^2 + x + 1 = 0$ over $\mathbb{F}_2$, and

$$K = \mathbb{F}_{16} = \left\{ \begin{array}{cccc} 0, & 1, & \gamma, & \gamma + 1, \\ \gamma^2, & \gamma^2 + 1, & \gamma^2 + \gamma, & \gamma^2 + \gamma + 1, \\ \gamma^3, & \gamma^3 + 1, & \gamma^3 + \gamma, & \gamma^3 + \gamma + 1, \\ \gamma^3 + \gamma^2, & \gamma^3 + \gamma^2 + 1, & \gamma^3 + \gamma^2 + \gamma, & \gamma^3 + \gamma^2 + \gamma + 1 \end{array} \right\}$$

where γ is a solution of $x^4 + x + 1 = 0$ over $\mathbb{F}_2$. The subgroup of $\mathbb{F}_{16}$ that corresponds to $\mathbb{F}_4$ is

$$\mathbb{F}_4 = \{0, 1, \gamma^2 + \gamma, \gamma^2 + \gamma + 1\}.$$

Here is an example of an involution of $\mathrm{O}(3, \mathbb{F}_4)$ coming from $\mathrm{O}(3, \mathbb{F}_{16})$. In this case $\mathrm{Inn}(A) \in \mathrm{Aut}(G_K, G_k)$ where

$$A = \begin{bmatrix} \gamma^2 & \gamma^2 & 1 \\ \gamma^2 & \gamma^2 + 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Then $\mathrm{Inn}(A)$ is an involution defined over an extension field K of k, and $\mathrm{Inn}(A)$ is an involution of $\mathrm{O}(3, k)$. Since

$$A^2 = \begin{bmatrix} 1 & \gamma^2 & \gamma^2 \\ \gamma^2 & 1 & \gamma^2 \\ \gamma^2 & \gamma^2 & 1 \end{bmatrix}$$

is strictly symmetric, we expect that $\mathrm{Inn}(A) \in \mathrm{Aut}(G_K)$ is an involution of G_K. Also, since k is a subset of K, we expect that, $\mathrm{Inn}(A) \in \mathrm{Aut}(G, G_k)$, and that it is an involution as well. $\square$

REFERENCES

[1] Silvana Abeasis. On a remarkable class of subvarieties of a symmetric variety. *Adv. in Math.*, 71(1):113–129, 1988.

[2] Cahit Arf. Untersuchungen über quadratische Formen in Körpern der Charakteristik 2. I. *J. Reine Angew. Math.*, 183:148–167, 1941.

[3] Michael Artin. *Algebra*. Prentice Hall Inc., Englewood Cliffs, NJ, 1991.

[4] Alexandre Beĭlinson and Joseph Bernstein. Localisation de g-modules. *C. R. Acad. Sci. Paris Sér. I Math.*, 292(1):15–18, 1981.

[5] Robert W. Benim, Aloysius G. Helminck, Ling Wu, and Christopher E. Dometrius. Involutions of $\mathrm{SO}(2n+1,k)$, $(n>2)$. *To appear.*

[6] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[7] E. Cartan. Sur une classe remarquable d'espaces de Riemann. *Bull. Soc. Math. France*, 54:214–264, 1926.

[8] E. Cartan. Sur une classe remarquable d'espaces de Riemann. II. *Bull. Soc. Math. France*, 55:114–134, 1927.

[9] K. K. A. Cunningham, T. J. Edgar, A. G. Helminck, B. F. Jones, H. Oh, R. Schwell, and J. F. Vasquez. On the Structure of Involutions and Symmetric Spaces of Dihedral Groups. *ArXiv e-prints*, 2012.

[10] C. De Concini and C. Procesi. Complete symmetric varieties. In *Invariant theory (Montecatini, 1982)*, volume 996 of *Lecture Notes in Math.*, pages 1–44. Springer, Berlin, 1983.

[11] C. De Concini and C. Procesi. Complete symmetric varieties. II. Intersection theory. In *Algebraic groups and related topics (Kyoto/Nagoya, 1983)*, volume 6 of *Adv. Stud. Pure Math.*, pages 481–513. North-Holland, Amsterdam, 1985.

[12] Jean Dieudonné. On the automorphisms of the classical groups. With a supplement by Loo-Keng Hua. *Mem. Amer. Math. Soc.*, 1951(2):vi+122, 1951.

[13] Jean Dieudonné. *La géométrie des groupes classiques*. Seconde édition, revue et corrigée. Springer-Verlag, Berlin, 1963.

[14] Christopher Edward Dometrius. *Relationship between symmetric and skew-symmetric bilinear forms on V = k(n) and involutions of SL(n,k) and SO(n,k,beta)*. ProQuest LLC, Ann Arbor, MI, 2003. Thesis (Ph.D.)–North Carolina State University.

[15] Ian Grojnowski. *Character sheaves on symmetric spaces*. ProQuest LLC, Ann Arbor, MI, 1992. Thesis (Ph.D.)–Massachusetts Institute of Technology.

[16] Larry C. Grove. *Classical groups and geometric algebra*, volume 39 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.

[17] Brian C. Hall. *Lie groups, Lie algebras, and representations*, volume 222 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003. An elementary introduction.

[18] Sigurdur Helgason. *Differential geometry, Lie groups, and symmetric spaces*, volume 34 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2001. Corrected reprint of the 1978 original.

[19] A. G. Helminck. On orbit decompositions for symmetric k-varieties. In *Symmetry and spaces*, volume 278 of *Progr. Math.*, pages 83–127. Birkhäuser Boston Inc., Boston, MA, 2010.

[20] Aloysius G. Helminck. Algebraic groups with a commuting pair of involutions and semisimple symmetric spaces. *Adv. in Math.*, 71(1):21–91, 1988.

[21] Aloysius G. Helminck. On the classification of k-involutions. *Adv. Math.*, 153(1):1–117, 2000.

[22] Aloysius G. Helminck and S. P. Wang. On rationality properties of involutions of reductive groups. *Adv. Math.*, 99(1):26–96, 1993.

[23] Aloysius G. Helminck and Ling Wu. Classification of involutions of $\mathrm{SL}(2, k)$. *Comm. Algebra*, 30(1):193–203, 2002.

[24] Aloysius G. Helminck, Ling Wu, and Christopher E. Dometrius. Involutions of $\mathrm{SL}(n, k)$, $(n > 2)$. *Acta Appl. Math.*, 90(1-2):91–119, 2006.

[25] F. Hirzebruch and P. Slodowy. Elliptic genera, involutions, and homogeneous spin manifolds. *Geom. Dedicata*, 35(1-3):309–343, 1990.

[26] Kenneth Hoffman and Ray Kunze. *Linear algebra*. Second edition. Prentice-Hall Inc., Englewood Cliffs, N.J., 1971.

[27] James E. Humphreys. *Linear algebraic groups*, volume 21 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1975.

[28] George Lusztig. Symmetric spaces over a finite field. In *The Grothendieck Festschrift, Vol. III*, volume 88 of *Progr. Math.*, pages 57–81. Birkhäuser Boston, Boston, MA, 1990.

[29] George Lusztig and David A. Vogan, Jr. Singularities of closures of K-orbits on flag manifolds. *Invent. Math.*, 71(2):365–379, 1983.

[30] Derek J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

[31] Steven Roman. *Advanced linear algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer, New York, third edition, 2008.

[32] Winfried Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.

[33] J.-P. Serre. *A course in arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1973.

[34] T. A. Springer. *Linear algebraic groups*, volume 9 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, second edition, 1998.

[35] Y. L. Tong and S. P. Wang. Geometric realization of discrete series for semisimple symmetric spaces. *Invent. Math.*, 96(2):425–458, 1989.

[36] David A. Vogan. Irreducible characters of semisimple Lie groups. III. Proof of Kazhdan-Lusztig conjecture in the integral case. *Invent. Math.*, 71(2):381–417, 1983.

[37] David A. Vogan, Jr. Irreducible characters of semisimple Lie groups. IV. Character-multiplicity duality. *Duke Math. J.*, 49(4):943–1073, 1982.

[38] Robert A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London Ltd., London, 2009.

[39] Ling Wu. *Classification of involutions of* $\mathrm{SL}(n,k)$ *and* $SO(2n+1,k)$. Thesis (Ph.D.)–North Carolina State University.

APPENDICES

Appendix A

Multiplication Tables

A.1 $\mathbb{F}_4$

The polynomial here is $f(x) = x^2 + x + 1$, with roots α and $\alpha + 1$.

	α	$\alpha+1$
α	$\alpha+1$	1
$\alpha+1$	1	α

Table A.1: Multiplication within $\mathbb{F}_4$

A.2 $\mathbb{F}_8$

The polynomial here is $f(x) = x^3 + x + 1$.

A.3 $\mathbb{F}_{16}$

The polynomial here is $f(x) = x^4 + x + 1$. Notice that $\mathbb{F}_4$ is a subgroup. The correspondence is that $\alpha \longleftrightarrow \gamma^2 + \gamma$ and $\alpha + 1 \longleftrightarrow \gamma^2 + \gamma + 1$.

1	β	$\beta+1$	β^2	β^2+1	$\beta^2+\beta$	$\beta^2+\beta+1$
β	β^2	$\beta^2+\beta$	$\beta+1$	1	$\beta^2+\beta+1$	β^2+1
$\beta+1$	$\beta^2+\beta$	β^2+1	$\beta^2+\beta+1$	β^2	1	β
β^2	$\beta+1$	$\beta^2+\beta+1$	$\beta^2+\beta$	β	β^2+1	1
β^2+1	1	β^2	β	$\beta^2+\beta+1$	$\beta+1$	$\beta^2+\beta$
$\beta^2+\beta$	$\beta^2+\beta+1$	1	β^2+1	$\beta+1$	β	β^2
$\beta^2+\beta+1$	β^2+1	β	1	$\beta^2+\beta$	β^2	$\beta+1$

Table A.2: Multiplication within $\mathbb{F}_8$

1	γ	$\gamma+1$	γ^2	γ^2+1	$\gamma^2+\gamma$	$\gamma^2+\gamma+1$	γ^3
γ	γ^2	$\gamma^2+\gamma$	γ^3	$\gamma^3+\gamma$	$\gamma^3+\gamma^2$	$\gamma^3+\gamma^2+\gamma$	$\gamma+1$
$\gamma+1$	$\gamma^2+\gamma$	γ^2+1	$\gamma^3+\gamma^2$	$\gamma^3+\gamma^2+\gamma+1$	$\gamma^3+\gamma$	γ^3+1	$\gamma^3+\gamma+1$
γ^2	γ^3	$\gamma^3+\gamma^2$	$\gamma+1$	$\gamma^2+\gamma+1$	$\gamma^3+\gamma+1$	$\gamma^3+\gamma^2+\gamma+1$	$\gamma^2+\gamma$
γ^2+1	$\gamma^3+\gamma$	$\gamma^3+\gamma^2+\gamma+1$	$\gamma^2+\gamma+1$	γ	$\gamma^3+\gamma^2+1$	γ^3	$\gamma^3+\gamma^2+\gamma$
$\gamma^2+\gamma$	$\gamma^3+\gamma^2$	$\gamma^3+\gamma$	$\gamma^3+\gamma+1$	$\gamma^3+\gamma^2+1$	$\gamma^2+\gamma+1$	1	γ^2+1
$\gamma^2+\gamma+1$	$\gamma^3+\gamma^2+\gamma$	γ^3+1	$\gamma^3+\gamma^2+\gamma+1$	γ^3	1	$\gamma^2+\gamma$	$\gamma^3+\gamma^2+1$
γ^3	$\gamma+1$	$\gamma^3+\gamma+1$	$\gamma^2+\gamma$	$\gamma^3+\gamma^2+\gamma$	γ^2+1	$\gamma^3+\gamma^2+1$	$\gamma^3+\gamma^2$
γ^3+1	1	γ^3	γ	$\gamma^3+\gamma+1$	$\gamma+1$	$\gamma^3+\gamma$	γ^2
$\gamma^3+\gamma$	$\gamma^2+\gamma+1$	$\gamma^3+\gamma^2+1$	$\gamma^3+\gamma^2+\gamma$	γ^2	γ^3+1	$\gamma+1$	$\gamma^3+\gamma^2+\gamma+1$
$\gamma^3+\gamma+1$	γ^2+1	$\gamma^3+\gamma^2+\gamma$	$\gamma^3+\gamma$	1	$\gamma^3+\gamma^2+\gamma+1$	γ^2	$\gamma^2+\gamma+1$
$\gamma^3+\gamma^2$	$\gamma^3+\gamma+1$	$\gamma^2+\gamma+1$	γ^2+1	γ^3+1	$\gamma^3+\gamma^2+\gamma$	γ	$\gamma^3+\gamma$
$\gamma^3+\gamma^2+1$	γ^3+1	γ^2	1	$\gamma^3+\gamma^2$	γ^3	γ^2+1	γ
$\gamma^3+\gamma^2+\gamma$	$\gamma^3+\gamma^2+\gamma+1$	1	$\gamma^3+\gamma^2+1$	$\gamma+1$	γ	$\gamma^3+\gamma^2$	γ^3+1
$\gamma^3+\gamma^2+\gamma+1$	$\gamma^3+\gamma^2+1$	γ	γ^3+1	$\gamma^2+\gamma$	γ^2	$\gamma^3+\gamma+1$	1

1	γ^3+1	$\gamma^3+\gamma$	$\gamma^3+\gamma+1$	$\gamma^3+\gamma^2$	$\gamma^3+\gamma^2+1$	$\gamma^3+\gamma^2+\gamma$	$\gamma^3+\gamma^2+\gamma+1$
γ	1	$\gamma^2+\gamma+1$	γ^2+1	$\gamma^3+\gamma+1$	γ^3+1	$\gamma^3+\gamma^2+\gamma+1$	$\gamma^3+\gamma^2+1$
$\gamma+1$	γ^3	$\gamma^3+\gamma^2+1$	$\gamma^3+\gamma^2+\gamma$	$\gamma^2+\gamma+1$	γ^2	1	γ
γ^2	γ	$\gamma^3+\gamma^2+\gamma$	$\gamma^3+\gamma$	γ^2+1	1	$\gamma^3+\gamma^2+1$	γ^3+1
γ^2+1	$\gamma^3+\gamma+1$	γ^2	1	γ^3+1	$\gamma^3+\gamma^2$	$\gamma+1$	$\gamma^2+\gamma$
$\gamma^2+\gamma$	$\gamma+1$	γ^3+1	$\gamma^3+\gamma^2+\gamma+1$	$\gamma^3+\gamma^2+\gamma$	γ^3	γ	γ^2
$\gamma^2+\gamma+1$	$\gamma^3+\gamma$	$\gamma+1$	γ^2	γ	γ^2+1	$\gamma^3+\gamma^2$	$\gamma^3+\gamma+1$
γ^3	γ^2	$\gamma^3+\gamma^2+\gamma+1$	$\gamma^2+\gamma+1$	$\gamma^3+\gamma$	γ	γ^3+1	1
γ^3+1	$\gamma^3+\gamma^2+1$	γ^2+1	$\gamma^3+\gamma^2$	$\gamma^2+\gamma$	$\gamma^3+\gamma^2+\gamma+1$	$\gamma^2+\gamma+1$	$\gamma^3+\gamma^2+\gamma$
$\gamma^3+\gamma$	γ^2+1	γ^3	γ	1	$\gamma^3+\gamma+1$	$\gamma^2+\gamma$	$\gamma^3+\gamma^2$
$\gamma^3+\gamma+1$	$\gamma^3+\gamma^2$	γ	γ^3+1	$\gamma^3+\gamma^2+1$	$\gamma^2+\gamma$	γ^3	$\gamma+1$
$\gamma^3+\gamma^2$	$\gamma^2+\gamma$	1	$\gamma^3+\gamma^2+1$	$\gamma^3+\gamma^2+\gamma+1$	$\gamma+1$	γ^2	γ^3
$\gamma^3+\gamma^2+1$	$\gamma^3+\gamma^2+\gamma+1$	$\gamma^3+\gamma+1$	$\gamma^2+\gamma$	$\gamma+1$	$\gamma^3+\gamma^2+\gamma$	$\gamma^3+\gamma$	$\gamma^2+\gamma+1$
$\gamma^3+\gamma^2+\gamma$	$\gamma^2+\gamma+1$	$\gamma^2+\gamma$	γ^3	γ^2	$\gamma^3+\gamma$	$\gamma^3+\gamma+1$	γ^2+1
$\gamma^3+\gamma^2+\gamma+1$	$\gamma^3+\gamma^2+\gamma$	$\gamma^3+\gamma^2$	$\gamma+1$	γ^3	$\gamma^2+\gamma+1$	γ^2+1	$\gamma^3+\gamma$

Table A.3: Multiplication within $\mathbb{F}_{16}$

Appendix B

Python Code

The bulk of the examples for finite fields were constructed using a combination of Maple and Python. I have written a small library of functions for working with finite fields in Python. In particular, creating multiplication tables has been useful. I have made my code available to the public via a Google Code project located on the Internet at `http://code.google.com/p/char2/`. The latest improvements will be kept at the Google Code project, and the code below is only current as of the publication of this dissertation. The code is licensed as Free Software, under the terms of the GNU General Public License `http://www.gnu.org/licenses/gpl.html`.

B.1 char2.py

```
# This file is part of char2.

# char2 is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 2 of the License, or
# (at your option) any later version.
#
# char2 is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with char2. If not, see <http://www.gnu.org/licenses/>.
#
# Copyright (C) 2013 Nathaniel Schwartz.

from math_functions import *
from math import pow, log
import sys

mtable = []       # Mulitplication table
r = -1            # The power of the field. The field will have size 2^r
poly = -1         # The irreducible (over {1,0}) polynomial for the field
setup = False     # Set to True when the field size and polynomial are set
register = -1     # The register for the calculator. Currently not functional

# Process command line options.
def getOption():
    option = raw_input("2=0: ").upper()
    cmd = option[0]
    if (cmd == 'Q'):
        exit()
    elif (cmd == 'S'):
        size(option[1:])
    elif (cmd == 'P'):
        polynomial(option[1:])
    elif (cmd == 'T'):
        table(option[1:])
    elif (cmd == 'R'):
        reset()
    elif (cmd == 'V'):
        view()
    elif option.find('+')>= 0:
        add(option)
    elif option.find('*') >= 0:
        multiply(option)
    else:
```

```
        print "Invalid option."

# Print the list of options so the user has information to make a choice.
def printOptions():
    print '='*73
    print 'Welcome to char2, a calculator for fininte fields in even characteristic.'
    print '='*73
    print "R\tReset the state of the program"
    print "S\tSet the size of the field"
    print "P\tSet the polynomial - takes an integer (eg. 7 -> 111 -> a^2 + a + 1)"
    print "T\tPrints the multiplication table - (1 -> numbers, 0 -> strings)"
    print "V\tView the current setup"
    print "Q\tQuits the program"
    print '\n'

# Convert the command line string (of an integer) to an integer.
def polynomial(string):
    input = ''
    try:
        input = int(string.split()[0])
    except IndexError:
        print "Try again."
        return
    if input > 2:
        global poly
        poly = input
    else:
        raise ValueError("Invalid polynomial.")
    # Here we go ahead and create the multiplication table if we can.
    if r > 0:
        global mtable
        global setup
        mtable = getTable(r,poly)
        setup = True

# Multiply some elements of the field.
def multiply(multiplicands):
    global register
    x = -1
    loc = multiplicands.split('*')
    if setup:
        try:
            x = int(loc[0])
        except ValueError:
            x = -1
        if (x < 0 and register > 0):
            x = register
        else:
            print "Register is empty!"
            return
```

```
        try:
            y = int(loc[1])
        except ValueError:
            print "Invalid multiplication input."
            return
        global mtable
        try:
            elt = mtable[x][y]
        except IndexError:
            print "Element isn't in the defined field."
            return
        print printElt(elt) + "\t[" + str(elt) + "]"
        register = elt
    else:
        print "Set options first!"

# Add some elements of the field.
def add(summands):
    x = -1
    global register
    loc = summands.split('+')
    if setup:
        try:
            x = int(loc[0])
        except ValueError:
            x = -1
        if (x < 0 and register > 0):
            x = register
        else:
            print "Register is empty!"
            return
        try:
            y = int(loc[1])
        except ValueError:
            print "Invalid addition input."
            return
        elt = addElts(x,y)
        print str(printElt(elt)) + "\t[" + str(elt) + "]"
        register = elt
    else:
        print "Set options first!"

# Print the multiplication table, either in integer or string format.
def table(option):
    input = ''
    try:
        input = int(option.split()[0])
    except IndexError:
        print "Try again."
        return
```

```
    if input == 0:
        printTable(mtable)
    elif input == 1:
        for row in mtable[1:]:
            print row[1:]
    else:
        raise ValueError("Invalid Table Option.")

# Set the size of the field. User input should be the size. We convert it to
# the power of 2 here.
def size(option):
    try:
        value = int(option.split()[0])
    except IndexError:
        print "Invalid size argument."
        return
    if value > 1:
        global r
        rtmp = int(log(value,2))
        if pow(2, rtmp) != value:
            print 'Field size should be a power of 2.'
            return
        else:
            r = rtmp
    else:
        raise ValueError("Invalid integer.")
    if poly > 0:
        global mtable
        global setup
        mtable = getTable(r,poly)
        setup = True

# View the current field setup.
def view():
    if r > 1:
        print 'The field has', int(pow(2,r)), 'elements, and the polynomial is',
            printElt(poly),
    else:
        print 'The field is not defined yet.'

# Reset the field setup.
def reset():
    global mtable
    global r
    global poly
    global setup
    mtable = []
    r = -1
    poly = -1
    setup = False
```

```
    register = -1

# EXECUTION LOOP
# ==============
# This is the main loop which runs the program
printOptions()
while(True):
    try:
        getOption()
    except ValueError as e:
        print e
```

B.2 math_functions.py

```
# This file is part of char2.

# char2 is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 2 of the License, or
# (at your option) any later version.
#
# char2 is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with char2. If not, see <http://www.gnu.org/licenses/>.
#
# Copyright (C) 2013 Nathaniel Schwartz.

from math import log, ceil

# Make a 2x2 array of values, a multiplication table.
def getTable(q,p):
    n = pow(2,q) - 1
    table = []
    table.append([0]*(n+1))
    for i in range(1,n + 1):
        row = [0]
        for j in range(1,n + 1):
            row.append(multiply(i,j,p,q))
        table.append(row)
    return table

# Print the multiplication table.
def printTable(table):
    size = len(table[1])
    wordLength = 0
    for i in range(size):
        word = printElt(i+1)
        if len(word) > wordLength:
            wordLength = len(word)
    overline = '+' + '-'*(wordLength+2)

    print '-' *((size - 1) * (wordLength + 3) + 1)
    for row in table[1:]:
        rowString = '| '
        for code in row[1:]:
            elt = printElt(code)
            sizeOfElement = len(elt)
            if sizeOfElement < wordLength:
```

```
                elt += ' '*(wordLength - sizeOfElement)
            rowString += elt + ' | '
        print rowString
        print overline * (size - 1) + '+'

# Multiply a and b, given the irreducible polynomial p and the size of the
# field q = 2^r. Here a and b are elements of F_q and the field has
# n = 2^q - 1 non-zero elements.
def multiply(a, b, p, q):
    result = []
    v = bv(a)
    w = bv(b)
    long = []
    short = []
    n = pow(2,q)

    #find the short array
    if len(v) >= len(w):
        long = v
        short = w
    else:
        long = w
        short = v
    size = len(long)

    #pad the shorter array
    short.reverse()
    for x in range(len(short), size):
        short.append(0)
    short.reverse()

    #multiply short * long
    tempv = []
    addends = []
    for x in range(size):
        temp = scale(short[size-x-1], long)
        for y in range(x):
            temp.append(0)
        addends.append(temp)
    for x in range(len(addends)):
        result = xor(result, addends[x])
    #if the number is bigger than the polynomial, mod xor that with p.
    intval = bv2int(result)
    while intval >= n:
        result = reduce(result, p)
        intval = bv2int(result)
        result = bv(intval)

    return intval
```

```
# Reduce an element to standard form.
# Eg, a^3 + a + 1 is not in F_4, so reduce it using a^2 + a + 1 = 0.
def reduce(vector, p):
    vec = vector[:]
    poly = bv(p)
    l = len(vector)
    diff = l - len(poly)
    temp = poly[:]
    for x in range(diff):
        temp.append(0)
    vec = xor(vec, temp)
    return vec

# Scale a vector by 1 or 0.
def scale(scalar, vector):
    result = []
    for x in range(len(vector)):
        result.append(scalar*vector[x])
    return result

# XOR the bits of two arrays.
def xor(a, b):
    result = []
    long = []
    short = []

    #find the short array
    if len(a) >= len(b):
        long = a
        short = b
    else:
        long = b
        short = a

    #pad the shorter array
    short.reverse()
    for x in range(len(short), len(long)):
        short.append(0)
    short.reverse()

    #do the xor operation
    for i in range(len(short)):
        result.append(long[i]^short[i]);
    for i in range(len(short), len(long)):
        result.append(long[i])

    return result

# Compute the binary representation of an integer, a vector of binary digits.
def bv(a):
```

```
    b = a
    result = []
    for i in range(1,len(bin(a))-1):
        result.append(b%2)
        b = b/2
    result.reverse()
    return result

# Converts a vector of binary digits to an integer.
def bv2int(v):
    v.reverse()
    result = 0
    for s in range(len(v)):
        result = result + v[s]*pow(2,s)
    v.reverse()
    return result

# Add two field elements.
def addElts(a,b):
    u = bv(a)
    v = bv(b)
    w = xor(u,v)
    return bv2int(w)

# Convert an element to a string.
def printElt(elt):
    if elt < 1:
        return '0'
    char = bv(elt)
    n = len(char)
    result = ''
    list = [i for i in reversed(range(len(char)))]
    for i in range(len(char)):
        if i == 0:
            if len(char) > 2:
                result = 'a^%i' % (list[i])
            if len(char) == 2:
                result = 'a'
            if len(char) == 1:
                result = '1'
            if len(char) == 0:
                result = '0'
        elif (i < n-2 and char[i] == 1):
            result = result + ' + a^%i' % (n-i-1)
        elif (i == n-2 and char[i] == 1):
            result = result + ' + a'
        elif (i == n-1 and char[i] == 1):
            result = result + ' + 1'
    return result
```