ABSTRACT

BENIM, ROBERT WAYNE. Isomorphy Classes of Involutions of $\mathrm{SO}(n, k, \beta)$ and $\mathrm{SP}(2n, k)$ where $n > 2$. (Under the direction of Aloysius Helminck.)

A first characterization of the isomorphism classes of k-involutions for any reductive algebraic groups defined over a perfect field was given in [Hel2000] using 3 invariants. In [HWD2004] a classification of all involutions on $\mathrm{SL}(n, k)$ for k algebraically closed, the real numbers, the p-adic numbers or a finite field was provided. In this paper, we build on these results to develop a detailed characterization of the isomorphy classes of involutions of $\mathrm{SO}(n, k, \beta)$ and $\mathrm{SP}(2n, k)$. We use these results to begin a classification of the isomorphy classes of involutions of $\mathrm{SO}(n, k, \beta)$ and $\mathrm{SP}(2n, k)$ where k is any field not of characteristic 2.

Isomorphy Classes of Involutions of $\mathrm{SO}(n, k, \beta)$ and $\mathrm{SP}(2n, k)$ where $n > 2$

by
Robert Wayne Benim

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

Mathematics

Raleigh, North Carolina

2014

APPROVED BY:

Naihuan Jing	Kailash Misra
Ernest Stitzinger	Aloysius Helminck Chair of Advisory Committee

BIOGRAPHY

Robert Wayne Benim was born 19 June 1984 in Portland, Oregon to parents Daniel and Uenina Benim. He grew up in the small town of Milwaukie, Oregon, with one older brother, Nicholas, and two dogs, Snowball and Samantha. He spent the majority of the first 26 years of his life in Milwaukie, and later Portland. Upon receiving his high school diploma at Milwaukie High School in 2003, he attended the University of Portland and Portland State University, where he earned a Bachelor's degree and a Master's degree, in 2007 and 2010 respectively, both in mathematics. After this, not being finished with his studies in mathematics, he enrolled in North Carolina State University's Ph.D. Mathematics program, and he became a student of Loek Helminck, who advised him in the research that is contained in this document.

ACKNOWLEDGEMENTS

I have many people to thank for my having gotten this far in my life. I may be the author of this paper, but in mathematics and life in general, nothing is every accomplished alone.

I would like to begin by thanking my parents, Daniel and Uenina Benim. You have always provided a home where I feel loved and had everything I could ever need. You have always supported my goals and dreams, and you never once discouraged me.

I would like to thank my brother Nick Benim. Throughout our childhoods you were my closest companion. In high school you challenged me to run cross country and track, making me into the runner I am today, and likely adding many years to my life.

I would like to thank my partner and best friend, Kristina Martin. Though you are relatively new in my life, I have never been as close to anyone as I am to you. You are always there for me, and you have become the rock that I lean on when I need support. I look forward to all of the travels and adventures that we still have to share.

I have had many friends in my life, and I am likely forgetting some now. But I would at least like to mention Danielle Johnson, Jeff Hayes, Ken Anderson, Jason Bonadurer, Tony Wright, Rachel Munyon, Lauren Kanikeberg, Daniel Brasch, Joe Schneider, Kate Snow, Aggie Jaeger, Beth Laskowski, Troy Parkinson, Jim Rohal, Aaron Herman, John Holodnak, Brandon Bock, Melissa Tolley, Kevin Penner, Jason Scott, Abby Bishop, Nathaniel Schwartz, and Mandi Sutherland. At one point or another, in some way, you have all been there for me, and I want you to know that I truly appreciate that.

This having been an academic pursuit, I want to be sure to thank all of the teachers that I have had in my life. I would first like to thank all of the teachers that I had at Seth Lewelling Elementary School, the now defunct Milwaukie Middle School, and Milwaukie High School. I would especially like to thank Jeff Gilbert, who was my coach, history teacher, mentor, and most of all my friend. Though we rarely have a chance to talk these days, I want you to know that you have had a profound impact on my life, and helped me realize the person I could be.

I would like to thank the entire mathematics department at the University of Portland, but I would especially like to thank Aaron Wootton, Lewis Lum, Chris Hallstrom, Stephanie Salomone, Ron Smit, and Meike Niederhausen. You were my early mentors in mathematics, and got me started on a long infinite road.

I would also like to thank the mathematics department at the Portland State University, but I would especially like to thank John Caughman and John Erdman. You both helped rekindle my love of math, and reminded me that I could become a good mathematician.

Lastly, I would like to thank the math department at North Carolina State University. I would especially like to thank my advisor, Loek Helminck. You have always managed to make time for me in your ridiculously busy schedule to answer all of the mathematical and professional questions that I have, and perhaps more importantly, you have always been there to give me a pep talk when I began to doubt myself. I look forward to continuing to correspond with you about our discoveries in mathematics. I would also like to thank the rest of my doctoral committee, Ernie Stitzinger, Kailash Misra, and Naihuan Jing, and my graduate school representative, Scott McCulloch. You have all taken the time to review my work, and ensure its quality and correctness, and I greatly appreciate that.

TABLE OF CONTENTS

LIST OF TABLES vi

Chapter 1 Introduction and Background 1
1.1 Preliminaries 2

Chapter 2 Isomorphy Classes of Involutions of $\mathrm{SO}(n,k,\beta)$ **6**
2.1 Automorphisms of $\mathrm{SO}(n,k,\beta)$ 6
2.2 Involutions of $\mathrm{SO}(n,k,\beta)$ 18
2.2.1 Type 1 Involutions 18
2.2.2 Type 2 Involutions 24
2.2.3 Type 3 Involutions 35
2.2.4 Type 4 Involutions 43
2.3 Types 1 and 2 Involutions as products of reflections 52
2.4 Maximal Number of Isomorphy classes 56
2.5 Explicit Examples 58
2.5.1 Algebraically Closed Fields 58
2.5.2 The Standard Real Orthogonal Group 59
2.5.3 Orthogonal Groups of $\mathbb{F}_q$ 60
2.5.4 p-adic examples 63

Chapter 3 Isomorphy Classes of Involutions of $\mathrm{SP}(2n,k)$ **68**
3.1 Automorphisms of $\mathrm{SP}(2n,k)$ 68
3.2 Involutions of $\mathrm{SP}(2n,k)$ 69
3.2.1 Type 1 Involutions 69
3.2.2 Type 2 Involutions 74
3.2.3 Type 3 Involutions 81
3.2.4 Type 4 Involutions 87
3.3 Maximal Number of Isomorphy classes 96
3.4 Explicit Examples 97
3.4.1 Type 2 Examples 97
3.4.2 Type 4 Examples 97

Chapter 4 Future Work **99**

REFERENCES **100**

LIST OF TABLES

Table 2.1 The various possible types of involutions of $\mathrm{SO}(n, k, \beta)$ 18
Table 2.2 Some values of $\tau_1(k)$ 57
Table 2.3 Some values of $\tau_2(m, k)$ 57
Table 2.4 Type 2 and Type 4 examples for $\mathrm{SO}(4, \mathbb{F}_p)$ 63
Table 2.5 X_1 and X_2 values when $k = \mathbb{Q}_p$, $p > 2$, and $-1 \in (\mathbb{Q}_p^*)^2$ 65
Table 2.6 X_1 and X_2 values when $k = \mathbb{Q}_p$, $p > 2$ and $-1 \notin (\mathbb{Q}_p^*)^2$ 66
Table 2.7 X_1 and X_2 values when $k = \mathbb{Q}_2$ 67

Table 3.1 The various possible types of involutions of $\mathrm{SP}(2n, k)$ 69

Chapter 1

Introduction and Background

Let G be a connected reductive algebraic group defined over a field k of characteristic not 2, ϑ an involution of G defined over k, H a k-open subgroup of the fixed point group of ϑ and G_k (resp. H_k) the set of k-rational points of G (resp. H). The variety G_k/H_k is called a symmetric k-variety. For $k = \mathbb{R}$ these symmetric k-varieties are also called real reductive symmetric spaces. These varieties occur in many problems in representation theory, geometry and singularity theory. To study these symmetric k-varieties one needs first a classification of the related k-involutions. A characterization of the isomorphism classes of the k-involutions was given in [Hel2000] essentially using the following 3 invariants:

(i) classification of admissible (Γ, ϑ)-indices.

(ii) classification of the G_k-isomorphism classes of k-involutions of the k-anisotropic kernel of G.

(iii) classification of the G_k-isomorphism classes of k-inner elements of G.

For more details, see [Hel2000]. The admissible (Γ, ϑ)-indices determine most of the fine structure of the symmetric k-varieties and a classification of these was included in [Hel2000] as well. For k algebraically closed or k the real numbers the full classification can be found in [Hel88]. For other fields a full classification of the remaining two invariants is still lacking. In particular the case of symmetric k-varieties over the p-adic numbers is of interest. We note that the above characterization was only proven for k a perfect field.

In [HWD2004] a full characterization of the isomorphism classes of k-involutions was given in the case that $G = \mathrm{SL}(n, k)$ and the characterization of k is not 2 which does not depend on any of the results in [Hel2000]. It was also shown how one may construct an outer-involution from a given non-degenerate symmetric or skew-symmetric bilinear form β of k^n. Using this characterization the possible isomorphism classes for k algebraically closed, the real numbers, the p-adic numbers and finite fields were classified. In [Schw2013] a full characterization of the isomorphism classes of k-involutions was provided in the case that $G = \mathrm{SL}(n,k)$ and the characterization of k is 2 which likewise does not depend on any of the results in [Hel2000]. [Schw2013] also contains a partial characterization of the involutions for $\mathrm{O}(n,k)$ when k is characteristic 2 provided. Likewise, partial results for $\mathrm{SO}(n,k,\beta)$ for n odd are provided in [Wu2002] and [Dom2003], and partial results for the characterization of inner-automorphisms of $\mathrm{SP}(2n,k)$ when the characteristic of k is not 2 are provided in [Jac2005].

In this paper we build upon the results of [Wu2002], [Dom2003], and [Jac2005] to give a characterization of involutions of $\mathrm{SO}(n,k,\beta)$, the special orthogonal group with respect to a symmetric bilinear form β on k^n, and $\mathrm{SP}(2n,k)$, the symplectic group, when the characteristic of the field k is not 2. We first show that if an automorphism $\vartheta = \mathrm{Inn}_A$ where $A \in \mathrm{GL}(n,\overline{k})$ leaves $\mathrm{SO}(n,k,\beta)$ or $\mathrm{SP}(2n,k)$ invariant, then we can assume A in $\mathrm{O}(n,k[\sqrt{\alpha}],\beta)$ or $\mathrm{SP}(2n,k[\sqrt{\alpha}])$ where $k[\sqrt{\alpha}]$ is a quadratic extension of k. In the symplectic case, this result can be found in [Jac2005]. Thus, to classify the involutions of $\mathrm{SO}(n,k,\beta)$ and $\mathrm{SP}(2n,k)$ it suffices to determine which $A \in \mathrm{SO}(n,k[\sqrt{\alpha}],\beta)$ or $\mathrm{SP}(2n,k[\sqrt{\alpha}])$ induce involutions of $\mathrm{SO}(n,k,\beta)$ or $\mathrm{SP}(2n,k)$, respectively, and to then determine the isomorphy classes of these involutions over $\mathrm{O}(n,k,\beta)$ or $\mathrm{SP}(2n,k)$, respectively. We give a full characterization (mostly for the standard orthogonal group) of involutions of $\mathrm{SO}(n,k,\beta)$ when k is algebraically closed, the real numbers, or a finite field of order odd p. Also, we give a full characterization of involutions of $\mathrm{SP}(2n,k)$ for k algebraically closed, the real numbers, or a finite field.

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 [Hum75] 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.

Our main reference for results regarding involutions of $\mathrm{SL}(n,k)$ will be [HWD2004]. Let k be a field of characteristic not 2, $\bar{k}$ the algebraic closure of k,

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

$$\mathrm{GL}(n,k) = \{A \in \mathrm{M}(n,k) \mid \det(A) \neq 0\}$$

and

$$\mathrm{SL}(n,k) = \{A \in \mathrm{M}(n,k) \mid \det(A) = 1\}.$$

Let k^* denote the product group of all the nonzero elements, $(k^*)^2 = \{a^2 \mid a \in k^*\}$ and $I_n \in \mathrm{M}(n,k)$ denote the identity matrix. We will sometimes use I instead of I_n when the dimension of the identity matrix is clear.

We recall some important definitions.

Definition 1.1.1. *Let* $\mathrm{Aut}(G_k)$ *denote the set of all automorphisms of* G_k*. For* $A \in \mathrm{GL}(n,\overline{k})$ *let* Inn_A *denote the inner automorphism defined by* $\mathrm{Inn}_A(X) = A^{-1}XA$ *for all* $X \in \mathrm{GL}(n,k)$*. Let* $\mathrm{Inn}(G_k) = \{\mathrm{Inn}_A \mid A \in G_k\}$ *denote the set of all inner automorphisms of* G_k *and let* $\mathrm{Inn}(G'_k, G_k)$ *denote the set of automorphisms* Inn_A *of* G_k *with* $A \in G'_k$*. If* Inn_A *is order 2, that is* Inn_A^2 *is the identity but* Inn_A *is not, then we call* Inn_A *an inner involution of* G*. We say that* ϑ *and* τ *in* $\mathrm{Aut}(G_k)$ *are isomorphic over a group* G'_k *if there is a* φ *in* $\mathrm{Inn}(G'_k, G_k)$ *such that* $\tau = \varphi^{-1}\vartheta\varphi$*. Equivalently, we say that* τ *and* ϑ *are in the same isomorphy class.*

For our purposes, G'_k will always be G_k itself, or a group which contains G_k. As an example of this sort of isomorphy in the literature, we consider [HWD2004], where the isomorphy classes of the inner-involutions of $\mathrm{SL}(n,k)$ in $\mathrm{Inn}(\mathrm{GL}(n,k), \mathrm{SL}(n,k))$ over $\mathrm{GL}(n,k)$ were classified. Here, two involutions ϑ and τ of $\mathrm{SL}(n,k)$ are isomorphic over $\mathrm{GL}(n,k)$ if there exists $\varphi \in \mathrm{Inn}(\mathrm{GL}(n,k), \mathrm{SL}(n,k))$ such that $\tau = \varphi^{-1}\vartheta\varphi$. It is also a common practice to define isomorphy over $\mathrm{Aut}(G'_k, G_k)$ instead of $\mathrm{Inn}(G'_k, G_k)$, again where G'_k is either G_k, or a group containing G_k.

Theorem 1.1.2. *Suppose the involution* $\vartheta \in \mathrm{Aut}(\mathrm{SL}(n,k))$ *is of inner type. (That is, suppose* $\vartheta \in \mathrm{Inn}(\mathrm{GL}(n,k), \mathrm{SL}(n,k))$*.) Then up to isomorphism over* $\mathrm{GL}(n,k)$*,* ϑ *is one of the following:*

(i) $\mathrm{Inn}_Y|_G$*, where* $Y = I_{n-i,i} \in \mathrm{GL}(n,k)$ *where* $i \in \left\{1, 2, \ldots, \lfloor \frac{n}{2} \rfloor\right\}$ *where*

$$I_{n-i,i} = \begin{pmatrix} I_{n-i} & 0 \\ 0 & I_i \end{pmatrix}$$

.

(ii) $\mathrm{Inn}_Y|_G$*, where* $Y = L_{\frac{n}{2},x} \in \mathrm{GL}(n,k)$ *where* $x \in k^*/k^{*2}$*,* $x \not\equiv 1 \mod k^{*2}$ *and*

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

Note that (ii) can only occur when n *is even.*

For the purposes of this paper, we will use matrices of the form $\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ xI_{\frac{n}{2}} & 0 \end{pmatrix}$ (and there multiples) rather than $L_{\frac{n}{2},x}$. Either of these serves as a member of the isomorphy class listed in the previous theorem. We will eventually see that all of the isomorphy classes of $\mathrm{SO}(n,k,\beta)$ and $\mathrm{SP}(2n,k)$ are just isomorphy classes of $\mathrm{SL}(n,k)$ (or $\mathrm{SL}(2n,k)$) that have been divided into multiple isomorphy classes.

We now begin to define the notion of a special orthogonal group. Let M be the matrix of a non-degenerate bilinear form β over k^n with respect to a basis $\{e_1, \dots e_n\}$ of V. We will say that M is the matrix of β if the basis $\{e_1, \dots e_n\}$ is the standard basis of k^n.

The typical notation for the orthogonal group is $\mathrm{O}(n,k)$, which is the group

$$\mathrm{O}(n,k) = \{A \in \mathrm{M}(n,k) \mid A^T A = I_n\}.$$

This group consists of the matrices which fix the standard dot product. This can be generalized to any non-degenerate bilinear β, which will yield the group

$$\mathrm{O}(n,k,\beta) = \{A \in \mathrm{M}(n,k) \mid \beta(Ax,Ay) = \beta(x,y)\}.$$

If M is the matrix of β with respect to the standard basis, then we can equivalently say

$$\mathrm{O}(n,k,\beta) = \{A \in \mathrm{M}(n,k) \mid A^T M A = M\}.$$

If β is symmetric, then we note that M is symmetric. In this case, we will call $\mathrm{O}(n,k,\beta)$ an *Orthogonal Group*. It is clear from this definition that all matrices in $\mathrm{O}(n,k,\beta)$ have determinant 1 or -1. We also define

$$\mathrm{SO}(n,k,\beta) = \mathrm{O}(n,k,\beta) \cap \mathrm{SL}(n,k).$$

We call this group a *Special Orthogonal Group*.

We note a couple of important facts, the first of which will be used repeatedly throughout this paper.

(i) Symmetric matrices are congruent to diagonal matrices, where the entries are are representatives of $k^*/(k^*)^2$.

(ii) If β_1 and β_2 correspond to M_1 and M_2, then $\mathrm{SO}(n,k,\beta_1)$ and $\mathrm{SO}(n,k,\beta_2)$ are isomorphic via

$$\Phi : \mathrm{SO}(n,k,\beta_1) \to \mathrm{SO}(n,k,\beta_2) : X \to Q^{-1}XQ$$

for some $Q \in \mathrm{GL}(n,k)$ if $cQ^T M_1 Q = M_2$ for some constant $c \in k$.

So, for orthogonal and special orthogonal groups, we will assume that β is such that M is diagonal. Then, to characterize the involutions of an orthogonal group where M is not diagonal, one can apply the characterization that will follow by simply using the isomorphism given above.

Lastly, two vectors $x, y \in k^n$ are said to be *orthogonal* with respect to the bilinear form β if $\beta(x, y) = 0$. We will eventually see that orthogonal vectors play an important role in the structure of involutions of $\mathrm{SO}(n, k, \beta)$.

We now begin to define the notion of a symplectic group. To begin, we consider the group $\mathrm{O}(n, k, \beta) = \{A \in \mathrm{M}(n, k) \mid A^T M A = M\}$ where β is skew-symmetric. It follows that M is a skew-symmetric matrix. Since we are assuming that β is non degenerate, then this forces the dimension of M to be even.

Invertible skew-symmetric matrices of even dimension are congruent to the matrix $J = J_{2n} = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$. Using an isomorphism like Φ from before, then we know that if β is skew-symmetric, then $\mathrm{O}(2n, k, \beta)$ is isomorphic to

$$\mathrm{SP}(2n, k) = \{A \in \mathrm{M}(n, k) \mid A^T J A = J\}.$$

We call this the *Symplectic Group*.

It can be shown that all matrices in $\mathrm{SP}(2n, k)$ have determinant 1, so in fact $\mathrm{SP}(2n, k)$ is a subgroup of $\mathrm{SL}(2n, k)$.

Chapter 2

Isomorphy Classes of Involutions of $\mathrm{SO}(n, k, \beta)$

2.1 Automorphisms of $\mathrm{SO}(n, k, \beta)$

It follows from a proposition on page 191 of [Bor91] that the outer automorphism group

$$\mathrm{Out}(\mathrm{SO}(n, \overline{k}, \beta)) = \mathrm{Aut}(\mathrm{SO}(n, \overline{k}, \beta)) / \mathrm{Inn}(\mathrm{SO}(n, \overline{k}, \beta))$$

must be a subgroup of the diagram automorphisms of the associated Dynkin diagram. If $n = 2m + 1$ and $m \geqslant 2$, then this Dynkin diagram is B_m which has only the trivial diagram automorphism. Thus, there are no outer automorphisms of $\mathrm{SO}(n, \overline{k}, \beta)$ when n is odd. If $n = 2m$ and $m \geqslant 4$, then this Dynkin diagram is D_m. The group of automorphisms of this Dynkin diagram is $\mathbb{Z}_2$ when $m > 4$, and is S_6 when $m = 4$, because of triality. But, it can be shown that the order 3 outer-automorphisms do not lift from D_4 to the orthogonal group. For the details, see Chapter 30 of [Bump2013]. So, when n is even, $\mathrm{Out}(\mathrm{SO}(n, \overline{k}, \beta)) = \mathbb{Z}_2$. We will see that the outer automorphisms are of the form Inn_A where $A \in \mathrm{O}(n, \overline{k}, \beta)$ and $\det(A) = -1$. When k is not algebraically closed, then all automorphisms of $\mathrm{SO}(n, k, \beta)$ will still be of the form Inn_A for some $A \in \mathrm{O}(n, \overline{k}, \beta)$ since Inn_A must also be an automorphism of $\mathrm{SO}(n, \overline{k}, \beta)$. Thus, the classifications and characterizations that follow in this paper consider all automorphisms and involutions of $\mathrm{SO}(n, k, \beta)$, assuming that n is sufficiently large.

We now examine which automorphisms will act as the identity on $\mathrm{SO}(n, k, \beta)$. This will prove to be useful when we classify matrix representatives for automorphisms. A similar lemma was proven in the case where n is odd and β is the standard dot product in [Wu2002], the dissertation of Ling Wu.

Lemma 2.1.1. *Assume $n > 2$. Let $A \in \mathrm{GL}(n, \overline{k})$. If Inn_A is the identity on $\mathrm{SO}(n, k, \beta)$, then*

A is a diagonal matrix.

Proof. Suppose A is such that Inn_A is the identity on $\mathrm{SO}(n,k,\beta)$. For $1 \leqslant r < s \leqslant n$, let X_{rs} be the diagonal matrix with all 1's, except in the in the rth and sth diagonal entries, where instead there are -1's. This matrix always lies in $\mathrm{SO}(n,k,\beta)$. So, we must have $AX_{rs} = X_{rs}A$. On the left side, the matrix is the same as A, but with the rth and sth columns negated. On the right side, the matrix is the same as A, but with the rth and sth rows negated. So, all entries of A on these rows and columns which aren't in the (r,r), (r,s), (s,r) or (s,s) components must be equal to 0, since this is the only number which equals its negative. To see that the (r,s) and (s,r) components of A must also equal 0, we can repeat this process for X_{rt}, where t is distinct from both r and s. (Note that this is where we use the fact that $n > 2$.) Thus, all off-diagonal elements of A are 0, which means A is diagonal. □

We want to be able to say more about the matrix A when Inn_A acts as the identity. It turns out that if we make the following assumption on the orthogonal group $\mathrm{SO}(n,k,\beta)$, then we can show that A is a multiple of the identity.

Definition 2.1.2. *Let k be a field and suppose β is a bilinear form on k^n such that $M = (\beta(\cdot,\cdot))$ is diagonal, with diagonal entries $m_1, ..., m_n$, which are representatives of $k^*/(k^*)^2$. If for each $m_i, m_j \in k^*/(k^*)^2$, $x^2 + \frac{m_i}{m_j}y^2 = 1$ has a solution (x,y) such that $y \neq 0$, then we call $\mathrm{SO}(n,k,\beta)$ a friendly orthogonal group.*

With this new terminology in mind, we get the following result.

Lemma 2.1.3. *Assume $n > 2$. Suppose $\mathrm{SO}(n,k,\beta)$ is a friendly orthogonal group. Let $A \in \mathrm{GL}(n,\overline{k})$. Then, Inn_A is the identity on $\mathrm{SO}(n,k,\beta)$ if and only if $A = \alpha I$ for some $\alpha \in \overline{k}^*$.*

Proof. We know from the previous lemma that A is diagonal. Let a_i represent the ith diagonal entry of A. Recall that we are assuming that M is diagonal. Label M's ith diagonal as m_i.

Then, there exists $a, b \in k$ where $b \neq 0$ such that $a^2 + \frac{m_i}{m_j} b^2 = 1$. For $1 \leqslant i < j \leqslant n$, let

$$Y_{ij} = \begin{pmatrix} 1 & 0 & \cdots & & & & & & & \cdots & 0 \\ 0 & 1 & & & & & & & & & \vdots \\ \vdots & & \ddots & & & & & & & & \\ & & & 1 & & & & & & & \\ & & & & a & 0 & \cdots & 0 & b & & \\ & & & & 0 & 1 & & & 0 & & \\ & & & & \vdots & & \ddots & & \vdots & & \\ & & & & 0 & & & 1 & 0 & & \\ & & & & -\frac{m_i}{m_j} b & 0 & \cdots & 0 & a & & \\ & & & & & & & & & 1 & \vdots \\ \vdots & & & & & & & & & \ddots & 0 \\ 0 & \cdots & & & & & & & \cdots & 0 & 1 \end{pmatrix},$$

where the noteworthy entries occur in the ith and jth rows and columns. It is a simple calculation to show that $Y_{ij}^T M Y_{ij} = M$, and that $\det(Y_{ij}) = 1$. So, $Y_{ij} \in \mathrm{SO}(n, k, \beta)$. Then, we know that $AY_{ij} = Y_{ij}A$. By comparing both sides of this equality and inspecting the (i, j) entry, we see that $ba_j = ba_i$. Since we are assuming that $b \neq 0$, then it follows that $a_i = a_j$. Since we can repeat this for all i and j, then it is clear that A is a multiple of the identity.

□

This result is only useful if we can show that $\mathrm{SO}(n, k, \beta)$ is commonly a friendly orthogonal group. In the following theorem, we see that most $\mathrm{SO}(n, k, \beta)$ are friendly.

Theorem 2.1.4. *(i) If* $\mathrm{Char}(k) \neq 2, 3$*, then* $\mathrm{SO}(n, k, \beta)$ *is a friendly orthogonal group.*

(ii) If $M = \begin{pmatrix} m_1 & & & \\ & m_2 & & \\ & & \ddots & \\ & & & m_n \end{pmatrix}$ *is such that* $m_i \neq -m_j$ *whenever* $i \neq j$ *and* $\mathrm{Char}(k) \neq 2$*, then* $\mathrm{SO}(n, k, \beta)$ *is a friendly orthogonal group.*

Proof. When $\mathrm{Char}(k) \neq 2$, then we see that $1 = x^2 + \alpha y^2$ has solution $(x, y) = \left(\frac{\alpha-1}{\alpha+1}, \frac{2}{\alpha+1}\right)$ when $\alpha \neq -1$. When $\mathrm{Char}(k) \neq 3$, then we see that $1 = x^2 - y^2$ has solution $(x, y) = \left(\frac{5}{3}, \frac{4}{3}\right)$. Based on these two solutions, it is clear that $x^2 + \frac{m_i}{m_j} y^2 = 1$ will always have a solution in k if $\mathrm{Char}(k) \neq 2, 3$, and also when $\frac{m_i}{m_j} \neq -1$ and $\mathrm{Char}(k) \neq 2$. □

To show that this condition on orthogonal groups is not trivial, we note a case where $\mathrm{SO}(n,k,\beta)$ is not a friendly orthogonal group.

Example 2.1.5. *Suppose $k = \mathbb{F}_3$ and that β is such that $M = \begin{pmatrix} I & 0 \\ 0 & -1 \end{pmatrix}$. Then, $\mathrm{SO}(n,\mathbb{F}_3,\beta)$ is not a friendly orthogonal group, because there is no solution to $x^2 - y^2 = 1$ where $y \neq 0$.*

We now state a definition that will help us characterize matrices that can induce automorphisms on $\mathrm{SO}(n,k,\beta)$.

Definition 2.1.6. *Fix a bilinear form β with matrix M. If $A \in \mathrm{GL}(n,k)$ is a matrix such $M^{-1}A^TMA = \alpha I_n$, then we call A $\alpha-$orthogonal.*

Note that orthogonal matrices are 1-orthogonal.

We now have the following preliminary result that characterizes automorphisms of friendly $\mathrm{SO}(n,k,\beta)$.

Lemma 2.1.7. *Assume $n > 2$ and that $\mathrm{SO}(n,k,\beta)$ is a friendly orthogonal group.*

If $A \in \mathrm{GL}(n,\overline{k})$, then $\mathrm{Inn}_A(\mathrm{SO}(n,k,\beta)) \subseteq \mathrm{SO}(n,k,\beta)$ if and only if A is α-orthogonal and $A = p\widetilde{A}$ where $p, \alpha \in \overline{k}$ and

(i) $\widetilde{A} \in \mathrm{SO}(n,\overline{k},\beta)$ if n odd, or

(ii) $\widetilde{A} \in \mathrm{O}(n,\overline{k},\beta)$ if n is even.

Proof. Suppose $A \in \mathrm{GL}(n,\overline{k})$ and $\mathrm{Inn}_A(\mathrm{SO}(n,k,\beta)) \subseteq \mathrm{SO}(n,k,\beta)$. Choose $X \in \mathrm{SO}(n,k,\beta)$. Then, $A^{-1}XA \in \mathrm{SO}(n,\overline{k},\beta)$. So,

$$I = (A^{-1}XA)^{-1}A^{-1}XA$$

$$= M^{-1}(A^{-1}XA)^TMA^{-1}XA$$

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

This implies that

$$A^{-1}X^{-1} = M^{-1}A^TX^T(A^{-1})^TMA^{-1},$$

which means

$$X^{-1} = AM^{-1}A^TX^T(A^{-1})^TMA^{-1}.$$

We can rewrite this as

$$M^{-1}X^TM = AM^{-1}A^TX^T(A^{-1})^TMA^{-1}.$$

If we transpose both sides, then we see that

$$MXM^{-1} = (A^{-1})^T MA^{-1}XAM^{-1}A^T.$$

Solving for the X term on the left, we get that

$$X = M^{-1}(A^{-1})^T MA^{-1}XAM^{-1}A^T M$$

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

By the previous theorem, it follows that $(AM^{-1}A^T M) = \alpha I$ for some $\alpha \in \overline{k}^*$. Thus, A is $\alpha-$orthogonal. Let $p = \sqrt{\alpha}$. Then let $\widetilde{A} = \frac{1}{p}A$. It follows that $M^{-1}\widetilde{A}^T M\widetilde{A} = \frac{1}{p^2}M^{-1}A^T MA = \frac{1}{\alpha}(\alpha I) = I$, which shows that $\widetilde{A}$ is orthogonal. That is, $\widetilde{A} \in \mathrm{O}(n, \overline{k}, \beta)$. If n is odd and $\det(\widetilde{A}) = -1$, then we can replace $\widetilde{A}$ with $-\widetilde{A}$, and instead have a matrix inside $\mathrm{SO}(n, \overline{k}, \beta)$.

Since the converse is clear, we have proven the statement. $\square$

In the following theorem which completes the characterization of automorphisms on friendly $\mathrm{SO}(n, k, \beta)$, we see that we do not need the algebraic closure of the field k, but either the field itself, or a quadratic extension. A similar theorem was proven in the case where n is odd and β is the standard dot product in [Wu2002], the dissertation of Ling Wu. The following result is much more general.

Theorem 2.1.8. *Assume $n > 2$ and that $\mathrm{SO}(n, k, \beta)$ is a friendly orthogonal group.*

(*a*) *If n is odd and A is in $\mathrm{O}(n, \overline{k}, \beta)$, then Inn_A keeps $\mathrm{SO}(n, k, \beta)$ invariant if and only if we can choose $A \in \mathrm{SO}(n, k, \beta)$.*

(*b*) *If n is even and A is in $\mathrm{O}(n, \overline{k}, \beta)$, then Inn_A keeps $\mathrm{SO}(n, k, \beta)$ invariant if and only if there exists $p \in \overline{k}$ and $B \in \mathrm{GL}(n, k)$ such that $B = pA$ and B is $\alpha-$orthogonal for some $\alpha \in k$. Further, we can show $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$ where each entry of A is a $k-$multiple of $\sqrt{\alpha}$.*

Proof. Let $n > 2$ be arbitrary, and suppose A is in $\mathrm{O}(n, \overline{k}, \beta)$ such that Inn_A keeps $\mathrm{SO}(n, k, \beta)$ invariant. Let X_{rs} be the diagonal matrix with all entries -1, except for the (r, r) and (s, s) entries, which are 1. Since M is diagonal, it is clear that $X_{rs} \in \mathrm{O}(n, k, \beta)$. If n is even, then $X \in \mathrm{SO}(n, k, \beta)$. If n is odd, then $-X \in \mathrm{SO}(n, k, \beta)$. So, we know that $\mathrm{Inn}_A(X_{rs})$ or $-\mathrm{Inn}_A(X_{rs})$ must lie in $\mathrm{SO}(n, k, \beta)$. It is also clear that $\mathrm{Inn}_A(I) \in \mathrm{SO}(n, k, \beta)$. So, both $\mathrm{Inn}_A(X_{rs})$ and $\mathrm{Inn}_A(I)$ have entries in k. Let us examine the entries of $\mathrm{Inn}_A(X_{rs})$:

$$\mathrm{Inn}_A(X_{rs}) = A^{-1}X_{rs}A = M^{-1}A^T MX_{rs}A$$

$$
= M^{-1}A^T M \begin{pmatrix} -1 &&&&&&&&&& \\ & \ddots &&&&&&&&& \\ && -1 &&&&&&&& \\ &&& 1 &&&&&&& \\ &&&& -1 &&&&&& \\ &&&&& \ddots &&&&& \\ &&&&&& -1 &&&& \\ &&&&&&& 1 &&& \\ &&&&&&&& -1 && \\ &&&&&&&&& \ddots & \\ &&&&&&&&&& -1 \end{pmatrix} \begin{pmatrix} \mathbf{a_1} \\ \vdots \\ \mathbf{a_n} \end{pmatrix}
$$

$$
= M^{-1}A^T \begin{pmatrix} m_1 & 0 & \cdots & \cdots & 0 \\ 0 & m_2 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & m_{n-1} & 0 \\ 0 & \cdots & \cdots & 0 & m_n \end{pmatrix} \begin{pmatrix} -\mathbf{a_1} \\ \vdots \\ -\mathbf{a_{r-1}} \\ \mathbf{a_r} \\ -\mathbf{a_{r+1}} \\ \vdots \\ -\mathbf{a_{s-1}} \\ \mathbf{a_s} \\ -\mathbf{a_{s+1}} \\ \vdots \\ -\mathbf{a_n} \end{pmatrix}
$$

$$
= \begin{pmatrix} m_1^{-1} & 0 & \cdots & \cdots & 0 \\ 0 & m_2^{-1} & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & m_{n-1}^{-1} & 0 \\ 0 & \cdots & \cdots & 0 & m_n^{-1} \end{pmatrix} \begin{pmatrix} \mathbf{a_1}^T & \cdots & \mathbf{a_n}^T \end{pmatrix} \begin{pmatrix} -m_1\mathbf{a_1} \\ \vdots \\ -m_{r-1}\mathbf{a_{r-1}} \\ m_r\mathbf{a_r} \\ -m_{r+1}\mathbf{a_{r+1}} \\ \vdots \\ -m_{s-1}\mathbf{a_{s-1}} \\ m_s\mathbf{a_s} \\ -m_{s+1}\mathbf{a_{s+1}} \\ \vdots \\ -m_n\mathbf{a_n} \end{pmatrix}
$$

$$
= \begin{pmatrix} m_1^{-1}\mathbf{a_1}^T & \cdots & m_n^{-1}\mathbf{a_n}^T \end{pmatrix} \begin{pmatrix} -m_1\mathbf{a_1} \\ \vdots \\ m_{r-1}\mathbf{a_{r-1}} \\ m_r\mathbf{a_r} \\ -m_{r+1}\mathbf{a_{r+1}} \\ \vdots \\ -m_{s-1}\mathbf{a_{s-1}} \\ m_s\mathbf{a_s} \\ -m_{s+1}\mathbf{a_{s+1}} \\ \vdots \\ -m_n\mathbf{a_n} \end{pmatrix}
$$

$$= \begin{pmatrix} \frac{a_{11}}{m_1} & \cdots & \frac{a_{n1}}{m_n} \\ \vdots & \ddots & \vdots \\ \frac{a_{1n}}{m_1} & \cdots & \frac{a_{nn}}{m_n} \end{pmatrix} \begin{pmatrix} -m_1 a_{11} & \cdots & -m_1 a_{1n} \\ \vdots & & \vdots \\ -m_{r-1} a_{r-1,1} & \cdots & -m_{r-1} a_{r-1,n} \\ m_r a_{r1} & \cdots & m_r a_{rn} \\ -m_{r+1} a_{r+1,1} & \cdots & -m_{r+1} a_{r+1,n} \\ \vdots & & \vdots \\ -m_{s-1} a_{s-1,1} & \cdots & -m_{s-1} a_{s-1,n} \\ m_s a_{s1} & \cdots & m_s a_{sn} \\ -m_{s+1} a_{s+1,1} & \cdots & -m_{s+1} a_{s+1,n} \\ \vdots & & \vdots \\ -m_n a_{n1} & \cdots & -m_n a_{nn} \end{pmatrix}$$

$$= (-a_{1i}a_{1j}\frac{m_1}{m_i} - \cdots - a_{r-1,i}a_{r-1,j}\frac{m_{r-1}}{m_i} + a_{ri}a_{rj}\frac{m_r}{m_i}$$
$$-a_{r+1,i}a_{r+1,j}\frac{m_{r+1}}{m_i} - \cdots - a_{s-1,i}a_{s-1,j}\frac{m_{s-1}}{m_i} + a_{si}a_{sj}\frac{m_s}{m_i}$$
$$-a_{s+1,i}a_{s+1,j}\frac{m_{s+1}}{m_i} - \cdots - a_{ni}a_{nj}\frac{m_n}{m_i})_{(i,j)}.$$

Since $\mathrm{Inn}_A(X_{rs})$ and $\mathrm{Inn}_A(I)$ have entries in k, then so does the matrix $\mathrm{Inn}_A(I)+\mathrm{Inn}_A(X_r)$. Using a similar calculation to the above, we can see that this matrix has entries $2a_{ri}a_{rj}\frac{m_r}{m_i} + 2a_{si}a_{sj}\frac{m_s}{m_i}$. It follows that $m_r a_{ri}a_{rj} + m_s a_{si}a_{sj} \in k$ for all i, j, r, s.

So, we have that

$$m_r a_{ri}a_{rj} - m_s a_{ti}a_{tj}$$

$$= (m_r a_{ri}a_{rj} + m_s a_{si}a_{sj}) - (m_r a_{ri}a_{rj} + m_t a_{ti}a_{tj}) \in k,$$

which means that

$$m_r a_{ri}a_{rj} = \frac{1}{2}(m_r a_{ri}a_{rj} - m_s a_{ti}a_{tj}) + \frac{1}{2}(m_r a_{ri}a_{rj} + m_s a_{ti}a_{tj}) \in k.$$

Since $m_r \in k$, then $a_{ri}a_{rj} \in k$ for all i, j, r.

Now, we consider the bilinear form β_1 which has matrix M^{-1}. We know that $X \in \mathrm{SO}(n, \overline{k}, \beta)$ if and only $X^T M X = M$. But, if that is the case for a given X, then it follows that

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

Thus, $(X^{-1})^T \in \mathrm{SO}(n, \overline{k}, \beta_1)$. Since this is a group, then we in fact know that $X^T \in \mathrm{SO}(n, \overline{k}, \beta_1)$.

It is then easy to see that $X \in \mathrm{SO}(n,k,\beta)$ if and only if $X^T \in \mathrm{SO}(n,k,\beta_1)$.

We further claim that Inn_{A^T} is an automorphism of $\mathrm{SO}(n,k,\beta_1)$. Suppose $Y \in \mathrm{SO}(n,k,\beta_1)$ and consider $\mathrm{Inn}_{A^T}(Y) = (A^T)^{-1}YA^T$. This matrix lies in $\mathrm{SO}(n,k,\beta_1)$ if and only if its inverse-transpose lies in $\mathrm{SO}(n,k,\beta)$. It's inverse transpose is $A(Y^{-1})^TA^{-1} = \mathrm{Inn}_{A^{-1}}((Y^{-1})^T)$. Since $\mathrm{Inn}_{A^{-1}}$ must be an automorphism of $\mathrm{SO}(n,k,\beta)$ because Inn_A is, and since $(Y^{-1})^T \in \mathrm{SO}(n,k,\beta)$ because $Y \in \mathrm{SO}(n,k,\beta_1)$, then we have proven our claim.

Since Inn_{A^T} is an automorphism of $\mathrm{SO}(n,k,\beta_1)$, then it follows from our earlier work that $a_{ir}a_{jr} \in k$ for all i,j,r.

We now recall from earlier the matrices $Y_{ij} \in \mathrm{SO}(n,k,\beta)$ where $\mathrm{SO}(n,k,\beta)$ is a friendly special orthogonal group. So, it must be the case that $\mathrm{Inn}_A(Y_{ij}) \in \mathrm{SO}(n,k,\beta)$. Let us examine the entries of $\mathrm{Inn}_A(Y_{ij})$:

$$\mathrm{Inn}_A(Y_{ij}) = A^{-1}Y_{ij}A = M^{-1}A^TMY_{ij}A$$

$$= M^{-1}A^TM \begin{pmatrix} 1 & 0 & \cdots & & & & & & & & \cdots & 0 \\ 0 & 1 & & & & & & & & & & \vdots \\ \vdots & & \ddots & & & & & & & & & \\ & & & 1 & & & & & & & & \\ & & & & a & 0 & \cdots & 0 & b & & & \\ & & & & 0 & 1 & & & 0 & & & \\ & & & & \vdots & & \ddots & & \vdots & & & \\ & & & & 0 & & & 1 & 0 & & & \\ & & & & -\frac{m_i}{m_j}b & 0 & \cdots & 0 & a & & & \\ & & & & & & & & & 1 & & \vdots \\ \vdots & & & & & & & & & & \ddots & 0 \\ 0 & \cdots & & & & & & & & \cdots & 0 & 1 \end{pmatrix} A$$

$$
= M^{-1}A^T \begin{pmatrix}
m_1 & 0 & \cdots & & & & & & & \cdots & 0 \\
0 & \ddots & & & & & & & & & \vdots \\
\vdots & & & & & & & & & & \\
 & & & m_{i-1} & & & & & & & \\
 & & & m_i a & 0 & \cdots & 0 & bm_i & & & \\
 & & & 0 & m_{i+1} & & & 0 & & & \\
 & & & \vdots & & \ddots & & \vdots & & & \\
 & & & 0 & & & m_{j-1} & 0 & & & \\
 & & & -m_i b & 0 & \cdots & 0 & m_j a & & & \\
 & & & & & & & & m_{j+1} & & \vdots \\
\vdots & & & & & & & & & \ddots & 0 \\
0 & \cdots & & & & & & & \cdots & 0 & m_n
\end{pmatrix} \begin{pmatrix} \mathbf{a_1} \\ \vdots \\ \mathbf{a_n} \end{pmatrix}
$$

$$
= \begin{pmatrix}
m_1^{-1} & 0 & \cdots & \cdots & 0 \\
0 & m_2^{-1} & & & \vdots \\
\vdots & & \ddots & & \vdots \\
\vdots & & & m_{n-1}^{-1} & 0 \\
0 & \cdots & \cdots & 0 & m_n^{-1}
\end{pmatrix} \begin{pmatrix} \mathbf{a_1}^T & \cdots & \mathbf{a_n}^T \end{pmatrix} \begin{pmatrix}
m_1 \mathbf{a_1} \\
\vdots \\
m_{i-1}\mathbf{a_{i-1}} \\
a m_i \mathbf{a_i} + b m_i \mathbf{a_j} \\
m_{i+1}\mathbf{a_{i+1}} \\
\vdots \\
m_{j-1}\mathbf{a_{j-1}} \\
-b m_i m_i \mathbf{a_i} + a m_j \mathbf{a_j} \\
m_{j+1}\mathbf{a_{j+1}} \\
\vdots \\
m_n \mathbf{a_n}
\end{pmatrix}
$$

$$= \begin{pmatrix} m_1^{-1}\mathbf{a_1}^T & \cdots & m_n^{-1}\mathbf{a_n}^T \end{pmatrix} \begin{pmatrix} m_1\mathbf{a_1} \\ \vdots \\ m_{i-1}\mathbf{a_{i-1}} \\ am_i\mathbf{a_i} + bm_i\mathbf{a_j} \\ m_{i+1}\mathbf{a_{i+1}} \\ \vdots \\ m_{j-1}\mathbf{a_{j-1}} \\ -bm_im_i\mathbf{a_i} + am_j\mathbf{a_j} \\ m_{j+1}\mathbf{a_{j+1}} \\ \vdots \\ m_n\mathbf{a_n} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{a_{11}}{m_1} & \cdots & \frac{a_{n1}}{m_n} \\ \vdots & \ddots & \vdots \\ \frac{a_{1n}}{m_1} & \cdots & \frac{a_{nn}}{m_n} \end{pmatrix} \begin{pmatrix} m_1a_{11} & \cdots & m_1a_{1n} \\ \vdots & & \vdots \\ m_{i-1}a_{i-1,1} & \cdots & m_{i-1}a_{i-1,n} \\ am_ia_{i1} + bm_ia_{j1} & \cdots & am_ia_{in} + bm_ia_{jn} \\ m_{i+1}a_{i+1,1} & \cdots & m_{i+1}a_{i+1,n} \\ \vdots & & \vdots \\ m_{j-1}a_{j-1,1} & \cdots & m_{j-1}a_{j-1,n} \\ -bm_ja_{i1} + am_ja_{j1} & \cdots & -bm_ia_{in} + am_ja_{jn} \\ m_{j+1}a_{j+1,1} & \cdots & m_{j+1}a_{j+1,n} \\ \vdots & & \vdots \\ m_na_{n1} & \cdots & m_na_{nn} \end{pmatrix}$$

$$= (a_{1s}a_{1t}\frac{m_1}{m_s} + \cdots + a_{i-1,s}a_{i-1,t}\frac{m_{i-1}}{m_i} + \left(\frac{a_{is}}{m_s}\right)(am_ia_{it} + bm_ia_{jt})$$

$$+a_{i+1,s}a_{i+1,t}\frac{m_{i+1}}{m_s} + \cdots a_{j-1,s}a_{j-1,t}\frac{m_{j-1}}{m_s} + \left(\frac{a_{js}}{m_s}\right)(-bm_ia_{it} + am_ja_{jt})$$

$$+a_{j+1,s}a_{j+1,t}\frac{m_{j+1}}{m_s} \cdots + a_{ns}a_{nt}\frac{m_n}{m_s})_{(s,t)}.$$

We know that $a, b, m_s, a_{is}a_{it}, a_{js}a_{jt} \in k$. Since each of the matrix entries of $\mathrm{Inn}_A(Y_{ij})$ must lie in k, then it follows that

$$\left(\frac{a_{is}}{m_s}\right)(am_ia_{it} + bm_ia_{jt}) + \left(\frac{a_{js}}{m_s}\right)(-bm_ia_{it} + am_ja_{jt}) \in k.$$

If we further apply the facts we just stated about what lies in k, then we see that

$$a_{is}a_{jt} - a_{js}a_{it} \in k,$$

for all i, j, s, t.

We now want to show that $a_{is}a_{jt} \in k$ for all i, j, s, t. Without loss of generality, we will assume that both a_{is} and a_{jt} are nonzero. We may assume this since each row and column must have at least one nonzero entry. If both $a_{is}, a_{jt} \in k$, then $a_{is}a_{jt} \in k$ is obvious, so we assume $a_{is} \notin k$. Recall that $a_{is}^2 \in k$.

It follows that

$$a_{is}^2 a_{jt} - (a_{is}a_{it})a_{js} = a_{is}(a_{is}a_{jt} - a_{js}a_{it}) \in k[a_{is}].$$

Since we also know that $a_{is}^2, a_{is}a_{it} \in k$ and $a_{jt}, a_{it} \in k[a_{jt}]$, then it follows that

$$a_{is}(a_{is}a_{jt} - a_{js}a_{it}) \in k[a_{jt}]$$

as well. Recall that $a_{jt}^2 \in k$. So, there exists $c, d, e, f \in k$ such that

$$c + da_{is} = a_{is}(a_{is}a_{jt} - a_{js}a_{it}) = e + fa_{jt}.$$

Since we are assuming that $a_{is} \notin k$, then it follows that both d and f are nonzero, and that $a_{jt} \notin k$. We see that

$$0 = (c - e) + (da_{is} - fa_{jt}).$$

It follows that $da_{is} - fa_{jt} \in k$. So, $da_{is} = fa_{jt} + g$ for some $g \in k$. Therefore, we can write $a_{is} = ua_{jt} + v$ where $u = \frac{f}{d}, v = \frac{g}{d} \in k$. We see that k contains

$$a_{is}^2 = (ua_{jt} + v)^2 = u^2 a_{jt}^2 + 2uva_{jt} + v^2.$$

Since $a_{jt} \notin k$, then it follows that $uv = 0$. Since $a_{is} = ua_{jt} + v \notin k$, then $u \neq 0$. So, $v = 0$ and $a_{is} = ua_{jt}$. Thus, $a_{is}a_{jt} = \frac{1}{u}a_{is}^2 \in k$, as desired. From this it is clear that $k[a_{is}] = k[a_{jt}]$ for all i, j, s, t (assuming that a_{is} and a_{jt} are both nonzero). So, let $\alpha = a_{is}^2$ where a_{is} is a fixed nonzero entry of A. Then, we have shown that all the entries of A are in $k[\sqrt{\alpha}]$. This means that $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$, and all of the entries of A are $k-$multiples of $\sqrt{\alpha}$, as desired.

If n is odd, then we can replace A with $-A$ to get a matrix in $\mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$. So, assume that $A \in \mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$. We now show that we do not need a quadratic extension of k when n is odd. Proceed by contradiction and assume $A \in \mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$ inducing the automorphism. Then, from our work above, we know that $\sqrt{\alpha}A \in \mathrm{GL}(n, k)$. Then,

$$\det(\sqrt{\alpha}A) = [\sqrt{\alpha}]^n \det(A) = \alpha^{\frac{n}{2}} \notin k,$$

which is a contradiction. So, if n is odd, we may assume that $A \in \mathrm{SO}(n, k, \beta)$.

□

2.2 Involutions of $\mathrm{SO}(n, k, \beta)$

We now begin to focus on involutions and their classification. We will distinguish different types of involutions. First, we note that for some involutions, φ, there exists $A \in \mathrm{O}(n, k, \beta)$ such that $\varphi = \mathrm{Inn}_A$, but not in all cases. Sometimes we must settle for $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta) \setminus \mathrm{O}(n, k, \beta)$.

This is not the only way in which we can distinguish between different types of involutions. If Inn_A is an involution, then $\mathrm{Inn}_{A^2} = (\mathrm{Inn}_A)^2$ is the identity map. We know from earlier that this means that $A^2 = \gamma I$ for some $\gamma \in \overline{k}$. But, we know for certain that A is orthogonal. So, A^2 is also orthogonal. That means that $(A^2)^T M (A^2) = M$, which implies $(\gamma I)^T M (\gamma I) = M$, which means $\gamma^2 = 1$. So, $\gamma = \pm 1$. Thus, we can also distinguish between different types of involutions by seeing if $A^2 = I$ or $A^2 = -I$. This gives the four types of involutions, which are outlined in Table 2.1.

Table 2.1: The various possible types of involutions of $\mathrm{SO}(n, k, \beta)$

	$A \in \mathrm{O}(n, k, \beta)$	$A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta) \setminus \mathrm{O}(n, k, \beta)$
$A^2 = I$	Type 1	Type 2
$A^2 = -I$	Type 3	Type 4

It follows from our characterization of automorphisms that when n is odd, that Type 2 and Type 4 involutions do not occur. But, we also see that if n is odd and A is orthogonal, then A^2 must have determinant 1. So, we see in addition that Type 3 involutions can also only occur when n is even.

2.2.1 Type 1 Involutions

We now find a structured form for the matrices of all types of involutions. We begin with Type 1 involutions. When n is odd, these are the only involutions. These were considered in [Wu2002] and [Dom2003], the dissertations of Ling Wu and Christopher Dometrius, respectively. The following is a generalization that also takes into account the case where n is even.

Lemma 2.2.1. *Suppose ϑ is a Type 1 involution of* $\mathrm{SO}(n,k,\beta)$*. Then, there exists* $A \in \mathrm{O}(n,k,\beta)$ *such that* $A = X \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix} X^{-1}$ *where* $s+t=n$ *and*

$$X = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} \in \mathrm{GL}(n,k),$$

where the x_i are orthogonal eigenvectors of A, meaning X^TMX is diagonal, and $s \leqslant t$.

Proof. Since $A^2 = I$, then all eigenvalues of A are ± 1. Since there are no repeated roots in the minimal polynomial of A, then we see that A is diagonalizable. We wish to construct bases for $E(A,1)$ and $E(A,-1)$ such that all the vectors lie in k^n. Let $s = \dim(E(A,-1))$ and $t = \dim(E(A,1))$, and observe that $s+t=n$ since A is diagonalizable. If $s > t$, then replace A with $-A$, and use this matrix instead. (It will induce the same involution.) Let $\{z_1, ..., z_n\}$ be a basis for k^n. For each i, let $u_i = (A-I)z_i$. Note that

$$Au_i = A(A-I)z_i = -(A-I)z_i = -u_i.$$

So, $\{u_1, ..., u_n\}$ must span $E(A,-1)$. Thus, we can appropriately choose s of these vectors and form a basis for $E(A,-1)$. Label these basis vectors as $y_1, ..., y_s$. We can similarly form a basis for $E(A,1)$. We shall call these vectors $y_{s+1}, ..., y_n$. Let Y be the matrix with the vectors $y_1, ..., y_n$ as its columns. Then, by construction,

$$Y^{-1}AY = \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix}.$$

We can rearrange to get

$$A = Y \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix} Y^{-1}.$$

Recall that $A^T = MAM^{-1}$, since $A \in \mathrm{O}(n,k,\beta)$. So,

$$\left(Y \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix} Y^{-1} \right)^T = M \left(Y \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix} Y^{-1} \right) M^{-1}.$$

This implies

$$(Y^{-1})^T \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix} Y^T = MY \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix} (MY)^{-1}$$

which means

$$\begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix} Y^T M Y = Y^T M Y \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix}.$$

So, $Y^T M Y = \begin{pmatrix} Y_1 & 0 \\ 0 & Y_2 \end{pmatrix}$, where Y_1 is $s \times s$, Y_2 is $t \times t$, and both are symmetric. It follows that there exists $N = \begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix} \in \mathrm{GL}(n,k)$ such that $N^T Y^T M Y N$ is diagonal. Let $X = YN$. Then,

$$\begin{aligned} X \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix} X^{-1} &= YN \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix} (YN)^{-1} \\ &= Y \begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix} \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix} \begin{pmatrix} N_1^{-1} & 0 \\ 0 & N_2^{-1} \end{pmatrix} Y^{-1} \\ &= Y \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix} Y^{-1} = A, \end{aligned}$$

where $X^T M X$ is diagonal. It follows from this last observation that the column vectors of X must be orthogonal with respect to β. □

We now want to examine when involutions of the same type are isomorphic. We first state a result from [Jon67] about symmetric matrices with entries from the p-adic numbers.

Lemma 2.2.2. *Symmetric matrices M_1 and M_2 with entries in $\mathbb{Q}_p$ are congruent if and only if*

$$\det(M_1) = \gamma^2 \det(M_2) \quad \textit{and} \quad c_p(M_1) = c_p(M_2)$$

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

Now we show conditions equivalent to isomorphy.

Theorem 2.2.3. *Suppose ϑ and φ are two Type 1 Involutions of $\mathrm{SO}(n,k,\beta)$ where $\vartheta = \mathrm{Inn}_A$ and $\varphi = \mathrm{Inn}_B$. Then, $A = X \begin{pmatrix} -I_{m_A} & 0 \\ 0 & I_{n-m_A} \end{pmatrix} X^{-1}$ and $B = Y \begin{pmatrix} -I_{m_B} & 0 \\ 0 & I_{n-m_B} \end{pmatrix} Y^{-1}$ where $m_A, m_B \leqslant \frac{n}{2}$, and*

$$X = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix}, Y = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \end{pmatrix} \in \mathrm{GL}(n,k)$$

have columns that are orthogonal eigenvectors of A and B respectively. We also have the diagonal matrices

$$X^T M X = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}$$

and

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

The following are equivalent:

(i) *ϑ is isomorphic to φ over* $\mathrm{SO}(n, k, \beta)$.

(ii) *A is conjugate to B or $-B$ over* $\mathrm{SO}(n, k, \beta)$.

(iii) *X_1 is congruent to Y_1 over* $\mathrm{GL}(m, k)$ *and X_2 is congruent to Y_2 over* $\mathrm{GL}(n - m, k)$, *or X_1 is congruent to Y_2 over* $\mathrm{GL}(\frac{n}{2}, k)$ *and X_2 is congruent to Y_1 over* $\mathrm{GL}(\frac{n}{2}, k)$.

(iv) *ϑ is isomorphic to φ over* $\mathrm{O}(n, k, \beta)$.

(v) *A is conjugate to B or $-B$ over* $\mathrm{O}(n, k, \beta)$.

(vi) *if $k = \mathbb{Q}_p$, there exists some $\gamma \in \mathbb{Q}_p$ such that*

$$\det(X_1) = \gamma^2 \det(Y_1), \;\; \det(X_2) = \gamma^2 \det(Y_2), \;\; c_p(X_1) = c_p(Y_1), \;\; \& \;\; c_p(X_2) = c_p(Y_2)$$

or

$$\det(X_1) = \gamma^2 \det(Y_2), \;\; \det(X_2) = \gamma^2 \det(Y_1), \;\; c_p(X_1) = c_p(Y_2), \;\; \& \;\; c_p(X_2) = c_p(Y_1).$$

Proof. First we note that in the event that $k = \mathbb{Q}_p$, then (vi) will be equivalent to (iii) by Lemma 2.2.2. We now show the equivalence of the other three conditions.

We now prove (i) is equivalent to (ii). First suppose A is conjugate to B over $\mathrm{SO}(n, k, \beta)$. Choose $Q \in \mathrm{SO}(n, k, \beta)$ such that $B = Q^{-1}AQ$, and let $\chi = \mathrm{Inn}_{Q^{-1}}$. Then, for all $U \in \mathrm{SO}(n, k, \beta)$, we have

$$\chi^{-1}\vartheta\chi(U) = Q^{-1}A^{-1}QUQ^{-1}AQ = (Q^{-1}AQ)^{-1}U(Q^{-1}AQ)$$

$$= B^{-1}UB = \varphi(U).$$

So, $\chi^{-1}\vartheta\chi = \varphi$. That is, ϑ is congruent to φ over $\mathrm{SO}(n, k, \beta)$.

Now suppose that A is conjugate to $-B$ over $\mathrm{SO}(n, k, \beta)$. Choose $Q \in \mathrm{SO}(n, k, \beta)$ such that $-B = Q^{-1}AQ$, and let $\chi = \mathrm{Inn}_{Q^{-1}}$. Then, for all $U \in \mathrm{SO}(n, k, \beta)$, we have

$$\chi^{-1}\vartheta\chi(U) = Q^{-1}A^{-1}QUQ^{-1}AQ = (Q^{-1}AQ)^{-1}U(Q^{-1}AQ)$$

$$= (-B)^{-1}U(-B) = B^{-1}UB = \varphi(U).$$

So, $\chi^{-1}\vartheta\chi = \varphi$. That is, ϑ is congruent to φ over $\mathrm{SO}(n,k,\beta)$.

Since the center of $\mathrm{SO}(n,k,\beta)$ is $\{I,-I\}$, then the converse follows similarly, so (i) and (ii) are equivalent. Likewise, we can show that (iv) and (v) are equivalent.

Next we show that (ii) implies (iii). First suppose that $Q^{-1}AQ = B$ for some $Q \in \mathrm{SO}(n,k,\beta)$. $Q^{-1}AQ = B$ implies

$$Q^{-1}X\begin{pmatrix} -I_{m_A} & 0 \\ 0 & I_{n-m_A}\end{pmatrix}X^{-1}Q = Y\begin{pmatrix} -I_{m_B} & 0 \\ 0 & I_{n-m_B}\end{pmatrix}Y^{-1}.$$

Since the matrices on both sides of the equality above must have the same eigenvalues with the same multiplicities, then we see that $m_A = m_B$, so we will just write m, and note that

$$-I_{m,n-m} = \begin{pmatrix} -I_m & 0 \\ 0 & I_{n-m}\end{pmatrix}.$$

Rearranging the previous equation, we have

$$I_{m,n-m}X^{-1}QY = X^{-1}QYI_{m,n-m},$$

which tells us that $X^{-1}QY = \begin{pmatrix} R_1 & 0 \\ 0 & R_2\end{pmatrix}$, where $R_1 \in \mathrm{GL}(m,k)$ and $R_2 \in \mathrm{GL}(n-m,k)$. Rearranging, we have that $QY = X\begin{pmatrix} R_1 & 0 \\ 0 & R_2\end{pmatrix}$. Since $Q \in \mathrm{O}(n,k,\beta)$, then we know that $Q^TMQ = M$.

So,

$$\begin{aligned} Y^TMY &= Y^TQ^TMQY \\ &= \begin{pmatrix} R_1 & 0 \\ 0 & R_2\end{pmatrix}^T (X^TMX)\begin{pmatrix} R_1 & 0 \\ 0 & R_2\end{pmatrix}. \end{aligned}$$

From here we see that $Y_1 = R_1^TX_1R_1$ and $Y_2 = R_2^TX_2R_2$.

Now suppose that $Q^{-1}AQ = -B$ for some $Q \in \mathrm{SO}(n,k,\beta)$. This implies

$$Q^{-1}X\begin{pmatrix} -I_{m_A} & 0 \\ 0 & I_{n-m_A}\end{pmatrix}X^{-1}Q = Y\begin{pmatrix} I_{m_B} & 0 \\ 0 & -I_{n-m_B}\end{pmatrix}Y^{-1}.$$

Since the matrices on both sides of the equality above must have the same eigenvalues with the same multiplicities, then we see that $m_A = n - m_B$. Since $m_A, m_B \leqslant \frac{n}{2}$, then it follows that

$m_A = m_B = \frac{n}{2}$. Rearranging the previous equation, we have

$$I_{\frac{n}{2},\frac{n}{2}} X^{-1}QY = X^{-1}QY I_{\frac{n}{2},\frac{n}{2}},$$

which tells us that $X^{-1}QY = \begin{pmatrix} 0 & R_1 \\ R_2 & 0 \end{pmatrix}$, where $R_1, R_2 \in \mathrm{GL}(\frac{n}{2}, k)$. Rearranging, we have that $QY = X \begin{pmatrix} 0 & R_1 \\ R_2 & 0 \end{pmatrix}$. Since $Q \in \mathrm{O}(n, k, \beta)$, then we know that $Q^T MQ = M$.

So,

$$Y^T MY = Y^T Q^T MQY$$
$$= \begin{pmatrix} 0 & R_1 \\ R_2 & 0 \end{pmatrix}^T (X^T MX) \begin{pmatrix} 0 & R_1 \\ R_2 & 0 \end{pmatrix}.$$

From here we see that $Y_2 = R_1^T X_1 R_1$ and $Y_1 = R_2^T X_2 R_2$.

This shows that *(ii)* implies *(iii)*.

Now show that *(iii)* implies *(ii)*. Assume that *(iii)* is the case. Specifically, assume that $R_1 \in \mathrm{GL}(m, k)$ and $R_2 \in \mathrm{GL}(n-m, k)$ such that $Y_1 = R_1^T X_1 R_1$ and $Y_2 = R_2^T X_2 R_2$. Let $R = \begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix}$. So, we have $Y^T MY = R^T (X^T MX) R$. Let $Q = XRY^{-1}$. We will now show that $Q^{-1}AQ = B$ and that $Q \in \mathrm{SO}(n, k, \beta)$.

$$Q^{-1}AQ = (XRY^{-1})^{-1} A (XRY^{-1})$$
$$= YR^{-1}X^{-1}AXRY^{-1} = YR^{-1}(-I_{m,n-m})RY^{-1}$$
$$= Y(-I_{m,n-m})Y^{-1} = B.$$

That is, $Q^{-1}AQ = B$.

Next, we must show that $Q \in \mathrm{SO}(n, k, \beta)$. We first show that $Q^T MQ = M$. Recall that $Y^T MY = R^T (X^T MX) R$. So,

$$Q^T MQ = (XRY^{-1})^T M (XRY^{-1})$$
$$= (Y^{-1})^T (R^T X^T MXR) Y^{-1} = (Y^{-1})^T (Y^T MY) Y^{-1} = M.$$

In the event that $\det(Q) = -1$, then we can replace the first column of X with its negative. This will have no effect on R or Y, so the new $Q = XRY^{-1}$ have determinant 1, and it will still be the case that $Q^{-1}AQ = B$ and $Q^T MQ = M$. So, $Q \in \mathrm{SO}(n, k, \beta)$.

If instead we assume that $R_1 \in \mathrm{GL}(m, k)$ and $R_2 \in \mathrm{GL}(n-m, k)$ such that $Y_2 = R_1^T X_1 R_1$

and $Y_1 = R_2^T X_2 R_2$, then if we let $R = \begin{pmatrix} 0 & R_1 \\ R_2 & 0 \end{pmatrix}$, then we can let $Q = XRY^{-1}$ and get that $Q^{-1}AQ = -B$ and $Q \in \mathrm{SO}(n, k, \beta)$. This shows that (iii) implies (ii).

We now show that (iv) and (v) are equivalent to the previous three conditions. First, we note that it is clear that (i) implies (iv). So, we need only show that (iv) or (v) implies one of the other three conditions. But, (v) implies (iii) from an argument very similar to the argument where we showed that (iii) implies (ii). Thus, all the conditions are equivalent.

□

We note that the equivalence of conditions (i) and (ii) in the previous theorem show that a Type 1 involution cannot be in the same isomorphy class as an involution of a different type. This will be the same for all types. That is, isomorphic involutions must be of the same type. We also note that this Theorem shows that isomorphy over $\mathrm{SO}(n, k, \beta)$ and $\mathrm{O}(n, k, \beta)$ are the same for Type 1 involutions. We will show in an explicit example that this does not occur in the Type 2 case. For the remaining three types of involutions, we will only find conditions for isomorphy over $\mathrm{O}(n, k, \beta)$. Again, recall that these three Types of involutions occur when n is even.

2.2.2 Type 2 Involutions

We have a similar characterization of the matrices and isomorphy classes in the Type 2 case. We first prove a result about that characterizes the eigenvectors in the Type 2 case.

Lemma 2.2.4. *Assume* $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$ *induces a Type-2 involution of* $\mathrm{SO}(n, k, \beta)$ *where* $\sqrt{\alpha} \notin k$. *Also suppose* $x, y \in k^n$ *such that* $x + \sqrt{\alpha} y \in E(A, -1)$. *Then,* $x - \sqrt{\alpha} y \in E(A, 1)$. *Likewise, if* $u, v \in k^n$ *such that* $u + \sqrt{\alpha} v \in E(A, 1)$. *Then,* $u - \sqrt{\alpha} v \in E(A, -1)$. *Further,* $\dim(E(A, 1)) = \dim(E(A, -1))$.

Proof. First, we observe that "$\sqrt{\alpha}-$conjugation," similar to the familiar complex conjugation ($i-$conjugation), preserves multiplication. That is,

$$(a + \sqrt{\alpha} b)(c + \sqrt{\alpha} d) = (ac + \alpha bd) + \sqrt{\alpha}(ad + bc)$$

and

$$(a - \sqrt{\alpha} b)(c - \sqrt{\alpha} d) = (ac + \alpha bd) - \sqrt{\alpha}(ad + bc).$$

So, "$\sqrt{\alpha}-$conjugation" will preserve multiplication on the matrix level as well. Because of this and since

$$A(x + \sqrt{\alpha} y) = -x - \sqrt{\alpha} y,$$

then it follows that

$$(-A)(x - \sqrt{\alpha}) = -x + \sqrt{\alpha}y.$$

We can multiply both sides to see that

$$A(x - \sqrt{\alpha}) = x - \sqrt{\alpha}y.$$

That is, $x - \sqrt{\alpha}y \in E(A, 1)$. This proves the first statement. An analogous argument proves the second.

To see that $\dim(E(A, 1)) = \dim(E(A, -1))$ is the case, note that the first statement tells us that $\dim(E(A, 1)) \leqslant \dim(E(A, -1))$, and that the second statement tells us that $\dim(E(A, 1)) \geqslant \dim(E(A, -1))$, since "$\sqrt{\alpha}$−conjugation" is an invertible operator on $k[\sqrt{\alpha}]^n$. ☐

We are now able to characterize the Type 2 involutions.

Lemma 2.2.5. *Suppose ϑ is a Type 2 involution of* $\mathrm{SO}(n, k, \beta)$*. Let A be the orthogonal matrix in* $\mathrm{O}(n, k[\sqrt{\alpha}], \beta)$ *such that* $\vartheta = \mathrm{Inn}_A$*. Then,*

$$A = \frac{-\sqrt{\alpha}}{\alpha} X \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix} X^{-1}$$

where

$$X = \begin{pmatrix} x_1 & x_2 & \cdots & x_{\frac{n}{2}} & y_1 & y_2 & \cdots & y_{\frac{n}{2}} \end{pmatrix} \in \mathrm{GL}(n, k),$$

where for each i, we have orthogonal vectors $x_i + \sqrt{\alpha}y_i \in E(A, -1)$ and orthogonal vectors $x_i - \sqrt{\alpha}y_i \in E(A, 1)$. Further,

$$X^T M X = \begin{pmatrix} X_1 & X_2 \\ X_2 & \frac{1}{\alpha}X_1 \end{pmatrix}$$

where X_1 and X_2 are diagonal matrices.

Proof. We wish to construct bases for $E(A, 1)$ and $E(A, -1)$ such that all the vectors lie in $k[\sqrt{\alpha}]^n$. From the previous lemma, we know that $\dim(E(A, 1)) = \dim(E(A, -1)) = \frac{n}{2}$. (Note that this means that n must be even for a Type 2 involution to occur.) Since Inn_A is a Type 1 involution of $\mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$, then we can apply Lemma 2.2.1 to find an orthogonal basis $\{x_1 + \sqrt{\alpha}y_1, ..., x_{\frac{n}{2}} + \sqrt{\alpha}y_{\frac{n}{2}}\}$ of $E(A, -1)$, where $x_1, ..., x_{\frac{n}{2}}, y_1, ..., y_{\frac{n}{2}} \in k^n$. By the previous lemma, we know that$\{x_1 - \sqrt{\alpha}y_1, ..., x_{\frac{n}{2}} - \sqrt{\alpha}y_{\frac{n}{2}}\}$ must be a basis for $E(A, 1)$. Let $X = \begin{pmatrix} x_1 & x_2 & \cdots & x_{\frac{n}{2}} & y_1 & y_2 & \cdots & y_{\frac{n}{2}} \end{pmatrix} \in \mathrm{GL}(n, k)$.

We now make a couple of observations. Suppose $u = x + \sqrt{\alpha}y$ is a -1-eigenvector of A such that $x, y \in k^n$. Then, we know $v = x - \sqrt{\alpha}y$ is a 1-eigenvector of A. Observe that

$$Ax = \frac{1}{2}A(u+v) = \frac{1}{2}(-u+v) = -\sqrt{\alpha}y.$$

It follows from this that

$$Ay = -\frac{\sqrt{\alpha}}{\alpha}x.$$

Since $Ax = -\sqrt{\alpha}y$ and $Ay = -\frac{\sqrt{\alpha}}{\alpha}x$, then it follows that

$$X^{-1}AX = \begin{pmatrix} 0 & -\frac{\sqrt{\alpha}}{\alpha}I_{\frac{n}{2}} \\ -\sqrt{\alpha}I_{\frac{n}{2}} & 0 \end{pmatrix}.$$

Rearranging this, we see that

$$A = -\frac{\sqrt{\alpha}}{\alpha}X \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix} X^{-1}.$$

Now, we need only prove the last statement to prove the Lemma. Since $\{x_1 + \sqrt{\alpha}y_1, ..., x_{\frac{n}{2}} + \sqrt{\alpha}y_{\frac{n}{2}}\}$ is an orthogonal set of vectors, then we know when $i \neq j$ that

$$0 = \beta(x_i + \sqrt{\alpha}y_i, x_j + \sqrt{\alpha}y_j) = (\beta(x_i, x_j) + \alpha\beta(y_i, y_j)) + \sqrt{\alpha}(\beta(x_i, y_j) + \beta(x_j, y_i)).$$

This tells us that

$$\beta(x_i, x_j) = -\alpha\beta(y_i, y_j)$$

and

$$\beta(x_i, y_j) = -\beta(x_j, y_i).$$

Since vectors from $E(A, 1)$ and $E(A, -1)$ are orthogonal, then we also know that

$$0 = \beta(x_i + \sqrt{\alpha}y_i, x_j - \sqrt{\alpha}y_j) = (\beta(x_i, x_j) - \alpha\beta(y_i, y_j)) + \sqrt{\alpha}(-\beta(x_i, y_j) + \beta(x_j, y_i)),$$

regardless of if i and j are distinct or equal.

This tells us that

$$\beta(x_i, x_j) = \alpha\beta(y_i, y_j)$$

and

$$\beta(x_i, y_j) = \beta(x_j, y_i).$$

So, when $i \neq j$, then we know that

$$\beta(x_i, y_j) = 0,$$

$$\beta(x_i, x_j) = 0,$$

and

$$\beta(y_i, y_j) = 0.$$

When $i = j$, we note that

$$\beta(x_i, x_i) = \alpha\beta(y_i, y_i).$$

Then, we have

$$X^T M X = \begin{pmatrix} X_1 & X_2 \\ X_2 & \frac{1}{\alpha}X_1 \end{pmatrix}$$

where X_1 and X_2 have been shown to be diagonal. □

We now show an example of a Type 2 Involution, and apply the previous lemma to it.

Example 2.2.6. *Assume that β is the standard dot product. Then,* Inn_A *can be a Type 2 involution of* $\mathrm{SO}(4, \mathbb{Q})$ *if A is symmetric and orthogonal, since this will imply that $A^2 = I$, and if the entries of A are all k-multiples of some $\sqrt{\alpha}$ such that $\sqrt{\alpha} \notin k$ but $\alpha \in k$. Observe that the matrix*

$$A = \frac{\sqrt{3}}{3}\begin{pmatrix} 0 & 1 & -1 & 1 \\ 1 & 0 & 1 & 1 \\ -1 & 1 & 1 & 0 \\ 1 & 1 & 0 & -1 \end{pmatrix}$$

is both symmetric and orthogonal. Since each entry is the $\mathbb{Q}-$multiple of $\sqrt{3}$, then it is clear that Inn_A *is a Type 2 involution of* $\mathrm{SO}(4, \mathbb{Q})$. *It can be shown that $E(A, -1)$ has dimension 2. An orthogonal basis for this subspace is formed by the vectors*

$$v_1 = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ 0 \\ 1 \end{pmatrix} + \sqrt{3}\begin{pmatrix} -\frac{1}{2} \\ -\frac{1}{2} \\ 0 \\ 0 \end{pmatrix}$$

and

$$v_2 = \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ 1 \\ 0 \end{pmatrix} + \sqrt{3} \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ 0 \\ 0 \end{pmatrix}.$$

It can be shown that

$$v_3 = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ 0 \\ 1 \end{pmatrix} - \sqrt{3} \begin{pmatrix} -\frac{1}{2} \\ -\frac{1}{2} \\ 0 \\ 0 \end{pmatrix}$$

and

$$v_4 = \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ 1 \\ 0 \end{pmatrix} - \sqrt{3} \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ 0 \\ 0 \end{pmatrix}$$

are orthogonal $1-$*eigenvectors of* A*, where these are the* $\sqrt{3}-$*conjugates of* v_1 *and* v_2*, respectively.*

Following the notation of the previous lemma, we have

$$X = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

where $X^T X = \begin{pmatrix} \frac{3}{3} & 0 & -\frac{1}{2} & 0 \\ 0 & \frac{3}{3} & 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}$ *and* $A = -\frac{\sqrt{3}}{3} X \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ 3I_{\frac{n}{2}} & 0 \end{pmatrix} X^{-1}$.

We now find conditions in the Type 2 case that are equivalent to isomorphy.

Theorem 2.2.7. *Suppose* ϑ *and* φ *are two Type 2 Involutions of* $\mathrm{SO}(n, k, \beta)$ *where* $\vartheta = \mathrm{Inn}_A$ *and* $\varphi = \mathrm{Inn}_B$*. Then,*

$$A = -\frac{\sqrt{\alpha}}{\alpha} X \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix} X^{-1} \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$$

where

$$X = \begin{pmatrix} x_1 & x_2 & \cdots & x_{\frac{n}{2}} & y_1 & y_2 & \cdots & y_{\frac{n}{2}} \end{pmatrix} \in \mathrm{GL}(n, k)$$

and the $x_i + \sqrt{\alpha} y_i$ *are the orthogonal basis of* $E(A, -1)$*, and*

$$X^T M X = \begin{pmatrix} X_1 & X_2 \\ X_2 & \frac{1}{\alpha} X_1 \end{pmatrix}$$

where X_1 *and* X_2 *are diagonal matrices,*

and

$$B = -\frac{\sqrt{\gamma}}{\gamma} Y \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \gamma I_{\frac{n}{2}} & 0 \end{pmatrix} Y^{-1} \in \mathrm{O}(n, k[\sqrt{\gamma}], \beta)$$

where

$$Y = \begin{pmatrix} \tilde{x}_1 & \tilde{x}_2 & \cdots & \tilde{x}_{\frac{n}{2}} & \tilde{y}_1 & \tilde{v}_2 & \cdots & \tilde{y}_{\frac{n}{2}} \end{pmatrix} \in \mathrm{GL}(n, k)$$

and the $\tilde{x}_i + \sqrt{\gamma} \tilde{y}_i$ *is the orthogonal eigenvectors of* $E(B, -1)$*, and*

$$Y^T M Y = \begin{pmatrix} Y_1 & Y_2 \\ Y_2 & \frac{1}{\alpha} Y_1 \end{pmatrix}$$

where Y_1 *and* Y_2 *are diagonal matrices, and the following are equivalent:*

(*i*) ϑ *is isomorphic to* φ *over* $\mathrm{O}(n, k, \beta)$*.*

(*ii*) A *is conjugate to* B *or* $-B$ *over* $\mathrm{O}(n, k, \beta)$*.*

(*iii*) $\alpha = \gamma$ *and* $Y^T M Y = R^T X^T M X R$ *where* $R = \begin{pmatrix} R_1 & R_2 \\ \alpha R_2 & R_1 \end{pmatrix} \in \mathrm{GL}(n, k)$*, or* $\alpha = \gamma$ *and* $Y^T M Y = R^T X^T M X R$ *where* $R = \begin{pmatrix} R_1 & R_2 \\ -\alpha R_2 & -R_1 \end{pmatrix} \in \mathrm{GL}(n, k)$*.*

(*iv*) *We can choose* X *and* Y *such that* $\alpha = \gamma$*, and for* $R = \begin{pmatrix} R_1 & R_2 \\ \alpha R_2 & R_1 \end{pmatrix} \in \mathrm{GL}(n, k)$ *we have*

$$Y_1 = R_1^T X_1 R_1 + \alpha R_2^T X_2 R_1 + \alpha R_1^T X_2 R_2 + \alpha R_2^T X_1 R_2$$

and

$$Y_2 = R_2^T X_1 R_1 + R_1^T X_2 R_1 + \alpha R_2^T X_2 R_2 + R_1^T X_1 R_2,$$

or for $R = \begin{pmatrix} R_1 & R_2 \\ -\alpha R_2 & -R_1 \end{pmatrix} \in \mathrm{GL}(n, k)$ *we have*

$$Y_1 = R_1^T X_1 R_1 - \alpha R_2^T X_2 R_1 - \alpha R_1^T X_2 R_2 + \alpha R_2^T X_1 R_2$$

and

$$Y_2 = R_2^T X_1 R_1 - R_1^T X_2 R_1 - \alpha R_2^T X_2 R_2 + R_1^T X_1 R_2.$$

Proof. Proving the equivalence of (i) and (ii) is identical to the proof in the previous theorem. So, we begin by showing that (ii) implies (iii). First suppose there exists $Q \in \mathrm{O}(n,k,\beta)$ such that $Q^{-1}AQ = B$. So, we have

$$Q^{-1}\frac{\sqrt{\alpha}}{\alpha}X\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix}X^{-1}Q = \frac{\sqrt{\gamma}}{\gamma}Y\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \gamma I_{\frac{n}{2}} & 0 \end{pmatrix}Y^{-1}.$$

Also, we know that since $A \in \mathrm{SO}(n,k[\sqrt{\alpha}],\beta)$ and $B \in \mathrm{SO}(n,k(\sqrt{\gamma}),\beta)$ are congruent over $\mathrm{O}(n,k,\beta)$, then we must be able to make a choice of γ such that $\alpha = \gamma$. Thus,

$$Q^{-1}X\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix}X^{-1}Q = Y\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix}Y^{-1}.$$

Rearranging, we see that

$$\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix}X^{-1}QY = X^{-1}QY\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix}.$$

Let $R = X^{-1}QY$, and note that $R \in \mathrm{GL}(n,k)$. Since $\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix}R = R\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix}$, then $R = \begin{pmatrix} R_1 & R_2 \\ \alpha R_2 & R_1 \end{pmatrix}$. Observe that $XR = QY$. Also, observe that since $Q \in \mathrm{SO}(n,k,\beta)$, then we know that $Q^TMQ = M$. It follows from these observations that

$$R^T(X^TMX)R = (XR)^TM(XR) = (QY)^TM(QY)$$

$$= Y^T(Q^TMQ)Y = Y^TMY.$$

If instead we assume that there exists $Q \in \mathrm{O}(n,k,\beta)$ such that $Q^{-1}AQ = -B$, then we can similarly show that $\alpha = \gamma$ and $Y^TMY = R^TX^TMXR$ where $R = \begin{pmatrix} R_1 & R_2 \\ -\alpha R_2 & -R_1 \end{pmatrix} \in \mathrm{GL}(n,k)$ for $R_1, R_2 \in \mathrm{M}(\frac{n}{2},k)$. This proves that (ii) implies (iii).

We now show that (iii) implies (ii). First assume $\alpha = \gamma$ and X^TMX is congruent to Y^TMY over $\mathrm{GL}(n,k)$ where $Y^TMY = R^TX^TMXR$ for $R = \begin{pmatrix} R_1 & R_2 \\ \alpha R_2 & R_1 \end{pmatrix}$, where $R_1, R_2 \in \mathrm{GL}(\frac{n}{2},k)$. Let $Q = XRY^{-1}$. Then, we observe that

$$Q^{-1}AQ = (XRY^{-1})^{-1}A(XRY^{-1}) = YR^{-1}(X^{-1}AX)RY^{-1}$$

$$= -\frac{-\sqrt{\alpha}}{\alpha}YR^{-1}\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix}RY^{-1} = -\frac{-\sqrt{\alpha}}{\alpha}Y\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix}R^{-1}RY^{-1}$$

$$= -\frac{-\sqrt{\alpha}}{\alpha}Y\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix}Y^{-1} = B.$$

So, to show that (ii) is indeed the case, we need only show that $Q \in \mathrm{O}(n, k, \beta)$. By construction, we know that $Q \in \mathrm{GL}(n, k)$. So, it is suffice to show $Q^TMQ = M$. But,

$$Q^TMQ = (XRY^{-1})^TM(XRY^{-1})$$

$$= (Y^{-1})^T(R^TX^TMXR)Y^{-1} = (Y^{-1})^T(Y^TMY)Y^{-1} = M.$$

If we instead assume that $\alpha = \gamma$ and X^TMX is congruent to Y^TMY over $\mathrm{GL}(n, k)$ where $Y^TMY = R^TX^TMXR$ for $R = \begin{pmatrix} R_1 & R_2 \\ -\alpha R_2 & -R_1 \end{pmatrix}$, where $R_1, R_2 \in \mathrm{GL}(\frac{n}{2}, k)$, then if we let $Q = XRY^{-1}$, we can similarly show that $Q^{-1}AQ = -B$ and $Q \in \mathrm{O}(n, k, \beta)$. This shows that (iii) implies (ii).

Lastly, matrix multiplication shows that (iii) and (iv) are equivalent.

□

The reader will notice that in the Type 1 case, our conditions gave us congruency of involutions over $\mathrm{SO}(n, k, \beta)$, but the Type 2 case gave us congruency of involutions over $\mathrm{O}(n, k, \beta)$. In the following example, we give an example that shows that the above Theorem cannot be strengthened by replacing $\mathrm{O}(n, k, \beta)$ with $\mathrm{SO}(n, k, \beta)$.

Example 2.2.8. *Consider the group* $\mathrm{SO}(4, \mathbb{F}_3)$. *That is, consider the case where k is the group of three elements, and the bilinear form is the standard dot product. A Type 2 involution is induced by the matrix*

$$A = i\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix} \in \mathrm{SO}(4, \mathbb{F}_3[i]).$$

By analyzing suitable eigenvectors for this matrix, we see that

$$X = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

where

$$A = iX^{-1} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix} X.$$

We also see that

$$X^T X = \begin{pmatrix} X_1 & X_2 \\ X_2 & 2X_1 \end{pmatrix}$$

where $X_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *and* $X_2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$.

Now, we also consider the Type 2 involution of $\mathrm{SO}(4, \mathbb{F}_3)$ *that is induced by the matrix*

$$B = i \begin{pmatrix} 0 & 0 & 2 & 1 \\ 0 & 0 & 2 & 2 \\ 2 & 2 & 0 & 0 \\ 1 & 2 & 0 & 0 \end{pmatrix} \in \mathrm{SO}(4, \mathbb{F}_3[i]).$$

By analyzing suitable eigenvectors for this matrix, we see that for

$$Y = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 2 & 1 \end{pmatrix},$$

we have

$$B = iY^{-1} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix} Y.$$

We also see that

$$Y^T Y = \begin{pmatrix} Y_1 & Y_2 \\ Y_2 & 2Y_1 \end{pmatrix}$$

where $Y_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *and* $Y_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

We have two ways of showing that these Type 2 involutions are congruent over $\mathrm{O}(4, \mathbb{F}_3)$. *First, we consider the matrix*

$$Q = \begin{pmatrix} 1 & 2 & 2 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 2 \\ 2 & 1 & 2 & 1 \end{pmatrix} \in \mathrm{O}(4, \mathbb{F}_3) \setminus \mathrm{SO}(4, \mathbb{F}_3).$$

Then, $B = Q^{-1}AQ$. *This is condition* (*ii*) *of the previous theorem.*

Secondly, if we let $R = \begin{pmatrix} R_1 & R_2 \\ 2R_2 & R_1 \end{pmatrix} \in \mathrm{GL}(4, \mathbb{F}_3)$ *where* $R_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *and* $R_2 = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$, *then we get that* $R^T Y^T Y R = X^T X$. *This is condition* (*iii*) *of the previous theorem.*

We note that during the author's computations, R *and* $Y^T Y$ *were discovered by using a Maple loop that used condition* (*iv*) *from the previous Theorem, and simply just tried every value of* R_1 *and* R_2. *The calculation considered thousands of possibilities. This is a brute force method that is not ideal, and certainly only possible when* k *is a finite field.* Y, *and then* B *were then calculated, and* Q *was computed using the formula* $Q = XRY^{-1}$, *as in the proof of the theorem.*

We now show that there does not exist $W \in \mathrm{SO}(4, \mathbb{F}_3)$ *such that* $B = W^{-1}AW$. *We proceed by contradiction and suppose that these does exist such an* W. *It then follows that* A *and* $QW^{-1} \in \mathrm{O}(4, \mathbb{F}_3)$ *are commuting matrices. It is a simple matter to show that matrices that commute with* A *must be of the form*

$$\begin{pmatrix} a & b & c & d \\ b & a+b & d & c+d \\ e & f & g & h \\ f & e+f & h & g+h \end{pmatrix}.$$

One such matrix is

$$\begin{pmatrix} 1 & 1 & 2 & 2 \\ 1 & 2 & 2 & 1 \\ 2 & 2 & 2 & 2 \\ 2 & 1 & 2 & 1 \end{pmatrix} \in \mathrm{SO}(4, \mathbb{F}_3).$$

But, all other such orthogonal matrices differ from this matrix only in that an even number of rows and/or columns have been multiplied by $2 = -1$ *or an even number of rows and/or* *columns have been swapped. All of these actions create matrices that will also have determinant 1. Thus, all the matrices in* $\mathrm{O}(4, \mathbb{F}_3)$ *which commute with* A *are also members of* $\mathrm{SO}(4, \mathbb{F}_3)$*, which contradicts* $QW^{-1} \in \mathrm{O}(4, \mathbb{F}_3)$ *commuting with* A*. So, no such* $W \in \mathrm{SO}(4, \mathbb{F}_3)$ *can exist, which means we cannot strengthen the above theorem by replacing* $\mathrm{O}(n, k, \beta)$ *with* $\mathrm{SO}(n, k, \beta)$ *in conditions* (i) *and* (ii)*.*

Corollary 2.2.9. *Suppose* Inn_A *and* Inn_B *are both Type 2 involutions of* $\mathrm{SO}(n, k, \beta)$*. Then,* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{O}(n, k, \beta)$ *if and only if they are isomorphic over* $\mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$*.*

Proof. When viewed as Type 2 involutions of $\mathrm{SO}(n, k, \beta)$, we can write

$$A = -\frac{\sqrt{\alpha}}{\alpha} U \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix} U^{-1} \text{ where } U^T M U = \begin{pmatrix} U_1 & U_2 \\ U_2 & \frac{1}{\alpha} U_1 \end{pmatrix}$$

and

$$B = -\frac{\sqrt{\alpha}}{\alpha} V \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix} V^{-1} \text{ where } V^T M V = \begin{pmatrix} V_1 & V_2 \\ V_2 & \frac{1}{\alpha} V_1 \end{pmatrix}$$

and U_1, U_2, V_1 and V_2 are diagonal matrices.

When Inn_A and Inn_B are viewed as involutions of $\mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$, then they are Type 1 involutions. Further, we can choose X and $Y \in \mathrm{GL}(n, k[\sqrt{\alpha}])$ such that $A = X \begin{pmatrix} -I_{\frac{n}{2}} & 0 \\ 0 & I_{\frac{n}{2}} \end{pmatrix} X^{-1}$, $B = Y \begin{pmatrix} -I_{\frac{n}{2}} & 0 \\ 0 & I_{\frac{n}{2}} \end{pmatrix} Y^{-1}$, and

$$X_1 = \frac{1}{2}(U_1 + \sqrt{\alpha} U_2),$$

$$X_2 = \frac{1}{2}(U_1 - \sqrt{\alpha} U_2),$$

$$Y_1 = \frac{1}{2}(V_1 + \sqrt{\alpha} V_2),$$

and

$$Y_2 = \frac{1}{2}(V_1 - \sqrt{\alpha} V_2).$$

This follows from the way in which U and V are constructed from the eigenvalues of A and B. We need to simply have X and Y consist of the appropriate eigenvectors, and mandate that the last $\frac{n}{2}$ columns of X and Y are the $\sqrt{\alpha}$-conjugates of the first $\frac{n}{2}$ columns. (The only exception to this is that we may need to negate the first column of X, so that we can preserve isomorphy of Inn_A and Inn_B over $\mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$, if we are assuming that. But, this will not change the value of X_1.)

Now, suppose Inn_A and Inn_B are isomorphic over $\mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$ as Type 1 involutions. Then, from Theorem 2.2.3 we know that Y_1 is congruent to either X_1 or X_2.

In the first case, we see that

$$\frac{1}{2}(V_1 + \sqrt{\alpha}V_2) = Y_1 = (R_1 + \sqrt{\alpha}R_2)^T X_1 (R_1 + \sqrt{\alpha}R_2)$$

$$= (R_1 + \sqrt{\alpha}R_2)^T \frac{1}{2}(U_1 + \sqrt{\alpha}U_2)(R_1 + \sqrt{\alpha}R_2),$$

where R_1 and R_2 are over k.

In the second case, we see that

$$\frac{1}{2}(V_1 + \sqrt{\alpha}V_2) = Y_1 = (R_1 + \sqrt{\alpha}R_2)^T X_2 (R_1 + \sqrt{\alpha}R_2)$$

$$= (R_1 + \sqrt{\alpha}R_2)^T \frac{1}{2}(U_1 - \sqrt{\alpha}U_2)(R_1 + \sqrt{\alpha}R_2),$$

where R_1 and R_2 are over k.

It follows from this that

$$V_1 = R_1^T U_1 R_1 + \alpha R_2^T U_2 R_1 + \alpha R_1^T U_2 R_2 + \alpha R_2^T U_1 R_2$$

and

$$V_2 = R_2^T U_1 R_1 + R_1^T U_2 R_1 + \alpha R_2^T U_2 R_2 + R_1^T U_1 R_2,$$

or

$$V_1 = R_1^T U_1 R_1 - \alpha R_2^T U_2 R_1 - \alpha R_1^T U_2 R_2 + \alpha R_2^T U_1 R_2,$$

and

$$V_2 = R_2^T U_1 R_1 - R_1^T U_2 R_1 - \alpha R_2^T U_2 R_2 + R_1^T U_1 R_2.$$

The previous theorem tells us that this means that Inn_A and Inn_B are isomorphic over $\mathrm{O}(n, k, \beta)$. Since the converse is clear, then we have shown what was needed.

□

2.2.3 Type 3 Involutions

We now examine the Type 3 case. Recall that φ is a Type 3 involution if $\varphi = \mathrm{Inn}_A$, where $A \in \mathrm{O}(n, k, \beta)$ and $A^2 = -I$. Such matrices have eigenvalues $\pm i$, and are diagonalizable because the minimal polynomial has no repeated roots. We begin by proving a couple or results about the eigenvectors of such matrices.

Lemma 2.2.10. *Suppose* $A \in \mathrm{O}(n, k, \beta)$ *induces a Type 3 involution of* $\mathrm{SO}(n, k, \beta)$. *Also* *suppose $x, y \in k^n$ such that $x + iy \in E(A, -i)$. Then, $x - iy \in E(A, i)$. Likewise, if $u, v \in k^n$ such that $u + iv \in E(A, i)$, then $u - iv \in E(A, -i)$. Further,* $\dim(E(A, i)) = \dim(E(A, -i))$.

Proof. Suppose $x, y \in k^n$ such that $x + iy \in E(A, -i)$. Then,

$$A(x + iy) = -i(x + iy)$$

implies

$$Ax + iAy = y - ix.$$

If we take the complex conjugate, then we see that

$$Ax - iAy = y + ix.$$

This implies

$$A(x - it) = i(x - it),$$

which shows that $x - iy \in E(A, i)$. A similar proof will show that if $u, v \in k^n$ such that $u + iv \in E(A, i)$, then $u - iv \in E(A, -i)$.

Since $x+iy \in E(A, -i)$ implies $x-iy \in E(A, i)$ and vice versa, then we see that $\dim(E(A, i))$ $= \dim(E(A, -i))$. $\square$

Lemma 2.2.11. *Suppose $\vartheta = \mathrm{Inn}_A$ is a Type 3 involution of $\mathrm{SO}(n, k, \beta)$ where $A \in \mathrm{O}(n, k, \beta)$. Then, we can find $x_1, ..., x_{\frac{n}{2}}, y_1, ..., y_{\frac{n}{2}} \in k^n$ such that the $x_j + iy_j$ are a basis for $E(A, -i)$ and the $x_j - iy_j$ are a basis for $E(A, i)$.*

Proof. Since Inn_A is Type 3, then we are assuming that $A \in \mathrm{O}(n, k, \beta)$ and $A^2 = -I$. Note that this also means that n is even. It follows that all eigenvalues of A are $\pm i$. Since there are no repeated roots in the minimal polynomial of A, then we see that A is diagonalizable. We wish to construct bases for $E(A, i)$ and $E(A, -i)$ such that all the vectors lie in $k[i]^n$. Let $\{z_1, ..., z_n\}$ be a basis for k^n. For each j, let $u_j = z_j + iAz_j$ Note that

$$Au_j = A(z_j + iAz_j) = (A + iA^2)z_j = (A - iI)z_j = -i(z_j + iAz_j) = -iu_j.$$

So, $\{u_1, ..., u_n\}$ must span $E(A, -i)$. Thus, we can appropriately choose $\frac{n}{2}$ of these vectors and form a basis for $E(A, -i)$. Note that each of these vectors lies in $k[i]^n$. Label these basis vectors as $v_1, ..., v_{\frac{n}{2}}$. We can write each of these vectors as $v_j = x_j + iy_j$. By the previous lemma, we know that $x_j - iy_j \in E(A, i)$. Since these vectors will be linearly independent, then they form a basis for $E(A, i)$.

$\square$

We are now able to prove results that characterize the matrices that induce Type 3 involutions, and then use these characterizations to find conditions on these involutions that are equivalent to isomorphy. We will have to prove our result by looking at separate cases, depending on whether or not $i = \sqrt{-1}$ lies in k. We begin by assuming that $i \in k$.

Lemma 2.2.12. *Assume $i \in k$ and suppose $\vartheta = \mathrm{Inn}_A$ is a Type 3 involution of $\mathrm{SO}(n, k, \beta)$, where $A \in \mathrm{O}(n, k, \beta)$. Then, $A = X \begin{pmatrix} -iI_{\frac{n}{2}} & 0 \\ 0 & iI_{\frac{n}{2}} \end{pmatrix} X^{-1}$ for some $X \in \mathrm{GL}(n, k)$, where $X^T M X = \begin{pmatrix} 0 & X_1 \\ X_1 & 0 \end{pmatrix}$, where X_1 is a diagonal matrix.*

Proof. We know from Lemma 2.2.11 that we have bases for $E(A, -i)$ and $E(A, I)$ that lie in k^n. We will show that we can in fact choose bases $a_1, ..., a_{\frac{n}{2}}$ for $E(A, -i) \cap k^n$ and $b_1, ..., b_{\frac{n}{2}}$ for $E(A, i) \cap k^n$ such that $\beta(a_j, a_l) = 0 = \beta(b_j, b_l)$ and $\beta(a_j, b_l)$ is nonzero if and only if $j = l$. We will build these bases recursively.

First, we know that we can choose some nonzero $a_1 \in E(A, -i) \cap k^n$. Then, since β is non degenerate, we can choose a vector t such that $\beta(a_1, t) \neq 0$. We note that $E(A, -i) \oplus E(A, i) = k^n$, so we can choose $t_{-i} \in E(A, -i) \cap k^n$ and $t_i \in E(A, i) \cap k^n$ such that $t = t_{-i} + t_i$. Since $\beta(a_1, t_{-i}) = 0$, then it follows that $\beta(a_1, t_i) \in k$ is nonzero. Let $b_1 = t_i$.

Let $E_1 = \mathrm{Span}_k(a_1, b_1)$ and let F_1 be the orthogonal complement of E_1 in k^n. Since the system of linear equations

$$\beta(a_1, x) = 0$$

$$\beta(b_1, x) = 0$$

has $n - 2$ free variables, then we see that F_1 has dimension $n - 2$.

We now wish to find $a_2 \in F_1 \cap E(A, -i)$. Similar to the construction in the previous lemma, we can choose $x \in F_1$, and let $a_2 = x + iAx$. It follows that $a_2 \in F_1 \cap E(A, -i)$. Now we want $b_2 \in F_2 \cap E(A, i)$ such that $\beta(a_2, b_2) = 1$. Since $\beta|_{F_1}$ is non degenerate, then there exists some $y \in F_2$ such that $\beta(a_2, y) \neq 0$. Similar to the construction of b_1, we see that this implies the existence a vector b_2 that fits our criteria.

Now, we let $E_2 = \mathrm{Span}_k(a_1, a_2, b_1, b_2)$ and let F_2 be the orthogonal complement of E_2 in k^n. We continue this same argument $\frac{n}{2}$ times, until we have the bases that we wanted to find. Let

$$X = (a_1, ..., a_{\frac{n}{2}}, b_1, ..., b_{\frac{n}{2}}).$$

Then, the result follows. □

Theorem 2.2.13. *Assume that $i \in k$. Then, if Inn_A and Inn_B are both Type 3 involutions of $\mathrm{SO}(n, k, \beta)$, then Inn_A and Inn_B are isomorphic over $\mathrm{O}(n, k, \beta)$.*

Proof. Suppose we have two such involutions of $\mathrm{SO}(n,k,\beta)$. Let them be represented by matrices $A, B \in \mathrm{O}(n,k,\beta)$. By the previous Lemma, we can choose diagonal $X, Y \in \mathrm{GL}(n,k)$ such that

$$X^{-1}AX = \begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix} = Y^{-1}BY,$$

$$X^TMX = \begin{pmatrix} 0 & X_1 \\ X_1 & 0 \end{pmatrix},$$

and

$$Y^TMY = \begin{pmatrix} 0 & Y_1 \\ Y_1 & 0 \end{pmatrix}.$$

Since X_1 and Y_1 are both invertible diagonal matrices, then we can choose R_1 and $R_2 \in \mathrm{GL}(\frac{n}{2},k)$ such that $Y_1 = R_1^T X_1 R_2$. Let $R = \begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix}$ and $Q = XRY^{-1}$. It follows from this that $R^TX^TMXR = Y^TMY$. We will show that $Q \in \mathrm{O}(n,k,\beta)$ and $Q^{-1}AQ = B$. This will then prove that Inn_A and Inn_B lie in the same isomorphy class.

First we show that $Q \in \mathrm{O}(n,k,\beta)$. Note that

$$Q^TMQ = (XRY^{-1})^TM(XRY^{-1}) = (Y^{-1})^TR^T(X^TMX)RY^{-1}$$

$$= (Y^{-1})^T(Y^TMY)Y^{-1} = M,$$

which proves this claim.

Lastly, we show that $Q^{-1}AQ = B$. We first note that R and $\begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix}$ commute. Then, we see that

$$Q^{-1}AQ = (XRY^{-1})^{-1}A(XRY^{-1}) = YR^{-1}(X^{-1}AX)RY^{-1}$$

$$= YR^{-1}\begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix}RY^{-1} = YR^{-1}R\begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix}Y^{-1}$$

$$= Y\begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix}Y^{-1} = B.$$

We have shown what was needed. □

We now begin examining the case where $i \notin k$.

Lemma 2.2.14. *Assume $i \notin k$ and suppose $\vartheta = \mathrm{Inn}_A$ is a Type 3 involution of* $\mathrm{SO}(n, k, \beta)$*. Then,* $A = U \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix} U^{-1}$ *for*

$$U = \begin{pmatrix} a_1 & a_2 & \cdots & a_{\frac{n}{2}} & b_1 & b_2 & \cdots & b_{\frac{n}{2}} \end{pmatrix} \in \mathrm{GL}(n, k),$$

where the $a_j + ib_j$ are a basis for $E(A, -i)$, the $a_j - ib_j$ are a basis for $E(A, i)$, and $U^T M U = \begin{pmatrix} U_1 & 0 \\ 0 & U_1 \end{pmatrix}$ is a diagonal matrix.

Proof. We know from Lemma 2.2.11 that we have bases for $E(A, -i)$ and $E(A, I)$ that lie in $k[i]^n$. We will show that we can in fact choose bases $a_1 + ib_1, ..., a_{\frac{n}{2}} + ib_{\frac{n}{2}}$ for $E(A, -i) \cap k[i]^n$ and $a_1 - ib_1, ..., a_{\frac{n}{2}} - ib_{\frac{n}{2}}$ for $E(A, i) \cap k[i]^n$ such that $\beta(a_j + ib_j, a_l - ib_l)$ is nonzero if and only if $j = l$. From this, we will be able to show that $\beta(a_j, a_l) = 0 = \beta(b_j, b_l)$ when $j \neq l$ and $\beta(a_j, b_l) = 0$ for all j and l. We will build these bases recursively.

Recall that given any vector $x \in k^n$, we know that $x + iAx \in E(A, -i)$. We want to choose $x \in k^n$ such that $\beta(x, x) \neq 0$. (The reasons for this will become apparent.) M is an invertible matrix, so there are at least n instances of $e_j^T M e_l \neq 0$. If there is an instance where $j = l$, let $x = e_j$. If not, then instead we have $e_j^T M e_l = 0 = e_l^T M e_j$, and we let $x = e_j + e_l$. Then,

$$\beta(x, x) = \beta(e_j + e_l, e_j + e_l) = 2\beta(e_j, e_l) \neq 0.$$

So, we have $x \in k^n$ such that $\beta(x, x) \neq 0$, and we have $x + iAx \in E(A, -i)$. Let $a_1 = x$ and $b_1 = Ax$. So, $a_1 + ib_1 \in E(A, -i)$ and $a_1 - ib_1 \in E(A, i)$. From this, it follows that

$$\beta(a_1 + ib_1, a_1 - ib_1) = (\beta(a_1, a_1) + \beta(b_1, b_1)) + i(-\beta(a_1, b_1) + \beta(a_1, b_1)$$

$$= 2\beta(a_1, a_1) = 2\beta(x, x) \neq 0.$$

Let $E_1 = \mathrm{Span}_{k[i]}(a_1 + ib_1, a_1 - ib_1) = \mathrm{Span}_{k[i]}(a_1, b_1)$, and let F_1 be the orthogonal complement of E_1 over $k[i]$. F_1 has dimension $n - 2$, and $\beta|_{F_1}$ is nondegenerate. So, we can find a nonzero vector $x \in F_1 \cap k^n$ such that $\beta|_{F_1}(x, x) = 0$. So, as in the last case, let $a_2 = x$ and $b_2 = Ax$. As before, we have $\beta(a_1 + ib_1, a_1 - ib_1) \neq 0$.

Let $E_2 = \mathrm{Span}_{k[i]}(a_1, a_2, b_1, b_2)$, and let F_2 be the orthogonal complement of E_2 over $k[i]$. In this manner, we can create the bases that we noted in the opening paragraph of this proof.

Note that we always have

$$0 = \beta(a_j + ib_j, a_l + ib_l) = (\beta(a_j, a_l) - \beta(b_j, b_l)) + i(\beta(a_j, b_l) + \beta(b_j, a_l)),$$

and when $j \neq l$ we have

$$0 = \beta(a_j + ib_j, a_l - ib_l) = (\beta(a_j, a_l) + \beta(b_j, b_l)) + i(-\beta(a_j, b_l) + \beta(b_j, a_l)).$$

This tells us that when $j \neq l$ that

$$\beta(a_j, b_l) = \beta(a_j, a_l) = \beta(b_j, b_l) = 0.$$

When $j = l$, we see that $\beta(b_j, b_j) = \beta(a_j, a_j)$ and that $\beta(a_j, b_j) = -\beta(b_j, a_j)$. The last of these shows that $\beta(a_j, b_l) = 0$, regardless of the values of j and l.

Let

$$U = (a_1, ..., a_{\frac{n}{2}}, b_1, ..., b_{\frac{n}{2}}).$$

Then, it follows that $U^T MU = \begin{pmatrix} U_1 & 0 \\ 0 & U_1 \end{pmatrix}$ where U_1 is a diagonal $\frac{n}{2} \times \frac{n}{2}$ matrix.

Lastly, since $b_j = Aa_j$, then it follows that $Ab_j = -a_j$. So, we have that

$$A = U \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix} U^{-1}.$$

□

We now look at an example that highlights some of these results that we have just proven in the Type 3 case.

Example 2.2.15. *Assume that β is the standard dot product. Then, Inn_A can be a Type 3 involution of $\mathrm{SO}(4, \mathbb{R})$ only if we can choose A such that it is skew-symmetric and orthogonal since this will imply that $A^2 = -I$, and if the entries of A lie in k. Observe that the matrix*

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

is both skew-symmetric and orthogonal with entries in k, so it induces a Type 3 involution. It can be shown that $E(A, -i)$ has dimension 2. A basis for this subspace is formed by the vectors

$$v_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} + i \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

and

$$v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + i \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

It can be shown that

$$v_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} - i \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

and

$$v_4 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} - i \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

are $i-$eigenvectors of A, where these are the conjugates of v_1 and v_2, respectively.

Following the notation of the previous lemma, we have

$$U = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

where $U^T U = I$ and $A = U \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix} U^{-1}$. We note that $U_1 = I$.

We now find conditions on Type 3 involutions that are equivalent to isomorphy, in the case that $i \notin k$.

Theorem 2.2.16. *Assume $i \notin k$. Then, if Inn_A and Inn_B are both Type 3 involutions of $\mathrm{SO}(n,k,\beta)$, then Inn_A and Inn_B are isomorphic over $\mathrm{O}(n,k,\beta)$.*

Proof. By the previous Lemma, we can choose a matrix $U \in \mathrm{GL}(n,k)$ such that

$$A = U \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix} U^{-1} \text{ for } U = \begin{pmatrix} a_1 & a_2 & \cdots & a_{\frac{n}{2}} & b_1 & b_2 & \cdots & b_{\frac{n}{2}} \end{pmatrix} \in \mathrm{GL}(n,k),$$

where the $a_j + ib_j$ are a basis for $E(A,-i)$, the $a_j - ib_j$ are a basis for $E(A,i)$, and $U^T M U = \begin{pmatrix} U_1 & 0 \\ 0 & U_1 \end{pmatrix}$ is a diagonal matrix.

Let

$$X = (a_1 + ib_1, ..., a_{\frac{n}{2}} + ib_{\frac{n}{2}}, a_1 - ib_1, ..., a_{\frac{n}{2}} - ib_{\frac{n}{2}}),$$

and consider Inn_A and Inn_B as involutions of $\text{SO}(n, k[i], \beta)$. By construction, we see that X is a matrix that satisfies the conditions of Lemma 2.2.12 for the group $\text{SO}(n, k[i], \beta)$. We note that $X_1 = 2U_1$. We also know by the previous Theorem that Inn_A and Inn_B are isomorphic (when viewed as involutions of $\text{SO}(n, k[i], \beta)$) over $\text{O}(n, k[i], \beta)$. So, we can choose $Q_i \in \text{O}(n, k[i], \beta)$ such that $Q_i^{-1} A Q_i = B$. Let $Y = Q_i^{-1} X$. We now show a couple of facts about Y.

First, we note that since Y was obtained from X via row operations, then for $1 \leqslant j \leqslant \frac{n}{2}$, the jth and $\frac{n}{2} + j$th columns are i-conjugates of one another.

Also, note that

$$Y^{-1} B Y = (Q_i^{-1} X)^{-1} B (Q_i^{-1} X) = X^{-1} Q_i B Q_i^{-1} X$$

$$= X^{-1} A X = \begin{pmatrix} -iI_{\frac{n}{2}} & 0 \\ 0 & iI_{\frac{n}{2}} \end{pmatrix}.$$

Lastly, we see that

$$Y^T M Y = (Q_i^{-1} X)^T M (Q_i^{-1} X) = X^T ((Q_i^{-1})^T M Q_i) X$$

$$= X^T M X = \begin{pmatrix} 0 & X_1 \\ X_1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2U_1 \\ 2U_1 & 0 \end{pmatrix}.$$

We can write

$$Y = (c_1 + id_1, ..., c_{\frac{n}{2}} + id_{\frac{n}{2}}, c_1 - id_1, ..., c_{\frac{n}{2}} - id_{\frac{n}{2}})$$

where $c_j, d_j \in k^n$. So, let

$$V = (c_1, ..., c_{\frac{n}{2}}, d_1, ..., d_{\frac{n}{2}}) \in \text{GL}(n, k).$$

It follows from what we have shown that $B = V \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix} V^{-1}$ where

$$V^T M V = \begin{pmatrix} U_1 & 0 \\ 0 & U_1 \end{pmatrix} = U^T M U.$$

Now, let $Q = UV^{-1}$. We will show that $Q^{-1} A Q = B$ and $Q \in \text{O}(n, k, \beta)$. This will prove that Inn_A and Inn_B are isomorphic over $\text{O}(n, k, \beta)$.

We first show that $Q \in \mathrm{O}(n, k, \beta)$.

$$Q^T M Q = (UV^{-1})^T M U V^{-1} = (V^{-1})^T (U^T M U) V^{-1} = (V^{-1})^T (V^T M V) V^{-1} = M.$$

Lastly, we show that $Q^{-1}AQ = B$.

$$Q^{-1}AQ = (UV^{-1})^{-1} A (UV^{-1}) = VU^{-1}AUV^{-1}$$
$$= V \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix} V^{-1} = B.$$

We have shown what was needed.

□

Combining the results from this section, we get the following corollary.

Corollary 2.2.17. *If* Inn_A *and* Inn_B *are both Type 3 involutions of* $\mathrm{SO}(n, k, \beta)$*, then* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{O}(n, k, \beta)$*. That is,* $\mathrm{SO}(n, k, \beta)$ *has at most one isomorphy class of Type 3 involutions.*

2.2.4 Type 4 Involutions

We now move on to a similar classification in the Type 4 case. First, we characterize the eigenvectors of the matrices that induce these involutions. Recall that we can choose $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$ such that each entry of A is a $k-$multiple of $\sqrt{\alpha}$, and that we know $A^2 = -I$. We begin by proving a couple of lemmas about the eigenspaces of these matrices.

Lemma 2.2.18. *Suppose* $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$ *induces a Type 4 involution of* $\mathrm{SO}(n, k, \beta)$*. Also suppose* $x, y \in k^n$ *such that* $x + \sqrt{-\alpha}y \in E(A, -i)$*. Then,* $x - \sqrt{-\alpha}y \in E(A, i)$*. Likewise, if* $u, v \in k^n$ *such that* $u + \sqrt{-\alpha}v \in E(A, i)$*. Then,* $u - \sqrt{-\alpha}v \in E(A, -i)$*. Further,* $\dim(E(A, i)) = \dim(E(A, -i))$*.*

Proof. Suppose $x, y \in k^n$ such that $x + \sqrt{-\alpha}y \in E(A, -i)$. Then,

$$A(x + \sqrt{-\alpha}y) = -i(x + \sqrt{-\alpha}y)$$

which implies

$$Ax + \sqrt{-\alpha}Ay = \sqrt{\alpha}y - ix.$$

Then, complex conjugation tells us that

$$Ax - \sqrt{-\alpha}Ay = \sqrt{\alpha}y + ix,$$

which tells us that

$$A(x - \sqrt{-\alpha}y) = i(x - \sqrt{-\alpha}y).$$

A similar argument shows that if $u, v \in k^n$ such that $u + \sqrt{-\alpha}v \in E(A, i)$. Then, $u - \sqrt{-\alpha}v \in E(A, -i)$.

Since $x + \sqrt{-\alpha}y \in E(A, -i)$ implies $x - \sqrt{-\alpha}y \in E(A, i)$ and vice versa, then we see that $\dim(E(A, i)) = \dim(E(A, -i))$. □

Lemma 2.2.19. *Suppose $\vartheta = \mathrm{Inn}_A$ is a Type 4 involution of $\mathrm{SO}(n, k, \beta)$ where $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$. Then, we can find $x_1, ..., x_{\frac{n}{2}}, y_1, ..., y_{\frac{n}{2}} \in k^n$ such that the $x + \sqrt{-\alpha}y$ are a basis for $E(A, -i)$ and the $x - \sqrt{-\alpha}y$ are a basis for $E(A, i)$.*

Proof. Since Inn_A is Type 4, then we are assuming that $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$ and $A^2 = -I$. Note that this also means that n is even. It follows that all eigenvalues of A are $\pm i$. Since there are no repeated roots in the minimal polynomial of A, then we see that A is diagonalizable. We wish to construct bases for $E(A, i)$ and $E(A, -i)$ such that all the vectors lie in $k[i]^n$. Let $\{z_1, ..., z_n\}$ be a basis for k^n. For each j, let $u_j = (\sqrt{\alpha}A - \sqrt{-\alpha}I)z_j$. Note that

$$Au_j = A(\sqrt{\alpha}A - \sqrt{-\alpha}I)z_j = (\sqrt{\alpha}A^2 - \sqrt{-\alpha}A)z_j = -i(\sqrt{\alpha}A - \sqrt{-\alpha}I)z_j = -iu_j.$$

So, $\{u_1, ..., u_n\}$ must span $E(A, -i)$. Thus, we can appropriately choose $\frac{n}{2}$ of these vectors and form a basis for $E(A, -i)$. Note that each of these vectors lies in $k[i]^n$. Label these basis vectors as $v_1, ..., v_{\frac{n}{2}}$. We can write each of these vectors as $v_j = x_j + \sqrt{-\alpha}y_j$. By the previous lemma, we know that $x_j - \sqrt{-\alpha}y_j \in E(A, i)$, and it follows that these will be linearly independent. Since there are $\frac{n}{2}$ of them, then they form a basis for $E(A, i)$.

□

We are now able to prove results that characterize the matrices that induce Type 4 involutions, and then use these characterizations to find conditions on these involutions that are equivalent to isomorphy. We will have separate cases, depending on whether or not $\sqrt{-\alpha}$ lies in k. We begin by assuming that $\sqrt{-\alpha} \in k$. Since we are also assuming that $\sqrt{\alpha} \notin k$, then it follows from these two assumptions that α and -1 lie in the same square class of k. Thus, we can assume in this case that $\alpha = -1$, which means $\sqrt{-\alpha} = 1$.

Lemma 2.2.20. *Assume $\sqrt{-\alpha} \in k$ and suppose $\vartheta = \mathrm{Inn}_A$ is a Type 4 involution of $\mathrm{SO}(n, k, \beta)$. Then, $A = X \begin{pmatrix} -iI_{\frac{n}{2}} & 0 \\ 0 & iI_{\frac{n}{2}} \end{pmatrix} X^{-1}$ for some $X \in \mathrm{GL}(n, k)$, where $X^TMX = \begin{pmatrix} 0 & X_1 \\ X_1 & 0 \end{pmatrix}$, and X_1 is diagonal.*

Proof. We know from Lemma 2.2.19 that we have bases for $E(A, -i)$ and $E(A, I)$ that lie in k^n. We will show that we can in fact choose bases $a_1, ..., a_{\frac{n}{2}}$ for $E(A, -i) \cap k^n$ and $b_1, ..., b_{\frac{n}{2}}$ for

$E(A, i) \cap k^n$ such that $\beta(a_j, a_l) = 0 = \beta(b_j, b_l)$ and $\beta(a_j, b_l)$ is nonzero if and only if $j = l$. We will build these bases recursively.

First, we know that we can choose some nonzero $a_1 \in E(A, -i) \cap k^n$. Then, since β is non degenerate, we can choose a vector t such that $\beta(a_1, t) \neq 0$. We note that $E(A, -i) \oplus E(A, i) = k^n$, so we can choose $t_{-i} \in E(A, -i) \cap k^n$ and $t_i \in E(A, i) \cap k^n$ such that $t = t_{-i} + t_i$. Since $\beta(a_1, t_{-i}) = 0$, then it follows that $\beta(a_1, t_i) \in k$ is nonzero. Let $b_1 = t_i$.

Let $E_1 = \text{Span}_k(a_1, b_1)$ and let F_1 be the orthogonal complement of E_1 in k^n. Since the system of linear equations

$$\beta(a_1, x) = 0$$

$$\beta(b_1, x) = 0$$

has $n - 2$ free variables, then we see that F_1 has dimension $n - 2$.

We now wish to find $a_2 \in F_1 \cap E(A, -i)$. Similar to the construction in the previous lemma, we can choose $x \in F_1$, and let $a_2 = (\sqrt{\alpha}A - \sqrt{-\alpha}I)x$. It follows that $a_2 \in F_1 \cap E(A, -i)$. Now we want $b_2 \in F_2 \cap E(A, i)$ such that $\beta(a_2, b_2)$ is nonzero. Since $\beta|_{F_1}$ is non degenerate, then there exists some $y \in F_2$ such that $\beta(a_2, y) \neq 0$. Similar to the construction of b_1, we see that this implies the existence a vector b_2 that fits our criteria.

Now, we let $E_2 = \text{Span}_k(a_1, a_2, b_1, b_2)$ and let F_2 be the orthogonal complement of E_2 in k^n. We continue this same argument $\frac{n}{2}$ times, until we have the bases that we wanted to find. Let

$$X = (a_1, ..., a_{\frac{n}{2}}, b_1, ..., b_{\frac{n}{2}}).$$

Then, the result follows. □

Here is an example of a Type 4 involution when $\sqrt{-\alpha} \in k$.

Example 2.2.21. *Assume that β is the standard dot product and that $k = \mathbb{F}_3$, the field of three elements. So, $\sqrt{2} = i$. Observe that the matrix*

$$A = i \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 2 & 2 & 0 & 0 \\ 2 & 1 & 0 & 0 \end{pmatrix}$$

is both skew-symmetric and orthogonal. Since each entry is $\mathbb{F}_3-$multiple of i, then it follows from our work on automorphisms that Inn_A *is an involution of* $\text{SO}(4, \mathbb{F}_3)$ *of Type 4. A basis for*

$E(A,-i)$ is formed by the vectors

$$v_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}$$

and

$$v_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

It can be shown that

$$v_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

and

$$v_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 1 \\ 0 \end{pmatrix}$$

are $i-$eigenvectors of A.

Following the notation of the previous lemma, we have

$$X = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

where $X^T X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$ *and* $A = -iX \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -i & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \end{pmatrix} X^{-1}$. *We also note that $X_1 = I$.*

Now we characterize the isomorphy classes of Type 4 involutions in the case where $\sqrt{-\alpha} \in k$.

Theorem 2.2.22. *Assume that $\sqrt{-\alpha} \in k$. Then, if Inn_A and Inn_B are both Type 4 involutions* *of* $\mathrm{SO}(n,k,\beta)$ *where the entries of* A *and* B *are* k*-multiples of* $\sqrt{\alpha}$*, then* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{O}(n,k,\beta)$*.*

Proof. Suppose we have two such involutions of $\mathrm{SO}(n,k,\beta)$. Let them be represented by matrices $A, B \in \mathrm{O}(n,k,\beta)$. By the previous Lemma, we can choose $X, Y \in \mathrm{GL}(n,k)$ such that

$$X^{-1}AX = \begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix} = Y^{-1}BY,$$

$$X^T M X = \begin{pmatrix} 0 & X_1 \\ X_1 & 0 \end{pmatrix},$$

and

$$Y^T M Y = \begin{pmatrix} 0 & Y_1 \\ Y_1 & 0 \end{pmatrix},$$

where X_1 and Y_1 are diagonal.

Since X_1 and Y_1 are both invertible diagonal matrices, then we can choose R_1 and $R_2 \in \mathrm{GL}(\frac{n}{2},k)$ such that $Y_1 = R_1^T X_1 R_2$. Let $R = \begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix}$ and $Q = XRY^{-1}$. It follows from this that $R^T X^T M X R = Y^T M Y$. We will show that $Q \in \mathrm{O}(n,k,\beta)$ and $Q^{-1}AQ = B$. This will then prove that Inn_A and Inn_B lie in the same isomorphy class.

First we show that $Q \in \mathrm{O}(n,k,\beta)$. Note that

$$Q^T M Q = (XRY^{-1})^T M (XRY^{-1}) = (Y^{-1})^T R^T (X^T M X) R Y^{-1}$$

$$= (Y^{-1})^T (Y^T M Y) Y^{-1} = M,$$

which proves this claim.

Lastly, we show that $Q^{-1}AQ = B$. We first note that R and $\begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix}$ commute. Then, we see that

$$Q^{-1}AQ = (XRY^{-1})^{-1} A (XRY^{-1}) = YR^{-1}(X^{-1}AX)RY^{-1}$$

$$= YR^{-1} \begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix} RY^{-1} = YR^{-1}R \begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix} Y^{-1}$$

$$= Y \begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix} Y^{-1} = B.$$

We have shown what was needed.

□

We now examine the case where $\sqrt{-\alpha} \notin k$.

Lemma 2.2.23. *Assume $\sqrt{-\alpha} \notin k$ and suppose $\vartheta = \mathrm{Inn}_A$ is a Type 4 involution of $\mathrm{SO}(n, k, \beta)$. Then, $A = -\frac{\sqrt{\alpha}}{\alpha} U \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ -\alpha I_{\frac{n}{2}} & 0 \end{pmatrix} U^{-1}$ for*

$$U = \begin{pmatrix} a_1 & a_2 & \cdots & a_{\frac{n}{2}} & b_1 & b_2 & \cdots & b_{\frac{n}{2}} \end{pmatrix} \in \mathrm{GL}(n, k),$$

where the $a_j + \sqrt{-\alpha} b_j$ are a basis for $E(A, -i)$, the $a_j - \sqrt{-\alpha} b_j$ are a basis for $E(A, i)$, and $U^T M U = \begin{pmatrix} U_1 & 0 \\ 0 & \frac{1}{\alpha} U_1 \end{pmatrix}$ is diagonal.

Proof. We know from Lemma 2.2.19 that we have bases for $E(A, -i)$ and $E(A, I)$ that lie in $k[\sqrt{-\alpha}]^n$. We will show that we can in fact choose bases $a_1 + \sqrt{-\alpha} b_1, ..., a_{\frac{n}{2}} + \sqrt{-\alpha} b_{\frac{n}{2}}$ for $E(A, -i) \cap k[i]^n$ and $a_1 - \sqrt{-\alpha} b_1, ..., a_{\frac{n}{2}} - \sqrt{-\alpha} b_{\frac{n}{2}}$ for $E(A, i) \cap k[\sqrt{-\alpha}]^n$ such that $\beta(a_j + \sqrt{-\alpha} b_j, a_l - \sqrt{-\alpha} b_l)$ is nonzero if and only if $j = l$. From this, we will be able to show that $\beta(a_j, a_l) = 0 = \beta(b_j, b_l)$ when $j \neq l$ and $\beta(a_j, b_l) = 0$ for all j and l. We will build these bases recursively.

Given any vector $x \in k^n$, we know that $x + iAx \in E(A, -i)$. We want to choose $x \in k^n$ such that $\beta(x, x) \neq 0$. (The reasons for this will become apparent.) M is an invertible matrix, so there are at least n instances of $e_j^T M e_l \neq 0$. If there is an instance where $j = l$, let $x = e_j$. If instead we have $e_j^T M e_l = 0 = e_l^T M e_j$, then let $x = e_j + e_l$. We note that this works because

$$\beta(x, x) = \beta(e_j + e_l, e_j + e_l) = 2\beta(e_j, e_l) \neq 0.$$

So, we have $x \in k^n$ such that $\beta(x, x) \neq 0$, and we have $x + iAx \in E(A, -i)$. Let $a_1 = x$ and $b_1 = \frac{1}{\sqrt{\alpha}} Ax$. So, $a_1 + \sqrt{-\alpha} b_1 \in E(A, -i)$ and $a_1 - \sqrt{-\alpha} b_1 \in E(A, i)$. From this, it follows that

$$\beta(a_1 + \sqrt{-\alpha} b_1, a_1 - \sqrt{-\alpha} b_1) = (\beta(a_1, a_1) + \alpha\beta(b_1, b_1)) + \sqrt{-\alpha}(-\beta(a_1, b_1) + \beta(a_1, b_1)$$

$$= \beta(x, x) + \alpha\beta\left(\frac{1}{\sqrt{\alpha}} Ax, \frac{1}{\sqrt{\alpha}} Ax\right) = 2\beta(x, x) \neq 0.$$

Let $E_1 = \mathrm{Span}_{k[\sqrt{-\alpha}]}(a_1 + \sqrt{-\alpha} b_1, a_1 - \sqrt{-\alpha} b_1) = \mathrm{Span}_{k[\sqrt{-\alpha}]}(a_1, b_1)$, and let F_1 be the orthogonal complement of E_1 over $k[\sqrt{-\alpha}]$. F_1 has dimension $n - 2$, and $\beta|_{F_1}$ is nondegenerate. So, we can find a nonzero vector $x \in F_1 \cap k^n$ such that $\beta|_{F_1}(x, x) = 0$. So, as in the last case, let $a_2 = x$ and $b_2 = \frac{1}{\sqrt{\alpha}} Ax$. As before, we have $\beta(a_2 + \sqrt{-\alpha} b_2, a_2 - \sqrt{-\alpha} b_2) \neq 0$.

Let $E_2 = \mathrm{Span}_{k[\sqrt{-\alpha}]}(a_1, a_2, b_1, b_2)$, and let F_2 be the orthogonal complement of E_2 over $k[\sqrt{-\alpha}]$. In this manner, we can create the bases that we noted in the opening paragraph of this proof.

Note that we always have

$$0 = \beta(a_j + \sqrt{-\alpha}b_j, a_l + \sqrt{-\alpha}b_l) = (\beta(a_j, a_l) - \alpha\beta(b_j, b_l)) + \sqrt{-\alpha}(\beta(a_j, b_l) + \beta(b_j, a_l)),$$

and when $j \neq l$ we have

$$0 = \beta(a_j + \sqrt{-\alpha}b_j, a_l - \sqrt{-\alpha}b_l) = (\beta(a_j, a_l) + \alpha\beta(b_j, b_l)) + \sqrt{-\alpha}(-\beta(a_j, b_l) + \beta(b_j, a_l)).$$

This tells us that when $j \neq l$ that

$$\beta(a_j, b_l) = \beta(a_j, a_l) = \beta(b_j, b_l) = 0.$$

When $j = l$, we see that $\beta(b_j, b_j) = \frac{1}{\alpha}\beta(a_j, a_j)$ and that $\beta(a_j, b_j) = -\beta(b_j, a_j)$. The last of these shows that $\beta(a_j, b_l) = 0$, regardless of the values of j and l.

Let

$$U = (a_1, ..., a_{\frac{n}{2}}, b_1, ..., b_{\frac{n}{2}}).$$

Then, it follows that $U^T M U = \begin{pmatrix} U_1 & 0 \\ 0 & \frac{1}{\alpha}U_1 \end{pmatrix}$ where U_1 is a diagonal $\frac{n}{2} \times \frac{n}{2}$ matrix.

Lastly, since $b_j = \frac{1}{\sqrt{\alpha}}Aa_j$, then it follows that $Ab_j = -\frac{1}{\sqrt{\alpha}}a_j$. So, we have that $A = -\frac{\sqrt{\alpha}}{\alpha}U \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ -\alpha I_{\frac{n}{2}} & 0 \end{pmatrix} U^{-1}$.

□

Here is an example of a Type 4 involution in the case that $\sqrt{-\alpha} \notin k$.

Example 2.2.24. *Assume that β is the standard dot product. Then, Inn_A can be a Type 4 involution of $\mathrm{SO}(4, \mathbb{Q})$ only if $A \notin \mathrm{O}(4, \mathbb{Q})$ is skew-symmetric and orthogonal (if we scale A appropriately), since this will imply that $A^2 = -I$. Observe that the matrix*

$$A = \frac{\sqrt{2}}{2} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ -1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \end{pmatrix}$$

is both skew-symmetric and orthogonal. Since each entry is $k-$multiple of $\sqrt{2}$, then it follows from our work on automorphisms that Inn_A is an involution of $\mathrm{SO}(4, \mathbb{Q})$ of Type 4. It can be *shown that $E(A,-i)$ has dimension 2. A basis for this subspace is formed by the vectors*

$$v_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} + \sqrt{-2}\begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ 0 \\ 0 \end{pmatrix}$$

and

$$v_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \sqrt{-2}\begin{pmatrix} -\frac{1}{2} \\ -\frac{1}{2} \\ 0 \\ 0 \end{pmatrix}.$$

It can be shown that

$$v_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} - \sqrt{-2}\begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ 0 \\ 0 \end{pmatrix}$$

and

$$v_4 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} - \sqrt{-2}\begin{pmatrix} -\frac{1}{2} \\ -\frac{1}{2} \\ 0 \\ 0 \end{pmatrix}$$

are $i-$eigenvectors of A, where these are the conjugates of v_1 and v_2, respectively.

Following the notation of the previous lemma, we have

$$U = \begin{pmatrix} 0 & 0 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & \frac{1}{2} & -\frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

where $U^TU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}$ *and* $A = -\frac{\sqrt{2}}{2}U\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -\sqrt{2} & 0 & 0 & 0 \\ 0 & -\sqrt{2} & 0 & 0 \end{pmatrix}U^{-1}$ *. We also note that $U_1 = I$.*

We now find conditions on Type 4 involutions that are equivalent to isomorphy in the case where $\sqrt{-\alpha} \notin k$.

Theorem 2.2.25. *Assume $\sqrt{-\alpha} \notin k$. Then, if* Inn_A *and* Inn_B *are both Type 4 involutions of* $\mathrm{SO}(n, k, \beta)$ *where the entries of A and B are k-multiples of $\sqrt{\alpha}$, then* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{O}(n, k, \beta)$.

Proof. By Lemma 2.2.23, we can choose a matrix $U \in \mathrm{GL}(n, k)$ such that

$$A = -\frac{\sqrt{\alpha}}{\alpha} U \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ -\alpha I_{\frac{n}{2}} & 0 \end{pmatrix} U^{-1}$$

for

$$U = \begin{pmatrix} a_1 & a_2 & \cdots & a_{\frac{n}{2}} & b_1 & b_2 & \cdots & b_{\frac{n}{2}} \end{pmatrix},$$

where the $a_j + \sqrt{-\alpha} b_j$ are a basis for $E(A, -i)$, the $a_j - \sqrt{-\alpha} b_j$ are a basis for $E(A, i)$, and $U^T M U = \begin{pmatrix} U_1 & 0 \\ 0 & \frac{1}{\alpha} U_1 \end{pmatrix}$ is diagonal.

Consider Inn_A and Inn_B as involutions of $\mathrm{SO}(n, k[\sqrt{-\alpha}], \beta)$. If $k[\sqrt{-\alpha}] = k[\sqrt{\alpha}]$, then these are Type 3 involutions of $\mathrm{SO}(n, k[\sqrt{-\alpha}], \beta)$, since A and B would have entries in the field, and $i \in k[\sqrt{-\alpha}]$. Otherwise, if $k[\sqrt{-\alpha}] \neq k[\sqrt{\alpha}]$, then these are Type 4 involutions where $\sqrt{-\alpha} \in k[\sqrt{-\alpha}]$.

Let

$$X = (a_1 + \sqrt{-\alpha} b_1, ..., a_{\frac{n}{2}} + \sqrt{-\alpha} b_{\frac{n}{2}}, a_1 - \sqrt{-\alpha} b_1, ..., a_{\frac{n}{2}} - \sqrt{-\alpha} b_{\frac{n}{2}}).$$

By construction, we see that X is a matrix that satisfies the conditions of Lemma 2.2.14 or Lemma 2.2.20 for the group $\mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$. We note that $X_1 = 2U_1$. We also know by Corollary 2.2.17 or Theorem 2.2.22 that Inn_A and Inn_B are isomorphic (when viewed as involutions of $\mathrm{SO}(n, k[\sqrt{-\alpha}], \beta)$) over $\mathrm{O}(n, k[\sqrt{-\alpha}], \beta)$. So, we can choose $Q_\alpha \in \mathrm{O}(n, k[\sqrt{-\alpha}], \beta)$ such that $Q_\alpha^{-1} A Q_\alpha = B$. Let $Y = Q_\alpha^{-1} X$. Since Y is constructed by doing row operations on X, then we can write

$$Y = (c_1 + \sqrt{-\alpha} d_1, ..., c_{\frac{n}{2}} + \sqrt{-\alpha} d_{\frac{n}{2}}, c_1 - \sqrt{-\alpha} d_1, ..., c_{\frac{n}{2}} - \sqrt{-\alpha} c_{\frac{n}{2}}),$$

where $c_j, d_j \in k^n$. We now show a couple of facts about Y.

First, we note that since Y was obtained from X via row operations, then for $1 \leqslant j \leqslant \frac{n}{2}$, the jth and $\frac{n}{2} + j$th columns are i-conjugates of one another.

Next, we observe that

$$Y^{-1} B Y = (Q_\alpha^{-1} X)^{-1} B (Q_\alpha^{-1} X) = X^{-1} Q_\alpha B Q_\alpha^{-1} X$$

$$= X^{-1} A X = \begin{pmatrix} -i I_{\frac{n}{2}} & 0 \\ 0 & i I_{\frac{n}{2}} \end{pmatrix}.$$

Lastly, we see that

$$Y^TMY = (Q_\alpha^{-1}X)^TM(Q_\alpha^{-1}X) = X^T((Q_\alpha^{-1})^TMQ_\alpha)X$$

$$= X^TMX = \begin{pmatrix} 0 & X_1 \\ X_1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2U_1 \\ 2U_1 & 0 \end{pmatrix}.$$

Let

$$V = (c_1, ..., c_{\frac{n}{2}}, d_1, ..., d_{\frac{n}{2}}) \in \mathrm{GL}(n,k).$$

It follows from what we have shown that $B = -\frac{\sqrt{\alpha}}{\alpha}V\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ -\alpha I_{\frac{n}{2}} & 0 \end{pmatrix}V^{-1}$ where $V^TMV = \begin{pmatrix} U_1 & 0 \\ 0 & \frac{1}{\alpha}U_1 \end{pmatrix} = U^TMU$.

Now, let $Q = UV^{-1}$. We will show that $Q^{-1}AQ = B$ and $Q \in \mathrm{O}(n,k,\beta)$. This will prove that Inn_A and Inn_B are isomorphic over $\mathrm{O}(n,k,\beta)$.

We first show that $Q \in \mathrm{O}(n,k,\beta)$.

$$Q^TMQ = (UV^{-1})^TMUV^{-1} = (V^{-1})^T(U^TMU)V^{-1} = (V^{-1})^T(V^TMV)V^{-1} = M.$$

Lastly, we show that $Q^{-1}AQ = B$.

$$Q^{-1}AQ = (UV^{-1})^{-1}A(UV^{-1}) = VU^{-1}AUV^{-1}$$

$$= -\frac{\sqrt{\alpha}}{\alpha}V\begin{pmatrix} 0 & I_{\frac{n}{2}} \\ -\alpha I_{\frac{n}{2}} & 0 \end{pmatrix}V^{-1} = B.$$

We have shown what was needed.

□

Combining the results from this section, we get the following corollary.

Corollary 2.2.26. *If* Inn_A *and* Inn_B *are both Type 4 involutions of* $\mathrm{SO}(n,k,\beta)$*, then* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{O}(n,k,\beta)$ *if and only if* A *and* B *have entries lying in the same field extension of* k*. That is,* $\mathrm{SO}(n,k,\beta)$ *has at most* $|k^*/(k^*)^2| - 1$ *isomorphy classes of Type 4 involutions.*

2.3 Types 1 and 2 Involutions as products of reflections

In this section, we take a slight detour from our main task of finding the isomorphy classes of involutions to see that if Inn_A is a Type 1 or 2 involution of $\mathrm{SO}(n,k,\beta)$ where $A \in \mathrm{O}(n,k[\sqrt{\alpha}],\beta)$, then A is actually the product of $m = \dim(E(A, -1))$ commuting reflections.

Definition 2.3.1. *Fix a non-degenerate symmetric bilinear form β. Choose a vector $x \in k^n$ such that $\beta(x, x) = x^T M x \neq 0$. We call matrices reflections if they are of the form $S_x = I - 2\frac{xx^T M}{x^T M x}$.*

We now recall some well-known facts about reflections that follow directly from the definition.

Proposition 2.3.2. *Suppose S_x is a reflection for some $x \in k^n$. Then we have the following:*

(i) $S_x(x) = -x$, *and x spans the -1 Eigenspace of S_x.*

(ii) *y is perpendicular to x if and only if $S_x(y) = y$.*

(iii) $S_x^2 = I$. *That is, S_x is an involution.*

(iv) $S_x \in \mathrm{O}(n, k, \beta) \setminus \mathrm{SO}(n, k, \beta)$.

We also recall this well-known fact from linear algebra.

Lemma 2.3.3. *Let $A, B \in \mathrm{GL}(n, k)$ be diagonalizable. Then, $AB = BA$ if and only if A and B are simultaneously diagonalizable.*

With the previous results in mind, we can show when two reflections are commutative.

Lemma 2.3.4. *Let $x_1, ..., x_n$ be an orthogonal basis for k^n with respect to a non-degenerate symmetric bilinear form β such that $x_i^T M x_j \neq 0$. Then, for any $x_i, x_j \in \{x_1, ..., x_n\}$, S_{x_i} and S_{x_j} commute.*

Proof. Assume the hypotheses. Then, let Q be the matrix with these vectors as the columns, where x_i is the ith column of Q. We will prove the result for x_1 and x_2, and observe that all other cases are similar. Note that

$$Q^{-1} S_{x_1} Q = \begin{pmatrix} -1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & & 0 \\ 0 & 0 & 1 & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

and

$$Q^{-1} S_{x_2} Q = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & & 0 \\ 0 & 0 & 1 & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

So, S_{x_1} and S_{x_2} are both simultaneously diagonalizable, therefore they must commute.

$\square$

We are now able to show that for A to induce a Type 1 or Type 2 involution on $\mathrm{SO}(n,k,\beta)$, then it must be the product of orthogonal reflections. That is, the vectors that induce these reflections are orthogonal to one another.

Proposition 2.3.5. *Suppose $A \in \mathrm{O}(n,k[\sqrt{\alpha}],\beta)$ is a matrix such that Inn_A is a Type 1 or Type 2 involution of $\mathrm{SO}(n,k,\beta)$, for some $\alpha \in k$. Then A can be minimally written as the product of $m \leqslant n$ orthogonal reflections of the form $S_x = I - 2\frac{xx^TM}{x^TMx}$ for some $x \in k[\sqrt{\alpha}]^n$. That is, we can write $A = S_{x_1}\cdots S_{x_m}$ where $x_i^TMx_j = 0$ whenever $i \neq j$. Further, $m = \dim(E(A,-1))$, that is, m is the dimension of the -1 eigenspace of A. If β is the standard dot product, then A is symmetric.*

Proof. Choose $x_1,...,x_m \in E(A,-1)$, where these vectors form an orthogonal basis of $E(A,-1)$ when viewed as a subspace of $k[\sqrt{\alpha}]^n$. We also know from previous results that all of these vectors are such that $x_i^TMx_i \neq 0$. Likewise, choose $x_{m+1},...,x_n \in E(A,1)$, where these vectors form an orthogonal basis of $E(A,1)$ when viewed as a subspace of $k[\sqrt{\alpha}]^n$ such that $x_i^TMx_i \neq 0$. We claim $A = S_{x_1}\cdots S_{x_m}$.

To prove this, we first show that $x_1,...,x_n$ forms an orthogonal basis for k^n. It suffices to show that 1-eigenvectors and -1-eigenvectors are orthogonal. So, suppose $Ax_i = x_i$ and $Ax_j = -x_j$. Then,

$$x_i^TMx_j = (Ax_i)^TM(-Ax_j) = -x_i^TA^TMAx_j = -x_i^TMx_j,$$

which can only be true if $x_i^TMx_j = 0$, as desired. So, $x_1,...,x_n$ is indeed an orthogonal basis of k^n.

We will now show that $A = S_{x_1}\cdots S_{x_m}$. Note that since the set

$$\{x_1,...,x_n\}$$

is orthogonal, that the reflections $S_{x_1},...,S_{x_m}$ are all pairwise commutative. So, it follows that

$$S_{x_1}\cdots S_{x_m}x_i = -x_i$$

when $1 \leqslant i \leqslant m$ and

$$S_{x_1}\cdots S_{x_m}x_i = x_i$$

when $m+1 \leqslant i \leqslant n$.

Choose $v \in k^n$ and write

$$v = \gamma_1x_1 + \cdots + \gamma_nx_n.$$

Observe that

$$\begin{aligned} Av &= A(\gamma_1 x_1 + \cdots + \gamma_n x_n) \\ &= \gamma_1 A x_1 + \cdots + \gamma_n A x_n \\ &= -\gamma_1 x_1 - \cdots - \gamma_m x_m + \gamma_{m+1} x_{m+1} + \cdots + \gamma_n x_n, \end{aligned}$$

and that

$$\begin{aligned} (S_{x_1} \cdots S_{x_m})v &= (S_{x_1} \cdots S_{x_m})(\gamma_1 x_1 + \cdots + \gamma_n x_n) \\ &= \gamma_1 (S_{x_1} \cdots S_{x_m}) x_1 + \cdots + \gamma_n (S_{x_1} \cdots S_{x_m}) x_n \\ &= -\gamma_1 x_1 - \cdots - \gamma_m x_m + \gamma_{m+1} x_{m+1} + \cdots + \gamma_n x_n. \end{aligned}$$

This proves that $A = S_{x_1} \cdots S_{x_m}$, and the rest of the claim in the general β case.

If we assume that β is the standard dot product, then $A^T = (S_{x_1} \cdots S_{x_m})^T = S_{x_m}^T \cdots S_{x_1}^T = S_{x_m} \cdots S_{x_1} = S_{x_1} \cdots S_{x_m} = A$, which shows that A is symmetric.

□

If we combine this with some of the results from the previous section, then we get the following theorem.

Theorem 2.3.6. *Suppose φ is a Type 1 or Type 2 involution of $\mathrm{SO}(n, k, \beta)$. Then, there exists an orthogonal matrix A such that $\mathrm{Inn}_A = \varphi$. Further, A is the product of $m \leqslant n$ orthogonal reflections. That is, $A = S_{x_1} \cdots S_{x_m}$ where $x_i^T M x_j = 0$ if $i \neq j$. Further,*

- *(i) if n is odd, then we can choose $x_i \in k^n$ for each i, and $A \in \mathrm{SO}(n, k, \beta)$;*
- *(ii) if n is even and $A \in \mathrm{O}(n, k, \beta)$, then we can choose $x_i \in k^n$ for each i;*
- *(iii) if n is even and $A \notin \mathrm{O}(n, k, \beta)$, then $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$ for some $\alpha \in k$ such that $\sqrt{\alpha} \notin k$ where $\sqrt{\alpha} A \in \mathrm{GL}(n, k)$, $m = \frac{n}{2}$ and $x_j = u_j + \sqrt{\alpha} v_j$ for some nonzero $u_j, v_j \in k^n$ for each j.*

We make one final observation in this section about involutions that are actually outer automorphisms of $\mathrm{SO}(n, \overline{k}, \beta)$. Recall that in this case n must be even.

Corollary 2.3.7. *If $k = \overline{k}$ and Inn_A is an involution of $\mathrm{SO}(n, \overline{k}, \beta)$, then Inn_A is an outer automorphism if and only if Inn_A is Type 1 or 2 and $\dim(E(A, -1))$ is odd. That is, the matrix A must be the product of an odd number of reflections.*

2.4 Maximal Number of Isomorphy classes

From the work we have done, it follows that the maximum number of isomorphy classes of involutions of $\mathrm{SO}(n,k,\beta)$ over $\mathrm{O}(n,k,\beta)$ is a function of the number of square classes of k, and the number of congruency classes of invertible diagonal matrices over k. We first define the following formulas.

Definition 2.4.1. *Let $\tau_1(k) = |k^*/(k^*)^2| - 1$ and $\tau_2(m,k)$ be the number of congruency classes of invertible symmetric matrices of $\mathrm{GL}(m,k)$ over $\mathrm{GL}(m,k)$.*

Let $C_1(n,k,\beta)$, $C_2(n,k,\beta)$, $C_3(n,k,\beta)$ and $C_4(n,k,\beta)$ be the number of isomorphy classes of $\mathrm{SO}(n,k,\beta)$ involutions over $\mathrm{O}(n,k,\beta)$ of types 1, 2, 3, and 4, respectively.

From our previous work, we have the following:

Corollary 2.4.2. *(i) If n is odd, then*

$$C_1(n,k,\beta) \leqslant \left(\sum_{m=1}^{\frac{n-1}{2}} \tau_2(n-m,k)\tau_2(m,k) \right).$$

If n is even, then

$$C_1(n,k,\beta) \leqslant \left(\sum_{m=1}^{\frac{n}{2}-1} \tau_2(n-m,k)\tau_2(m,k) \right) + \binom{\tau_2(\frac{n}{2},k)}{2} + \tau_2\left(\frac{n}{2},k\right).$$

(ii) If n is even, then

$$C_2(n,k,\beta) \leqslant \tau_1(k) \left(\binom{\tau_2(\frac{n}{2},k)}{2} + \tau_2\left(\frac{n}{2},k\right) \right).$$

(iii) If n is even, then

$$C_3(n,k,\beta) \leqslant 1.$$

(iv) If n is even, then

$$C_4(n,k,\beta) \leqslant \tau_1(k).$$

(v) If n is odd, then $C_2(n,k,\beta) = C_3(n,k,\beta) = C_4(n,k,\beta) = 0$.

We now list values of τ_1 and τ_2 for a few classes of fields.

Table 2.2: Some values of $\tau_1(k)$

k	$\overline{k}$	$\mathbb{R}$	$\mathbb{F}_q$, $2 \not| q$	$\mathbb{Q}_2$, $p \neq 2$	$\mathbb{Q}_2$
$\tau_1(k)$	0	1	1	3	7

Table 2.3: Some values of $\tau_2(m,k)$

k	$\overline{k}$	$\mathbb{R}$	$\mathbb{F}_q$, $2 \not| q$
$\tau_1(k)$	1	2	$m+1$

For the $\mathbb{Q}_p$, τ_2 is a bit more difficult. Here we have

$$\tau_2(m, \mathbb{Q}_p) = \begin{cases} 1 + \cdots \begin{pmatrix} 3 \\ m \end{pmatrix}, & m \leqslant 3 \\ 2^3, & m \geqslant 3 \end{cases}$$

when $p \neq 2$ and

$$\tau_2(m, \mathbb{Q}_2) = \begin{cases} 1 + \cdots \begin{pmatrix} 7 \\ m \end{pmatrix}, & m \leqslant 7 \\ 2^7, & m \geqslant 7 \end{cases}.$$

Based on these values of τ_1 and τ_2, it is a straightforward matter to compute the maximal value of $C_j(n,k,\beta)$ for the fields mentioned above. We do so explicitly for the fields $\overline{k}$, $\mathbb{R}$, and $\mathbb{F}_q$ where $2 \not| q$.

Corollary 2.4.3. *Suppose $k = \overline{k}$*

(i) If n is odd, then $C_1(n,\overline{k},\beta) \leqslant \frac{n-1}{2}$. If n is even, then $C_1(n,\overline{k},\beta) \leqslant \frac{n}{2}$.

(ii) $C_2(n,\overline{k},\beta) = 0$.

(iii) If n is odd, then $C_3(n,\overline{k},\beta) = 0$. If n is even, then $C_3(n,\overline{k},\beta) \leqslant 1$.

(iv) $C_4(n,\overline{k},\beta) = 0$.

Now suppose $k = \mathbb{R}$

(i) If n is odd, then

$$C_1(n,\mathbb{R},\beta) \leqslant \sum_{m=1}^{\frac{n-1}{2}} (m+1)(n-m+1).$$

If n is even, then

$$C_1(n,\mathbb{R},\beta) \leqslant \left(\sum_{m=1}^{\frac{n-1}{2}} (m+1)(n-m+1)\right) + \begin{pmatrix} \frac{n}{2}+1 \\ 2 \end{pmatrix} + \frac{n}{2} + 1.$$

(*ii*) *If n is odd, then $C_2(n,\mathbb{R},\beta) = 0$. If n is even, then*

$$C_2(n,\mathbb{R},\beta) \leqslant \begin{pmatrix} \frac{n}{2}+1 \\ 2 \end{pmatrix} + \frac{n}{2} + 1.$$

(*iii*) *If n is odd, then $C_3(n,\mathbb{R},\beta) = 0$. If n is even, then $C_3(n,\mathbb{R},\beta) \leqslant 1$.*

(*iv*) *If n is odd, then $C_4(n,\mathbb{R},\beta) = 0$. If n is even, then $C_4(n,\mathbb{R},\beta) \leqslant 1$.*

Lastly, suppose $k = \mathbb{F}_q$ such that $2 \not| q$.

(*i*) *If n is odd, then $C_1(n,\mathbb{F}_q,\beta) \leqslant 2n-2$. If n is even, then $C_1(n,\mathbb{F}_q,\beta) \leqslant 2n-1$.*

(*ii*) *If n is odd, then $C_2(n,\mathbb{F}_q,\beta) = 0$. If n is even, then $C_2(n,\mathbb{F}_q,\beta) \leqslant 3$.*

(*iii*) *If n is odd, then $C_3(n,\mathbb{F}_q,\beta) = 0$. If n is even, then $C_3(n,\mathbb{F}_q,\beta) \leqslant 1$.*

(*iv*) *If n is odd, then $C_4(n,\mathbb{F}_q,\beta) = 0$. If n is even, then $C_4(n,\mathbb{F}_q,\beta) \leqslant 1$.*

2.5 Explicit Examples

2.5.1 Algebraically Closed Fields

We now find the exact number of isomorphy classes for some friendly $\mathrm{SO}(n,k,\beta)$. We begin by looking at the case where $k = \overline{k}$. Note that all symmetric non degenerate bilinear forms are congruent to the dot product over an algebraically closed field.

Corollary 2.5.1. *Assume $k = \overline{k}$. If ϑ is an involution of $\mathrm{SO}(n,k)$, then ϑ is isomorphic to Inn_A where $A = \begin{pmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{pmatrix}$ and $0 \leqslant m < \frac{n}{2}$, or $A = \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix}$.*

Proof. Since k is algebraically closed, we know that all involutions of $\mathrm{SO}(n,k)$ are of Type 1 or 3. We first deal with the Type 1 case. We can write $A = X \begin{pmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{pmatrix} X^{-1}$, where we know X^TX is diagonal. We know that X^TX must be congruent to I. Since we are looking for representatives of our isomorphy class, we assume $X^T X = I$, and we can choose $X = I$, which means $A = \begin{pmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{pmatrix}$ is a representative of our isomorphy class.

We see that Type 3 involutions will exist since $J = \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ -I_{\frac{n}{2}} & 0 \end{pmatrix}$ will induce a Type 3 involution. Thus, these is one isomorphy class of Type 3 involutions. $\square$

We note that in this case, that the maximal number of isomorphy classes do in fact exist. That is, in Corollary 2.4.3, for the case where $k = \overline{k}$, we have equality in every statement.

2.5.2 The Standard Real Orthogonal Group

We now examine the case where β is the standard dot product, and $k = \mathbb{R}$.

Corollary 2.5.2. *If ϑ is an involution of* $\mathrm{SO}(n, \mathbb{R})$*, then ϑ is isomorphic to* Inn_A *where* $A = \begin{pmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{pmatrix}$ *and $0 \leqslant m \leqslant \frac{n}{2}$, or $A = \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix}$. There are no Type 2 or Type 4 involutions for this group.*

Proof. We begin with involutions of Type 1 and proceed in a fashion similar to the previous corollary. So, we can write $A = X \begin{pmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{pmatrix} X^{-1}$, where we know $X^T X$ is diagonal. Based on the conditions of Lemma 2.2.3, we know that $X^T X$ congruent to a diagonal matrix with entries all 1's and -1's. Since we are looking for a representative of our congruence class, let us assume we have equality. But, we see that there can be no -1's in the diagonal since $k = \mathbb{R}$ and $X^T X$ would have to have negative eigenvalues. So, we assume $X^T X = I_n$, which means we can choose $X = I_n$. So, $A = \begin{pmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{pmatrix}$ is a representative of our isomorphy class.

We now assume we have an involution of Type 2, and we will make use of Lemma 2.2.7. We can write $A = -\frac{\sqrt{\alpha}}{\alpha} X \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix} X^{-1}$ where $X^T X = \begin{pmatrix} X_1 & 0 \\ 0 & \frac{1}{\alpha} X_1 \end{pmatrix}$ is diagonal. We recall that $\alpha \in \mathbb{R}^*$ but $\sqrt{\alpha} \notin \mathbb{R}^*$. So, α must be a negative number, and we can choose $\alpha = -1$. That is, $X^T X = \begin{pmatrix} X_1 & 0 \\ 0 & -X_1 \end{pmatrix}$. But, this is a contradiction, because when $k = \mathbb{R}$, there does not exist any nonzero vectors x such that $x^T x \leqslant 0$, so the whole diagonal of $X^T X$ must be positive, which is not possible. This shows that there are no Type 2 involutions in this case. In a similar way, we can show that there are also no Type 4 involutions in this case.

In the Type 3 case, we have $A = X \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix} X^{-1}$ where $X^T X = \begin{pmatrix} X_1 & 0 \\ 0 & X_1 \end{pmatrix}$ is diagonal. Similar to the Type 1 case, we know that $X^T X$ must be congruent to I, so we may assume that X^TX is I, and choose $X = I$ as our representative. Then, we get that $A = \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix}$ is a representative of the only Type 3 isomorphy class. $\square$

Unlike the algebraically closed case, we note that in this case, that the maximal number of isomorphy classes do not exist. That is, in Corollary 2.4.3, for the case where $k = \mathbb{R}$, we have an explicit example where we do not have equality. In fact, given that we have seen that the Type 1 and 3 cases must exist for this group, we actually have the minimal number of isomorphy classes possible.

2.5.3 Orthogonal Groups of $\mathbb{F}_q$

We begin by examining the Type 1 involutions where $k = \mathbb{F}_q$ where $q = p^h$ for all cases where $p \geqslant 5$, and one of the cases where $p = 3$. This is a complete classification of the involutions when n is odd. We note that for these fields we have $|(k^*)^2| = 2$. So, we will use 1 and M_q as representatives of of the distinct square classes. Based on properties of symmetric matrices over $k = \mathbb{F}_q$, we know that up to congruence, there are two possibilities for M: either $M = I_n$ or $M = \begin{pmatrix} I_{n-1} & 0 \\ 0 & M_q \end{pmatrix}$. In the latter case, if $p = 3$, the group may not be friendly. So, the following results may not cover this case.

Corollary 2.5.3. *First, assume that $M = I_n$. Suppose ϑ is a Type 1 involution of $\mathrm{SO}(n, \mathbb{F}_q)$. Then ϑ is isomorphic to Inn_A where we can write $A = I_{n-m,m}$ for $0 \leqslant m \leqslant \frac{n}{2}$ or*

$$A = \begin{pmatrix} -I_{m-1} & 0 & 0 & 0 \\ 0 & 1 - 2\frac{a^2}{M_q} & 0 & \frac{2ab}{M_q} \\ 0 & 0 & I_{n-m-1} & 0 \\ 0 & \frac{2ab}{M_q} & 0 & 1 - 2\frac{b^2}{M_q} \end{pmatrix}$$

for $0 \leqslant m \leqslant \frac{n}{2}$, where M_q is a nontrivial non-square in $\mathbb{F}_q$ where $a^2 + b^2 = M_q$ and $a, b \in \mathbb{F}_q$.

Now, assume that $M = \begin{pmatrix} I_{n-1} & 0 \\ 0 & M_q \end{pmatrix}$. Suppose ϑ is an involution of $\mathrm{SO}(n, \mathbb{F}_q, \beta)$. Then ϑ is isomorphic to Inn_A where we can write

$$A = I_{n-m,m} \quad \textit{or} \quad A = \begin{pmatrix} -I_{n-m-1} & & \\ & I_m & \\ & & -1 \end{pmatrix}$$

for $0 \leqslant m \leqslant \frac{n}{2}$.

Proof. We will use the same methods that we used in the proofs of the previous corollaries. That is, we will use the equivalent conditions of Lemma 2.2.3 to prove that the matrices listed above will be representatives of the isomorphy classes of the involutions of $\mathrm{SO}(n, \mathbb{F}_q)$.

We can write $A = X \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix} X^{-1}$, where $s + t = n$ and we know

$$X^T M X = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}$$

must be diagonal, and X_1 is an $s \times s$ matrix, and X_2 is a $t \times t$ matrix. It is a result from [HWD2004] that any diagonal matrix over $\mathbb{F}_q$ must be congruent to either I or $\begin{pmatrix} I & 0 \\ 0 & M_q \end{pmatrix}$ where M_q is some fixed non-square in $\mathbb{F}_q$. So, we know from the equivalent conditions in Lemma 2.2.3 that X_1 and X_2 must each be congruent to I or $\begin{pmatrix} I & 0 \\ 0 & M_q \end{pmatrix}$ (sizing the matrices appropriately). Let us first assume that $M = I$. Since $\det(X^T X) = (\det(X))^2$ is a square, we observe that X_1 and X_2 must be simultaneously congruent to either I or $\begin{pmatrix} I & 0 \\ 0 & M_q \end{pmatrix}$ (again, sizing appropriately).

Since we are searching for a representative of the congruence class, we can assume that $X^T X$ is either I or $\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & M_q & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & M_q \end{pmatrix}$. In the first case, we can let $X = I$, which means $A = \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix}$.

In the latter case, we here we assume $X^T X = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & M_q & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & M_q \end{pmatrix}$, we can let

$$X = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & a & 0 & b \\ 0 & 0 & I & 0 \\ 0 & -b & 0 & a \end{pmatrix}$$

where we choose a and b so that $a^2 + b^2 = M_q$. It follows from this that

$$A = \begin{pmatrix} -I_{m-1} & 0 & 0 & 0 \\ 0 & 1 - 2\frac{a^2}{M_q} & 0 & \frac{2ab}{M_q} \\ 0 & 0 & I_{n-m-1} & 0 \\ 0 & \frac{2ab}{M_q} & 0 & 1 - 2\frac{b^2}{M_q} \end{pmatrix}.$$

If we now assume that $M = \begin{pmatrix} I_{n-1} & 0 \\ 0 & M_q \end{pmatrix}$, then we have that $X^T M X$ is congruent to $\begin{pmatrix} I_{n-1} & 0 \\ 0 & M_q \end{pmatrix}$ or $\begin{pmatrix} I_{\frac{n}{2}-1} & 0 & 0 \\ 0 & M_q & 0 \\ 0 & 0 & I_{\frac{n}{2}} \end{pmatrix}$. In the first case, since we are looking for a representative of our congruence class, we can assume $X^T \begin{pmatrix} I_{n-1} & 0 \\ 0 & M_q \end{pmatrix} X = \begin{pmatrix} I_{n-1} & 0 \\ 0 & M_q \end{pmatrix}$. This means we can choose $A = \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix}$ as our representative. If instead $X^T M X$ is congruent to $\begin{pmatrix} I_{\frac{n}{2}-1} & 0 & 0 \\ 0 & M_q & 0 \\ 0 & 0 & I_{\frac{n}{2}} \end{pmatrix}$, then we can choose $X = \begin{pmatrix} I_{s-1} & & & \\ & 0 & & 1 \\ & & I_{t-1} & \\ & 1 & & 0 \end{pmatrix}$. This gives representative $A = \begin{pmatrix} -I_{s-1} & & \\ & I_t & \\ & & -1 \end{pmatrix}$.

□

We note that in these cases, we have that if n is odd, then $C_1(n, \mathbb{F}_q, \beta) = 2n - 2$, and if n is even, then $C_1(n, \mathbb{F}_q, \beta) = 2n - 1$. That is, for $k = \mathbb{F}_q$, we always have the maximal number of Type 1 involutions. If n is even, does this occur for the other types of involutions? We now restrict our attention to the case where n is even and β is the standard dot product. We have seen that we can have at most one class of Type 3 involutions, and we note that in fact $C_3(n, \mathbb{F}_q) = 1$ since the orthogonal matrix $A = \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ -I_{\frac{n}{2}} & 0 \end{pmatrix}$ will always induce a Type 3 involution.

Lastly, we need only consider Type 2 and Type 4 involutions. We know that $C_2(n, \mathbb{F}_q) \leqslant 3$ and $C_4(n, \mathbb{F}_q) \leqslant 1$. We will specifically look at the cases where q =3, 5, and 7. For these cases, we see that we have existence of both Type 2 and Type 4 involutions via the matrices in Table 2.4.

We note that these examples will all generalize to higher dimensions, so it is clear that for

Table 2.4: Type 2 and Type 4 examples for $\mathrm{SO}(4, \mathbb{F}_p)$

k	Type 2	Type 4
$\mathbb{F}_3$	$i\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$	$i\begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 \end{pmatrix}$
$\mathbb{F}_5$	$\sqrt{2}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 4 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 4 \end{pmatrix}$	$\sqrt{2}\begin{pmatrix} 1 & 4 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 1 & 1 \end{pmatrix}$
$\mathbb{F}_7$	$\sqrt{3}\begin{pmatrix} 1 & 3 & 0 & 0 \\ 3 & 6 & 0 & 0 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 3 & 6 \end{pmatrix}$	$\sqrt{3}\begin{pmatrix} 1 & 4 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 3 & 1 \end{pmatrix}$

these fields, whenever n is even we have $C_2(n, \mathbb{F}_q), C_4(n, \mathbb{F}_q) \geqslant 1$. So, for these three specific fields, we know that $C_4(n, \mathbb{F}_q) = 1$, and that the number of isomorphy classes of Type 4 involutions are maximized as well. But, for $\mathrm{SO}(4, \mathbb{F}_p)$ where $p = 3$, 5, and 7, we have done computations in Maple which use the conditions of Theorem 2.2.7 that show that for these fields, $C_2(4, \mathbb{F}_p) = 1$. So, the number of Type 2 isomorphy classes is not maximized in these cases, despite the other three types being maximized. While we have been unable to prove this up to this point, we believe that this is a pattern that would continue. That is, we have the following conjecture:

Conjecture 2.5.4. *Suppose that* $\mathrm{SO}(n, k)$ *is a finite friendly orthogonal group and that* n *is even. Then,* $C_2(n, k) = C_4(n, k) = \tau_1(k)$.

2.5.4 p-adic examples

We now turn our attention to the case where $k = \mathbb{Q}_p$. We will assume $M = I_n$. We show a classification of the isomorphy classes of the Type 1 involutions of $\mathrm{SO}(n, \mathbb{Q}_p)$ where $p > 2$, using Lemma 2.2.3. Note that if n is odd, then this is a complete classification of the isomorphy classes of all the involutions of $\mathrm{SO}(n, \mathbb{Q}_p)$.

Recall that the classification of involutions breaks down to analyzing the diagonal matrix $X^TX = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}$, specifically by looking at the congruency classes of X_1 and X_2. The final condition of Lemma 2.2.3 gave us conditions on the square class of the determinant and the Hasse symbol to classify the isomorphy classes for $\mathrm{SO}(n, \mathbb{Q}_p)$. Using these conditions, we have classified all of the possible isomorphy classes of Type 1 involutions based on what the values of X_1 and X_2 would be for a representative of the congruency class in Tables 2.5 and 2.6. To show that each of these possible congruency classes exists, one would need to find a matrix X such that $X^T X = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}$. This would then determine A. In the case where $-1 \notin (\mathbb{Q}_p^*)^2$, this will always be the case. To see that this is true, note that $X^T X = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}$ will always be a symmetric matrix with a determinant that is in the same square class as 1. When $-1 \notin (\mathbb{Q}_p^*)^2$, all such matrices are such that $c_p \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix} = 1$ is the case. So, $\begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}$ will be congruent to I_n, which gives us the existence of X such that $X^T X = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}$. In the case where $-1 \in (\mathbb{Q}_p^*)^2$, then it is possible that $c_p \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix} = -1$. For these cases, it is not clear (to the author) that there exists X such that $X^T X = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}$.

Table 2.5: X_1 and X_2 values when $k = \mathbb{Q}_p$, $p > 2$, and $-1 \in (\mathbb{Q}_p^*)^2$

X_1	X_2	$\det(X_1)$ and $\det(X_2)$	$c_p(X_1)$	$c_p(X_2)$
I_n	I_n	1	1	1
I_n	$\begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & N_p & 0 \\ 0 & 0 & 0 & pN_p \end{pmatrix}$	1	1	-1
$\begin{pmatrix} I_{n-1} & 0 \\ 0 & p \end{pmatrix}$	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & p \end{pmatrix}$	p	1	1
$\begin{pmatrix} I_{n-1} & 0 \\ 0 & p \end{pmatrix}$	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & N_p & 0 \\ 0 & 0 & pN_p \end{pmatrix}$	p	1	-1
$\begin{pmatrix} I_{n-1} & 0 \\ 0 & N_p \end{pmatrix}$	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & N_p \end{pmatrix}$	N_p	1	1
$\begin{pmatrix} I_{n-1} & 0 \\ 0 & N_p \end{pmatrix}$	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & pN_p \end{pmatrix}$	N_p	1	-1
$\begin{pmatrix} I_{n-1} & 0 \\ 0 & pN_p \end{pmatrix}$	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & pN_p \end{pmatrix}$	pN_p	1	1
$\begin{pmatrix} I_{n-1} & 0 \\ 0 & pN_p \end{pmatrix}$	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & N_p \end{pmatrix}$	pN_p	1	-1
$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & N_p \end{pmatrix}$	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & N_p \end{pmatrix}$	pN_p	-1	-1
$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & pN_p \end{pmatrix}$	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & pN_p \end{pmatrix}$	N_p	-1	-1
$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & N_p & 0 \\ 0 & 0 & pN_p \end{pmatrix}$	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & N_p & 0 \\ 0 & 0 & pN_p \end{pmatrix}$	p	-1	-1
$\begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & N_p & 0 \\ 0 & 0 & 0 & pN_p \end{pmatrix}$	$\begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & N_p & 0 \\ 0 & 0 & 0 & pN_p \end{pmatrix}$	1	-1	-1

Table 2.6: X_1 and X_2 values when $k = \mathbb{Q}_p$, $p > 2$ and $-1 \notin (\mathbb{Q}_p^*)^2$

X_1	X_2	$\det(X_1)$ and $\det(X_2)$	$c_p(X_1)$	$c_p(X_2)$
I_n	I_n	1	1	1
$\begin{pmatrix} I_{n-1} & 0 \\ 0 & p \end{pmatrix}$	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & p \end{pmatrix}$	p	-1	-1
$\begin{pmatrix} I_{n-1} & 0 \\ 0 & p \end{pmatrix}$	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & N_p & 0 \\ 0 & 0 & pN_p \end{pmatrix}$	p	- 1	1
$\begin{pmatrix} I_{n-1} & 0 \\ 0 & N_p \end{pmatrix}$	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & N_p \end{pmatrix}$	N_p	1	1
$\begin{pmatrix} I_{n-1} & 0 \\ 0 & pN_p \end{pmatrix}$	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & pN_p \end{pmatrix}$	pN_p	-1	-1
$\begin{pmatrix} I_{n-1} & 0 \\ 0 & pN_p \end{pmatrix}$	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & N_p \end{pmatrix}$	pN_p	-1	1
$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & N_p \end{pmatrix}$	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & N_p \end{pmatrix}$	pN_p	1	1
$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & N_p & 0 \\ 0 & 0 & pN_p \end{pmatrix}$	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & N_p & 0 \\ 0 & 0 & pN_p \end{pmatrix}$	p	1	1

We now assume that $p = 2$, and we construct a classification of the Type 1 involutions. We again note that if n is odd, then this is a complete classification. We see that ± 1, ± 2, ± 3 and ± 6 are representatives for all of the the distinct square classes of $(\mathbb{Q}_2^*)^2$. For this case, we have not constructed tables with complete classifications of the two sets of isomorphy classes. Instead, we have constructed a table, Table 2.7, where we have a diagonal matrix over $\mathbb{Q}_2$ for each possible pair of determinant square class and value of Hasse symbol. A potential isomorphy class is determined by choosing for X_1 and X_2 any pair of matrices on this table where the two given matrices have determinants in the same square class. So, given the different possible Hasse symbol values, there are at most 24 isomorphy classes of Type 1 involutions. As in some of the previous cases, it is not immediately clear that there does or does not exist a matrix X in each of these cases such that $X^T X = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}$.

Table 2.7: X_1 and X_2 values when $k = \mathbb{Q}_2$

$\det(Y)$ square class	$c_f(Y) = 1$	$c_p(Y) = -1$
1	I_n	$\begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & -6 \end{pmatrix}$
-1	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & -1 \end{pmatrix}$
2	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & 2 \end{pmatrix}$
-2	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & -2 \end{pmatrix}$	$\begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & -6 \end{pmatrix}$
3	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & 3 \end{pmatrix}$	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$
-3	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -3 \end{pmatrix}$	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & -3 \end{pmatrix}$
6	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & 6 \end{pmatrix}$	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$
-6	$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 6 \end{pmatrix}$	$\begin{pmatrix} I_{n-1} & 0 \\ 0 & -6 \end{pmatrix}$

Chapter 3

Isomorphy Classes of Involutions of $\mathrm{SP}(2n, k)$

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

It follows from a proposition on page 191 of [Bor91] that $\mathrm{Aut}(\mathrm{SP}(2n, \overline{k}))/\operatorname{Inn}(\mathrm{SP}(2n, \overline{k})))$ must be a subgroup of the diagram automorphisms of the Dynkin diagram C_n. Since C_n only has the trivial diagram autormphism, then we have that $\mathrm{Aut}(\mathrm{SP}(2n, \overline{k})) = \mathrm{Inn}(\mathrm{SP}(2n, \overline{k}))$. When k is not algebraically closed, then all automorphisms of $\mathrm{SP}(2n, k)$ will still be of the form Inn_A for some $A \in \mathrm{SP}(n, \overline{k})$ since all automorphisms of $\mathrm{SP}(2n, k)$ must also be an automorphism of $\mathrm{SP}(n, \overline{k})$. Thus, the classifications and characterizations that follow in this paper consider all automorphisms and involutions of $\mathrm{SP}(2n, k)$.

We now examine which automorphisms will act as the identity on $\mathrm{SP}(2n, k)$. This will prove to be useful when we classify matrix representatives for automorphisms. The following two results are from [Jac2005], the dissertation of Farrah Jackson.

Theorem 3.1.1. *Let $G = \mathrm{SP}(2n, k)$. If $\mathrm{Inn}_A|_G = \mathrm{id}$ for some $A \in \mathrm{GL}(2n, \overline{k})$, then $A = pI$ for some $p \in \overline{k}$.*

From this, Jackson proved the following result that characterizes automorphisms of $\mathrm{SP}(2n, k)$. We will see that for Inn_A to be an involution of $\mathrm{SP}(2n, k)$, that we can not only assume that A is symplectic, but that the entries of A must lie in k, or an algebraic extension of k.

Theorem 3.1.2. *(i) Suppose $A \in \mathrm{GL}(2n, \bar{k})$. The automorphism Inn_A keeps $\mathrm{SP}(2n, \bar{k})$ invariant if and only if $A = pM$ for some $p \in \bar{k}$ and $M \in \mathrm{SP}(2n, \bar{k})$.*

(ii) If $A \in \mathrm{SP}(2n, \bar{k})$, then Inn_A keeps $\mathrm{SP}(2n, k)$ invariant if and only if we can show $A \in \mathrm{SP}(2n, k[\sqrt{\alpha}])$ where each entry of A is a $k-$multiple of $\sqrt{\alpha}$, for some $\alpha \in k$.

3.2 Involutions of $\mathrm{SP}(2n, k)$

We now begin to focus on involutions and the classification of their isomorphy classes. We will distinguish different types of involutions. First, we note that for some involutions, φ, there exists $A \in \mathrm{SP}(2n, k)$ such that $\varphi = \mathrm{Inn}_A$, but not in all cases. Sometimes we must settle for $A \in \mathrm{SP}(2n, k[\sqrt{\alpha}]) \setminus \mathrm{SP}(2n, k)$.

This is not the only way in which we can distinguish between different types of involutions. If Inn_A is an involution, then $\mathrm{Inn}_{A^2} = (\mathrm{Inn}_A)^2$ is the identity map. We know from above that this means that $A^2 = \gamma I$ for some $\gamma \in \overline{k}$. But, we know that A is symplectic. So, A^2 is also symplectic. That means that $(A^2)^T J (A^2) = J$, which implies $(\gamma I)^T J (\gamma I) = J$, which means $\gamma^2 = 1$. So, $\gamma = \pm 1$. Thus, we can also distinguish between different types of involutions by seeing if $A^2 = I$ or $A^2 = -I$. This gives the four types of involutions, which are outlined in Table 3.1.

Table 3.1: The various possible types of involutions of $\mathrm{SP}(2n, k)$

	$A \in \mathrm{SP}(2n, k)$	$A \in \mathrm{SP}(2n, k[\sqrt{\alpha}]) \setminus \mathrm{SP}(n, k)$
$A^2 = I$	Type 1	Type 2
$A^2 = -I$	Type 3	Type 4

3.2.1 Type 1 Involutions

We first characterize the matrices that induce Type 1 involutions in the following lemma.

Lemma 3.2.1. *Suppose ϑ is a Type 1 involution of* $\mathrm{SP}(2n, k)$*. Then,*

$$A = X \begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix} X^{-1}$$

where $s + t = 2n$ and $X^T J X = J$. That is, $X \in \mathrm{SP}(2n, k)$.

Proof. Since $\mathrm{Inn}_A^2 = I$ and $A \in \mathrm{SP}(2n, k)$, then it follows that $A^2 = I$. So, all eigenvalues of A are ± 1. Since there are no repeated roots in the minimal polynomial of A, then we see that A is diagonalizable. Let $s = \dim(E(A, 1))$ and $t = \dim(E(A, -1))$, and observe that $s + t = 2n$ since A is diagonalizable. We will first show that both s and t must be even. To do this, we proceed by contradiction and assume that s and t are both odd. So, there exists some $Y \in \mathrm{GL}(n, \overline{k})$ such that $Y^{-1}AY = \begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix}$. Since A is symplectic, then it follows that

$$\begin{aligned} J = A^T J A &= \left(Y \begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix} Y^{-1} \right)^T JY \begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix} Y^{-1} \\ &= (Y^{-1})^T \begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix} Y^T JY \begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix} Y^{-1}. \end{aligned}$$

This implies that

$$\begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix} Y^T JY = (Y^T JY) \begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix},$$

where $Y^T JY$ is an invertible skew-symmetric matrix. So, $Y^T JY = \begin{pmatrix} Y_1 & 0 \\ 0 & Y_2 \end{pmatrix}$ for some invertible skew symmetric matrices Y_1 and Y_2, which are $s \times s$ and $t \times t$, respectively. But odd dimensional skew symmetric matrices cannot be invertible, so this is a contradiction. Thus, s and t must be even.

We now wish to construct bases for $E(A, 1)$ and $E(A, -1)$ such that all the vectors lie in k^n. Let $\{z_1, ..., z_n\}$ be a basis for k^n. For each i, let $u_i = (A + I)z_i$. Note that

$$Au_i = A(A + I)z_i = (A + I)z_i = u_i.$$

So, $\{u_1, ..., u_n\}$ must span $E(A, 1)$. Thus, we can appropriately choose s of these vectors and form a basis for $E(A, 1)$. Label these basis vectors as $y_1, ..., y_{\frac{s}{2}}, y_{n+1}, ..., y_{n+\frac{s}{2}}$. We can similarly form a basis for $E(A, -1)$. We shall call these vectors $y_{\frac{s}{2}+1}, ..., y_n, y_{n+\frac{s}{2}+1}, ..., y_{2n}$. Let Y be the matrix with the vectors $y_1, ..., y_{2n}$ as its columns. Then, by construction,

$$Y^{-1}AY = \begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix}.$$

We can rearrange to get

$$A = Y \begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix} Y^{-1}.$$

Recall that $A^T = JAJ^{-1}$, since $A \in \mathrm{SP}(2n, k)$. So,

$$\left(Y \begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix} Y^{-1} \right)^T = J \left(Y \begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix} Y^{-1} \right) J^{-1}.$$

This implies

$$(Y^{-1})^T \begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix} Y^T = JY \begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix} (JY)^{-1},$$

which means

$$\begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix} Y^T JY = Y^T JY \begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix}.$$

So, $Y^T JY = \begin{pmatrix} Y_1 & 0 & Y_2 & 0 \\ 0 & Y_3 & 0 & Y_4 \\ -Y_2^T & 0 & Y_5 & 0 \\ 0 & -Y_4^T & 0 & Y_6 \end{pmatrix}$, where Y_1 and Y_5 are $\frac{s}{2} \times \frac{s}{2}$ skew-symmetric matrices, Y_3 and Y_6 are $\frac{t}{2} \times \frac{t}{2}$ skew-symmetric matrices, Y_2 is a $\frac{s}{2} \times \frac{s}{2}$ matrix and Y_4 is a $\frac{t}{2} \times \frac{t}{2}$ matrix.

We can choose a permutation matrix $Q \in \mathrm{O}(2n, k)$ such that

$$A = YQ \begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix} Q^{-1} Y^{-1}$$

and

$$Y^TJY = Q\begin{pmatrix} Y_1 & Y_2 & 0 & 0 \\ -Y_2^T & Y_5 & 0 & 0 \\ 0 & 0 & Y_3 & Y_4 \\ 0 & 0 & -Y_4^T & Y_6 \end{pmatrix}Q^{-1}.$$

Let $Y_7 = \begin{pmatrix} Y_1 & Y_2 \\ -Y_2^T & Y_5 \end{pmatrix}$ and $Y_8 = \begin{pmatrix} Y_3 & Y_4 \\ -Y_4^T & Y_6 \end{pmatrix}$. Note that both Y_7 and Y_8 are skew-symmetric. We can rearrange the above statement to be

$$Q^TY^TJYQ = \begin{pmatrix} Y_7 & 0 \\ 0 & Y_8 \end{pmatrix}.$$

It follows that there exists $N = \begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix} \in \mathrm{GL}(n,k)$ such that

$$N^TQ^TY^TJYQN = \begin{pmatrix} 0 & I_{\frac{s}{2}} & 0 & 0 \\ -I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{\frac{t}{2}} \\ 0 & 0 & -I_{\frac{t}{2}} & 0 \end{pmatrix}.$$

We see that we can again use the permutation matrix Q to get

$$QN^TQ^TY^TJYQNQ^T = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} = J.$$

Let $X = YQNQ^T$. Then,

$$X\begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix}X^{-1} = YQNQ^T\begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix}(YQNQ^T)^{-1}$$

$$= YQ\begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix}\begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix}\begin{pmatrix} N_1^{-1} & 0 \\ 0 & N_2^{-1} \end{pmatrix}Q^{-1}Y^{-1}$$

$$= YQ\begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix}Q^{-1}Y^{-1}$$

$$= Y \begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix} Y^{-1} = A,$$

where $X^T J X = J$. From this last observation, it follows that $X \in \mathrm{SP}(2n, k)$. □

Using this characterization, we now find conditions on these involutions that are equivalent to isomorphy.

Theorem 3.2.2. *Suppose* Inn_A *and* Inn_B *both induce Type 1 involutions for* $\mathrm{SP}(2n, k)$ *for* A *and* $B \in \mathrm{SP}(2n, k)$*. Then,* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{SP}(2n, k)$ *if and only if the dimension of* $E(A, 1)$ *equals the dimension of* $E(B, 1)$ *or* $E(B, -1)$*.*

Proof. We first prove that Inn_A is isomorphic to Inn_B over $\mathrm{SP}(2n, k)$ is equivalent to A being conjugate to B or $-B$ over $\mathrm{SP}(2n, k)$. Suppose A is conjugate to B over $\mathrm{SP}(2n, k)$. Choose $Q \in \mathrm{SP}(2n, k)$ such that $B = Q^{-1}AQ$. Then, for all $U \in \mathrm{SP}(2n, k)$, we have

$$\begin{aligned} Q^{-1}A^{-1}QUQ^{-1}AQ &= (Q^{-1}AQ)^{-1}U(Q^{-1}AQ) \\ &= B^{-1}UB. \end{aligned}$$

So, $(\mathrm{Inn}_Q)^{-1}\,\mathrm{Inn}_A\,\mathrm{Inn}_Q = \mathrm{Inn}_B$. That is, Inn_A is isomorphic to Inn_B over $\mathrm{SP}(2n, k)$. Likewise, if A is conjugate to $-B$, then we can show Inn_A is isomorphic to Inn_B over $\mathrm{SP}(2n, k)$. This argument is easily reversible.

From this, it is clear that if Inn_A and Inn_B are isomorphic over $\mathrm{SP}(2n, k)$, then the dimension of $E(A, 1)$ equals the dimension of $E(B, 1)$ or $E(B, -1)$. We need only show the converse.

First, suppose that the dimension of $E(A, 1)$ equals the dimension of $E(B, 1)$. By the previous lemma, we can choose $X, Y \in \mathrm{SP}(2n, k)$ such that

$$X^{-1}AX = \begin{pmatrix} I_{\frac{s}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{t}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{s}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{t}{2}} \end{pmatrix} = Y^{-1}BY.$$

Let $Q = XY^{-1}$. Note that $Q \in \mathrm{SP}(2n, k)$. Then, we have $Q^{-1}AQ = B$, and we have already shown that this implies Inn_A is isomorphic to Inn_B over $\mathrm{SP}(2n, k)$.

If the dimension of $E(A, 1)$ equals the dimension of $E(B, -1)$, then we can similarly show that there exists $Q \in \mathrm{SP}(2n, k)$ such that $Q^{-1}AQ = -B$, which also implies Inn_A is isomorphic to Inn_B over $\mathrm{SP}(2n, k)$.

$\square$

From this theorem, the number of isomorphy classes of Type 1 involutions is clear. We note that this number is independent of the field k.

Corollary 3.2.3. $\mathrm{SP}(2n, k)$ *has* $\frac{n}{2}$ *or* $\frac{n-1}{2}$ *isomorphy classes of Type 1 involutions. (Whichever is an integer.)*

3.2.2 Type 2 Involutions

We have a similar characterization of the matrices and isomorphy classes in the Type 2 case. We first prove a result that characterizes the eigenvectors in the Type 2 case.

Lemma 3.2.4. *Suppose* $A \in \mathrm{SP}(2n, k[\sqrt{\alpha}], \beta) \setminus \mathrm{SP}(2n, k, \beta)$ *induces a Type-2 involution of* $\mathrm{SP}(n, k, \beta)$ *where* $\sqrt{\alpha} \notin k$*. Also suppose* $x, y \in k^{2n}$ *such that* $x + \sqrt{\alpha}y \in E(A, -1)$*. Then,* $x - \sqrt{\alpha}y \in E(A, 1)$*. Likewise, if* $u, v \in k^{2n}$ *such that* $u + \sqrt{\alpha}v \in E(A, 1)$*. Then,* $u - \sqrt{\alpha}v \in E(A, -1)$*. Further,* $\dim(E(A, 1)) = \dim(E(A, -1))$*.*

Proof. First, we observe that "$\sqrt{\alpha}-$conjugation," similar to the familiar complex conjugation ($i-$conjugation), preserves multiplication. That is,

$$(a + \sqrt{\alpha}b)(c + \sqrt{\alpha}d) = (ac + \alpha bd) + \sqrt{\alpha}(ad + bc)$$

and

$$(a - \sqrt{\alpha}b)(c - \sqrt{\alpha}d) = (ac + \alpha bd) - \sqrt{\alpha}(ad + bc).$$

So, "$\sqrt{\alpha}-$conjugation" will preserve multiplication on the matrix level as well. Because of this and since

$$A(x + \sqrt{\alpha}y) = -x - \sqrt{\alpha}y,$$

then it follows that

$$(-A)(x - \sqrt{\alpha}) = -x + \sqrt{\alpha}y.$$

We can multiply both sides to see that

$$A(x - \sqrt{\alpha}) = x - \sqrt{\alpha}y.$$

That is, $x - \sqrt{\alpha}y \in E(A, 1)$. This proves the first statement. An analogous argument proves the second.

To see that $\dim(E(A, 1)) = \dim(E(A, -1))$ is the case, note that the first statement tells us that $\dim(E(A, 1)) \leqslant \dim(E(A, -1))$, and that the second statement tells us that $\dim(E(A, 1)) \geqslant \dim(E(A, -1))$, since "$\sqrt{\alpha}-$conjugation" is an invertible operator on $k[\sqrt{\alpha}]^n$. $\square$

We are now able to characterize the Type 2 involutions. Note that this result combined with our results from the Type 1 case shows that if n is odd, then $\mathrm{SP}(2n,k)$ will not have any Type 2 involutions.

Lemma 3.2.5. *Suppose ϑ is a Type 2 involution of* $\mathrm{SP}(2n,k)$*. Let A be the symplectic matrix in* $\mathrm{SP}(2n,k[\sqrt{\alpha}])$ *such that $\vartheta = \mathrm{Inn}_A$. Then,*

$$A = \frac{\sqrt{\alpha}}{\alpha} X \begin{pmatrix} 0 & I_n \\ \alpha I_n & 0 \end{pmatrix} X^{-1}$$

where

$$X = \begin{pmatrix} x_1 & x_2 & \cdots & x_n & y_1 & y_2 & \cdots & y_n \end{pmatrix} \in \mathrm{GL}(2n,k),$$

where for each i, we have that $x_i + \sqrt{\alpha} y_i \in E(A,1)$ and $x_i - \sqrt{\alpha} y_i \in E(A,-1)$. Further,

$$X^T J X = \frac{1}{2} \begin{pmatrix} J & 0 \\ 0 & \frac{1}{\alpha} J \end{pmatrix}.$$

Proof. We wish to construct bases for $E(A,1)$ and $E(A,-1)$ such that all the vectors lie in $k[\sqrt{\alpha}]^{2n}$. From the previous lemma, we know that $\dim(E(A,1)) = \dim(E(A,-1)) = n$. Since Inn_A is a Type 1 involution of $\mathrm{SP}(2n,k[\alpha])$, then we can apply Lemma 3.2.1 to find a basis $\{x_1+\sqrt{\alpha}y_1, ..., x_n+\sqrt{\alpha}y_n\}$ of $E(A,1)$, where $x_1, ..., x_n, y_1, ..., y_n \in k^{2n}$. By the previous lemma, we know that$\{x_1-\sqrt{\alpha}y_1, ..., x_{\frac{n}{2}}-\sqrt{\alpha}y_{\frac{n}{2}}\}$ must be a basis for $E(A,1)$. Further, based on Lemma 3.2.1, we can assume that these vectors are chosen so that if

$$Y = (x_1+\sqrt{\alpha}y_1, ..., x_{\frac{n}{2}}+\sqrt{\alpha}y_{\frac{n}{2}}, x_1-\sqrt{\alpha}y_1, ..., x_{\frac{n}{2}}-\sqrt{\alpha}y_{\frac{n}{2}}, x_{\frac{n}{2}+1}+\sqrt{\alpha}y_{\frac{n}{2}+1}, ...$$

$$..., x_n+\sqrt{\alpha}y_n, x_{\frac{n}{2}+1}-\sqrt{\alpha}y_{\frac{n}{2}+1}, ..., x_n-\sqrt{\alpha}y_n),$$

then we know that

$$A = Y \begin{pmatrix} I_{\frac{n}{2}} & 0 & 0 & 0 \\ 0 & -I_{\frac{n}{2}} & 0 & 0 \\ 0 & 0 & I_{\frac{n}{2}} & 0 \\ 0 & 0 & 0 & -I_{\frac{n}{2}} \end{pmatrix} Y^{-1}$$

where $Y^T J Y = J$.

Let $X = \begin{pmatrix} x_1 & x_2 & \cdots & x_{\frac{n}{2}} & y_1 & y_2 & \cdots & y_{\frac{n}{2}} \end{pmatrix} \in \mathrm{GL}(n,k)$.

We now make a couple of observations. Suppose $u = x + \sqrt{\alpha} y$ is a 1-eigenvector of A such that $x, y \in k^n$. Then, we know $v = x - \sqrt{\alpha} y$ is a -1-eigenvector of A. Observe that

$$Ax = \frac{1}{2}A(u+v) = \frac{1}{2}(u-v) = \sqrt{\alpha}y.$$

It follows from this that

$$Ay = \frac{\sqrt{\alpha}}{\alpha}x.$$

Since $Ax = \sqrt{\alpha}y$ and $Ay = \frac{\sqrt{\alpha}}{\alpha}x$, then it follows that

$$X^{-1}AX = \begin{pmatrix} 0 & \frac{\sqrt{\alpha}}{\alpha} I_{\frac{n}{2}} \\ \sqrt{\alpha} I_{\frac{n}{2}} & 0 \end{pmatrix}.$$

Rearranging this, we see that

$$A = \frac{\sqrt{\alpha}}{\alpha} X \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix} X^{-1}.$$

Now, we need only prove the last statement to prove the Lemma. Since $Y^T J Y = J$, then we know that if $1 \leqslant i \leqslant \frac{n}{2}$ and $j \neq \frac{n}{2} + i$, then

$$0 = \beta(x_i + \sqrt{\alpha}y_i, x_j + \sqrt{\alpha}y_j) = (\beta(x_i, x_j) + \alpha\beta(y_i, y_j)) + \sqrt{\alpha}(\beta(x_i, y_j) + \beta(x_j, y_i))$$

and that

$$0 = \beta(x_i + \sqrt{\alpha}y_i, x_j - \sqrt{\alpha}y_j) = (\beta(x_i, x_j) - \alpha\beta(y_i, y_j)) + \sqrt{\alpha}(-\beta(x_i, y_j) + \beta(x_j, y_i)).$$

So, we have that $\beta(x_i, x_j) + \alpha\beta(y_i, y_j) = 0$, $\beta(x_i, y_j) + \beta(x_j, y_i) = 0$, $\beta(x_i, x_j) - \alpha\beta(y_i, y_j) = 0$, and $-\beta(x_i, y_j) + \beta(x_j, y_i) = 0$. It follows from this that when $1 \leqslant i \leqslant \frac{n}{2}$ and $j \neq \frac{n}{2} + i$, we have

$$\beta(x_i, x_j) = \beta(y_i, y_j) = \beta(x_i, y_j) = \beta(y_i, x_j) = 0.$$

Now suppose that $1 \leqslant i \leqslant \frac{n}{2}$ and $j = \frac{n}{2} + i$. Then, we have

$$1 = \beta(x_i + \sqrt{\alpha}y_i, x_j + \sqrt{\alpha}y_j) = (\beta(x_i, x_j) + \alpha\beta(y_i, y_j)) + \sqrt{\alpha}(\beta(x_i, y_j) + \beta(x_j, y_i))$$

and that

$$0 = \beta(x_i + \sqrt{\alpha}y_i, x_j - \sqrt{\alpha}y_j) = (\beta(x_i, x_j) - \alpha\beta(y_i, y_j)) + \sqrt{\alpha}(-\beta(x_i, y_j) + \beta(x_j, y_i)).$$

Similar to the first case, we have that $\beta(x_i, y_j) = 0 = \beta(y_i, x_j) = 0$, and we have

$$1 = \beta(x_i, x_j) + \alpha\beta(y_i, y_j)$$

and

$$0 = \beta(x_i, x_j) - \alpha\beta(y_i, y_j).$$

Thus, when $1 \leqslant i \leqslant \frac{n}{2}$ and $j = \frac{n}{2} + i$, we have that $\beta(x_i, x_j) = \frac{1}{2}$ and $\beta(y_i, y_j) = \frac{1}{2\alpha}$. So, we have that $X^T JX = \frac{1}{2}\begin{pmatrix} J & 0 \\ 0 & \frac{1}{\alpha}J \end{pmatrix}$.

□

We now consider a couple of examples of Type 2 involutions.

Example 3.2.6. *Consider the matrix*

$$A = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

Inn_A *is a Type 2 involution of* $\mathrm{SP}(4, \mathbb{Q})$ *since* $A^2 = I$ *and each entry of* A *is a* $\mathbb{Q}$*-multiple of* $\sqrt{2}$*. A basis for* $E(A, 1)$ *that matches the conditions of Lemma 3.2.5 is formed by the vectors*

$$v_1 = \begin{pmatrix} 0 \\ 0 \\ -\frac{1}{8} \\ -\frac{1}{8} \end{pmatrix} + \sqrt{2}\begin{pmatrix} 0 \\ 0 \\ -\frac{1}{8} \\ 0 \end{pmatrix}$$

and

$$v_2 = \begin{pmatrix} 0 \\ 4 \\ 1 \\ 1 \end{pmatrix} + \sqrt{2}\begin{pmatrix} 2 \\ -2 \\ 1 \\ 0 \end{pmatrix}.$$

It can be shown that

$$v_3 = \begin{pmatrix} 0 \\ 0 \\ -\frac{1}{8} \\ -\frac{1}{8} \end{pmatrix} - \sqrt{2} \begin{pmatrix} 0 \\ 0 \\ -\frac{1}{8} \\ 0 \end{pmatrix}$$

and

$$v_4 = \begin{pmatrix} 0 \\ 4 \\ 1 \\ 1 \end{pmatrix} - \sqrt{2} \begin{pmatrix} 2 \\ -2 \\ 1 \\ 0 \end{pmatrix}$$

are basis vectors for $E(A, -1)$ that also match the conditions of Lemma 3.2.5.

Following the notation of the previous lemma, we have

$$X = \begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 4 & 0 & -2 \\ -\frac{1}{8} & 1 & -\frac{1}{8} & 1 \\ -\frac{1}{8} & 1 & 0 & 0 \end{pmatrix},$$

where $X^T JX = \begin{pmatrix} 0 & \frac{1}{2} & 0 & 0 \\ -\frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{4} \\ 0 & 0 & -\frac{1}{4} & 0 \end{pmatrix}$ *and* $A = \frac{\sqrt{2}}{2} X \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ 2I_{\frac{n}{2}} & 0 \end{pmatrix} X^{-1}$.

Example 3.2.7. *Let k be any field that does not contain $i = \sqrt{-1}$. For example, k could be $\mathbb{R}$, or $\mathbb{F}_p$ or $\mathbb{Q}_p$ where p is congruent to $3 \mod 4$. Consider the matrix*

$$A = i \begin{pmatrix} 1 & 1 & 0 & 0 \\ -2 & -1 & 0 & 0 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

Inn_A *is a Type 2 involution of $\mathrm{SP}(4, k)$ since $A^2 = I$ and each entry of A is a k-multiple of i. A basis for $E(A, 1)$ that matches the conditions of Lemma 3.2.5 is formed by the vectors*

$$v_1 = \begin{pmatrix} -\frac{1}{2} \\ 1 \\ 1 \\ 1 \end{pmatrix} + i \begin{pmatrix} \frac{1}{2} \\ 0 \\ -1 \\ 0 \end{pmatrix}$$

and

$$v_2 = \begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ 1 \\ 1 \end{pmatrix} + i \begin{pmatrix} 0 \\ \frac{1}{2} \\ -1 \\ 0 \end{pmatrix}$$

It can be shown that

$$v_3 = \begin{pmatrix} -\frac{1}{2} \\ 1 \\ 1 \\ 1 \end{pmatrix} - i \begin{pmatrix} \frac{1}{2} \\ 0 \\ -1 \\ 0 \end{pmatrix}$$

and

$$v_4 = \begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ 1 \\ 1 \end{pmatrix} - i \begin{pmatrix} 0 \\ \frac{1}{2} \\ -1 \\ 0 \end{pmatrix}$$

are basis vectors for $E(A, -1)$ that also match the conditions of Lemma 3.2.5.

Following the notation of the previous lemma, we have

$$X = \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ 1 & \frac{1}{2} & 0 & \frac{1}{2} \\ 1 & 1 & -1 & -1 \\ 1 & 1 & 0 & 0 \end{pmatrix},$$

where $X^T JX = \begin{pmatrix} 0 & \frac{1}{2} & 0 & 0 \\ -\frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & \frac{1}{2} & 0 \end{pmatrix}$ *and* $A = -iXJX^{-1}$.

Using our characterization of Type 2 involutions, we now find conditions on Type 2 involutions that are equivalent to isomorphy.

Theorem 3.2.8. *Suppose A and B both induce Type 2 involutions of* $\mathrm{SP}(2n, k)$ *where we write*

$$A = \frac{\sqrt{\alpha}}{\alpha} X \begin{pmatrix} 0 & I_n \\ \alpha I_n & 0 \end{pmatrix} X^{-1}$$

and

$$B = \frac{\sqrt{\beta}}{\beta} Y \begin{pmatrix} 0 & I_n \\ \beta I_n & 0 \end{pmatrix} Y^{-1}$$

where

$$X = \begin{pmatrix} x_1 & x_2 & \cdots & x_n & y_1 & y_2 & \cdots & y_n \end{pmatrix} \in \mathrm{GL}(2n,k)$$

and

$$Y = \begin{pmatrix} \tilde{x_1} & \tilde{x_2} & \cdots & \tilde{x}_n & \tilde{y}_1 & \tilde{y}_2 & \cdots & \tilde{y}_n \end{pmatrix} \in \mathrm{GL}(2n,k),$$

where for each i, we have that $x_i + \sqrt{\alpha} y_i \in E(A,1)$, $x_i - \sqrt{\alpha} y_i \in E(A,-1)$, $\tilde{x}_i + \sqrt{\alpha}\tilde{y}_i \in E(B,1)$, $\tilde{x}_i - \sqrt{\alpha}\tilde{y}_i \in E(B,-1)$, and we know that

$$X^T J X = \frac{1}{2} \begin{pmatrix} J & 0 \\ 0 & \frac{1}{\alpha} J \end{pmatrix}$$

and

$$Y^T J Y = \frac{1}{2} \begin{pmatrix} J & 0 \\ 0 & \frac{1}{\beta} J \end{pmatrix}.$$

Then, Inn_A *and* Inn_B *are isomorphic over* $\mathrm{SP}(2n,k)$ *if and only α and β lie in the same square class of k.*

Proof. First, we note that if there exists $Q \in \mathrm{SP}(2n,k)$ such that $Q^{-1}AQ = B$, then Inn_A and Inn_B are isomorphic over $\mathrm{SP}(2n,k)$. Secondly, we note that this can be the case if and only if α and β are in the same square class. So, to prove this theorem, we can simply assume that $\alpha = \beta$ and we will show that there exists such a a $Q \in \mathrm{SP}(2n,k)$.

Let $Q = XY^{-1}$. First, we note that

$$Q^T J Q = (XY^{-1})^T J (XY^{-1}) = (Y^{-1})^T (X^T J X) Y^{-1} = (Y^{-1})^T (Y^T J Y) Y^{-1} = J,$$

so we see that $Q \in \mathrm{SP}(2n,k)$.

Lastly, we see that

$$Q^{-1}AQ = (XY^{-1})^{-1} A (XY^{-1}) = Y(X^{-1}AX)Y^{-1}$$

$$= \frac{\sqrt{\alpha}}{\alpha} Y \begin{pmatrix} 0 & I_n \\ \alpha I_n & 0 \end{pmatrix} Y^{-1} = B.$$

□

From here, it is clear that the number of Type 2 involution isomorphy classes is dependent on n and on the number of square classes of the field k.

Corollary 3.2.9. *If n is even, then $\mathrm{SP}(2n,k)$ has at most $|k^*/(k^*)^2| - 1$ isomorphy classes of Type 2 involutions. If n is odd, then $\mathrm{SP}(2n,k)$ has no Type 2 involutions.*

3.2.3 Type 3 Involutions

We now examine the Type 3 case. Recall that φ is a Type 3 involution if $\varphi = \mathrm{Inn}_A$, where $A \in \mathrm{SP}(2n,k)$ and $A^2 = -I$. Such matrices have eigenvalues $\pm i$, and are diagonalizable because the minimal polynomial has no repeated roots. We begin by proving a couple of results about the eigenvectors of such matrices.

Lemma 3.2.10. *Suppose $A \in \mathrm{SP}(2n,k)$ induces a Type 3 involution of $\mathrm{SP}(2n,k)$. Also suppose $x, y \in k^n$ such that $x + iy \in E(A,-i)$. Then, $x - iy \in E(A,i)$. Likewise, if $u, v \in k^n$ such that $u + iv \in E(A,i)$. Then, $u - iv \in E(A,-i)$. Further, $\dim(E(A,i)) = \dim(E(A,-i))$.*

Proof. Recall that complex conjugation preserves multiplication. This applies at the matrix level as well as at the scalar level. Because of this and since

$$A(x+iy) = -i(x-iy) = y - ix,$$

then it follows that

$$A(x-iy) = y + ix = i(x-iy).$$

That is, $x - iy \in E(A,-i)$. This proves the first statement. An analogous argument proves the second.

To see that $\dim(E(A,i)) = \dim(E(A,-i))$ is the case, note that the first statement tells us that $\dim(E(A,i)) \leqslant \dim(E(A,-i))$, and that the second statement tells us that $\dim(E(A,i)) \geqslant \dim(E(A,-i))$. □

Lemma 3.2.11. *Suppose $A \in \mathrm{SP}(2n,k)$ induces a Type 3 involution of $\mathrm{SP}(2n,k)$. Then, there exists $x_1, ..., x_n, y_1, ..., y_n \in k^{2n}$ such that the $x_j + iy_j$ form a basis for $E(A,i)$ and the $x_j - iy_j$ form a basis for $E(A,-i)$.*

Proof. Since Inn_A is Type 3, then we are assuming that $A \in \mathrm{SP}(2n,k)$ and $A^2 = -I$. It follows that all eigenvalues of A are $\pm i$. Since there are no repeated roots in the minimal polynomial of A, then we see that A is diagonalizable. We wish to construct bases for $E(A,i)$ and $E(A,-i)$ such that all the vectors lie in $k[i]^{2n}$. Let $\{z_1, ..., z_{2n}\}$ be a basis for k^{2n}. For each j, let $u_j = (A + iI)z_j$. Note that

$$Au_j = A(A+iI)z_j = (A^2 + iA)z_j = (-I + iA)z_j = i(A+iI)z_j = iu_j.$$

So, $\{u_1, ..., u_{2n}\}$ must span $E(A,i)$. Thus, we can appropriately choose n of these vectors and form a basis for $E(A,i)$. We can reorder, and assume that the n chosen vectors are $u_1, ..., u_n$. Let $x_j = Ax_j$ and $y_j = z_j$. Then, these eigenvectors are of the form $x_j + iy_j$. By the previous lemma, we know that $x_j - iy_j \in E(A,-i)$. This proves the statement.

$\square$

We are now able to prove results that characterize the matrices that induce Type 3 involutions, and then use these characterizations to find conditions on these involutions that are equivalent to isomorphy. We will have to prove this by looking at separate cases depending on whether or not $i = \sqrt{-1}$ lies in k. We begin by assuming that $i \in k$.

Lemma 3.2.12. *Assume $i \in k$ and suppose $\vartheta = \mathrm{Inn}_A$ is a Type 3 involution of $\mathrm{SP}(2n,k)$, where $A \in \mathrm{SP}(2n,k)$. Then, $A = X \begin{pmatrix} iI_n & 0 \\ 0 & -iI_n \end{pmatrix} X^{-1}$ for some $X \in \mathrm{GL}(n,k)$, where $X^T J X = \begin{pmatrix} 0 & X_1 \\ -X_1 & 0 \end{pmatrix}$ where X_1 is diagonal.*

Proof. We know from Lemma 3.2.11 that we have bases for $E(A,i)$ and $E(A,-i)$ that lie in k^{2n}. We will show that we can in fact choose bases $a_1, ..., a_n$ for $E(A,i) \cap k^{2n}$ and $b_1, ..., b_n$ for $E(A,-i) \cap k^{2n}$ such that $\beta(a_j, a_l) = 0 = \beta(b_j, b_l)$ and $\beta(a_j, b_l)$ is nonzero if and only if $j = l$. We will build these bases recursively.

First, we know that we can choose some nonzero $a_1 \in E(A,i) \cap k^{2n}$. Then, since β is non degenerate, we can choose a vector t such that $\beta(a_1, t) \neq 0$. We note that $E(A,i) \oplus E(A,-i) = k^{2n}$, so we can choose $t_i \in E(A,i) \cap k^{2n}$ and $t_{-i} \in E(A,-i) \cap k^{2n}$ such that $t = t_i + t_{-i}$. Since $\beta(a_1, t_i) = 0$, then it follows that $\beta(a_1, t_{-i}) \in k$ is nonzero. Let $b_1 = t_{-i}$.

Let $E_1 = \mathrm{Span}_k(a_1, b_1)$ and let F_1 be the orthogonal complement of E_1 in k^{2n}. Since the system of linear equations

$$\beta(a_1, x) = 0$$

$$\beta(b_1, x) = 0$$

has $2n-2$ free variables, then we see that F_1 has dimension $2n-2$.

We now wish to find $a_2 \in F_1 \cap E(A,i)$. Similar to the construction in the previous lemma, we can choose $x \in F_1$, and let $a_2 = Ax + ix$. Now we want $b_2 \in F_2 \cap E(A-,i)$ such that $\beta(a_2, b_2)$ is nonzero. Since $\beta|_{F_1}$ is non degenerate, then there exists some $y \in F_2$ such that $\beta(a_2, y) \neq 0$. Similar to the construction of b_1, we see that this implies the existence of a vector b_2 that fits our criteria.

Now, we let $E_2 = \mathrm{Span}_k(a_1, a_2, b_1, b_2)$ and let F_2 be the orthogonal complement of E_2 in k^n. We continue this same argument n times, until we have the bases that we wanted to find. Let

$$X = (a_1, ..., a_n, b_1, ..., b_n).$$

Then, the result follows. $\square$

We can now use this characterization to show that all such involutions must be isomorphic.

Theorem 3.2.13. *Assume that $i \in k$. Then, if* Inn_A *and* Inn_B *are both Type 3 involutions of* $\mathrm{SP}(2n,k)$*, then* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{SP}(2n,k)$*.*

Proof. Suppose we have two such involutions of $\mathrm{SP}(2n,k)$. Let them be represented by matrices $A, B \in \mathrm{SP}(2n,k)$. By the previous Lemma, we can choose $X, Y \in \mathrm{GL}(n,k)$ such that

$$X^{-1}AX = \begin{pmatrix} iI_n & 0 \\ 0 & -iI_n \end{pmatrix} = Y^{-1}BY,$$

$$X^TJX = \begin{pmatrix} 0 & X_1 \\ -X_1 & 0 \end{pmatrix}$$

and

$$Y^TJY = \begin{pmatrix} 0 & Y_1 \\ -Y_1 & 0 \end{pmatrix}$$

where X_1 and Y_1 are diagonal.

Since X_1 and Y_1 are both invertible diagonal matrices, then we can choose R_1 and $R_2 \in \mathrm{GL}(\frac{n}{2},k)$ such that $Y_1 = R_1^T X_1 R_2$. Let $R = \begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix}$ and $Q = XRY^{-1}$. We will show that $Q \in \mathrm{SP}(2n,k)$ and $Q^{-1}AQ = B$. This will then prove that Inn_A and Inn_B lie in the same isomorphy class.

First we show that $Q \in \mathrm{SP}(2n,k)$. Note that

$$Q^TJQ = (XRY^{-1})^T J (XRY^{-1}) = (Y^{-1})^T R^T (X^TJX) RY^{-1}$$

$$= (Y^{-1})^T (Y^TJY) Y^{-1} = J,$$

which proves this claim.

Lastly, we show that $Q^{-1}AQ = B$. We first note that R and $\begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix}$ commute. Then, we see that

$$Q^{-1}AQ = (XRY^{-1})^{-1} A (XRY^{-1}) = YR^{-1}(X^{-1}AX)RY^{-1}$$

$$= YR^{-1} \begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix} RY^{-1} = YR^{-1}R \begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix} Y^{-1}$$

$$= Y \begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix} Y^{-1} = B.$$

We have shown what was needed.

□

We now examine the case where $i \notin k$, beginning with a characterization of the matrices that induce these involutions.

Lemma 3.2.14. *Assume $i \notin k$. Suppose $\vartheta = \mathrm{Inn}_A$ is a Type 3 involution of $\mathrm{SP}(2n, k)$. Then,* $A = U \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} U^{-1} = UJU^{-1}$ *for*

$$U = \begin{pmatrix} a_1 & a_2 & \cdots & a_n & b_1 & b_2 & \cdots & b_n \end{pmatrix} \in \mathrm{GL}(2n, k),$$

where the $a_j + ib_j$ are a basis for $E(A, i)$, the $a_j - ib_j$ are a basis for $E(A, -i)$, and $U^T JU = \begin{pmatrix} 0 & U_1 \\ -U_1 & 0 \end{pmatrix}$, where U_1 is diagonal.

Proof. We know from Lemma 3.2.11 that we have bases for $E(A, i)$ and $E(A, -i)$ that lie in $k[i]^{2n}$. We will show that we can in fact choose bases $a_1 + ib_1, ..., a_n + ib_n$ for $E(A, i) \cap k[i]^{2n}$ and $a_1 - ib_1, ..., a_n - ib_n$ for $E(A, -i) \cap k[i]^{2n}$ such that $\beta(a_j + ib_j, a_l - ib_l)$ is nonzero if and only if $j = l$. From this, we will be able to show that $\beta(a_j, a_l) = 0 = \beta(b_j, b_l)$ when $j \neq l$ and $\beta(a_j, b_l) = 0$ for all j and l. We will build these bases recursively.

Recall that given any vector $x \in k^{2n}$, we know that $Ax + ix \in E(A, i)$. We want to choose $x \in k^{2n}$ such that $x^T A^T Jx \neq 0$. (The reasons for this will become apparent.) If $e_j^T A^T Je_j \neq 0$, we can let $x = e_j$. Suppose that this doesn't occur for any j.

Since $A^T J$ is invertible, we know that for more than $2n$ pairs of j and l we have $e_j^T A^T Je_l \neq 0$. Also, we see that since A is symplectic and $A^T JA = J$, then we have that

$$A^T J = JA^{-1} = JA^3 = -JA$$

and that

$$(A^T J)^T = J^T A = -JA = A^T J.$$

That is, $A^T J$ is symmetric. So, $e_j^T A^T Je_j = e_l^T A^T Je_l$. Then, we can let $x = e_j + e_l$. Then, we have

$$x^T A^T Jx = e_j A^T Je_l + e_l A^T Je_j = 2e_j A^T Je_l \neq 0.$$

In either case, we have many choices for x.

Let $x \in k^{2n}$ be a vector from above. We have $Ax + ix \in E(A, i)$. Let $a_1 = Ax$ and $b_1 = x$. So, $a_1 + ib_1 \in E(A, i)$ and $a_1 - ib_1 \in E(A, -i)$. From this, it follows that

$$\beta(a_1 + ib_1, a_1 - ib_1) = (\beta(a_1, a_1) + \beta(b_1, b_1)) + i(-\beta(a_1, b_1) + \beta(b_1, a_2))$$

$$= 0 + i(-\beta(Ax, x) + \beta(x, Ax)$$

$$= -2i\beta(Ax, x) = -2i(x^T A^T Jx) \neq 0.$$

Let $E_1 = \mathrm{Span}_{k[i]}(a_1 + ib_1, a_1 - ib_1) = \mathrm{Span}_{k[i]}(a_1, b_1)$, and let F_1 be the orthogonal complement of E_1 over $k[i]$. F_1 has dimension $2n-2$, and $\beta|_{F_1}$ is nondegenerate. So, we can find a nonzero vector $x \in F_1 \cap k^{2n}$ such that $\beta|_{F_1}(Ax, x) \neq 0$. So, as in the last case, let $a_2 = Ax$ and $b_2 = x$. Similar to before, we have $\beta(a_2 + ib_2, a_2 - ib_2) \neq 0$.

Let $E_2 = \mathrm{Span}_{k[i]}(a_1, a_2, b_1, b_2)$, and let F_2 be the orthogonal complement of E_2 over $k[i]$. In this manner, we can create the bases that we noted in the opening paragraph of this proof.

Note that we always have

$$0 = \beta(a_j + ib_j, a_l + ib_l) = (\beta(a_j, a_l) - \beta(b_j, b_l)) + i(\beta(a_j, b_l) + \beta(b_j, a_l)),$$

and when $j \neq l$ we have

$$0 = \beta(a_j + ib_j, a_l - ib_l) = (\beta(a_j, a_l) + \beta(b_j, b_l)) + i(-\beta(a_j, b_l) + \beta(b_j, a_l)).$$

This tells us that when $j \neq l$ that

$$\beta(a_j, b_l) = \beta(a_j, a_l) = \beta(b_j, b_l) = 0.$$

When $j = l$, we know that $\beta(b_j, b_j) = 0 = \beta(a_j, a_j)$. Lastly, we see that $\beta(a_j, b_j) = -\beta(b_j, a_j)$.

Let

$$U = (a_1, ..., a_n, b_1, ..., b_n).$$

Then, it follows that $U^T JU = \begin{pmatrix} 0 & U_1 \\ -U_1 & 0 \end{pmatrix}$ where X_1 is a diagonal $n \times n$ matrix.

Lastly, since $Ab_j = a_j$, then it follows that $Aa_j = -b_j$. So, we have that

$$A = U \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} U^{-1}.$$

□

We now show that if $i \notin k$, then we also have that there is only one isomorphy class of Type 3 involutions.

Theorem 3.2.15. *Assume $i \notin k$. Then, if* Inn_A *and* Inn_B *are both Type 3 involutions of* $\mathrm{SP}(2n, k)$*, then* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{SP}(2n, k)$.

Proof. By the previous Lemma, we can choose a matrix $U \in \mathrm{GL}(n,k)$ such that

$$A = U \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix} U^{-1}$$

for

$$U = \begin{pmatrix} a_1 & a_2 & \cdots & a_{\frac{n}{2}} & b_1 & b_2 & \cdots & b_{\frac{n}{2}} \end{pmatrix} \in \mathrm{GL}(n,k),$$

where the $a_j + ib_j$ are a basis for $E(A,i)$, the $a_j - ib_j$ are a basis for $E(A,-i)$, and $U^TJU = \begin{pmatrix} 0 & U_1 \\ -U_1 & 0 \end{pmatrix}$ for diagonal matrix U_1.

Let

$$X = (a_1 + ib_1, ..., a_{\frac{n}{2}} + ib_{\frac{n}{2}}, a_1 - ib_1, ..., a_{\frac{n}{2}} - ib_{\frac{n}{2}}),$$

and consider Inn_A and Inn_B as involutions of $\mathrm{SP}(2n, k[i])$. By construction, we see that X is a matrix that satisfies the conditions of Lemma 3.2.12 for the group $\mathrm{SP}(2n, k[i])$. We note that $X_1 = -2iU_1$. We also know by the previous Theorem that Inn_A and Inn_B are isomorphic over $\mathrm{SP}(2n, k[i])$. So, we can choose $Q_i \in \mathrm{SP}(2n, k[i])$ such that $Q_i^{-1}AQ_i = B$. Let $Y = Q_i^{-1}X$. We now show a couple of facts about Y.

First, we note that since Y was obtained from X via row operations, then for $1 \leqslant j \leqslant \frac{n}{2}$, the jth and $\frac{n}{2} + j$th columns are i-conjugates of one another.

Also, note that

$$Y^{-1}BY = (Q_i^{-1}X)^{-1}B(Q_i^{-1}X) = X^{-1}Q_iBQ_i^{-1}X$$

$$= X^{-1}AX = \begin{pmatrix} -iI_{\frac{n}{2}} & 0 \\ 0 & iI_{\frac{n}{2}} \end{pmatrix}.$$

Lastly, we see that

$$Y^TJY = (Q_i^{-1}X)^TJ(Q_i^{-1}X) = X^T((Q_i^{-1})^TJQ_i)X$$

$$= X^TJX = \begin{pmatrix} 0 & X_1 \\ -X_1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -2iU_1 \\ 2iU_1 & 0 \end{pmatrix}.$$

Write

$$Y = (c_1 + id_1, ..., c_{\frac{n}{2}} + id_{\frac{n}{2}}, c_1 - id_1, ..., c_{\frac{n}{2}} - id_{\frac{n}{2}}),$$

and let

$$V = (c_1, ..., c_{\frac{n}{2}}, d_1, ..., d_{\frac{n}{2}}).$$

It follows from what we have shown that

$$B = V \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix} V^{-1} \text{ where } V^TJV = \begin{pmatrix} 0 & U_1 \\ -U_1 & 0 \end{pmatrix} = U^TMU.$$

Now, let $Q = UV^{-1}$. We will show that $Q^{-1}AQ = B$ and $Q \in \mathrm{SP}(2n,k)$. This will prove that Inn_A and Inn_B are isomorphic over $\mathrm{SP}(2n,k)$.

We first show that $Q \in \mathrm{SP}(2n,k)$.

$$Q^TJQ = (UV^{-1})^TJUV^{-1} = (V^{-1})^T(U^TJU)V^{-1} = (V^{-1})^T(V^TJV)V^{-1} = J.$$

Lastly, we show that $Q^{-1}AQ = B$.

$$Q^{-1}AQ = (UV^{-1})^{-1}A(UV^{-1}) = VU^{-1}AUV^{-1}$$

$$= V \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix} V^{-1} = B.$$

We have shown what was needed.

□

Combining the results from this section, we get the following corollary.

Corollary 3.2.16. *If* Inn_A *and* Inn_B *are both Type 3 involutions of* $\mathrm{SP}(2n,k)$*, then* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{SP}(2n,k)$*. That is,* $\mathrm{SP}(2n,k)$ *has exactly one isomorphy class of Type 3 involutions. Further, the matrix* J *is a representative matrix for this isomorphy class.*

3.2.4 Type 4 Involutions

We now move on to a similar classification in the Type 4 case. First, we characterize the eigenvectors of the matrices that induce these involutions. Recall that we can choose $A \in \mathrm{SP}(2n,k[\sqrt{\alpha}])$ such that each entry of A is a $k-$multiple of $\sqrt{\alpha}$, and that we know $A^2 = -I$. We begin by proving a couple of lemmas about the eigenspaces of these matrices.

Lemma 3.2.17. *Suppose* $A \in \mathrm{SP}(2n,k[\sqrt{\alpha}])$ *induces a Type 4 involution of* $\mathrm{SP}(2n,k)$*. Also suppose* $x,y \in k^{2n}$ *such that* $x+\sqrt{-\alpha}y \in E(A,i)$*. Then,* $x-\sqrt{-\alpha}y \in E(A,-i)$*. Likewise, if* $u,v \in k^{2n}$ *such that* $u+\sqrt{-\alpha}v \in E(A,-i)$*. Then,* $u-\sqrt{-\alpha}v \in E(A,i)$*. Further,* $\dim(E(A,i)) = \dim(E(A,-i))$*.*

Proof. Suppose $x,y \in k^n$ such that $x+\sqrt{-\alpha}y \in E(A,-i)$. Then,

$$A(x+\sqrt{-\alpha}y) = -i(x+\sqrt{-\alpha}y)$$

which implies

$$Ax + \sqrt{-\alpha}Ay = \sqrt{\alpha}y - ix.$$

Then, complex conjugation tells us that

$$Ax - \sqrt{-\alpha}Ay = \sqrt{\alpha}y + ix,$$

which tells us that

$$A(x - \sqrt{-\alpha}y) = i(x - \sqrt{-\alpha}y).$$

A similar argument shows that if $u, v \in k^n$ such that $u + \sqrt{-\alpha}v \in E(A, i)$. Then, $u - \sqrt{-\alpha}v \in E(A, -i)$.

Since $x + \sqrt{-\alpha}y \in E(A, -i)$ implies $x - \sqrt{-\alpha}y \in E(A, i)$ and vice versa, then we see that $\dim(E(A, i)) = \dim(E(A, -i))$.

□

Lemma 3.2.18. *Suppose $\vartheta = \mathrm{Inn}_A$ is a Type 4 involution of $\mathrm{SP}(2n, k)$ where $A \in \mathrm{SP}(2n, k[\sqrt{\alpha}])$. Then, we can find $x_1, ..., x_n, y_1, ..., y_n \in k^n$ such that the $x + \sqrt{-\alpha}y$ are a basis for $E(A, i)$ and the $x - \sqrt{-\alpha}y$ are a basis for $E(A, -i)$.*

Proof. Since Inn_A is Type 4, then we are assuming that $A \in \mathrm{SP}(2n, k[\sqrt{\alpha}])$ and $A^2 = -I$. It follows that all eigenvalues of A are $\pm i$. Since there are no repeated roots in the minimal polynomial of A, then we see that A is diagonalizable. We wish to construct bases for $E(A, i)$ and $E(A, -i)$ such that all the vectors lie in $k[i]^{2n}$. Let $\{z_1, ..., z_{2n}\}$ be a basis for k^{2n}. For each j, let $u_j = (\sqrt{\alpha}A + \sqrt{-\alpha}I)z_j$. Note that

$$Au_j = A(\sqrt{\alpha}A + \sqrt{-\alpha}I)z_j = (\sqrt{\alpha}A^2 + \sqrt{-\alpha}A)z_j = i(\sqrt{\alpha}A + \sqrt{-\alpha}I)z_j = iu_j.$$

So, $\{u_1, ..., u_n\}$ must span $E(A, i)$. Thus, we can appropriately choose n of these vectors and form a basis for $E(A, i)$. Note that each of these vectors lies in $k[i]^{2n}$. Label these basis vectors as $v_1, ..., v_n$. We can write each of these vectors as $v_j = x_j + \sqrt{-\alpha}y_j$. By the previous lemma, we know that $x_j - \sqrt{-\alpha}y_j \in E(A, -i)$, and that these vectors form a basis for $E(A, -i)$.

□

We are now able to prove results that characterize the matrices that induce Type 4 involutions, and then use these characterizations to find conditions on these involutions that are equivalent to isomorphy. We will have separate cases, depending on whether or not $\sqrt{-\alpha}$ lies in k. We begin by assuming that $\sqrt{-\alpha} \in k$. Since we are also assuming that $\sqrt{\alpha} \notin k$, then it follows from these two assumptions that α and -1 lie in the same square class of k. Thus, we can assume in this case that $\alpha = -1$, which means $\sqrt{-\alpha} = 1$.

Lemma 3.2.19. *Assume $\sqrt{-\alpha} \in k$ and suppose ϑ is a Type 4 involution of* $\mathrm{SP}(2n,k)$*. Then,* $A = X \begin{pmatrix} iI_{\frac{n}{2}} & 0 \\ 0 & -iI_{\frac{n}{2}} \end{pmatrix} X^{-1}$ *for some* $X \in \mathrm{GL}(2n,k)$*, where* $X^TJX = \begin{pmatrix} 0 & X_1 \\ -X_1 & 0 \end{pmatrix}$ *and* X_1 *is diagonal.*

Proof. We know from Lemma 3.2.18 that we have bases for $E(A,i)$ and $E(A,-i)$ that lie in k^{2n}. We will show that we can in fact choose bases $a_1,...,a_n$ for $E(A,i)\cap k^{2n}$ and $b_1,...,b_n$ for $E(A,-i)\cap k^{2n}$ such that $\beta(a_j,a_l) = 0 = \beta(b_j,b_l)$ and $\beta(a_j,b_l)$ is nonzero if and only if $j = l$. We will build these bases recursively.

First, we know that we can choose some nonzero $a_1 \in E(A,i)\cap k^{2n}$. Then, since β is non degenerate, we can choose a vector t such that $\beta(a_1,t) \neq 0$. We note that $E(A,i)\oplus E(A,-i) = k^{2n}$, so we can choose $t_i \in E(A,i)\cap k^{2n}$ and $t_{-i} \in E(A,-i)\cap k^{2n}$ such that $t = t_i + t_{-i}$. Since $\beta(a_1,t_i) = 0$, then it follows that $\beta(a_1,t_{-i}) \in k$ is nonzero. Let $b_1 = t_{-i}$.

Let $E_1 = \mathrm{Span}_k(a_1,b_1)$ and let F_1 be the orthogonal complement of E_1 in k^{2n}. Since the system of linear equations

$$\beta(a_1,x) = 0$$

$$\beta(b_1,x) = 0$$

has $2n-2$ free variables, then we see that F_1 has dimension $2n-2$.

We now wish to find $a_2 \in F_2 \cap E(A,i)$. Similar to the construction in the previous lemma, we can choose $x \in F_1$, and let $a_2 = \sqrt{\alpha}Ax + \sqrt{-\alpha}x$. Now we want $b_2 \in F_2 \cap E(A-,i)$ such that $\beta(a_2,b_2)$ is nonzero. Since $\beta|_{F_1}$ is non degenerate, then there exists some $y \in F_2$ such that $\beta(a_2,y) \neq 0$. Similar to the construction of b_1, we see that this implies the existence a vector b_2 that fits our criteria.

Now, we let $E_2 = \mathrm{Span}_k(a_1,a_2,b_1,b_2)$ and let F_2 be the orthogonal complement of E_2 in k^n. We continue this same argument n times, until we have the bases that we wanted to find. Let

$$X = (a_1,...,a_n,b_1,...,b_n).$$

Then, the result follows. □

Here is an example of a Type 4 involution when $\sqrt{-\alpha} \in k$.

Example 3.2.20. *Let k be $\mathbb{R}$. So, $\alpha = -1$. Notice that $\sqrt{-\alpha} = 1 \in \mathbb{R}$. Consider the matrix*

$$A = i\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

Inn_A *is a Type 4 involution of* $\mathrm{SP}(4,k)$ *since* $A^2 = -I$ *and each entry of* A *is a* k*-multiple of* i*. A basis for* $E(A,1)$ *that matches the conditions of Lemma 3.2.19 is formed by the vectors* $v_1 = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ *and* $v_2 = \frac{\sqrt{2}}{2}\begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \end{pmatrix}$*. It can also be shown that* $v_3 = \frac{\sqrt{2}}{2}\begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$ *and* $v_4 = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$ *are basis vectors for* $E(A,-1)$ *that also match the conditions of Lemma 3.2.19.*

Following the notation of the previous lemma, we have

$$X = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix},$$

where $X^TJX = J$ *and* $A = X\begin{pmatrix} iI_{\frac{n}{2}} & 0 \\ 0 & -iI_{\frac{n}{2}} \end{pmatrix}X^{-1}$ *.*

Now we characterize the isomorphy classes of Type 4 involutions in the case where $\sqrt{-\alpha} \in k$.

Theorem 3.2.21. *Assume that* $\sqrt{-\alpha} \in k$*. Then, if* Inn_A *and* Inn_B *are both Type 4 involutions of* $\mathrm{SP}(2n,k)$ *such that* $A, B \in \mathrm{SP}(2n, k[\sqrt{\alpha}])$*, then* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{SP}(2n,k)$*.*

Proof. Suppose we have two such involutions of $\mathrm{SP}(2n,k)$. Let them be represented by matrices $A, B \in \mathrm{SP}(2n,k)$. By the previous Lemma, we can choose $X, Y \in \mathrm{GL}(n,k)$ such that

$$X^{-1}AX = \begin{pmatrix} iI_n & 0 \\ 0 & -iI_n \end{pmatrix} = Y^{-1}BY,$$

$$X^TJX = \begin{pmatrix} 0 & X_1 \\ -X_1 & 0 \end{pmatrix},$$

and

$$Y^TJY\begin{pmatrix} 0 & Y_1 \\ -Y_1 & 0 \end{pmatrix},$$

where X_1 and Y_1 are diagonal.

Since X_1 and Y_1 are both invertible diagonal matrices, then we can choose R_1 and $R_2 \in$

$\mathrm{GL}(\frac{n}{2}, k)$ such that $Y_1 = R_1^T X_1 R_2$. Let $R = \begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix}$ and $Q = XRY^{-1}$. It follows from this that $R^T X^T JXR = Y^T JY$. We will show that $Q \in \mathrm{SP}(2n, k)$ and $Q^{-1}AQ = B$. This will then prove that Inn_A and Inn_B lie in the same isomorphy class.

First we show that $Q \in \mathrm{SP}(2n, k)$. Note that

$$Q^T JQ = (XRY^{-1})^T J(XRY^{-1}) = (Y^{-1})^T R^T (X^T JX)RY^{-1}$$

$$= (Y^{-1})^T (Y^T JY)Y^{-1} = J,$$

which proves this claim.

Lastly, we show that $Q^{-1}AQ = B$. We first note that R and $\begin{pmatrix} iI & 0 \\ 0 & -iI \end{pmatrix}$ commute. Then, we see that

$$Q^{-1}AQ = (XRY^{-1})^{-1}A(XRY^{-1}) = YR^{-1}(X^{-1}AX)RY^{-1}$$

$$= YR^{-1}\begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix}RY^{-1} = YR^{-1}R\begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix}Y^{-1}$$

$$= Y\begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix}Y^{-1} = B.$$

□

We now examine the case where $\sqrt{-\alpha} \notin k$. We begin with a characterization of the matrices that induce Type 4 involutions in this case.

Lemma 3.2.22. *Assume $\sqrt{-\alpha} \notin k$. Suppose $\vartheta = \mathrm{Inn}_A$ is a Type 4 involution of $\mathrm{SP}(2n, k)$. Then, $A = \frac{\sqrt{\alpha}}{\alpha}U\begin{pmatrix} 0 & I_n \\ -\alpha I_n & 0 \end{pmatrix}U^{-1}$ for*

$$U = \begin{pmatrix} a_1 & a_2 & \cdots & a_n & b_1 & b_2 & \cdots & b_n \end{pmatrix} \in \mathrm{GL}(2n, k),$$

where the $a_j + \sqrt{-\alpha}b_j$ are a basis for $E(A, i)$, the $a_j - \sqrt{-\alpha}b_j$ are a basis for $E(A, -i)$, and $U^T JU = \begin{pmatrix} 0 & U_1 \\ -U_1 & 0 \end{pmatrix}$, where U_1 is diagonal.

Proof. We know from Lemma 3.2.18 that we have bases for $E(A, i)$ and $E(A, -i)$ that lie in $k[\sqrt{-\alpha}]^{2n}$. We will show that we can in fact choose bases $a_1 + \sqrt{-\alpha}b_1, ..., a_n + \sqrt{-\alpha}b_n$ for $E(A, i) \cap k[\sqrt{-\alpha}]^{2n}$ and $a_1 - \sqrt{-\alpha}b_1, ..., a_n - \sqrt{-\alpha}b_n$ for $E(A, -i) \cap k[\sqrt{-\alpha}]^{2n}$ such that $\beta(a_j + ib_j, a_l - ib_l)$ is nonzero if and only if $j = l$. From this, we will be able to show that

$\beta(a_j, a_l) = 0 = \beta(b_j, b_l)$ when $j \neq l$ and $\beta(a_j, b_l) = 0$ for all j and l. We will build these bases recursively.

Recall that given any vector $x \in k^{2n}$, we know that $\sqrt{\alpha}Ax + \sqrt{-\alpha}x \in E(A, i)$. We want to choose $x \in k^{2n}$ such that $x^T A^T Jx \neq 0$. That is, such that $\beta(Ax, x) \neq 0$. (The reasons for this will become apparent.) If $e_j^T A^T Je_j \neq 0$, we can let $x = e_j$. Suppose that this doesn't occur for any j.

Since $A^T J$ is invertible, we know that for more than $2n$ pairs of j and l we have $e_j^T A^T Je_l \neq 0$. Also, we see that since A is symplectic and $A^T JA = J$, then we have that

$$A^T J = JA^{-1} = JA^3 = -JA$$

and that

$$(A^T J)^T = J^T A = -JA = A^T J.$$

That is, $A^T J$ is symmetric. So, $e_j^T A^T Je_j = e_l^T A^T Je_l$. Then, we can let $x = e_j + e_l$. Then, we have

$$x^T A^T Jx = e_j A^T Je_l + e_l A^T Je_j = 2e_j A^T Je_l \neq 0.$$

In either case, we have many choices for x.

Let $x \in k^{2n}$ be a vector from above. We have $\sqrt{\alpha}Ax + \sqrt{-\alpha}x \in E(A, i)$. Let $a_1 = \sqrt{\alpha}Ax$ and $b_1 = x$. So, $a_1 + \sqrt{-\alpha}b_1 \in E(A, i)$ and $a_1 - \sqrt{-\alpha}b_1 \in E(A, -i)$. From this, it follows that

$$\beta(a_1+\sqrt{-\alpha}b_1, a_1-\sqrt{-\alpha}b_1) = (\beta(\sqrt{\alpha}Ax, \sqrt{\alpha}Ax)+\alpha\beta(x, x))+\sqrt{-\alpha}(-\beta(\sqrt{\alpha}Ax, x)+\beta(x, \sqrt{\alpha}Ax)$$

$$= 2\alpha i\beta(x, Ax) \neq 0.$$

Let $E_1 = \mathrm{Span}_{k[\sqrt{-\alpha}]}(a_1 + \sqrt{-\alpha}b_1, a_1 - \sqrt{-\alpha}b_1) = \mathrm{Span}_{k[\sqrt{-\alpha}]}(a_1, b_1)$, and let F_1 be the orthogonal complement of E_1 over $k[\sqrt{-\alpha}]$. F_1 has dimension $2n-2$, and $\beta|_{F_1}$ is nondegenerate. So, we can find a nonzero vector $x \in F_1 \cap k^{2n}$ such that $\beta|_{F_1}(x, -Ax) \neq 0$. So, as in the last case, let $a_2 = \sqrt{\alpha}Ax$ and $b_2 = x$. As before, we have $\beta(a_2 + \sqrt{-\alpha}b_2, a_2 - \sqrt{-\alpha}b_2) \neq 0$.

Let $E_2 = \mathrm{Span}_{k[\sqrt{-\alpha}]}(a_1, a_2, b_1, b_2)$, and let F_2 be the orthogonal complement of E_2 over $k[\sqrt{-\alpha}]$. In this manner, we can create the bases that we noted in the opening paragraph of this proof.

Note that we always have

$$0 = \beta(a_j + \sqrt{-\alpha}b_j, a_l + \sqrt{-\alpha}b_l) = (\beta(a_j, a_l) - \alpha\beta(b_j, b_l)) + \sqrt{-\alpha}(\beta(a_j, b_l) + \beta(b_j, a_l)),$$

and when $j \neq l$ we have

$$0 = \beta(a_j + \sqrt{-\alpha}b_j, a_l - \sqrt{-\alpha}b_l) = (\beta(a_j, a_l) + \alpha\beta(b_j, b_l)) + \sqrt{-\alpha}(-\beta(a_j, b_l) + \beta(b_j, a_l)).$$

This tells us that when $j \neq l$ that

$$\beta(a_j, b_l) = \beta(a_j, a_l) = \beta(b_j, b_l) = 0.$$

When $j = l$, we know that $\beta(b_j, b_j) = 0 = \beta(a_j, a_j)$. Lastly, we see that $\beta(a_j, b_j) = -\beta(b_j, a_j)$.

Let

$$U = (a_1, ..., a_n, b_1, ..., b_n).$$

Then, it follows that $U^T JU = \begin{pmatrix} 0 & U_1 \\ -U_1 & 0 \end{pmatrix}$ where U_1 is a diagonal $n \times n$ matrix.

Since $Aa_j = -\sqrt{\alpha} b_j$ and $Ab_j = \frac{\sqrt{\alpha}}{\alpha} a_j$, then we have $A = \frac{\sqrt{\alpha}}{\alpha} U \begin{pmatrix} 0 & I_n \\ -\alpha I_n & 0 \end{pmatrix} U^{-1}$.

We have shown what was needed. $\square$

The following is an example of a Type 4 involution where $\sqrt{-\alpha} \notin k$.

Example 3.2.23. *Let $k = \mathbb{F}_5$ and consider $\alpha = 2$. Note that $\sqrt{-\alpha} = \sqrt{3} \notin k$.*

Consider the matrix

$$A = \sqrt{2} \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \\ 3 & 0 & 4 & 0 \\ 0 & 3 & 0 & 4 \end{pmatrix}.$$

Inn_A *is a Type 4 involution of* $\mathrm{SP}(4, k)$ *since $A^2 = -I$ and each entry of A is a k-multiple of $\sqrt{2}$. A basis for $E(A, 1)$ that matches the conditions of Lemma 3.2.22 is formed by the vectors*

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 4 \\ 0 \end{pmatrix} + \sqrt{2} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

and

$$v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 4 \end{pmatrix} + \sqrt{2} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}.$$

It can be shown that

$$v_3 = \begin{pmatrix} 1 \\ 0 \\ 4 \\ 0 \end{pmatrix} - \sqrt{2} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

and

$$v_4 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 4 \end{pmatrix} - \sqrt{2} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

are basis vectors for $E(A,-1)$ that also match the conditions of Lemma 3.2.22.

Following the notation of the Lemma 3.2.22, we have

$$U = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 4 & 0 & 1 & 0 \\ 0 & 4 & 0 & 1 \end{pmatrix},$$

where $U^T J U = \begin{pmatrix} 0 & U_1 \\ -U_1 & 0 \end{pmatrix}$ for $U_1 = 2I$ and $A = \frac{\sqrt{2}}{2} U \begin{pmatrix} 0 & I \\ -2I & 0 \end{pmatrix} U^{-1}$.

We now find conditions on Type 4 involutions where $\sqrt{-\alpha} \notin k$ that are equivalent to isomorphy.

Theorem 3.2.24. *Assume $\sqrt{-\alpha} \notin k$. Then, if Inn_A and Inn_B are both Type 4 involutions of $\mathrm{SP}(2n,k)$ where the entries of A and B are k-multiples of $\sqrt{\alpha}$, then Inn_A and Inn_B are isomorphic over $\mathrm{SP}(2n,k)$.*

Proof. By Lemma 3.2.22, we can choose a matrix $U \in \mathrm{GL}(n,k)$ such that

$$A = \frac{\sqrt{\alpha}}{\alpha} U \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ -\alpha I_{\frac{n}{2}} & 0 \end{pmatrix} U^{-1}$$

for

$$U = \begin{pmatrix} a_1 & a_2 & \cdots & a_{\frac{n}{2}} & b_1 & b_2 & \cdots & b_{\frac{n}{2}} \end{pmatrix},$$

where the $a_j + \sqrt{-\alpha} b_j$ are a basis for $E(A,i)$, the $a_j - \sqrt{-\alpha} b_j$ are a basis for $E(A,-i)$, and $U^T J U = \begin{pmatrix} 0 & U_1 \\ -U_1 & 0 \end{pmatrix}$ for diagonal U_1.

Consider Inn_A and Inn_B as involutions of $\mathrm{SP}(2n, k[\sqrt{-\alpha}])$. If $k[\sqrt{-\alpha}] = k[\sqrt{\alpha}]$, then these are Type 3 involutions of $\mathrm{SP}(2n, k[\sqrt{-\alpha}])$, since A and B would have entries in the field, and $i \in k[\sqrt{-\alpha}]$. Otherwise, if $k[\sqrt{-\alpha}] \neq k[\sqrt{\alpha}]$, then these are Type 4 involutions where $\sqrt{-\alpha} \in k[\sqrt{-\alpha}]$.

Let

$$X = (a_1 + \sqrt{-\alpha}b_1, ..., a_{\frac{n}{2}} + \sqrt{-\alpha}b_{\frac{n}{2}}, a_1 - \sqrt{-\alpha}b_1, ..., a_{\frac{n}{2}} - \sqrt{-\alpha}b_{\frac{n}{2}}).$$

By construction, we see that X is a matrix that satisfies the conditions of Lemma 3.2.14 or Lemma 3.2.19 for the group $\mathrm{SP}(2n, k[\sqrt{\alpha}])$. We note that $X_1 = -2iU_1$. We also know by Corollary 3.2.16 or Theorem 3.2.21 that Inn_A and Inn_B are isomorphic (when viewed as involutions of $\mathrm{SO}(n, k[\sqrt{-\alpha}], \beta)$) over $\mathrm{O}(n, k[\sqrt{-\alpha}], \beta)$. So, we can choose $Q_\alpha \in \mathrm{SP}(2n, k[\sqrt{-\alpha}])$ such that $Q_\alpha^{-1}AQ_\alpha = B$. Let $Y = Q_\alpha^{-1}X$. Since Y is constructed by doing row operations on X, then we can write

$$Y = (c_1 + \sqrt{-\alpha}d_1, ..., c_{\frac{n}{2}} + \sqrt{-\alpha}d_{\frac{n}{2}}, c_1 - \sqrt{-\alpha}d_1, ..., c_{\frac{n}{2}} - \sqrt{-\alpha}c_{\frac{n}{2}}),$$

where $c_j, d_j \in k^n$. We now show a couple of facts about Y.

First, we note that since Y was obtained from X via row operations, then for $1 \leqslant j \leqslant \frac{n}{2}$, the jth and $\frac{n}{2} + j$th columns are i-conjugates of one another.

Next, we observe that

$$Y^{-1}BY = (Q_\alpha^{-1}X)^{-1}B(Q_\alpha^{-1}X) = X^{-1}Q_\alpha B Q_\alpha^{-1}X$$

$$= X^{-1}AX = \begin{pmatrix} iI_{\frac{n}{2}} & 0 \\ 0 & -iI_{\frac{n}{2}} \end{pmatrix}.$$

Lastly, we see that

$$Y^TJY = (Q_\alpha^{-1}X)^TJ(Q_\alpha^{-1}X) = X^T((Q_\alpha^{-1})^TJQ_\alpha)X$$

$$= X^TJX = \begin{pmatrix} 0 & X_1 \\ -X_1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -2iU_1 \\ 2iU_1 & 0 \end{pmatrix}.$$

Let

$$V = (c_1, ..., c_{\frac{n}{2}}, d_1, ..., d_{\frac{n}{2}}) \in \mathrm{GL}(n, k).$$

It follows from what we have shown that $B = \frac{\sqrt{\alpha}}{\alpha}V \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ -\alpha I_{\frac{n}{2}} & 0 \end{pmatrix} V^{-1}$ where $V^TJV = \begin{pmatrix} 0 & U_1 \\ -U_1 & 0 \end{pmatrix} = U^TJU$.

Now, let $Q = UV^{-1}$. We will show that $Q^{-1}AQ = B$ and $Q \in \mathrm{SP}(2n, k)$. This will prove that Inn_A and Inn_B are isomorphic over $\mathrm{SP}(2n, k)$.

We first show that $Q \in \mathrm{SP}(2n,k)$.

$$Q^T JQ = (UV^{-1})^T JUV^{-1} = (V^{-1})^T(U^T JU)V^{-1} = (V^{-1})^T(V^T JV)V^{-1} = J.$$

Lastly, we show that $Q^{-1}AQ = B$.

$$Q^{-1}AQ = (UV^{-1})^{-1}A(UV^{-1}) = VU^{-1}AUV^{-1}$$

$$= \frac{\sqrt{\alpha}}{\alpha} V \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ -\alpha I_{\frac{n}{2}} & 0 \end{pmatrix} V^{-1} = B.$$

We have shown what was needed.

□

Combining the results from this section, we get the following corollary.

Corollary 3.2.25. *If* Inn_A *and* Inn_B *are both Type 4 involutions of* $\mathrm{SP}(2n,k)$*, then* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{SP}(2n,k)$ *if and only if* A *and* B *have entries lying in the same field extension of* k*. That is,* $\mathrm{SP}(2n,k)$ *has at most* $|k^*/(k^*)^2| - 1$ *isomorphy classes of Type 4 involutions.*

3.3 Maximal Number of Isomorphy classes

From the work we have done, it follows that the maximum number of isomorphy classes of $\mathrm{SP}(2n,k)$ is a function of the number of square classes of k and n. We first define the following formulas.

Definition 3.3.1. *Let* $C_1(2n,k)$*,* $C_2(2n,k)$*,* $C_3(2n,k)$ *and* $C_4(2n,k)$ *be the number of isomorphy classes of involutions of* $\mathrm{SP}(2n,k)$ *of types 1, 2, 3, and 4, respectively.*

From our previous work, we have the following:

Corollary 3.3.2. *(i) If* n *is odd, then* $C_1(2n,k) = \frac{n-1}{2}$*. If* n *is even, then* $C_1(2n,k) = \frac{n}{2}$*.*

(ii) If n *is odd, then* $C_2(2n,k) = 0$*. If* n *is even, then* $C_2(2n,k) \leqslant |k^*/(k^*)^2| - 1$*.*

(iii) $C_3(2n,k) = 1$*.*

(iv) $C_4(2n,k) \leqslant |k^*/(k^*)^2| - 1$*.*

3.4 Explicit Examples

We have shown that the number of isomorphy classes of Type 1 and Type 3 involutions depends only on n, and not the field k. Since Type 2 and Type 4 involutions do not occur when k is algebraically closed, then the previous corollary tells us the number of isomorphy classes in this case. In addition to this example, we will also consider the cases where $k = \mathbb{R}$ and $k = \mathbb{F}_p$.

3.4.1 Type 2 Examples

We first consider the Type 2 case. So, we may assume that n is even. First, let us suppose that k is $\mathbb{R}$ or $\mathbb{F}_q$ where -1 is not a square in $\mathbb{F}_q$. Without loss of generality, assume $\alpha = -1$. Let A_1 be an $n \times n$ block diagonal matrix where each block is the 2×2 matrix $i \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then, let $A = \begin{pmatrix} A_1 & 0 \\ 0 & (A_1^{-1})^T \end{pmatrix}$. This matrix induces a Type 2 involution on $\mathrm{SP}(2n, k)$.

Now, let us suppose that $k = \mathbb{F}_q$ where -1 is a square. Let $\alpha \in k^*$ be a non-square. Then, we can choose $a, b \in k$ such that $a^2 + b^2 = \frac{1}{\alpha}$. Let A_1 be an $n \times n$ block diagonal matrix where each block is the 2×2 matrix $\sqrt{\alpha} \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$. Then, let $A = \begin{pmatrix} A_1 & 0 \\ 0 & (A_1^{-1})^T \end{pmatrix}$. This matrix induces a Type 2 involution on $\mathrm{SP}(2n, k)$. So if k is finite or real, then $\mathrm{SP}(2n, k)$ has the maximal number of Type 2 isomorphy classes.

3.4.2 Type 4 Examples

Now we consider the Type 4 case. So, n may be even or odd. Let us again begin by supposing that k is $\mathbb{R}$ or $\mathbb{F}_q$ where -1 is not a square in $\mathbb{F}_q$. Then, the matrix $\begin{pmatrix} iI_n & 0 \\ 0 & -iI_n \end{pmatrix}$ induces a Type 4 involution, and $\mathrm{SP}(2n, k)$ has the maximal number of isomorphy classes in this case, regardless of if n is odd or even.

Now, let us suppose that $k = \mathbb{F}_q$ where -1 is a square. Let $\alpha \in k^*$ be a non-square and choose $a, b \in k$ such that $a^2 + b^2 = \alpha$. If we let $U = \begin{pmatrix} cI_n & dI_n \\ -dI_n & cI_n \end{pmatrix}$ and then let

$$A = \frac{\sqrt{\alpha}}{\alpha} U \begin{pmatrix} 0 & I_n \\ -\alpha I_n & 0 \end{pmatrix} U^{-1}$$

$$= \frac{\sqrt{\alpha}}{\alpha^2} \begin{pmatrix} (1-\alpha)cdI_n & (c^2 + \alpha d^2)I_n \\ -(c^2 + \alpha d^2)I_n & -(1-\alpha)cdI_n \end{pmatrix}.$$

A induces a Type 4 involution on $\mathrm{SP}(2n, k)$. We have shown that if k is finite or real, then $\mathrm{SP}(2n, k)$ has the maximal number of Type 4 isomorphy classes. Thus, if k is real or finite it has the maximal number of all types of isomorphy classes.

While we have been unable to prove that this is the case for any field k, we believe that this is the case That is, we have the following conjecture:

Conjecture 3.4.1. *(i) If n is odd, then $C_1(2n, k) = \frac{n-1}{2}$. If n is even, then $C_1(2n, k) = \frac{n}{2}$.*

(ii) If n is odd, then $C_2(2n, k) = 0$. If n is even, then $C_2(2n, k) = |k^*/(k^*)^2| - 1$.

(iii) $C_3(2n, k) = 1$.

(iv) $C_4(2n, k) = |k^*/(k^*)^2| - 1$.

Chapter 4

Future Work

We have characterized and counted the isomorphy classes of involutions of friendly $\mathrm{SO}(n,k)$ over $\mathrm{O}(n,k)$ when k is an algebraically closed field or the real numbers, and we have partial results for the finite prime fields and the p-adic numbers. We have also characterized and counted the isomorphy classes of the involutions for $\mathrm{SP}(2n,k)$ over algebraically closed fields, the real numbers, and for a finite field of characteristic not 2. We also have constructed the tools to classify similar isomorphy classes of the involutions of other friendly $\mathrm{SO}(n,k,\beta)$ over $\mathrm{O}(n,k,\beta)$. In the future, we would like to completely classify the isomorphy classes of these involutions over these fields, and to also repeat this process for other symmetric bilinear forms β. Of particular interest would be the bilinear form β that corresponds to $M = \begin{pmatrix} -I_{n-1} & 0 \\ 0 & 1 \end{pmatrix}$. Then, $\mathrm{O}(n,k,\beta)$ is a generalization of the Lorentz group. We would also like to find isomorphy classes for friendly $\mathrm{SO}(n,k,\beta)$ over $\mathrm{SO}(n,k,\beta)$, which we have only done in the odd case. In addition we would like to characterize the isomorphy classes of the involutions in the cases where the characteristic of k is 3, but the group is not friendly. Moving beyond involutions of orthogonal and symplectic groups, we want to consider automorphisms or finite order $m > 2$. These give rise to generalized symmetric spaces in the same manner that involutions give rise to symmetric spaces. This is something that we want to consider for $\mathrm{SL}(n,k)$, $\mathrm{SO}(n,k,\beta)$ and $\mathrm{SP}(2n,k)$.

REFERENCES

[And71] G. Andrews,. *Number Theory.* W. B. Saunders Company, 1971.

[Art57] E. Artin. *Geometric Algebra.* Wiley-Interscience, 1957.

[Art91] M. Artin. *Algebra.* Prentice Hall, Englewood Cliffs, NJ, 1991.

[Bak2001] A. Baker. *Matrix Groups: An Introduction to Lie Group Theory.* Springer, 2001.

[Bor91] A. Borel. *Linear Algebraic Groups*, volume 126 of *Graduate texts in mathematics.* Springer Verlag, New York, 2nd enlarged edition, 1991.

[BT65] A. Borel and J. Tits. Groupes réductifs. *Inst. Hautes Études Sci. Publ. Math.*, 27:55–152, 1965.

[BT72] A. Borel and J. Tits. Complments á l'article: Groupes réductifs. *Publications Mathématiques de l'IHÉS*, 41:253-276, 1972.

[Bump2013] D. Bump. *Lie Groups*, volume 225 of *Graduate texts in mathematics.* Springer Verlag, New York, 2nd edition, 2013.

[Cur84] M. Curtis *Matrix Groups*, Springer-Verlag, New York, Second Edition, 1984.

[Die63] J. Dieudonne. *La Geometrie Des Groupes Classiques.* Springer-Verlag, 1963.

[Dom2003] C. Dometrius. *Relationship between Symmetric and Skew-symmetric Bilinear Forms on $V = k^n$ and Involutions of* $\mathrm{SL}(n, k)$ *and* $\mathrm{SO}(n, k, \beta)$. PhD Thesis, North Carolina State University, 2005.

[Hal00] B. Hall. *Lie Groups, Lie Algebras, and Representations.* Springer, 2000.

[Hel78] S. Helgason. *Differential Geometry, Lie Groups, and Symmetric Spaces.* Academic Press, 1978.

[Hel88] A. G. Helminck. Algebraic groups with a commuting pair of involutions and semisimple symmetric spaces. *Adv. in Math.*, 71:21–91, 1988.

[Hel2000] Helminck, A. G., On the Classification of k-involutions I. *Adv. in Math.* (2000).**153**(1), 1–117.

[HW93] A. G. Helminck and S. P. Wang. On rationality properties of involutions of reductive groups. *Adv. in Math.*, 99:26–96, 1993.

[HW2002] Aloysius G. Helminck and Ling Wu. Classification of involutions of $\mathrm{SL}(2, k)$. *Comm. Algebra*, 30(1):193–203, 2002.

[HWD2004] Aloysius G. Helminck, Ling Wu and Christopher Dometrius. Involutions of $\mathrm{SL}(n, k)$, $(n > 2)$. *Acta Appl. Math.*, **90**, 91-119, 2006.

[Hum75] J. E. Humphreys. *Linear algebraic groups*, volume 21 of *Graduate Texts in Mathematics*. Springer Verlag, New York, 1975.

[Jac2005] F. Jackson. *Characterizations of Involutions of* $\mathrm{SP}(2n, k)$. PhD Thesis, North Carolina State University, 2005.

[Jon67] B.W. Jones. *The Arithmetic of Quadratic Forms*. Mathematical Association of America, 1967.

[Ome78] O. O'Meara *Symplectic Groups*, volume 16 of *Mathematical Surveys*. American Mathematical Society, Providence, Rhode Island, 1978.

[Sch85] W. Scharlau. *Quadratic and Hermitian Forms*, volume 270 of *Grundlehren der mathematischen Wissenschaften*. Springer Verlag, Berlin-Heidelberg-New York-Tokyo, 1985.

[Schw2013] N. Schwartz. *On the Classification of k-involutions of* $\mathrm{SL}(n, k)$ *and* $\mathrm{O}(n, k)$ *over fields of Characteristic 2*. PhD Thesis, North Carolina State University, 2013.

[Ser73] J.P. Serre. *A Course in Arithmetic*. Springer-Verlag, 1973.

[Spr81] T. A. Springer. *Linear algebraic groups*, volume 9 of *Progr. Math.* Birkhäuser, Boston/Basel/Stuttgart, 1981.

[Szy97] K. Szymiczek. *Bilinear Algebra: An Introduction to the Algebraic Theory of Quadratic Forms*, volume 7 of *Algebra, Logic and Applications*. Gordon and Breach Science Publishers, Amsterdam, 1997.

[Wey46] H. Weyl. *The Classical Groups, Their Invariants and Representations*, Princeton University Press, Princeton, New Jersey, 1946.

[Wu2002] L. Wu. *Classification of Involutions of* $\mathrm{SL}(n,k)$ *and* $\mathrm{SO}(2n+1,k)$. PhD Thesis, North Carolina State University, 2002.