Isomorphy Classes of Involutions of SO(n, k, β), $n > 2$

**Robert W. Benim, Christopher E. Dometrius,
Aloysius G. Helminck, and Ling Wu**

Communicated by G. Ólafsson

Abstract. A first characterization of the isomorphism classes of k-involutions for any reductive algebraic group defined over a perfect field was given in *On the Classification of k-involutions I* using 3 invariants. In *Involutions of* SL(n, k), ($n > 2$) a full classification of all k-involutions on SL(n, k) for k algebraically closed, the real numbers, the p-adic numbers or a finite field was provided. In *Isomorphy Classes of Involutions of* SP($2n, k$), ($n > 2$), a similar classification was given for all k-involutions of SP($2n, k$). In this paper, we find analogous results to develop a detailed characterization of the k-involutions of SO(n, k, β), where β is any non-degenerate symmetric bilinear form and k is any field not of characteristic 2. We use these results to characterize the isomorphy classes of k-involutions of SO(n, k, β) for all bilinear forms, β when char(k) $\neq$ 2, 3, and for some bilinear forms when char(k) = 3. When $n \neq 3, 4, 6, 8$, then the characterization considers all involutions. If $n = 3, 4, 6, 8$, then the characterization only considers inner involutions.
Mathematics Subject Classification 2010: 14M15, 20G05, 20G15, 20K30.
Key Words and Phrases: Orthogonal Group, symmetric spaces, involutions, inner automophisms.

1. Introduction

Let G be a connected reductive algebraic group defined over a field k of characteristic not 2, θ a k-involution of G, i.e. a k-automorphism of G of order two, 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/H is called a symmetric variety and G_k/H_k is called a symmetric k-variety. For k the real numbers or the p-adic numbers, the symmetric k-varieties are also called reductive (real or p-adic) symmetric spaces or simply (real or p-adic) symmetric spaces. Symmetric spaces play an important role in many areas of mathematics and physics, but probably best known are the representations associated with these symmetric spaces which have been studied by many prominent mathematicians starting with a study of compact groups and their representations by Cartan [Car29], to a study of Riemannian symmetric spaces and real (and p-adic) groups by Harish Chandra [HC84] to a more recent study of the non Riemannian symmetric spaces (see for example

[vdBS97a, Far79, FJ80, ŌS80]) leading to a Plancherel formula in 1996 proven independently by Delorme [Del98] and van den Ban and Schlichtkrull [vdBS97b]. These authors further develop these ideas in [AO05]. Once this Plancherel formula was obtained the attention shifted to p-adic symmetric spaces (see for example [DH14, CD14, Del13, HH02, HH05]). In the late 1980's generalizations of these reductive symmetric spaces to other base fields started to play a role in other areas, like in the study of arithmetic subgroups (see [TW89]), the study of character sheaves (see for example [Lus90, Gro92]), geometry (see [DCP83, DCP85] and [Abe88]), singularity theory (see [LV83] and [HS90]), and the study of Harish Chandra modules (see [BB81] and [Vog83, Vog82]). This prompted Helminck and Wang to commence a study of rationality properties of symmetric k-varieties over general base fields, see [HW93] for some first results.

To study these symmetric k-varieties for any field k, one needs a classification. The isomorphy of these symmetric k-varieties can be reduced to the $\mathrm{Inn}(G, G_k)$-isomorphy of the related k-involutions (see [HW93]). Here $\mathrm{Inn}(G, G_k)$ is the set of inner automorphisms of G that leave G_k invariant. A characterization of these isomorphism classes of the k-involutions was given in [Helm2000] essentially using the following 3 invariants:

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

2. classification of the G_k-isomorphism classes of k-involutions of the k-anisotropic kernel of G.

3. classification of the G_k-isomorphism classes of k-inner elements of G.

For more details, see [Helm2000]. The admissible (Γ, θ)-indices determine most of the fine structure of the symmetric k-varieties and a classification of these was included in [Helm2000] 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 [HWD04, HW02] a full characterization of the $\mathrm{Inn}(G, G_k)$-isomorphism classes of k-involutions was given in the case that $G = \mathrm{SL}(n, k)$ which does not depend on any of the results in [Helm2000]. It was also shown how one may construct an outer-k-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. A similar classification for $G = \mathrm{SP}(2n, k)$, the Symplectic groups, can be found in [BHJ15].

We note that much work has been done in characterizing automorphisms of $\mathrm{O}(n, k, \beta)$, notably the works of Diedonne in [Die51] and [Die63], Rickart in [Ric50] and [Ric51], and Wonenburger in [Won62]. These results consider automorphisms of G_k under the action of the full automorphism group of G_k, so these results do not directly apply to the problem of isomorphy of k-involutions under the action of the subgroup $\mathrm{Inn}(G, G_k)$ of $\mathrm{Aut}(G_k)$ as considered in this paper.

In this paper we study k-involutions of $\mathrm{SO}(n, k, \beta)$, the special orthogonal group with respect to a symmetric bilinear form β on k^n. We give a characterization of the isomorphy classes of k-involutions of $\mathrm{SO}(n, k, \beta)$, which come from inner automorphisms Inn_A of the general linear group $\mathrm{GL}(n, \overline{k})$. In section 2, we state many of the important definitions and initial observations. In section 3 we show that if a k-automorphism $\theta = \mathrm{Inn}_A$ where $A \in \mathrm{GL}(n, \overline{k})$ leaves $\mathrm{SO}(n, k, \beta)$ invariant, then we can assume A is in $\mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$ when n is odd, and A is in $\mathrm{O}(n, k[\sqrt{\alpha}], \beta)$ when n is even, where $k[\sqrt{\alpha}]$ is a quadratic extension of k. Further, we show that each entry of A must be a k-multiple of $\sqrt{\alpha}$. To prove these results, we require that either $\mathrm{char}(k) \neq 3$, or we require a restriction on the bilinear form β. In section 4, we have the main results of the paper. We determine which $A \in \mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$ if n is odd and which $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$ if n is even induce k-involutions of $\mathrm{SO}(n, k, \beta)$ of the form Inn_A. We will see that when n is odd, there is only one type of these k-involutions, and if n is even, there are four types of these k-involutions. For each type, we determine nice conditions that are equivalent to isomorphy of these k-involutions over $\mathrm{SO}(n, k, \beta)$ if n is odd and over $\mathrm{O}(n, k, \beta)$ if n is even. When $n \neq 3, 4, 6, 8$, the k-involutions of the form Inn_A will be all of the k-involutions of $\mathrm{SO}(n, k, \beta)$. In section 5, we discuss the maximal number of possible isomorphy classes of k-involutions of the form Inn_A. In section 6 we look at some explicit examples of orthogonal groups, most of which are the standard orthogonal group, when k is algebraically closed, the real numbers, a finite field of order odd $q = p^m$, or the p-adic numbers

2. 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 k-involutions of $\mathrm{SL}(n, k)$ will be [HWD04]. 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 multiplicative 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 and theorems from [HWD04].

Definition 2.1.   Let G be an algebraic groups defined over a field k. Let G_k be the k-rational points of G. Let $\mathrm{Aut}(G, G_k)$ denote the the set of k-automorphisms of G_k. That is, $\mathrm{Aut}(G, G_k)$ is the set of automorphisms of G which fix G_k. We say

$\theta \in \mathrm{Aut}(G, G_k)$ is a *k-involution* if $\theta^2 = \mathrm{Id}$ but $\theta \neq \mathrm{Id}$. That is, a k-involution is a k-automorphism of order 2.

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

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

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

In [HWD04], the isomorphy classes of the inner-k-involutions of $\mathrm{SL}(n,k)$ were classified, and they are as follows:

Theorem 2.2. *Suppose the k-involution $\theta \in \mathrm{Aut}(\mathrm{SL}(n,k))$ is of inner type. Then up to isomorphism over $\mathrm{GL}(n,k)$, θ is one of the following:*

1. $\mathrm{Inn}_Y|_G$, 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

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

2. $\mathrm{Inn}_Y|_G$, where $Y = L_{\frac{n}{2},x} \in \mathrm{GL}(n,k)$ where x is a fixed element of a coset of k^*/k^{*2}, $x \not\equiv 1 \mod k^{*2}$ and

$$L_{\frac{n}{2},x} = \begin{pmatrix} 0 & 1 & \ldots & 0 & 0 \\ x & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & \ldots & x & 0 \end{pmatrix}.$$

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 their multiples) rather than $L_{\frac{n}{2},x}$. Either of these serves as a member of the isomorphy class listed in the previous theorem. It will become apparent that the isomorphy classes of k-involutions $\mathrm{SO}(n,k,\beta)$ over $\mathrm{O}(n,k,\beta)$ are just isomorphy classes of $\mathrm{SL}(n,k)$ over $\mathrm{GL}(n,k)$ 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

$\{e_1, \ldots e_n\}$ of k^n. We will say that M is the matrix of β if the basis $\{e_1, \ldots e_n\}$ is the standard basis of k^n.

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

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

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

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

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

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

It is clear from this definition that all matrices in $O(n, k, \beta)$ have determinant 1 or -1. We define the *special orthogonal group of β* to be the group

$$SO(n, k, \beta) = O(n, k, \beta) \cap SL(n, k),$$

and we define the *group of similitudes of β* to be the group

$$GO(n, k, \beta) = \{A \in M(n, k) \mid \beta(Ax, Ay) = \alpha\beta(x, y), \alpha \in k^*\}.$$

We note that

$$GO(n, k, \beta) = \{A \in M(n, k) \mid A^T M A = \alpha M, \alpha \in k^*\}.$$

We say two $n \times n$ matrices A and B are considered *congruent* over k if there exists $Q \in GL(n, k)$ such that $Q^T A Q = B$. We also say that A and B are *congruent* via Q.

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

1. Symmetric matrices are congruent to diagonal matrices when $\text{char}(k) \neq 2$, where the entries of the diagonal matrix are are representatives of the cosets of $k^*/(k^*)^2$.

2. If β_1 and β_2 correspond to M_1 and M_2, then $SO(n, k, \beta_1)$ and $SO(n, k, \beta_2)$ are isomorphic via

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

for some $Q \in GL(n, k)$ if and only if $Q^T M_1 Q = M_2$ (M_1 and M_2 are congruent via Q).

So, we will assume that β is such that M is diagonal. Then, to classify the k-involutions of an orthogonal group where M is not diagonal, one can apply the characterization that will follow by simply using the isomorphism Φ given above.

We say 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 k-involutions of $SO(n, k, \beta)$.

Lastly, we will always assume, whether stated or not, that $n > 2$ and that $\text{char}(k) \neq 2$.

3. k-automorphisms of $\mathrm{SO}(n, k, \beta)$

In this paper, we consider the k-involutions that lie in the group $\mathrm{Inn}(\mathrm{GL}(n, \overline{k}), \mathrm{SO}(n, k, \beta))$. When n is odd, this group turns out to be $\mathrm{Inn}(\mathrm{SO}(n, \overline{k}, \beta), \mathrm{SO}(n, k, \beta))$, and when n is even, this group turns out to be $\mathrm{Inn}(\mathrm{O}(n, \overline{k}, \beta), \mathrm{SO}(n, k, \beta))$. We will see that when n is odd and $n \neq 3$, that all of the k-involutions of $\mathrm{SO}(n, k, \beta)$ will be inner k-involutions of $\mathrm{SO}(n, k, \beta)$ over $\mathrm{SO}(n, \overline{k}, \beta)$, and when n is even and $n \neq 4, 6, 8,$, that all of the k-involutions of $\mathrm{SO}(n, k, \beta)$ will be inner k-involutions of $\mathrm{SO}(n, k, \beta)$ over $\mathrm{O}(n, \overline{k}, \beta)$. We will show isomorphy conditions of these k-involutions over $\mathrm{SO}(n, k, \beta)$ when n is odd, and over $\mathrm{O}(n, k, \beta)$ when n is even.

It follows from a proposition on page 191 of [Bor91] that the outer k-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 $m \geq 2$, then this Dynkin diagram is B_m which has only the trivial diagram automorphism. Thus, there are no outer k-automorphisms of $\mathrm{SO}(n, \overline{k}, \beta)$ when n is odd and $n \geq 5$. If $n = 2m$ and $m \geq 4$, then this Dynkin diagram is D_m. The group of automorphisms of this Dynkin diagram is $\mathbb{Z}_2$ when $m > 4$. So, when n is even and $n \geq 10$, $\mathrm{Out}(\mathrm{SO}(n, \overline{k}, \beta)) = \mathbb{Z}_2$. The outer k-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 k-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 k-automorphism of $\mathrm{SO}(n, \overline{k}, \beta)$. Thus, the characterizations that follow in this paper consider all k-automorphisms and k-involutions of $\mathrm{SO}(n, k, \beta)$, assuming that $n \neq 3, 4, 6, 8$. In the cases where $n = 3, 4, 6, 8$, the results that follow only consider the k-automorphisms and k-involutions that can be written as Inn_A for some $A \in \mathrm{GL}(n, \overline{k})$.

We now examine which k-automorphisms will act as the identity on $\mathrm{SO}(n, k, \beta)$. This will prove to be useful when we classify matrix representatives for k-automorphisms.

Lemma 3.1.   *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 $1 \leq r < s \leq n$, let X_{rs} be the diagonal matrix with all 1's, except 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 $\text{SO}(n, k, \beta)$, then we can show that A is a multiple of the identity.

Definition 3.2.   Let k be a field and suppose β is a bilinear form on k^n such that it has matrix representation M, where M is diagonal with diagonal entries $m_1, \ldots, m_n$, which are representatives in k^* of cosets of $k^*/(k^*)^2$. If for each pair m_s and m_t, $x^2 + \frac{m_s}{m_t}y^2 = 1$ has a solution (x, y) such that $y \neq 0$, then we call $\text{SO}(n, k, \beta)$ a *friendly orthogonal group*.

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

Lemma 3.3.   *Assume $n > 2$. Suppose $\text{SO}(n, k, \beta)$ is a friendly orthogonal group. Let $A \in \text{GL}(n, \overline{k})$. Then, Inn_A is the identity on $\text{SO}(n, k, \beta)$ 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. Let m_i represent the ith diagonal entry of M. Then, there exists $a, b \in k$ where $b \neq 0$ such that $a^2 + \frac{m_s}{m_t}b^2 = 1$. For $1 \leq i < j \leq n$, let

$$
Y_{st} = \begin{pmatrix}
1 & 0 & \cdots & & & & & & & \cdots & 0 \\
0 & 1 & & & & & & & & & \vdots \\
\vdots & & \ddots & & & & & & & & \\
& & & 1 & & & & & & & \\
& & & & a & 0 & \cdots & 0 & b & & \\
& & & & 0 & 1 & & & 0 & & \\
& & & & \vdots & & \ddots & & \vdots & & \\
& & & & 0 & & & 1 & 0 & & \\
& & & & -\frac{m_s}{m_t}b & 0 & \cdots & 0 & a & & \\
& & & & & & & & & 1 & \vdots \\
\vdots & & & & & & & & & \ddots & 0 \\
0 & \cdots & & & & & & & \cdots & 0 & 1
\end{pmatrix},
$$

where the noteworthy entries occur in the sth and tth rows and columns. It is a simple calculation to show that $Y_{st}^T M Y_{st} = M$, and that $\det(Y_{st}) = 1$. So, $Y_{st} \in \text{SO}(n, k, \beta)$. Then, we know that $AY_{st} = Y_{st}A$. By comparing both sides of this equality and inspecting the (s, t) entry, we see that $ba_t = ba_s$. Since we are assuming that $b \neq 0$, then it follows that $a_t = a_s$. Since we can repeat this for all s and t, then it is clear that A is a multiple of the identity.   ∎

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

Lemma 3.4.   *1. If* $\mathrm{char}(k) \neq 2, 3$*, then* $\mathrm{SO}(n, k, \beta)$ *is a friendly orthogonal group.*

2. *If* $M = \begin{pmatrix} m_1 & & & \\ & m_2 & & \\ & & \ddots & \\ & & & m_n \end{pmatrix}$ *is such that* $m_s \neq -m_t$ *whenever* $s \neq t$ *and* $\mathrm{char}(k) \neq 2$*, then* $\mathrm{SO}(n, k, \beta)$ *is a friendly orthogonal group.*

3. *If* $\mathrm{char}(k) = 3$*,* i *is a fixed square root of* -1*, and* $i \in k$*, then* $\mathrm{SO}(n, k, \beta)$ *is a friendly group. (So, if* k *contains* $\mathbb{F}_3[i] = \mathbb{F}_9$*, then* $\mathrm{SO}(n, k, \beta)$ *is a friendly 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 $x^2 + \frac{m_s}{m_t} y^2 = 1$ will always have a solution in k if $\mathrm{char}(k) \neq 2, 3$, and also when $\frac{m_s}{m_t} \neq -1$ and $\mathrm{char}(k) \neq 2$.

    Suppose $\mathrm{char}(k) = 3$, and let i be a fixed square root of -1. If $i \in k$, then $1 = x^2 - y^2$ has the solution $(0, i)$, which proves the third case. ∎

    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 3.5.   Suppose $k = \mathbb{F}_3$ and that β is such that $M = \begin{pmatrix} I_{n-1} & 0 \\ 0 & -1 \end{pmatrix}$. 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 $y \neq 0$.

    For the remainder of the paper, we will assume that all orthogonal groups are friendly.

    Fix a bilinear form β with matrix M. If $A \in \mathrm{GL}(n, k)$ is a matrix such $M^{-1}A^T M A = \alpha I_n$, then
$$A \in \mathrm{GO}(n, k, \beta) = \{A \in \mathrm{M}(n, k) \mid \beta(Ax, Ay) = \alpha\beta(x, y), \alpha \in k\},$$
the group of similitudes of β.

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

Lemma 3.6.   *Assume* $n > 2$*. 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* $A \in \mathrm{GO}(n, \overline{k}, \beta)$*,* $A = p\widetilde{A}$ *where* $p \in \overline{k}$*, and*

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

2. $\widetilde{A} \in \mathrm{O}(n, \overline{k}, \beta)$ *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, $A^{-1}XA \in \mathrm{SO}(n, k, \beta)$. So,

$$
\begin{aligned}
I &= (A^{-1}XA)^{-1}A^{-1}XA \\
&= M^{-1}(A^{-1}XA)^{T}MA^{-1}XA \\
&= M^{-1}A^{T}X^{T}(A^{-1})^{T}MA^{-1}XA.
\end{aligned}
$$

This implies that

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

which means

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

We can rewrite this as

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

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

$$
\begin{aligned}
X &= M^{-1}(A^{-1})^{T}MA^{-1}XAM^{-1}A^{T}M \\
&= (AM^{-1}A^{T}M)^{-1}X(AM^{-1}A^{T}M).
\end{aligned}
$$

By Lemma 3.3, it follows that $(AM^{-1}A^{T}M) = \alpha I$ for some $\alpha \in \overline{k}^{*}$. Thus, $A \in \mathrm{GO}(n, \overline{k}, \beta)$. Choose $p \in \overline{k}$ such that $p^{2} = \alpha$. 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. ∎

In the following theorem which completes the characterization of k- automorphisms on $\mathrm{SO}(n, k, \beta)$, we see that we can choose the entries of A to be in k or a quadratic extension of k. For the remainder of this paper, we will use $\sqrt{\alpha}$ to denote a fixed square root of $\alpha \in k^{*}$.

Theorem 3.7. *Assume $n > 2$.*

1. *If n is odd and A is in $\mathrm{SO}(n, \overline{k}, \beta)$, then Inn_{A} keeps $\mathrm{SO}(n, k, \beta)$ invariant if and only if we can choose $\widetilde{A} \in \mathrm{SO}(n, k, \beta)$ such that $\mathrm{Inn}_{\widetilde{A}} = \mathrm{Inn}_{A}$.*

2. *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 $B \in \mathrm{GO}(n, k, \beta)$ such that $B = pA$. 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 $O(n, \overline{k}, \beta)$ such that Inn_A keeps $SO(n, k, \beta)$ invariant. Let a_{ij} be the (i, j) entry of A. We break the proof into steps. At the beginning of each step, we state what we shall prove in that step.

Step One: $a_{ri}a_{rj} + a_{si}a_{sj} \in k$ for all i, j, r, s.

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 $X_{rs} \in O(n, k, \beta)$. If n is even, then $X_{rs} \in SO(n, k, \beta)$. If n is odd, then $-X_{rs} \in SO(n, k, \beta)$. So, we know that $\text{Inn}_A(X_{rs})$ or $-\text{Inn}_A(X_{rs})$ must lie in $SO(n, k, \beta)$. It is also clear that $\text{Inn}_A(I) \in SO(n, k, \beta)$. So, both $\text{Inn}_A(X_{rs})$ and $\text{Inn}_A(I)$ have entries in k. Let us examine the entries of $\text{Inn}_A(X_{rs})$:

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

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

$$= \left(a_{ri}a_{rj} + a_{si}a_{sj} - \sum_{l \neq r,s} a_{li}a_{lj} \right)_{(i,j)}.$$

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

Step Two: $a_{ri}a_{rj} \in k$ for all i, j, r.

Choose integer t distinct from r and s such that $1 \leq t \leq n$. We have that

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

which means that

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

for all i, j, r.

Step Three: $a_{ir}a_{jr} \in k$ for all i, j, r.

Now, we consider the bilinear form β_1 which has matrix M^{-1} (using the standard basis for k^n). We know that $X \in SO(n, \overline{k}, \beta)$ 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 also 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 a k-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 $\mathrm{SO}(n,k,\beta)$. The inverse-transpose of $\mathrm{Inn}_{A^T}(Y)$ is $A(Y^{-1})^T A^{-1} = \mathrm{Inn}_{A^{-1}}((Y^{-1})^T) = (\mathrm{Inn}_A)^{-1}((Y^{-1})^T)$. This proves our claim.

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

Step Four: $a_{si}a_{tj} - a_{ti}a_{sj} \in k$, for all i,j,s,t.

We now recall the matrices $Y_{st} \in \mathrm{SO}(n,k,\beta)$ from the proof of Lemma 3.3. So, it must be the case that $\mathrm{Inn}_A(Y_{st}) \in \mathrm{SO}(n,k,\beta)$. Let us examine the entries of $\mathrm{Inn}_A(Y_{st})$:

$$
\begin{aligned}
\mathrm{Inn}_A(Y_{st}) &= A^{-1}Y_{st}A \\
&= (M^{-1}A^T)(MY_{st}A)
\end{aligned}
$$

$$
= \begin{pmatrix} \frac{a_{11}}{m_1} & \cdots & \frac{a_{n1}}{m_1} \\ \vdots & \ddots & \vdots \\ \frac{a_{1n}}{m_n} & \cdots & \frac{a_{nn}}{m_n} \end{pmatrix}
\begin{pmatrix}
m_1 a_{11} & \cdots & m_1 a_{1n} \\
\vdots & & \vdots \\
m_{s-1}a_{s-1,1} & \cdots & m_{s-1}a_{s-1,n} \\
am_s a_{s1} + bm_s a_{t1} & \cdots & am_s a_{sn} + bm_s a_{tn} \\
m_{s+1}a_{s+1,1} & \cdots & m_{s+1}a_{s+1,n} \\
\vdots & & \vdots \\
m_{t-1}a_{t-1,1} & \cdots & m_{t-1}a_{t-1,n} \\
-bm_t a_{s1} + am_t a_{t1} & \cdots & -bm_t a_{sn} + am_t a_{tn} \\
m_{t+1}a_{t+1,1} & \cdots & m_{t+1}a_{t+1,n} \\
\vdots & & \vdots \\
m_n a_{n1} & \cdots & m_n a_{nn}
\end{pmatrix}
$$

$$
= \left(a_{si}(aa_{sj} + ba_{tj}) + a_{ti}(-ba_{sj} + aa_{tj}) + \sum_{l \neq s,t} a_{li}a_{lj} \right)_{(i,j)}.
$$

Since each of the matrix entries of $\mathrm{Inn}_A(Y_{ij})$ must lie in k and we also know that $a_{li}a_{lj} \in k$ for $1 \leq l \leq n$ from Step Two, then it follows that

$$
a_{si}(aa_{sj} + ba_{tj}) + a_{ti}(-ba_{sj} + aa_{tj})
$$
$$
= a(a_{si}a_{sj}) + b(a_{si}a_{tj}) - b(a_{ti}a_{sj}) + a(a_{ti}a_{tj}) \in k.
$$

We know $b \in k$, and that $a_{si}a_{sj}$ and $a_{ti}a_{tj} \in k$ by Step Two. So, we see that $a_{si}a_{tj} - a_{ti}a_{sj} \in k$, for all i,j,s,t.

Step Five: $a_{si}a_{tj} \in k$ for all i,j,s,t.

Substep Five A : $a_{si}(a_{si}a_{tj} - a_{ti}a_{sj}) = ca_{si}$ for $c \in k$.

If both a_{si} and $a_{tj} \in k$, then $a_{is}a_{jt} \in k$ is clear. So, we will assume $a_{tj} \notin k$. We will also assume that $a_{si} \neq 0$, since if $a_{si} = 0$, then it is again clear that $a_{si}a_{tj} \in k$.

From Step Four, we know that

$$a_{si}a_{tj} - a_{ti}a_{sj} \in k.$$

It follows that

$$a_{si}(a_{si}a_{tj} - a_{ti}a_{sj}) \in k[a_{si}].$$

Let $c = a_{si}a_{tj} - a_{ti}a_{sj}$. Then, we have $a_{si}(a_{si}a_{tj} - a_{ti}a_{sj}) = ca_{si}$ for $c \in k$.

Substep Five B : $a_{si}(a_{si}a_{tj} - a_{ti}a_{sj}) = da_{tj}$ for $d \in k$.

We now consider $a_{si}(a_{si}a_{tj} - a_{ti}a_{sj}) = a_{si}^2 a_{tj} - a_{si}a_{sj}a_{ti}$ in a different fashion. From Step Two, we know that $a_{ti}a_{tj} \in k$. Also recall that we are assuming $a_{tj} \notin k$. Since Step Two also tells us that $a_{tj}^2 \in k$, then it follows that a_{ti} and a_{tj} must lie in the same coset of $k^*/(k^*)^2$. So, there exists $p \in k$ such that $a_{ti} = pa_{tj}$. From these observations, we see that

$$a_{si}(a_{si}a_{tj} - a_{ti}a_{sj}) = (a_{si}^2 - a_{si}a_{sj}p)a_{tj}.$$

From Step Two, we know that $a_{si}^2, a_{si}a_{sj} \in k$. Let $d = a_{si}a_{tj} - a_{ti}a_{sj}$, and note that $d \in k$. We have just shown that $a_{si}(a_{si}a_{tj} - a_{ti}a_{sj}) = da_{tj}$ for $d \in k$.

Substep Five C: $a_{si}a_{tj} \in k$ for all i, j, s, t.

Combining Substeps Five A and B, we see that $ca_{si} = da_{tj}$ for some $c, d \in k$. We prove this step by considering the two cases where $c \neq 0$ and $c = 0$.

If $c \neq 0$, then $d \neq 0$. Further, we have that $a_{si} = \frac{d}{c}a_{tj}$. From this, we see that $a_{si}a_{tj} = \frac{d}{c}a_{tj}^2$. Since $\frac{d}{c} \in k$ by assumption and a_{tj}^2 by Step Two, then we have that $a_{si}a_{tj} \in k$.

Alternatively, if $c = 0$, then since $c = a_{si}a_{tj} - a_{ti}a_s$, we know that $a_{si}a_{tj} = a_{ti}a_{sj}$. Recall that in Substep Five B that $a_{ti} = pa_{tj}$ for $p \in k$. Combining these facts, we have that

$$a_{si}a_{tj} = a_{ti}a_{sj} = pa_{tj}a_{sj}.$$

By Step Three, we know that $a_{tj}a_{sj} \in k$. So, it follows that $a_{si}a_{tj} \in k$.

Step Six: $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$ for some $\alpha \in k$.

From Step Five, it is clear that $k[a_{si}] = k[a_{tj}]$ for all i, j, s, t (assuming that a_{is} and a_{jt} are both nonzero). Fix a nonzero entry a_{si} of A. Let $\alpha = a_{is}^2$ and denote a_{si} as $\sqrt{\alpha}$. 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.

Step Seven: If n is odd, then $A \in \mathrm{SO}(n, k, \beta)$.

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 $A \in \mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$ where $\sqrt{\alpha} \notin k$. From Step Six 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, then $A \in \mathrm{SO}(n, k, \beta)$. ∎

4. k-involutions of $\mathrm{SO}(n, k, \beta)$

We now begin to focus on k-involutions and their characterization, as well as the characterization of their isomorphy classes. We will distinguish different types of k-involutions. First, we note that for some k-involutions, ϕ, there exists $A \in \mathrm{O}(n, k, \beta)$ such that $\phi = \mathrm{Inn}_A$, but not in all cases. Sometimes we must settle for $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta) \setminus \mathrm{O}(n, k, \beta)$ where each entry of A is a k-multiple of $\sqrt{\alpha}$.

This is not the only way in which we can distinguish between different types of k-involutions. If Inn_A is a k-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 k-involutions by seeing if $A^2 = I$ or $A^2 = -I$. This gives the four types of k-involutions, which are outlined in Table 1. It follows from our characterization of k-automorphisms

Table 1: The various possible types of k-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

that when n is odd, that Type 2 and Type 4 k-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 k-involutions can also only occur when n is even.

In the following theorem, we show that an isomorphy class of k-involutions will lie neatly into exactly one of these types of k-involutions. First we need a lemma with a condition equivalent to isomorphism over $\mathrm{O}(n, k, \beta)$.

Lemma 4.1. *Assume* Inn_A *and* Inn_B *are* k-*involutions of* $\mathrm{SO}(n, k, \beta)$ *where* A *lies in* $\mathrm{O}(n, k, \beta)$ *or in* $\mathrm{O}(n, k[\sqrt{\alpha}], \beta)$ *and each entry of* A *is a* k-*multiple of* $\sqrt{\alpha}$, *and likewise for* B. *Then,* Inn_A *and* Inn_B *are isomorphic over* $\mathrm{O}(n, k, \beta)$ *(or* $\mathrm{SO}(n, k, \beta)$*) if and only if there exists* $Q \in \mathrm{O}(n, k, \beta)$ *(or* $\mathrm{SO}(n, k, \beta)$*) such that* $Q^{-1}AQ = B$ *or* $-B$.

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

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

So, $\mathrm{Inn}_Q \mathrm{Inn}_A \mathrm{Inn}_{Q^{-1}} = \mathrm{Inn}_B$. That is, Inn_A and Inn_B are isomorphic over $\mathrm{O}(n,k,\beta)$ (or $\mathrm{SO}(n,k,\beta)$).

To prove the converse, we now assume that Inn_A and Inn_B are isomorphic over $\mathrm{O}(n,k,\beta)$ (or $\mathrm{SO}(n,k,\beta)$). So, there exists $Q \in \mathrm{O}(n,k,\beta)$ (or $\mathrm{SO}(n,k,\beta)$) such that $\mathrm{Inn}_Q \mathrm{Inn}_A \mathrm{Inn}_{Q^{-1}} = \mathrm{Inn}_B$. Thus, for all $U \in \mathrm{SO}(n,k,\beta)$, we have

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

which implies

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

So, $Q^{-1}AQB^{-1}$ commutes with all elements of $\mathrm{SO}(n,k,\beta)$. The center of $\mathrm{SO}(n,k,\beta)$ is $\{I\}$ if n is odd and $\{I,-I\}$ if n is even. So, $Q^{-1}AQ = B$ or $-B$. ∎

Theorem 4.2. *Assume Inn_A and Inn_B are k-involutions of $\mathrm{SO}(n,k,\beta)$ where A lies in $\mathrm{O}(n,k,\beta)$ or in $\mathrm{O}(n,k[\sqrt{\alpha}],\beta)$ and each entry of A is a k-multiple of $\sqrt{\alpha}$, and likewise for B. If Inn_A and Inn_B are isomorphic over $\mathrm{O}(n,k,\beta)$, then they must be k-involutions of the same type.*

Proof. Assume Inn_A and Inn_B are isomorphic over $\mathrm{O}(n,k,\beta)$. By Lemma 4.1 we can assume there exists $Q \in \mathrm{O}(n,k,\beta)$ such that $Q^{-1}AQ = B$ or $-B$. This implies that

1. $A \in \mathrm{O}(n,k,\beta)$ if and only if $B \in \mathrm{O}(n,k,\beta)$; and

2. $A^2 = I$ if and only if $B^2 = I$.

Thus, Inn_A and Inn_B must be of the same type. ∎

We introduce the notation $E(A,\lambda)$ to refer to the eigenspace of a matrix A corresponding to eigenvalue λ, where we assume the vectors lie in $\overline{k}^n$. In practice, we will be concerned with basis vectors that lie either in k, or a particular quadratic extension of k.

4.1. Type 1 k-involutions.
We now find a structured form for the matrices of all types of k-involutions. We begin with Type 1 k-involutions. When n is odd, these are the only k-involutions.

Lemma 4.3. *Suppose θ is a Type 1 k-involution of $\mathrm{SO}(n,k,\beta)$. Then, there exists $A \in \mathrm{O}(n,k,\beta)$ such that $A = X \left(\begin{smallmatrix} -I_s & 0 \\ 0 & I_t \end{smallmatrix} \right) X^{-1}$ where $s+t=n$, $s \le t$, 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 $X^T M X$ is diagonal.

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 want to construct bases for $E(A,1)$ and $E(A,-1)$ such that all the basis

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 k-involution.) Let $\{z_1, \ldots, z_n\}$ 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, $\{u_1, \ldots, u_n\}$ 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 $y_1, \ldots, y_s$. We can similarly form a basis for $E(A, 1)$. We shall call these vectors $y_{s+1}, \ldots, y_n$. Let Y be the matrix with the vectors $y_1, \ldots, y_n$ 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

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

So, $Y^T MY = \begin{pmatrix} Y_1 & 0 \\ 0 & Y_2 \end{pmatrix}$, 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 $N^T Y^T MY N$ 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 $X^T MX$ is diagonal. It follows from this last observation that the column vectors of X must be orthogonal with respect to β. ∎

Now we show conditions equivalent to isomorphy. Note that we say two matrices are A and B are *congruent* over a group G if there exists $Q \in G$ such that $Q^{-1}AQ = B$.

Theorem 4.4.   *Suppose θ and ϕ are two Type 1 k-involutions of $SO(n, k, \beta)$ where $\theta = \mathrm{Inn}_A$ and $\phi = \mathrm{Inn}_B$. 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 $m_A, m_B \leq \frac{n}{2}$, and*

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

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

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

The following are equivalent:

1. *θ is isomorphic to ϕ over $SO(n, k, \beta)$.*

2. *A is conjugate to B or $-B$ over $SO(n, k, \beta)$.*

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

4. *θ is isomorphic to ϕ over $O(n, k, \beta)$.*

5. *A is conjugate to B or $-B$ over $O(n, k, \beta)$.*

Proof.   The equivalence of (i) and (ii) follows from Lemma 4.1, as does the equivalence of (iv) and (v).

Next we show that (ii) implies (iii). First suppose that $Q^{-1}AQ = B$ for some $Q \in SO(n, k, \beta)$. $Q^{-1}AQ = B$ 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 $m_A = m_B$. Let $m = m_A = m_B$, and recall from Theorem 2.2 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
$$R_1 \in \mathrm{GL}(m,k) \text{ and } R_2 \in \mathrm{GL}(n-m,k).$$
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 $Q^T M Q = M$.

So,

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

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

Now suppose that $Q^{-1} A Q = -B$ 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 $m_A, m_B \le \frac{n}{2}$, then it follows that $m_A = m_B = \frac{n}{2}$. Rearranging the previous equation, we have
$$I_{\frac{n}{2},\frac{n}{2}} X^{-1} Q Y = X^{-1} Q Y I_{\frac{n}{2},\frac{n}{2}},$$

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 $Q^T M Q = M$.

So,

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

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 we 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 $Y^T M Y = R^T (X^T M X) R$. Let $Q = X R Y^{-1}$. We will now show that $Q^{-1} A Q = B$ and that $Q \in \mathrm{SO}(n,k,\beta)$.

$$Q^{-1} A Q = (X R Y^{-1})^{-1} A (X R Y^{-1})$$
$$= Y R^{-1} X^{-1} A X R Y^{-1}$$
$$= Y R^{-1} (-I_{m,n-m}) R Y^{-1}$$
$$= Y(-I_{m,n-m}) Y^{-1} = B.$$

Next, we must show that $Q \in \mathrm{SO}(n,k,\beta)$. We first show that $Q^T M Q = M$.

Recall that $Y^T M Y = R^T (X^T M X) R$. So,

$$\begin{aligned} Q^T M Q &= (XRY^{-1})^T M (XRY^{-1}) \\ &= (Y^{-1})^T (R^T X^T M X R) Y^{-1} \\ &= (Y^{-1})^T (Y^T M Y) Y^{-1} \\ &= M. \end{aligned}$$

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 $Q^{-1} A Q = B$ and $Q^T M Q = M$. 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 $R = \left(\begin{smallmatrix} 0 & R_1 \\ R_2 & 0 \end{smallmatrix} \right)$, then we can let $Q = XRY^{-1}$ and get that $Q^{-1} A Q = -B$ 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 (ii) implies (iii). Thus, all the conditions are equivalent. ∎

We 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 k-involutions. We will show in an explicit example that this does not occur in the Type 2 case. For the remaining three types of k-involutions, we will only find conditions for isomorphy over $\mathrm{O}(n, k, \beta)$. Again, recall that these three Types of k-involutions only occur when n is even. So, when n is odd, we have conditions on the matrices A and B that are equivalent to isomorphy of Inn_A and Inn_B over $\mathrm{SO}(n, k, \beta)$.

4.2. Type 2 k-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 4.5. *Suppose $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta) \setminus \mathrm{O}(n, k, \beta)$ induces a Type 2 k-involution of $\mathrm{SO}(n, k, \beta)$ where $\sqrt{\alpha} \notin k$. Recall that the entries of A are all k-multiples of $\sqrt{\alpha}$. Then, for $x, y \in k^n$, $x + \sqrt{\alpha} y \in E(A, -1)$ if and only if $x - \sqrt{\alpha} y \in E(A, 1)$. Further, $\dim(E(A, 1)) = \dim(E(A, -1))$.*

Proof. Suppose $a, b \in k$. Then, we refer to the Galois automorphism of the field $k[\sqrt{\alpha}]$ over k that sends $a + \sqrt{\alpha} b$ to $a - \sqrt{\alpha} b$ as "$\sqrt{\alpha}$-conjugation." Since this mapping is an automorphism, it must preserve multiplication. Further, for a matrix $X = Y + \sqrt{\alpha} Z$ for Y, Z with entries in k, we say that $Y - \sqrt{\alpha} Z$ is the "$\sqrt{\alpha}$-conjugate" of X. We note that this mapping will preserve multiplication of matrices.

Assume $x, y \in k^n$, such that $x + \sqrt{\alpha} y \in E(A, -1)$. Since

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

then the "$\sqrt{\alpha}$-conjugate" is

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

We note that the "$\sqrt{\alpha}$-conjugate" of A is $-A$ because each entry of A is a k-multiple of $\sqrt{\alpha}$. We can multiply both side by -1 to see

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

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

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

We are now able to characterize the Type 2 k-involutions.

Lemma 4.6. *Suppose θ is a Type 2 k-involution of $\mathrm{SO}(n, k, \beta)$. Let A be an orthogonal matrix in $\mathrm{O}(n, k[\sqrt{\alpha}], \beta)$ such that $\theta = \mathrm{Inn}_A$. 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 begin by constructing bases for $E(A, 1)$ and $E(A, -1)$ such that all the basis 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 k-involution to occur.) Since Inn_A is a Type 1 k-involution of $\mathrm{SO}(n, k[\sqrt{\alpha}], \beta)$, then we can apply Lemma 4.3 to find an orthogonal basis $\{x_1 + \sqrt{\alpha}y_1, \ldots, x_{\frac{n}{2}} + \sqrt{\alpha}y_{\frac{n}{2}}\}$ of $E(A, -1)$, where $x_1, \ldots, x_{\frac{n}{2}}, y_1, \ldots, y_{\frac{n}{2}} \in k^n$. By the previous lemma, we know that $\{x_1 - \sqrt{\alpha}y_1, \ldots, x_{\frac{n}{2}} - \sqrt{\alpha}y_{\frac{n}{2}}\}$ 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

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

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 $\{x_1 + \sqrt{\alpha}y_1, \ldots, x_{\frac{n}{2}} + \sqrt{\alpha}y_{\frac{n}{2}}\}$ 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

$$\beta(x_i, x_j) = \alpha\beta(y_i, y_j) \text{ and}$$
$$\beta(x_i, y_j) = \beta(x_j, y_i).$$

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

$$\beta(x_i, y_j) = 0,$$
$$\beta(x_i, x_j) = 0, \text{ and}$$
$$\beta(y_i, y_j) = 0.$$

When $i = j$, we note that

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

Then, we have

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

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

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

Example 4.7.   Assume that β is the standard dot product. Then, Inn_A can be a Type 2 k-involution of $SO(4, \mathbb{Q})$ if A is symmetric and orthogonal (since this will imply that $A^2 = I$), and if the entries of A are all $\mathbb{Q}$-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 a $\mathbb{Q}$-multiple of $\sqrt{3}$, then it is clear that Inn_A is a Type 2 k-involution of $SO(4, \mathbb{Q})$. 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 follows from Lemma 4.5 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 4.8. *Suppose θ and ϕ are two Type 2 k-involutions of $\mathrm{SO}(n, k, \beta)$ where $\theta = \mathrm{Inn}_A$ and $\phi = \mathrm{Inn}_B$. 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

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

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

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

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

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

4. *$k[\sqrt{\alpha}] = k[\sqrt{\gamma}]$ and we can choose X and Y such that 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.   The equivalence of (i) and (ii) follows from Lemma 4.1. 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 γ must be a k-multiple of α. So, $k[\sqrt{\alpha}] = k[\sqrt{\gamma}]$. Without loss of generality, we may assume $\gamma = \alpha$. 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 $Q^T MQ = M$. It follows from these observations that

$$R^T(X^T MX)R = (XR)^T M(XR) = (QY)^T M(QY) = Y^T(Q^T MQ)Y = Y^T MY.$$

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 $k[\sqrt{\alpha}] = k[\sqrt{\gamma}]$, so we may assume without loss of generality that $\alpha = \gamma$, and we can similarly show that $Y^T MY = R^T X^T MXR$ 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 $X^T MX$ is congruent to $Y^T MY$ over $\mathrm{GL}(n, k)$ where $Y^T MY = R^T X^T MXR$ 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

$$\begin{aligned} Q^{-1}AQ &= (XRY^{-1})^{-1}A(XRY^{-1}) \\ &= YR^{-1}(X^{-1}AX)RY^{-1} \\ &= -\frac{\sqrt{\alpha}}{\alpha}YR^{-1} \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix} RY^{-1} \\ &= -\frac{\sqrt{\alpha}}{\alpha}Y \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix} R^{-1}RY^{-1} \\ &= -\frac{\sqrt{\alpha}}{\alpha}Y \begin{pmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{pmatrix} Y^{-1} = B. \end{aligned}$$

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, we must show $Q^T MQ = M$.

This follows because

$$
\begin{aligned}
Q^T M Q &= (XRY^{-1})^T M (XRY^{-1}) \\
&= (Y^{-1})^T (R^T X^T M X R) Y^{-1} \\
&= (Y^{-1})^T (Y^T M Y) Y^{-1} = M.
\end{aligned}
$$

If we instead assume that $\alpha = \gamma$ and $X^T M X$ is congruent to $Y^T M Y$ over $\mathrm{GL}(n, k)$ where $Y^T M Y = R^T X^T M X R$ for $R = \left(\begin{smallmatrix} R_1 & R_2 \\ -\alpha R_2 & -R_1 \end{smallmatrix} \right)$, where $R_1, R_2 \in \mathrm{GL}(\frac{n}{2}, k)$, then if we let $Q = XRY^{-1}$, we can similarly show that $Q^{-1} A Q = -B$ 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 isomorphy of k-involutions over $\mathrm{SO}(n, k, \beta)$, but the Type 2 case gave us isomorphy of k-involutions over $\mathrm{O}(n, k, \beta)$. In the following example, we give an example that shows that isomorphy over $\mathrm{O}(n, k, \beta)$ is not the same as isomorphy over $\mathrm{SO}(n, k, \beta)$ for Type 2 k-involutions.

Example 4.9. Consider the group $\mathrm{SO}(4, \mathbb{F}_3)$. That is, consider the case where k is the field of three elements, and the bilinear form is the standard dot product. Let i denote a fixed square root of $2 = -1$. A Type 2 k-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

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

We also see that

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

where $X_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)$ and $X_2 = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix} \right)$.

Now, we also consider the Type 2 k-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 k-involutions are congruent over $O(4, \mathbb{F}_3)$. First, we consider the matrix

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

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

Secondly, if we let $R = \begin{pmatrix} R_1 & R_2 \\ 2R_2 & R_1 \end{pmatrix} \in GL(4, \mathbb{F}_3)$ 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 now show that there does not exist $W \in SO(4, \mathbb{F}_3)$ such that $B = W^{-1}AW$. We proceed by contradiction and suppose that there does exist such an W. It then follows that A and $QW^{-1} \in O(4, \mathbb{F}_3)$ 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

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

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 $O(4, \mathbb{F}_3)$ which commute with A are also members of $SO(4, \mathbb{F}_3)$, which contradicts

$QW^{-1} \in O(4, \mathbb{F}_3) \setminus SO(4, \mathbb{F}_3)$ commuting with A. So, no such $W \in SO(4, \mathbb{F}_3)$ can exist, which means we cannot strengthen the above theorem by replacing $O(n, k, \beta)$ with $SO(n, k, \beta)$ in conditions (i) and (ii).

Theorem 4.10. *Suppose Inn_A and Inn_B are both Type 2 k-involutions of $SO(n, k, \beta)$. Then, Inn_A and Inn_B are isomorphic over $O(n, k, \beta)$ if and only if they are isomorphic over $SO(n, k[\sqrt{\alpha}], \beta)$.*

Proof. When viewed as Type 2 k-involutions of $SO(n, k, \beta)$, 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 k-involutions of $SO(n, k[\sqrt{\alpha}], \beta)$, then they are Type 1 k-involutions. Further, we can choose X and $Y \in GL(n, k[\sqrt{\alpha}])$ 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 $SO(n, k[\sqrt{\alpha}], \beta)$, 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 $SO(n, k[\sqrt{\alpha}], \beta)$ as Type 1 k-involutions. Then, from Theorem 4.4 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. ∎

4.3. Type 3 k-involutions.

We now examine the Type 3 case. Recall that ϕ is a Type 3 k-involution if $\phi = \mathrm{Inn}_A$, where $A \in \mathrm{O}(n, k, \beta)$ and $A^2 = -I$. Such matrices have eigenvalues $\pm i$, where i is a fixed square root of -1, and are diagonalizable because the minimal polynomial has no repeated roots. We are now able to prove results that characterize the matrices that induce Type 3 k-involutions, and then use these characterizations to find conditions on these k-involutions that are equivalent to isomorphy. We will have to prove our result by looking at separate cases, depending on whether or not i lies in k. We begin by assuming that $i \in k$.

Lemma 4.11.   *Assume $i \in k$ and suppose $\theta = \mathrm{Inn}_A$ is a Type 3 k-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 first show that there are bases for $E(A, -i)$ and $E(A, i)$ that lie in k^n. Let $\{z_1, \ldots, z_n\}$ 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, $\{u_1, \ldots, u_n\}$ must span $E(A, -i)$. Thus, we can appropriately choose $m = \dim(E(A, -i))$ of these vectors and form a basis for $E(A, -i)$. Note that each of these vectors lies in k^n since $i \in k$. Label these basis vectors as $v_1, \ldots, v_m$, and renumber the z_j's so that we can write $v_j = z_j + iAz_j$.

Let $v_j' = z_j - iAz_j$ for $j = 1, \ldots, m$. We can show that these vectors are linearly independent, and lie in $E(A, i)$. Note that this shows $\dim(E(A, i)) \geq \dim(E(A, -i))$. We can similarly show the reverse inequality, so we have that $\dim(E(A, i)) = \dim(E(A, -i))$, and $m = \frac{n}{2}$.

Next, we will show that we can in fact choose bases $a_1, \ldots, a_{\frac{n}{2}}$ for $E(A, -i) \cap k^n$ and $b_1, \ldots, b_{\frac{n}{2}}$ 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 need to find $a_2 \in F_1 \cap E(A, -i)$. Similar to the beginning of this proof, 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

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

Then, the result follows.   ∎

Theorem 4.12.   *Assume that $i \in k$. Then, if Inn_A and Inn_B are both Type 3 k-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 k-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

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

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

and

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

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 $R = \left(\begin{smallmatrix} R_1 & 0 \\ 0 & R_2 \end{smallmatrix} \right)$ 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 $Q^{-1} A Q = B$. This will then prove that Inn_A and Inn_B lie in the same isomorphy class by Lemma 4.1.

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

$$
\begin{aligned}
Q^T M Q &= (XRY^{-1})^T M (XRY^{-1}) \\
&= (Y^{-1})^T R^T (X^T M X) R Y^{-1} \\
&= (Y^{-1})^T (Y^T M Y) Y^{-1} \\
&= M,
\end{aligned}
$$

which proves this claim.

Lastly, we show that $Q^{-1} A Q = B$. We first note that R and $\left(\begin{smallmatrix} -iI & 0 \\ 0 & iI \end{smallmatrix} \right)$ commute. Then, we see that

$$
\begin{aligned}
Q^{-1} A Q &= (XRY^{-1})^{-1} A (XRY^{-1}) \\
&= Y R^{-1} (X^{-1} A X) R Y^{-1} \\
&= Y R^{-1} \left(\begin{array}{cc} -iI & 0 \\ 0 & iI \end{array} \right) R Y^{-1} \\
&= Y R^{-1} R \left(\begin{array}{cc} -iI & 0 \\ 0 & iI \end{array} \right) Y^{-1} \\
&= Y \left(\begin{array}{cc} -iI & 0 \\ 0 & iI \end{array} \right) Y^{-1} \\
&= B. \qquad \blacksquare
\end{aligned}
$$

We now begin examining the case where $i \notin k$. When i is not in k, then we have the Galois automorphism, Ψ, on $k[i]$ such that $\Psi(a + bi) = a - bi$ for $a, b \in k$. This map extends in a natural way to vectors and matrices with entries in $k[i]$.

We begin by proving a couple or results about the eigenvectors of such matrices.

Lemma 4.13. *Assume $i \notin k$ and suppose $A \in \mathrm{O}(n, k, \beta)$ induces a Type 3 k-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 $u - iv \in E(A, -i)$.*

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 apply the Galois automorphism Ψ to this equality, then we see that

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

This implies

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

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 $u - iv \in E(A, -i)$. ∎

Lemma 4.14.   *Assume $i \notin k$ and suppose $\theta = \mathrm{Inn}_A$ is a Type 3 k-involution of* $\mathrm{SO}(n, k, \beta)$ *where $A \in \mathrm{O}(n, k, \beta)$. Then, we can find $x_1, \ldots, x_{\frac{n}{2}}, y_1, \ldots, y_{\frac{n}{2}} \in k^n$ such that the $x_j + iy_j$ are a basis for $E(A, -i)$ and the $x_j - iy_j$ are a basis for $E(A, i)$. Further, $\dim(E(A, i)) = \dim(E(A, -i))$.*

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 begin by constructing bases for $E(A, i)$ and $E(A, -i)$ such that all the basis vectors lie in $k[i]^n$. Let $\{z_1, \ldots, z_n\}$ 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, $\{u_1, \ldots, u_n\}$ must span $E(A, -i)$. Thus, we can appropriately choose $m = \dim(E(A, -i))$ 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 $v_1, \ldots, v_m$. We can write each of these vectors as $v_j = x_j + iy_j$. By the previous lemma, we know that $x_j - iy_j \in E(A, i)$. It can also be shown that these vectors will are linearly independent. So, $\dim(E(A, i)) \geq \dim(E(A, -i))$. We can similarly show the reverse inequality. Thus, $\dim(E(A, i)) = \frac{n}{2} = \dim(E(A, -i))$, and the $x_j - iy_j$ form a basis for $E(A, i)$. ∎

We can now characterize the matrices that induce Type 3 k-involutions when $i \notin k$.

Lemma 4.15.   *Assume $i \notin k$ and suppose $\theta = \mathrm{Inn}_A$ is a Type 3 k-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 4.14 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 $a_1 + ib_1, \ldots, a_{\frac{n}{2}} + ib_{\frac{n}{2}}$ for $E(A, -i) \cap k[i]^n$ and $a_1 - ib_1, \ldots, a_{\frac{n}{2}} - ib_{\frac{n}{2}}$ 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,

$$\begin{aligned} \beta(x, x) &= \beta(e_j + e_l, e_j + e_l) \\ &= 2\beta(e_j, e_l) \\ &\neq 0. \end{aligned}$$

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

$$\begin{aligned} \beta(a_1 + ib_1, a_1 - ib_1) &= (\beta(a_1, a_1) + \beta(b_1, b_1)) + i(-\beta(a_1, b_1) + \beta(a_1, b_1) \\ &= 2\beta(a_1, a_1) = 2\beta(x, x) \\ &\neq 0. \end{aligned}$$

Let $E_1 = \text{Span}_{k[i]}(a_1 + ib_1, a_1 - ib_1) = \text{Span}_{k[i]}(a_1, b_1)$, 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 $E_2 = \text{Span}_{k[i]}(a_1, a_2, b_1, b_2)$, 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

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

Then, it follows that $U^T M U = \left(\begin{smallmatrix} U_1 & 0 \\ 0 & U_1 \end{smallmatrix} \right)$ 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

$$A = U \left(\begin{array}{cc} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{array} \right) U^{-1}. \qquad \blacksquare$$

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

Example 4.16. Assume that β is the standard dot product. Then, θ can be a Type 3 k-involution of $SO(4, \mathbb{R})$ only if we can choose $A \in O(4, \mathbb{R})$ such that $A^2 = -I$. This means the matrix must satisfy $A^T = -A$. That is, the matrix must be skew-symmetric. Observe that the matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \in O(4, \mathbb{R})$$

is skew-symmetric, so it induces a Type 3 k-involution of $SO(4, \mathbb{R})$. 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 $U^T U = I_4$ and $A = U \begin{pmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{pmatrix} U^{-1}$. Using the notation of Lemma 4.15, we note that $U_1 = I_2$.

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

Theorem 4.17.   *Assume $i \notin k$. Then, if Inn_A and Inn_B are both Type 3 k-involutions of $\mathrm{SO}(n, k, \beta)$, then Inn_A and Inn_B are isomorphic over $\mathrm{O}(n, k, \beta)$.*

Proof.   By the Lemma 4.15, 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 $U^T M U = \begin{pmatrix} U_1 & 0 \\ 0 & U_1 \end{pmatrix}$ is a diagonal matrix.

Let

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

and consider Inn_A and Inn_B as k-involutions of $\mathrm{SO}(n, k[i], \beta)$. By construction, we see that X is a matrix that satisfies the conditions of Lemma 4.11 for the group $\mathrm{SO}(n, k[i], \beta)$. We note that $X_1 = 2U_1$. We also know by Theorem 4.12 that Inn_A and Inn_B are isomorphic (when viewed as k-involutions of $\mathrm{SO}(n, k[i], \beta)$) over $\mathrm{O}(n, k[i], \beta)$. So, we can choose $Q_i \in \mathrm{O}(n, k[i], \beta)$ 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 $1 \le j \le \frac{n}{2}$, the jth and $\frac{n}{2} + j$th columns are i-conjugates of one another.

Also, note that

$$\begin{aligned} Y^{-1} B Y &= (Q_i^{-1} X)^{-1} B (Q_i^{-1} X) \\ &= X^{-1} Q_i B Q_i^{-1} X \\ &= X^{-1} A X \\ &= \begin{pmatrix} -iI_{\frac{n}{2}} & 0 \\ 0 & iI_{\frac{n}{2}} \end{pmatrix}. \end{aligned}$$

Lastly, we see that

$$\begin{aligned} Y^T M Y &= (Q_i^{-1} X)^T M (Q_i^{-1} X) \\ &= X^T ((Q_i^{-1})^T M Q_i) X \\ &= X^T M X \\ &= \begin{pmatrix} 0 & X_1 \\ X_1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 2U_1 \\ 2U_1 & 0 \end{pmatrix}. \end{aligned}$$

We can write

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

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

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

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 $Q^{-1}AQ = B$ and $Q \in \mathrm{O}(n, k, \beta)$. This will prove that Inn_A and Inn_B are isomorphic over $\mathrm{O}(n, k, \beta)$ by Lemma 4.1.

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

$$\begin{aligned} Q^T M Q &= (UV^{-1})^T MUV^{-1} \\ &= (V^{-1})^T (U^T M U) V^{-1} \\ &= (V^{-1})^T (V^T M V) V^{-1} \\ &= M. \end{aligned}$$

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

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

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

Corollary 4.18.   *If* Inn_A *and* Inn_B *are both Type 3 k-involutions of* $\mathrm{SO}(n, k, \beta)$ *where* $A, B \in \mathrm{O}(n, k, \beta)$, *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 k-involutions.*

4.4. Type 4 k-involutions.

We now move on to a similar characterization in the Type 4 case. 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 will then use these characterizations to find conditions on these k-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 $\sqrt{-\alpha} = 1$ and $\sqrt{\alpha} = i$, a fixed square root of -1.

Lemma 4.19.   *Assume* $\sqrt{-\alpha} \in k$ *and suppose* $\theta = \mathrm{Inn}_A$ *is a Type 4 k-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* $X^T M X = \begin{pmatrix} 0 & X_1 \\ X_1 & 0 \end{pmatrix}$, *and* X_1 *is diagonal.*

Proof.   Firstly, we show that there exists bases for for $E(A, -i)$ and $E(A, i)$ that lie in k^n. Let $\{z_1, \ldots, z_n\}$ be a basis for k^n. For each j, let $u_j = (\sqrt{\alpha}A -$

$\sqrt{-\alpha}I)z_j$. Note that $u_j \in k^n$ since $\sqrt{-\alpha} = 1$ and each entry of A is a k-multiple of $\sqrt{\alpha}$. since $\sqrt{-\alpha} = 1$. Further,

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

So, $\{u_1, \ldots, u_n\}$ must span $E(A, -i)$. Thus, we can appropriately choose $m = \dim(E(A, -i))$ of these vectors and form a basis for $E(A, -i)$. Note that each of these vectors lies in k^n. Label these basis vectors as $v_1, \ldots, v_m$. Renumber the z_j's so that we can write $v_j = (\sqrt{\alpha}A - \sqrt{-\alpha}I)z_j$. For $j = 1, \ldots, m$, let $v'_j = (\sqrt{\alpha}A + \sqrt{-\alpha}I)z_j$. We can show that these vectors are linearly independent and lie in $E(A, i)$. Note that this implies $\dim(E(A, i)) \geq \dim(E(A, -i))$. We can similarly show the reverse inequality. So, $\dim(E(A, i)) = \frac{n}{2} = \dim(E(A, -i))$, and the v'_j's form a a basis for $E(A, i)$ in k^n.

We will now show that we can in fact choose bases $a_1, \ldots, a_{\frac{n}{2}}$ for $E(A, -i) \cap k^n$ and $b_1, \ldots, b_{\frac{n}{2}}$ 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 from the beginning of the proof 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 $t \in k^n$ 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 want to find $a_2 \in F_1 \cap E(A, -i)$. Similar to the construction in the above, 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

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

Then, the result follows.   ∎

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

Example 4.20.   Assume that β is the standard dot product and that $k = \mathbb{F}_3$, the field of three elements. So, the square roots of 2 are $\pm i$. In the notation of the previous lemma, note that $\sqrt{-\alpha} = 1$. Observe that the matrix

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

satisfies the relation $A^2 = -I_4$. Since each entry of A is a $\mathbb{F}_3$-multiple of i, then it follows that Inn_A is a k-involution of $\mathrm{SO}(4, \mathbb{F}_3)$ 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

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

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 k-involutions in the case where $\sqrt{-\alpha} \in k$.

Theorem 4.21.   *Assume that $\sqrt{-\alpha} \in k$. Then, if Inn_A and Inn_B are both Type 4 k-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 k-involutions of $\mathrm{SO}(n, k, \beta)$. Let them be represented by matrices $A, B \in \mathrm{O}(n, k, \beta)$. By Lemma 4.19, 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 by Lemma 4.1.

First we show that $Q \in \mathrm{O}(n, k, \beta)$. By construction, the entries of Q lie in k. Also, note that

$$\begin{aligned}
Q^T M Q &= (XRY^{-1})^T M (XRY^{-1}) \\
&= (Y^{-1})^T R^T (X^T M X) R Y^{-1} \\
&= (Y^{-1})^T (Y^T M Y) Y^{-1} \\
&= M,
\end{aligned}$$

which proves $Q \in \mathrm{O}(n, k, \beta)$.

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

$$\begin{aligned}
Q^{-1}AQ &= (XRY^{-1})^{-1} A (XRY^{-1}) \\
&= YR^{-1}(X^{-1}AX)RY^{-1} \\
&= YR^{-1} \begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix} RY^{-1} \\
&= YR^{-1}R \begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix} Y^{-1} \\
&= Y \begin{pmatrix} -iI & 0 \\ 0 & iI \end{pmatrix} Y^{-1} \\
&= B. \qquad \blacksquare
\end{aligned}$$

We now examine the case where $\sqrt{-\alpha} \notin k$. We begin by proving a lemma about the eigenspaces of the matrices that induce these Type 4 k-involutions.

Lemma 4.22.   *Assume $\sqrt{-\alpha} \notin k$ and suppose $\theta = \mathrm{Inn}_A$ is a Type 4 k-involution of $\mathrm{SO}(n, k, \beta)$ where $A \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$. Then, we can find $x_1, \ldots, x_{\frac{n}{2}}$, $y_1, \ldots, y_{\frac{n}{2}} \in k^n$ such that the $x_j + \sqrt{-\alpha} y_j$ are a basis for $E(A, -i)$ and the $x_j - \sqrt{-\alpha} y_j$ are a basis for $E(A, i)$. Further, $\dim(E(A, i)) = \dim(E(A, -i))$.*

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 begin by constructing bases for $E(A, i)$ and $E(A, -i)$ such that all the basis vectors lie in $k[\sqrt{-\alpha}]^n$. Let $\{z_1, \ldots, z_n\}$ be a basis for k^n. For each j, let $u_j = (\sqrt{\alpha} A - \sqrt{-\alpha} I) z_j$. Note that

$$
\begin{aligned}
Au_j &= A(\sqrt{\alpha} A - \sqrt{-\alpha} I) z_j \\
&= (\sqrt{\alpha} A^2 - \sqrt{-\alpha} A) z_j \\
&= -i(\sqrt{\alpha} A - \sqrt{-\alpha} I) z_j \\
&= -i u_j.
\end{aligned}
$$

So, $\{u_1, \ldots, u_n\}$ 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 $k[\sqrt{-\alpha}]^n$. Label these basis vectors as $v_1, \ldots, v_m$. We can write each of these vectors as $v_j = x_j + \sqrt{-\alpha} y_j$. We can similarly show that $v'_j = x_j - \sqrt{-\alpha} y_j \in E(A, i)$, and that the set $v'_1, \ldots, v'_m$ is linearly independent. So, $\dim(E(A, i)) \geq \dim(E(A, -i))$. We can similarly show the reverse inequality. It follows from these observations that $\dim(E(A, i)) = \frac{n}{2} = \dim(E(A, -i))$, and that the v'_j's form a basis for $E(A, i)$ in $k[\sqrt{\alpha}]^n$. ∎

Lemma 4.23.   *Assume $\sqrt{-\alpha} \notin k$ and suppose $\theta = \mathrm{Inn}_A$ is a Type 4 k-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 4.22 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 $a_1 + \sqrt{-\alpha} b_1, \ldots, a_{\frac{n}{2}} + \sqrt{-\alpha} b_{\frac{n}{2}}$ for $E(A, -i) \cap k[i]^n$ and $a_1 - \sqrt{-\alpha} b_1, \ldots, a_{\frac{n}{2}} - \sqrt{-\alpha} b_{\frac{n}{2}}$ 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 thi, 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 $E_1 = \text{Span}_{k[\sqrt{-\alpha}]}(a_1 + \sqrt{-\alpha}b_1, a_1 - \sqrt{-\alpha}b_1) = \text{Span}_{k[\sqrt{-\alpha}]}(a_1, b_1)$, 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 $E_2 = \text{Span}_{k[\sqrt{-\alpha}]}(a_1, a_2, b_1, b_2)$, 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

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

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 k-involution in the case that $\sqrt{-\alpha} \notin k$.

Example 4.24. Assume that β is the standard dot product. Observe that the matrix

$$A = \frac{\sqrt{2}}{2} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ -1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \end{pmatrix} \in O(4, \mathbb{Q}[\sqrt{2}])$$

is such that $A^2 = -I_4$. Since each entry of A is a $\mathbb{Q}$-multiple of $\sqrt{2}$, then it follows that Inn_A is an k-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 $U^T U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}$ 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 k-involutions that are equivalent to isomorphy in the case where $\sqrt{-\alpha} \notin k$.

Theorem 4.25. *Assume $\sqrt{-\alpha} \notin k$. Then, if Inn_A and Inn_B are both Type 4 k-involutions of $\mathrm{SO}(n, k, \beta)$ where $A, B \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$, then Inn_A and Inn_B are isomorphic over $\mathrm{O}(n, k, \beta)$.*

Proof. By Lemma 4.23, 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 k-involutions of $\text{SO}(n, k[\sqrt{-\alpha}], \beta)$. If $k[\sqrt{-\alpha}] = k[\sqrt{\alpha}]$, then these are Type 3 k-involutions of $\text{SO}(n, k[\sqrt{-\alpha}], \beta)$, 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 k-involutions where $\sqrt{-\alpha} \in k[\sqrt{-\alpha}]$.

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

By construction, we see that X is a matrix that satisfies the conditions of Lemma 4.15 or Lemma 4.19 for the group $\text{SO}(n, k[\sqrt{\alpha}], \beta)$. We note that $X_1 = 2U_1$. We also know by Corollary 4.18 or Theorem 4.21 that Inn_A and Inn_B are isomorphic (when viewed as k-involutions of $\text{SO}(n, k[\sqrt{-\alpha}], \beta)$) over $\text{O}(n, k[\sqrt{-\alpha}], \beta)$. So, we can choose $Q_\alpha \in \text{O}(n, k[\sqrt{-\alpha}], \beta)$ 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
$$Y = (c_1 + \sqrt{-\alpha}d_1, \ldots, c_{\frac{n}{2}} + \sqrt{-\alpha}d_{\frac{n}{2}}, c_1 - \sqrt{-\alpha}d_1, \ldots, c_{\frac{n}{2}} - \sqrt{-\alpha}c_{\frac{n}{2}}),$$

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 $1 \leq j \leq \frac{n}{2}$, the jth and $\frac{n}{2} + j$th columns are i-conjugates of one another.

Next, we observe that
$$\begin{aligned} Y^{-1}BY &= (Q_\alpha^{-1}X)^{-1}B(Q_\alpha^{-1}X) \\ &= X^{-1}Q_\alpha B Q_\alpha^{-1}X \\ &= X^{-1}AX \\ &= \begin{pmatrix} -iI_{\frac{n}{2}} & 0 \\ 0 & iI_{\frac{n}{2}} \end{pmatrix}. \end{aligned}$$

Lastly, we see that
$$\begin{aligned} Y^T MY &= (Q_\alpha^{-1}X)^T M(Q_\alpha^{-1}X) \\ &= X^T((Q_\alpha^{-1})^T M Q_\alpha)X \\ &= X^T MX \\ &= \begin{pmatrix} 0 & X_1 \\ X_1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 2U_1 \\ 2U_1 & 0 \end{pmatrix}. \end{aligned}$$

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

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
$V^T M V = \begin{pmatrix} U_1 & 0 \\ 0 & \frac{1}{\alpha} U_1 \end{pmatrix} = U^T M U$.

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 $\mathrm{O}(n, k, \beta)$ by Lemma 4.1.

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

$$
\begin{aligned}
Q^T M Q &= (UV^{-1})^T M U V^{-1} \\
&= (V^{-1})^T (U^T M U) V^{-1} \\
&= (V^{-1})^T (V^T M V) V^{-1} \\
&= M.
\end{aligned}
$$

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

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

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

Corollary 4.26.   *If Inn_A and Inn_B are both Type 4 k-involutions of $\mathrm{SO}(n, k, \beta)$ where $A, B \in \mathrm{O}(n, k[\sqrt{\alpha}], \beta)$, then Inn_A and Inn_B are isomorphic over $\mathrm{O}(n, k, \beta)$. That is, $\mathrm{SO}(n, k, \beta)$ has at most $|k^*/(k^*)^2| - 1$ isomorphy classes of Type 4 k-involutions.*

5.   Maximal Number of Isomorphy classes

From the work we have done, it follows that the maximum number of isomorphy classes of k-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 5.1.   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 $\mathrm{SO}(n, k, \beta)$ k-involutions over $\mathrm{O}(n, k, \beta)$ of types 1, 2, 3, and 4, respectively.

From our previous work, we have the following:

Corollary 5.2.   *1. If n is odd, then*

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

If n is even, then

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

2. *If n is even, then*

$$C_2(n, k, \beta) \leq \tau_1(k) \left(\frac{\tau_2(\frac{n}{2}, k)(\tau_2(\frac{n}{2}, k) + 1)}{2} \right).$$

3. *If n is even, then*
$$C_3(n, k, \beta) \leq 1.$$

4. *If n is even, then*
$$C_4(n, k, \beta) \leq \tau_1(k).$$

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

Proof.   We first consider type 1 involutions:

1. Recall that if Inn_A is a type 1 involution of $\mathrm{SO}(n, k, \beta)$ where $A \in \mathrm{O}(n, k, \beta)$, then
$$A = X \begin{pmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{pmatrix} X^{-1}$$
and
$$X^T M X = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}.$$

By Theorem 4.4, we know that we need only count the number of choices for congruecy classes of X_1 and X_2 over $\mathrm{GL}(m, k)$ and $\mathrm{GL}(n - m, k)$. If n is odd, then

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

If n is even, then

$$C_1(n, k, \beta) \leq \left(\sum_{m=1}^{\frac{n}{2}-1} \tau_2(n-m, k)\tau_2(m, k) \right) + \left(\begin{array}{c} \tau_2(\frac{n}{2}, k) \\ 2 \end{array} \right) + \tau_2\left(\frac{n}{2}, k \right)$$

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

2. We now consider Type 2 involutions when n is even. From Theorem 4.10, we know that two Type 2 involutions, Inn_A and Inn_B, are isomorphic over $O(n, k, \beta)$ if and only if they are isomorphic over $SO(n, k, \beta)$. That is, they're isomorphic if and only if they are isomorphic when viewed as type 1 involutions of $SO(n, k, \beta)$. Using Theorem 4.4 as in the above case, and acknowledging that the eigenspaces of A for 1 and -1 are both of dimension $\frac{n}{2}$, when we count the congruecy classes of X_1 and X_2 over $GL(\frac{n}{2}, k)$, we see that

$$C_2(n, k, \beta) \leq \tau_1(k) \left(\left(\begin{array}{c} \tau_2(\frac{n}{2}, k) \\ 2 \end{array} \right) + \tau_2\left(\frac{n}{2}, k\right) \right)$$

$$= \tau_1(k) \left(\frac{\tau_2(\frac{n}{2}, k)(\tau_2(\frac{n}{2}, k) + 1)}{2} \right).$$

3. We now consider Type 3 involutions when n is even. Then, from Corollary 4.18, we know that $C_3(n, k, \beta) \leq 1$.

4. We now consider Type 4 involutions when n is even. Then, from Theorem 4.26, we know that $C_4(n, k, \beta) \leq \tau_1(k)$.

5. If n is odd, then as previously noted, $SO(n, k, \beta)$ will not have any involutions of Types 2, 3 or 4. ∎

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

Table 2: Some values of $\tau_1(k)$

k	$\bar{k}$	$\mathbb{R}$	$\mathbb{F}_q$, $2 \nmid q$	$\mathbb{Q}_p$, $p \neq 2$	$\mathbb{Q}_2$
$\tau_1(k)$	0	1	1	3	7

Table 3: Some values of $\tau_2(m, k)$

k	$\bar{k}$	$\mathbb{R}$	$\mathbb{F}_q$, $2 \nmid q$
$\tau_2(m, k)$	1	m+1	2

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

$$\tau_2(m, \mathbb{Q}_p) = \begin{cases} 1 + \cdots \left(\begin{array}{c} 3 \\ m \end{array} \right), & m \leq 3 \\ 2^3, & m \geq 3, \end{cases}$$

when $p \neq 2$, and

$$\tau_2(m, \mathbb{Q}_2) = \begin{cases} 1 + \cdots \left(\begin{array}{c} 7 \\ m \end{array} \right), & m \leq 7 \\ 2^7, & m \geq 7. \end{cases}$$

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 $2 \nmid q$.

Corollary 5.3. *For fields algebraically closed, real, or finite where but order not divisible by 2, the maximal number of possible isomorphy classes are the values listed in Table 4.*

Table 4: Maximal Number of Isomorphy Classes

k	n	Type 1	Type 2	Type 3	Type 4
$k = \overline{k}$	odd	$\frac{n-1}{2}$	0	0	0
	even	$\frac{n}{2}$	0	1	0
$k = \mathbb{R}$	odd	$\frac{1}{12}(n^3 + 6n^2 - n - 6)$	0	0	0
	even	$\frac{1}{12}(n^3 + 6n^2 + 2n)$	$\frac{1}{8}(n^2 + 6n + 8)$	1	1
$k = \mathbb{F}_q$	odd	$2n - 6$	0	0	0
	even	$2n - 1$	3	1	3

Proof. We use the previous corollary and Tables 2 and 3 to do the following computations. Note that the computations for the Type 3 and 4 cases is clear.

Suppose $k = \overline{k}$

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

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

   Now suppose $k = \mathbb{R}$

1. If n is odd, then

$$C_1(n, \mathbb{R}, \beta) \leq \sum_{m=1}^{\frac{n-1}{2}} (m+1)(n-m+1)$$
$$= \frac{1}{12}(n^3 + 6n^2 - n - 6).$$

If n is even, then

$$C_1(n, \mathbb{R}, \beta) \leq \left(\sum_{m=1}^{\frac{n}{2}-1} (m+1)(n-m+1) \right) + \binom{\frac{n}{2}+1}{2} + \frac{n}{2} + 1$$
$$= \frac{1}{12}(n^3 + 6n^2 + 2n).$$

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

$$C_2(n, \mathbb{R}, \beta) \le \binom{\frac{n}{2} + 1}{2} + \frac{n}{2} + 1$$
$$= \frac{1}{8}(n^2 + 6n + 8).$$

Lastly, suppose $k = \mathbb{F}_q$ such that $2 \nmid q$.

1. If n is odd, then $C_1(n, \mathbb{F}_q, \beta) \le 2n - 6$. If n is even, then $C_1(n, \mathbb{F}_q, \beta) \le 2n - 1$.

2. If n is odd, then $C_2(n, \mathbb{F}_q, \beta) = 0$. If n is even, then $C_2(n, \mathbb{F}_q, \beta) \le 3$.   ■

6.   Explicit Examples

6.1. Algebraically Closed Fields.

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

Corollary 6.1.   *Assume $k = \bar{k}$. If θ is an k-involution of $SO(n, k)$, then θ is isomorphic to Inn_A where $A = \left(\begin{smallmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{smallmatrix} \right)$ and $0 \le m < \frac{n}{2}$, or $A = \left(\begin{smallmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{smallmatrix} \right)$.*

Proof.   Since k is algebraically closed, we know that all k-involutions of $SO(n, k)$ are of Type 1 or 3. We first consider the Type 1 case. We will now find a representative matrix A for each isomorphy class of Type 1 k-involutions. Suppose θ is a Type 1 k-involution. We will find a representative matrix A for the isomorphic class containing θ. We know we can assume $A \in O(n, k)$. Further, by Lemma 4.3 we can write $A = X \left(\begin{smallmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{smallmatrix} \right) X^{-1}$, where we know $X^T X$ is diagonal. Since $k = \bar{k}$, then we also assume that $X^T X$ must be congruent to I_n. Since we are looking for a representative A of our isomorphy class, we may assume $X^T X = I_n$, and we can choose $X = I_n$. This means $A = \left(\begin{smallmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{smallmatrix} \right)$ is a representative of our isomorphy class.

We see that Type 3 k-involutions will exist since $J = \left(\begin{smallmatrix} 0 & I_{\frac{n}{2}} \\ -I_{\frac{n}{2}} & 0 \end{smallmatrix} \right)$ will induce a Type 3 k-involution. Thus, there is one isomorphy class of Type 3 k-involutions.   ■

We note that in this case, that the maximal number of isomorphy classes do in fact exist. That is, in Corollary 5.3, for the case where $k = \bar{k}$, we have equality in every statement.

6.2. The Standard Real Orthogonal Group.

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

Corollary 6.2.   *If θ is an k-involution of $\mathrm{SO}(n, \mathbb{R})$, then θ is isomorphic to* Inn_A *where* $A = \left(\begin{smallmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{smallmatrix} \right)$ *and* $0 \leq m \leq \frac{n}{2}$, *or* $A = \left(\begin{smallmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{smallmatrix} \right)$. *There are no Type 2 or Type 4 k-involutions for this group.*

Proof.   We first consider the Type 1 case. We will find a representative matrix A for each isomorphy class of Type 1 k-involutions. Suppose θ is a Type 1 k-involution. We will find a representative matrix A for the isomorphy class containing θ. We know we can assume $A \in \mathrm{O}(n, k)$. Further, by Lemma 4.3 we can write $A = X \left(\begin{smallmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{smallmatrix} \right) X^{-1}$, where we know $X^T X$ is congruent to a diagonal where the diagonal entries are all 1's and -1's. Since we are looking for a representative of our isomorphy class, let us assume we have $X^T X$ is equal to this diagonal matrix. We see that there can be no -1's in the diagonal matrix since $k = \mathbb{R}$. So, we assume $X^T X = I_n$, which means we can choose $X = I_n$. So, $A = \left(\begin{smallmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{smallmatrix} \right)$ is a representative of our isomorphy class.

We proceed by contradiction to show that there are now Type 2 k-involutions of $\mathrm{SO}(n, \mathbb{R})$. Suppose θ is a Type 2 k-involution. We want to find A such that $\theta = \mathrm{Inn}_A$, By Lemma 4.8 we can write $A = -\frac{\sqrt{\alpha}}{\alpha} X \left(\begin{smallmatrix} 0 & I_{\frac{n}{2}} \\ \alpha I_{\frac{n}{2}} & 0 \end{smallmatrix} \right) X^{-1}$ where $X^T X = \left(\begin{smallmatrix} X_1 & 0 \\ 0 & \frac{1}{\alpha} X_1 \end{smallmatrix} \right)$ 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, $X^T X = \left(\begin{smallmatrix} X_1 & 0 \\ 0 & -X_1 \end{smallmatrix} \right)$. But, this is a contradiction, because when $k = \mathbb{R}$, there does not exist any nonzero vectors x such that $x^T x \leq 0$, so the whole diagonal of $X^T X$ must be positive, which is not possible. This shows that there are no Type 2 k-involutions in this case. In a similar way, we can show that there are also no Type 4 k-involutions in this case.

We know that there is at most one isomorphy class of Type 3 k-involutions by Corollary 5.3. Since $A = \left(\begin{smallmatrix} 0 & -I_{\frac{n}{2}} \\ I_{\frac{n}{2}} & 0 \end{smallmatrix} \right)$ induces a Type 3 k-involution, then A is a representative of the only Type 3 isomorphy class. ∎

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 5.3, 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.

6.3. Orthogonal Groups of $\mathbb{F}_q$.

We begin by examining the Type 1 k-involutions where $k = \mathbb{F}_q$ and $q = p^h$ for all cases where $p \geq 3$. This is a complete classification of the k-involutions when n is odd. We note that for these fields we have $|k^*/(k^*)^2| = 2$. So, we will use 1 and δ_q as representatives of of the distinct field 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 $M = \left(\begin{smallmatrix} I_{n-1} & 0 \\ 0 & \delta_q \end{smallmatrix} \right)$.

Theorem 6.3.   *Let δ_q be a non-square in $\mathbb{F}_q$. Choose $a, b \in \mathbb{F}_q$ where $a^2 + b^2 = \delta_q$ and $a, b \in \mathbb{F}_q$. If n is even, then there are $n + 2$ isomorphy classes of Type 1 involutions of $\mathrm{SO}(n, \mathbb{F}_q, \beta)$, and if n is odd, there are $n + 1$ isomorphy classes of*

Type 1 involutions of $\mathrm{SO}(n, \mathbb{F}_q, \beta)$. *In Table 5, we list matrices A such that each matrix is the representative of one of these isomorphy classes, for each case of M.*

Table 5: All of the distinct Isomorphy Classes for Type 1 Automorphisms, Inn_A, of $\mathrm{SO}(n, \mathbb{F}_q, \beta)$

M	$m, 0 \leq m \leq \frac{n}{2}$	For each m such that $0 \leq m \leq \frac{n}{2}$
I_n	$A = I_{n-m,m}$	$A = \begin{pmatrix} -I_{n-m-1} & 0 & 0 & 0 \\ 0 & 1 - 2\frac{a^2}{\delta_q} & 0 & \frac{2ab}{\delta_q} \\ 0 & 0 & I_{m-1} & 0 \\ 0 & \frac{2ab}{\delta_q} & 0 & 1 - 2\frac{b^2}{\delta_q} \end{pmatrix}$
$\begin{pmatrix} I_{n-1} & 0 \\ 0 & \delta_q \end{pmatrix}$	$A = I_{n-m,m}$	$A = \begin{pmatrix} -I_{n-m-1} & & \\ & I_m & \\ & & -1 \end{pmatrix}$

Proof. We will use the equivalent conditions of Lemma 4.4 to prove that the matrices listed above will distinctly be representatives of the isomorphy classes of the k-involutions of $\mathrm{SO}(n, \mathbb{F}_q)$.

If θ is a Type 1 k-involution, then by Lemma 4.3 we can choose a matrix A such that $\theta = \mathrm{Inn}_A$ and we can write $A = X \begin{pmatrix} -I_{n-m} & 0 \\ 0 & I_m \end{pmatrix} X^{-1}$, where

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

must be diagonal, and X_1 is an $(n-m) \times (n-m)$ matrix, and X_2 is an $m \times m$ matrix, for some m where $0 \leq m \leq \frac{n}{2}$. It is a well known fact that any diagonal matrix over $\mathbb{F}_q$ must be congruent to either I_n or $\begin{pmatrix} I_{n-1} & 0 \\ 0 & \delta_q \end{pmatrix}$ where δ_q is some fixed non-square in $\mathbb{F}_q$. So, from the equivalent conditions in Theorem 4.4 it is known that X_1 and X_2 must each be congruent to I or $\begin{pmatrix} I & 0 \\ 0 & \delta_q \end{pmatrix}$ (sizing the matrices appropriately).

Case 1: β is the standard dot product, and $M = I$.

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 $\begin{pmatrix} I & 0 \\ 0 & \delta_q \end{pmatrix}$ (again, sizing appropriately).

Further, since we are searching for a representative of the congruence class, it can be assumed that $X^T M X$ is either I or $\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & \delta_q & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & \delta_q \end{pmatrix}$. These are the only possibilities, and also they must correspond to distinct isomorphy classes of Type 1 k-involutions under the conditions of Theorem 4.4.

Subcase 1.1: $X^T X = I$.

We can let $X = I$, which means $A = \begin{pmatrix} -I_{n-m} & 0 \\ 0 & I_m \end{pmatrix}$ is the representative of the isomorphy class.

Subcase 1.2: $X^T X = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & \delta_q & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & \delta_q \end{pmatrix}$.

We can let

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

It follows from this that

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

is a representative of the isomorphy class.

Case 2: β is such that $M = \begin{pmatrix} I_{n-1} & 0 \\ 0 & \delta_q \end{pmatrix}$.

Since $\det(X^T M X) = \delta_q(\det(X))^2$ is a non-square, we observe that X_1 must be congruent to I and X_2 must be congruent to $\begin{pmatrix} I & 0 \\ 0 & \delta_q \end{pmatrix}$ (sizing appropriately), or vice versa.

Further, since we are searching for a representative of the congruence class, it can be assumed that $X^T M X$ is either M or $\begin{pmatrix} I_{\frac{n}{2}-1} & 0 & 0 \\ 0 & \delta_q & 0 \\ 0 & 0 & I_{\frac{n}{2}} \end{pmatrix}$. These are the only possibilities, and also they must correspond to distinct isomorphy classes of Type 1 k-involutions under the conditions of Theorem 4.4.

Subcase 2.1: $X^T M X = M$.

In the first case, since we are looking for a representative of our congruence class, we can assume $X^T \begin{pmatrix} I_{n-1} & 0 \\ 0 & \delta_q \end{pmatrix} X = \begin{pmatrix} I_{n-1} & 0 \\ 0 & \delta_q \end{pmatrix}$. This means we can assume $X = I$ choose $A = \begin{pmatrix} -I_s & 0 \\ 0 & I_t \end{pmatrix}$ as the representative of the isomorphy class.

Subcase 2.2: $X^T M X = \begin{pmatrix} I_{\frac{n}{2}-1} & 0 & 0 \\ 0 & \delta_q & 0 \\ 0 & 0 & I_{\frac{n}{2}} \end{pmatrix}$.

We can choose $X = \begin{pmatrix} I_{n-m-1} & & & \\ & 0 & & 1 \\ & & I_{m-1} & \\ & 1 & & 0 \end{pmatrix}$. This gives representative $A = \begin{pmatrix} -I_{n-m-1} & & \\ & I_m & \\ & & -1 \end{pmatrix}$. ∎

We now spend some time considering the other three types of involutions. If n is odd, then the Types 2, 3 and 4 involutions will not occur, so we assume n is even. For the remaining three types of k-involutions, we restrict our attention to the case where β is the standard dot product. In this case, it is clear that $A = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$ will induce a Type 3 k-involution, and that $C_3(n,k) = 1$.

We know that $C_2(n, \mathbb{F}_q) \leq 3$ and $C_4(n, \mathbb{F}_q) \leq 1$. 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 k-involutions via the matrices in Table 6.

We note that these examples will all generalize to higher dimensions, so it is clear that for these fields that whenever n is even, $C_2(n, \mathbb{F}_q), C_4(n, \mathbb{F}_q) \geq 1$.

Table 6: Type 2 and Type 4 examples for $SO(4, \mathbb{F}_p)$

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

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 k-involutions are maximized. But, for $SO(4, \mathbb{F}_p)$ where $p = 3$, 5, and 7, we have done computations in Maple which use the conditions of Theorem 4.8 that show that $C_2(4, \mathbb{F}_p) = 1$. So, the number of Type 2 isomorphy classes is not maximized in these cases. 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 6.4. Suppose that $SO(n, k)$ is a finite orthogonal group and that n is even. Then, $C_2(n, k) = C_4(n, k) = 1$.

6.4. p-adic numbers.

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 possible isomorphy classes of the Type 1 k-involutions of $SO(n, \mathbb{Q}_p)$ where $p > 2$, using Lemma 4.4. Note that if n is odd and $n \neq 3$, then this all of the possible isomorphy classes of the k-involutions of $SO(n, \mathbb{Q}_p)$. We note that we say "possible" because we don't show existence, but rather we use our characterization of Type 1 k-involutions to show which classes may exist. It still remains to be shown which of these possible classes does exist.

We first state a result from [Jon67] about symmetric matrices with entries from the p-adic numbers.

Lemma 6.5. Symmetric matrices M_1 and M_2 with entries in $\mathbb{Q}_p$ are congruent if and only if $\det(M_1) = \gamma^2 \det(M_2)$ and $c_p(M_1) = c_p(M_2)$, where $c_p(M)$ denotes the Hasse symbol of matrix M.

We use this to prove a result that is an extension of Theorem 4.4 in the case that $k = \mathbb{Q}_p$.

Corollary 6.6. *Assume the hypotheses of Theorem 4.4. Statements (i) through (v) of Theorem 4.4 are equivalent the following condition:*
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. We note that this condition is equivalent to (iii) of Theorem 4.4 by Lemma 6.5. ∎

Corollary 6.6 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 k-involutions based on what the values of X_1 and X_2 would be for a representative of the congruency class in Tables 7 and 8. We note that each isomorphy class is determined by the triple $(\det(X_1) = \det(X_2), c_p(X_1), c_p(X_2))$. 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 authors) that there exists X such that $X^T X = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}$.

Table 7: X_1 and X_2 values when $k = \mathbb{Q}_p$, $p > 2$, and $-1 \in (\mathbb{Q}_p^*)^2$

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

X_1	X_2	$\det(X_1), \det(X_2)$	$c_p(X_1)$	$c_p(X_2)$
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 k-involutions. We again note that if n is odd and $n \neq 3$, 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 9, where there is 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 k-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 9: X_1 and X_2 values when $k = \mathbb{Q}_2$

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

Acknowledgements

References

[Abe88]   Abeasis, S. *On a remarkable class of subvarieties of a symmetric variety*, Adv. in Math. **71** (1988), 113–129.

[AO05]   Anker, J-P., and B. Ørsted, "Lie Theory: Harmonic Analysis on Symmetric Spaces - General Plancherel Theorems," Birkhäuser Basel, First Edition, 2005.

[vdBS97a] van den Ban, E. P., and H. Schlichtkrull, *Fourier transform on a semisimple symmetric space*, Invent. Math. **130** (1997), 517–574.

[vdBS97b] —, *The most continuous part of the Plancherel decomposition for a reductive symmetric space*, Ann. of Math. (2) **145** (1997), 267–364.

[BB81]   Beilinson, A., and J. Bernstein, *Localisation de $\mathfrak{g}$-modules*, C.R. Acad. Sci. Paris **292** (1981), 15–18.

[BHJ15]   Benim, R. W., A. G. Helminck, and F. Jackson Ward, *Isomorphy Classes of Involutions of* $\mathrm{SP}(2n, k)$, $n > 2$, J. of Lie Theory **25** (2015), 903–947.

[Bor91]   Borel, A., "Linear Algebraic Groups," Graduate Texts in Mathematics **126**, Springer Verlag, New York, 2nd enlarged edition, 1991.

[BT65]   Borel, A., and J. Tits, *Groupes réductifs*, Inst. Hautes Études Sci. Publ. Math. **27** (1965), 55–152.

[BT72]   — *Compléments a l'article "groupes réductifs"*, Inst. Hautes Études Sci. Publ. Math. **41** (1972), 253–276.

[Car29]   Cartan, E., *Groupes simples clos et ouvert et géométrie Riemannienne*, J. Math. Pures Appl. **8** (1929), 1–33.

[CD14]   Carmona, J., and P. Delorme, *Constant term of Eisenstein integrals on a reductive p-adic symmetric space*, Trans. Amer. Math. Soc. **366** (2014), 5323–5377.

[DCP83]   De Concini, C., and C. Procesi, *Complete symmetric varieties*, in: Invariant theory (Montecatini, 1982), Lecture Notes in Math. **996**, Springer Verlag, Berlin, 1983, 1–44.

[DCP85]   —, *Complete symmetric varieties. II. Intersection theory*, in: Algebraic groups and related topics (Kyoto/Nagoya, 1983), North-Holland, Amsterdam, 1985, 481–513.

[Del98]   Delorme, P., *Formule de Plancherel pour les espaces symétriques réductifs*, Ann. of Math. (2) **147** (1998), 417–452.

[Del13]   —, *Formule de Plancherel pour les fonctions deWhittaker sur un groupe réductif p-adique*, Ann. Inst. Fourier (Grenoble) **63** (2013), 155–217.

[DH14]   Delorme, P., and P. Harinck, *Wave packets in the Schwartz space of a reductive p-adic symmetric space*, J. Lie Theory **24** (2014), 41–75.

[Die51]   Dieudonne, J., "On the Automorphisms of the Classical Groups," American Mathematical Society, Provicende, RI, 1951.

[Die63]   —. "La Géometrie Des Groupes Classiques," Springer-Verlag, Berlin etc., 1963.

[Far79]   Faraut, J., *Distributions sphérique sur les espaces hyperboliques*, J. Math. pures et appl. **58** (1979), 369–444.

[FJ80]   Flensted-Jensen, M., *Discrete series for semisimple symmetric spaces*, Annals of Math. **111** (1980), 253–311.

[Gro92]   Grojnowski, I., "Character sheaves on symmetric spaces," Ph.D. Thesis, Massachusetts Institute of Technology, June 1992.

[HC84]   Harish-Chandra, "Collected papers, Vol. I-IV," Springer Verlag, New York, 1984, 1944–1983, Edited by V. S. Varadarajan.

[Hel88]   Helminck, A. G., *Algebraic groups with a commuting pair of involutions and semisimple symmetric spaces*, Adv. in Math. **71** (1988), 21–91.

[Helm2000] —, *On the Classification of k-involutions I*, Adv. in Math. **153** (2000), 1–117.

[HH02]   Helminck, A. G., and G. F. Helminck, *Spherical distribution vectors*, Acta Appl. Math. **73** (2002), 39–57.

[HH05]   —, *Multiplicity one for representations corresponding to spherical distribution vectors of class ρ*, Acta Appl. Math. **86** (2005), 21–48.

[HW93]   Helminck, A. G., and S. P. Wang, *On rationality properties of involutions of reductive groups*, Adv. in Math. **99** (1993), 26–96.

[HW02]   Helminck, A. G., and L. Wu, *Classification of involutions of* $\mathrm{SL}(2,k)$, Comm. Algebra, **30** (2002), 193–203.

[HWD04]   Helminck, A. G., L. Wu, and C. Dometrius, *Involutions of* $\mathrm{SL}(n,k)$, $(n > 2)$, Acta Appl. Math. **90** (2006), 91–119.

[HS90]   Hirzebruch, F., and P. J. Slodowy, *Elliptic genera, involutions, and homogeneous spin manifolds*, Geom. Dedicata **35** (1990), 309–343.

[Hum75]   Humphreys, J. E., "Linear algebraic groups," Graduate Texts in Mathematics **21**, Springer Verlag, New York, 1975.

[Jon67]   Jones, B. W., "The Arithmetic of Quadratic Forms," Mathematical Association of America, 1967.

[Lus90]   Lusztig, G., *Symmetric spaces over a finite field*, in; The Grothendieck Festschrift Vol. III (Boston, MA), Progr. Math., **88**, Birkhäuser, 1990, 57–81.

[LV83]   Lusztig, G., and D. A. Vogan, *Singularities of closures of K-orbits on flag manifolds*, Invent. Math. **71** (1983), 365–379.

[ŌS80]   Ōshima, T. and J. Sekiguchi, *Eigenspaces of invariant differential operators in an affine symmetric space*, Invent. Math. **57** (1980), 1–81.

[Ric50]   Rickart, C. E., *Isomorphic Groups of Linear Transformations I.* American J. of Math. **72** (1950), 451–464.

[Ric51]   —, *Isomorphic Groups of Linear Transformations II.* American J. of Math. **73** (1951), 697–716.

[Spr81]   Springer, T. A., "Linear algebraic groups," Progr. Math. **9**, Birkhäuser, Boston, Basel, Stuttgart, 1981.

[TW89]   Tong, Y. L., and S. P. Wang, *Geometric realization of discrete series for semisimple symmetric space*, Invent. Math. **96** (1989), 425–458.

[Vog82]   Vogan, D. A.,
            Irreducible characters of semi-simple Lie groups IV, Character-multiplicity duality, Duke Math. J. **49** (1982), 943–1073.

[Vog83]   —, *Irreducible characters of semi-simple Lie groups III. Proof of the Kazhdan-Lusztig conjectures in the integral case*, Invent. Math. **71** (1983), 381–417.

[Won62]   Wonenburger, M., *The Automorphisms of the Group Rotations and its Projective Group Corresponding to Quadratic Forms of any Index*, *Canadian J. of Math.* **15** (1963), 302–303.

Robert W. Benim
Pacific University
Department of Mathematics
and Computer Science
2043 College Way
Forest Grove, OR 97116
rbenim@gmail.com

Christopher E. Dometrius
Forsyth Technical Community College
Math, Science & Technologies Division
2100 Silas Creek Parkway
Winston-Salem, North Carolina 27103
cdometrius@forsythtech.edu

Aloysius G. Helminck
North Carolina State University
Department of Mathematics
2108 SAS Hall
Box 8205
Raleigh, North Carolina 27695
loek@ncsu.edu

Ling Wu
North Carolina State University
Department of Mathematics
2108 SAS Hall
Box 8205
Raleigh, North Carolina 27695
ling_wu@hotmail.com