Abstract

**Dometrius, Christopher.** Relationship Between Symmetric and Skew-Symmetric Bilinear Forms on \( V = k^n \) and Involutions of \( \text{SL}(n, k) \) and \( \text{SO}(n, k, \beta) \) (under the direction of Dr. Aloysius Helminck). In this paper, we show how viewing involutions on matrix groups as having been induced by a given non-degenerate symmetric or skew-symmetric bilinear form on the vector space of corresponding dimension can lead to a classification up to isomorphism of the resulting reductive symmetric space in the group setting. We establish a direct link between bilinear algebraic properties of the vector space \( V = k^n \) for an arbitrary field \( k \) of characteristic not 2 and involutions of the matrix group \( G \), where \( G \) is a subgroup of \( \text{GL}(n, k) \). Symmetric spaces are defined in terms of involutions, and the development of this classification theory which classifies the involutions also classifies the symmetric spaces coming from these involutions.

We classify all involutions on \( \text{SL}(n, k) \) and develop important foundations for a full classification of the involutions of \( \text{SO}(n, k, \beta) \) where \( \beta \) is any non-degenerate symmetric bilinear form. We prove that all involutions of \( \text{SO}(n, k, \beta) \) are inner when \( n \) is odd. Additionally, we provide criteria for the matrix which gives the conjugation that is the inner involution of \( \text{SO}(n, k, \beta) \), which covers all involutions when \( n \) is odd and all involutions which can be written as conjugations when \( n \) is even, a fact which is proven in this thesis.
RELATIONSHIP BETWEEN SYMMETRIC AND SKEW-SYMMETRIC BILINEAR FORMS ON $V = K^N$ AND INVOLUTIONS OF $\text{SL}(N, K)$ AND $\text{SO}(N, K, \beta)$

BY

Christopher Dometrius

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

DEPARTMENT OF MATHEMATICS

RALEIGH
June 30, 2003

APPROVED BY:

________________________________________________________________________

________________________________________________________________________

CHAIR OF ADVISORY COMMITTEE
This thesis and the work that went into it are dedicated to my advising professor and mentor Dr. Aloysius Helminck and to my son Holden, who continually gives me the inspiration required for such endeavors.
Biography

Christopher Dometrius was born in San Diego, CA on December 27, 1971. He graduated high school in 1990 from Lubbock High School and got his Bachelor of Arts in Mathematics from Texas Tech University, also in Lubbock, Texas, in August 1994. Since Fall 1997 he has attended graduate school and taught classes in the Mathematics Department at North Carolina State in Raleigh, obtaining his Master of Science degree in Spring 2000. He passed his preliminary written examinations in Algebra, Topology, and Linear/Lie Algebra and now focuses on Algebra. He has a son, a stepson, and two guitars.
Acknowledgements

I would like to first acknowledge my advisor and personal friend Loek Helminck, without whom I would not have had the confidence and backing to pursue a PhD, and my son Holden, who continues to amaze me with his youthful insight. Additional acknowledgement is due towards my stepson Zane for his patience and my wife Carla for being the initial encouragement for me to pursue a graduate degree in Mathematics. My friend Dan Gagliardi deserves special acknowledgement as a source of strong spiritual support and mathematical inspiration. My good friends Marice Tsai and Joe Ferrer deserve mention for their personal support in times when it was much needed. Dr. Jennifer Fowler (who worked with Loek Helminck along with Dr. Gagliardi and myself) is also deserving of mention for mathematical support and motivation. Also deserving of special mention are all the professors at NCSU who provided me with motivation and confidence and generally set the tone for my development in Mathematics. This would include Dr. Ernest Stitzinger, with whom I have spent many an hour in discussions professional and personal, and who along with Dr. Helminck I consider the prime example of what it takes to achieve the elusive goal of being both a gifted mathematician and a truly wonderful person. Additionally it would include Dr. Tom Lada and Dr. Naihuan Jing (the other members of my committee), who inspired me with their obvious enthusiasm for the study and teaching of Mathematics. Lastly, I would like to thank all our receptionists, most specifically Brenda Currin and Di Bucklad, our librarian Carolyn Gunton, and our former Graduate Secretary April Jackson, for providing a wholly positive atmosphere in our department.
# Table of Contents

## List of Tables

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>vii</td>
</tr>
</tbody>
</table>

## 1 Introduction

1.1 The History of Symmetric Spaces ................................... 1
1.2 The History of Bilinear Algebra .................................... 3
1.3 The Link Between Bilinear Algebra and Symmetric Spaces .......... 4
1.4 Summary of Results ................................................... 6

## 2 Preliminaries

2.1 Symmetric Spaces .................................................... 14
2.1.1 Preliminaries ..................................................... 14
2.1.2 Definition of Symmetric Spaces .................................. 15
2.2 Bilinear Forms ...................................................... 16
2.3 Isomorphism of Involution ............................................ 17
2.4 Involutions Obtained from Bilinear Forms .......................... 18
2.4.1 Adjoint of a Matrix .............................................. 18
2.4.2 Using the Adjoint to Construct Involutions ..................... 20
2.4.3 Orthogonal Group of the Form ................................... 20
2.4.4 Symmetric Spaces Revisited ..................................... 21
2.5 Semi-Congruence and the Classification Theorem .................. 22
2.6 Why Focus on \( SL(n, k) \)? .......................................... 26

## 3 Involutions of \( SL(2, k) \)

3.1 Preliminaries .......................................................... 28
3.2 Importance of the Square-Class Group \( k^*/(k^*)^2 \) .......... 29
3.3 The \( p \)-adic Numbers ............................................... 33
3.4 Classification of Involution of \( SL(2, k) \) ......................... 34
3.5 A Note on the Skew-Symmetric Form on \( k^2 \) .................... 35
3.6 Illustration of Resulting Symmetric Spaces ......................... 36
3.7 Table of Involutions of \( G = SL(2, k) \) .......................... 37
# 4 Involutions of SL\((n, k)\)

4.1 Preliminaries ................................................. 40
4.2 Outer Involutions of SL\((n, k)\) ................................... 40
4.3 Congruence Properties of Symmetric / Skew-Symmetric \(n \times n\) Matrices ... 43
4.4 Classification of Outer Involutions of SL\((n, k)\) for \(k \neq \mathbb{Q}_p\) ............ 44
4.5 Classification of Outer Involutions of \(G = SL(n, \mathbb{Q}_p)\) ....................... 48
  4.5.1 Results for \(k = \mathbb{Q}_2\) ................................ 48
  4.5.2 Results for \(k = \mathbb{Q}_p\) \((p \neq 2)\) .......................... 53
4.6 Classification of Inner Involutions of SL\((n, k)\) .................................... 55
  4.6.1 Inner Involutions of SL\((n, k)\) .................................. 55
  4.6.2 Theory for Classifying Inner Involutions of \(G\) ............................... 57
  4.6.3 Summary of Inner Classes for \(n\) Even .................................. 57

# 5 Involutions of SO\((n, k, \beta)\)

5.1 Meaning of the Term “Orthogonal” ................................ 61
5.2 Matrices \(A\) Such That \(\text{Inn}_A = \text{Id}\) .................................. 62
5.3 Matrices \(A\) Such That \(\text{Inn}_A\) is an Automorphism of \(G\) ........................ 74
  5.3.1 Characterization Theorem ........................................ 74
  5.3.2 Proof of Characterization Theorem Part I ............................ 75
  5.3.3 Proof of Characterization Theorem Part II for \(n = 3\) .................... 79
  5.3.4 Proof of Characterization Theorem Part II for \(n = 4\) .................... 86
  5.3.5 General Proof of Characterization Theorem Part II, \(n\) Odd ............... 96
  5.3.6 General Proof of Characterization Theorem Part II, \(n\) Even .............. 100
5.4 Results for \(G = SO(n, k, \beta), n\) Odd .......................... 107
  5.4.1 Some Theory for \(G = SO(n, k, \beta), n\) Odd .......................... 107
  5.4.2 Some Results for \(G = SO(n, k), n\) Odd ......................... 108
  5.4.3 More Theory for \(G = SO(n, k, \beta), n\) Odd ...................... 111

List of References .................................................. 120
List of Tables

3.1 Involutions on SL(2, k) ................................................................. 39

4.1 Outer Involutions of $G$ over $k \neq \mathbb{Q}_p$ ......................................... 47
4.2 Outer Involutions of $G$ over $k = \mathbb{Q}_2$ ............................................. 52
4.3 Outer Involutions of $G$ over $k = \mathbb{Q}_p$ ($p \neq 2$) .............................. 56
4.4 Inner Involution Classes on $G$ .......................................................... 59
4.5 Summary: Number of Involution Classes of $G$ ....................................... 60
Chapter 1

Introduction

1.1 The History of Symmetric Spaces

The work of this thesis relates to Lie groups (or algebraic groups) and symmetric spaces obtained from these. The main goal is a field-independent method of classifying symmetric spaces up to isomorphism. The way of approaching this is to classify the involutions which give us our symmetric space. We obtain our symmetric space by starting with a reductive linear algebraic group $\bar{G}$ defined over an arbitrary field $k$ (of characteristic not equal to 2) and analyzing the space $G/H$, where $\bar{H}$ is the fixed point group of an involution of $\bar{G}$ and $G$, resp. $H$, are the sets of $k$-rational points of $\bar{G}$, resp. $\bar{H}$. Classification of the involution leads to classification of the subgroup $H$, which enables us to characterize the related symmetric space $G/H$. The main focus for this dissertation predominantly involves the relationship between the bilinear algebraic properties of a given non-degenerate symmetric or skew-symmetric bilinear form on the vector space $V = k^n$ and corresponding group-theoretic properties of related involutions of linear algebraic groups $G$ contained in $GL(n, k)$.

Symmetric spaces are of importance in many fields of science, but their main use has been in mathematics and physics. The study of symmetric spaces involves group theory, geometry, field theory, linear algebra, and Lie algebras, as well as involving the related disciplines of topology, manifold theory, and analysis. Symmetric spaces have been studied almost 100 years, with the initial theory focusing on symmetric spaces over the real numbers.
Chapter 1. Introduction

and their important role in mathematical physics, representation theory, harmonic analysis, and differential geometry. More recently the field of research has expanded to include the study of these spaces over general fields of characteristic not 2, and the applications of such generalization has been shown to yield results important to not only the areas mentioned above but also to number theory, quadratic forms, algebraic geometry, combinatorics, automorphic functions, and more.

The original pioneer in the study of symmetric spaces was E. Cartan, who initiated and developed the theory in the 1920s. In [Helg78], Sigurdur Helgason outlines Cartan’s development of the machinery for investigating symmetric spaces. Cartan formulated the problem of classifying Riemannian locally symmetric spaces, defined as “Riemannian manifolds for which the curvature tensor is invariant under all parallel translations,” in two different ways. The first involved studying the holonomy group of a Riemannian manifold, which is the group of linear transformations of the tangent space of the manifold at a given point resulting from parallel translation along closed curves which start at the given point. Such holonomy groups coming from different points in the manifold are all isomorphic, so that the point may be chosen arbitrarily. Cartan showed that for a given Lie algebra of the identity element of holonomy group, if a tensor satisfies certain formulas and also satisfies the criteria for a curvature tensor, then there is a locally symmetric space where it is the curvature tensor for the symmetric space at a given point. Helgason uses this to extend the locally symmetric space to a globally symmetric space. Cartan then pointed out that this reduced the classification problem to two other problems: that of classifying all holonomy groups of the symmetric spaces and the problem of determining the curvature tensor of a symmetric space up to a constant using the holonomy group. Cartan was able to use his established work on finite-dimensional Lie algebras to attack the former, but for the latter “the necessarily extensive calculations were not carried out in all details” due to the development of an easier approach [Helg78].

Cartan’s second formulation of the problem of classifying these Riemannian locally symmetric spaces is the approach which Helgason used, and inspires the approach used in this thesis. It is based upon using the equivalence between the curvature tensor being
invariant and the geodesic symmetry with respect to a given point being a local isometry. When a Riemannian globally symmetric space has the property that the geodesic symmetry will always extend to a global isometry, then Helgason points out that these spaces “have a transitive group of isometries and can be represented as coset spaces $G/K$ [the same as our $G/H$] where $G$ is a connected Lie group with an involutive automorphism $\rho$ whose fixed point set is (essentially) $K$ [again, $H$ in our notation]”. After dividing out a motion group of a Euclidean space, this group $G$ will then become semi-simple. This restricts the problem to investigating involutions of semisimple Lie algebras. Helgason proved the equivalence of these two formulations of a symmetric space. In this paper we do not focus on the Lie algebra setting, but we use this idea of how the problem is realized in a group-theoretic context, and we extend the situation for groups defined over arbitrary fields $k$ of characteristic not equal to 2. These generalized symmetric spaces for arbitrary fields $k$ of characteristic not equal to 2 were introduced by Helminck and Wang in [HW93] and they are also called symmetric $k$-varieties.

1.2 The History of Bilinear Algebra

Interestingly, about the same time that Cartan was developing the idea of symmetric spaces, the beginnings of modern Bilinear Algebra were also being developed. In the 1920s, H. Hasse solved the algebraic part of Hilbert’s problem 11 of his 23 problems by theorizing and proving an equivalence criteria for quadratic forms defined over algebraic number fields. This inspired the 1937 paper by Ernst Witt—who is regarded as the major pioneer in this field just as Cartan was the major pioneer in the field of symmetric spaces—on the theory of Bilinear Algebra (more specifically, the theory of quadratic forms). In his recent text *Bilinear Algebra: An Introduction to the Algebraic Theory of Quadratic Forms*, Kazimierz Szymiczek outlines this history of the development of modern Bilinear Algebra [Szy97]. Witt, considered the father of this field of study, simplified the earlier work by Hasse and also simplified a proof by Emil Artin that an invariant now referred to as the *Hasse algebra*, which Artin introduced, is well-defined. In this manner Witt drew upon a number of sources to
Chapter 1. Introduction

develop his theory. In addition to noting that Witt’s motivation stems from many well-known mathematicians including Gauss, Euler, Minkowski, and Hilbert, Szymiczek points out that it is in fact “customary to believe that Pierre Fermat is responsible for turning attention to the beauty and importance of the subject of quadratic forms [i.e. Bilinear Algebra] in number theory.”

Among Witt’s contributions are what are now termed the Orthogonal Complement Theorem, the Cancellation Theorem, the Witt decomposition of a bilinear space, the Witt ring of similarity classes of nonsingular symmetric spaces, the introduction of the Clifford algebra of an arbitrary quadratic form (which he used to prove that the Hasse algebra of a quadratic form is a an equivalence invariant which is well-defined), and the Witt Chain Isometry Theorem. Other major contributors to this endeavor over the years include Albrecht Pfister, J.K. Arason, M. Knebusch, J. Milnor, and D. Husemoller. Witt’s research worked under the same assumption we use in this thesis that the characteristic of the base field \( k \) is not 2, although Knebusch, Milnor, and Husemoller in particular were able to introduce the general notion of the Witt ring of bilinear forms over an arbitrary commutative ring. The study of Bilinear Algebra is both elegant and contemporary, as noted by Szymiczek in a comment to the reader: “[If] you have some more specialized knowledge of algebra, particularly of field theory, there is a branch of Bilinear Algebra awaiting your activity. Transcendental extensions, valuation theory, \( K \)-theory of fields, algebraic number theory, commutative algebra, finite dimensional algebras—all provide routes for investigations with deep results available and fascinating open problems”. As this was written recently, in 1997, this provides encouragement to those researching the ideas and properties of modern Bilinear Algebra.

1.3 The Link Between Bilinear Algebra and Symmetric Spaces

With this introduction, we work to tie together these different areas of mathematics, finding bonds between the group setting of isomorphism of symmetric spaces and the bilinear
algebraic ideas of congruence of non-degenerate symmetric and skew-symmetric bilinear forms over arbitrary fields $k$ whose characteristic is not 2. The major link comes when we show how given such a bilinear form we may construct an involution of the matrix group defined over the same field $k$. This link is realized in what we term the Classification Theorem, presented in Chapter 2.

Most of the reductive linear algebraic groups are defined by bilinear forms. Since the fixed point group of an involution is also reductive, one can expect that many involutions are associated to symmetric or skew-symmetric bilinear forms. We show that all outer involutions of $SL(n, k)$ come from bilinear forms, as well as all inner involutions of $SO(n, k, \beta)$ ($n > 2$) for a general bilinear form $\beta$ not necessarily the standard dot product. In particular, when $n$ is odd all involutions of $SO(n, k, \beta)$ are inner, which allows us to show in this work the important result that all involutions of $SO(n, k, \beta)$ come from bilinear forms when $n$ is odd.

Specifically, this thesis focuses on what information we can obtain about a particular symmetric space by looking at the bilinear algebraic properties of a non-degenerate symmetric or skew-symmetric bilinear form over the vector space $V = k^n$, where $k$ is the field over which the algebraic group $G$ is defined. Given such a form $\beta$ and a matrix $A \in M_n(k)$, we define its adjoint $A'$ by the formula

$$\beta(Ax, y) = \beta(x, A'y)$$

for all $x, y \in V$.

We then define our involution $\theta_\beta$ by $\theta_\beta(A) = (A')^{-1}$, and the properties of the adjoint guarantee that this is indeed an involution of $G$. The subgroup $H$ is then defined to be the fixed-point group of $\theta_\beta$.

A major goal is the classification of such involutions up to $Inn(G)$-isomorphism, where 2 involutions $\theta$ and $\tau$ are isomorphic if and only if $\tau$ can be obtained from $\theta$ via conjugation by an inner automorphism of $G$. In this dissertation we show that 2 involutions obtained from non-degenerate symmetric/skew-symmetric forms are isomorphic if and only if $\beta_\tau$ and $\beta_\theta$ are congruent up to multiplication by an element in the center of $G$ (so for $SL(n, k)$ this means congruent up to a scalar multiple). This yields a nice classification of outer involutions.
of $\text{SL}(n, k)$. Moving on to $\text{SO}(n, k, \beta)$, the special orthogonal group corresponding to a bilinear form $\beta$, since it is proven in this paper that all inner involutions of $\text{SO}(n, k, \beta)$ are restrictions of outer involutions of $\text{SL}(n, k)$ to $\text{SO}(n, k, \beta)$, all inner involutions in this case come from bilinear forms as well. So in this case we have 2 bilinear forms: one for the group and one for the involution. The classification of these involutions for $\text{SL}(n, k)$ gives us a first invariant to characterize the isomorphism classes of inner involutions for $\text{SO}(n, k, \beta)$. The next step is to determine into how many $\text{SO}(n, k, \beta)$-isomorphism classes one $\text{SL}(n, k)$-isomorphism class splits. This depends on the field in question, and we investigate how to classify this for a number of fields, including algebraically closed fields, the real numbers, $p$-adic numbers and finite fields.

This machinery we develop sets up a framework for determining isomorphism classes of involutions of different subgroups of $\text{SL}(n, k)$. This specific discipline promises continuing classification problems as well as more general problems in the area of symmetric spaces over arbitrary fields, and the research may be expanded to include many other properties of these symmetric spaces, like the double coset decompositions $H \backslash G / H$ and $P \backslash G / H$, where $P$ is a parabolic $k$-subgroup. These decompositions are generalizations of the Cartan and Iwasawa decompositions in the real case. This field of study has the promise of continued importance due to its relevance in such a wide variety of inter-related disciplines, with some of my fellow graduate students working on computer algorithms to determine the structure of symmetric spaces by looking in particular at the root spaces and weight lattices related to the the symmetric spaces, while others study the harmonic analysis of these symmetric spaces over the $p$-adic numbers.

1.4 Summary of Results

(1) In Chapter 2 we give a criterion for the isomorphism of 2 involutions on $\text{GL}(n, k)$ coming from bilinear forms which we call the Classification Theorem, using a notion we call "semi-congruence" of 2 bilinear forms. We prove that we may also use this criteria for investigating the involutions of $\text{SL}(n, k)$. This allows us to focus on the bilinear-algebraic
Condition (2) We show that all involutions of $SL(2, k)$, for $k$ a general field of characteristic not 2, come from bilinear forms. The aforementioned criterion for isomorphism is then used for a complete classification of all involutions of $SL(2, k)$. We determine the number of involutions up to isomorphism for the different fields of importance:

(a) $k = \bar{k}$: There is 1 involution up to isomorphism, corresponding to the 1 congruence class of bilinear forms represented by the identity matrix.

(b) $k = \mathbb{R}$: There are 2 involutions, relating to the 2 semi-congruence classes of bilinear forms represented by the identity matrix and by the matrix $M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. We point out the distinction between the 2 semi-congruence classes and the 3 congruence classes, as well as why we use the former rather than the latter for our classification of the related involutions.

(c) $k = \mathbb{Q}$: We determine that there are infinitely many involutions over the rational numbers.

(d) $k = \mathbb{F}_p$ ($p \neq 2$): There are 2 involutions, one coming from the bilinear form represented by the identity matrix and one coming from the matrix $M = \begin{pmatrix} 1 & 0 \\ 0 & S_p \end{pmatrix}$ where $S_p$ is a representative of the element of $(\mathbb{k}^*)/(\mathbb{k}^*)^2$ of the set of non-squares of $\mathbb{k}^*$.

(e) $k = \mathbb{Q}_2$: There are 8 involution classes, coming from the bilinear forms represented by the identity matrix and by $M = \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix}$ where $m = -1, 2, -2, 3, -3, 6, or -6$.

(f) $k = \mathbb{Q}_p$ ($p \neq 2$): We get 4 classes of involutions, corresponding to the bilinear forms represented by the identity matrix and by $M = \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix}$ with $m = p, S_p, or pS_p$.

(g) We comment on the reason the skew-symmetric bilinear forms and their involutions on $SL(2, k)$ give no additional results, and we give an illustration to support our claim.

Condition (3) The setting is then extended to $SL(n, k)$ where $n > 2$. Here, we show that all outer involutions come from bilinear forms, and use the Classification Theorem to classify these
for the important fields in the study of symmetric spaces. We show that the number of outer involutions is determined in part by the size of the square-class group \((k^*)/(k^*)^2\). We remark that the inner involutions of \(\text{SL}(n, k)\) do not come from bilinear forms, and we use a different system to classify these as well. It is shown that the number of inner involutions is always \(\frac{n-1}{2}\) when \(n\) is odd, so that it does not depend upon the field \(k\). The number of inner involutions coming from bilinear forms over \(V\) where \(V\) has even dimension, however, will depend not only upon the dimension of \(V\) but also upon the field \(k\) and its square-class group. We include skew-symmetric bilinear forms and their involutions in addition to those involutions coming from symmetric bilinear forms when \(n\) is even.

The results for inner and outer involutions on \(\text{SL}(n, k)\) for \(n > 2\) are treated separately, and here we summarize their combined results. We introduce some notation to be used for certain matrices:

\[
I_{n-i,i} = \begin{pmatrix}
I_{n-i \times n-i} & 0 \\
0 & -I_{i \times i}
\end{pmatrix}
\]

\[
J_{2m} = \begin{pmatrix}
0 & I_{m \times m} \\
-I_{m \times m} & 0
\end{pmatrix}
\]

\[
L_{n,x} = \begin{pmatrix}
0 & 1 & \ldots & 0 & 0 \\
x & 0 & \ldots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & 0 & 1 \\
0 & 0 & \ldots & x & 0
\end{pmatrix}
\]

\[
M_{n,x,y,z} = \begin{pmatrix}
I_{n-3 \times n-3} & 0 & 0 & 0 \\
0 & x & 0 & 0 \\
0 & 0 & y & 0 \\
0 & 0 & 0 & z
\end{pmatrix}
\]

The inner involutions are always represented by \(\text{Inn}_A\) where \(A\) is one of the \(\frac{n-1}{2}\) matrices \(I_{n-i,i}\), where \(i = 1, 2, \ldots, \frac{n-1}{2}\), when \(n\) is odd. For the inner involutions in the case where \(n\) is even, we have the same involutions \(\text{Inn}_A\) with \(A = I_{n-i,i}, \ i = 1, 2, \ldots, \frac{n}{2}\) plus the
Chapter 1. Introduction

\[(k^*)/(k^*)^2\] - 1 matrices represented by \(L_{n,x}\) where \(x\) is a representative of any of the cosets of non-square elements of \((k^*)/(k^*)^2\). When \(k = \bar{k}\) there are no additional involutions \(\text{Inn}_{L_{n,x}}\).

(a) \(k = \bar{k}\): When \(n\) is odd, there are \(\frac{n+1}{2}\) involutions, \(\frac{n-1}{2}\) inner involutions plus 1 outer involution. The sole outer involution comes from the symmetric bilinear form represented by the identity matrix. For even \(n\), there are \(\frac{n}{2} + 2\) classes of involutions, \(\frac{n}{2}\) inner involutions plus 2 outer involutions, the one coming from the symmetric bilinear form with representative matrix the identity matrix and the one coming from the class of skew-symmetric forms represented by \(J_{2m}\). For all fields, there is exactly 1 involution from a skew-symmetric form in the even case and no such involutions in the odd case (since there are no skew-symmetric forms which are non-degenerate in the odd case).

(b) \(k = \mathbb{R}\): When \(n\) is odd, there are exactly \(n\) involutions up to isomorphism, the \(\frac{n-1}{2}\) inner ones as well as \(\frac{n+1}{2}\) outer involutions. The outer involutions come from the symmetric bilinear forms represented by the matrices \(I_{n-i,i}\) \((i = 1, 2, \ldots \frac{n-1}{2})\), plus the identity matrix. When \(n\) is even, there are \(\frac{n}{2} + 1\) inner involutions and \(\frac{n}{2} + 2\) outer involutions. The outer involutions include the ones coming from the symmetric bilinear forms mentioned in the odd case plus the one coming from the skew-symmetric form, for a total of \(n + 3\) involutions in all.

(c) \(k = \mathbb{Q}\): As in the \(\text{SL}(2, k)\) case, there are infinitely many involutions over the rational numbers. We remark that there are only finitely many involutions (specifically, \(\frac{n-1}{2}\)) of inner type when \(n\) is odd.

(d) \(k = \mathbb{F}_p\) \((p \neq 2)\): When \(n\) is odd, there are \(\frac{n-1}{2} + 2\) involutions, the \(\frac{n-1}{2}\) inner involutions, plus the 2 outer involutions coming from the symmetric form with the identity matrix and the symmetric form represented by the matrix \(M_{n,1,1,S_p}\). When \(n\) is even, there are \(\frac{n}{2} + 4\) classes of involutions, the \(\frac{n}{2} + 1\) inner ones and 3 outer involutions. The outer ones are the 2 outer ones from the odd case plus the one from the skew-symmetric form \(J_{2m}\).

(e) \(k = \mathbb{Q}_2\): When \(n\) is even, there are \(\frac{n}{2} + 17\) involutions, comprised of the \(\frac{n}{2} + 7\) inner involutions (since \(|(k^*)/(k^*)^2| - 1 = 7\) and 10 outer involutions. There are the 9 outer
involutions corresponding to the symmetric forms represented by the identity matrix and by
the 7 matrices $M_{n, 1, 1, x}$ where $x \in \{-1, 2, -2, 3, -3, 6, -6\}$, as well as the involution of
the skew-symmetric form $J_{2m}$. The tenth outer involution differs depending upon whether $n = 2 \text{ mod } (4)$ or $n = 0 \text{ mod } (4)$. In the first case we get the involution from the symmetric
bilinear form $M_{n, 2, 3, -6}$, whereas in the second case the form inducing the involution is
represented by the matrix $M_{n, 2, 3, 6}$.

When $n$ is odd, the situation also depends upon the value of $n \text{ mod } (4)$, whether it is 1 or 3.

(i) $n = 1 \text{ mod } (4)$: There are $\frac{n+1}{2}$ involutions, the $\frac{n-1}{2}$ inner ones and the outer involution
corresponding to the symmetric form with the identity matrix.

(ii) $n = 3 \text{ mod } (4)$: There are $\frac{n+3}{2}$ involutions, all the ones from above plus the outer
involution which comes from the symmetric bilinear form $M_{n, 2, 3, 6}$.

In the case where $k = \mathbb{Q}_p$ ($p \neq 2$), there are always the $\frac{n-1}{2}$ inner involutions for $n$ odd
or the $\frac{n}{2} + 3$ inner involutions for even $n$ since $|(k^*)/(k^*)^2| - 1 = 3$. However, the outer
involution classes are different depending not only on dim($V$) = $n$ but also on whether or
not $-1$ is a square in $\mathbb{Q}_p$.

(f) $k = \mathbb{Q}_p$ ($p \neq 2$) $- 1 \not\in (\mathbb{Q}_p)^2$: When $n$ is even, we have different results depending
upon the value of $n \text{ mod } (4)$.

(i) $n = 0 \text{ mod } (4)$: There are 6 outer involutions. The involutions representing these
isomorphism classes are the ones coming from the skew-symmetric form $J_{2m}$, the sym-
metric form corresponding to the identity matrix, and the symmetric forms with matrices
$M_{1,1,p}, M_{n,1,1,S_p}, M_{n,1,1,PS_p}$ and $M_{n,p,S_p,PS_p}$. Combining inner and outer involutions, there
are $\frac{p}{2} + 9$ involutions in all.

(ii) $n = 2 \text{ mod } (4)$: There are also 6 outer involutions in this case. The bilinear forms
from which they come are the same as above with the exception that we replace the form
$M_{n,p,S_p,PS_p}$ by $M_{n,1,p,PS_p}$. So there are still $\frac{n}{2} + 9$ involutions total. When $n$ is odd, we also
have differing results for the outer involutions which depend upon the value of $n \text{ mod } (4)$:
Chapter 1. Introduction

(i) \( n = 1 \mod(4) \): There is 1 outer involution only, which comes from the standard inner product—the symmetric bilinear form represented by the identity \( n \times n \) matrix. There are \( \frac{n+1}{2} \) involutions total.

(ii) \( n = 3 \mod(4) \): We add to the 1 outer involution above the one coming from the symmetric form \( M_{n,p,S_p,pS_p} \). There are \( \frac{n+3}{2} \) involutions in all.

(g) \( k = \mathbb{Q}_p \ (p \neq 2) \): When \( n \) is even, there are 6 outer involutions in this case just as in the case where \(-1\) is not a square in \( \mathbb{Q}_p \). A couple of the involutions come from different semi-congruence classes of bilinear forms than in the previous situation, however.

(i) \( n = 0 \mod(4) \): The 6 forms which give our involutive classes are the symmetric form \( J_{2m} \), the standard dot product with the identity matrix, and the forms \( M_{n,1,1,p} \), \( M_{n,1,1,S_p} \), \( M_{n,1,1,pS_p} \), and \( M_{n,1,p,p} \). As in the earlier situation, there are \( \frac{n}{2} + 9 \) involutions after combining the inner and outer involutions.

(ii) \( n = 2 \mod(4) \): The 6 forms are the same as above, except that we replace the class of bilinear forms with matrix \( M_{n,1,p,p} \) by the class with matrix \( M_{n,p,S_p,pS_p} \). As before, we have a total of \( \frac{n}{2} + 9 \) involutions.

When \( n \) is odd and \(-1 \in (\mathbb{Q}_p^*)^2 \) we have the same 2 involutions as in the case where \(-1 \not\in (\mathbb{Q}_p^*)^2 \) and \( n = 3 \mod(4) \). Recall that these classes came from the 2 forms the standard dot product \( (M = I_{n \times n}) \) and the form with matrix \( M_{n,p,S_p,pS_p} \). There are a total of \( \frac{n+3}{2} \) involutions in this case.

(4) We move to \( G = \text{SO}(n, k) \ (n > 2) \) and prove that \( \text{Inn}_A \approx \text{Inn}_B \) over \( G \) if and only if the inner involutions \( \text{Inn}_A \) and \( \text{Inn}_B \) are isomorphic over \( \text{SL}(n, k) \) and the outer involutions \( \text{Inn}_A \theta \) and \( \text{Inn}_B \theta \) (where \( \theta \) is the outer involution \( \theta(X) = (X^T)^{-1} \)) are isomorphic over \( \text{SL}(n, k) \) as well. It is then shown that when \( k \) is algebraically closed or the real numbers, there is exactly one isomorphism class of involutions on \( G \) for each isomorphism class of inner involutions on \( \text{SL}(n, k) \). We show that each class of inner involutions on \( \text{SL}(n, k) \) over a finite field \( \mathbb{F}_p \ (p \neq 2) \) splits into 2 different classes over \( G \), and we give a specific example to illustrate this. We also establish that the classes over the \( p \)-adic numbers can
be narrowed down to an investigation of those classes having triple values $d_{\alpha,c_1,c_2}$, where $\alpha$ represent the square class of the determinant of the matrix, and the $c_i$ values are the Hasse symbols for specific diagonal matrices which are given and explained later in this thesis. This narrows down the problem to looking at the forms with the 32 possible triple values when $p = 2$ and 16 when $p \neq 2$ and seeing which of these induce isomorphic involutions.

(5) We look at the group $G = \text{SO}(n, k, \beta)$ where $\beta$ is any non-degenerate symmetric bilinear form on $V = k^n$. An extensive proof, with illustrations to illuminate the complicated equations in the proof, is given that an automorphism $\text{Inn}_A$ is the identity automorphism on $G$ if and only if $A$ is a scalar multiple of the identity matrix.

(6) Still working with $G = \text{SO}(n, k, \beta)$, we show that an automorphism $\text{Inn}_A$ keeps $\tilde{G} = \text{SO}(n, \tilde{k}, \beta)$ invariant if and only if $A$ is a scalar multiple of a matrix in $\tilde{G}$. This is part one of what we call the Characterization Theorem 5.2.

(7) We remark that when $k$ is an algebraically closed field, the real numbers, or a finite field we can always take our matrix $M$ representing the bilinear form to be a diagonal matrix with a 1 in the $[1, 1]$ and $[2, 2]$ positions. We can also do this over the $p$-adic numbers when $n > 4$ and in all but a few cases when $n = 3$ or $n = 4$. In fact, the only cases over the $p$-adic numbers where we cannot make this assumption about the matrix $M$ of the form are when the semi-congruence class of $\beta$ is represented by $M_{3,p,S_p,S_p}$ or by $M_{4,p,S_p,S_p}$ over $\mathbb{Q}_p$, $p \neq 2$ and when the semi-congruence class is represented by $M_{3,2,3,6}$ or by $M_{4,2,3,6}$ over $\mathbb{Q}_2$. The cases of $M_{4,p,S_p,S_p}$ and $M_{3,p,S_p,S_p}$ only occur when $-1$ is not a square in $\mathbb{Q}_p$.

So for the important fields utilized in this thesis (we do not investigate very thoroughly the case where $k = \mathbb{Q}$ as there are infinitely many isomorphism classes of involutions in this case) we always have this assumption on $M$ when $n > 4$ and almost always can make the assumption when $n = 3$ or 4. This covers the majority of cases over which symmetric spaces are typically studied.

Making this assumption that the form $\beta$ for the group $G = \text{SO}(n, k, \beta)$ can be represented by such a matrix $M$, and using the result from part one of the Characterization
Theorem 5.2, we prove part two of the Characterization Theorem 5.2. This states that for such forms $\beta$ (meaning all symmetric bilinear forms $\beta$ over algebraically closed fields, the real numbers, and finite fields, and all but the few exceptions outlined above for forms over the $p$-adic numbers) the automorphism $\text{Inn}_A$ with $A \in \bar{G}$ keeps $G$ invariant if and only if $A$ is a scalar multiple of a matrix in $G$.

(8) We come to the important conclusion that when the matrix of $\beta$ may be chosen to be $M = \text{diag}(1, 1, m_3, \ldots, m_n)$, all involutions of $G = \text{SO}(n, k, \beta)$ are inner when $n$ is odd, and show that as a consequence all involutions in this case come from bilinear forms. Additionally, all automorphisms which can be written as conjugations are “almost” inner when $n$ is even in the sense that we can choose our matrix $A$ to reside in $O(n, k, \beta)$.

As mentioned above, this covers all symmetric bilinear forms over $V = k^n$ when $n > 4$ and $k = \bar{k}, k = \mathbb{R}, k = \mathbb{F}_p, p \neq 2$ or $k = \mathbb{Q}_p$, and all forms over these fields when $n = 3$ or 4 except the few cases over the $p$-adic numbers referred to previously.

(9) Lastly, we summarize our results and their usefulness, and set up some more theory for a future full classification.
Chapter 2

Preliminaries

2.1 Symmetric Spaces

As elaborated upon in Chapter 1, the goal of this dissertation is an investigation of reductive symmetric spaces. Of main importance to our study of different symmetric spaces will be the relationship between bilinear forms (and the associated properties of Bilinear Algebra) and the isomorphism classes of related involutions on subgroups of $GL(n, k)$. In this chapter we begin the development of the tools we will use in this endeavor. We will show how, given a bilinear symmetric or skew-symmetric form over a field $k$, an involution of the related group is obtained. Thus, it will be shown that such bilinear forms may serve as an important tool in our understanding of the corresponding symmetric spaces.

2.1.1 Preliminaries

Our basic reference for reductive groups will be the papers of Borel and Tits [BT65], [BT72] and also the books of Borel [Bor91], Humphreys [Hum72] and Springer [Spr81]. We shall follow their notations and terminology. All algebraic groups and algebraic varieties are taken over an arbitrary field $k$ (of characteristic $\neq 2$) and all algebraic groups considered are linear algebraic groups.

Throughout this thesis we will use the following notation. Let $k$ be a field of characteristic not 2, $k_1$ an extension field of $k$, $\bar{k}$ the algebraic closure of $k$, $V = k^n$ a finite-dimensional
vector space over a field $k$, $\tilde{V} = \bar{k}^n$,

$$M_n(k) = M(n, k) = \{n \times n\text{-matrices with entries in } k\},$$

$$\text{GL}(V) = \text{GL}_n(k) = \text{GL}(n, k) = \{A \in M_n(k) \mid \det(A) \neq 0\}$$

and

$$\text{SL}(V) = \text{SL}_n(k) = \text{SL}(n, k) = \{A \in M_n(k) \mid \det(A) = 1\}.$$ 

Let $k^*$ denote the product group of all the nonzero elements, $(k^*)^2 = \{a^2 \mid a \in k^*\}$ and $\text{Id} \in M_n(k)$ denote the identity automorphism. Throughout this thesis $G$ will be a reductive linear algebraic group defined over $k$ and we denote its set of $k$-rational points by $G$. We will assume that $G$ is a subgroup of $\text{GL}(n, k)$.

### 2.1.2 Definition of Symmetric Spaces

Let’s first define symmetric spaces. The definition relies upon first defining an involution. Recall that the order of an automorphism $\theta$ (denoted $\text{ord}(\theta)$) is the smallest integer $x$ such that $\theta^x = \text{Id}$.

**Definition 1 (Involution).** Let $\text{Aut}(G)$ denote the set of all automorphisms of $G$. The automorphism $\theta \in \text{Aut}(G)$ is an **involution** of $G$ if $\text{ord}(\theta) = 2$, (i.e. if $\theta^2 = \text{Id}$ and $\theta \neq \text{Id}$).

**Definition 2 (Symmetric Spaces).** Given an involution $\theta$ on our group $G$, the **symmetric space** $X$ is defined as $G/H$ where $G^\theta = H$ is the fixed-point group of the involution $\theta$. One can also characterize this symmetric space as the subvariety $X = \{x\theta(x)^{-1} \mid x \in G\}$ of $G$. Then $X \simeq G/H$. For $k = \bar{k}$ algebraically closed the set $X$ is the connected component containing the identity of $Q = \{x \in G \mid \theta(x) = x^{-1}\}$.

**Remarks 1.** (1) Two symmetric spaces $X_1$ and $X_2$ are isomorphic if and only if their corresponding fixed-point groups $H_1$ and $H_2$ are isomorphic.

(2) Many of these involutions will be shown to come from symmetric or skew-symmetric bilinear forms. We shall see that the theory of bilinear forms can give us criteria for classification of these symmetric spaces via the fixed-point group of the involution.
(3) Since the study of bilinear forms has many known results and the study of involutions has a lesser bulk of known theory, the intent is that the study of the relationship between the two will result in transporting difficult problems in the algebraic group setting to the better known context of Bilinear Algebra.

(4) In particular, it will be shown that our construction of involutions from a given symmetric/skew-symmetric form results in the fixed-point group of the involution being equal to the orthogonal group which the form yields (“the” orthogonal group \(\text{SO}(n,k)\) being the particular orthogonal group coming from the standard dot product).

### 2.2 Bilinear Forms

Let \(V\) be the vector space \(V = k^n\), where \(k\) is any field with characteristic \(k \neq 2\). Recall that a \textit{bilinear form} on \(V\) is a bilinear map \(\beta : V \times V \rightarrow k\). The matrix associated with the form \(\beta\) is the matrix \(M = (m_{i,j})\) with \(m_{i,j} = \beta(e_i, e_j)\), where \(\{e_i\}\) is any ordered basis for \(V\). Then we have \(\beta(x, y) = x^T M y \quad \forall x, y \in V\).

**Remark 1.** [Art91] The properties of the form \(\beta\) carry over to the matrix \(M\):

1. \(\beta\) is a \textit{symmetric bilinear form} (i.e. \(\beta(x, y) = \beta(y, x) \quad \forall x, y \in V\)) if and only if \(M\) is a \textit{symmetric matrix} (i.e. \(M = M^T\)).

2. \(\beta\) is a \textit{skew-symmetric bilinear form} (i.e. \(\beta(x, y) = -\beta(y, x) \quad \forall x, y \in V\)) if and only if \(M\) is a \textit{skew-symmetric matrix} (i.e. \(M = -M^T\)).

3. \(\beta\) is \textit{non-degenerate} (i.e. \(\beta(x, y) = 0 \quad \forall y \in V\) only if \(x = 0\)) if and only if \(\text{nullspace}(M) = 0\).

**Remark 2.** Note that property (3) is equivalent to saying that \(\det(M) \neq 0\), which means that \(M\) must then be invertible. We will be dealing exclusively with non-degenerate forms, so all matrices \(M\) representing bilinear forms may be assumed to be invertible.

**Definition 3 (Congruence of Bilinear Forms).** \(M_1\) is \textit{congruent} to \(M_2\) (\(M_1 \cong M_2\)) over the field \(k\) if there exists a matrix \(Q \in \text{GL}(n,k)\) such that \(M_2 = Q^T M_1 Q\).
Note that the matrix of the form $\beta$ is dependent upon the choice of basis $\{e_i\}$. The following theorem is well known, and its proof can be found in [Art91].

**Theorem 2.1.** Two matrices $M_1$ and $M_2$ represent the same bilinear form with respect to different bases if and only if they are congruent.

**Remark 3.** If $M_1$ represents the matrix of the form $\beta$ with respect to the basis $\mathcal{B}_N$ and $M_2$ represents the matrix of the form $\beta$ with respect to the basis $\mathcal{B}_G$, then the matrix $Q$ that gives the congruence relation is the change of basis matrix from $\mathcal{B}_G$ to $\mathcal{B}_N$.

**Example 2.1 (Illustration).** Let $x_1$ and $y_1$ be vectors in $V$ with coordinates relative to basis $\mathcal{B}_N$, and let $x_2$ and $y_2$ be the same vectors with coordinates relative to $\mathcal{B}_G$. Suppose that $M_1$ and $M_2$ are the matrices of a given bilinear form $\beta$ with respect to the two different bases, and that $Q$ is the change of basis matrix from $\mathcal{B}_G$ to $\mathcal{B}_N$. Then

$$\beta(x_1, y_1) = \beta(Qx_2, Qy_2) = (Qx_2)^T M_1 (Qy_2) = x_2^T Q^T M_1 Q y_2$$

and

$$\beta(x_2, y_2) = x_2^T M_2 y_2.$$

These values must be equal if each $M_1$ and $M_2$ each represent the same bilinear form $\beta$. This will occur if and only if $M_2 = Q^T M_1 Q$ and $M_2 \cong M_1$. This illustrates that congruence is to bilinear forms what similarity is to linear transformations (i.e. a change of basis in both situations).

### 2.3 Isomorphism of Involutions

**Definition 4 (Isomorphic Involutions).** For $A \in \text{GL}(n, k)$ let $\text{Inn}_A$ denote the inner automorphism defined by $\text{Inn}_A(X) = A^{-1}X A \quad \forall X \in \text{GL}(n, k)$. Let $\text{Inn}_k(G) = \{ \text{Inn}_A \mid A \in G \}$ denote the set of all inner automorphisms of $G$ and let $\text{Inn}(G)$ denote the set of automorphisms $\text{Inn}_A$ of $G$ with $A \in \overline{G}$ such that $\text{Inn}_A(G) = G$.

(1) We say that $\theta$ and $\tau$ in $\text{Aut}(G)$ are $\text{Inn}(G)$-isomorphic if there is a $\phi$ in $\text{Inn}(G)$ such that $\tau = \phi^{-1} \theta \phi$. 
(2) We say that $\theta$ and $\tau$ in $\text{Aut}(G)$ are $\text{Aut}(G)$ isomorphic if there exists a $\phi$ in $\text{Aut}(G)$ such that $\tau = \phi^{-1}\theta\phi$.

Remark 4.  
(1) Note that an automorphism of $G \subseteq \text{GL}(n, k)$ may actually come from an element $A \in \text{GL}(n, \bar{k})$, so long as $\text{Inn}_A$ (=conjugation by A) keeps $G$ invariant.

(2) Notice that $\theta \approx^{\text{Inn}} \tau \implies \theta \approx^{\text{Aut}} \tau$. Thus, the set of $\text{Inn}(G)$–isomorphism classes contains the set of all $\text{Aut}(G)$–isomorphism classes.

(3) Just as congruence of bilinear forms represents the resulting change in the matrix of the form under a change of basis, $\text{Inn}(G)$-isomorphism between two automorphisms $\theta$ and $\tau$ represents the change in the matrix of an element of $G$ (conveniently viewed as a linear transformation on $\text{GL}(V, V)$) under a change of basis as well.

(4) This thesis concentrates predominantly on identifying isomorphism classes of involutions under the $\text{Inn}(G)$-isomorphism criteria, so for our purposes that is the type of isomorphism indicated when we write $\theta \approx \tau$.

2.4 Involutions Obtained from Bilinear Forms

2.4.1 Adjoint of a Matrix

Definition 5. Let $M$ be the matrix of a non-degenerate bilinear form over $V = k^n$ which is either symmetric or skew-symmetric, and let $A \in \text{GL}(n, k)$. The adjoint of $A$ with respect to $\beta$ (denoted $A'$) is defined as the matrix that satisfies the relation $\beta(Ax, y) = \beta(x, A'y)$. If it is clear from the context which bilinear form $\beta$ we are considering, then we will also just call this the adjoint of $A$.

It follows from the definition that

$$\beta(Ax, y) = (Ax)^T My = x^T A^T My = x^T MA'y = \beta(x, A'y)$$

which implies

$$A^T M = MA'. $$
So we get the following equation expressing $A'$ in terms of $A$ and $M$, which we will use consistently in this paper.

$$A' = M^{-1}A^T M$$  \hspace{1cm} (2.1)

**Theorem 2.2 (Properties of the Adjoint):**

1. $(A')' = A$
2. $(A')^{-1} = (A^{-1})'$
3. $(AB)' = B'A'$

**Proof.** (1)

$$(A')' = M^{-1}((A')^T)^{-1}M = M^{-1}((M^{-1}(A^T)^{-1}M)^T)^{-1}M$$

$$= M^{-1}M^T A(M^{-1})^T M.$$

This last expression equals $A$ since $M = M^T$ or $M = -M^T$.

(2)

$$(A')^{-1} = (M^{-1}A^T M)^{-1} = M^{-1}(A^T)^{-1}M$$

which equals

$$M^{-1}(A^{-1})^T M = (A^{-1})'$$

since the transpose and inverse operations commute.

(3)

$$(AB)' = M^{-1}(AB)^T M$$

$$= M^{-1}B^T A^T M$$

$$= M^{-1}B^T (MM^{-1}) A^T M$$

$$= (M^{-1}B^T M)(M^{-1}A^T M)$$

$$= B'A'$$
When dealing with the standard dot product, \( M = I_{n \times n} \). In this case, the adjoint of \( A \) is simply \( A^T \). Then it is easy to see the familiarity of these properties as simply generalizations of the properties of the transpose operation.

### 2.4.2 Using the Adjoint to Construct Involutions

**Definition 6.** Given a bilinear form on \( V \) with matrix \( M \), we define \( \theta = \theta_M \) by \( \theta(A) = (A')^{-1} \). Using Equation 2.1 we see that \( \theta(A) = M^{-1}(A^T)^{-1}M \).

**Proposition 1.** \( \theta \) is an involution of \( \text{GL}(n, k) \).

**Proof.** This follows from the shown properties (1)-(3) of the adjoint in Theorem 2.2.

\[
\theta(AB) = ((AB)')^{-1} = ((AB)^{-1})' = ((B)^{-1}(A)^{-1})' = (A')^{-1}(B')^{-1} = \theta(A)\theta(B)
\]

and

\[
\theta^2(A) = (((A')^{-1})')^{-1} = (A')' = A.
\]

In this way we may always obtain an involution of the matrix group over the field \( k \) given a symmetric or skew-symmetric (and non-degenerate) bilinear form on the vector space \( V = k^n \). This thesis attacks the problem of determining if all involutions may be obtained in this manner, and concludes in the following chapters that this answer will sometimes be yes depending upon the particular group in question. Even for groups where not all the involutions can be realized in this way, it turns out that many involutions will be determined by these bilinear forms.

### 2.4.3 Orthogonal Group of the Form

**Definition 7.** Given a non-degenerate bilinear symmetric/skew-symmetric form \( \beta \) on \( V = k^n \), the **orthogonal group** \( \text{O}(n, k, \beta) \) is defined as

\[
\text{O}(n, k, \beta) = \{ A \in \text{GL}(n, k) \mid \beta(Ax, Ay) = \beta(x, y) \}.
\]
Thus, the orthogonal group consists of invertible matrices that preserve the bilinear form (i.e. that preserve length, when dealing with a positive definite form, where the notion of length may be defined).

Elements of the orthogonal group will also preserve angles between vectors, so that the images of 2 vectors in $G$ which are orthogonal (perpendicular) to each other remain perpendicular. In this sense these matrices preserve our sense of the geometry of $V$. When the bilinear form $\beta$ is the standard dot product represented by the identity matrix, its orthogonal group is the familiar group $O(n, k)$ (we assume $\beta$ is the dot product with this notation). It is comprised of the rotation and reflection properties, with the rotations representing the elements of $O(n, k)$ which have determinant 1 and the reflections all having determinant $-1$.

2.4.4 Symmetric Spaces Revisited

Given this method of obtaining an involution $\theta$ from a bilinear form $\beta$, we may now re-define the symmetric spaces for $GL(n, k)$:

**Definition 8 (Symmetric Space II).** Let $X = \{AA' \mid A \in GL(n, k)\}$. Then $X = \{A(\theta(A))^{-1} \mid A \in GL(n, k)\} \simeq GL(n, k)/O(n, k, \beta)$. If $G$ is a subgroup of $GL(n, k)$, invariant under taking the adjoint, then $X_1 = X \cap G \simeq G/(G \cap O(n, k, \beta))$ is exactly the symmetric space as defined in Definition 2.

**Remark 5.** Two fixed point groups $H_{\beta_1} = O(n, k, \beta_1)$ and $H_{\beta_2} = O(n, k, \beta_2)$ are isomorphic if and only if $\theta_1 \approx \theta_2$.

Thus, if an involution comes from a non-degenerate symmetric/skew-symmetric bilinear form, the classification of the related symmetric space comes from classifying the bilinear form (which in turn classifies the fixed-point group $H = O(n, k, \beta)$).
2.5 Semi-Congruence and the Classification Theorem

Now that we have shown how to obtain involutions of matrix groups from non-degenerate symmetric or skew-symmetric bilinear forms on the vector space $V = k^n$, where $k$ is a field whose characteristic is not equal to two, we will show how to use bilinear algebraic properties to determine the isomorphism classes of these involutions. Since congruence of bilinear forms describes which forms are identical to each other under a change of basis for $V$ and Inn-$G$ isomorphism identifies which involutions represent other involutions after a change of basis operation, it makes sense that these ideas are related.

A first question to pose is: Is there a one-to-one correspondence between congruence classes of symmetric/skew-symmetric bilinear forms and isomorphism classes of their involutions? A second question which comes immediately to mind is that of whether all involutions come from bilinear forms. In general, the answers to these questions will be negative, but the answer to the first will be seen to be “almost” while the second can be answered in the affirmative in some cases. We begin by looking at the former and noting that congruent forms do indeed provide isomorphic involutions.

**Theorem 2.3.** Let $M_1$ and $M_2$ be the matrices of bilinear forms $\beta_1$ and $\beta_2$ over $V = k^n$, respectively, and let $\theta_1$ and $\theta_2$ be the corresponding involutions on $\text{GL}(n, k)$ (i.e. $\theta_1(A) = M_1^{-1}(A^T)^{-1}M_1 \forall A \in \text{GL}(n, k)$ and likewise for $\theta_2$ and $M_2$). If $M_1 \cong M_2$, then $\theta_1 \approx \theta_2$.

**Proof.** Suppose $M_1 \cong M_2$ over $k$ with $M_2 = Q^T M_1 Q$ for some $Q \in \text{GL}(n, k)$. Using the formulas for $\theta_1$ and $\theta_2$, we get that $\forall A \in \text{GL}(n, k),$

$$\theta_2(A) = \text{Inn}_M(A^T)^{-1} = \text{Inn}_{Q^TM_1Q}(A^T)^{-1}.$$

This yields

$$\theta_2(A) = (Q^T M_1 Q)^{-1}(A^T)^{-1}(Q^T M_1 Q)$$
so that
\[
\theta_2(A) = \left(Q^{-1}M_1^{-1}(Q^T)^{-1}(A^T)^{-1}((Q^T)M_1Q)\right)
\]
\[
= \left(Q^{-1}(M_1^{-1}((Q^T)^{-1}A^{-1}Q^T)M_1)\right)Q
\]
\[
= Q^{-1}\Inn_{M_1}((QAQ^{-1})^T)^{-1}Q
\]
\[
= Q^{-1}\Inn_{M_1}((\Inn_{Q^{-1}}(A))^T)^{-1}Q
\]
\[
= Q^{-1}\theta_1(\Inn_{Q^{-1}}(A))Q
\]
\[
= \Inn_Q(\theta_1(\Inn_{Q^{-1}}(A))
\]
\[
= \Inn_Q\theta_1\Inn_{Q^{-1}}(A) \quad \forall A \in \GL(n,k).
\]

This means that
\[
\theta_2 = \Inn_Q\theta_1\Inn_{(Q^{-1})},
\]
which means \(\theta_2 = (\phi)^{-1}\theta_1\phi\) with \(\phi = \Inn_{Q^{-1}}\). Therefore, \(\theta_2 \approx \theta_1\) over \(\GL(n,k)\) via \(\phi = \Inn_{Q^{-1}}\).

Here we start to see the relationship between congruence of bilinear symmetric/skew-symmetric forms and isomorphism of the induced involutions. A one-to-one correspondence between congruent forms and isomorphic involutions would be ideal, but we shall see that we don’t quite get an equivalence statement here.

**Theorem 2.4.** Suppose \(\theta_1\) and \(\theta_2\) are involutions on \(\GL(n,k)\) which come from symmetric or skew-symmetric bilinear forms represented by the matrices \(M_1\) and \(M_2\), respectively, over \(V = k^n\) (i.e. \(\theta_1(A) = (A')^{-1}\) where \(A' = M_1^{-1}A^T M_1\) and similarly for \(\theta_2\)). If \(\theta_1 \approx \theta_2\), then \(M_2 = \alpha Q^T M_1 Q\) for some matrix \(Q \in \GL(n,k)\) and some scalar \(\alpha \in \bar{k}\).

**Proof.** We begin by applying the definition of \(\text{Inn}-G\) isomorphism to obtain \(\theta_2 = \phi^{-1}\theta_1\phi\), for some \(\phi \in \text{Inn \GL(n,k)}\) (which means \(\phi = \Inn_P\) for some \(P \in \GL(n, \bar{k})\)). By definition of construction of the involutions from their related bilinear forms, we get that \(\forall A \in \GL(n,k),\)

\[
\theta_2(A) = M_2^{-1}(A^T)^{-1}M_2
\]
and also that
\[ \theta_2(A) = \phi^{-1}\theta_1\phi(A) = \text{Inn}_{P^{-1}} \text{Inn}_{M_1}((\text{Inn}_P(A))^T)^{-1}. \]
The right side of this last equation expands to
\[ \text{Inn}_{P^{-1}}(M_1^{-1}((P^{-1}AP)^{-1}M_1) = PM_1^{-1}(P^T)(A^T)^{-1}(P^T)^{-1}M_1P^{-1}. \]
Equating these two forms for \( \theta_2(A) \), and solving for \( (A^T)^{-1} \) we obtain
\[ M_2P(M_1)^{-1}P^T(A^T)^{-1}(P^T)^{-1}M_1P^{-1}M_2^{-1} = (A^T)^{-1} \]
which is equivalent to saying
\[ M_2P(M_1)^{-1}P^T A(P^T)^{-1}M_1 P^{-1}M_2^{-1} = ((P^T)^{-1}M_1P^{-1}M_2^{-1})^{-1} A((P^T)^{-1}M_1P^{-1}M_2^{-1}) = A. \]
So we have that
\[ \text{Inn}_{(P^T)^{-1}M_1P^{-1}M_2^{-1}} = \text{Id}. \]
For any group \( G \), \( \text{Inn}_Y = \text{Id} \) on \( G \) \( \implies \) \( Y \in Z(G) \), \( (Z(G) \) denoting the center of \( G \)).
Since the center of \( \text{GL}(n, k) \) is known to be the set \( \{\alpha I_{nxn} | \alpha \in k^*\} \), our result is that
\[ (P^T)^{-1}M_1P^{-1}M_2^{-1} = \gamma I_{nxn} \]
or equivalently,
\[ \gamma M_2 = (P^T)^{-1}M_1P^{-1} \]
i.e.
\[ M_2 = \alpha (P^T)^{-1}M_1P^{-1} \]
where \( \alpha = 1/\gamma \). We can choose \( \gamma \) (and therefore \( \alpha \)) to be in \( \bar{k} \) since such a scalar multiple of the identity matrix still commutes with \( \text{GL}(n, k) \). So our result is shown by substituting \( Q = P^{-1} \) and then \( M_2 = \alpha Q^TM_1Q. \) \( \square \)

We do not quite obtain congruence due to the extra scalar \( \alpha \) that results, yet it is clear that we are close to the desired outcome. Thus, we see that we need a new concept--a slight "tweaking" of the congruence definition--to get an equivalence statement. This leads to the following important definition and theorem.
**Chapter 2. Preliminaries**

**Definition 9.** Two bilinear forms on $V = k^n$ with associated matrices $M_1$ and $M_2$ are **semi-congruent over $k$** ($M_1 \cong^s M_2$) if there exists a $Q \in \text{GL}(n, k)$ and an $\alpha \in \overline{k}$ such that $M_2 = \alpha Q^T M_1 Q$.

Note that congruence implies semi-congruence and not conversely.

**Proposition 2.** Although semi-congruence doesn’t imply congruence, we have

$$M_1 \cong^s M_2 \implies \theta_{M_1} \approx \theta_{M_2}.$$  

**Proof.** Conjugation by a scalar multiple of a matrix is identical to the conjugation by that matrix:

$$\text{Inn}_{\alpha M}(A) = (\alpha M)^{-1} A (\alpha M) = (\alpha^{-1} \alpha) M^{-1} AM = M^{-1} AM = \text{Inn}_M(A)$$

The condition $M_1 \cong^s M_2$ is equivalent to saying that $M_1 \cong \alpha M_2$, which we know from Theorem 2.3 implies that $\theta_{M_1} \approx \theta_{\alpha M_2}$. Yet $\theta_{\alpha M_2} = \theta_{M_2}$ since $\theta_{\alpha M_2}(A) = \text{Inn}_{\alpha M_2}(A^T)^{-1} = \text{Inn}_{M_2}(A^T)^{-1} = \theta_{M_2}(A)$. So we obtain the same involution regardless of the effect of the scalar $\alpha$ on the bilinear form. This forces that $\theta_{M_1} \approx \theta_{M_2}$, and the proposition is thereby proven.

**Theorem 2.5 (Classification Theorem).** If $\theta_1$ and $\theta_2$ are involutions on $\text{GL}(n, k)$ which come from bilinear symmetric/skew-symmetric forms in the manner shown before, then $M_1 \cong^s M_2$ over $k$ $\iff$ $\theta_{M_1} \approx \theta_{M_2}$.

**Proof.** This is really just a combination of previous theorems and propositions in this section. The implication $M_1 \cong^s M_2 \implies \theta_{M_1} \approx \theta_{M_2}$ is precisely Proposition 2 proven above, which itself relies on Theorem 2.3. The reverse implication that $\theta_{M_1} \approx \theta_{M_2} \implies M_1 \cong^s M_2$ over $k$ is a direct result of Theorem 2.4, which states that if $\theta_{M_1} \approx \theta_{M_2}$, then $M_2 = \alpha Q^T M_1 Q$ for some matrix $Q \in \text{GL}(n, k)$ and some scalar $\alpha \in \overline{k}$. This is exactly the definition of semi-congruence of 2 bilinear forms given in Definition 9 above, so that $M_1 \cong^s M_2$. Thus, the 2 statements are seen to be equivalent.
2.6 Why Focus on $\text{SL}(n, k)$?

In the following chapters we concentrate on $\text{SL}(n, k)$ (beginning with $\text{SL}(2, k)$) and subgroups of $\text{SL}(n, k)$. It is reasonable to ask why we are starting with $\text{SL}(n, k)$ rather than $\text{GL}(n, k)$ in our analysis. One reason for this is that all involutions on $\text{SL}(2, k)$ will be shown to come from bilinear forms. There are involutions on $\text{GL}(2, k)$, however, which do not come from bilinear forms. Notice that the nature of the defined involution forces a certain restriction on the determinant of the image of a matrix under the involution:

\[
\det(\theta(A)) = \det(M^{-1}(A^T)^{-1}M) = \det(A^{-1}) = 1/\det(A) \tag{2.2}
\]

So for example, the involution on $\text{GL}(2, k)$ defined by $\tau(A) = \begin{pmatrix} a_{2,2} & a_{2,1} \\ a_{1,2} & a_{1,1} \end{pmatrix}$ cannot come from a bilinear form since $\det(\tau(A)) = \det(A) \neq 1/\det(A)$ unless $A$ has determinant 1.

**Lemma 1.** An automorphism $\theta$ coming from a bilinear form is an involution on $\text{GL}(n, k) \iff$ it is an involution on $\text{SL}(n, k)$.

**Proof.** Given an involution on $\text{GL}(n, k)$ coming from a bilinear form, we can always restrict the involution to $\text{SL}(n, k)$ and we’re guaranteed that it will keep $\text{SL}(n, k)$ invariant since Equation 2.2 tells us the determinant of the image of a matrix $A$ under the action of the involution will be $1/\det(A) = 1$, guaranteeing that it is an involution of $\text{SL}(n, k)$ as well.

Conversely, given an involution $\theta_M(A) = \text{Inn}_M(A^T)^{-1}$ of $\text{SL}(n, k)$, it is easy to see that this will remain an involution even when “lifted” from $\text{SL}(n, k)$ to be allowed to act on $\text{GL}(n, k)$.

Most importantly, the isomorphism classes will remain intact.

**Theorem 2.6.** Two involutions $\theta_1$ and $\theta_2$ are isomorphic over $\text{GL}(n, k) \iff$ they are isomorphic over $\text{SL}(n, k)$.

**Proof.** $\iff$: If $\theta_1 \approx \theta_2$ over $\text{SL}(n, k)$, then obviously there is a matrix $P$ in $\text{GL}(n, k)$ (namely, the same matrix as for $\text{SL}(n, k)$) such that $\theta_1 \approx \theta_2$ via $\phi = \text{Inn}_P$ over $\text{GL}(n, k)$. 
\[
\hat{P} = \left(1/\sqrt[n]{\det(P)}\right) P
\]

The determinant of \( \hat{P} \) will be 1 so that \( \hat{P} \in \text{SL}(n, k) \):

\[
\det(\hat{P}) = \left(1/\sqrt[n]{\det(P)}\right)^n (\det(P)) = 1
\]

So it is still the case that \( \theta_1 \approx \theta_2 \). The matrix entries of \( \hat{P} \) and the scalar we factor out of \( P \) might not belong to \( k \) but may require an extension field of \( k \). Recall, however, that \( \text{Inn}_P \) where \( P \) has entries outside of \( k \) still has \( \text{Inn}_P \in \text{Inn}(\text{SL}(n, k)) \) so long as \( \text{SL}(n, k) \) remains invariant under the conjugation. This is clear since scalar multiples of a matrix do not change the action of the conjugation on \( \text{SL}(n, k) \). \( \square \)
Chapter 3

Involution on SL(2, k)

3.1 Preliminaries

Now let’s focus specifically on the group SL(2, k). Using different methods a first classification of the isomorphism classes of involutions of SL(2, k) was given in [HW02]. This classification did not use bilinear forms and also did not classify the bilinear forms related to the involutions. In this chapter we will give a classification of both the involutions and their bilinear forms.

Our basic reference for reductive groups will be the papers of Borel and Tits [BT65], [BT72] and also the books of Borel [Bor91], Humphreys [Hum72] and Springer [Spr81]. We shall follow their notations and terminology. All algebraic groups and algebraic varieties are taken over an arbitrary field $k$ (of characteristic $\neq 2$) and all algebraic groups considered are linear algebraic groups. For this chapter $G$ will denote SL(2, $k$), $\tilde{G}$ will denote SL(2, $\bar{k}$), and all bilinear forms are taken over the vector spaces $V = k^2$ or $\tilde{V} = \bar{k}^2$. Let $k^*$ denote the product group of all nonzero elements of $k$, $(k^*)^2 = \{ x^2 \mid x \in k^* \}$, and let Id denote the identity automorphism on $G$. 
3.2 Importance of the Square-Class Group $k^*/(k^*)^2$

In this subsection we first review some results about the characterization of the isomorphism classes of involutions from [HW02], needed for characterization using bilinear forms.

**Lemma 2.** [Bor91]

1. If $k$ is an algebraically closed field, $\text{Aut}(G) = \text{Inn}(G)$.

2. If $k$ is not algebraically closed and $\theta \in \text{Aut}(G)$, there exists an extension field $k_1$ and a $\phi \in \text{Inn}(\text{SL}(2, k_1))$ such that $\phi|_G = \theta$.

**Lemma 3.** Suppose that $\text{Inn}_A = \text{Id}$ on $G$, where $A \in \text{GL}(2, k_1)$. Then $A = \alpha I_{2 \times 2}$ for some scalar $\alpha \in k_1$.

**Proof.** Let $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ and suppose that $\text{Inn}_A = \text{Id}$ on $G$. Then $A^{-1}XA = X \forall X \in G$ which implies that $XA = AX$. Let $X_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $X_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Then

$$X_1A = \begin{pmatrix} a_{11} & -a_{12} \\ a_{21} & -a_{22} \end{pmatrix}$$

and

$$AX_1 = \begin{pmatrix} a_{11} & a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}.$$ 

Since these must be equal we have $a_{12} = a_{21} = 0$ (since $\text{char } k \neq 2$).

Also,

$$X_2A = \begin{pmatrix} a_{21} & a_{22} \\ -a_{11} & -a_{12} \end{pmatrix}$$

and

$$AX_2 = \begin{pmatrix} -a_{12} & a_{11} \\ -a_{22} & a_{21} \end{pmatrix}.$$ 

So $a_{11} = a_{22}$. Let $\alpha = a_{11}$. Then we’ve shown that $A = \alpha I_{2 \times 2}$. □
Lemma 4. [Wu02] Let \( G_1 \) denote \( G \) over an extension field \( k_1 \) of \( k \). The inner automorphism \( \text{Inn}_A \in \text{Inn} \ G_1 \) keeps \( G \) invariant (i.e. \( \text{Inn}_1(X) \in G \ \forall X \in G \)) if and only if \( A = \alpha B \) for some \( \alpha \) in \( k_1 \) and some \( B \) in \( \text{GL}(2, k) \).

Remark 6. Since \( \text{Inn}_{\alpha B} = \text{Inn}_B \), this means that we can write every automorphism (and more specifically, every involution) of \( \text{SL}(2, k) \) as the restriction of a conjugation \( \text{Inn}_B \) to \( \text{SL}(2, k) \) where \( B \) is in \( \text{GL}(2, k) \).

These are results for automorphisms of \( G \) in general. Now, let’s switch to the case where the automorphism is an involution of \( G \).

Theorem 3.1. All involutions on \( \text{SL}(2, k) \) have the form \( \theta = \text{Inn}_B \), where \( B \) has the form
\[
B = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}, \quad \text{and} \ \alpha \ \text{is in} \ k.
\]

Proof. By Remark 6 we can assume all involutions \( \theta \) of \( G \) have the form \( \theta = \text{Inn}_A \) where \( A \in \text{GL}(2, k) \). So \((\text{Inn}_A)^2 = \text{Inn}_A^2 = \text{Id} \) which implies \( A^2 = \alpha I_{2 \times 2} \). If we let
\[
A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}
\]
then the matrix \( A^2 \) has the form
\[
\begin{pmatrix} a_{1,1}^2 + a_{1,2}a_{2,1} & (a_{1,1} + a_{2,2})a_{1,2} \\ (a_{1,1} + a_{2,2})a_{2,1} & a_{2,2}^2 + a_{1,2}a_{2,1} \end{pmatrix}.
\]
So
\[
(a_{1,1} + a_{2,2})a_{1,2} = (a_{1,1} + a_{2,2})a_{2,1} = 0.
\]

(1) First we’ll show that \((a_{1,1} + a_{2,2}) = 0 \). Suppose \((a_{1,1} + a_{2,2}) \neq 0 \). Then \( a_{1,2} = a_{2,1} = 0 \) since \( A^2 \) is diagonal, so \( A \) is diagonal as well. Since \( \alpha = a_{1,1}^2 + a_{1,2}a_{2,1} = a_{2,2}^2 + a_{1,2}a_{2,1} \), then \( a_{1,1} = a_{2,2} \) or \( a_{1,1} = -a_{2,2} \). The latter situation is impossible, however, since \((a_{1,1} + a_{2,2}) \neq 0 \). Therefore, \( a_{1,1} = a_{2,2} \) and \( A = a_{1,1}I_{2 \times 2} \). Yet in this case, \( \theta = \text{Inn}_A = \text{Inn}_{a_{1,1}I_{2 \times 2}} = \text{Id} \). Since the identity automorphism is not an involution, we have a contradiction to our assumption and conclude that \((a_{1,1} + a_{2,2}) = 0 \).

(2) Since \((a_{1,1} + a_{2,2}) = 0 \), \( a_{1,1} = -a_{2,2} \). If \( a_{1,2} = a_{2,1} = 0 \) then \( A = \begin{pmatrix} a_{1,1} & 0 \\ 0 & -a_{1,1} \end{pmatrix} \).

Then \( A \) is conjugate to
\[
\begin{pmatrix} 0 & a_{1,1} \\ a_{1,1} & 0 \end{pmatrix}
\]
via \( P = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \) since
\[
P^{-1}AP = \begin{pmatrix} 0 & a_{1,1} \\ a_{1,1} & 0 \end{pmatrix}.
\]
If either \( a_{1,2} \) or \( a_{2,1} \) is not zero, suppose \( a_{1,2} \neq 0 \). Then
Chapter 3. Involutions of $\text{SL}(2, k)$

we have that $A$ is conjugate to $\begin{pmatrix} 0 & a_{1,2} \\ a_{1,1}/a_{1,2} + a_{2,1} & 0 \end{pmatrix}$ via $P = \begin{pmatrix} 1 & 0 \\ -a_{1,1}/a_{1,2} & 1 \end{pmatrix}$ since $P^{-1}AP = \begin{pmatrix} 0 & a_{1,2} \\ a_{1,1}/a_{1,2} + a_{2,1} & 0 \end{pmatrix}$. If $a_{1,2} = 0$ and $a_{2,1} \neq 0$ we use instead $P = \begin{pmatrix} 1 & a_{1,1}/a_{2,1} \\ 0 & 1 \end{pmatrix}$ and get $P^{-1}AP = \begin{pmatrix} 0 & a_{2,1}^2/a_{1,2} \\ a_{2,1} & 0 \end{pmatrix}$. In any case, we have the following conclusion: $A$ must be conjugate to a matrix with the form $\begin{pmatrix} 0 & \alpha_1 \\ \alpha_2 & 0 \end{pmatrix}$ for some scalars $\alpha_1$ and $\alpha_2$ in $k$.

(3) If $A$ is conjugate to $Y = \begin{pmatrix} 0 & \alpha_1 \\ \alpha_2 & 0 \end{pmatrix}$ via $P^{-1}AP = Y$ then $\text{Inn}_A \approx \text{Inn}_Y$ via $\phi = \text{Inn}_P$. So these matrices $Y$ give all the isomorphism classes of involutions of $G$. Since multiplying/dividing $Y$ by a constant does not change the involution $\text{Inn}_Y$, we can take $\hat{Y} = \frac{1}{\alpha_2} Y$ and get the same involution. Therefore, all isomorphism classes of involutions of $G$ can be represented by the matrices $\begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}$.

Now, let $M$ be the matrix of a non-degenerate symmetric bilinear form over $k$.

**Lemma 3.1.** [Szy97]

1. $M$ is congruent to a diagonal matrix with non-zero entries.
2. Any rearrangement of the diagonal matrix $M$ results in another matrix in the same congruence class, congruent via an orthogonal permutation matrix $P$.

**Theorem 3.2 (All Involutions of $G$ Come From Bilinear Forms).** All involutions on $\text{SL}(2, k)$ have the form $\theta_M$ where $M$ is the matrix of a symmetric bilinear form and $\theta_M$ its corresponding involution.

**Proof.** Let $M$ be the matrix of a non-degenerate symmetric bilinear form on $V = k^n$ (char $k \neq 2$). We can normalize the $[1, 1]$ entry of $M$ to 1 and write $M = \begin{pmatrix} 1 & 0 \\ 0 & m_2 \end{pmatrix}$.
without changing the involution of the form since a scalar doesn’t affect the involution:

$$\theta_M(A) = \text{Inn}_M(A^T)^{-1} = \text{Inn}_{\frac{1}{m_1}}M(A^T)^{-1} = \theta_{\frac{1}{m_1}M}(A)$$

Notice that for $A \in G$, $(A^T)^{-1} = \text{Inn}_{\hat{B}}(A)$ where $\hat{B} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Let $B = \hat{B}M \in \text{GL}(2, k)$. Then, $\theta_M = \text{Inn}_M \text{Inn}_{\hat{B}} = \text{Inn}_{\hat{B}M} = \text{Inn}_B$, where $B = \hat{B}M = \begin{pmatrix} 0 & -m_2 \\ 1 & 0 \end{pmatrix}$.

From Theorem 3.1 we had that all involutions of $G$ may be written as $\text{Inn}_B$ where $B = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}$. So we take $\alpha = -m_2$ and state that all involutions on $\text{SL}(2, k)$ come from bilinear symmetric forms.

The different ways of choosing $m_2$ will determine the isomorphism classes of the involution $\theta_M = \text{Inn}_B$. Now all we have to do is determine which choices for $m_2$ give semi-congruent matrices and the Classification Theorem 2.5 tells us that we will have determined all the involution classes.

**Theorem 3.3 (Square Class Theorem).** Let $M$ be the matrix associated with a symmetric bilinear form on $V = k^2$ (char $k \neq 2$). The semi-congruence classes of symmetric bilinear forms over $V$ are determined by the square class group $k^*/(k^*)^2$. That is, two choices $\gamma_1$ and $\gamma_2$ for $m_2$ give isomorphic involutions $\theta_M_i$ over $k$ ($i = 1..2$) if and only if $\gamma_1 = \alpha^2 * \gamma_2$ for some $\alpha \in k$.

**Proof.** $\iff$: Let the matrix $M_i$ of the form be $M = \begin{pmatrix} 1 & 0 \\ 0 & \gamma_i \end{pmatrix}$. If $\gamma_1 = \alpha^2 * \gamma_2$ for 2 such matrices $M_1$ and $M_2$, then $M_1 = Q^T M_2 Q$ where $Q = \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$. Then $M_1 \cong M_2$ (so also they are semi-congruent), and by the Classification Theorem 2.5 we know that their involutions are isomorphic.

$\implies$: If the 2 involutions $\theta_{M_1}$ and $\theta_{M_2}$ are isomorphic, then we know from the Classification Theorem 2.5 that $M_1$ and $M_2$ are semi-congruent. Taking determinants of both sides of
Chapter 3. Involutions of $\text{SL}(2, k)$

$M_1 = cQ^T M_2 Q$ where $c$ is a scalar in $k^*$ yields $\gamma_1 = c^2 (\det Q)^2 \gamma_2 = (c \det Q)^2 \gamma_2$. We let $\alpha = c \det Q$ and obtain our result that $\gamma_1 = \alpha^2 \gamma_2$ for some $\alpha \in k$.

**Corollary 1.** The number of isomorphism classes of involutions of $\text{SL}(2, k)$ is equal to $|k^*/(k^*)^2|$, and each representative $\theta$ has the form $\theta = \text{Inn}_B$, where $B = \begin{pmatrix} 0 & -m_2 \\ 1 & 0 \end{pmatrix}$ and $m$ is a representative of $k^*/(k^*)^2$.

### 3.3 The $p$-adic Numbers

One field over which we will work is the field of $p$-adic numbers $\mathbb{Q}_p$. This is defined as the completion of the field of rational numbers $\mathbb{Q}$, which is the rationals plus all of their limit points. The notion of a limit point depends upon a given norm. For the $p$-adics we take this norm to be the $p$-norm. We write elements of $\mathbb{Q}_p$ as

$$\mathbb{Q}_p = \{ \sum_{i=-n}^{\infty} a_i p^i \mid a_i = 0, 1, \ldots, p-1 \in \mathbb{Z} \}$$

Then the $p$-norm for a given prime number $p$ and a given $p$-adic number $x = \sum_{i=-n}^{\infty} a_i p^i$ is defined to be $|x|_p = p^{-n}$. This gives us a sense of distance with which to define our limit points and therefore the completion of the rationals with respect to this norm.

As is clear from Corollary 1, the size of the square-class group of a field is a critical piece of information used in classifying our bilinear forms and our involutions. We will use this not only for $\text{SL}(2, k)$ in this chapter, but for $\text{SL}(n, k)$ ($n > 2$) later in this thesis as well. The following properties are essential, and proofs may be found in [Rob2000]. Since $\text{char} \mathbb{Q}_p = 0$ for any prime $p$, we use $p = 2$ in addition to all the odd primes.

**Proposition 3.** (1) The cosets $(\mathbb{Q}_2^*)/(\mathbb{Q}_2^*)^2$ are represented by the eight elements of the set $S = \{ 1, -1, 2, -2, 3, -3, 6, -6 \}$.

(2) The cosets $(\mathbb{Q}_p^*)/(\mathbb{Q}_p^*)^2$ $p \neq 2$ are represented by the four elements $1, p, S_p, pS_p$, where $S_p$ is the “smallest” non-square element of $\mathbb{Q}_p$. 

3.4 Classification of Involutions of SL(2, k)

(1) \( k = \overline{k} \): If our field is algebraically closed, there is only one element in the square class group, with representative 1. There is only one congruence class of symmetric non-degenerate bilinear forms, with representative \( M = Id_{n \times n} \). Thus, over an algebraically closed field all forms are equivalent to the standard dot product. All involutions are therefore isomorphic, with representative \( \theta = \text{Inn}_{B_1} \), where \( B_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \) with \( \theta(A) = \text{Inn}_M(A^T)^{-1} = (A^T)^{-1} \).

(2) \( k = \mathbb{R} \): Over the real numbers, there are 3 congruence classes of symmetric bilinear forms, with \( M_1 = Id, M_3 = -Id \), and \( M_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \). Two of these however, \( Id_{n \times n} \) and \( -Id_{n \times n} \), are in the same semi-congruence class. Thus, there are only 2 isomorphism classes of involutions over the real numbers. They are represented by \( \theta = \text{Inn}_{B_1} \) (same \( \theta \) as for \( k = \overline{k} \)), and by \( \tau = \text{Inn}_{B_2} \), where \( B_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \).

The action of \( \tau \) is: \( \tau(A) = \begin{pmatrix} a_{2,2} & a_{2,1} \\ a_{1,2} & a_{1,1} \end{pmatrix} \).

Example 3.1. Consider \( \theta = \text{Inn}_{B_1} \) and \( \tau = \text{Inn}_{B_2} \) from above. On SL(2, \( \mathbb{C} \)) they are isomorphic since \( M_1 \cong M_2 \) via \( Q = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \):

\[
\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}^T (Id) \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}
\]

Yet there is no such matrix \( Q \) \( GL(2, \mathbb{R}) \) which gives this relationship, so the conjugations represent separate involution classes over the real numbers.

(3) \( k = \mathbb{Q} \): This case is not very enlightening since \( |(k^*)/(k^*)^2| = \infty \). There are infinitely many congruence classes and infinitely many semi-congruence classes. So there are infinitely many isomorphism classes of involutions.

(4) \( k = \mathbb{F}_p \ (p \neq 2) \): Since \( (k^*)/(k^*)^2 \) consists of only 2 cosets—the set of squares and the set of non-squares, there are 2 semi-congruence classes (and 2 congruence classes as
well), represented by $M = \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix}$, where $m$ is either 1 or $S_p$ the “smallest” non-square element of $\mathbb{F}_p$.

**Example 3.2.** Consider the two symmetric forms represented by $M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ and $M_2 = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$ and their induced involutions $\theta_1$ and $\theta_2$. Over $\mathbb{F}_5$ they are congruent via multiplication of $M_1$ by $Q^T$ on the left and $Q$ on the right where $Q = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. Yet, over $\mathbb{F}_7$ they aren’t congruent as no such $Q$ does the trick.

This is due to the two cosets of $(\mathbb{F}_5^*)/((\mathbb{F}_5^*)^2$ being $\{1, 4\}$ and $\{2, 3\}$ while for $\mathbb{F}_7$ the 2 cosets are $\{1, 2, 4\}$ and $\{3, 5, 6\}$. Thus, we get 2 isomorphism classes of involutions as well.

**The p-adic Numbers**

Recall that the characteristic of $\mathbb{Q}_p$ is zero for any $p$, so we may use $p = 2$ as well.

(5) $k = \mathbb{Q}_2$: Here we get eight semi-congruence classes represented by $M$ as above with $m = 1, -1, 2, -2, 3, -3, 6, -6$ since these elements represent the 8 cosets in $(\mathbb{Q}_2^*)/(\mathbb{Q}_2^*)^2$. So there are 8 classes of involutions on $\text{SL}(2, \mathbb{Q}_2)$.

(6) $k = \mathbb{Q}_p \ (p \neq 2)$: We get only 4 semi-congruence classes, represented by $M$ with $m = 1, p, S_p, pS_p$, with $S_p$ the same as for $\mathbb{F}_p$. Notice that this is a generalization of the case for $\mathbb{Q}_2$ except that each of the negatives of these 4 choices gave different involutions since $-1$ is not a square in $\mathbb{Q}_2$. Thus, there are 4 isomorphism classes of involutions on $\mathbb{Q}_p$.

This gives a complete classification of involutions on $\text{SL}(2, k)$ for the most important fields $k$ such that the characteristic of $k$ is not 2.

### 3.5 A Note on the Skew-Symmetric Form on $k^2$

There are no involutions coming from skew-symmetric bilinear forms on $k^2$. 
Lemma 5. (1) All skew-symmetric bilinear forms on \( k^2 \) are semi-congruent to the form represented by the matrix

\[
M = \begin{pmatrix}
0 & -1 \\
1 & 0
\end{pmatrix}.
\]

(2) The only induced automorphism from the skew-symmetric form on \( k^2 \) is therefore

\[
\theta(A) = \text{Inn}_M(A^T)^{-1} = A \quad \text{(i.e. } \theta_M \text{ is the identity automorphism)} \text{ which is not an involution.}
\]

Proof. (1) A skew-symmetric form is represented by a skew-symmetric matrix \( M \). The requirement that \( M = -M^T \) forces \( M \) to have the form

\[
\begin{pmatrix}
0 & -\alpha \\
\alpha & 0
\end{pmatrix}
\]

which is semi-congruent to \( \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \).

(2) Simply note that \( \text{Inn}_M(A) = (A^T)^{-1} \forall A \in G \). So \( \theta_M = \text{Inn}_M \text{Inn}_M = \text{Inn}_M^2 = \text{Id} \). \( \square \)

When we showed that \( \theta \) defined by \( \theta(A) = \text{Inn}_M(A^T)^{-1} \) was an involution, we actually showed that \( \theta^2 \) was the identity, rather than showing \( \text{ord}(\theta) = 2 \). This is equivalent except in this specific case where \( \theta = \text{Id} \). Thus, there are no involutions induced by the skew-symmetric form. Otherwise, the fixed-point group of \( \theta \) would be \( H = G \) and the resulting symmetric space would be \( X = G/G = \{e\} \).

3.6 Illustration of Resulting Symmetric Spaces

As an example of what the nature of our symmetric spaces will be which we obtain from these involutions, let’s specify the case where \( k = \mathbb{R} \). We have two involutions:

\[
\theta_1(A) = (A^T)^{-1}
\]
and
\[
\theta_2(A) = \begin{pmatrix}
a_{2,2} & a_{2,1} \\
a_{1,2} & a_{1,1}
\end{pmatrix}.
\]

The first fixed-point group \( H_1 \) of \( \theta_1 \) is
\[
H_1 = \{ A \in G | (A^T)^{-1} = A \ (i.e. A^T = A^{-1}) \} = \text{SO}(2, k)
\]
which is the standard 2-dimensional special orthogonal group of rotations. Each of its matrix entries has the form
\[
A = \begin{pmatrix}
\alpha & \beta \\
-\beta & \alpha
\end{pmatrix}
\]
where \( \alpha^2 + \beta^2 = 1 \), and \( H_1 \) is isomorphic to the unit circle. Thus, the symmetric space \( X = G/H = G/\text{SO}(2, k) \) comes from treating all the rotations as being identified with the identity automorphism. Two matrices in \( G \) are considered identical if they differ only by a rotation. This make sense instinctively as when one considers a traditional “map” one does not consider it functionally different if it is rotated.

The matrix elements of \( H_2 \) the fixed-point group of \( \theta_2 \) have the form
\[
A = \begin{pmatrix}
\alpha & \beta \\
\beta & \alpha
\end{pmatrix}
\]
where \( \alpha^2 - \beta^2 = 1 \), and \( H_2 = \text{SO}(1, 1) \) is isomorphic to a hyperbola. Its symmetric space is \( X = G/H_2 \). Notice that the fixed-point group here is closed and non-compact, whereas the fixed-point group \( H_1 \) of \( \theta_1 \) is closed and compact. These are the 2 resulting symmetric spaces obtained from \( G \) over \( k = \mathbb{R} \).

### 3.7 Table of Involutions of \( G = \text{SL}(2, k) \)

To summarize the results of this chapter, we give a table with representatives of the isomorphism classes of involutions on \( G \) over algebraically closed fields (i.e. the complex numbers), the real numbers, finite fields, and the \( p \)-adic numbers. The theory is field independent with the exception that the characteristic of \( k \) is not 2, and the table illustrates the
results over all important fields in the study of symmetric spaces. In the table the matrix $B$ is

$$B = \hat{B}M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}M = \begin{pmatrix} 0 & 1 \\ -m & 0 \end{pmatrix}$$

which gives $\text{Inn}_B(A) = \text{Inn}_M(A^T)^{-1} \forall A \in G$. Also, to shorten things for the $\mathbb{Q}_2$ case we let $S = \{1, -1, 2, -2, 3, -3, 6, -6\}$. 

### Chapter 3. Involutions of $\text{SL}(2, k)$

<table>
<thead>
<tr>
<th>Field</th>
<th>Semi-Congruence Class $M$</th>
<th>Involution $\theta = \text{Inn}_B$</th>
<th>Action of the Involution on $G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k = \mathbb{K}$</td>
<td>$M = I_{2 \times 2}$</td>
<td>$B = \begin{pmatrix} 0 &amp; -1 \ 1 &amp; 0 \end{pmatrix}$</td>
<td>$\theta(A) = (A^T)^{-1}$</td>
</tr>
<tr>
<td>$k = \mathbb{R}$</td>
<td>$M_1 = I_{2 \times 2}$</td>
<td>$B_1 = \begin{pmatrix} 0 &amp; -1 \ 1 &amp; 0 \end{pmatrix}$</td>
<td>$\theta_1(A) = (A^T)^{-1}$</td>
</tr>
<tr>
<td></td>
<td>$M_2 = \begin{pmatrix} 1 &amp; 0 \ 0 &amp; -1 \end{pmatrix}$</td>
<td>$B_2 = \begin{pmatrix} 0 &amp; 1 \ 1 &amp; 0 \end{pmatrix}$</td>
<td>$\theta_2(A) = \begin{pmatrix} a_{2,2} &amp; a_{2,1} \ -a_{1,2}/a_i &amp; a_{1,1} \end{pmatrix}$</td>
</tr>
<tr>
<td>$k = \mathbb{Q}$</td>
<td>$M_i = \begin{pmatrix} 1 &amp; 0 \ 0 &amp; a_i \end{pmatrix}$</td>
<td>$B_i = \begin{pmatrix} 0 &amp; -a_i \ 1 &amp; 0 \end{pmatrix}$ for any $i = i_1, i_2 \in \mathbb{N}$ such that $q \in \mathbb{Q}$</td>
<td>$\theta_i(A) = \begin{pmatrix} a_{2,2} &amp; -a_i a_{2,1} \ -a_{1,2}/a_i &amp; a_{1,1} \end{pmatrix}$</td>
</tr>
<tr>
<td>$k = \mathbb{F}_p$</td>
<td>$M_1 = I_{2 \times 2}$</td>
<td>$B_1 = \begin{pmatrix} 0 &amp; -1 \ 1 &amp; 0 \end{pmatrix}$</td>
<td>$\theta_1(A) = (A^T)^{-1}$</td>
</tr>
<tr>
<td>$p \neq 2$</td>
<td>$M_2 = \begin{pmatrix} 1 &amp; 0 \ 0 &amp; S_p \end{pmatrix}$</td>
<td>$B_2 = \begin{pmatrix} 0 &amp; -S_p \ 1 &amp; 0 \end{pmatrix}$</td>
<td>$\theta_2(A) = \begin{pmatrix} a_{2,2} &amp; -S_p a_{2,1} \ -a_{1,2}(S_p)^{-1} &amp; a_{1,1} \end{pmatrix}$</td>
</tr>
<tr>
<td>$k = \mathbb{Q}_2$</td>
<td>$M_i = \begin{pmatrix} 1 &amp; 0 \ 0 &amp; a_i \end{pmatrix}$</td>
<td>$B_i = \begin{pmatrix} 0 &amp; -a_i \ 1 &amp; 0 \end{pmatrix}$ for any $i = a_i \in {S}$</td>
<td>$\theta_i(A) = \begin{pmatrix} a_{2,2} &amp; -a_{1,2}(a_i)^{-1} \ -a_{1,2}(a_i)^{-1} &amp; a_{1,1} \end{pmatrix}$</td>
</tr>
<tr>
<td>$k = \mathbb{Q}_p$</td>
<td>$M_i = \begin{pmatrix} 1 &amp; 0 \ 0 &amp; a_i \end{pmatrix}$</td>
<td>$B_i = \begin{pmatrix} 0 &amp; -a_i \ 1 &amp; 0 \end{pmatrix}$ for any $i = a_i \in {1, 2, 3, 6}$</td>
<td>$\theta_i(A) = \begin{pmatrix} a_{2,2} &amp; -a_i a_{2,1} \ -a_{1,2}(a_i)^{-1} &amp; a_{1,1} \end{pmatrix}$</td>
</tr>
</tbody>
</table>
Chapter 4

Involutions of $\text{SL}(n, k)$ for $n > 2$

4.1 Preliminaries

Our basic reference for reductive groups will be the papers of Borel and Tits [BT65], [BT72] and also the books of Borel [Bor91], Humphreys [Hum72] and Springer [Spr81]. We shall follow their notations and terminology. All algebraic groups and algebraic varieties are taken over an arbitrary field $k$ (of characteristic $\neq 2$) and all algebraic groups considered are linear algebraic groups.

For this chapter, $G$ will denote $\text{SL}(n, k)$ and $\tilde{G}$ will denote $\text{SL}(n, \tilde{k})$, where it is understood that $n > 2$ (most of the results in this chapter will not hold in the specific case that $n = 2$). All bilinear forms are taken over the vector spaces $V = k^n$ or $\tilde{V} = \tilde{k}^n$. Let $k^*$ denote the product group of all nonzero elements of $k$, $(k^*)^2 = \{x^2 \mid x \in k^*\}$, and let $\text{Id}$ denote the identity automorphism on $G$.

4.2 Outer Involutions of $\text{SL}(n, k)$

Unlike the case for $\text{SL}(2, k)$, not all involutions on $\text{SL}(n, k)$ will come from bilinear forms when $n > 2$, but all those that are not inner will.

Definition 10. An automorphism $\theta$ of $G$ is said to be an outer automorphism if $\theta \notin \text{Inn} G$.

Lemma 6. [Bor91]
Chapter 4. Involutions of $\text{SL}(n, k)$

(1) If $k$ is algebraically closed, then $|\text{Aut}(G)/\text{Inn}(G)| = 2$.

(2) Any outer automorphism can be written as $\text{Inn}_M \phi$, where $\phi$ is a fixed outer automorphism.

Remark 7. For our purposes it will be most convenient to take for $\phi$ the involution defined by $\phi(A) = (A^T)^{-1}$.

Now, since our construction of involutions from bilinear forms is $\theta(A) = M^{-1}(A^T)^{-1}M = \text{Inn}_M(\phi(A))$, the isomorphism classes of outer involutions will come once again from our semi-congruence classes of bilinear forms. We need first to check whether all outer involutions come from these forms.

**Lemma 7.**

(1) $\text{Inn}_M \phi$ is an involution of $G \iff \phi(M)M \in Z(G)$.

(2) $\phi(M)M \in Z(G) \iff M$ is symmetric or skew-symmetric.

(3) $\text{Inn}_M \phi$ is an involution of $G \iff M$ is symmetric or skew-symmetric, and $M$ is only skew-symmetric if $n$ is even.

**Proof.**

(1) We know that $\text{Inn}_M \phi$ is an involution $\iff (\text{Inn}_M \phi)^2 = \text{Id}$ on $G$. Then the following are each equivalent:

(a) $\text{Inn}_M \phi \text{Inn}_M \phi(X) = X \forall X \in G$

(b) $\text{Inn}_M \phi(M^{-1}\phi(X)M) = \text{Inn}_M \phi(M^{-1})\phi(\phi(X))\phi(M) = X$

(c) $M^{-1}\phi(M^{-1})X\phi(M)M = X$

(d) $X\phi(M)M = \phi(M)MX \forall X \in G$

(e) $\phi(M)M \in Z(G)$

(2) $\iff$: If $M$ is symmetric, then $M = M^T$ and $\phi(M)M = (M^T)^{-1}M = M^{-1}M = I_{n \times n}$, which is clearly in $Z(G)$. If $M$ is skew-symmetric, then $M = -M^T$ and $\phi(M)M = (M^T)^{-1}M = (-M)^{-1}M = -I_{n \times n}$, which is also in $Z(G)$.
Chapter 4. Involutions of SL(n, k)

\[ \implies: \text{If } \phi(M)M = (M^T)^{-1}M \in Z(G) \text{ then } (M^T)^{-1}MX = X(M^T)^{-1}M \forall X \in G \]
and so \((M^T)^{-1}MXM^{-1}M^T = X \forall X \in G\). Then

\[ \text{Inn}_{M^{-1}M^T} = \text{Id}, \implies M^{-1}M^T = \alpha I_{n \times n} \]

for some \(\alpha \in k\). So \(M^T = \alpha M\). Taking determinants of both sides,

\[ \det(M) = (\alpha)^n \det(M), \implies \alpha^n = 1. \]

If \(n\) is odd, then \(\alpha = 1\) and \(M = M^T\). If \(n\) is even, then \(\alpha = 1\) or \(-1\), and \(M = M^T\)
or \(M = -M^T\).

(3) The third statement follows immediately from the first two propositions. \(\Box\)

We’ve already shown that our \(\theta_M = \text{Inn}_M \phi\) is an involution, but this lemma tells us that all outer involutions will be \(\theta_M\) for some symmetric or skew-symmetric matrix \(M\). So we have the following application of the Classification Theorem 2.5.

**Theorem 4.1 (Outer Classification Theorem).** If \(\theta_1\) and \(\theta_2\) are outer involutions on \(\text{SL}(n, k)\), then they come from bilinear symmetric or skew-symmetric forms represented by \(M_1\) and \(M_2\) (respectively), and

\[ M_1 \cong^s M_2 \text{ over } k \iff \theta_1 \approx \theta_2. \]

**Proof.** The proof is fairly clear from the original Classification Theorem 2.5 and the preceding lemmas and remarks. Let \(\phi\) denote the outer involution defined by \(\phi(X) = (X^T)^{-1}\). Given bilinear symmetric or skew-symmetric forms on \(V = k^n\) represented by matrices \(M_1\) and \(M_2\), the involution of the form is by definition \(\theta_{M_i} = \text{Inn}_{M_i} \phi\). We’ve shown in Lemma 6 and Lemma 7 that all outer involutions of \(G\) have this form, where the matrix of the conjugation is symmetric or skew-symmetric. Therefore all the outer involutions of \(G\) come from bilinear symmetric or skew-symmetric forms, and the Classification Theorem 2.5 proven in Chapter 2 gives us the equivalence between semi-congruence of these forms and isomorphism of their involutions. \(\Box\)
Chapter 4. Involutions of $\text{SL}(n, k)$

Corollary 2. $\text{Inn}_M \phi \approx \text{Inn}_M \phi$ over $G \iff M_1 \cong^s M_2$ over $k$.

Hence, once again our classification of (outer) involutions reduces to a classification of bilinear forms via semi-congruence.

4.3 Congruence Properties of Symmetric/Skew-Symmetric $n \times n$ Matrices

Some well-known information from bilinear algebra will be immensely useful for what follows.

Theorem 4.2. (1) Symmetric matrices are congruent to diagonal matrices whose entries are representatives of the square-class group $k^*/(k^*)^2$.

(2) Skew-Symmetric matrices are congruent to the $(2m) \times (2m)$ matrix $J_{2m}$, where $n = 2m$ and

\[ J_{2m} = \begin{pmatrix} 0 & I_{m \times m} \\ -I_{m \times m} & 0 \end{pmatrix} \]

Proof. (1) When we referred to [Szy97] for the proof of Lemma 3.1 in Chapter 3, his proof was that $n \times n$ symmetric matrices (not simply $2 \times 2$ matrices) are congruent to diagonal matrices. Then it is also true that if $b_1, b_2, \ldots, b_n \in k^*$ then

\[ \text{diag}(a_1, a_2, \ldots, a_n) \cong \text{diag}(b_1^2a_1, b_2^2a_2, \ldots, b_n^2, a_n) \]

over $k$ via $Q = \text{diag}(b_1, b_2, \ldots, b_n)$ since

\[ \text{diag}(b_1^2a_1, b_2^2a_2, \ldots b_n^2, a_n) = Q^T \text{diag}(a_1, a_2, \ldots, a_n)Q. \]

This shows the first claim to be true.

(2) This is a well-known result, and we refer to [Art91] for this result.

Lemma 8. (1) We can choose our matrix $M$ representing the classes of semi-congruent symmetric matrices to be a diagonal matrix with only non-zero diagonal entries.
Chapter 4. Involutions of SL($n, k$)

(2) We only obtain the lone congruence class (hence there’s only one semi-congruence class) of skew-symmetric matrices when $n$ is even.

Proof. (1) The only bilinear forms in consideration are non-degenerate, which means $\det(M) \neq 0$. This requires non-zero elements along the diagonal of a diagonal matrix $M$.

(2) If $M$ is skew-symmetric then $M = -M^T \implies \det(M) = (-1)^n \det(M)$, $\implies n$ is even or $\det(M) = 0$, the latter being impossible with a matrix representing a non-degenerate form. Thus, $n$ is even. 

The above information tells us that to use semi-congruence properties of bilinear forms to classify their induced outer involutions, it suffices to focus on diagonal matrices (and in fact we can divide out the $[1, 1]$ entry of our matrix $M$ of the bilinear form to normalize the first diagonal element to 1) and the matrix $J_{2m}$.

4.4 Classification of Outer Involutions of SL($n, k$) for $k \neq H11937$

(1) $k = \bar{k}$: In $n$ dimensions there is only one congruence class of symmetric non-degenerate bilinear forms and only one congruence class of skew-symmetric forms as well. Hence there is only one semi-congruence class of each.

(a) $n$ odd: All forms are equivalent to the standard dot product, so there is one isomorphism class of involutions, that represented by $\phi$.

(b) $n$ even: Here we add the skew-symmetric forms induced involution, with the skew-symmetric form represented by $M = J_{2m}$. There are two classes of involutions, represented by $\phi$ and $\text{Inn}_{J_{2m}} \phi$.

(2) $k = \mathbb{R}$: All congruence classes of symmetric forms are given by $M = I_{n-i,i}$ $i = 0, 1, \ldots, n$ where $I_{n-i,i} = \begin{pmatrix} I_{n-i \times n-i} & 0 \\ 0 & -I_{i \times i} \end{pmatrix}$. When $n$ is even, we also have $M = J_{2m}$ representing the sole congruence class for skew-symmetric forms. Thus, the symmetric
Chapter 4. Involutions of $\text{SL}(n, k)$

forms have $n + 1$ congruence classes, but only $\frac{n+1}{2}$ semi-congruence classes since $I_{n-i,i} = -I_{i,n-i}$.

(a) **n odd**: There are $\frac{n+1}{2}$ isomorphism classes of involutions, represented by $\text{Inn}_M \phi$, where $M = I_{n-i,i}$ $i = 0, 1, \ldots, \frac{n-1}{2}$.

(b) **n even**: There are $\frac{n}{2} + 2$ classes of involutions, represented by $\text{Inn}_M \phi$, where $M = I_{n-i,i}$ $i = 0, 1, \ldots, \frac{n}{2}$ or $J_{2m}$.

(3) $k = \mathbb{Q}$: As in the case when $n = 2$, there are infinitely many congruence classes and infinitely many isomorphism classes of involutions.

Before proceeding to finite fields and $p$-adic fields, we need to introduce some notation for some matrices that will be used.

**Notation 1.** $I_{n-i,i}$ and $J_{2m}$ have already been introduced. Let

$$L_{n,x} = \begin{pmatrix} 0 & 1 & \ldots & 0 & 0 \\ \vdots & x & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & \ldots & x & 0 \end{pmatrix}.$$

Notice that $J_{2m} \cong L_{n,-1}$. Let

$$M_{n,x,y,z} = \begin{pmatrix} I_{n-3 \times n-3} & 0 & 0 & 0 \\ 0 & x & 0 & 0 \\ 0 & 0 & y & 0 \\ 0 & 0 & 0 & z \end{pmatrix}.$$

(4) $k = \mathbb{F}_p$ $(p \neq 2)$: First we need 2 useful lemmas.

**Lemma 9.**

(1) $|\mathbb{F}_p^*/(\mathbb{F}_p^*)^2| = 2$ when $p \neq 2$.

(2) Every element of $k = \mathbb{F}_p$ $(p \neq 2)$ can be written as the sum of 2 squares in $\mathbb{F}_p$. 
Chapter 4. Involutions of $\text{SL}(n, k)$

Proof. (1) Define $\rho$ on $\mathbb{F}_p$ by $\rho(x) = x^2$. Since the equation $x^2 = 1$ has 2 solutions, $|\ker \rho| = 2$. Then since $\mathbb{F}_p/\ker \rho \approx \text{Im } \rho$ and $\text{Im } \rho = \mathbb{F}_p^*/(\mathbb{F}_p^*)^2$, we see that $|\mathbb{F}_p^*/(\mathbb{F}_p^*)^2| = 2$.

(2) It is known that $|\mathbb{F}_p^2| = \frac{p+1}{2}$ from the first result and adding the zero element, which is also a square. Let $x$ be a non-square element of $\mathbb{F}_p$. It is clear that $|\{x - \mathbb{F}_p^2\}| = \frac{p+1}{2}$ as well. This means that $\mathbb{F}_p^2 \cap \{x - \mathbb{F}_p^2\}$ is non-empty since $\dim \mathbb{F}_p^2 + \dim \{x - \mathbb{F}_p^2\} = \frac{p+1}{2} + \frac{p+1}{2} = p+1$.

Given any element $x \in \mathbb{F}_p$, if $x$ is a square then it is certainly a sum of 2 squares, itself plus zero. If $x$ is not a square, then there is an element $q$ of $\mathbb{F}_p$ which is in $\mathbb{F}_p^2 \cap \{x - \mathbb{F}_p^2\}$. Therefore, this element $q = a^2$ for some $a \in \mathbb{F}_p$ and $q = x - b^2$ for some $b \in \mathbb{F}_p$. Equating these 2 forms for $q$ tells us that $a^2 = x - b^2$, or equivalently, $x = a^2 + b^2$. Thus, any element can be written as the sum of two squares. \hfill \Box

Lemma 10. Over $\mathbb{F}_p$ ($p \neq 2$) we have that for any $2 \times 2$ block $A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$,

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \cong I_{2 \times 2}.$$  

Proof. The second part of Lemma 9 tells us that $\frac{1}{\alpha} = b^2 + c^2$ for some $b, c \in \mathbb{F}_p$ since it is in $\mathbb{F}_p$ as well. Let $P = \begin{pmatrix} b & -c \\ c & b \end{pmatrix}$. Then

$$P^T A P = \begin{pmatrix} (b^2 + c^2)\alpha & 0 \\ 0 & (b^2 + c^2)\alpha \end{pmatrix} = I_{2 \times 2}$$

and $A \cong I_{2 \times 2}$. \hfill \Box

So we can get either all 1’s on the diagonal or at most we have one $S_p$ left over in the $(n, n)$ slot.

(1) $n$ odd: We have 2 congruence and 2 semi-congruence classes of symmetric bilinear forms, given by $M = \text{Id}$ and $M = M_{n, S_p}$. Therefore we get 2 involution classes, represented by $\phi$ and $\text{Inn}_{M_{n, S_p}} \phi$.

(2) $n$ even: We have 3 isomorphism classes of involutions, the 2 from above plus $\text{Inn}_{J_{2m}} \phi$. 

### Chapter 4. Involutions of SL(n, k)

Table 4.1: Outer Involutions of G over $k \neq \mathbb{Q}_p$

<table>
<thead>
<tr>
<th>Field</th>
<th>Semi-Congruence Class $M$</th>
<th>Involution Class on $G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k = k$</td>
<td>$M = I_{n \times n}$</td>
<td>$\theta(A) = (A^T)^{-1}$</td>
</tr>
<tr>
<td>$n$ odd</td>
<td>$M = I_{n \times n}$</td>
<td>$\theta_1(A) = (A^T)^{-1}$</td>
</tr>
<tr>
<td>$n$ even</td>
<td>$M = I_{n \times n}$</td>
<td>$\theta_2(A) = \text{Inn}<em>{J</em>{2m}(A^T)}^{-1}$</td>
</tr>
<tr>
<td>$n$ even</td>
<td>$M = J_{2m}$ ($n = 2m$)</td>
<td>$\theta_2(A) = \text{Inn}<em>{J</em>{2m}(A^T)}^{-1}$</td>
</tr>
<tr>
<td>$k = \mathbb{R}$</td>
<td>$M_i = I_{n-i,i}$</td>
<td>$\theta_i(A) = \text{Inn}_{M_i(A^T)}^{-1}$</td>
</tr>
<tr>
<td>$n$ odd</td>
<td>$i = 0, 2, \ldots, \frac{n-1}{2}$</td>
<td>$\theta_i(A) = \text{Inn}_{M_i(A^T)}^{-1}$</td>
</tr>
<tr>
<td>$n$ even</td>
<td>$i = 0, 1, 2, \ldots, \frac{n}{2}$</td>
<td>$\theta_J(A) = \text{Inn}<em>{J</em>{2m}(A^T)}^{-1}$</td>
</tr>
<tr>
<td>$n$ even</td>
<td>$M_{\frac{n}{2}+2} = J_{2m}$</td>
<td>$\theta_J(A) = \text{Inn}<em>{J</em>{2m}(A^T)}^{-1}$</td>
</tr>
<tr>
<td>$k = \mathbb{Q}$</td>
<td>$M_{\alpha_2,\ldots,\alpha_n} = \begin{pmatrix} 1 &amp; 0 &amp; 0 &amp; \ldots &amp; 0 \ \vdots &amp; a_2 &amp; 0 &amp; \ldots &amp; 0 \ \vdots &amp; 0 &amp; a_3 &amp; \ldots &amp; 0 \ \vdots &amp; \vdots &amp; \vdots &amp; \ddots &amp; \vdots \ 0 &amp; 0 &amp; 0 &amp; 0 &amp; a_n \end{pmatrix}$</td>
<td>$\theta_{\alpha_2,\ldots,\alpha_n}(A) = \text{Inn}<em>{M</em>{\alpha_2,\ldots,\alpha_n}(A^T)}^{-1}$</td>
</tr>
<tr>
<td>$n$ odd</td>
<td>$\alpha_i \in \mathbb{Q}^*/\mathbb{Q}^*2$</td>
<td>$\theta_{\alpha_2,\ldots,\alpha_n}(A) = \text{Inn}<em>{M</em>{\alpha_2,\ldots,\alpha_n}(A^T)}^{-1}$</td>
</tr>
<tr>
<td>$n$ even</td>
<td>$M_{\alpha_2,\ldots,\alpha_n} = \begin{pmatrix} 1 &amp; 0 &amp; 0 &amp; \ldots &amp; 0 \ \vdots &amp; a_2 &amp; 0 &amp; \ldots &amp; 0 \ \vdots &amp; 0 &amp; a_3 &amp; \ldots &amp; 0 \ \vdots &amp; \vdots &amp; \vdots &amp; \ddots &amp; \vdots \ 0 &amp; 0 &amp; 0 &amp; 0 &amp; a_n \end{pmatrix}$</td>
<td>$\theta_{\alpha_2,\ldots,\alpha_n}(A) = \text{Inn}<em>{M</em>{\alpha_2,\ldots,\alpha_n}(A^T)}^{-1}$</td>
</tr>
<tr>
<td>$n$ even</td>
<td>$M_J = J_{2m}$</td>
<td>$\theta_J(A) = \text{Inn}<em>{J</em>{2m}(A^T)}^{-1}$</td>
</tr>
<tr>
<td>$k = \mathbb{F}_p$, $p \neq 2$</td>
<td>$M_1 = I_{n \times n}$</td>
<td>$\theta_1(A) = (A^T)^{-1}$</td>
</tr>
<tr>
<td>$n$ odd</td>
<td>$M_2 = \begin{pmatrix} I_{(n-1) \times (n-1)} &amp; 0 \ 0 &amp; S_p \end{pmatrix}$</td>
<td>$\theta_2(A) = \text{Inn}_{M_2(A^T)}^{-1}$</td>
</tr>
<tr>
<td>$n$ even</td>
<td>$M_2 = \begin{pmatrix} I_{(n-1) \times (n-1)} &amp; 0 \ 0 &amp; S_p \end{pmatrix}$</td>
<td>$\theta_3(A) = \text{Inn}_{M_3(A^T)}^{-1}$</td>
</tr>
<tr>
<td>$n$ even</td>
<td>$M_3 = J_{2m}$</td>
<td>$\theta_3(A) = \text{Inn}_{M_3(A^T)}^{-1}$</td>
</tr>
</tbody>
</table>
Chapter 4. Involutions of $\text{SL}(n, k)$

4.5 Classification of Outer Involutions of $G = \text{SL}(n, \mathbb{Q}_p)$

The case for the $p$-adic numbers will be much messier than what we’ve seen so far. We need some background theory about the $p$-adic numbers first.

**Definition 11 ($p$-sign, Hasse Symbol).** Given a matrix $M$, let $D_i$ be the determinant of the upper left $i \times i$ square submatrix of $M$. Define the $p$-sign of two non-zero $p$-adic numbers to be $(\alpha, \beta)_p = 1$ if $ax^2 + \beta y^2 = 1$ has a solution in $\mathbb{Q}_p$, $-1$ otherwise. Then the Hasse Symbol $c_p(M)$ of $M$ is defined by

$$c_p(M) = (-1, -D_n)_p \prod_{i=1}^{n-1} (D_i, -D_{i+1})_p.$$

This definition seems complicated, but the Hasse Symbol is merely a product of 1s and $-1$s, so that its choices are limited to 1 or $-1$. The following formula can be found in [Szy97].

**Lemma 11.** If $M$ is an $n \times n$ matrix and $\alpha \in \mathbb{Q}_p$ we have the following formula:

$$c_p(\alpha A) = \begin{cases} 
(a, -1)^{n/2}_p (\alpha, D_n)_p c_p(M) & \text{if } n \text{ is even} \\
(a, -1)^{(n+1)/2}_p c_p(M) & \text{if } n \text{ is odd}
\end{cases}.$$

This new information leads to an essential theorem. For its proof we refer to [Jon55].

**Theorem 4.3.** Two symmetric matrices $M_1$ and $M_2$ with entries in $\mathbb{Q}_p$ are congruent if and only if

$$\det(M_1) = \alpha^2 \det(M_2) \quad \text{and} \quad c_p(M_1) = c_p(M_2).$$

4.5.1 Results for $k = \mathbb{Q}_2$

By the previous theorem we see that one factor in congruence of 2 symmetric matrices is whether their determinants are in the same square-class group of $\mathbb{Q}_2$. This means that we are limited to at most 8 choices for a representative of the square class of the determinant $\{1, -1, 2, -2, 3, -3, 6, -6\}$, and the Hasse symbol has only the choices 1 and $-1$. So at
most there will be 16 semi-congruence classes of symmetric forms over \( \mathbb{Q}_2 \). To represent these classes we will use the dual value \((\alpha, c)\), where \(\alpha\) is the representative of the square class group and \(c\) is the Hasse symbol. Let \(d_{\alpha,c} = (\alpha, c)\), where \(\alpha\) has the eight choices from above and \(c\) is 1 or \(-1\). For \(\mathbb{Q}_2\) then, there are the 16 choices mentioned above.

(1) \(n\) even:

(a) \(n = 4k\): We get 10 semi-congruence classes. The first is represented by \(M = I_{n \times n}\) and the second by \(M = J_{2m}\). We also get \(M = M_{n,2,3,6}\). The other 7 choices are \(M = M_{n,1,1,x}\) where \(x\) is chosen from \{-1, 2, -2, 3, -3, 6, -6\} (\(M_{n,1,1,1}\) being simply the identity matrix that we’ve already counted). Ignoring for a second the skew-symmetric case represented by \(M = J_{2m}\), these matrices represent the semi-congruence forms for the matrices with dual values

\[
d_{1,1}, d_{1,-1}, d_{-1,1}, d_{2,1}, d_{-2,1}, d_{3,1}, d_{-3,1}, d_{6,1}, d_{-6,1}.
\]

For each of these choices \(M\), we get the involution class represented by \(\theta_M = \text{Inn}_M \phi\).

These results stem from the fact that the matrices with dual value \(d_{1,1}\) aren’t semi-congruent to those with dual value \(d_{1,-1}\). The first give us \(\phi\) and the second give \(\text{Inn}_{M_{n,2,3,6}} \phi\) identifying the involution classes. To show this we use Theorem 11 for \(n = 4k\) and obtain

\[
c_2(\alpha M) = (\alpha, D_n) c_2(M).
\]

When a matrix has determinant 1, then \(ax^2 + y^2 = 1\) having a solution in \(\mathbb{Q}_2\) implies \((\alpha, D_n)_2 = 1\) and \(c_2(\alpha A) = c_2(M)\) from the above equation. Thus, its Hasse symbol must remain the same under scalar multiplication. So \(d_{1,1}\) and \(d_{1,-1}\) represent different semi-congruence classes. Notice that \(M_{n,2,3,6}\) has \(\det(M_{n,2,3,6}) = 6^2\) (so its determinant is in the same square-class group as 1) and Hasse symbol \(c(M_{n,2,3,6}) = -1\).

On the other hand, \((\gamma, 1)\) and \((\gamma, -1)\) will give us semi-congruent matrices for \(\gamma \neq 1\) since in this case we can multiply by a scalar and change the Hasse symbol without changing the semi-congruence classes. To understand this, we see that for \(\gamma \neq 1\), the equation \(ax^2 + D_n y^2 = 1\) will not always have a solution, so equation 4.1 will be \(c_2(\alpha A) = -c_2(A)\)
for some $\alpha$. This means that multiplication of $M$ by an appropriate scalar can change the sign of the Hasse symbol without changing the semi-congruence class.

So there are 10 isomorphism classes of outer involutions over $\text{SL}(n, \mathbb{Q}_2)$ when $n = 4k$.

(b) $n = 4k + 2$: Again we get 10, but instead of obtaining the semi-congruence class of $M_{n,2,3,6}$ we get one represented by $M = M_{n,2,3,−6}$. The formula from Theorem 11 now gives us

$$c_2(\alpha M) = (\alpha, -1)^{2k+1}(\alpha, D_n) c_2(M)$$

which yields

$$c_2(\alpha M) = (\alpha, -1)^2(\alpha, -D_n) c_2(M) = (\alpha, D_n)^2 c_2(M).$$

Since $\det(M) = -1$ gives us $(\alpha, -D_n)^2 = (\alpha, 1)^2 = 1$, we obtain $c_2(\alpha M) = c_2(M)$ when $\det(M) = -1$. This results in $d_{-1,1}$ and $d_{-1,-1}$ representing different classes of forms. However, now $(\gamma, 1)$ matrices and $(\gamma, -1)$ matrices are semi-congruent for $\gamma \neq -1$ since there is some $\alpha$ which will change the Hasse sign. Thus, we replace the class typified by $d_{1,−1}$ from the $n = 4k$ case by $d_{-1,-1}$ and get $\text{Inn}_{M_{n,2,3,−6}} \phi$, and still we have 10 classes of involutions.

(2) $n$ odd: When $n$ is odd, we can multiply a matrix $M$ by the scalar $\gamma = \det(M)$ to get

$$\det(\gamma M) = (\gamma)^{2k}(\gamma) \det(M)$$

$$= (\gamma)^2 \det(M) \mod (\mathbb{Q}_2^*)^2$$

$$= (\det(M))^2 \mod (\mathbb{Q}_2^*)^2$$

$$= 1 \mod (\mathbb{Q}_2^*)^2$$

which means that we have matrices with determinants representing all the different square-classes of forms congruent to each other. From this we see that the representative of the square class group for the determinant can always be taken to be 1. So our only choices for matrices of the symmetric form (no skew-symmetric non-degenerate forms in the odd case) are those with dual value $d_{1,1}$ and $d_{1,−1}$. 
Chapter 4. Involutions of $SL(n, k)$

(a) $n = 4k + 1$: Here we can replace a matrix $M$ with dual value $d_{1,1}$ by a scalar multiple $\alpha M$ and get the same square-class for the determinant but with Hasse symbol changed to $c_2(\alpha M) = -1$. This result comes from using the formula from Theorem 11 to obtain

$$c_2(\alpha M) = (\alpha, -1)^{2k+1} c_2(M) = (\alpha, -1) c_2(M).$$

There will be an $\alpha$ such that $ax^2 - y^2 = 1$ will not have a solution in $\mathbb{Q}_2$, which means we’ll obtain $(\alpha, -1)_2 = -1$ and $c_2(\alpha M) = -c_2(M)$. Therefore the two classes of matrices with dual value $d_{1,1}$ and $d_{1,-1}$ are semi-congruent. So there is only one isomorphism class of involutions over $SL(n, \mathbb{Q}_2)$ for $n = 4k + 1$. The sole representative is $\phi$.

(b) $n = 4k + 3$: Now, there is no $\alpha$ that works as above. Theorem 11 ensures that

$$c_2(\alpha M) = (\alpha, -1)^{2k+2} c_2(M) = c_2(M).$$

Hence, any multiplication by a scalar $\alpha$ does not change the Hasse symbol, and $d_{1,1}$ and $d_{1,-1}$ give different classes of forms. As in the even case, this gives us $\phi$ and $\text{Inn}_{M_n,2,3,6}$ as the involutions representing the two different dual classes of symmetric forms.

This completes the classification for outer involutions of $SL(n, \mathbb{Q}_2)$. The results are illustrated in the following table.
### Table 4.2: Outer Involutions of $G$ over $k = \mathbb{Q}_2$

<table>
<thead>
<tr>
<th>dim($V$)</th>
<th>Dual Value $d_{\alpha,\epsilon}$ of the Semi-Congruence Class</th>
<th>Matrix $M$ such that $\theta(A) = \text{Inn}_M(A^T)^{-1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n = 4k$</td>
<td>$d_{1,1}$</td>
<td>$M_1 = I_{n \times n}$</td>
</tr>
<tr>
<td></td>
<td>$d_{1,-1}$</td>
<td>$M_{n,2,3,6}$</td>
</tr>
<tr>
<td></td>
<td>$d_{-1,1}$</td>
<td>$M_{n,1,1,-1}$</td>
</tr>
<tr>
<td></td>
<td>$d_{2,1}$</td>
<td>$M_{n,1,1,2}$</td>
</tr>
<tr>
<td></td>
<td>$d_{-2,1}$</td>
<td>$M_{n,1,1,-2}$</td>
</tr>
<tr>
<td></td>
<td>$d_{3,1}$</td>
<td>$M_{n,1,1,3}$</td>
</tr>
<tr>
<td></td>
<td>$d_{-3,1}$</td>
<td>$M_{n,1,1,-3}$</td>
</tr>
<tr>
<td></td>
<td>$d_{6,1}$</td>
<td>$M_{n,1,1,6}$</td>
</tr>
<tr>
<td></td>
<td>$d_{-6,1}$</td>
<td>$M_{n,1,1,-6}$</td>
</tr>
<tr>
<td></td>
<td>$M = J_{2m}$</td>
<td></td>
</tr>
<tr>
<td>$n = 4k + 1$</td>
<td>$d_{1,1}$</td>
<td>$M = I_{n \times n}$</td>
</tr>
<tr>
<td>$n = 4k + 2$</td>
<td>$d_{1,1}$</td>
<td>$M_1 = I_{n \times n}$</td>
</tr>
<tr>
<td></td>
<td>$d_{1,-1}$</td>
<td>$M_{n,1,1,-1}$</td>
</tr>
<tr>
<td></td>
<td>$d_{-1,1}$</td>
<td>$M_{n,2,3,6}$</td>
</tr>
<tr>
<td></td>
<td>$d_{-1,-1}$</td>
<td>$M_{n,1,1,2}$</td>
</tr>
<tr>
<td></td>
<td>$d_{2,1}$</td>
<td>$M_{n,1,1,-2}$</td>
</tr>
<tr>
<td></td>
<td>$d_{-2,1}$</td>
<td>$M_{n,1,1,3}$</td>
</tr>
<tr>
<td></td>
<td>$d_{3,1}$</td>
<td>$M_{n,1,1,-3}$</td>
</tr>
<tr>
<td></td>
<td>$d_{6,1}$</td>
<td>$M_{n,1,1,6}$</td>
</tr>
<tr>
<td></td>
<td>$d_{-6,1}$</td>
<td>$M_{n,1,1,-6}$</td>
</tr>
<tr>
<td></td>
<td>$M = J_{2m}$</td>
<td></td>
</tr>
<tr>
<td>$n = 4k + 3$</td>
<td>$d_{1,1}$</td>
<td>$M = I_{n \times n}$</td>
</tr>
<tr>
<td></td>
<td>$d_{1,-1}$</td>
<td>$M_{n,2,3,6}$</td>
</tr>
</tbody>
</table>
Chapter 4. Involutions of $\text{SL}(n, k)$

4.5.2 Results for $k = \mathbb{Q}_p \ (p \neq 2)$

The results for $p \neq 2$ are similar in that much of what was said above still holds, except now we have only 8 choices for the dual value $d_{p,c}$ instead of 16 (since there exist only the 4 representatives $\gamma$ of the square-class group instead of 8.) Our choices for $\gamma$ are $\{1, p, Sp, pSp\}$. Again, the choices for $\mathbb{Q}_2$ were each of these plus their negatives.

(1) $n$ even

(a) $n = 4k$: There are 6 classes of involutions. We get 5 semi-congruence classes of symmetric forms, represented by matrices with dual values

$$d_{1,1}, d_{1,-1}, d_{p,1}, \text{ and } d_{Sp,1}, d_{pSp,1}.$$ 

And we still have the class yielded by $M = J_{2m}$.

Involutions coming from the same dual values can be different depending on $p$. Specifically, they depend upon whether or not $-1$ is a square in $(\mathbb{Q}_p^*)^2$.

(i) $-1 \notin (\mathbb{Q}_p^*)^2$: The involutions are $\phi, \text{Inn}_{J_{2m}} \phi$, and $\text{Inn}_M \phi$, where $M = M_{n,\gamma}$ with $\alpha \in \{p, S_p, pS_p\}$ or $M = M_{n,p,Sp,pSp}$. The matrices $M_{n,\gamma}$ correspond to the dual classes $d_{\gamma,1}$, and $M_{n,1,p,p}$ corresponds to the $d_{1,-1}$ class. This is similar to the $\mathbb{Q}_2$ case since $-1$ is not a square in $\mathbb{Q}_2$.

(ii) $-1 \in (\mathbb{Q}_p^*)^2$: We still get 6 involutions, but here the involution coming from the dual class $d_{1,-1}$ is $\text{Inn}_{M_{n,1,p,p}} \phi$.

(b) $n = 4k + 2$: There are also 6 classes of involutions in this case, and again they depend upon whether or not $-1$ is a square in $\mathbb{Q}_p$.

(i) $-1 \notin (\mathbb{Q}_p^*)^2$: In this case we get the formula $c_p(\alpha A) = (\alpha, -D_n)_p c_p(A)$. So for $\det(A) \neq -1$, $(\alpha, -D_n)_p = (\alpha, -\gamma)_p$ and there will be an $\alpha$ such that $(\alpha, -\gamma)_p = -1$ and then $c_p(\alpha A) = -c_p(A)$. This means that $d_{\gamma,1}$ represents a semi-congruent class of bilinear forms to $d_{\gamma,-1}$ for $\gamma \neq -1$.

Since $n$ is even it is true that $\det(\alpha A)$ will be an even power of $\alpha$ times $\det(A)$, which means that multiplication by a scalar cannot change the square-class of the determinant of a matrix in this case. Thereby, it is seen that $d_{\gamma,1,c}$ is not congruent to $d_{\gamma,2,c}$ for $\gamma_1 \neq \gamma_2$. 
Chapter 4. Involutions of \( \text{SL}(n, k) \)

For \( \det(A) = -1 \), the above equation will become

\[
c_p(\alpha A) = (\alpha, 1)_p c_p(A) = c_p(A),
\]

which indicates that the \( d_{-1,1} \) class cannot be semi-congruent to the \( d_{-1,-1} \) class. If \(-1\) is not a square, then \( d_{-1,c} = d_{S_p,c} \) since \(-1\) is in the same square-class as \( S_p \). Therefore, we get different classes of involutions for those coming from the 5 semi-congruence classes represented by \( d_{1,1}, d_{p,1}, d_{S_p,1}, d_{S_p,-1}, \) and \( d_{pS_p,1} \). The corresponding matrix of the form is, respectively, \( I_{n \times n}, M_{n,1,1,p}, M_{n,1,p,S_p}, M_{n,1,1,S_p} \) and \( M_{n,1,1,pS_p} \). We also have the skew-symmetric class with \( M = J_{2m} \). These are 5 of the same involutions as in the \( n = 4k \) class, with the one different involution class coming from the semi-congruence class represented by \( d_{S_p,-1} \).

(ii) \(-1 \in (\mathbb{Q}_p^*)^2\): Here we have that

\[
\det(A) = -1 = 1 \implies c_p(\alpha A) = (\alpha, 1)_p c_p(A) = c_p(A).
\]

Hence, we get the same 5 dual classes as in the \( n = 4k \) case. The 6 involutions obtained are identical to the case \( n = 4k, -1 \in (\mathbb{Q}_p^*)^2 \).

This takes care of the cases where \( n \) is even.

(2) \( n \) is odd:

(a) \( n = 4k + 1 \): Again this depends upon whether or not \(-1\) is a square in \((\mathbb{Q}_p^*)^2\).

(i) \(-1 \notin (\mathbb{Q}_p^*)^2\): As was the case for \( \mathbb{Q}_2 \), we get only one dual class \( d_{1,1} \). The only involution class is that of \( \phi \).

(ii) \(-1 \in (\mathbb{Q}_p^*)^2\): If \(-1\) is a square in \( \mathbb{Q}_p \), then \( d_{1,1} \) and \( d_{1,-1} \) and we have 2 isomorphism classes of involutions \( \phi \) and \( \text{Inn}_{M_{n,p,S_p,S_p}} \phi \).

(b) \( n = 4k + 3 \):

(i) \(-1 \notin (\mathbb{Q}_p^*)^2\): We have 2 dual classes of symmetric forms, \( d_{1,1} \) and \( d_{1,-1} \), which give the 2 involutions \( \phi \) and \( \text{Inn}_{M_{n,p,S_p,S_p}} \phi \).
(ii) $-1 \in (\mathbb{Q}_p^*)^2$: We have the same 2 dual classes and the same 2 involution classes as when $-1$ is a square for $n = 4k + 1$ above.

This completes the isomorphism classes of involutions over the field of $p$-adic numbers, and these last results for $k = \mathbb{Q}_p$ ($p \neq 2$) are illustrated in the table that follows.

We now have a complete, field-independent classification of involutions on SL($n, k$) which come from non-degenerate symmetric or skew-symmetric bilinear forms, which means we have classified all the outer involutions of $G = \text{SL}(n, k)$ over the most important fields $k$ of characteristic not equal to 2.

### 4.6 Classification of Inner Involutions of SL($n, k$)

#### 4.6.1 Inner Involutions of SL($n, k$)

Not all involutions on SL($n, k$) come from bilinear forms. Those that do not are the inner involutions, which means that for a given involution $\theta$, there is a matrix $Y$ such that $\theta(A) = \text{Inn}_Y(A) = Y^{-1}AY \quad \forall A \in \text{SL}(n, k)$. A classification of these was given by Ling Wu in [Wu02], to which we refer the reader for the theorems and proofs. In the following we briefly review these results since they will be needed later on. Our first lemma tells us that this $Y$ may be chosen to have entries in our desired field $k$.

**Lemma 12.** Let $\theta \in \text{Inn}(G)$ and suppose $Y \in \text{GL}(n, \bar{k})$. Then $\text{Inn}_Y$ keeps $G$ invariant (i.e. is an automorphism of $G$) $\iff Y = \alpha B$ for some $\alpha \in \bar{k}$ and $B \in \text{GL}(n, k)$.

If $\text{Inn}_Y$ is an involution, then $\text{Inn}_{Y^2} = \text{Id}$. So Lemma 12 says that $Y^2 = \alpha I_{n \times n}$.

**Lemma 13.** Let $Y \in \text{GL}(n, k)$ with $Y^2 = \alpha I_{n \times n}$. Then

1. If $\alpha = \gamma^2 \in (k^*)^2$, then $Y$ is conjugate to $\gamma I_{n-i,i} \quad i = 0, 1, \ldots, n$.

2. If $\alpha \not\in (k^*)^2$, then $Y$ is conjugate to $\gamma L_{n, \alpha}$. This case occurs only when $n$ is even.

The following lemma comes immediately from the previous lemma and the proof is left to the reader.
Chapter 4. Involutions of SL\((n, k)\)

Table 4.3: Outer Involutions of \(G\) over \(k = \mathbb{Q}_p\) \((p \neq 2)\)

<table>
<thead>
<tr>
<th>(\dim(V))</th>
<th>Dual Value (d_{\alpha,c}) of the Semi-Congruence Class</th>
<th>Matrix (M) such that (\theta(A) = \text{Inn}_M(A^T)^{-1})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(-1 \notin (\mathbb{Q}_p^*)^2)</td>
<td>(d_{1,1})</td>
<td>(M_1 = I_{n \times n})</td>
</tr>
<tr>
<td>(n = 4k)</td>
<td>(d_{1,-1})</td>
<td>(M_{n,p,p,pS_p})</td>
</tr>
<tr>
<td>(n = 4k)</td>
<td>(d_{p,1})</td>
<td>(M_{n,1,1,p})</td>
</tr>
<tr>
<td>(n = 4k)</td>
<td>(d_{S_p,1})</td>
<td>(M_{n,1,1,S_p})</td>
</tr>
<tr>
<td>(n = 4k)</td>
<td>(d_{pS_p,1})</td>
<td>(M_{n,1,1,pS_p})</td>
</tr>
<tr>
<td>(n = 4k + 1)</td>
<td>(d_{1,1})</td>
<td>(M = J_{2m})</td>
</tr>
<tr>
<td>(n = 4k + 2)</td>
<td>(d_{1,-1})</td>
<td>(M_{n,p,p,pS_p})</td>
</tr>
<tr>
<td>(n = 4k + 2)</td>
<td>(d_{p,1})</td>
<td>(M_{n,1,1,p})</td>
</tr>
<tr>
<td>(n = 4k + 2)</td>
<td>(d_{S_p,1})</td>
<td>(M_{n,1,1,S_p})</td>
</tr>
<tr>
<td>(n = 4k + 2)</td>
<td>(d_{pS_p,1})</td>
<td>(M_{n,1,1,pS_p})</td>
</tr>
<tr>
<td>(n = 4k + 3)</td>
<td>(d_{1,1})</td>
<td>(M = I_{n \times n})</td>
</tr>
<tr>
<td>(n = 4k + 3)</td>
<td>(d_{1,-1})</td>
<td>(M_{n,p,p,pS_p})</td>
</tr>
<tr>
<td>(-1 \notin (\mathbb{Q}_p^*)^2)</td>
<td>(d_{1,1})</td>
<td>(M_1 = I_{n \times n})</td>
</tr>
<tr>
<td>(n = 4k)</td>
<td>(d_{1,-1})</td>
<td>(M_{n,1,1,p})</td>
</tr>
<tr>
<td>(n = 4k)</td>
<td>(d_{p,1})</td>
<td>(M_{n,1,1,p})</td>
</tr>
<tr>
<td>(n = 4k)</td>
<td>(d_{S_p,1})</td>
<td>(M_{n,1,1,S_p})</td>
</tr>
<tr>
<td>(n = 4k)</td>
<td>(d_{pS_p,1})</td>
<td>(M_{n,1,1,pS_p})</td>
</tr>
<tr>
<td>(n = 4k + 1)</td>
<td>(d_{1,1})</td>
<td>(M = J_{2m})</td>
</tr>
<tr>
<td>(n = 4k + 2)</td>
<td>(d_{1,-1})</td>
<td>(M_{n,p,p,pS_p})</td>
</tr>
<tr>
<td>(n = 4k + 2)</td>
<td>(d_{p,1})</td>
<td>(M_{n,1,1,p})</td>
</tr>
<tr>
<td>(n = 4k + 2)</td>
<td>(d_{S_p,1})</td>
<td>(M_{n,1,1,S_p})</td>
</tr>
<tr>
<td>(n = 4k + 2)</td>
<td>(d_{pS_p,1})</td>
<td>(M_{n,1,1,pS_p})</td>
</tr>
<tr>
<td>(n = 4k + 3)</td>
<td>(n = 4k + 3)</td>
<td>Same Results as for (-1 \notin (\mathbb{Q}_p^*)^2)</td>
</tr>
</tbody>
</table>
**Chapter 4. Involutions of SL(n, k)**

**Lemma 14.** The isomorphism classes of inner involutions of $G$ are determined by the conjugacy classes of $I_{n-i,i}$ up to a scalar if $n$ is odd, and also by the conjugacy classes up to a scalar of $L_{n,\alpha}$ ($\alpha$ a representative of $(k^*)^2$) if $n$ is even.

### 4.6.2 Theory for Classifying Inner Involutions of $G$

**Remark 8.** Two inner involutions $\text{Inn}_{Y_1}$ and $\text{Inn}_{Y_2}$ are isomorphic $\iff$ $Y_1$ is conjugate to $\alpha Y_2$ for some $\alpha \in \bar{k}$.

**Remark 9.** (1) The matrices $I_{n-i,i}$ and $\alpha I_{n-j,j}$ are conjugate for some $\alpha \in k$ $\iff$:

(a) $\alpha = 1$ and $i = j$, or

(b) $\alpha = -1$ and $j = n - i$.

(2) Suppose $p, q \in \bar{k}^*/(k^*)^2$. Then $L_{n,p}$ is conjugate to $\alpha L_{n,q}$ for some $\alpha \in k$ $\iff$ $\frac{p}{q} \in (k^*)$ (i.e. if $p$ and $q$ are in the same coset).

**Theorem 4.4 (Inner Classification Theorem).** Given an inner involution $\theta = \text{Inn}_Y$ of $\text{SL}(n, k)$, then up to isomorphism $Y$ is:

1. $I_{n-i,i}$  $i = 1, 2, \ldots, \lfloor \frac{n}{2} \rfloor$, or

2. $L_{n,\alpha}$  $\alpha \in (k^*)/(k^*)^2$ with $\alpha \neq 1 \bmod((k^*)^2)$.

**Corollary 3.** The number of isomorphism classes of inner involutions of $\text{SL}(n, k)$ ($n > 2$) is $\frac{n-1}{2}$ if $n$ is odd and $\frac{n}{2} + ||(k^*)/((k^*)^2)|| - 1$ if $n$ is even.

So for odd dimension, the isomorphism classes of inner involutions depends only on $n$. Representative matrices are given by $I_{n-i,i}$  $i = 1, 2, \ldots, \frac{n-1}{2}$.

### 4.6.3 Summary of Inner Classes for $n$ Even

1. $k = \bar{k}$: There are $\frac{n}{2}$ involutions, with representative matrices $I_{n-i,i}$  $i = 1, 2, \ldots, \frac{n}{2}$.
Chapter 4. Involutions of $\text{SL}(n, k)$

(2) $k = \mathbb{R}$: There are $\frac{n^2}{2} + 1$ involutions, represented by $I_{n-i,i}$ ($i = 1, 2, \ldots, \frac{n^2}{2}$) and $L_{n,-1}$.

(3) $k = \mathbb{Q}$: There are $\infty$ many involutions, with matrix $I_{n-i,i}$ ($i = 1, 2, \ldots, \frac{n^2}{2}$) or $L_{n,a}$, where $a$ is any representative $a \neq 1 \mod (k^*)^2$ of the square-class group.

(4) $k = \mathbb{F}_p$ ($p \neq 2$): There are $\frac{n^2}{2} + 1$ involutions up to isomorphism. Representing matrices are $I_{n-i,i}$ ($i = 1, 2, \ldots, \frac{n^2}{2}$) and $L_{n,S_p}$.

(5) $k = \mathbb{Q}_2$: There are $\frac{n^2}{2} + 7$ classes of involutions, given by matrices $I_{n-i,i}$ ($i = 1, 2, \ldots, \frac{n^2}{2}$) and $L_{n,a}$, where $a \in \{-1, 2, -2, 3, -3, 6, -6\}$.

(6) $k = \mathbb{Q}_p$ ($p \neq 2$): There are $\frac{n^2}{2} + 3$ isomorphism classes of inner involutions, with matrix representatives the same as for $\mathbb{Q}_2$ above except that now our choices for $a$ are limited to $\{p, S_p, pS_p\}$.

We conclude with two tables summarizing the isomorphism classes of involutions on $G = \text{SL}(n, k)$. The first table summarizes the inner involutions (i.e. the ones that do not come from symmetric or skew-symmetric bilinear forms), while the second table summarizes the total number of involutions (inner and outer) on $G$ over a given field $k$. 
### Table 4.4: Inner Involution Classes on $G$

<table>
<thead>
<tr>
<th>Field</th>
<th>Number of Inner Involutions</th>
<th>Representative Matrix $Y$ such that $\theta = \text{Inn}_Y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$ odd, $k = \text{any field}$</td>
<td>$\frac{n-1}{2}$</td>
<td>$Y = I_{n-i,i}$ $i = 1, 2, \ldots, \frac{n-1}{2}$</td>
</tr>
<tr>
<td>$n$ even</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$k = \bar{k}$</td>
<td>$\frac{n}{2}$</td>
<td>$Y = I_{n-i,i}$ $i = 1, 2, \ldots, \frac{n}{2}$</td>
</tr>
<tr>
<td>$k = \mathbb{R}$</td>
<td>$\frac{n}{2} + 1$</td>
<td>$Y = I_{n-i,i}$ $i = 1, 2, \ldots, \frac{n}{2}$ $Y = L_{n-1}$</td>
</tr>
<tr>
<td>$k = \mathbb{Q}$</td>
<td>$\infty$</td>
<td>$Y = I_{n-i,i}$ $i = 1, 2, \ldots, \frac{n}{2}$ $Y = L_{n,\alpha}$ $\alpha \neq 1 \mod (\mathbb{Q}^n)^2$</td>
</tr>
<tr>
<td>$k = \mathbb{F}_p$ $p \neq 2$</td>
<td>$\frac{n}{2} + 1$</td>
<td>$Y = I_{n-i,i}$ $i = 1, 2, \ldots, \frac{n}{2}$ $Y = L_{n,S_p}$</td>
</tr>
<tr>
<td>$k = \mathbb{Q}_2$</td>
<td>$\frac{n}{2} + 7$</td>
<td>$Y = I_{n-i,i}$ $i = 1, 2, \ldots, \frac{n}{2}$ $Y = L_{n,\alpha}$ $\alpha \in {-1, \pm 2, \pm 3, \pm 6}$</td>
</tr>
<tr>
<td>$k = \mathbb{Q}_p$ $p \neq 2$</td>
<td>$\frac{n}{2} + 3$</td>
<td>$Y = I_{n-i,i}$ $i = 1, 2, \ldots, \frac{n}{2}$ $Y = L_{n,\alpha}$ $\alpha \in {p, S_p, pS_p}$</td>
</tr>
</tbody>
</table>
### Table 4.5: Summary: Number of Involution Classes of $G$

<table>
<thead>
<tr>
<th>Field</th>
<th>dim($V$)</th>
<th>Number of Outer Involutions</th>
<th>Number of Inner Involutions</th>
<th>Total Number of Involutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k = \bar{k}$</td>
<td>$n$ odd</td>
<td>1</td>
<td>$\frac{n-1}{2}$</td>
<td>$\frac{n+1}{2}$</td>
</tr>
<tr>
<td></td>
<td>$n$ even</td>
<td>2</td>
<td>$\frac{n}{2}$</td>
<td>$\frac{n}{2} + 2$</td>
</tr>
<tr>
<td>$k = \mathbb{R}$</td>
<td>$n$ odd</td>
<td>$\frac{n+1}{2}$</td>
<td>$\frac{n-1}{2}$</td>
<td>$n$</td>
</tr>
<tr>
<td></td>
<td>$n$ even</td>
<td>$\frac{n}{2} + 2$</td>
<td>$\frac{n}{2} + 1$</td>
<td>$n + 3$</td>
</tr>
<tr>
<td>$k = \mathbb{Q}$</td>
<td>$n$ odd</td>
<td>$\infty$</td>
<td>$\frac{n-1}{2}$</td>
<td>$\infty$</td>
</tr>
<tr>
<td></td>
<td>$n$ even</td>
<td>$\infty$</td>
<td>$\infty$</td>
<td>$\infty$</td>
</tr>
<tr>
<td>$k = \mathbb{F}_p$</td>
<td>$n$ odd</td>
<td>2</td>
<td>$\frac{n-1}{2}$</td>
<td>$\frac{n+3}{2}$</td>
</tr>
<tr>
<td>$p \neq 2$</td>
<td>$n$ even</td>
<td>3</td>
<td>$\frac{n}{2} + 1$</td>
<td>$\frac{n}{2} + 4$</td>
</tr>
<tr>
<td>$k = \mathbb{Q}_2$</td>
<td>$n = 4k$</td>
<td>10</td>
<td>$\frac{n}{2} + 7$</td>
<td>$\frac{n}{2} + 17$</td>
</tr>
<tr>
<td></td>
<td>$n = 4k + 1$</td>
<td>1</td>
<td>$\frac{n-1}{2}$</td>
<td>$\frac{n+1}{2}$</td>
</tr>
<tr>
<td></td>
<td>$n = 4k + 2$</td>
<td>10</td>
<td>$\frac{n}{2} + 7$</td>
<td>$\frac{n}{2} + 17$</td>
</tr>
<tr>
<td></td>
<td>$n = 4k + 3$</td>
<td>2</td>
<td>$\frac{n-1}{2}$</td>
<td>$\frac{n+3}{2}$</td>
</tr>
<tr>
<td>$k = \mathbb{Q}_p$</td>
<td>$n = 4k$</td>
<td>6</td>
<td>$\frac{n}{2} + 3$</td>
<td>$\frac{n}{2} + 9$</td>
</tr>
<tr>
<td>$p \neq 2$</td>
<td>$n = 4k + 1$</td>
<td>1</td>
<td>$\frac{n-1}{2}$</td>
<td>$\frac{n+1}{2}$</td>
</tr>
<tr>
<td></td>
<td>$-1 \not\in (\mathbb{Q}_p^*)^2$</td>
<td>2</td>
<td>$\frac{n-1}{2}$</td>
<td>$\frac{n+3}{2}$</td>
</tr>
<tr>
<td></td>
<td>$n = 4k + 2$</td>
<td>6</td>
<td>$\frac{n}{2} + 3$</td>
<td>$\frac{n}{2} + 9$</td>
</tr>
<tr>
<td></td>
<td>$n = 4k + 3$</td>
<td>2</td>
<td>$\frac{n-1}{2}$</td>
<td>$\frac{n+3}{2}$</td>
</tr>
</tbody>
</table>
Chapter 5

Involutions of SO($n$, $k$, $\beta$)

5.1 Meaning of the Term “Orthogonal"

The goal here is to first determine which involutions of $\text{SL}(n, k)$ keep $\text{SO}(n, k, \beta)$ invariant. The typical notation for the orthogonal groups with determinant 1 is merely $\text{SO}(n, k)$ depending on the field $k$. The convention implicit in this notation is that “orthogonal” means that in the bilinear vector space $V = k^n$, two vectors $x$ and $y$ are considered orthogonal by definition if $\beta(x, y) = x_1y_1 + x_2y_2 + \cdots + x_ny_n = 0$, where $\beta$ is the standard dot product, represented by the matrix $I_{n \times n}$.

We see that orthogonal groups consist of matrices which keep the lengths of vectors and the angles between vectors fixed. This means that the length of a vector $x$ defined by $l(x) = \sqrt{\beta(x, x)} = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}$ equals the length $l(A(x)) = \sqrt{\beta(A(x), A(x))}$ for any $A \in G = \text{SO}(n, k)$. This is why the rotation and reflection operations comprise the orthogonal groups of matrices, with only the rotations having the required determinant 1 while the reflections are represented by matrices with determinant $-1$ due to the fact that they are orientation-reversing rather than preserving the orientation between two vectors. These each preserve length as defined in the intuitive manner above.

In fact, the orthogonal matrices form a group $\text{O}(n, k)$ consisting of only two cosets under the surjection $\pi : O \rightarrow \{1, -1\}$ defined by $\pi(A) = \text{det}(A)$ ([Art91]). Not only do they preserve length, they also preserve angles between vectors. Since “orthogonal” means
"perpendicular," the images of two orthogonal vectors will still be orthogonal after the operation of the group element, so it is seen that $\beta(A(x), A(y)) = 0$. This is the definition in the general case.

**Definition 12 (Orthogonal).** Two vectors $x, y \in V = k^n$ are said to be orthogonal with respect to the bilinear form $\beta$ if $\beta(x, y) = 0$.

Consider, however, a different symmetric bilinear form on $V = k^n$:

**Example 5.1.** For any 2 vectors $x$ and $y$ in $V$ define a bilinear form on $V$ by $\beta(x, y) = \det(A = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix})$. Then, 2 vectors are orthogonal if and only if $\det(A) = 0$, which means if and only if the vectors $x$ and $y$ are parallel! [Szy97]

The symmetric form in the example above will not be studied in depth here because it is a degenerate form represented by a singular matrix, but it gives us an idea of how generalizing our notion of orthogonality to spaces with different bilinear forms can be not only less than intuitive, it can be totally counter-intuitive. It is possible then that the matrices comprising the orthogonal group where the term is understood to relate to a general bilinear form may be quite different than our well-known groups $O(n, k)$ and $SO(n, k)$. For this reason, we will use the notation $SO(n, k, \beta)$ to indicate that our results will hold for a general non-degenerate symmetric form $\beta$ on $V = k^n$.

### 5.2 Matrices $A$ Such That $\text{Inn}_A = \text{Id}$

Suppose that the inner automorphism given by conjugation by a matrix $A$ is the identity element of the automorphism group. What does this require of the structure of the matrix $A$? Recall that when we focused on automorphisms of $\text{SL}(n, k)$ it was required that the matrix be a scalar multiple of $I_{n \times n}$. The following theorem shows the not at all trivial result that the same holds for a matrix $A$ whose conjugation is the identity on the special orthogonal subgroup:
Chapter 5. Involutions of $SO(n, k, \beta)$

**Theorem 5.1.** Let $\beta$ be a non degenerate symmetric bilinear form on a vector space $V = k^n$, $G = SO(n, k, \beta)$ and let $A \in GL(n, \bar{k})$. The inner automorphism $\text{Inn}_A$ is the identity $\text{Id}$ automorphism on $\bar{G} \iff A = \alpha I_{n \times n}$ for some scalar $\alpha \in \bar{k}^*$.

Before giving the formal proof, let us illustrate the method and its effectiveness by looking at examples for differing dimension $n$ of the bilinear space to illustrate the idea of the proof. Then the results indicated by the examples will be shown with formulas which work for general dimension $n$.

The idea of the proof is this: We will start by showing that for the entries $a_{i,j}$ of the matrix $A$ such that $\text{Inn}_A = \text{Id}$, it is necessary that $a_{i,i} = a_{j,j}$ $\forall i, j \in \{1, 2, \ldots, n\}$. We will also show that $a_{i,j} = 0$ when $i \neq j$. This will be done by taking considering the action of the matrix $A \in GL(n, \bar{k})$ and well-chosen entries $X \in \bar{G}$. We will first illustrate the result with the following examples of an odd and even rank case.

**Example 5.2 ($n = 3$).** Our bilinear form $\beta$ is represented by the symmetric matrix

\[
M_3 = \begin{pmatrix}
1 & 0 & 0 \\
0 & m_2 & 0 \\
0 & 0 & m_3
\end{pmatrix}.
\]

For a matrix $X$ to be in $SO(3, \bar{k}, \beta)$ it is necessary that $\theta_{M_3}(X) = M_3^{-1}(X^T)^{-1}M_3 = (X)$ since the orthogonal group of the form is defined to be the fixed-point group of the corresponding involution. It is also necessary that $X$ has determinant 1 to be in $SO(3, \bar{k}, \beta)$ rather than merely in the larger group $O(3, \bar{k}, \beta)$. We let

\[
X_{3,1} = \begin{pmatrix}
0 & \sqrt{m_2} & 0 \\
\frac{-1}{\sqrt{m_2}} & 0 & 0 \\
0 & 0 & 1
\end{pmatrix}
\]

and

\[
X_{3,2} = \begin{pmatrix}
1 & 0 & 0 \\
0 & 0 & \frac{\sqrt{m_3}}{\sqrt{m_2}} \\
0 & \frac{-\sqrt{m_3}}{\sqrt{m_2}} & 0
\end{pmatrix}.
\]
We first show that the defined matrices $X$ are in $\text{SO}(3, \tilde{k}, \beta)$. Clearly $\det(X_{3,1}) = \det(X_{3,2}) = 1$ and

$$
\theta_{M_3}(X_{3,1}) = \begin{pmatrix}
0 & \sqrt{m_2} & 0 \\
-1 & 0 & 0 \\
0 & 0 & 1
\end{pmatrix}
$$

$$
\theta_{M_3}(X_{3,2}) = \begin{pmatrix}
1 & 0 & 0 \\
0 & 0 & \sqrt{m_3} \\
0 & -\sqrt{m_3} & 0
\end{pmatrix}.
$$

So we see that the matrices $X_{3,i}$ are in $\tilde{G}$ where $i = 1, 2$.

Since $\text{Inn}_A = \text{Id}$ on $\tilde{G}$, we have that $A^{-1}X_{3,i}A = X_{3,i}$, or equivalently

$$
X_{3,i}A = AX_{3,i}.
$$

We call the left side of this equation $L_{3,i}$ and the right side $R_{3,i}$ and denote by equation $[j, k]$ the equation obtained by equating the $[j, k]$ entries of each of the matrix products for each $i = 1, 2$.

$$
R_{3,1} := A_3X_{3,1} = \begin{pmatrix}
\frac{-a_{12}}{\sqrt{m_2}} & a_{11}\sqrt{m_2} & a_{13} \\
\frac{-a_{22}}{\sqrt{m_2}} & a_{21}\sqrt{m_2} & a_{23} \\
\frac{-a_{32}}{\sqrt{m_2}} & a_{31}\sqrt{m_2} & a_{33}
\end{pmatrix}
$$

$$
L_{3,1} := X_{3,1}A_3 = \begin{pmatrix}
a_{21}\sqrt{m_2} & a_{22}\sqrt{m_2} & a_{23}\sqrt{m_2} \\
\frac{-a_{11}}{\sqrt{m_2}} & \frac{-a_{12}}{\sqrt{m_2}} & \frac{-a_{13}}{\sqrt{m_2}} \\
a_{31} & a_{32} & a_{33}
\end{pmatrix}
$$

Either equation $[1, 2]$ or equation $[2, 1]$ guarantee that $a_{11} = a_{22}$. Also, equation $[1, 3]$ and equation $[2, 3]$ imply

$$
\sqrt{m_2}a_{23} = a_{13} = -a_{13}
$$
so that \( a_{13} = a_{23} = 0 \). Similarly, equation [3, 1] and equation [3, 2] combine to force

\[
\sqrt{m_2}a_{31} = a_{32} = -a_{32}
\]

so that \( a_{31} = a_{32} = 0 \).

We still need \( a_{22} = a_{33}, a_{21} = 0, \) and \( a_{12} = 0 \). To show this we will use the results for \( X_{3,2}, \) noting that \( X_{3,2}A_3 = A_3X_{3,2} \) and proceeding as with \( X_{3,1} \) and its resulting matrix products.

\[
L_{3,2} := X_{3,2}A_3 = \begin{pmatrix}
  a_{11} & -a_{13}\sqrt{m_2}/\sqrt{m_3} & a_{12}\sqrt{m_3}/\sqrt{m_2} \\
  -a_{23}\sqrt{m_2}/\sqrt{m_3} & a_{22}\sqrt{m_3}/\sqrt{m_2} \\
  -a_{33}\sqrt{m_2}/\sqrt{m_3} & a_{32}\sqrt{m_3}/\sqrt{m_2}
\end{pmatrix}
\]

\[
R_{3,2} := A_3X_{3,2} = \begin{pmatrix}
  a_{11} & a_{12} & a_{13} \\
  a_{31}\sqrt{m_3}/\sqrt{m_2} & a_{32}\sqrt{m_3}/\sqrt{m_2} & a_{33}\sqrt{m_3}/\sqrt{m_2} \\
  -a_{21}\sqrt{m_2}/\sqrt{m_3} & -a_{22}\sqrt{m_2}/\sqrt{m_3} & -a_{23}\sqrt{m_2}/\sqrt{m_3}
\end{pmatrix}
\]

Either equation [2, 3] or equation [3, 2] will give the result \( a_{22} = a_{33} \); from our earlier result that \( a_{11} = a_{22} \), we now know that the diagonal entries are all equal. We use equations [2, 1] and [3, 1] to get

\[
\frac{\sqrt{m_2}}{\sqrt{m_3}}a_{31} = a_{21} = -a_{21}.
\]

This forces \( a_{21} = a_{31} = 0 \). Lastly, we use equations [1, 2] and [1, 3] to obtain

\[
\frac{\sqrt{m_2}}{\sqrt{m_3}}a_{13} = a_{12} = -a_{12}
\]

so that \( a_{12} = a_{13} = 0 \).

So we see the idea for \( n = 3 \). Setting \( X_{3,i}A_3 = A_3X_{3,i} \) we get \( a_{i,i} = a_{i+1,i+1} \) from either equation \([i, i + 1]\) or equation \([i + 1, i]\), \( i = 1, \ldots, 2 \) and likely for \( i = 1, \ldots, n - 1 \) in general). This proves all the diagonal entries are equal. For \( i = 1 \) we use equation \([1, 3]\) and \([2, 3]\) to show \( a_{13} = a_{23} = 0 \) and equations \([3, 1]\) and \([3, 2]\) to show the same of \( a_{31} = a_{32} = 0 \). When \( i = 2 \), we obtained this information on \( a_{12} \) and \( a_{13} \) from equations \([1, 2]\) and \([1, 3]\) and similarly for \( a_{21} \) and \( a_{31} \).
The pattern for showing the non-diagonal elements of $A_3$ to be zero seems to be this: Given the equations $[i, j]$ and $[i + 1, j]$ with $j \neq i, i + 1$ give $a_{i,j} = a_{i+1,j} = 0$. Equations $[j, i]$ and $[j, i + 1]$ with $j \neq i, i + 1$ give $a_{j,i} = a_{j,i+1} = 0$. Since $i$ ranges from 1 to 2 this will cover all the entries $a_{i,j}$, resulting in $a_{j,j} = a_{k,k}$, and $a_{j,k} = 0 \ \forall \ j \neq k$. Therefore, $A = \alpha I_{3 \times 3}$, $\alpha \in \bar{k}$.

Example 5.3 ($n = 4$). We will carry out a similar process for $n = 4$. Here we will need 3 matrices $X \in \text{SO}(4, k, \beta)$ instead of 2. Let

$$M_4 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & m_2 & 0 & 0 \\ 0 & 0 & m_3 & 0 \\ 0 & 0 & 0 & m_4 \end{pmatrix}$$

and

$$X_{4,1} := \begin{pmatrix} 0 & \sqrt{m_2} & 0 & 0 \\ \frac{-1}{\sqrt{m_2}} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then $\det(X_{4,1}) = 1$ and

$$\theta_{M_4}(X_{4,1}) = \begin{pmatrix} 0 & \sqrt{m_2} & 0 & 0 \\ \frac{-1}{\sqrt{m_2}} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

This shows that $X_{4,1}$ is in $\bar{G} = \text{SO}(4, \bar{k}, \beta)$. Let

$$X_{4,2} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & \frac{\sqrt{m_3}}{\sqrt{m_2}} & 0 \\ 0 & \frac{-\sqrt{m_2}}{\sqrt{m_3}} & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$
Then $\det(X_{4,2}) = 1$ and

\[
\theta_{M_4}(X_{4,2}) = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & \sqrt{m_3} & 0 \\
0 & -\sqrt{m_2} & 0 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}.
\]

This shows that $X_{4,2}$ is in $\tilde{G} = \text{SO}(4, \tilde{k}, \beta)$. Let

\[
X_{4,3} := \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & \sqrt{m_4} \\
0 & 0 & -\sqrt{m_3} & 0
\end{pmatrix}.
\]

Then $\det(X_{4,3}) = 1$ and

\[
\theta_{M_4}(X_{4,3}) = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & \sqrt{m_4} \\
0 & 0 & -\sqrt{m_3} & 0
\end{pmatrix}.
\]

This shows us that $X_{4,i} \in \tilde{G}$ for each $i = 1, \ldots, n - 1$ (so here, for each $i = 1, \ldots, 3$). Now let’s focus on the fact that $X_{4,1}A_4 = A_4X_{4,1}$. As before, we define the matrices $L_{4,i} = X_{4,i}A_4$ and $R_{4,i} = A_4X_{4,i}$ for each $i$, and again we define by equation $[j, k]$ the equation resulting from equating the $[j, k]$ entries of each of these.

\[
R_{4,1} := A_4X_{4,1} = \begin{pmatrix}
-\frac{a_{12}}{\sqrt{m_2}} & a_{11} \sqrt{m_2} & a_{13} & a_{14} \\
-\frac{a_{22}}{\sqrt{m_2}} & a_{21} \sqrt{m_2} & a_{23} & a_{24} \\
-\frac{a_{32}}{\sqrt{m_2}} & a_{31} \sqrt{m_2} & a_{33} & a_{34} \\
-\frac{a_{42}}{\sqrt{m_2}} & a_{41} \sqrt{m_2} & a_{43} & a_{44}
\end{pmatrix}
\]
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

$L_{4,1} := X_{4,1} A_4 = \begin{pmatrix}
  a_{21}\sqrt{m_2} & a_{22}\sqrt{m_2} & a_{23}\sqrt{m_2} & a_{24}\sqrt{m_2} \\
  \frac{-a_{11}}{\sqrt{m_2}} & \frac{-a_{12}}{\sqrt{m_2}} & \frac{-a_{13}}{\sqrt{m_2}} & \frac{-a_{14}}{\sqrt{m_2}} \\
  a_{31} & a_{32} & a_{33} & a_{34} \\
  a_{41} & a_{42} & a_{43} & a_{44}
\end{pmatrix}$

As with the case where $n = 3$, $i = 1$ equation [1, 2] or equation [2, 1] yield $a_{11} = a_{22}$.

Equation [1, 3] coupled with [2, 3] implies

$\sqrt{m_2}a_{23} = a_{13} = -a_{13}, \quad \Rightarrow \quad a_{13} = a_{23} = 0.$

In a similar fashion, we also get zero for the $A$ entries corresponding to equation pairs [1, 4] and [2, 4] (so that $a_{14} = a_{24} = 0$), [3, 1] and [3, 2], and [4, 1] paired with [4, 2].

As was the case for $n = 3$, it is seen that for $i = 1$ we still have that for $i = 1, 2, \ldots, n - 1$, the equations coming from $X_{n,i}$ give

$\sqrt{m_i}a_{i+1, j} = a_{i, j} = -a_{i, j}.$

from equations $[i, j]$ and $[i + 1, j]$ and

$\sqrt{m_i}a_{j, i+1} = a_{j, i} = -a_{j, i}.$

from equations $[j, i]$ and $[j, i + 1]$ when $j \neq i, i + 1$, which forces $a_{i, j} = a_{i+1, j} = a_{j, i} = a_{j, i+1} = 0$. Additionally, either equation $[i, i + 1]$ or equation $[i + 1, i]$ shows the result $a_{i, i} = a_{i+1, i+1}$. Let’s see if this pattern continues with the results for $X_{4,2}$ and $X_{4,3}$.

Consider now the case for $i = 2$ and the resulting equations:

$R_{4,2} := A_4 X_{4,2} = \begin{pmatrix}
  a_{11} & -a_{13}\sqrt{m_2} & a_{12}\sqrt{m_3} & a_{14} \\
  \frac{-a_{21}}{\sqrt{m_3}} & \frac{-a_{23}}{\sqrt{m_2}} & \frac{-a_{22}}{\sqrt{m_3}} & \frac{-a_{24}}{\sqrt{m_2}} \\
  a_{31} & a_{32} & a_{33} & a_{34} \\
  a_{41} & a_{42} & a_{43} & a_{44}
\end{pmatrix}$
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

$L_{4,2} := X_{4,2}A_4 = \left( \begin{array}{cccc}
    a_{11} & a_{12} & a_{13} & a_{14} \\
    a_{31} \sqrt{m_3} & a_{32} \sqrt{m_3} & a_{33} \sqrt{m_3} & a_{34} \sqrt{m_3} \\
    -a_{21} \sqrt{m_2} & -a_{22} \sqrt{m_2} & -a_{23} \sqrt{m_2} & -a_{24} \sqrt{m_2} \\
    \sqrt{m_3} & \sqrt{m_3} & \sqrt{m_3} & \sqrt{m_3} \\
    a_{41} & a_{42} & a_{43} & a_{44}
\end{array} \right)$

Equation $[2, 3]$ or $[3, 2]$ requires $a_{22} = a_{33}$. From equations $[2, j]$ and $[3, j]$ where $j \neq 2, 3$ we get $a_{2j} = a_{3j} = 0$ (recall that the $m_i$ entries of the matrix of the form are nonzero with the assumption of a non-degenerate form); $[j, 2]$ together with $[j, 3]$ imply $a_{j,2} = a_{j,3} = 0$.

Summarizing our knowledge of $A$, we had from $i = 1$ (using $X_{4,1}$ results) that Equation $[2, 3]$ or $[3, 2]$ requires $a_{22} = a_{33}$. From equations $[2, j]$ and $[3, j]$ where $j \neq 2, 3$ we get $a_{2j} = a_{3j} = 0$ (recall that the $m_i$ entries of the matrix of the form are nonzero with the assumption of a non-degenerate form); $[j, 2]$ together with $[j, 3]$ implies $a_{j,2} = a_{j,3} = 0$.

Summarizing our knowledge of $A$, we had from $i = 1$ (using $X_{4,1}$ results) that

\begin{align*}
a_{13} &= a_{23} = 0 & \text{from } [1, 3] \text{ and } [2, 3] \\
a_{14} &= a_{24} = 0 & \text{from } [1, 4] \text{ and } [2, 4] \\
a_{31} &= a_{32} = 0 & \text{from } [3, 1] \text{ and } [3, 2] \\
a_{41} &= a_{42} = 0 & \text{from } [4, 1] \text{ and } [4, 2] \\
a_{11} &= a_{22} & \text{from } [1, 2] \text{ and } [2, 1]
\end{align*}

The equations stemming from $i = 2$ resulted in

\begin{align*}
a_{21} &= a_{31} = 0 & \text{from } [2, 1] \text{ and } [3, 1] \\
a_{24} &= a_{34} = 0 & \text{from } [2, 4] \text{ and } [3, 4] \\
a_{12} &= a_{13} = 0 & \text{from } [1, 2] \text{ and } [1, 3] \\
a_{42} &= a_{43} = 0 & \text{from } [4, 2] \text{ and } [4, 3] \\
a_{22} &= a_{33} & \text{from } [2, 3] \text{ and } [3, 2]
\end{align*}
Chapter 5. Involutions of SO(n, k, β) 70

Note that these 2 groups of results combine to yield $a_{11} = a_{22} = a_{33}$.

The only thing remaining to show to prove that $A_4 = aI_{4\times4}$ is that $a_{44}$ is equal to any of the other 3 diagonal elements. It is for this single result that we need the third matrix $X_{4,3}$.

$$R_{4,3} := A_4 X_{4,3} = \begin{pmatrix} a_{11} & a_{12} & -a_{14} \sqrt{m_3} & a_{13} \sqrt{m_3} \\ a_{21} & a_{22} & -a_{24} \sqrt{m_3} & a_{23} \sqrt{m_3} \\ a_{31} & a_{32} & -a_{34} \sqrt{m_3} & a_{33} \sqrt{m_3} \\ a_{41} & a_{42} & -a_{44} \sqrt{m_3} & a_{43} \sqrt{m_3} \end{pmatrix}$$

$$L_{4,3} := X_{4,3} A_4 = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} \sqrt{m_3} & a_{32} \sqrt{m_3} & a_{33} \sqrt{m_3} & a_{34} \sqrt{m_3} \\ -a_{31} \sqrt{m_3} & -a_{32} \sqrt{m_3} & -a_{33} \sqrt{m_3} & -a_{34} \sqrt{m_3} \end{pmatrix}$$

Our last necessary step in showing $A_4 = aI_{4\times4}$ is showing $a_{33} = a_{44}$, which the above computation shows will come from either equation $[4, 3]$ or equation $[3, 4]$. Therefore, $A_4 = aI_{4\times4}$.

Before trying to generalize for any $i$ and $n$ simultaneously, we will keep $n = 4$ and substitute $i = 1, 2, 3$ into the above groupings of equations. Then we will see whether our equations still hold for $i = 2, 3$.

The results from above for $i = 1$ with $i$ substituted into the equations become:

- $a_{i,3} = a_{i+1,3} = 0$ from $[i, 3]$ and $[i + 1, 3]$
- $a_{i,4} = a_{i+1,4} = 0$ from $[i, 4]$ and $[i + 1, 4]$
- $(i.e. a_{i,j} = a_{i+1,j} = 0$ from $[i, j]$ and $[i + 1, j]$ $j \neq i, i + 1)$
- $a_{3i} = a_{3i+1} = 0$ from $[3, i]$ and $[3, i + 1]$
- $a_{4i} = a_{4i+1} = 0$ from $[4, i]$ and $[4, i + 1]$
- $(i.e. a_{j,i} = a_{j,i+1} = 0$ from $[j, i]$ and $[j, i + 1]$ $j \neq i, i + 1)$
- $a_{i,i} = a_{i+1,i+1} = 0$ from $[i, i + 1]$ or $[i + 1, i]$
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

The results from above for $i = 2$ with $i = 1$ substituted into the equations become:

\[
\begin{align*}
    a_{i,1} &= a_{i+1,1} = 0 & \text{from} & \ [i, 1] \quad \text{and} \quad [i + 1, 1] \\
    a_{i,4} &= a_{i+1,4} = 0 & \text{from} & \ [i, 4] \quad \text{and} \quad [i + 1, 4] \\
    (\text{i.e.} a_{i,j} &= a_{i+1,j} = 0 & \text{from} & \ [i, j] \quad \text{and} \quad [i + 1, j] \\
    a_{1i} &= a_{1i+1} = 0 & \text{from} & \ [1, i] \quad \text{and} \quad [1, i + 1] \\
    a_{4i} &= a_{4i+1} = 0 & \text{from} & \ [4, i] \quad \text{and} \quad [4, i + 1] \\
    (\text{i.e.} a_{j,i} &= a_{j,i+1} = 0 & \text{from} & \ [j, i] \quad \text{and} \quad [j, i + 1] \\
    a_{i,i} &= a_{i+1,i+1} & \text{from} & \ [i, i + 1] \quad \text{and} \quad [i + 1, i]
\end{align*}
\]

We’ve already seen that $a_{i,i} = a_{i+1,i+1}$ for $i = 3$ also from the earlier illustration using the matrix $X_{4,3}$. It is clear from a glance at $R_{4,3}$ and $L_{4,3}$ that substituting $i = 3$ would also result in the above formulas in terms of $i$ and $i + 1$.

In this fashion we can see that when analyzing the $n = 3$ case to predict formulas obtained by abstracting to any dimension $n$ and any $i = 1, 2, \ldots, n - 1$ our primary formulas hold true. The combination of these examples of the action on $A_n$ on $\bar{G}$ have proven the result for $n = 3$ and $n = 4$. We will always need $n - 1$ matrices $X_{n,i}$ to get these results, and the pattern is independent of the dimension. So here is the formal proof, whose steps are clear with the illumination of the preceding paragraphs and computations.

**Proof of Theorem 5.1.** Suppose $n > 2$. Given a field $k$ with char $k \neq 2$ and a symmetric bilinear form $\beta$ on $V = k^n$, let $M_n$ be the matrix of the form and $\text{SO}(n, k, \beta)$ be the fixed point group of the involution coming from $\beta$. Suppose that $A_n$ is a matrix such that $\text{Inn}_{A_n} = \text{Id}$ on $\bar{G} = \text{SO}(n, \bar{k}, \beta)$. The task at hand is to show that $A_n$ must be a scalar multiply of the identity $n \times n$ matrix for some scalar in $\bar{k}$. So we will show $a_{j,k} = 0 \ \text{for} \ j \neq k$ and $a_{j,j} = a_{k,k} \ \forall j, k$.

For $i = 1, 2, \ldots, n - 1$ denote by $Y_{2,i}$ the $2 \times 2$ matrices

\[
Y_{2,i} := \begin{pmatrix}
0 & \sqrt{m_{i+1}} \\
-\sqrt{m_i} & 0
\end{pmatrix}
\]
Chapter 5. Involutions of SO($n, k, \beta$)

Note that $\det(Y_{2,i}) = 1$. Now use each of these matrices $Y_{2,i}$ to construct $n - 1$ matrices $X_{n,i}$ having the following form:

$$X_{n,i} := \begin{pmatrix} I_{i-1,i-1} & \cdots & 0 \\ \vdots & Y_{2,i} & \vdots \\ 0 & \cdots & I_{n-i-1 \times n-i-1} \end{pmatrix}$$

We remark that $\det(X_{n,i}) = \det(Y_{2,i}) = 1$ and that $m_1$ is assumed to be one to make things somewhat simpler. To see that $X_{n,i}$ is in $\bar{G}$ first let us denote by $M_{2,i}$ the $2 \times 2$ matrix

$$\begin{pmatrix} m_i & 0 \\ 0 & m_{i+1} \end{pmatrix}$$

Then

$$\theta_{M_n}(X_{n,i}) = M_n^{-1}(X_{n,i}^T)^{-1}M_n$$

$$= \begin{pmatrix} I_{i-1 \times i-1} & 0 \cdots 0 & 0 \\ 0 & 0 \vdots M_{2,i} \vdots & 0 \\ 0 & 0 \cdots 0 & I_{n-i-1 \times n-i-1} \end{pmatrix} \begin{pmatrix} I_{i-1,i-1} & 0 \cdots 0 & 0 \\ 0 & 0 \vdots (Y_{2,i}^T)^{-1} \vdots & 0 \\ 0 & 0 \cdots 0 & I_{n-i-1 \times n-i-1} \end{pmatrix}$$

$$\ast \begin{pmatrix} I_{i-1 \times i-1} & 0 \cdots 0 & 0 \\ 0 & 0 \vdots M_{2,i} \vdots & 0 \\ 0 & 0 \cdots 0 & I_{n-i-1 \times n-i-1} \end{pmatrix} \begin{pmatrix} I_{i-1,i-1} & 0 \cdots 0 & 0 \\ 0 & 0 \vdots M_{2,i}^{-1}(Y_{2,i}^T)^{-1}M_{2,i} \vdots & 0 \\ 0 & 0 \cdots 0 & I_{n-i-1 \times n-i-1} \end{pmatrix}$$

$$= \begin{pmatrix} I_{i-1 \times i-1} & 0 \cdots 0 & 0 \\ 0 & 0 \vdots M_{2,i}^{-1}(Y_{2,i}^T)^{-1}M_{2,i} \vdots & 0 \\ 0 & 0 \cdots 0 & I_{n-i-1 \times n-i-1} \end{pmatrix}$$
\[
\begin{pmatrix}
I_{i-1,i-1} & \ldots & 0 \\
\vdots & Y_{2,i} & \vdots \\
0 & \ldots & I_{n-i-1 \times n-i-1}
\end{pmatrix}
= X_{n,i}.
\]

Hence, it is clear that \(X_{n,i}\) is in \(\bar{G}\). The inner automorphism \(\text{Inn}_{A_n}\) is the identity operator on \(\bar{G}\) only if \(A_n^{-1}X_{n,i}A_n\), or equivalently, \(X_{n,i}A_n = A_nX_{n,i}\). As in the illustration of the idea of the proof, we call the left side of this equality \(L_{n,i}\) and the right side \(R_{n,i}\) and the equations resulting from equating each of the \([k, j]\) elements equation \([k, j]\).

In general, once we fix an \(i = 1, 2, \ldots, n-1\) we have that combining equations \([i, j]\) and \([i+1, j]\) for \(j \neq i, i+1\) gives the results
\[
\frac{\sqrt{m_i}}{\sqrt{m_{i+1}}}a_{i+1,j} = a_{i,j} = -a_{i,j} = \frac{-a_{i,j}}{a_{i+1,j}}
\]
and
\[
\frac{\sqrt{m_{i+1}}}{\sqrt{m_i}}a_{i,j} = a_{i+1,j} = -a_{i+1,j}.
\]
Therefore \(a_{i,j} = a_{i+1,j} = 0\) for \(j \neq i, i+1\).

Additionally, combining equations \([j, i]\) and \([j, i+1]\) for \(j \neq i, i+1\) will show that
\[
\frac{\sqrt{m_j}}{\sqrt{m_{i+1}}}a_{j,i+1} = a_{j,i} = -a_{j,i}
\]
and
\[
\frac{\sqrt{m_{i+1}}}{\sqrt{m_i}}a_{j,i} = a_{j,i+1} = -a_{j,i+1}.
\]
Therefore \(a_{j,i} = a_{j,i+1} = 0\) for \(j \neq i, i+1\). Since \(i\) runs from 1 to \(n-1\), this will show that every entry of \(A_n\) not on the diagonal is zero.

Lastly, each set of equations for a given \(i\) ensures that \(a_{i,i} = a_{i+1,i+1}\). The accepted values of \(i\) allow for us to say safely that \(a_{j,j} = a_{k,k}\) \(\forall j, k = 1, \ldots, n\). Call any diagonal element \(\alpha\) and we achieve the desired goal of showing that \(A_n\) must be \(\alpha I_{n \times n}\) for some \(\alpha \in \mathbb{k}\). \(\square\)
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

5.3 Matrices $A$ Such That $\text{Inn}_A$ is an Automorphism of $G$

5.3.1 Characterization Theorem

Given the amount of work needed to show that $A_n = \alpha I_{n \times n}$ when $\text{Inn}_A = \text{Id}$ on $\tilde{G}$ it makes sense to ask how this helps us classify involutions of $G$. The main use of this result is that it will be the main tool to prove the Characterization Theorem.

**Remark 10.** When $k$ is algebraically closed and $n$ is odd, we have that $\text{Aut} \ G = \text{Inn} \ G$.

This means that every automorphism (and consequently every involution) of $\tilde{G} = \text{SO}(n, \bar{k}, \beta)$ is inner when $n$ is odd. Not only can an automorphism of $\tilde{G}$ be written as a conjugation by a matrix with entries necessarily in $\bar{k}$, it can be shown to be a conjugation by a matrix $A_n$ which happens to lie in $\tilde{G}$, not just in $\text{SL}(n, \bar{k})$.

But what does this say about automorphisms – and more specifically, about involutions – on $G = \text{SO}(n, k, \beta)$ for a general field $k$ and $n$ odd? The ideal situation would be that these automorphisms are all inner, which is to say that they are conjugations by a matrix $A_n$ which are not only fixed by the action of $\theta_M$ for a given symmetric bilinear form represented by $M$ but have all their entries residing in $k$, not simply in $\bar{k}$. As will be shown in this section, any automorphism on a matrix group defined over $k = \bar{k}, \mathbb{R}, \mathbb{F}_p$ or $\mathbb{Q}_p$ which is a conjugation (all those for $n$ even which are conjugations and every single automorphism of $G$ when $n$ is odd) is proven to be inner when $n$ is odd and $n \geq 5$ and “almost” inner when $n$ is even and $n \geq 4$ in the sense that we will be able to take $A_n \in \text{O}(n, k, \beta)$. We note the following:

**Lemma 15.** (1) Suppose $k = \bar{k}, \mathbb{R}, \mathbb{F}_p$. Then given a non-degenerate bilinear symmetric form $\beta$ on $V = k^n$ with $n > 2$ with $M$ the matrix representing $\beta$, we may assume $M = \text{diag}(1, 1, m_3, m_4, \ldots, m_n)$.

(2) If $k = \mathbb{Q}_p$ we may always assume $M = \text{diag}(1, 1, m_3, m_4, \ldots, m_n)$ when $n > 4$ and assume this form for $M$ when $n = 3$ or $4$ with the 2 exceptions when $\beta$ has matrix representative $M_{3,p, S_p, pS_p}$ or $M_{4,p, S_p, pS_p}$. The case where $M = M_{4,p, S_p, pS_p}$ occurs only for fields $\mathbb{Q}_p$ where $-1$ is not a square.
(3) If \( k = \mathbb{Q}_2 \) we may always assume \( M = \text{diag}(1, 1, m_3, m_4, \ldots, m_n) \) when \( n > 4 \) and assume this form for \( M \) when \( n = 3 \) or \( 4 \) with the 2 exceptions when \( \beta \) has matrix representative \( M_{3,2,3,6} \) or \( M_{4,2,3,6} \).

**Proof.** Our choices for symmetric bilinear forms are those giving the semi-congruence classes of diagonal matrices referred to throughout this text. Referring to Table 4.1, Table 4.2, and Table 4.3 we find these results to be the case. \( \square \)

**Theorem 5.2 (Characterization Theorem).** Suppose \( \beta \) is a non-degenerate symmetric bilinear form with matrix \( M \) over \( V = k^n \) where \( \text{char } k \neq 2 \) and \( \bar{G} = \text{SO}(n, \bar{k}, \beta) \), where \( n > 2 \).

(1) If \( A \in \text{GL}(n, \bar{k}) \), then the automorphism \( \text{Inn}_A \) of \( \text{GL}(n, \bar{k}) \) keeps \( \bar{G} \) invariant (i.e. is an automorphism of \( \bar{G} \) as well) \( \iff \ A = \alpha \hat{A}, \) where \( \alpha \in \bar{k} \) and

(a) \( \hat{A} \in \bar{G} \) if \( n \) is odd,

(b) \( \hat{A} \in \bar{G} \) or \( \hat{A} \in \text{O}(n, \bar{k}, \beta) \) and \( \det(\hat{A}) = -1 \) if \( n \) is even.

(2) If \( A \) is in \( \bar{G} \), or if \( n \) is even and \( \text{O}(n, \bar{k}, \beta) \), then the inner automorphism \( \text{Inn}_A \) of \( \bar{G} \) keeps \( G \) invariant (i.e. is an automorphism of \( G \) as well) \( \iff \ A = \alpha \hat{A} \) for some \( \alpha \in \bar{k} \) and

(a) \( \hat{A} \in G \) if \( n \) is odd,

(b) \( \hat{A} \in G \) or \( \hat{A} \in \text{O}(n, k, \beta) \) and \( \det(\hat{A}) = -1 \) if \( n \) is even.

**Remark 11.** By Lemma 15 we can assume that the matrix \( M \) satisfies the condition in Theorem 5.2(2) for \( k = \bar{k}, \mathbb{R}, \mathbb{F}_p \) and \( k = \mathbb{Q}_p \) with \( n > 4 \).

### 5.3.2 Proof of Characterization Theorem Part I

Proving these claims relies on use of Theorem 5.1 to prove the first statement, and then using the first claim to prove the second statement. As we will see, the second will take significantly more work.
Chapter 5. Involutions of SO\((n, k, \beta)\)

Proof of Part I. \(\iff\): This direction is clear since \(\alpha \hat{A}\) gives the same conjugation as \(\hat{A}\). Since \(\hat{A}\) is in \(\tilde{G}\), its related automorphism of \(\text{GL}(n, \tilde{k})\) must also retain closure of \(\tilde{G}\). Thus, \(\text{Inn}_A = \text{Inn}_{\alpha \hat{A}}\) is an automorphism of \(\tilde{G}\).

\(\Longrightarrow\): Let \(A\) be a matrix in \(\text{GL}(n, \tilde{k})\) such that \(\text{Inn}_A\) keeps \(\tilde{G}\) invariant, and let \(X \in \tilde{G}\). Also, let \(M\) be the \(n \times n\) invertible, diagonal matrix representing the non-degenerate symmetric bilinear form \(\beta\). Then \(X\) being in the orthogonal group of \(\beta\) over \(\tilde{k}\) implies

\[
\theta_M(X) = M^{-1}(X^T)^{-1}M = X
\]

since the orthogonal group is the fixed-point group of the induced involution \(\theta_M\) of the form. So \((X^T)^{-1} = MXM^{-1}\).

Since \(A^{-1}XA\) is in \(\tilde{G}\) due to \(A\) keeping \(\tilde{G}\) invariant, this matrix product also satisfies the above criteria of the action of the involution of the form on its orthogonal group:

\[
\theta_M(A^{-1}XA) = M^{-1}((A^{-1}XA)^T)^{-1}M = A^{-1}XA.
\]

It is seen that

\[
AM^{-1}((A^{-1}XA)^T)^{-1}MA^{-1} = AM^{-1}A^T(X^T)^{-1}(A^T)^{-1}MA^{-1}
\]
\[
= AM^{-1}A^T(MXM^{-1})(A^T)^{-1}MA^{-1}
\]
\[
= (M^{-1}(A^T)^{-1}MA^{-1})^{-1}X(M^{-1}(A^T)^{-1}MA^{-1})
\]
\[
= X
\]

This demonstrates that

\[
\text{Inn}_{M^{-1}(A^T)^{-1}MA^{-1}} = \text{Id} \text{ on } \tilde{G}.
\]

Using the conclusion of Theorem 5.1, this implies that

\[
M^{-1}(A^T)^{-1}MA^{-1} = \gamma I_{n\times n}
\]

or equivalently,

\[
M^{-1}(A^T)^{-1}M = \gamma A
\]
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

for some $\gamma \in \bar{k}$. Replace $A$ by $\tilde{A} = \alpha A$ (i.e. $A = \frac{1}{\alpha} \tilde{A}$) where $\alpha = \sqrt[n]{\gamma} \in \bar{k}$. Then,

$$M^{-1}(\tilde{A}^T)^{-1} M \tilde{A}^{-1} = M^{-1}((\alpha A)^T)^{-1} M (\alpha A)^{-1}$$

$$= M^{-1}(1/\alpha)(A^T)^{-1} M (1/\alpha)A^{-1}$$

$$= (1/\alpha)^2 (M^{-1}(A^T)^{-1} MA^{-1})$$

$$= (1/\alpha)^2 (\gamma) I_{n \times n} = (1/\sqrt[n]{\gamma})^2 (\gamma) I_{n \times n}$$

$$= (1/\gamma)(\gamma) I_{n \times n} = I_{n \times n}$$

The conclusion is that

$$M^{-1}(\tilde{A}^T)^{-1} M \tilde{A}^{-1} = I_{n \times n}$$

which implies

$$\theta_M(\tilde{A}) = M^{-1}(\tilde{A}^T)^{-1} M = \tilde{A}.$$  

The matrix $\tilde{A}$ is thereby seen to be in $O(n, \bar{k}, \beta)$. Now all we have to do is to ensure that we get a matrix in $\text{SO}(n, \bar{k}, \beta)$ which gives the same inner automorphism (i.e. the same conjugation). It seems reasonable that we should be able to do this since taking scalar multiples of a matrix does not change the resultant conjugation.

Recall that $X \in O(n, k)$ for $\beta$ the standard dot product–represented by the identity $M = I_{n \times n}$ matrix–restricted the set of possible determinants of $X$ to $\{1, -1\}$. This fact does not change in the general case, where $\beta$ is a general form.

**Lemma 16.** If $\beta$ is a non-degenerate, symmetric bilinear form on $V = k^n$ with orthogonal group $O(n, k, \beta)$, then

$$X \in O(n, k, \beta) \implies \det(X) = \{1, -1\}.$$  

**Proof of Lemma.** Let $\beta$ be represented by the diagonal $n \times n$ matrix $M$. Then $X \in O(n, k, \beta)$ implies

$$\theta_M(X) = M^{-1}(X^T)^{-1} M = X$$

so that

$$\det(X) = \det(X^T)^{-1} = \det(X^{-1}) = \frac{1}{\det(X)}$$
which implies

\[(\det(X))^2 = 1 \implies \det(X) = \{1, -1\}.\]  

Now if \(\det(\hat{A}) = 1\) obviously we’re done and \(A = (1/\alpha)\hat{A} = (-1/\alpha)\hat{A}\) with \((1/\alpha) \in \bar{k}\) and \(\hat{A} \in \bar{G}\). If the determinant is \(-1\) we treat this situation differently depending upon whether \(n\) is even or odd.

**Case \(n\) is odd:**
Replace \(\hat{A}\) by \(\hat{A} = -\hat{A}\). Then the inner automorphism \(\text{Inn}_A = \text{Inn}_{\hat{A}} = \text{Inn}_{\hat{A}}\) remains unchanged, and \(\det(\hat{A}) = (-1)^n(\det(\hat{A})) = -(\det(\hat{A})) = 1\). The new matrix \(\hat{A}\) is still in \(O(n, \bar{k}, \beta)\) since

\[
\theta_M(\hat{A}) = M^{-1}(\hat{A}^T)^{-1}M \\
= M^{-1}(-\hat{A}^T)^{-1}M \\
= -M^{-1}(\hat{A}^T)^{-1}M \\
= -\hat{A} = \hat{A}.
\]

Through this it is seen that \(\hat{A} \in \bar{G} = \text{SO}(n, \bar{k}, \beta)\). Therefore, \(A = (1/\alpha)\hat{A} = (-1/\alpha)\hat{A}\) with \((-1/\alpha) \in \bar{k}\) and \(\hat{A} \in \bar{G}\) when \(n\) is odd.

**Case \(n\) is even:**
In the case of \(n\) even we must be content with \(\hat{A} = \tilde{A}\) living in \(O(n, \bar{k}, \beta)\) and not necessarily being of determinant 1. We can multiply \(\tilde{A}\) by a scalar to obtain a determinant 1 matrix \(\hat{A}\) by using \(\hat{A} = \frac{1}{n/\sqrt{\det(\tilde{A})}} \tilde{A}\). We verify its determinant by:

\[
\det(\hat{A}) = \det \left( \frac{1}{n/\sqrt{\det(\tilde{A})}} \tilde{A} \right) = \frac{1}{\left(\frac{n}{\sqrt{\det(\tilde{A})}} \right)^{n/2}(\det(\tilde{A}))} = \frac{1}{\det(\tilde{A})} (\det(\tilde{A})) = 1
\]

However, although this scalar multiplication does not change the inner automorphism \(\text{Inn}_A\), it changes whether the matrix lives in \(O(n, \bar{k}, \beta)\). Unfortunately this attempt at
“fixing” the nature of the matrix means that consequentially

\[
M^{-1}(\hat{A}^T)^{-1}M = M^{-1}\left(\left(\frac{1}{\sqrt[n]{\det(\tilde{A})}}\right)^T\right)^{-1}M
\]

\[
= \sqrt[n]{\det(\tilde{A})}M^{-1}(\tilde{A}^T)^{-1}M
\]

\[
= \sqrt[n]{\det(\tilde{A})}\hat{A}
\]

This only equals \(\hat{A} = \frac{1}{\sqrt[n]{\det(\tilde{A})}}\tilde{A}\) if \(\sqrt[n]{\det(\tilde{A})} = \frac{1}{\sqrt[n]{\det(\tilde{A})}}\) i.e. if \(\left(\sqrt[n]{\det(\tilde{A})}\right)^2 = 1\), which is impossible since \(\det(\tilde{A}) = -1\) \(\implies\) that squaring an even root of \(-1\) cannot possibly result in \(1\). Hence, we are content with \(\hat{A} = \tilde{A} = aA\), or \(A = (1/a)\hat{A}\) with \((1/a) = (1/\sqrt[n]{\gamma}) \in \bar{k}\) and \(\hat{A} \in \tilde{G}\) or \(\hat{A} \in O(n, \bar{k}, \beta)\) with \(\det(\hat{A}) = -1\).

This proves the first part of the Characterization Theorem. \(\square\)

### 5.3.3 Proof of Characterization Theorem Part II for \(n = 3\)

Now we look at proving statement (2) of Theorem 5.2. As in the proof of Theorem 5.1 we will first give a number of examples to illustrate the complicated summations which we use in the formal proof.

If we start with the automorphism given by the conjugation \(\text{Inn}_A\) of \(G\) where \(A\) is in \(\tilde{G}\), then \(\text{Inn}_A\) must surely keep \(\tilde{G}\) invariant as well. We know from the results of the first part of this theorem that we can then assume that \(A\) is a scalar multiple of a matrix actually residing in \(\tilde{G}\). Since the conjugation resulting from this scalar multiple is identical to the conjugation by the matrix in \(\tilde{G}\), we may start with the assumption that any automorphism of \(G\) which is a conjugation by a matrix may be viewed as conjugation by a matrix living in \(\tilde{G}\). So we start with the assumption that \(A\) is in \(\tilde{G}\).

Assume that the automorphism \(\text{Inn}_A\) of \(\tilde{G}\) keeps \(G\) invariant as well. The claim of the second part of Theorem 5.2 is that we can actually take this matrix to be in \(G\) rather than just in \(\tilde{G}\) then. That is to say that given the non-degenerate, symmetric bilinear form \(\beta\) on \(V = k^n\) represented by the \(n \times n\) diagonal matrix \(M_n\), if \(A\) satisfies \(M_n^{-1}(A^T)^{-1}M_n = A\)
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

and $\text{Inn}_A$ keeps $G$ invariant, then the $A$ is a scalar multiple of a matrix having all entries in $k$ and still satisfying the above relation.

Here is the outline for how we show this. We will show that all combinations $a_{ij}a_{kl}$ belong to the base field $k$ of $G$. Then if $A$ does not already have elements all residing in $k$ we replace $A$ by $\hat{A} = a_{ij}A$ where $a_{ij}$ is any entry of $A$. Necessarily then, the new matrix $\hat{A}$ will have entries in $k$.

We first show that $a_{ri}a_{rj} + a_{sj}a_{sj} \in k$ for all $i, j, r, s$ such that $r \neq s$. We then use this to show that $a_{ri}a_{rj} \in k$ for all $i, j, r = 1, \ldots, n$. Second, we use this preliminary information to show that $a_{ri}a_{sj}$ for all $i, j, r, s$ where $r \neq s$. This will give use the obtained conclusion mentioned in the previous paragraph, which will show all entries of the new matrix $\hat{A}$ may be considered elements of $k$. Lastly, we see under what circumstances we can get a matrix of determinant 1 so that $\hat{A} \in G$ and when we must settle for $\hat{A} \in O(n, k, \beta)$. We will verify this result first in the case that $n = 3$ and $n = 4$.

The Case $n = 3$:

1. We begin by showing $a_{ri}a_{rj} + a_{sj}a_{sj} \in k$ when $r \neq s$. We let $M_3 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & m_2 & 0 \\ 0 & 0 & m_3 \end{pmatrix}$.

Denote by $X_{3,2,3}$ the $3 \times 3$ diagonal matrix with $-1$ in the [2, 2] and [3, 3] slots and 1 for the remaining diagonal entry:

$$X_{3,2,3} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Note that $\det(X_{3,2,3}) = 1$. Since the matrix is diagonal and $M_3$ is diagonal (representing a symmetric form) and diagonal matrices commute with one another, it is clear that $M_3^{-1}(X_{3,2,3})^{-1}M_3 = X_{3,2,3}$ and consequently $X_{3,2,3} \in G$. Since $A$ is in $\bar{G}$ we know that $M_3^{-1}(A^T)^{-1}M_3 = A$, or equivalently, $A^{-1} = M_3^{-1}(A^T)M_3$. We use this to write

$$\text{Inn}_A(X) = A^{-1}XA = M_3^{-1}(A^T)M_3XA$$
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

each time we apply $\text{Inn}_A$.

With the assumption that $\text{Inn}_A$ keeps $G$ invariant (i.e. is an automorphism of $G$) and adding that $I_{3 \times 3}$ is clearly in $G$, we know that the difference of each $[i, j]$ entry of $\text{Inn}_A(I_{3 \times 3})$ and of $\text{Inn}_A(X_{3,2,3})$ are in $k$. This means that their difference is in $k$ as well. We get a handle on the essence of this statement and its consequences by looking at $\text{Inn}_A(I_{3 \times 3}) - \text{Inn}_A(X_{3,2,3})$ and each of the $[i, j]$ entries of this difference which must be in $k$.

$$
\text{Inn}_A(I_{3 \times 3}) = \\
\begin{pmatrix}
a_{11}^2 + a_{21}^2 m_2 + a_{31}^2 m_3 & a_{11}a_{12} + a_{22}a_{22} m_2 + a_{31}a_{32} m_3 & a_{11}a_{13} + a_{21}a_{23} m_2 + a_{31}a_{33} m_3 \\
a_{12} a_{12} a_{12} m_2 + a_{22} a_{22} m_2 + \frac{a_{31} a_{31} m_3}{m_2} & a_{12}^2 a_{22} m_2 + a_{22}^2 + \frac{a_{32} a_{32} m_3}{m_2} & a_{12} a_{13} + a_{22} a_{23} m_2 + \frac{a_{32} a_{33} m_3}{m_2} \\
\frac{a_{13} a_{11} m_3}{m_2} + \frac{a_{23} a_{21} m_2}{m_3} + a_{33} a_{31} & \frac{a_{13} a_{12} m_3}{m_2} + \frac{a_{23} a_{22} m_2}{m_3} + a_{33} a_{32} & \frac{a_{13} a_{13} m_3}{m_2} + \frac{a_{23} a_{23} m_3}{m_2} + a_{33} a_{33} \\
\end{pmatrix}
$$

$$
\text{Inn}_A(X_{3,2,3}) = \\
\begin{pmatrix}
a_{11}^2 - a_{31}^2 m_3 & a_{11}a_{12} - a_{22}a_{22} m_2 - a_{31}a_{32} m_3 & a_{11}a_{13} - a_{22}a_{23} m_2 - a_{31}a_{33} m_3 \\
\frac{a_{12} a_{12} a_{12} m_2}{m_2} - a_{22} a_{22} m_2 - \frac{a_{32} a_{32} m_3}{m_2} & a_{12}^2 - a_{22}^2 - \frac{a_{32} a_{32} m_3}{m_2} & a_{12} a_{13} - a_{22} a_{23} m_2 - \frac{a_{32} a_{33} m_3}{m_2} \\
\frac{a_{13} a_{11} m_3}{m_2} - \frac{a_{23} a_{21} m_2}{m_3} - a_{33} a_{31} & \frac{a_{13} a_{12} m_3}{m_2} - \frac{a_{23} a_{22} m_2}{m_3} - a_{33} a_{32} & \frac{a_{13} a_{13} m_3}{m_2} - \frac{a_{23} a_{23} m_3}{m_2} - a_{33} a_{33} \\
\end{pmatrix}
$$

$$
\text{Inn}_A(I_{3 \times 3}) - \text{Inn}_A(X_{3,2,3}) = \\
\begin{pmatrix}
2a_{12}^2 m_2 + 2a_{31} a_{31} m_3 & 2a_{22} a_{22} m_2 + 2a_{31}a_{32} m_3 & 2a_{21} a_{23} m_2 + 2a_{31}a_{33} m_3 \\
2a_{22} a_{22} + \frac{a_{32} a_{32} m_3}{m_2} & 2a_{22}^2 + a_{32}^2 m_3 & 2a_{22} a_{23} + \frac{a_{32} a_{33} m_3}{m_2} \\
2\frac{a_{32} a_{31} m_2}{m_3} + 2a_{33} a_{31} & 2\frac{a_{32} a_{32} m_3}{m_3} + 2a_{33} a_{32} & 2a_{33}^2 m_3 + 2a_{33}^2 m_3 \\
\end{pmatrix}
$$

We can see that with the matrix $X_{3,2,3}$ having $-1$ in the $[i, i]$ spot with $i = 2, 3$ that the resulting matrix difference has each $[i, j]$ entry equal to

$$
a_{2i} a_{2j} \frac{m_2}{m_i} + a_{3i} a_{3j} \frac{m_3}{m_i}
$$

which must be in $k$. Since $m_i$ is in $k$ for all $i = 1, \ldots, 3$, those terms do not affect whether this sum is in $k$. In this way, we see that each sum $a_{2i} a_{2j} + a_{3i} a_{3j}$ is in $k$, this observation resulting from the output when considering the matrix $X \in G$ with $-1$ in the $[2, 2]$ and $[3, 3]$ spot.
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

We further reinforce the notion that using $-1$ in the $[r, r]$ and $[s, s]$ spots requires that $a_{ri}a_{rj} + a_{si}a_{sj} \in k$ by looking at the same steps using $X_{3,1,2}$ the diagonal matrix with $-1$ in the $[1, 1]$ and $[2, 2]$ positions in the place of $X_{3,2,3}$ in the preceding equations. With a straightforward calculation similar to that done for $X_{3,2,3}$ it is clear that $X_{3,1,2} \in G$.

$$X_{3,1,2} := \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\text{Inn}_A(I_{3 \times 3} - X_{3,1,2}) = \begin{pmatrix} 2a_{11}^2 + 2a_{21}^2m_2 & 2a_{11}a_{12} + 2a_{21}a_{22}m_2 & 2a_{11}a_{13} + 2a_{21}a_{23}m_2 \\ 2a_{12}a_{11} + 2a_{22}a_{21} & 2a_{12}^2 + 2a_{22}^2 & 2a_{12}a_{13} + 2a_{22}a_{23} \\ 2a_{13}a_{11} + 2a_{23}a_{21} & 2a_{13}a_{12} + 2a_{23}a_{22}m_2 & 2a_{13}a_{13} + 2a_{23}a_{23} \end{pmatrix}$$

Our supposition was correct. Now that we have $-1$ in the $[1, 1]$ and $[2, 2]$ positions we have each $[i, j]$ entry equal to $a_{1i}a_{1j}m_1 + a_{2i}a_{2j}m_2$ which must be in $k$. Using similar reasoning as before, we see that this forces $a_{1i}a_{1j} + a_{2i}a_{2j}$ to reside in $k$. Using the matrix $X_{3,1,3}$ with $-1$ in the $[1, 1]$ and $[3, 3]$ positions will complete the illustration that we now know that $a_{ri}a_{rj} + a_{si}a_{sj}$ is in $k$ for all $i, j = 1, \ldots, 3$ and $r \neq s$.

(2) We use this information to show that $a_{ri}a_{rj} \in k$ for all $r = 1, \ldots, 3$. Without loss of generality we just need to show that $a_{1i}a_{1j} \in k$. Consider the equality

$$a_{1i}a_{1j} = (a_{1i}a_{1j} + a_{2i}a_{2j} + a_{3i}a_{3j}) - (a_{2i}a_{2j} + a_{3i}a_{3j})$$

The sum $a_{1i}a_{1j} + a_{2i}a_{2j} + a_{3i}a_{3j}$ must be in $k$ since it comes from the $[i, j]$ position of $\text{Inn}_A(I_{3 \times 3})$ from above. Since $a_{2i}a_{2j} + a_{3i}a_{3j}$ has been shown to be in $k$ as well, this difference must be in $k$. Thus, we have verified that $a_{ri}a_{rj} \in k$ for all $r = 1, \ldots, 3$.

(3) Now we must show that $a_{ri}a_{s} \in k$ for $r \neq s$. We start by showing $a_{1i}a_{2j} \in k$. 


Let $Y_{3,1} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $Y_{3,2} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. We illustrate that these matrices are in $G$: $\det(Y_{3,1}) = \det(Y_{3,2}) = 1$ and

$$\theta_{M_3}(Y_{3,1}) = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\theta_{M_3}(Y_{3,2}) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

The automorphism $\text{Inn}_A$ is assumed to keep $G$ invariant, so we apply it to $Y_{3,1}$ and $Y_{3,2}$, again substituting for $A^{-1}$ the equivalent string $M_3^{-1}A^T M_3$. Let $N_{3,i}$ be the image of $Y_{3,i}$ under the action of $\text{Inn}_A$.

$$N_{3,1} := \text{Inn}_A(Y_{3,1}) = \begin{pmatrix}
a_1^2 m_3 \\
-a_1 a_2 + a_{11} a_{22} + a_{31} a_{32} m_3 \\
-a_{11} a_{22} + a_{21} a_{12} + a_{31} a_{32} m_3 \\
-a_{11} a_{22} + a_{21} a_{12} + a_{31} a_{32} m_3 \\
-a_{21} a_{12} + a_{11} a_{22} + a_{31} a_{32} m_3 \\
-a_{11} a_{22} + a_{21} a_{12} + a_{31} a_{32} m_3 \\
-a_{11} a_{22} + a_{21} a_{12} + a_{31} a_{32} m_3 \\
-a_{11} a_{22} + a_{21} a_{12} + a_{31} a_{32} m_3 \\
-a_{21} a_{12} + a_{11} a_{22} + a_{31} a_{32} m_3 \\
-a_{11} a_{22} + a_{21} a_{12} + a_{31} a_{32} m_3 \\
-a_{11} a_{22} + a_{21} a_{12} + a_{31} a_{32} m_3 \\
-a_{21} a_{12} + a_{11} a_{22} + a_{31} a_{32} m_3 \\
-a_{11} a_{22} + a_{21} a_{12} + a_{31} a_{32} m_3 \\
-a_{11} a_{22} + a_{21} a_{12} + a_{31} a_{32} m_3 \\
-a_{21} a_{12} + a_{11} a_{22} + a_{31} a_{32} m_3 \\
-a_{11} a_{22} + a_{21} a_{12} + a_{31} a_{32} m_3 \\
-a_{11} a_{22} + a_{21} a_{12} + a_{31} a_{32} m_3 \\
-a_{21} a_{12} + a_{11} a_{22} + a_{31} a_{32} m_3 \end{pmatrix}$$

$$N_{3,2} := \text{Inn}_A(Y_{3,2}) = \begin{pmatrix}
2 a_1 a_{11} - a_1^2 m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \\
2 a_1 a_{12} + a_{11} a_{22} - a_{31} a_{32} m_3 \end{pmatrix}$$

With each of these required to be back in $G$, we note that the matrix representing the sum of these combinations—although not necessarily in $G$—must have entries in the base field $k$ as well.

$$N_{3,1} + N_{3,2} = \begin{pmatrix}
2 a_1 a_{11} & 2 a_{11} a_{22} & 2 a_{11} a_{23} \\
2 a_1 a_{12} & 2 a_{12} a_{12} & 2 a_{12} a_{23} \\
2 a_1 a_{12} & 2 a_{12} a_{12} & 2 a_{12} a_{23} \\
2 a_1 a_{12} & 2 a_{12} a_{12} & 2 a_{12} a_{23} \end{pmatrix}$$
The \([i, j]\) entry is \(2a_{1i}a_{2j}\). So we have \(a_{1i}a_{2j} \in k\). There is no significant difference between choosing this combination rather than \(a_{1i}a_{3j}\), although this is not clear. After all, it is the third entry of \(M_3\) which differs from the 1s and \(-1\)s used elsewhere, and the \([3, 3]\) entry of \(Y_{3,i}\) may cause difficulties since it lies on the diagonal whereas the upper left-hand \(2 \times 2\) submatrix of \(Y_{3,i}\) is orthogonal for each \(i\). The following illustrations show that determining that \(a_{3i}a_{1j} \in k\) does not differ significantly.

The matrix \(A^{-1}\) must be in \(\tilde{G}\) since \(A\) is. Also, \(A^{-1}\) must keep \(G\) invariant since \(A\) is bijective onto \(G\). Let's look at the action of \(\text{Inn}_{A^{-1}}\) on the matrices \(Y_{3,i}\). We use the notation \(Z_{3,i}\) to indicate the image of \(Y_{3,i}\) under the action of \(\text{Inn}_{A^{-1}}\). In the following computations we use in place of \(A^{-1}\) the matrix product \(M_3^{-1}A^T M_3\), which comes from solving \(\theta_{M_3}(A) = M_3^{-1}A^T M_3 = A\) for \(A^{-1}\). This changes the computation to \(\text{Inn}_A(X) = M_3^{-1}A^T M_3 X A\).

\[
Z_{3,1} := \text{Inn}_{A^{-1}}(Y_{3,1}) = \begin{pmatrix}
\frac{a_{11}^2}{m_3} & -2a_1a_{12} + a_{11}a_{22} + \frac{a_{21}a_{13}}{m_3} & -a_{12}a_{13}m_3 + a_{11}a_{32}m_3 + a_{13}a_{33} \\
-a_{11}a_{22} + a_{21}a_{12} + \frac{a_{23}a_{13}}{m_3} & \frac{a_{22}^2}{m_3} & -a_{22}a_{13}m_3 + a_{21}a_{32}m_3 + a_{23}a_{33} \\
-a_{11}a_{32} + a_{12}a_{31} + \frac{a_{13}a_{31}}{m_3} & -a_{21}a_{32} + a_{22}a_{31} + \frac{a_{23}a_{31}}{m_3} & a_{33}^2
\end{pmatrix}
\]

\[
Z_{3,2} := \text{Inn}_{A^{-1}}(Y_{3,2}) = \begin{pmatrix}
2a_{11}a_{12} - \frac{a_{11}^2}{m_3} & a_{21}a_{12} + a_{11}a_{22} + \frac{a_{21}a_{13}}{m_3} & a_{12}a_{13}m_3 + a_{11}a_{32}m_3 - a_{13}a_{33} \\
a_{21}a_{12} + a_{11}a_{22} + \frac{a_{23}a_{13}}{m_3} & 2a_{21}a_{22} - \frac{a_{22}^2}{m_3} & a_{22}a_{31}m_3 + a_{21}a_{32}m_3 - a_{23}a_{33} \\
a_{12}a_{31} + a_{11}a_{22} + \frac{a_{13}a_{31}}{m_3} & a_{22}a_{31} + a_{21}a_{32} + \frac{a_{23}a_{31}}{m_3} & 2a_{32}a_{31}m_3 - a_{33}^2
\end{pmatrix}
\]

Since the entries of the matrices \(Z_{3,i}\) must belong to \(k\), so must the entries of the sum of the matrices.

\[
Z_{3,1} + Z_{3,2} = \begin{pmatrix}
2a_{11}a_{12} & 2a_{11}a_{22} & -2a_{11}a_{32} \\
2a_{21}a_{12} & 2a_{21}a_{22} & -2a_{21}a_{32} \\
2a_{12}a_{31} & 2a_{22}a_{31} & -2a_{32}a_{31}
\end{pmatrix}
\]

We do not immediately obtain \(a_{3j}a_{ik} \in k\) for each desired pair in consideration. However, it is not necessary to get each pair inside of \(k\) directly. The \([i, j]\) entry is either \(2a_{1i}a_{j2}\)
or $-2a_{i1}a_{j2}$, so it yields $a_{i1}a_{j2}$ in the base field $k$. In particular, the [3, 2] entry shows $a_{31}a_{22}$ in $k$. This will be all we need. The following lemma holds for any $n > 2$.

**Lemma 17.** Assume $a_{ri}a_{sj} \in k \; \forall \; i, j = 1, \ldots, n$ and $r, s < t$ and that the specific combination $a_{ti}a_{si}$ is in $k$. Then $a_{ri}a_{rj} \in k \; \forall r < t, \; \forall i, j = 1, \ldots, n$.

**Proof.** Rewrite $a_{ri}a_{rj}$ ($r = 1, 2, \ldots, t - 1$) as

$$\frac{a_{ti}a_{ri}a_{rj}a_{sj}}{a_{ti}a_{si}a_{sj}}.$$

This term is in $k$ since $a_{ti}a_{ri}a_{rj}a_{sj}$ and $a_{ti}a_{si}a_{sj}$ are all in $k$ (when $r = 1, 2, \ldots, t - 1$). $\square$

This shows we were correct to state that we can show that a specific product $a_{31}a_{22}$ is in $k$ and without loss of generality obtain all products $a_{3i}a_{rj}$ in $k$. Hence, we have shown that all products $a_{ri}a_{sj} \; i, j, r, s = 1, \ldots, 3$ reside in the base field $k$.

(4) Fix any entry $a_{ij}$ of $A$ and consider the matrix $B = a_{ij}A$. Each element of $B$ has the form $a_{ij}a_{ii}$ and therefore resides in $k$. So $B$ is in $GL(3, k)$. Since $\text{Inn}_A = \text{Inn}_B$, $\text{Inn}_B$ keeps $G$ invariant as well, and consequently $B^{-1}(X^T)^{-1}B \in G$. Substituting

$$BM_3^{-1}((B^{-1}XB)^T)^{-1}M_3B^{-1} = BM_3^{-1}B^T(X^T)^{-1}(B^T)^{-1}M_3B^{-1}$$

$$= X$$

$$= M_3^{-1}(X^T)^{-1}M_3$$

So

$$M_3BM_3^{-1}B^T(X^T)^{-1}(B^T)^{-1}M_3B^{-1}M_3^{-1} = (X^T)^{-1}$$

Taking the transpose and inverse of each side:

$$M_3^{-1}(B^T)^{-1}M_3B^{-1}XBM_3^{-1}B^TM_3 = X$$

So

$$\text{Inn}_{BM_3^{-1}B^TM_3} = \text{Id}.$$
This means that \( BM_3^{-1}B^T M_3 = \alpha I_{3 \times 3} \) for some \( \alpha \in \tilde{k} \). Taking determinants of both sides tells us that \( \det(B)^2 = (\alpha)^3 \) or \( \alpha = \sqrt[3]{\det(B)^2} \). Let \( \hat{B} = \frac{1}{\sqrt[3]{\alpha}} B \). Then

\[
\hat{B} M_3^{-1} \hat{B}^T M_3 = \frac{1}{\left(\sqrt[3]{\det(B)^2}\right)^2} BM_3^{-1} B^T M_3
\]

\[
= \frac{1}{\alpha} I_{3 \times 3} = I_{3 \times 3}
\]

and \( \hat{B} \in O(3, k, \beta) \) since

\[
M_3^{-1} \hat{B}^T M_3 = \hat{B}^{-1} \implies M_3^{-1}(\hat{B}^T)^{-1} M_3 = \hat{B}.
\]

We use

\[
\hat{A} := \hat{B} = \frac{1}{\sqrt[3]{\alpha}} B = \frac{1}{\sqrt[3]{\alpha}} a_{ij} A
\]

if the determinant of \( \hat{B} \) is 1. If the determinant of \( \hat{B} \) is \(-1\), we use

\[
\hat{A} = -\hat{B} = -\frac{1}{\sqrt[3]{\alpha}} B = -\frac{1}{\sqrt[3]{\alpha}} a_{ij} A.
\]

Then \( \hat{A} \) is still in \( O(3, k, \beta) \) and has determinant 1, so it belongs to \( G \). Therefore \( A = \gamma \hat{A} \), with \( \hat{A} \in G \).

### 5.3.4 Proof of Characterization Theorem Part II for \( n = 4 \)

We’ve shown the result for \( n = 3 \). Since the behavior of these matrices may differ depending upon whether \( n \) is even or odd, we illustrate the case for \( n = 4 \) before stating the formal proof for general \( n \).

**The Case \( n = 4 \):**

We follow a similar path as when \( n = 3 \).
Chapter 5. Involutions of \( \text{SO}(n, k, \beta) \)

(1) We denote the matrix of the symmetric form by

\[
M_4 = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & m_3 & 0 \\
0 & 0 & 0 & m_4
\end{pmatrix}
\]

and let

\[
X_{4,2,3} = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 \\
0 & 0 & -1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}.
\]

Assuming \( \text{Inn}_A \) keeps \( G \) invariant, we simplify the induced automorphism

\[
\text{Inn}_A(X) = M_4^{-1} A^T M_4 X A
\]

since \( A \) is assumed to be in \( \bar{G} \). The output of \( \text{Inn}_A \) acting on \( X_{4,2,3} \) and on \( I_{4,2,3} \) (with the above substitution made for \( A^{-1} \)) must have entries in \( k \):

\[
\text{Inn}_A(I_{4\times 4}) =
\begin{pmatrix}
a_{11}^2 + a_{21}^2 + a_3^2 m_3 + a_4^2 m_4 & a_{11} a_{12} + a_{21} a_{22} + a_{31} a_{32} m_3 + a_{41} a_{42} m_4 \\
a_{11} a_{12} + a_{21} a_{22} + a_{31} a_{32} m_3 + a_{41} a_{42} m_4 & a_{11}^2 + a_{12}^2 + a_{21}^2 + a_{22}^2 + a_3^2 m_3 + a_4^2 m_4 \\
a_{11} a_{13} + a_{21} a_{23} + a_{31} a_{33} m_3 + a_{41} a_{43} m_4 & a_{11} a_{14} + a_{21} a_{24} + a_{31} a_{34} m_3 + a_{41} a_{44} m_4 \\
a_{12} a_{13} + a_{22} a_{23} + a_{32} a_{33} m_3 + a_{42} a_{43} m_4 & a_{12} a_{14} + a_{22} a_{24} + a_{32} a_{34} m_3 + a_{42} a_{44} m_4
\end{pmatrix}
\]

\[
\text{Inn}_A(X_{4,2,3}) =
\begin{pmatrix}
a_{11}^2 + a_{21}^2 + a_3^2 m_3 + a_4^2 m_4 & a_{11} a_{12} + a_{21} a_{22} + a_{31} a_{32} m_3 + a_{41} a_{42} m_4 \\
a_{11} a_{12} + a_{21} a_{22} + a_{31} a_{32} m_3 + a_{41} a_{42} m_4 & a_{11}^2 + a_{12}^2 + a_{21}^2 + a_{22}^2 + a_3^2 m_3 + a_4^2 m_4 \\
a_{11} a_{13} + a_{21} a_{23} + a_{31} a_{33} m_3 + a_{41} a_{43} m_4 & a_{11} a_{14} + a_{21} a_{24} + a_{31} a_{34} m_3 + a_{41} a_{44} m_4 \\
a_{12} a_{13} + a_{22} a_{23} + a_{32} a_{33} m_3 + a_{42} a_{43} m_4 & a_{12} a_{14} + a_{22} a_{24} + a_{32} a_{34} m_3 + a_{42} a_{44} m_4
\end{pmatrix}
\]
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

$\text{Inn}_A(I_{4 \times 4}) + \text{Inn}_A(X_{4,2,3}) =$

\[
\begin{pmatrix}
2a_{11}^2 + a_{41}^2 m_4 & a_{11}a_{12} + 2a_{41}a_{42}m_4 & 2a_{11}a_{13} + 2a_{41}a_{43}m_4 & 2a_{11}a_{14} + 2a_{41}a_{44}m_4 \\
2a_{11}a_{12} + 2a_{41}a_{42}m_4 & 2a_{12}^2 + a_{42}^2 m_4 & 2a_{12}a_{13} + 2a_{42}a_{43}m_4 & 2a_{12}a_{14} + 2a_{42}a_{44}m_4 \\
2a_{11}a_{13} + 2a_{41}a_{43}m_4 & 2a_{12}a_{13} + 2a_{42}a_{43}m_4 & 2a_{13}^2 + a_{43}^2 m_4 & 2a_{13}a_{14} + 2a_{43}a_{44}m_4 \\
2a_{11}a_{14} + 2a_{41}a_{44}m_4 & 2a_{12}a_{14} + 2a_{42}a_{44}m_4 & 2a_{13}a_{14} + 2a_{43}a_{44}m_4 & 2a_{14}^2 + a_{44}^2 m_4
\end{pmatrix}
\]

$\text{Inn}_A(I_{4 \times 4}) - \text{Inn}_A(X_{4,2,3}) =$

\[
\begin{pmatrix}
2a_{21}^2 + a_{31}^2 m_3 & 2a_{21}a_{22} + 2a_{31}a_{32}m_3 & 2a_{21}a_{23} + 2a_{31}a_{33}m_3 & 2a_{21}a_{24} + 2a_{31}a_{34}m_3 \\
2a_{21}a_{22} + 2a_{31}a_{32}m_3 & 2a_{22}^2 + a_{32}^2 m_3 & 2a_{22}a_{23} + 2a_{32}a_{33}m_3 & 2a_{22}a_{24} + 2a_{32}a_{34}m_3 \\
2a_{21}a_{23} + 2a_{31}a_{33}m_3 & 2a_{22}a_{23} + 2a_{32}a_{33}m_3 & 2a_{23}^2 + a_{33}^2 m_3 & 2a_{23}a_{24} + 2a_{33}a_{34}m_3 \\
2a_{21}a_{24} + 2a_{31}a_{34}m_3 & 2a_{22}a_{24} + 2a_{32}a_{34}m_3 & 2a_{23}a_{24} + 2a_{33}a_{34}m_3 & 2a_{24}^2 + a_{34}^2 m_3
\end{pmatrix}
\]

We can see that using $X_{4,r,s}$ the diagonal $4 \times 4$ matrix with 1s on the diagonal except $-1$ in the $[r, r]$ and $[s, s]$ slots, respectively, we can get any product $2a_{ri}a_{rj}(\frac{m_r}{m_1}) + 2a_{si}a_{sj}(\frac{m_s}{m_1})$ to be shown to be in $k$. The $m_i$ terms, being in $k$, don’t affect the location of the product of the $A$ terms. We conclude that $a_{ri}a_{rj} + a_{si}a_{sj}$ is in $k$ for all $i, j, r, s = 1, \ldots, 4$.

(2) We show that $a_{ri}a_{rj} \in k$. Without loss of generality, we show $a_{1i}a_{1j} \in k$. From the action of the automorphism on the identity $4 \times 4$ matrix, we look at the $[i, j]$ entry of this
Chapter 5. Involutions of \( \text{SO}(n, k, \beta) \)

product

\[ [i, j] = a_{1i}a_{1j}\left(\frac{m_1}{m_i}\right) + \cdots + a_{4i}a_{4j}\left(\frac{m_4}{m_i}\right) \]

which is in \( k \), we use the identity

\[
a_{1i}a_{1j}\left(\frac{m_1}{m_i}\right) = \left(a_{1i}a_{1j}\left(\frac{m_1}{m_i}\right) + \cdots + a_{4i}a_{4j}\left(\frac{m_4}{m_i}\right)\right) - \frac{1}{2}\left(a_{2i}a_{2j}\left(\frac{m_2}{m_i}\right) + a_{3i}a_{3j}\right) - \frac{1}{2}\left(a_{4i}a_{4j}\left(\frac{m_4}{m_i}\right) + a_{2i}a_{2j}\left(\frac{m_2}{m_i}\right)\right) - \frac{1}{2}\left(a_{3i}a_{3j}\left(\frac{m_3}{m_i}\right) + a_{4i}a_{4j}\left(\frac{m_4}{m_i}\right)\right)
\]

Since each pair \( a_{ri}a_{rj} \in k \), so is the overall sum \( a_{1i}a_{1j} \). Without loss of generality, we may state that \( a_{ri}a_{rj} \) is in \( k \).

(3) We show that \( a_{ri}a_{sj} \in k \) when \( r \neq s \). We’ll look at the action of \( \text{Inn}_A \) on the matrices

\[
Y_{4,1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad Y_{4,2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}
\]

and to find the sum \( \text{Inn}_A(Y_{4,1}) + \text{Inn}_A(Y_{4,2}) \) which must have entries in \( k \). Adhering to the notation used for \( n = 3 \), we let \( N_{4,i} = \text{Inn}_A(Y_{4,i}) \). It is clear that \( \det(Y_{4,1}) = \det(Y_{4,2}) = 1 \), and straightforward to check that

\[
\theta_{M_4}(Y_{4,1}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}
\]

\[
\theta_{M_4}(Y_{4,2}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}
\]
Chapter 5. Involutions of SO(n, k, \beta)
and \( Y \) and matrices \( A \) the action of \( \text{Inn} \)

So the action of \( \text{Inn} \)

A \( a \) is in \( k \) if \( a \) is in \( k \), it is clear that \( a_1 a_2 \) is in \( k \).

The \([i, j]\) entries of \( \text{Inn}_A(Y_{4,1}) \), and \( \text{Inn}_A(Y_{4,2}) \) are

\[
\begin{pmatrix}
2a_{11}^2 m_i + 2a_{11} a_{12} + 2a_{11} a_{22} + 2a_{11} a_{22} m_i \\
2a_{12} a_{12} + 2a_{12} a_{12} a_{24} + 2a_{12} a_{24} a_{24} m_i \\
2a_{13} a_{23} + 2a_{13} a_{23} + 2a_{13} a_{23} m_i \\
2a_{14} a_{24} + 2a_{14} a_{24} + 2a_{14} a_{24} m_i \\
\end{pmatrix}
\]

The \([i, j]\) entries of \( \text{Inn}_A(Y_{4,1}) \) and \( \text{Inn}_A(Y_{4,2}) \) are

\[
a_{1i} a_{2j} \left( \frac{m_1}{m_i} \right) - a_{2i} a_{1j} \left( \frac{m_2}{m_i} \right) + a_{3i} a_{3j} \left( \frac{m_3}{m_i} \right) + a_{4i} a_{4j} \left( \frac{m_4}{m_i} \right)
\]

and

\[
a_{1i} a_{2j} \left( \frac{m_1}{m_i} \right) + a_{2i} a_{1j} \left( \frac{m_2}{m_i} \right) - a_{3i} a_{3j} \left( \frac{m_3}{m_i} \right) + a_{4i} a_{4j} \left( \frac{m_4}{m_i} \right).
\]

So the \([i, j]\) entry of the sum is \( 2a_{1i} a_{2j} \left( \frac{m_1}{m_i} \right) + 2a_{4i} a_{4j} \left( \frac{m_4}{m_i} \right) \). Since \( a_{4i} a_{4j} \) and the terms \( m_i \) are in \( k \), it is clear that \( a_1 a_2 \) is in \( k \).

(4) We now need to show that some \( a_{3i} a_{1j} \) and some \( a_{4i} a_{1j} \) are in \( k \) for \( l = 1 \) or 2, and then Lemma 17 will show that all combinations \( a_{r_1} a_{s_1} \) are in \( k \). To do this, we consider the action of \( \text{Inn}_{A-1} \), which also must keep \( G \) invariant, on \( Y_{4,1}, Y_{4,2} \) and also on the two

matrices \( Y_{4,3} := \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \) and \( Y_{4,4} := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \). We first ensure that \( Y_{4,3} \)

and \( Y_{4,4} \) are in \( G \). Note that \( \det(Y_{4,3}) = \det(Y_{4,4}) = 1 \). Also,
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

\[
\theta_{M_4}(Y_{4,3}) = \begin{pmatrix}
0 & -1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
\]

\[
\theta_{M_4}(Y_{4,4}) = \begin{pmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & -1
\end{pmatrix}
\]

So the matrices are in $G$.

We define $Z_{4,i} := \text{Inn}_{A^{-1}}(Y_{4,i})$ and take sums and differences of these matrices since these combinations will necessarily have entries in $k$.

\[
Z_{4,1} := \text{Inn}_{A^{-1}}(Y_{4,1}) = \\
\left(\begin{array}{cccc}
\frac{a_1^2}{m_3} + \frac{a_4^2}{m_4} & -a_21a_{12} + a_{11}a_{22} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} \\
-a_11a_{22} + a_12a_{12} + \frac{a_{13}a_{13}}{m_3} + \frac{a_{14}a_{14}}{m_4} & \frac{a_2^2}{m_3} + \frac{a_4^2}{m_4} \\
-a_11a_{32} + a_31a_{12} + \frac{a_{33}a_{13}}{m_3} + \frac{a_{34}a_{14}}{m_4} & -a_21a_{32} + a_31a_{22} + \frac{a_{33}a_{23}}{m_3} + \frac{a_{34}a_{24}}{m_4} \\
-a_11a_{42} + a_41a_{12} + \frac{a_{43}a_{13}}{m_3} + \frac{a_{44}a_{14}}{m_4} & -a_21a_{42} + a_41a_{22} + \frac{a_{43}a_{23}}{m_3} + \frac{a_{44}a_{24}}{m_4}
\end{array}\right)
\]

\[
Z_{4,2} := \text{Inn}_{A^{-1}}(Y_{4,2}) = 
\]
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

\[
\begin{pmatrix}
2a_{12}a_{11} - \frac{a_{13}^2}{m_3} + \frac{a_{14}^2}{m_4} & a_{21}a_{12} + a_{11}a_{22} - \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} \\
a_{11}a_{22} + a_{21}a_{12} - \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} & 2a_{22}a_{21} - \frac{a_{23}^2}{m_3} + \frac{a_{24}^2}{m_4} \\
a_{11}a_{32} + a_{31}a_{12} - \frac{a_{33}a_{13}}{m_3} + \frac{a_{34}a_{14}}{m_4} & 2a_{21}a_{32} + a_{31}a_{22} - \frac{a_{23}a_{33}}{m_3} + \frac{a_{24}a_{34}}{m_4} \\
a_{11}a_{42} + a_{41}a_{12} - \frac{a_{33}a_{13}}{m_3} + \frac{a_{34}a_{14}}{m_4} & 2a_{21}a_{42} + a_{41}a_{22} - \frac{a_{33}a_{23}}{m_3} + \frac{a_{34}a_{24}}{m_4}
\end{pmatrix}
\]

\[
a_{12}a_{31}m_3 + a_{11}a_{32}m_3 - a_{13}a_{33} + \frac{a_{23}a_{32}m_3}{m_4} \quad 2a_{32}a_{31}m_3 - a_{33}^2 + \frac{a_{34}^2m_3}{m_4} \quad a_{31}a_{42}m_3 + a_{32}a_{41}m_3 - a_{33}a_{43} + \frac{a_{34}a_{43}m_3}{m_4}
\]

\[
Z_{4,3} := \text{Inn}_{A^{-1}}(Y_{4,3}) =
\begin{pmatrix}
\frac{a_{2}^2}{m_3} + \frac{a_{4}^2}{m_4} & \frac{a_{2}^2}{m_3} + \frac{a_{4}^2}{m_4} & \frac{a_{2}^2}{m_3} + \frac{a_{4}^2}{m_4} \\
a_{11}a_{22} - a_{21}a_{12} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} & a_{21}a_{12} - a_{11}a_{22} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} & a_{21}a_{12} - a_{11}a_{22} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} \\
a_{11}a_{32} - a_{31}a_{12} + \frac{a_{33}a_{13}}{m_3} + \frac{a_{34}a_{14}}{m_4} & a_{11}a_{32} - a_{31}a_{12} + \frac{a_{33}a_{13}}{m_3} + \frac{a_{34}a_{14}}{m_4} & a_{11}a_{32} - a_{31}a_{12} + \frac{a_{33}a_{13}}{m_3} + \frac{a_{34}a_{14}}{m_4} \\
a_{11}a_{42} - a_{41}a_{12} + \frac{a_{33}a_{13}}{m_3} + \frac{a_{34}a_{14}}{m_4} & a_{11}a_{42} - a_{41}a_{12} + \frac{a_{33}a_{13}}{m_3} + \frac{a_{34}a_{14}}{m_4} & a_{11}a_{42} - a_{41}a_{12} + \frac{a_{33}a_{13}}{m_3} + \frac{a_{34}a_{14}}{m_4}
\end{pmatrix}
\]

\[
a_{12}a_{31}m_3 + a_{11}a_{32}m_3 + a_{13}a_{33} + \frac{a_{14}a_{34}m_3}{m_4} \quad a_{22}a_{31}m_3 + a_{21}a_{32}m_3 + a_{23}a_{33} + \frac{a_{24}a_{34}m_3}{m_4} \quad a_{32}a_{41}m_3 + a_{31}a_{42}m_3 + a_{33}a_{43} + \frac{a_{34}a_{44}m_3}{m_4}
\]

\[
Z_{4,4} := \text{Inn}_{A^{-1}}(Y_{4,4}) =
\begin{pmatrix}
\frac{a_{2}^2}{m_3} + \frac{a_{4}^2}{m_4} & \frac{a_{2}^2}{m_3} + \frac{a_{4}^2}{m_4} & \frac{a_{2}^2}{m_3} + \frac{a_{4}^2}{m_4} \\
a_{12}a_{13} - a_{13}a_{12} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} & a_{12}a_{13} - a_{13}a_{12} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} & a_{12}a_{13} - a_{13}a_{12} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} \\
a_{12}a_{23} - a_{23}a_{12} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} & a_{12}a_{23} - a_{23}a_{12} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} & a_{12}a_{23} - a_{23}a_{12} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} \\
a_{12}a_{34} - a_{34}a_{12} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} & a_{12}a_{34} - a_{34}a_{12} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4} & a_{12}a_{34} - a_{34}a_{12} + \frac{a_{23}a_{13}}{m_3} + \frac{a_{24}a_{14}}{m_4}
\end{pmatrix}
\]
Chapter 5. Involutions of $SO(n, k, \beta)$

\[
\begin{pmatrix}
2a_{12}a_{11} + \frac{a_{12}^2}{m_3} - \frac{a_{14}^2}{m_4} & a_{21}a_{12} + a_{11}a_{22} + \frac{a_{23}a_{13}}{m_3} - \frac{a_{23}a_{14}}{m_4} \\
a_{11}a_{22} + a_{21}a_{12} + \frac{a_{23}a_{13}}{m_3} - \frac{a_{23}a_{14}}{m_4} & 2a_{22}a_{21} + \frac{a_{21}^2}{m_3} - \frac{a_{24}^2}{m_4} \\
a_{11}a_{32} + a_{31}a_{12} + \frac{a_{33}a_{13}}{m_3} - \frac{a_{33}a_{14}}{m_4} & a_{21}a_{32} + a_{31}a_{22} + \frac{a_{33}a_{23}}{m_3} - \frac{a_{33}a_{24}}{m_4} \\
a_{11}a_{42} + a_{41}a_{12} + \frac{a_{43}a_{13}}{m_3} - \frac{a_{43}a_{14}}{m_4} & a_{21}a_{42} + a_{41}a_{22} + \frac{a_{43}a_{23}}{m_3} - \frac{a_{43}a_{24}}{m_4}
\end{pmatrix}
\]

\[
\begin{align*}
a_{12}a_{31}m_3 + a_{11}a_{32}m_3 + a_{13}a_{33} & - \frac{a_{12}a_{33}m_3}{m_4} - a_{12}a_{41}m_4 + a_{11}a_{42}m_4 + \frac{a_{11}a_{41}m_4}{m_3} - a_{14}a_{44} \\
a_{22}a_{31}m_3 + a_{21}a_{32}m_3 + a_{23}a_{33} & - \frac{a_{22}a_{33}m_3}{m_4} - a_{22}a_{41}m_4 + a_{21}a_{42}m_4 + \frac{a_{21}a_{41}m_4}{m_3} - a_{24}a_{44} \\
2a_{32}a_{31}m_3 + a_{23}^2 - \frac{a_{23}^2m_3}{m_4} & a_{32}a_{41}m_4 + a_{31}a_{42}m_4 + \frac{a_{31}a_{41}m_4}{m_3} - a_{34}a_{44} \\
a_{31}a_{42}m_3 + a_{32}a_{41}m_3 + a_{33}a_{43} & - \frac{a_{33}a_{43}m_3}{m_4} - 2a_{41}a_{42}m_4 + \frac{a_{44}^2m_4}{m_3} - a_{44}^2
\end{align*}
\]

We show that $a_{31}a_{12}$ and $a_{41}a_{12}$ belong to $k$. Notice first that the $[i, j]$ entry of $Z_{4,1}$ is

\[
a_{i1}a_{j2}m_j - a_{i2}a_{j1}m_j + a_{i3}a_{j3}m_j m_3 + a_{i4}a_{j4}m_j m_4,
\]

the $[i, j]$ entry of $Z_{4,2}$ is

\[
a_{i1}a_{j2}m_j + a_{i2}a_{j1}m_j - a_{i3}a_{j3}m_j m_3 + a_{i4}a_{j4}m_j m_4,
\]

the $[i, j]$ entry of $Z_{4,3}$ is

\[
-a_{i1}a_{j2}m_j + a_{i2}a_{j1}m_j + a_{i3}a_{j3}m_j m_3 + a_{i4}a_{j4}m_j m_4,
\]

and the $[i, j]$ entry of $Z_{4,4}$ is

\[
a_{i1}a_{j2}m_j + a_{i2}a_{j1}m_j + a_{i3}a_{j3}m_j m_3 - a_{i4}a_{j4}m_j m_4.
\]

Therefore, the $[i, j]$ entries of $Z_{4,1} + Z_{4,3}$, $Z_{4,1} + Z_{4,2}$, and $Z_{4,1} + Z_{4,4}$ are (respectively)

\[
2a_{i3}a_{j3} \frac{m_i}{m_3} + 2a_{i4}a_{j4} \frac{m_i}{m_4},
2a_{i1}a_{j2}m_j + 2a_{i4}a_{j4} \frac{m_i}{m_4},
\]

and

\[
2a_{i1}a_{j2}m_j + 2a_{i3}a_{j3} \frac{m_i}{m_3},
\]
Notice that

\[-a_{i2}a_{j1}m_j = \left( a_{i1}a_{j2}m_j - a_{i2}a_{j1}m_j + a_{i3}a_{j3} \frac{m_j}{m_3} + a_{i4}a_{j4} \frac{m_j}{m_4} \right) - \left( \frac{1}{2} \right) \left( a_{i1}a_{j2}m_j + a_{i3}a_{j3} \frac{m_j}{m_3} \right) - \left( \frac{1}{2} \right) \left( a_{i1}a_{j2}m_j + a_{i4}a_{j4} \frac{m_j}{m_4} \right) - \left( \frac{1}{2} \right) \left( a_{i3}a_{j3} \frac{m_j}{m_3} + a_{i4}a_{j4} \frac{m_j}{m_4} \right).\]

Then \(-a_{i2}a_{j1}m_j \in k\), since each of the four terms that comprise it have been shown to belong to \(k\). So \(a_{i2}a_{j1} \in k\) since \(-m_j \in k\). In particular, \(a_{12}a_{31}\) and \(a_{12}a_{41}\) are in the base field, which combined with the conclusion of Lemma 17 gives all products \(a_{ri}a_{sj}\) in \(k\).

(5) Fix any entry \(a_{i j}^\ast\) of \(A\) and consider the matrix \(B = a_{i j}^\ast A\). Each element of \(B\) has the form \(a_{i j}^\ast a_{i, j}\) and therefore resides in \(k\). So \(B\) is in \(\text{GL}(4, k)\). Since \(\text{Inn}_A = \text{Inn}_B\), \(\text{Inn}_B\) keeps \(G\) invariant as well, and consequently \(B^{-1}(X^T)^{-1}B \in G\). Substituting \(M_4^{-1}(\text{Inn}_B(X)^T)^{-1}M_4 = \text{Inn}_B(X) = B^{-1}XB\) and

\[
BM_4^{-1}((B^{-1}XB)^T)^{-1}M_4B^{-1} = BM_4^{-1}B^T(X^T)^{-1}(B^T)^{-1}M_4B^{-1} = X = M_4^{-1}(X^T)^{-1}M_4.
\]

So

\[
M_4BM_4^{-1}B^T(X^T)^{-1}(B^T)^{-1}M_4B^{-1}M_4^{-1} = (X^T)^{-1}
\]

Taking the transpose and inverse of each side:

\[
M_4^{-1}(B^T)^{-1}M_4B^{-1}XBM_4^{-1}B^TM_4 = X
\]

So

\[
\text{Inn}_B M_4^{-1}B^TM_4 = \text{Id}.
\]
This means that $BM_4^{-1}B^T M_4 = \alpha I_{4 \times 4}$ for some $\alpha \in \tilde{k}$. Taking determinants of both sides tells us that $\det(B)^2 = (\alpha)^4$ or $\alpha = \sqrt[4]{\det(B)^2}$. Let $\hat{B} = \frac{1}{\sqrt[4]{\alpha}} B$. Then

$$BM_4^{-1}\hat{B}^T M_4 = \left(\frac{1}{\sqrt[4]{\det(B)^2}}\right)^2 BM_4^{-1}B^T M_4$$

$$= \frac{1}{\alpha} I_{4 \times 4} = I_{4 \times 4}$$

and $\hat{B} \in O(4, k, \beta)$ since

$$M_4^{-1}\hat{B}^T M_4 = \hat{B}^{-1} \implies M_4^{-1}(\hat{B}^T)^{-1} M_4 = \hat{B}.$$

We use

$$\hat{A} := \hat{B} = \frac{1}{\sqrt[4]{\alpha}} B = \frac{1}{\sqrt[4]{\alpha}} a_{ij}A$$

if the determinant of $\hat{B}$ is 1. If the determinant of $\hat{B}$ is $-1$ we cannot always change it to 1 since $\hat{A} := \frac{1}{\sqrt[4]{-1}} \hat{B}$—although having $\det(\hat{A}) = \left(-\frac{1}{\sqrt[4]{-1}}\right)^4 \det(\hat{B}) = (-1)(-1) = 1$—will no longer be in $O(4, k, \beta)$:

$$\hat{A}M_4^{-1}\hat{A}^T M_4 = \left(\frac{1}{\sqrt[4]{-1}}\right)^2 \hat{B}M_4^{-1}\hat{B}^T M_4 = (-\sqrt[-4]{-1})I_{4 \times 4}$$

Therefore $A = \gamma \hat{A}$, with $\hat{A} \in G$ or $\hat{A} \in O(4, k, \beta)$ and $\det(\hat{A}) = -1$.

### 5.3.5 General Proof of Characterization Theorem Part II, $n$ Odd

We have proven the result for $n = 3$ and $n = 4$. The proof for the general case $n > 2$ will follow the same pattern. With these numerous illustrations, the main idea of our steps will now be clear. We’ll treat the even and odd cases separately as the steps differ slightly.
Proof. Suppose $n$ is odd. Let $M_n$ be the matrix of the symmetric bilinear form,

$$
M_n = \begin{pmatrix}
1 & 0 & \ldots & \ldots & \ldots & 0 \\
0 & m_2 & 0 & \ldots & \ldots & 0 \\
0 & 0 & m_3 & 0 & \ldots & 0 \\
\vdots & \vdots & 0 & \ddots & \ddots & 0 \\
m_{i+1} & 0 & 0 & \ddots & \ddots & \ddots \\
\vdots & \vdots & 0 & \ddots & \ddots & \ddots \\
0 & 0 & 0 & \ddots & \ddots & m_{n-1} \\
0 & \ldots & \ldots & \ldots & \ldots & m_n
\end{pmatrix}
$$

We know that all automorphisms of $G$ when $n$ is odd are conjugations which keep $\tilde{G}$ invariant and therefore they can all be taken to be of the form $\text{Inn}_A$, where $A = aB$, for some $a \in \tilde{k}$, and some $B \in \tilde{G}$. Furthermore, $\text{Inn}_A = \text{Inn}_aB = \text{Inn}_B$, so that we may begin by assuming our automorphism of $G$ has the form $\text{Inn}_A$ for some $A \in \tilde{G}$. We show that $A = a\hat{A}$, where $a \in \tilde{k}$ and $\hat{A} \in G$.

(1) We first show $a_{ri}a_{rj} \in k\forall r, i, j = 1, 2, \ldots, n$. Denote by $X_{n,r}$ the diagonal matrix with 1 in the $[r,r]$ spot and $-1$s elsewhere. It is clear that $X_{n,r}$ is in $G$ and that $I_{n \times n} \in G$ as well. So the entries of $\text{Inn}_A(X_{n,r})$ and $\text{Inn}_A(I_{n \times n})$ as well as the sum of these matrices are in $k$ (even though the sum may not itself be in $G$). Since $A$ is in $\tilde{G}$ we know that $M_n^{-1}(A^T)^{-1}M_n = A$, or equivalently, $A^{-1} = M_n^{-1}(A^T)M_n$. We write

$$
\text{Inn}_A(X) = A^{-1}XA = M_n^{-1}(A^T)M_nXA
$$

in place of $\text{Inn}_A$ in our computations.

Now the $[i, j]$ entry of $\text{Inn}_A(X_{n,r})$ is

$$
-\frac{a_{1i}a_{1j}}{m_i} - a_{2i}a_{2j}\frac{m_2}{m_i} - \cdots + a_{ri}a_{rj}\frac{m_r}{m_i} - \cdots - a_{ni}a_{nj}\frac{m_n}{m_i}
$$
Chapter 5. Involutions of $SO(n, k, \beta)$

and the $[i, j]$ entry of $\text{Inn}_A(I_{n \times n})$ is

$$a_{1i}a_{1j} \frac{1}{m_i} + a_{2i}a_{2j} \frac{m_2}{m_i} + \cdots + a_{ni}a_{nj} \frac{m_n}{m_i}.$$ 

So the $[i, j]$ entry of the difference $\text{Inn}_A(I_{n \times n}) - \text{Inn}_A(X_n, r)$ is $2a_{ri}a_{rj} \frac{m_r}{m_i}$. Since the $m_i$ are in $k$ so is $a_{ri}a_{rj}$.

(2) We show $a_{ri}a_{sj} \in k$ for $r \neq s$. For this we take $m_2 = 1$ since all matrices of symmetric bilinear forms representing our semi-congruence classes can be taken to have at least two 1s on the diagonal when $n$ is odd. The first step is to show $a_{1i}a_{2j} \in k$.

Let $Y_{n, 1}$ be the matrix

$$
\begin{pmatrix}
0 & -1 & 0 & \ldots & 0 \\
1 & 0 & 0 & \ldots & 0 \\
0 & 0 & & & \\
\vdots & \vdots & & \ddots & \\
0 & 0 & & & -I_{n-2 \times n-2}
\end{pmatrix}
$$

and let $Y_{n, 2}$ be

$$
\begin{pmatrix}
0 & 1 & 0 & \ldots & 0 \\
1 & 0 & 0 & \ldots & 0 \\
0 & 0 & & & \\
\vdots & \vdots & & \ddots & \\
0 & 0 & & & -I_{n-2 \times n-2}
\end{pmatrix}
$$

Let $N_{n, i} = \text{Inn}_A(Y_{n, i})$. We have that the $[i, j]$ element of $N_{n, 1}$ and $N_{n, 2}$ are (respectively) $a_{1i}a_{2j} \frac{1}{m_i} - a_{1j}a_{2i} \frac{1}{m_i} + a_{3i}a_{3j} \frac{m_3}{m_i}$ and $a_{1i}a_{2j} \frac{1}{m_i} + a_{1j}a_{2i} \frac{1}{m_i} - a_{3i}a_{3j} \frac{m_3}{m_i}$ resulting in their sum having the form

$$(N_{n, 1} + N_{n, 2})_{i, j} = 2a_{1i}a_{2j}.$$ 

Then $a_{1i}a_{2j} \in k$.

(3) We recall that for each $r = 1, 2, \ldots, n$, by Lemma 17 all we need to show to verify $a_{ri}a_{sj} \in k$ is a single $a_{ri}a_{sj}$ is all we need for each $r > 2$ to get our desired outcome. We make use of the action of $\text{Inn}_{A^{-1}}$. Since $A \in \tilde{G} \implies A^{-1} \in \tilde{G}$, we have the
relation $M_n^{-1}((A^{-1}T)^{-1}M_n = M_n^{-1}A^TM_n = A^{-1}$ which causes $\text{Inn}_{A^{-1}}(X) = AXA^{-1} = AXM_n^{-1}ATM_n$. Also, since $\text{Inn}_{A}$ is bijective onto $G$ it is clear that $\text{Inn}_{A^{-1}}$ must keep $G$ invariant as well. We use the above form of the action of $\text{Inn}_{A^{-1}}$ in our following computations.

We’ll look at the action of $\text{Inn}_{A^{-1}}$ on the matrices $Z_{n,i} := \text{Inn}_{A^{-1}}(Y_{n,i})$. As before, we identify the $[i, j]$ entries of $Z_{n,1}$ and $Z_{n,2}$ as adhering to the formulas

$$-a_{1i}a_{2j}m_j + a_{i1}a_{j2}m_j + \frac{a_{i3}a_{j3}m_j}{m_3} + \cdots + \frac{a_{in}a_{jn}m_j}{m_n}$$

and

$$a_{1i}a_{2j}m_j + a_{i1}a_{j2}m_j - \frac{a_{i3}a_{j3}m_j}{m_3} - \cdots - \frac{a_{in}a_{jn}m_j}{m_n}.$$  

We know that the sum of these elements remain in $k$ by closure, the sum being

$$(Z_{n,1} + Z_{n,2})_{i,j} = 2a_{i1}a_{j2}m_j.$$  

Knowing that $a_{i1}a_{j2} \in k$, we use Lemma 17 to determine that $a_{ri}a_{sj} \in k \forall r \neq s$.

(4) Fix any entry $a_{ij}$ of $A$ and consider the matrix $B = a_{ij}A$. Each element of $B$ has the form $a_{ij}a_{ij}$ and therefore resides in $k$. So $B$ is in GL$(n, k)$. Since $\text{Inn}_A = \text{Inn}_B$, $\text{Inn}_B$ keeps $G$ invariant as well, and consequently $B^{-1}(X^T)^{-1}B \in G$. Substituting $M_n^{-1}(\text{Inn}_B(X)^T)^{-1}M_n = \text{Inn}_B(X) = B^{-1}XB$ and

$$BM_n^{-1}((B^{-1}XB)^T)^{-1}M_nB^{-1} = BM_n^{-1}B^T(X^T)^{-1}(B^T)^{-1}M_nB^{-1}$$

$$= X$$

$$= M_n^{-1}(X^T)^{-1}M_n.$$  

So

$$M_nBM_n^{-1}B^T(X^T)^{-1}(B^T)^{-1}M_nB^{-1}M_n^{-1} = (X^T)^{-1}$$

Taking the transpose and inverse of each side:

$$M_n^{-1}(B^T)^{-1}M_nB^{-1}XBM_n^{-1}B^TM_n = X$$
So

$$\text{Inn}_{BM_3^{-1}B^T M_3} = \text{Id}.$$ 

This means that $BM_n^{-1}B^T M_n = \alpha I_{n \times n}$ for some $\alpha \in \tilde{k}$. Taking determinants of both sides tells us that $\det(B)^2 = (\alpha)^n$ or $\alpha = \sqrt[n]{(\det(B)^2)}$. Let $\hat{B} = \frac{1}{\sqrt[n]{\alpha}} B$. Then

$$\hat{B} M_n^{-1} \hat{B}^T M_n = \left(\frac{1}{\sqrt[n]{(\det(B)^2)}}\right)^2 BM_n^{-1} B^T M_n = \frac{1}{\alpha} I_{n \times n} = I_{n \times n}$$

and $\hat{B} \in O(n, k, \beta)$ since

$$M_n^{-1} \hat{B}^T M_n = \hat{B}^{-1} \implies M_n^{-1} (\hat{B}^T)^{-1} M_n = \hat{B}.$$

We use

$$\hat{A} := \hat{B} = \frac{1}{\sqrt[n]{\alpha}} B = \frac{1}{\sqrt[n]{\alpha}} a_{i,j} A$$

if the determinant of $\hat{B}$ is 1. If the determinant of $\hat{B}$ is $-1$, we use $\hat{A} = -\hat{B} = -\frac{1}{\sqrt[n]{\alpha}} B = -\frac{1}{\sqrt[n]{\alpha}} a_{i,j} A$. Then $\hat{A}$ is still in $O(n, k, \beta)$ and has determinant 1, so it belongs to $G$. Therefore $A = \gamma \hat{A}$, with $\hat{A} \in G$.

\[\Box\]

5.3.6 General Proof of Characterization Theorem Part II, $n$ Even 

The even case will be similar but more challenging due to the constraint of the determinant of elements of $G$ being 1. We use the same $M_n$ as in the odd case.

Proof. (1) We begin by showing $a_{ri}a_{rj} \in k$. As before, assuming Inn$_A$ keeps $G$ invariant, we simplify the induced automorphism Inn$_A(X) = M_n^{-1} A^T M_n X A$ since $A$ is assumed to be in $\tilde{G}$. We use the notation $X_{n,r,s}$ for the diagonal matrix with 1 in the $[r,r]$ and $[s,s]$ positions and $-1$s elsewhere. It is obvious that $I_{n \times n}$ and $X_{n,r,s}$ belong to $G$, which consequently means that the entries of Inn$_A(I_{n \times n})$, Inn$_A(X_{n,r,s})$ and any sum or difference
of these matrices contains entries that must reside in \( k \). We list the formulas for the \([i, j]\) entry of \( \text{Inn}_A(I_{n \times n}) \):

\[
a_{1i}a_{1j} \frac{1}{m_i} + a_{2i}a_{2j} \frac{1}{m_i} + \cdots + a_{ni}a_{nj} \frac{m_n}{m_i}
\]

and the \([i, j]\) entry of \( \text{Inn}_A(X_{n,r,s}) \):

\[
- a_{1i}a_{1j} \frac{1}{m_i} - a_{2i}a_{2j} \frac{1}{m_i} - \cdots - a_{ri}a_{rj} \frac{m_r}{m_i} - \cdots + a_{si}a_{sj} \frac{m_s}{m_i} - \cdots - a_{ni}a_{nj} \frac{m_n}{m_i}.
\]

The sum of these has entries adhering to the formula

\[
2a_{ri}a_{rj} \frac{m_r}{m_i} + 2a_{si}a_{sj} \frac{m_s}{m_i} \in k
\]

This proves that any pair \( a_{ri}a_{rj} \frac{m_r}{m_i} + a_{si}a_{sj} \frac{m_s}{m_i} \) is in the base field for \( r \neq s \).

(2) It is not clear that if we obtain \( a_{1i}a_{1j} \in k \) we also get all \( a_{ri}a_{rj} \in k \) since \( m_i \) is not 1 for \( i > 2 \). So we show that \( a_{3i}a_{3j} \in k \). Use the identity

\[
a_{3i}a_{3j} \frac{m_3}{m_i} = \left( a_{1i}a_{1j} \frac{1}{m_i} + a_{2i}a_{2j} \frac{1}{m_i} + \cdots + a_{ni}a_{nj} \frac{m_n}{m_i} \right)
\]

\[
- (1/2) \left( a_{1i}a_{1j} \frac{1}{m_i} + a_{2i}a_{2j} \frac{1}{m_i} \right)
\]

\[
- (1/2) \left( a_{2i}a_{2j} \frac{1}{m_i} + a_{4i}a_{4j} \frac{m_4}{m_i} \right)
\]

\[
- (1/2) \left( a_{4i}a_{4j} \frac{m_4}{m_i} + a_{5i}a_{5j} \frac{m_5}{m_i} \right) - \cdots
\]

\[
\cdots - (1/2) \left( a_{ni}a_{nj} \frac{m_n}{m_i} + a_{1i}a_{1j} \frac{1}{m_i} \right)
\]

Every combination contained in the parentheses are in \( k \), so that \( a_{3i}a_{3j} \frac{m_3}{m_i} \in k \). Thus, all \( a_{ri}a_{rj} \frac{m_r}{m_i} \in k \), which implies \( a_{ri}a_{rj} \) is in \( k \).

We show that \( a_{ri}a_{sj} \in k \) when \( r \neq s \).
Chapter 5. Involution of $SO(n, k, \beta)$

(3) We first show that $a_{1i}a_{2j} \in k$. Let

$$Y_{n,1} = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ -1 & 0 & 0 & \ldots & 0 \\ 0 & 0 \\ \vdots & \vdots & I_{n-2 \times n-2} \\ 0 & 0 \end{pmatrix}$$

and

$$Y_{n,2} = \begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 1 & 0 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 \\ \vdots & \vdots & \vdots & -I_{n-3 \times n-3} \\ 0 & 0 & 0 \end{pmatrix}$$

It is clear that these matrices belong to $G$.

The $[i, j]$ terms of $\text{Inn}_A(Y_{n,1})$ and $\text{Inn}_A(Y_{n,2})$ are, in order:

$$a_{1i}a_{2j} \left( \frac{1}{m_i} \right) - a_{2i}a_{1j} \left( \frac{1}{m_i} \right) + a_{3i}a_{3j} \left( \frac{m_3}{m_i} \right) + \cdots + a_{ni}a_{nj} \frac{m_n}{m_i}$$

and

$$a_{1i}a_{2j} \left( \frac{1}{m_i} \right) + a_{2i}a_{1j} \left( \frac{1}{m_i} \right) + a_{3i}a_{3j} \left( \frac{m_3}{m_i} \right) - a_{4i}a_{4j} \left( \frac{m_4}{m_i} \right) - \cdots - a_{ni}a_{nj} \frac{m_n}{m_i}.$$

The entries of the sum of these, which must belong to $k$, are

$$2a_{1i}a_{2j} \left( \frac{1}{m_i} \right) + 2a_{3i}a_{3j} \left( \frac{m_3}{m_i} \right) .$$

Using our discovery that $a_{ri}a_{rj} \in k$ we achieve $2a_{1i}a_{2j} \left( \frac{1}{m_i} \right) \in k$ and ultimately $a_{1i}a_{2j} \in k$.

(4) To conclude decisively that all $a_{ri}a_{sj}$ live back in $k$ it is sufficient to show that the specific entries $a_{r1}a_{12}$ belong to $k$ for each $r \neq 1, 2$ and then apply Lemma 17. Recalling
that $\text{Inn}_{A^{-1}}$ must keep $G$ invariant, we investigate the action of $\text{Inn}_{A^{-1}}$ on $Y_{n,1}, Y_{n,2}$ and also on some other matrices which we need to utilize. Let

$$Y_{n,3} := \begin{pmatrix} 0 & -1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \vdots & \vdots & I_{n-2 \times n-2} \\ 0 & 0 & \vdots & \vdots \\ \end{pmatrix}$$

and

$$Y_{n,4} := \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \vdots & \vdots & -I_{n-3 \times n-3} \\ 0 & 0 & 0 & \vdots & \vdots & \vdots \\ \end{pmatrix}.$$

For the image values of $\text{Inn}_{A^{-1}}$ acting on these matrices of $G$, we see that the formula identifying the $[i, j]$ term for each case differs only in the location of the sole negative term. For convenience, we’ll use the notation $Z_{n,i} := \text{Inn}_{A^{-1}}(Y_{n,i})$. Again, we use the formula $\text{Inn}_{A^{-1}}(X) = AXM_{n}^{-1}A^{T}M_{n}$ since $A^{-1} \in \tilde{G}$.

$$(Z_{n,1})_{ij} = a_{i1}a_{j2}m_j - a_{i2}a_{j1}m_j + a_{i3}a_{j3}\frac{m_j}{m_3} + \cdots + a_{in}a_{jn}\frac{m_j}{m_n}$$

$$(Z_{n,2})_{ij} = a_{i1}a_{j2}m_j + a_{i2}a_{j1}m_j - a_{i3}a_{j3}\frac{m_j}{m_3} + \cdots + a_{in}a_{jn}\frac{m_j}{m_n}$$

$$(Z_{n,3})_{ij} = -a_{i1}a_{j2}m_j + a_{i2}a_{j1}m_j + a_{i3}a_{j3}\frac{m_j}{m_3} + \cdots + a_{in}a_{jn}\frac{m_j}{m_n}$$

$$(Z_{n,4})_{ij} = a_{i1}a_{j2}m_j + a_{i2}a_{j1}m_j + a_{i3}a_{j3}\frac{m_j}{m_3} - a_{i4}a_{j4}\frac{m_j}{m_4} - \cdots - a_{in}a_{jn}\frac{m_j}{m_n}$$

Adding $Z_{n,1}$ and $Z_{n,2}$ and subtracting $Z_{n,1}$ from $Z_{n,2}$ provides

$$(Z_{n,1} + Z_{n,2})_{ij} = 2a_{i3}a_{j3}\frac{m_j}{m_3} + 2a_{i4}a_{j4}\frac{m_j}{m_4} + \cdots + 2a_{in}a_{jn}\frac{m_j}{m_n}$$
and

$$(Z_{n,2} - Z_{n,1}),_j = 2a_{i2}a_{j1}m_j - 2a_{i3}a_{j3} \frac{m_j}{m_3}$$

both of which terms are in $k$. Finally, adding $Z_{n,3} + Z_{n,4}$ the $[i, j]$ term is

$$2a_{i2}a_{j1}m_j + 2a_{i3}a_{j3} \frac{m_j}{m_3}.$$

It is obvious that the 2s are irrelevant and can be divided out (here we make use of the assumption that $\text{char } k \neq 2$). We subtract out each of these sums/differences from $(Z_{n,1})_{i,j}$ and find that it simplifies to the product of the $a_{i,j}$ entries we were seeking to isolate:

$$a_{i1}a_{j2}m_j = \left( a_{i1}a_{j2}m_j - a_{i2}a_{j1}m_j + a_{i3}a_{j3} \frac{m_j}{m_3} + \cdots + a_{in}a_{jn} \frac{m_j}{m_n} \right)$$

$$- \left( a_{i3}a_{j3} \frac{m_j}{m_3} + a_{i4}a_{j4} \frac{m_j}{m_4} + \cdots + a_{in}a_{jn} \frac{m_j}{m_n} \right)$$

$$+ (1/2) (a_{i2}a_{j1}m_j + a_{i3}a_{j3}) + (1/2) (a_{i2}a_{j1}m_j - a_{i3}a_{j3})$$

Each of the three combinations of terms inside the parentheses have just been shown to belong to $k$. Therefore, $a_{i1}a_{j2}m_j$ and consequently $a_{i1}a_{j2}$ are in the field $k$. We apply Lemma 17 with $a_{31}a_{12} \in k$ to get all combinations $a_{3i}a_{sj}$ for $s = 1, 2$ and the continue in an inductive fashion applying the lemma to $a_{4i}a_{12}$ to obtain $a_{4i}a_{sj}$ for $s = 1, 2, 3$, and so on. In this fashion we find all combinations $a_{ri}a_{sj}$ belonging to $k$.

(5) Similar to the method used for the odd case, we fix any entry $a_{i,j}$ of $A$ and consider the matrix $B = a_{i,j}A$. Each element of $B$ has the form $a_{i,j}a_{ij}$ and therefore resides in $k$ since we endured numerous computations just to show that $a_{ri}a_{sj}$ are all in $k$. So $B$ is in $\text{GL}(n, k)$. Since $\text{Inn}_A = \text{Inn}_B$, $\text{Inn}_B$ keeps $G$ invariant as well, and consequently $B^{-1}XB \in G \forall X \in G$. Performing $\theta_{M_n}$ on $\text{Inn}_B(X)$ ($X \in G$) we find $M_n^{-1}(\text{Inn}_B(X)^T)^{-1}M_n = \text{Inn}_B(X) = B^{-1}XB,$
$M_n^{-1}((B^{-1}XB)\,^T)^{-1}M_n = M_n^{-1}B\,^T\,(X\,^T)^{-1}(B\,^T)^{-1}M_n$

$= B^{-1}XB$

so that

$BM_n^{-1}B\,^T\,(X\,^T)^{-1}(B\,^T)^{-1}M_nB^{-1} = X = M_n^{-1}(X\,^T)^{-1}M_n$.

Equating these expressions of $(X\,^T)^{-1}$ produces

$M_nBM_n^{-1}B\,^T\,(X\,^T)^{-1}(B\,^T)^{-1}M_nB^{-1}M_n^{-1} = (X\,^T)^{-1}$

Taking the transpose and inverse of each side shows:

$M_n^{-1}(B\,^T)^{-1}M_nB^{-1}XB\,M_n^{-1}B\,^T\,M_n = X$.

So

$\text{Inn}_{BM_n^{-1}B\,^T\,M_n} = \text{Id}$.

This means that $BM_n^{-1}B\,^T\,M_n = \alpha I_{n\times n}$ for some $\alpha \in \mathbb{k}$. Taking determinants of both sides tells us that $\det(B)^2 = (\alpha)^n$ or $\alpha = \sqrt[n]{\det(B)^2}$. Let $\hat{B} = \frac{1}{\sqrt[n]{\alpha}}B$. Then

$\hat{B}\,M_n^{-1}\hat{B}\,^T\,M_n = \left(\frac{1}{\sqrt[n]{\det(B)^2}}\right)^2 BM_n^{-1}B\,^T\,M_n$

$= \frac{1}{\alpha}I_{n\times n}$

$= I_{n\times n}$

and $\hat{B} \in O(n, k, \beta)$ since

$M_n^{-1}\hat{B}\,^T\,M_n = \hat{B}^{-1} \implies M_n^{-1}(\hat{B}\,^T)^{-1}M_n = \hat{B}$. 

We use
\[ \hat{A} := \hat{B} = \frac{1}{\sqrt{\alpha}} B = \frac{1}{\sqrt{\alpha}} a_{i;j} A \]
if the determinant of \( \hat{B} \) is 1. If the determinant of \( \hat{B} \) is \(-1\) we cannot always change it to 1 since \( \hat{A} := \frac{1}{\sqrt{-1}} \hat{B} \)–although having \( \det(\hat{A}) = \frac{1}{n/2} \sqrt{-1} \)
\( \hat{B} \)–will no longer be in \( O(n, k, \beta) \):
\[
\hat{A} M_n^{-1} \hat{A}^T M_n = \left( \frac{1}{\sqrt{-1}} \right)^2 \hat{B} M_n^{-1} \hat{B}^T M_n = \frac{1}{n/2} I_{n \times n}
\]
Therefore \( A = \gamma \hat{A} \), with \( \hat{A} \in G \) or \( \hat{A} \in O(n, k, \beta) \) and \( \det(\hat{A}) = -1 \).

The main summary of these results in the odd case is an important one in classifying those automorphisms that are also involutions. It will give us a start on a method for classifying involutions of \( \text{SO}(n, k, \beta) \).

**Corollary 4.** When \( n \) is odd, all automorphisms of \( \text{SO}(n, k, \beta) \) are inner for any non-degenerate symmetric bilinear form \( \beta \) with matrix \( M \) satisfying the criteria of Lemma 15.

**Proof.** All automorphisms of \( \text{SO}(n, k, \beta) \) can be written as a conjugation by a matrix \( A \in \text{GL}(n, \bar{k}) \) by Remark 10 when \( M \) may be written with a 1 in the \( [1, 1] \) and \( [2, 2] \) entries. By the first part of the Characterization Theorem 5.2 proven in this chapter, we can take the matrix \( A \) to belong to \( \tilde{G} \). Then \( \text{Inn}_A \) being an automorphism of \( G \) means \( A = \alpha \hat{A} \) for some \( \alpha \in \bar{k} \) and some \( \hat{A} \in G \). So the automorphism equals \( \text{Inn}_A = \text{Inn}_{\hat{A}} \), \( \hat{A} \) is in \( G \), and the automorphism is inner over \( G = \text{SO}(n, k, \beta) \).

In summary, we’ve discovered that all automorphisms (and hence all involutions) of \( G \) may be taken to be conjugations \( \text{Inn}_A \) for some \( A \in G \) when \( n > 4 \) and \( k = \bar{k}, \mathbb{R}, \mathbb{F}_p \) \( p \neq 2, \mathbb{Q}_p \) and that this is also true when \( n = 2 \) or \( n = 3 \) and the matrix \( M \) of the form \( \beta \) is not \( M_3, p, s_p, p s_p \), \( M_4, p, s_p, p s_p \) over \( \mathbb{Q}_p \) or \( M_3, 2, 3, 6 \), \( M_4, 2, 3, 6 \) over \( \mathbb{Q}_2 \). We’ve also seen that any automorphism over \( G \) where \( n \) is even can be taken to be “almost inner” under these choices for \( M \) in the sense that we can take the matrix to be in \( \text{O}(n, k, \beta) \) even if we may not assume that the determinant of \( A \) is \(-1\).
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

5.4 Results for $G = \text{SO}(n, k, \beta), n$ Odd

5.4.1 Some Theory for $G = \text{SO}(n, k, \beta), n$ Odd

We’ve found that all involutions of $G$ are inner when $n$ is odd except in the rare cases when $M$ may not be represented as $M = \text{diag}(1, 1, m_3, \ldots, m_n)$. We must check which involutions of $\text{SL}(n, k)$ remain involutions when restricted to $G$. The following lemma will be helpful.

**Lemma 18.** Let $\phi$ be an involution of $\text{SL}(n, k)$ coming from a symmetric bilinear form over $V = k^n$ (char $k \neq 2$) with representative matrix $M$ adhering to the criteria of Lemma 15 and $G$ its corresponding fixed-point group. So $\phi$ is the outer involution $\text{Inn}_M$ theta where $\theta(X) = (X^T)^{-1}$. Then the involution $\tau$ of $\text{SL}(n, k)$ keeps $G$ invariant (i.e. is still an involution when restricted to $G$) $\iff \tau \phi = \phi \tau$ on $\text{SL}(n, k)$.

**Proof.** $\iff$: Suppose $\tau \phi = \phi \tau$ on $\text{SL}(n, k)$. Then they are equal on $G$ as well. Since $\tau \phi(X) = \tau(X)$ and $\phi \tau(X) = \tau \phi(X) = \tau(X) \forall X \in G$, it is seen that $\tau(X)$ is in the fixed-point group of $\phi$. In other words, $\tau(X) \in G$ and $\tau$ keeps $G$ invariant.

$\implies$: Suppose $\tau$ keeps $G$ invariant. Then $\tau = \text{Inn}_A$ for some $A \in G$, so that this matrix $A$ which gives the conjugation has $A = M^{-1}(A^T)^{-1} M$. So

$$
\tau \phi(X) = \text{Inn}_A \phi(X) = \text{Inn}_A(M^{-1}(X^T)^{-1} M) = A^{-1}M^{-1}(X^T)^{-1} MA
$$

and

$$
\phi \tau(X) = \phi \text{Inn}_A(X) \\
= \phi(A^{-1}XA) \\
= M^{-1}((A^{-1}XA)^T)^{-1}M \\
= M^{-1}A^T(X^T)^{-1}(A^T)^{-1}M.
$$

We substitute $A^T = MA^{-1}M^{-1}$ and $(A^T)^{-1} = MAM^{-1}$ into the second equation and obtain

$$
\phi \tau(X) = M^{-1}(MA^{-1}M^{-1})(X^T)^{-1}(MAM^{-1})M
$$
or
\[ \phi \tau(X) = A^{-1}M^{-1}(X^T)^{-1}MA = \tau \phi(X) \quad \forall X \in G \]

The previous results help us determine which inner and outer involutions of \( SL(n, k) \) remain involutions on \( G \), but it does not tell us which involution classes remain intact when restricted to \( G \).

**Remark 12.**
(1) All involutions of \( G \) are restrictions of either inner or outer involutions of \( SL(n, k) \).

(2) All involutions of \( G \) come from bilinear symmetric forms.

Note that when we showed all involutions of \( G \) are inner over \( G \) (for a given bilinear form \( \beta \) and its matrix \( M \) satisfying Lemma 15), we obtained that all involutions of \( G \) come from bilinear symmetric forms. Any inner involution of \( G \) has the form \( \text{Inn}_A \) for some matrix \( A \in G \). We can view the involution as the restriction of the outer involution \( \text{Inn}_A = \text{Inn}_A \theta_M = \text{Inn}_A \text{Inn}_M \theta (\theta(X) = (X^T)^{-1}) \) of \( SL(n, k) \) to \( G \) or the restriction of the inner involution \( \text{Inn}_A \) of \( SL(n, k) \) to \( G \). It is therefore the same as the outer involution of \( SL(n, k) \) coming from the form with matrix \( AM \) restricted to \( G \). This matrix will still be symmetric since the matrices representing both the inner and outer classes over \( SL(n, k) \) are diagonal when \( n \) is odd.

### 5.4.2 Some Results for \( G = SO(n, k), \ n \text{ Odd} \)

**Theorem 5.3.** Let \( \theta \) be the involution on \( SL(n, k) \) defined by \( \theta(X) = (X^T)^{-1} \). Let \( \tau \) and \( \phi \) be involutions of \( SO(n, k) \) coming from symmetric bilinear forms on \( V = k^n \) with matrices \( M_1 \) and \( M_2 \), respectively, where \( n \) is odd and the orthogonal group is taken with respect to the standard dot product (i.e. \( SO(n, k) \) is the fixed-point group of \( \theta \)). Then \( \tau \approx \phi \) over \( SO(n, k) \) \iff \( M_2 = \alpha Q^T M_1 Q \) for some \( Q \in SL(n, k) \) and \( M_2 = \alpha Q^{-1} M_1 Q \), where this \( Q \) and \( \alpha \) are the same \( Q \in SL(n, k), \alpha \in \bar{k} \) in each equation.
Chapter 5. Involutionsof \( SO(n, k, \beta) \)

**Proof.** \( \iff \) Given that \( M_2 = \alpha Q^T M_1 Q \) we know that \( M_2 \cong_s M_1 \) over \( G \), which implies \( \tau \approx \phi \) over \( G \).

\( \implies \): Suppose \( \tau \approx \phi \) over \( G = SO(n, k) \). The involutions \( \tau \) and \( \phi \) can be viewed as the restrictions of the inner involutions \( \text{Inn}_{M_1} \) and \( \text{Inn}_{M_2} \) of \( SL(n, k) \) (respectively) to \( G \). Since \( \text{Inn}_{M_1} \approx \text{Inn}_{M_2} \) via a matrix in \( G \), we know that \( M_2 = \alpha Q^{-1} M_1 Q \) for some \( Q \in G \) and \( \alpha \in \kappa \). We can also view \( \tau \) and \( \phi \) as the restrictions of the outer involutions \( \text{Inn}_{M_1} \theta \) and \( \text{Inn}_{M_2} \theta \) (respectively) of \( SL(n, k) \) to \( G \). Then there is a matrix \( \hat{Q} \in G \) and a scalar \( \hat{\alpha} \) such that \( M_2 = \hat{\alpha} (\hat{Q}^T) M_1 \hat{Q} \). Since \( \hat{Q} \in G \), \( \hat{Q}^T = \hat{Q}^{-1} \) and the equation becomes \( M_2 = \hat{\alpha} (\hat{Q}^{-1}) M_1 \hat{Q} \). Equating these two different forms for \( M_2 \) yields \( \hat{\alpha} (\hat{Q}^{-1}) M_1 \hat{Q} = \alpha Q^{-1} M_1 Q \), which implies \( \hat{\alpha} Q^{-1} M_1 Q (\hat{Q})^{-1} = M_1 \). Since this works for all symmetric bilinear forms with matrix \( M_1 \), we have that \( \text{Inn}_{Q(\hat{Q})^{-1}} = \text{Id} \) and \( Q = c\hat{Q} \). Equating determinants shows that \( c = 1 \) since \( \det Q = \det \hat{Q} = 1 \) and \( n \) is odd. Combining results we have \( M_2 = \hat{\alpha} Q^T M_1 Q = \alpha Q^{-1} M_1 Q \) and \( \det(M_2) = (\hat{\alpha})^n \det(M_1) = (\alpha)^n \det(M_1) \), so that \( \hat{\alpha} = \alpha \) (since \( n \) is odd). Therefore \( M_2 = \alpha Q^T M_1 Q = \alpha Q^{-1} M_1 Q \). \( \square \)

**Remark** 13. One isomorphism class of inner or outer involutions on \( SL(n, k) \) may split into 2 or more isomorphism classes when restricted to act upon \( SO(n, k, \beta) \) for a general non-degenerate symmetric bilinear form \( \beta \).

We can see the validity of this remark by using our theorem for \( SO(n, k) \), where \( \beta \) is the standard inner product with matrix \( M = I_{n \times n} \). Let’s look at some useful consequences of the criteria given in the theorem. Let \( G = SO(n, k) \) :

\( k = \tilde{k} \) :

When our field is algebraically closed, all matrices \( M_1 \) and \( M_2 \) are congruent to \( I_{n \times n} \) and so also semi-congruent to \( I_{n \times n} \). So this half of our criteria for isomorphic involutions provides no restrictions. Therefore, the isomorphism classes of inner involutions of \( SL(n, \tilde{k}) \) remain intact. There is exactly one isomorphism class of involutions of \( G \) for each class of inner involutions of \( SL(n, \tilde{k}) \).
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

Example 5.4. This illustrates the previous remark concerning the splitting of classes of involutions under restriction to $G$. There is only one outer involution up to isomorphism over $\text{SL}(n, \bar{k})$, represented by the identity matrix. Yet restricted to $G$ this class splits into $\frac{n-1}{2}$ classes given by the matrices $M = I_{n-i,i} \ i = 1, 2, \ldots, \frac{n-1}{2}$. The isomorphism classes of the inner involutions of $\text{SL}(n, \bar{k})$ remain intact, however. This is not always the case as the inner classes may split as well.

$k = \mathbb{R}$:

Over the real numbers, our inner and outer classes of involutions on $\text{SL}(n, k)$ were identical with the one exception of the choice of the matrix $M = I_{n \times n}$. When restricted to $G = \text{SO}(n, k)$, however, the outer involution $\text{Inn}_M \theta$ is the identity, which is not an involution. In this fashion we see that there is exactly one isomorphism class of involutions on $G$ for each class of inner involutions on $\text{SL}(n, k)$. On the other hand, there is one less class of outer involutions under restriction to $G$. The involutions come from the forms with representative matrices $I_{n-i,i} \ i = 1, 2, \ldots, \frac{n-1}{2}$.

Remark 14. Although some of the matrices $I_{n-i,i}$ are not technically in $G$ since they have determinant $-1$, we can always multiply a given matrix by $-1$ and get a matrix in $G$ since $n$ is odd. Rather than develop a new notation, we use the matrices $I_{n-i,i}$ for consistent notation with our results for $\text{SL}(n, k)$ with this understanding of the technicality of the determinant of our matrix $M$.

$k = \mathbb{F}_p \ (p \neq 2)$:

In this situation we will see that a class of inner involutions on $\text{SL}(n, k)$ may split into different classes over $G = \text{SO}(n, k)$ as well as the outer involution classes. Recall that the two classes of inner involutions on $\text{SL}(n, k)$ are represented by the matrices of the bilinear forms given by $M = I_{n \times n}$ and $M_{n,1,1,Sp}$. For each isomorphism class of inner involutions on $\text{SL}(n, k)$, some of the matrices representing this class will be semi-congruent to the identity matrix while others will be semi-congruent to $M_{n,1,1,Sp}$. Therefore each class of
inner involutions splits into 2 classes when restricted to $G$. There are exactly 2 isomorphism classes of involutions on $G$ for each class of inner involutions on $\text{SL}(n,k)$. The inner and outer classes of involutions of $\text{SL}(n,k)$ split into disparate classes when restricted to $G$.

**Example 5.5.** Let $G = \text{SO}(3, \mathbb{F}_p)$. The matrices $M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $M_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ both represent the same class of inner involutions on $\text{SL}(3, \mathbb{F}_p)$. They represent different classes of involutions on $G$, however, since $M_1 \cong^s I_{3\times 3}$ while $M_2 \cong^s M_{3,1,1,Sp}$. This illustrates the splitting of an inner class of involutions of $\text{SL}(3, \mathbb{F}_p)$ under restriction to $G$.

**5.4.3 More Theory for $G = \text{SO}(n, k, \beta)$, $n$ Odd**

Now we have seen how some of these tools may be used for the standard special orthogonal group $\text{SO}(n,k)$ when $n$ is odd. We return to the general case once more to develop more machinery for the more complicated situation where $\beta$ is any non-degenerate symmetric bilinear form.

The following theorems are generalizations of theorems given in [Wu02] for $\text{SO}(n,k)$ for odd $n$, where we generalize the situation to $G = \text{SO}(n,k,\beta)$ where $\beta$ is any non-degenerate symmetric bilinear form whose matrix is not one of the $3 \times 3$ or $4 \times 4$ matrices over $\mathbb{Q}_p$ singled out by Lemma 15, so we use a similar notation. In the following it is assumed that $\theta$ is the involution $\theta(X) = (X^T)^{-1}$.

**Theorem 5.4.** Let $\beta_1$ be a non-degenerate symmetric bilinear form over $V = k^n$ (where $n$ is odd and $k$ is any field whose characteristic is not 2) with matrix $M_1$, satisfying the criteria of Lemma 15 and let $G = \text{SO}(n,k,\beta_1)$ be its special orthogonal group. Suppose that $\phi$ is an involution of $G$ induced by the non-degenerate bilinear form $\beta_2$ with representative matrix $M_2$. Then there exists a matrix $A \in G$ such that $\phi = \text{Inn}_A = \text{Inn}_{M_2} \theta$ on $G$ and $A = X^{-1} I_{n-i,i} X$, where $X \in \text{GL}(n,k)$ with $XM_1^{-1}X^T$ a diagonal matrix.

**Proof.** We know from the Characterization Theorem 5.2 that $\phi = \text{Inn}_A$ for some $A \in G$. 

If $\text{Inn}_A$ is an involution then $\text{Inn}_{A^2} = \text{Id}$ on $G$ and then Theorem 5.1 tells us that we must have $A^2 = aI_{n \times n}$. Since $A$ has determinant 1 and $n$ is odd, $a = 1$ and $A^2 = I_{n \times n}$. This means that the eigenvalues of $A$ satisfy $\lambda^2 = 1$ and must be either 1 or $-1$. Thus, $A$ is seen to be similar to $I_{n-i,i}$ and there is a matrix $Y \in \text{GL}(n, k)$ such that $A = Y^{-1}I_{n-i,i}Y$. Since $A \in G$,

$$M_1^{-1}((Y^{-1}I_{n-i,i}Y)^T)^{-1}M_1 = Y^{-1}I_{n-i,i}Y.$$  

Since $(I_{n-i,i}^T)^{-1} = I_{n-i,i}$ we have

$$M_1^{-1}Y^T I_{n-i,i}(Y^T)^{-1}M_1 = Y^{-1}I_{n-i,i}Y,$$

or

$$YM_1^{-1}Y^T I_{n-i,i} = I_{n-i,i}YM_1^{-1}Y^T$$

since $I_{n-i,i}^{-1} = I_{n-i,i}$. This means that $YM_1^{-1}Y^T = \begin{pmatrix} Y_1 & 0 \\ 0 & Y_2 \end{pmatrix}$. Furthermore, $YM_1^{-1}Y^T$ is symmetric since $(YM_1^{-1}Y^T)^T = Y(M_1^{-1})^TY^T = YM_1^{-1}Y^T$ (recall that $M_1$ is symmetric), ensuring that $Y_1^T = Y_1$ and $Y_2^T = Y_2$. Symmetric matrices are congruent to diagonal matrices, so there exists a matrix $N \in \text{GL}(n, k)$ such that $NYM_1^{-1}Y^TN^T$ is diagonal.

Due to the form of $YM_1^{-1}Y^T = \begin{pmatrix} Y_1 & 0 \\ 0 & Y_2 \end{pmatrix}$ we may also assume that $N$ has the form

$$N = \begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix}.$$  

We let $X = NY$ and conclude that this $X$ satisfies the conditions stated in the theorem:

(1)  

$$X M_1^{-1}X^T = NYM_1^{-1}Y^TN^T$$

which is diagonal.
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

(2)

$$X^{-1}I_{n-i,i}X = (NY)^{-1}I_{n-i,i}NY = Y^{-1}N^{-1}I_{n-i,i}NY$$

$$= Y^{-1} \begin{pmatrix} N_1^{-1}N_1 & 0 \\ 0 & N_2^{-1}N_2 \end{pmatrix} Y$$

$$= Y^{-1}I_{n-i,i}Y = A$$

\[\square\]

**Theorem 5.5.** Let $\beta_1$, $\beta_2$, and $\beta_3$ be non-degenerate symmetric bilinear forms over $V = k^n$ (where $n$ is odd and $k$ is any field whose characteristic is not 2) with matrices $M_1$, $M_2$, and $M_3$ (respectively), where $M_1$ satisfies Lemma 15. Let $G = \text{SO}(n, k, \beta_1)$ be the special orthogonal group corresponding to $\beta_1$. Suppose that $\phi$ and $\tau$ are the involutions of $G$ induced by the forms $\beta_2$ and $\beta_3$ (respectively). Let $A$ and $B$ be matrices such that $\phi = \text{Inn}_A = \text{Inn}_{M_2}\theta$ and $\tau = \text{Inn}_B = \text{Inn}_{M_3}\theta$ on $G$ with $A = X^{-1}I_{n-i,i}X$, $B = Y^{-1}I_{n-i,i}Y$, and

$$XM_1^{-1}X^T = \begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_n \end{pmatrix}, \quad YM_1^{-1}Y^T = \begin{pmatrix} b_1 & 0 & \ldots & 0 \\ 0 & b_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & b_n \end{pmatrix}.$$  

Then the following are equivalent statements:

(1) $\phi \approx \tau$ over $G$.

(2) $B = Q^{-1}AQ$ via a matrix $Q \in G$. 
Chapter 5. Involutions of SO(n, k, \beta)  

(3) 

\[
\begin{pmatrix}
 a_{1} & 0 & \ldots & 0 \\
 0 & a_{2} & \ldots & 0 \\
 \vdots & \vdots & \ddots & \vdots \\
 0 & 0 & \ldots & a_{n-i}
\end{pmatrix}
\begin{pmatrix}
 b_{1} & 0 & \ldots & 0 \\
 0 & b_{2} & \ldots & 0 \\
 \vdots & \vdots & \ddots & \vdots \\
 0 & 0 & \ldots & b_{n-i}
\end{pmatrix}
\sim
\begin{pmatrix}
 a_{n-i+1} & 0 & \ldots & 0 \\
 0 & a_{n-i+2} & \ldots & 0 \\
 \vdots & \vdots & \ddots & \vdots \\
 0 & 0 & \ldots & a_{n}
\end{pmatrix}
\begin{pmatrix}
 b_{n-i+1} & 0 & \ldots & 0 \\
 0 & b_{n-i+2} & \ldots & 0 \\
 \vdots & \vdots & \ddots & \vdots \\
 0 & 0 & \ldots & b_{n}
\end{pmatrix}
\]

and

Proof. We show that (1) and (2) are equivalent, and then show that (2) $\implies$ (3) and vice versa through separate arguments to complete the equivalence.

(1) $\implies$ (2): We know that if $\phi \approx \tau$ over $G$ then the inner involutions $\phi = \text{Inn}_A$ and $\tau = \text{Inn}_B$ are isomorphic over SL(n, k), via the same matrix $Q \in G$, ensuring that $A$ is conjugate to $B$ times a scalar (i.e. $A = \alpha Q^{-1} B Q$ for some $\alpha \in \bar{k}$). Since all determinants of these matrices are 1, it is clear that $\alpha = 1$ and $A = Q^{-1} B Q$.

(2) $\implies$ (1): If $A = Q^{-1} B Q$ via a matrix $Q \in G$ then $\text{Inn}_A = \text{Inn}_Q^{-1} B \text{Inn}_Q = \text{Inn}_Q^{-1} \text{Inn}_B \text{Inn}_Q$ and $\phi \approx \tau$ over $G$.

(2) $\implies$ (3): Assume that there exists a matrix $Q \in G$ such that $B = Q^{-1} A Q$. In terms of the component matrices $X$ and $Y$ of $A$ and $B$ this means that

\[Q^{-1} X^{-1} I_{n-i,i} X Q = Y^{-1} I_{n-i,i} Y\]

or equivalently,

\[I_{n-i,i} X Q Y^{-1} = X Q Y^{-1} I_{n-i,i}, \implies X Q Y^{-1} = I_{n-i,i} X Q Y^{-1} I_{n-i,i}.\]

So $X Q Y^{-1} = \begin{pmatrix} Q_1 & 0 \\ 0 & Q_2 \end{pmatrix}$ where $Q_1$ is of dimension $n - i \times n - i$ and $Q_2$ is an $i \times i$
matrix. Then \(XQ = \begin{pmatrix} Q_1 & 0 \\ 0 & Q_2 \end{pmatrix} Y\). We know that
\[
M_1^{-1}(Q^T)^{-1}M_1 = Q, \quad \implies M_1^{-1} = QM_1^{-1}Q^T
\]

which causes
\[
XM_1^{-1}X^T = XQ M_1^{-1}Q^TX^T = \left( \begin{pmatrix} Q_1 & 0 \\ 0 & Q_2 \end{pmatrix} Y \right) M_1^{-1} \left( Y^T \begin{pmatrix} Q_1^T & 0 \\ 0 & Q_2^T \end{pmatrix} \right).
\]

So we confirm the relation
\[
\begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_n \end{pmatrix} = \begin{pmatrix} b_1 & 0 & \ldots & 0 \\ 0 & b_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & b_n \end{pmatrix} \begin{pmatrix} Q_1^T & 0 \\ 0 & Q_2^T \end{pmatrix}.
\]

This is only possible if
\[
\begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_{n-i} \end{pmatrix} = Q_1 \begin{pmatrix} b_1 & 0 & \ldots & 0 \\ 0 & b_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & b_{n-i} \end{pmatrix} Q_1^T
\]

and
\[
\begin{pmatrix} a_{n-i+1} & 0 & \ldots & 0 \\ 0 & a_{n-i+2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_n \end{pmatrix} = Q_2 \begin{pmatrix} b_{n-i+1} & 0 & \ldots & 0 \\ 0 & b_{n-i+2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & b_n \end{pmatrix} Q_2^T.
\]
Thus,

\[
\begin{pmatrix}
a_1 & 0 & \ldots & 0 \\
0 & a_2 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & a_{n-i}
\end{pmatrix}
\begin{pmatrix}
b_1 & 0 & \ldots & 0 \\
0 & b_2 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & b_{n-i}
\end{pmatrix}
\]

and

\[
\begin{pmatrix}
a_{n-i+1} & 0 & \ldots & 0 \\
0 & a_{n-i+2} & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & a_n
\end{pmatrix}
\begin{pmatrix}
b_{n-i+1} & 0 & \ldots & 0 \\
0 & b_{n-i+2} & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & b_n
\end{pmatrix}
\]

(3) $\implies$ (2): Suppose there is an $n - i \times n - i$ matrix $Q_1$ and an $i \times i$ matrix $Q_2$ such that

\[
\begin{pmatrix}
a_1 & 0 & \ldots & 0 \\
0 & a_2 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & a_{n-i}
\end{pmatrix}
= Q_1
\begin{pmatrix}
b_1 & 0 & \ldots & 0 \\
0 & b_2 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & b_{n-i}
\end{pmatrix}
Q_1^T
\]

and

\[
\begin{pmatrix}
a_{n-i+1} & 0 & \ldots & 0 \\
0 & a_{n-i+2} & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & a_n
\end{pmatrix}
= Q_2
\begin{pmatrix}
b_{n-i+1} & 0 & \ldots & 0 \\
0 & b_{n-i+2} & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & b_n
\end{pmatrix}
Q_2^T.
\]

Denote by $Q$ the matrix $\begin{pmatrix} Q_1 & 0 \\ 0 & Q_2 \end{pmatrix}$ and let $Z = X^{-1}QY$. Then $A$ and $B$ are conjugate via
this $Z$:

\[
Z^{-1}AZ = (X^{-1}QY)^{-1}A(X^{-1}QY)
= Y^{-1}Q^{-1}XAX^{-1}QY
= Y^{-1}Q^{-1}X(X^{-1}I_{n-i,i}X)X^{-1})QY
= Y^{-1}Q^{-1}I_{n-i,i}QY
= Y^{-1}\begin{pmatrix}
1 & 0 \\
0 & -Q_2^{-1}Q_1
\end{pmatrix}Y
= Y^{-1}I_{n-i,i}Y = B
\]

Now we simply need to check that $Z \in G$.

\[
ZM_1^{-1}Z^TM_1 = X^{-1}QYM_1^{-1}Y^TQ^T(X^T)^{-1}M_1
= X^{-1}Q\begin{pmatrix}
b_1 & 0 & \ldots & 0 \\
0 & b_2 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & b_n
\end{pmatrix}Q^T(X^T)^{-1}M_1
= X^{-1}(XM_1^{-1}X^T)(X^T)^{-1}M_1 = M_1^{-1}M_1 = I_{n \times n}
\]

Therefore,

\[
ZM_1^{-1}Z^TM_1 = I_{n \times n}, \implies Z^{-1} = M_1^{-1}Z^TM_1, \implies M_1^{-1}(Z^T)^{-1}M_1 = Z
\]

so $Z \in O(n, k, \beta_1)$. If $\det(Z) = 1$, then $A$ is conjugate to $B$ via $Z \in G$. If $\det(Z) = -1$, then we replace $Z$ by $-Z$ and the above equations do not change as each sign change is countered by a second sign change in the same equation (so we still have $Z \in O(n, k, \beta_1)$). Since $n$ is assumed to be odd, $\det(-Z) = -\det(Z) = 1$ and it is seen that $Z \in G$. Hence, $B = Z^{-1}MZ$ and $A$ is conjugate to $B$ over $G$. This shows $(2) \iff (3)$ and completes the proof as the equivalence of $(1)$ and $(2)$ has already been shown. □
Chapter 5. Involutions of $\text{SO}(n, k, \beta)$

With this theorem we can see the results we found earlier for $G = \text{SO}(n, k)$ where $\beta$ is the standard dot product on $V = k^n$. For instance, for $k = \mathbb{F}_p$ we had that the classes of inner involutions on $\text{SL}(n, \mathbb{F}_p)$ split into 2 different classes under restriction to $G$, depending on the semi-congruence classes of their representative matrices. These 2 classes come from looking at the 2 congruence classes of

$$
\begin{pmatrix}
a_1 & 0 & \cdots & 0 \\
0 & a_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & a_{n-i}
\end{pmatrix}
$$

and

$$
\begin{pmatrix}
a_{n-i+1} & 0 & \cdots & 0 \\
0 & a_{n-i+2} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & a_n
\end{pmatrix}
$$

where $A = X^{-1}I_{n-i,i}X$ and

$$XX^T = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\
0 & a_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & a_n
\end{pmatrix}.$$

Over the $p$-adic numbers, recall that we used the dual values $d_{\alpha, c}$ where $\alpha$ is the representative of the determinant of the representative matrix $\pmod{(k^*)^2}$. In the situation for $G = \text{SO}(n, \mathbb{Q}_p, \beta)$ we instead look at the triple values $d_{\alpha, c_1, c_2}$, where $\alpha$ still represents the determinant, $c_1$ is the Hasse symbol for the diagonal matrix

$$
\begin{pmatrix}
a_1 & 0 & \cdots & 0 \\
0 & a_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & a_{n-i}
\end{pmatrix}
$$
and $c_2$ is the Hasse symbol for the diagonal matrix

\[
\begin{pmatrix}
a_{n-i+1} & 0 & \ldots & 0 \\
0 & a_{n-i+2} & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & a_n
\end{pmatrix}.
\]

This indicates that we focus on the 16 triple values for $p \neq 2$ instead of the 8 we investigated over $\text{SL}(n, k)$, and we look at the 32 triple values for $p = 2$ rather than the 16 we focused on over $\text{SL}(n, k)$. It is clear that this requires much work either to construct a general theory for such classification or for working on a case-by-case basis.

These results help set up the framework for a complete classification of involutions of $G$ and the bilinear forms which induce these involutions. For each symmetric bilinear form we must fix its special orthogonal group, determine which other bilinear forms give involutions of $G$ upon restricting their involutions of $\text{SL}(n, k)$ to $G$, and then determine the isomorphism classes of these remaining involutions on $G$. A good beginning strategy is to fix one bilinear form and its orthogonal group $G$ and determine the classes of involutions on $G$ and then see whether the pattern generalizes. Combining this with the machinery developed in this thesis will likely produce a theoretical approach to classifying involutions over $\text{SO}(n, k, \beta)$ for a general bilinear form $\beta$. The cases for $n$ odd will be more immediate and should provide a solid foundation for completing the classification for the even case.
List of References


References


