ABSTRACT

ABSHER, JOHN M. On the Isomorphy Classes of Involutions over $\mathrm{SO}(2n, k)$. (Under the direction of Dr. Aloysius Helminck).

The study of symmetric spaces involves group theory, field theory, linear algebra, and Lie algebras, as well as involving the related disciplines of topology, manifold theory, and analysis. The notion of symmetric space was generalized in the 1980's to groups defined over arbitrary base fields. In particular, if G is an algebraic group defined over a field k of characteristic not 2, θ is an automorphism of order 2 of G, and H is the fixed point group of θ, then the homogeneous space G/H is called a symmetric space. It can be identified with the subvariety $Q = \{g\theta(g)^{-1} \mid g \in G\}$ of G.

These generalized symmetric varieties are especially of interest in representation theory, especially when the base field k is the p-adic numbers, a finite field or a number field. A full classification of these symmetric spaces for arbitrary fields is still an open problem.

The main focus for my thesis concerns a classification of these symmetric spaces for G the special orthogonal group defined over an arbitrary field.

On the Isomorphy Classes of Involutions over SO$(2n, k)$

by
John M. Absher

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

Mathematics

Raleigh, North Carolina

2010

APPROVED BY:

Dr. Naihuan Jing	Dr. Amassa Fauntleroy
Dr. Aloysius Helminck Chair of Advisory Committee	Dr. Ernest Stitzinger

BIOGRAPHY

John M. Absher was born in Durham, NC in 1983. He is not yet dead. Having been afflicted with serious sinus-related health problems from earliest childhood, he loathed math and had no energy to pursue it until tenth grade geometry, under Mr. Crary. The analytical structure of geometry was very appealing to him, and thence he knew he wanted to pursue higher education in mathematics. His health began to improve after his last sinus operation, when he was sixteen or seventeen, which was under the brilliant Dr. Malenbaum, who all but saved his life. His health has gradually improved every year hence and as such he has been blessed with sufficient energy and motivation to pursue his studies.

He received a B.S. in Mathematics at the University of North Carolina at Chapel Hill, and received such excellent instruction there that he was able to take all of his qualifying exams over his first summer of graduate school, i.e., summer 2006. At that time, all of these exams at North Carolina State University had to be taken simultaneously, so in the opinion of many that was no mean feat.

He has many outside interests besides his interest in math, and they include history, religion, politics, chess, Latin, ancient Greek, French (to a lesser extent), and Christian theology. He is also one of those rare people who are perfectly happy in solitude.

ACKNOWLEDGMENTS

To begin with, I have to think my incomparable thesis advisor, Dr. Aloysius (Loek) Helminck, who is one of the most wise and talented yet unpretentious people I have ever known. His assistance and sense of humor were invaluable aids to completing graduate school, and his kind permission to pursue other interests which were themselves challenging and time-consuming (viz., Latin and ancient Greek) were invaluable in making graduate school enjoyable.

I must also thank my parents, Martha and Stan Absher, for their assistance, advice, and support. Both of them have had experience in academia, the former as an Associate Dean at Duke, the latter having received a Ph.D. in English at Duke. There were many times when their advice, and particularly my mom's advice, being as she is a very experienced administrator, helped me get through difficulties I would not have known how to deal with otherwise.

There have been many people who made my graduate school experience richer, many of whom were or are (at the time of this writing) fellow graduate students in math. These include but are not limited to the following: Mike Allocca, Brandon Blevins, Kate Brenneman, Catherine Buell, Amanda Criner, Nick Giffen (and Nick's cat J.J.), Janine Haugh, Sharon Hutton, Louis Levy, David Mokrauer, Emma Norbrothen, Richard Petersen, Ellen Peterson, Patrick Sigmon, Ryan Therkelsen, Kyle Thompson, Qiang Wang, Tom Wears, and Zahava Wilstein. I did not get to know half of them as well as I should have liked, which was my own fault for being solitary and something of a workaholic.

Let me also take the time to thank the other members of my thesis committee besides Loek (who lets anyone call him "Loek"), Drs. Ernest Stitzinger ("Stitz" to almost anyone), Naihuan Jing, and Amassa Fauntleroy. I enjoyed all of their classes which I got an opportunity to take, and I regret that I was never able to take a class with the latter. I have also enjoyed their lively senses of humor.

I would also like to thank my instructors in Latin and ancient Greek, who helped me explore an interest I had never had time for as an undergraduate and helped me develop a talent I had never known that I possessed. These are Drs. Everette Wheeler and Zola

Packman in Latin, and the late Dr. Mark Sosower and Dr. Zola Packman again in ancient Greek. They all made the difficult subjects they taught lively and enjoyable, which I once thought was impossible in a language class.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

My thesis studies Lie groups (or algebraic groups) and the (generalized) symmetric spaces obtained from them. The study of symmetric spaces involves group theory, field theory, linear algebra, and Lie algebras, as well as involving the related disciplines of topology, manifold theory, and analysis. The notion of symmetric space was generalized in the 1980's to groups defined over arbitrary base fields. In particular, if G is an algebraic group defined over a field k of characteristic not 2, θ is an automorphism of order 2 of G, and H is the fixed point group of θ, then the homogeneous space G/H is called a symmetric space. It can be identified with the subvariety $Q = \{g\theta(g)^{-1} \mid g \in G\}$ of G.

These generalized symmetric varieties are especially of interest in representation theory, especially when the base field k is the p-adic numbers, a finite field or a number field. A full classification of these symmetric spaces for arbitrary fields is still an open problem.

The main focus for my thesis concerns a classification of these symmetric spaces for G the special orthogonal group defined over an arbitrary field. Symmetric spaces have been studied over 100 years, with the initial theory focusing on symmetric spaces over the real numbers and their important role in mathematical physics, representation theory, harmonic analysis, and differential geometry. More recently the field of research has expanded to include the study of these spaces over general fields of characteristic not 2, and the applications of such generalization has been shown to yield results important to not only the areas mentioned above but also to number theory, quadratic forms, algebraic geometry, combinatorics, automorphic functions, and more. We obtain our symmetric space by starting with a reductive linear algebraic group (matrix group) G defined over an arbitrary field (of characteristic not equal to 2) and analyzing the space G/H, where H is the fixed point group of an involution of G. Classification of the involution leads to classification of the subgroup H, which enables us to characterize the related symmetric space G/H. The symmetric space can also be identified with the subvariety $Q = \{g\theta(g)^{-1} \mid g \in G\}$ of G. A full classification of these symmetric spaces for arbitrary fields is still an open problem. The main focus for my thesis concerns a classification of these symmetric spaces for G the special orthogonal group defined over an arbitrary field. For $g \in \mathrm{SO}(2n, K)$ where K is an extension field of k the corresponding inner automorphism of $\mathrm{SO}(2n, K)$ is denoted by $\mathrm{Inn}(g)$.

Definition 1. *If ϕ and ψ are involutions over $\mathrm{SO}(2n, k)$ then ϕ is isomorphic to ψ if there is an inner automorphism $\omega \in \mathrm{Aut}(\mathrm{SO}(2n, k))$ such that $\omega^{-1}\phi\omega = \psi$. By abuse of notation, isomorphy classes of involutions with respect to conjugacy will also be called conjugacy classes of involutions.*

Definition 2. *If K is an extension field of k and ϕ and ψ are involutions of $\mathrm{SO}(2n, k)$ then they are K-isomorphic if there is an inner automorphism $\omega \in \mathrm{Aut}(\mathrm{SO}(2n, K))$ such that $\omega^{-1}\phi\omega = \psi$. By abuse of notation, K-isomorphy classes of involutions with respect to conjugacy will also be called K-conjugacy classes of involutions.*

Thus, for the classification one considers the notion of isomorphism up to $\mathrm{Inn}(G)$, where two involutions θ and τ are isomorphic iff τ can be obtained from θ via conjugation by an inner automorphism of G. Involutions of $\mathrm{SL}(n, k)$ were classified by Dometrius, Helminck, and Wu, and the classification of $\mathrm{SO}(2n + 1, k)$ was done by Ling Wu. I have classified the involutions of $\mathrm{SO}(2n, k)$. I first showed that all involutions of $\mathrm{SO}(2n, k)$ are restrictions of involutions of $\mathrm{SL}(2n, k)$ to $\mathrm{SO}(2n, k)$. Then I determined which isomorphy classes of involutions of $\mathrm{SL}(2n, k)$ have a representative that leaves $\mathrm{SO}(2n, k)$ invariant. The final step is to determine in how many $\mathrm{SO}(2n, k)$-isomorphy classes one $\mathrm{SL}(2n, k)$-isomorphy class splits. This depends on the field in question and in many cases one $\mathrm{SL}(2n, k)$-isomorphy class splits in several $\mathrm{SO}(2n, k)$-isomorphy classes.

Over any algebraically closed field of characteristic not equal to two, there is one isomorphy class of involutions in $\mathrm{SO}(2n,k)$ for every isomorphy class of $\mathrm{SL}(2n,k)$. The same is true over the real numbers $\mathbb{R}$. However, over the finite field of p elements, denoted $\mathbb{F}_p$, there are two isomorphy classes of $\mathrm{SO}(2n,k)$ for every one in $\mathrm{SL}(2n,k)$. The situation is much more complicated over $\mathbb{Q}_p$. There are sixteen isomorphy classes in the case $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$, although they are different in these cases, and there are thirty-two classes in the case $p = 2$.

From that, it is necessary to determine what the fixed-point groups of these isomorphy classes of involutions are. That requires algebra, by which I have determined that, e.g., if $A, B \in \mathrm{GL}(n,k)$ and $A = (a_{ij})$ and $B = \mathrm{diag}(b_1, \ldots, b_n)$. Then $ABA^T = B$ iff for all $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, two properties hold:

1. $\displaystyle\sum_{\ell=1}^{n} a_{i\ell}^2 b_\ell = b_i$

2. $\displaystyle\sum_{\ell=1}^{n} a_{i\ell} a_{j\ell} b_\ell = 0$

Using this result and others like it I computed the fixed-point group of each isomorphy class of involutions over $\mathbb{Q}_p$.

The next step is to determine which of these classes are compact, and which are not. It turns out that the majority of them are not compact. Some of them are compact only for suitably small n, and many of them are never compact. A major part of this result is the fact that whereas if $p \equiv 1 \pmod 4$ then every p-adic number in $\mathbb{Q}_p$ is the sum of the squares of two p-adic numbers, if $p \equiv 3 \pmod 4$ or $p = 2$ then this is not true. That restricts the size of n in many fixed-point groups, so that if n is too small certain fixed-point groups do not exist over $\mathrm{SO}(2n,k)$.

From there, I have investigated the involution classes and fixed-point groups of the quadratic extensions of each class of p-adic field, i.e., of each field $\mathbb{Q}_p$ where $p \equiv 1 \pmod 4$, $p \equiv 3 \pmod 4$, and $p = 2$. There are some differences between these case and the previous cases (over $\mathbb{Q}_p$ unextended).

Further results are related to quadratic elements. Firstly, I have shown what the diagram automorphisms are for the root system of $\mathrm{SO}(2n,k)$, which is D_ℓ, given the divers ways in which various roots (or dots, on the graph) may be fixed points. I also identified a maximal torus in $\mathrm{SO}(2n,k)$ and proved that that is what it is. That required tedious-to-compute results related to eigenvalues, the form of matrices in $\mathrm{SO}(2,k)$, and other such things.

Chapter 2

Preliminaries, Recollections, and Notations

In this thesis, I have made use of the following notation: I_n will denote the $n \times n$ identity matrix, $I_{s,t}$ will denote the matrix $\begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix}$, $\ni$ means "such that," and k will denote a field. Also, J_A will denote the operator $J_A : X \mapsto A^{-1}XA$ for all X in $\mathrm{GL}(2n, k)$, and $\mathrm{Inn}(G)$ will denote the set of all inner automorphisms in G. Further, $\mathbb{F}$ will always denote an algebraically closed field, not necessarily of characteristic zero, and $c_p(A)$ will always represent the Hasse symbol of A. Also, $\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$.

Furthermore, $\lceil \ \rceil$ denotes the "ceiling" function which sends any real number ξ to the next integer greater than or equal to ξ. Similarly, $\lfloor \ \rfloor$ denotes the floor function, and $\mathbb{F}$ denotes an algebraically closed field of characteristic not equal to two.

I have made use of the following outside theorems: the first one was proven by Ling Wu and Christopher Dometrius, and it appears in the Ph.D. thesis of the latter [2, Theorem 5.2 on p. 75].

Outside Theorem 1. *Suppose β is a non-degenerate symmetric bilinear form with matrix M over $V = k^n$ where $\mathrm{char}(k) \neq 2$ and $\bar{G} = \mathrm{SO}(2n, \bar{k})$, assuming $n > 2$.*

i. *If $A \in \mathrm{GL}(2n, \bar{k})$ then the automorphism $J_A : X \mapsto A^{-1}XA$ of $\mathrm{GL}(2n, \bar{k})$ keeps $\bar{G}$*

invariant iff $A = \alpha A^*$*, where* $\alpha \in \bar{k}$ *and*

a. $A^* \in \bar{G}$ *if* n *is odd*

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

ii. *If* A *is in* $\bar{G}$ *for any* n*, or* $\mathrm{O}(n, \bar{k}, \beta)$ *where* n *is even, then the inner automorphism* J_A *of* $\bar{G}$ *keeps* G *invariant iff* $A = \alpha A^*$ *where* $\alpha \in \bar{k}$ *and*

a. $A^* \in G$ *if* n *is odd*

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

The next result is from Burton, and it is a well-known and essential result about the p-adic numbers [6, pp. 27-28]. The definitions of the terms contained in it can be found in chapter four.

Outside Theorem 2. *Let* $\alpha, \beta, \gamma, \rho$*, and* σ *be nonzero numbers in the p-adic field* $\mathbb{Q}_p$*. Let* $(\alpha|p)$ *be the value of the Legendre symbol* $(\alpha_0|p)$ *where* α_0 *is the first term in the p-adic expansion of* α*. Also let* $(\alpha, \beta)_\infty$ *be the value of the Hilbert symbol over* $\mathbb{R}$ *and let* $(\alpha, \beta)_p$ *be the value of the Hilbert symbol in* $\mathbb{Q}_p$*. Then we have the following:*

1. $(\alpha, \beta)_\infty = 1$ *unless* $\alpha < 0$ *and* $\beta < 0$

2. $(\alpha, \beta)_p = (\beta, \alpha)_p$

3. $(\alpha\rho^2, \beta\sigma^2)_p = (\alpha, \beta)_p$

4. $(\alpha, -\alpha)_p = 1$

5. *If* $\alpha = p^n a_1$ *and* $\beta = p^m b_1$ *with* a_1 *and* b_1 *units then:*

i. *if* p *is odd then* $(\alpha, \beta)_p = (-1|p)^{nm}(a_1|p)^m(b_1|p)^n$

ii. *else if* $p = 2$*, then* $(\alpha, \beta)_p = (2|a_1)^m(2|b_1)^n(-1)^{\frac{(a_1-1)(b_1-1)}{4}}$

6. *If* p *is prime to* $2\alpha\beta$*,* $(\alpha, \beta)_p = 1$ *for* $p \neq \infty$ *provided* α *and* β *are p-adic integers.*

7. $(\alpha, \beta)_p(\alpha, \gamma)_p = (\alpha, \beta\gamma)_p$

8. $(\alpha, \alpha)_p = (\alpha, -1)_p$

9. $(\alpha\rho, \beta\rho)_p = (\alpha, \beta)_p(\rho, -\alpha\beta)_p$

10. *If β is not a square in $\mathbb{Q}_p$ and $c = \pm 1$ then for each prime p there is an integer α such that $(\alpha, \beta)_p = c$. Furthermore, if m as defined in property 5 is odd, then such an α can be found that is prime to p.*

11. *If a and b are in $\mathbb{Q}^*$, the set of non-zero rational numbers, then*

$$\prod_{p\ prime\ and\ p\ =\ \infty} (a, b)_p = 1$$

The next result can be found in Mahler [7, Theorem 1 on p. 72].

Outside Theorem 3. *The non-squares of $\mathbb{Q}_p$ are represented by the elements $-1, \pm 2, \pm 3$, and ± 6. If $p > 2$, the non-squares of $\mathbb{Q}_p$ are represented by N_p, p, and pN_p. This means that there are seven distinct quadratic extensions of $\mathbb{Q}_2$, viz., $\mathbb{Q}_2(\sqrt{-1})$, $\mathbb{Q}_2(\sqrt{2})$, $\mathbb{Q}_2(\sqrt{-2})$, $\mathbb{Q}_2(\sqrt{3})$, $\mathbb{Q}_2(\sqrt{-3})$, $\mathbb{Q}_2(\sqrt{6})$, and $\mathbb{Q}_2(\sqrt{-6})$. Also, there are three distinct quadratic extensions of $\mathbb{Q}_p$ if $p > 2$, and they are $\mathbb{Q}_p(\sqrt{N_p})$, $\mathbb{Q}_p(\sqrt{p})$, and $\mathbb{Q}_p(\sqrt{pN_p})$. Note that if $-1 \notin \mathbb{Q}_p^{*2}$ then one can use -1 in place of N_p, as I did below.*

The next result is a result by Drs. Helminck and Wang, the former of whom is my thesis adviser. It can be found in their paper [5, Proposition 10].

Outside Theorem 4. *Let G be a connected, reductive, algebraic k-group with $\mathrm{char}(k) = 0$, let χ be an involution of G, and let $X = \{x\chi(x)^{-1} \mid x \in G\}$. If $G^\chi \cap [G, G]$ is anisotropic over k then X_k consists of semi-simple elements.*

The next result is a result of elementary number theory, and a proof can be found in Rosen [8, Lemma 3.9 on pp. 112-113].

Outside Theorem 5. *Let $n \in \mathbb{Z}$ be such that $n > 0$ and n is odd. Then there is a one-to-one correspondence between differences (not sums) of squares of integers (in $\mathbb{Z}$) that equal n and factorizations of n into two positive integers.*

The next result was proven by Ling Wu in his doctoral thesis [11, Lemma 11 on p. 26].

Outside Theorem 6. *In the finite field $\mathbb{F}_p$, -1 is a square iff $p \equiv 1 \pmod 4$.*

Now here is another result from elementary number theory on the integers $\mathbb{Z}$. This one is very useful in proving whether every element of $\mathbb{Q}_p$ is a square or not. Specifically, it is a result on linear diophantine equations in two variables. A proof can be found in Rosen [8, Theorem 3.21 on pp. 120-121].

Outside Theorem 7. *Let $a, b \in \mathbb{Z}$ be such that the greatest common divisor of a and b is d. The equation $ax + by = c$ has no solutions in $\mathbb{Z}$ if d does not divide c, i.e., if there is no integer m such that $md = c$. On the other hand, if d does divide c (so such an integer m exists) then there are infinitely many solutions to $ax + by = c$ over $\mathbb{Z}$. Furthermore, if $x = x_0$, $y = y_0$ is a solution to the equation then every solution is of the form $x = x_0 + \frac{b}{d}n$, $y = y_0 - \frac{a}{d}n$, where $n \in \mathbb{Z}$.*

This last outside theorem is very useful in computing the fixed-point groups and whether they are compact over $\mathbb{Q}_p$.

Outside Theorem 8. *Over any p-adic field $\mathbb{Q}_p$, $\forall\ a_1, a_2, a_3, a_4, a_5 \in \mathbb{Q}_p^*$, $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 = 0$ has a non-trivial solution. That implies $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = a_5$ has a solution. This result can be found in Scharlau [9, Theorem 6.3 on p. 187].*

Chapter 3

Involution Isomorphy Classes with Respect to Conjugation Classes over $\mathrm{SO}(2n, k)$ where $k = \mathbb{R}$, $\mathbb{F}_p$

3.1 Results Over General Fields

The first needed result in classifying isomorphism classes of involutions over $\mathrm{SO}(2n, k)$ with respect to conjugacy, which I also call ”conjugacy classes of involutions” by abuse of notation, is one that gives an idea of what form the involutions over $\mathrm{SO}(2n, k)$ take. These involutions are classified according to the inner involutions J_A, $A \in \mathrm{SO}(2n, k)$. That is true according to the following theorem:

Theorem 1. *Suppose β is a non-degenerate symmetric bilinear form with matrix M over $V = k^n$ where* $\mathrm{char}(k) \neq 2$ *and $\bar{G} = \mathrm{SO}(2n, \bar{k})$, assuming $n > 2$.*

- ***i.*** *If $A \in \mathrm{GL}(2n, \bar{k})$ then the automorphism $J_A : X \mapsto A^{-1}XA$ of $\mathrm{GL}(2n, \bar{k})$ keeps $\bar{G}$ invariant iff $A = \alpha A^*$, where $\alpha \in \bar{k}$ and*
  - ***a.*** *$A^* \in \bar{G}$ if n is odd*
  - ***b.*** *$A^* \in \bar{G}$ or $A^* \in \mathrm{O}(n, \bar{k}, \beta)$ and $\det(A^*) = -1$ if n is even*

ii. *If A is in $\bar{G}$ for any n, or $\mathrm{O}(n,\bar{k},\beta)$ where n is even, then the inner automorphism J_A of $\bar{G}$ keeps G invariant iff $A=\alpha A^*$ where $\alpha\in\bar{k}$ and*

a. *$A^*\in G$ if n is odd*

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

Theorem 1 was proven by Ling Wu and Christopher Dometrius, and it appears in the Ph.D. thesis of the latter [2, Theorem 5.2 on p. 75]. The theorem shows that the notion of classifying conjugacy classes of involutions by the inner involutions is valid, and the following proposition gives an idea of what form the inner involutions actually take.

Proposition 1. *Suppose $\theta=J_A$ is an involution of $G\equiv\mathrm{SO}(2n,k)$. Then if $A\in G$, $A=A_0^{-1}\begin{pmatrix} I_s & 0\\ 0 & -I_t\end{pmatrix}A_0$ where $A_0\in\mathrm{GL}(2n,k)$, $A_0A_0^T$ is diagonal, $s+t=2n$, and s and t are both even. It is also possible that $A\in\mathrm{O}(2n,k)$ and that A still has the same form but $A\notin G$, then s and t are both odd.*

Proof. For all involutions θ of G, $\theta=J_A$. $J_A^2=id$ so $\forall\ X\in G, J_A^2(X)=A^{-2}XA^2=X\Rightarrow XA^2=A^2X$ so $A^2=cI_{2n}$. It has elsewhere been proven that $c=1$, so the minimal polynomial of J_A is $(x+1)(x-1)$. Thus, the eigenvalues of J_A are ±1.

As a result, $\exists\ A_0\in\mathrm{GL}(2n,k)\ni A=A_0^{-1}I_{s,t}A_0$. Since $A\in G$, $A^{-1}=A^T$, or in other words,

$$A_0^T\begin{pmatrix} I_s & 0\\ 0 & -I_t\end{pmatrix}(A_0^{-1})^T=A_0^{-1}\begin{pmatrix} I_s & 0\\ 0 & -I_t\end{pmatrix}A_0$$

$\therefore A_0A_0^TI_{s,t}=I_{s,t}A_0A_0^T$. Call this equation "$(*)$".

Let $A_0A_0^T=\begin{pmatrix} X_{11} & X_{12}\\ X_{21} & X_{22}\end{pmatrix}$, where X_{11} is an $s\times s$ block, X_{12} is an $s\times t$ block, X_{21} is an $t\times s$ block, and X_{22} is an $t\times t$ block. Then from $(*)$,

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

$\therefore X_{12} = -X_{12}$ and $X_{21} = -X_{21}$, so $X_{12} = 0_{s\times t}$ and $X_{21} = 0_{t\times s}$.
$\therefore A_0A_0^T = \begin{pmatrix} X_{11} & 0 \\ 0 & X_{22} \end{pmatrix}$.

$(A_0A_0^T)^T = A_0A_0^T$ so $\begin{pmatrix} X_{11}^T & 0 \\ 0 & X_{22}^T \end{pmatrix} = \begin{pmatrix} X_{11} & 0 \\ 0 & X_{22} \end{pmatrix}$, which of course implies $X_{11} = X_{11}^T$ and $X_{22} = X_{22}^T$, so $A_0A_0^T$ is symmetric. Since symmetric matrices are congruent to diagonal matrices, there is a $s \times s$ matrix N_1 such that $N_1X_{11}X_{11}^TN_1^T$ is diagonal and there is a $t \times t$ matrix N_2 such that $N_2X_{22}X_{22}^TN_2^T$ is diagonal. Thus, if $N = \begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix}$ then $NA_0A_0^TN^T = (NA_0)(NA_0)^T$ is diagonal. Ergo, $(NA_0)^{-1}\begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix}(NA_0) = A_0^{-1}N^{-1}\begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix}NA_0$
$= A_0^{-1}\begin{pmatrix} N_1^{-1} & 0 \\ 0 & -N_2^{-1} \end{pmatrix}\begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix}A_0 = A_0^{-1}I_{s,t}A_0$
$\therefore$ One can always pick $A = A_0^{-1}I_{s,t}A_0 \ni A_0A_0^T$ is diagonal.

Furthermore, $\det A = \det(A_0^{-1}I_{s,t}A_0) = \det(A_0^{-1})\det(I_{s,t})\det(A_0) = \det(A_0)^{-1}(-1)^t$ $\det(A_0) = (-1)^t = 1$ so t must be even. Since $s + t = 2n$, s is even too.

If s and t are even, $A \in \mathrm{SO}(2n, k)$, but it is possible that s and t are both odd and $A \in \mathrm{O}(2n, k)$ but $A \notin \mathrm{SO}(2n, k)$. Then J_A will still represent an involution on $\mathrm{SO}(2n, k)$ by Theorem 1. Q.E.D.

A result is needed that will help classify these involutions over $\mathrm{SO}(2n, k)$ for k not only equal to $\mathbb{F}$, the algebraically closed field of characteristic not equal to two, and $\mathbb{R}$ and $\mathbb{F}_p$, but $\mathbb{Q}_p$ as well. The latter case will be considered in the following chapter.

But before one can begin classifying the conjugacy classes of involutions, one must have a way to determine whether or not any two given involutions are equivalent. The following proposition provides just such a set of criteria, which are all that is needed in the case $G = \mathrm{SO}(2n, k)$.

Theorem 2. *Suppose θ and ϕ are two involutions of $G \equiv \mathrm{SO}(2n, k)$ in the same $\mathrm{GL}(2n, k)$-conjugacy class. Let A and B be matrices such that $\theta = J_A$, $\phi = J_B$, and A and B satisfy the conditions of Proposition 1. Suppose further that $A = A_0^{-1}I_{s,t}A_0$, $B = B_0^{-1}I_{s,t}B_0$, $A_0A_0^T =$*

$\operatorname{diag}(a_1, ..., a_{2n})$, *and* $B_0B_0^T = \operatorname{diag}(b_1, ..., b_{2n})$. *Then the following are equivalent.*

i. *θ is conjugate to ϕ over G*

ii. *A is conjugate to B over G*

iii. $\operatorname{diag}(a_1, ..., a_s)$ *is congruent to* $\operatorname{diag}(b_1, ..., b_s)$ *and* $\operatorname{diag}(a_{s+1}, ..., a_{2n})$ *is congruent to* $\operatorname{diag}(b_{s+1}, ..., b_{2n})$

iv. *If k is the p-adic field $\mathbb{Q}_p$ then there are $\tau_1, \tau_2 \in \mathbb{Q}_p^*$ that are not necessarily distinct such that $a_1a_2...a_s = \tau_1^2 b_1b_2...b_s$, $a_{s+1}a_{s+2}...a_{2n} = \tau_2^2 b_{s+1}b_{s+2}...b_{2n}$, $c_p(a_1, a_2, ..., a_s) = c_p(b_1, b_2, ..., b_s)$, and $c_p(a_{s+1}, a_{s+2}, ..., a_{2n}) = c_p(b_{s+1}, b_{s+2}, ..., b_{2n})$*

Proof. $\boxed{i. \Rightarrow ii.}$ Firstly, assume result *i.* is true. Then let $\theta = \rho^{-1}\phi\rho$, where $\rho \in \operatorname{Inn}(G)$. Then $\forall\ X \in G$, $\theta(X) = (\rho^{-1}\phi\rho)(X) = \rho^{-1}(\phi(\rho(X)))$, so $A^{-1}XA = CB^{-1}C^{-1}XCBC^{-1}$. Now, $CB^{-1}C^{-1}A^{-1}XACBC^{-1} = X$ so $CB^{-1}C^{-1}A^{-1}X = XCB^{-1}C^{-1}A^{-1} \Rightarrow CB^{-1}C^{-1}A^{-1} = aI_{2n}$, where $a \in K$ and $a \neq 0$.

$\therefore \frac{1}{a}CBC^{-1} = A$

$I_{2n} = AA^T = \frac{1}{a^2}CBC^TCB^TC^T = \frac{1}{a^2}CBB^TC^T = \frac{1}{a^2}CC^T = \frac{1}{a^2}I_{2n}$, so $a = \pm 1$. Since $A \in G$, $1 = \det(A) = \det(\frac{1}{a}CBC^T) = \frac{1}{a}\det(C)\det(B)\det(C)^{-1} = \frac{1}{a}\det(B)$ (since $C^{-1} = C^T$). Now, since $B \in G$, $\det(B) = 1$ so $1 = \frac{1}{a} \Rightarrow a = 1$.

$\therefore A = CBC^T = CBC^{-1}$.

$\boxed{ii. \Rightarrow i.}$ Assume *ii.*, and let $A = CBC^{-1} = CBC^T$. Define $\rho(X) = C^TXC$. Then $\rho^{-1}(\phi(\rho(X))) = CB^TC^TXCBC^T = A^TXA = \theta(X)$ so θ and ϕ are indeed conjugate.

$\boxed{ii. \Rightarrow iii.}$ Assume *ii.* Then $A = CBC^T = CBC^{-1}$, so

$$A_0^{-1}I_{s,t}A_0 = CB_0^{-1}I_{s,t}B_0C^{-1}$$

In that case,

$$(A_0^T)^{-1}A_0^{-1}I_{s,t}A_0A_0^T = (A_0^T)^{-1}CB_0^{-1}I_{s,t}B_0C^{-1}A_0^T$$

$$(A_0^T)^{-1}A_0^{-1}I_{s,t}A_0A_0^T = (A_0^T)^{-1}C[B_0^T(B_0^T)^{-1}]B_0^{-1}I_{s,t}B_0[B_0^T(B_0^T)^{-1}]C^{-1}A_0^T$$

Therefore,

$$(A_0A_0^T)^{-1}I_{s,t}(A_0A_0^T) = [(B_0^T)^{-1}C^{-1}A_0^T]^{-1}(B_0B_0^T)^{-1}I_{s,t}(B_0B_0^T)[(B_0^T)^{-1}C^{-1}A_0^T]$$

Now, by assumption $A_0A_0^T$ and $B_0B_0^T$ are diagonal, so they and their inverses both commute with $I_{s,t}$ since $I_{s,t}$ is also diagonal.

$\therefore I_{s,t} = [(B_0^T)^{-1}C^{-1}A_0^T]^{-1}I_{s,t}[(B_0^T)^{-1}C^{-1}A_0^T]$, so $(B_0^T)^{-1}C^{-1}A_0^T$ commutes with $I_{s,t}$ as well.

Ergo, it must be true that $(B_0^T)^{-1}C^{-1}A_0^T = \begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix}$, where N_1 is $s \times s$ and N_2 is $t \times t$. Also, inasmuch as $\det((B_0^T)^{-1}C^{-1}A_0^T) \neq 0$, $\det(N_1) \neq 0$ and $\det(N_2) \neq 0$, so $[(B_0^T)^{-1}C^{-1}A_0^T]^{-1} = \begin{pmatrix} N_1^{-1} & 0 \\ 0 & N_2^{-1} \end{pmatrix}$. For ease of reference, let $N = \begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix}$.

From these formulas, it is clear that $A_0^T = CB_0^TN$, so $A_0 = N^TB_0C^T$. Then $A_0A_0^T = N^TB_0C^TCB_0^TN$. Since $C \in G$, $C^T = C^{-1}$ so $A_0A_0^T = N^TB_0B_0^TN$, which implies that $\operatorname{diag}(a_1, ..., a_{2n}) = N^T \operatorname{diag}(b_1, ..., b_{2n})N$. Therefore, $\operatorname{diag}(a_1, ..., a_s) = N_1^T \operatorname{diag}(b_1, ..., b_s)N_1$ and $\operatorname{diag}(a_{s+1}, ..., a_{2n}) = N_2^T \operatorname{diag}(b_{s+1}, ..., b_{2n})N_2$

$\boxed{iii. \Rightarrow ii.}$ Now assume *iii.* and let $\operatorname{diag}(a_1, ..., a_s) = N_1^T \operatorname{diag}(b_1, ..., b_s)N_1$ and similarly let $\operatorname{diag}(a_{s+1}, ..., a_{2n}) = N_2^T \operatorname{diag}(b_{s+1}, ..., b_{2n})N_2$. Let $N = \begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix}$ and $M = A_0^{-1}NB_0$ as well. Then

$$\begin{aligned}
M^{-1}AM &= B_0^{-1}N^{-1}A_0AA_0^{-1}NB_0 \\
&= B_0^{-1}N^{-1}A_0(A_0^{-1}I_{s,t}A_0)A_0^{-1}NB_0 \\
&= B_0^{-1}N^{-1}I_{s,t}NB_0 \\
&= B_0^{-1}\begin{pmatrix} N_1^{-1} & 0 \\ 0 & N_2^{-1} \end{pmatrix}\begin{pmatrix} I_s & 0 \\ 0 & -I_t \end{pmatrix}\begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix}B_0 \\
&= B_0^{-1}\begin{pmatrix} N_1^{-1} & 0 \\ 0 & N_2^{-1} \end{pmatrix}\begin{pmatrix} N_1 & 0 \\ 0 & -N_2 \end{pmatrix}B_0 \\
&= B_0^{-1}I_{s,t}B_0 \\
&= B
\end{aligned}$$

$\boxed{iii. \Rightarrow iv.}$ Assume *iii.* There is a theorem that two symmetric matrices A and B are congruent iff $det(A) = \tau^2 det(B)$ and $c_p(A) = c_p(B)$, where $\tau \in \mathbb{Q}_p^*$ and $c_p(x)$ is the Hasse symbol of x [11, Theorem 7, p. 35]. Given that, then by *iii.*, $a_1...a_s = \tau_1^2 b_1...b_s$ and $a_{s+1}...a_{2n} = \tau_2^2 b_{s+1}...b_{2n}$, where $\tau_1, \tau_2 \in \mathbb{Q}_p^*$ and τ_1, τ_2 may be distinct. Further, $c_p(a_1, a_2, ..., a_s) = c_p(b_1, b_2, ..., b_s)$ and $c_p(a_{s+1}, a_{s+2}, ..., a_{2n}) = c_p(b_{s+1}, b_{s+2}, ..., b_{2n})$.

$\boxed{iv. \Rightarrow iii.}$ Assume *iv.* Then *iii.* follows immediately from the theorem I mentioned above. Q.E.D.

3.2 $\mathbb{R}$ and $\mathbb{F}_p$

Now it is possible to begin classifying the conjugacy classes of involutions themselves (meaning, by abuse of notation, the isomorphism classes of involutions with respect to conjugacy). To that end, the following lemma makes the proof of the third proposition, which will address this issue, much nicer. It states that in the case $\mathrm{SO}(2, k)$, there are two orbits of matrices in $\mathrm{GL}(2, k)$ with respect to congruency.

Lemma 1. *The orbit of* $\mathrm{diag}(\alpha, \beta) \in \mathrm{GL}(2, k)$ *where* $k = \mathbb{F}_p$ *over* $\mathrm{SO}(2, k)$ *is as follows:* $\mathrm{diag}(\alpha, \beta)$ *is congruent to a multiple of* $\mathrm{diag}(1, a^2)$*,* $a \in \mathbb{F}_p^*$*, if the diagonal components of the matrix are both squares of* $\mathbb{F}_p^*$ *or to a multiple of* I_2 *if they are equal, and it is congruent to a multiple of* $\mathrm{diag}(1, c^*)$ *otherwise, where* c^* *is any non-square element of* $\mathbb{F}_p^*$*.*

Proof. Let $A = \mathrm{diag}(a, b)$, $a \neq 0$, $b \neq 0$ and let $C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$. Then $C^TAC = C^T \begin{pmatrix} ac_{11} & ac_{12} \\ bc_{21} & bc_{22} \end{pmatrix} = \begin{pmatrix} ac_{11}^2 + bc_{21}^2 & ac_{12}c_{11} + bc_{22}c_{21} \\ ac_{11}c_{12} + bc_{21}c_{22} & ac_{12}^2 + bc_{22}^2 \end{pmatrix}$

Now, if a and b are both squares of $\mathbb{F}_p$, a^{-1} is also a square so one has $A = a\,\mathrm{diag}(1, a^{-1}b)$, which is in the desired format. So set $C = I_2$ and C^TAC is naturally in the desired format too.

On the other hand, if a is a square but b is not, then one already has obtain a multiple of $\mathrm{diag}(1, c^*)$, where c^* is any non-square of $\mathbb{F}_p$, for by setting $c^* = a^{-1}b$ one obtains $\mathrm{diag}(a, b) = a\,\mathrm{diag}(1, c^*)$. Or, if desired, one can conjugate by $C^* = \mathrm{diag}(a^{-1/2}, a^{1/2})$ to obtain $\mathrm{diag}(1, ab)$ which is also in the needed format.

Also, if a is not a square of $\mathbb{F}_p$ but b is, then if one takes $C = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ then one obtains $\mathrm{diag}(b, a)$, whence one can obtain a multiple of $\mathrm{diag}(1, c^*)$ as before.

The last possibility is that both a and b are not squares of $\mathbb{F}_p$. In that case, if $a = b$, the matrix $A = \mathrm{diag}(a, a) = aI_2$ is already of the desired form. Otherwise, $A = a\,\mathrm{diag}(1, a^{-1}b)$

so in this case A is already in the format $\beta\,\mathrm{diag}(1, c^*)$.

Thus, in every case it turns out that a suitable matrix is an element of $\mathrm{SO}(2n, k)$, which completes the proof. Q.E.D.

Now I am ready to give the first classification of conjugacy classes of involutions, and to prove that it is valid. This result is valid on the fields $k = \mathbb{F}, \mathbb{R}$, or the finite field $\mathbb{F}_p$, where $\mathbb{F}$ is the algebraically closed field of characteristic not equal to two. The proof is tedious, and it uses induction.

Proposition 2. *For $k = \mathbb{F}, \mathbb{R}$, or the finite field $\mathbb{F}_p$, the isomorphy classes of involutions of $\mathrm{SO}(2n, k)$ are as follows:*

1. *If $k = \mathbb{F}$, there is only one $\mathrm{SO}(2n, k)$ conjugacy class for each $\mathrm{GL}(2n, k)$ conjugacy class.*

2. *If $k = \mathbb{R}$, the same thing is true.*

3. *Else if $k = \mathbb{F}_p$ then there are two $\mathrm{SO}(2n, k)$ conjugacy classes for each $\mathrm{GL}(2n, k)$ conjugacy class. The representatives of these classes are $I_{2n}^{-1} I_{s,t} I_{2n} = I_{s,t}$ and $X^{-1} I_{s,t} X$, where $X = \begin{pmatrix} I_{s-1} & 0 & 0 & 0 \\ 0 & \alpha & -\beta & 0 \\ 0 & \beta & \alpha & 0 \\ 0 & 0 & 0 & I_{t-1} \end{pmatrix}$ and $\alpha^2 + \beta^2$ is not a square of $\mathbb{F}_p$ (which implies $p \neq 2$).*

Proof. $\boxed{1.}$ $\forall\ \theta \in \mathrm{Inn}(G), \theta = J_A$ where $A = A_0^{-1} I_{s,t} A_0$ and $A_0 \in \mathrm{GL}(2n, k), A_0^T A_0 = \mathrm{diag}(a_1, ..., a_{2n})$. By Theorem 2, J_A is conjugate to J_B iff $A_0^T A_0$ is congruent to $B_0^T B_0 = \mathrm{diag}(b_1, ..., b_{2n})$, where $B = B_0^{-1} I_{s,t} B_0$. Because $\mathbb{F}$ is algebraically closed, there is a matrix $N \in \mathrm{GL}(2n, k) \ni N^T B_0^T B_0 N = I_{2n}$. For example, let $N = \mathrm{diag}(b_1^{-1/2}, b_2^{-1/2}, \ldots, b_{2n}^{-1/2})$, noting that no $b_i =$ because $\det(B_0^T B_0) \neq 0$ (see part 2 below). Thus, if N^* is $\frac{1}{(\det N)^{1/2n}} N$, $(N^*)^T B_0^T B_0 (N^*) = \frac{1}{(\det N)^{1/4n}} I_{2n}$ and N can be selected such that $N^* \in \mathrm{SO}(2n, k)$. (For example, the N I gave above has this property, which would mean $(N^*)^{-1} = (N^*)^T$.)

Ergo, $A_0^T(N^*)^T B_0^T B_0 N^* A_0 = \frac{1}{\xi} A_0^T I_{2n} A_0$ where ξ is some positive power of $(\det N)^{-1} \Rightarrow (\xi^{1/2n} N^* A_0)^T B_0^T B_0 (\xi^{1/2n} N^* A_0) = A_0^T A_0$ so J_A is conjugate to J_B.

$\boxed{2.}$ Let J_A, J_B, A, and B be defined as in the proof of **1.** Then since J_B is an involution, the product $B_0^T B_0$ is positive definite, so $\forall\ i \in \{1, 2, ..., 2n\}, b_i > 0$. Let $C = (c_{ij})$ be a $2n \times 2n$ matrix. Then $C^T B_0^T B_0 C =$

$$\begin{pmatrix} c_{11}b_1 & c_{21}b_2 & \dots & c_{2n,1}b_n \\ c_{12}b_1 & c_{22}b_2 & \dots & c_{2n,2}b_n \\ \vdots & \vdots & \ddots & \vdots \\ c_{1,2n}b_1 & c_{2,2n}b_2 & \dots & c_{2n,2n}b_n \end{pmatrix} C$$

$$= \begin{pmatrix} c_{11}^2 b_1 + c_{21}^2 b_2 + \ldots + c_{2n,1}^2 b_n & \dots & c_{11}b_1c_{12} + \ldots + c_{2n,1}b_nc_{2n,2} \\ \vdots & \ddots & \vdots \\ c_{1,2n}b_1c_{11} + c_{2,2n}b_2c_{21} + \ldots + c_{2n,2n}b_nc_{2n,1} & \dots & c_{1,2n}^2 b_1 + \ldots + c_{2n,2n}^2 b_n \end{pmatrix}$$

If $\forall\ i \in \{1, 2, ..., 2n\}$ one sets $c_{ii} = \dfrac{1}{\sqrt{b_i}}$ and if for all $i \neq j$ one sets $c_{ij} = 0$, then the result will be I_{2n}. Additionally, $C \in \mathrm{GL}(2n, k)$. (Because the product $B_0^T B_0$ is positive definite, $\forall\ i \in \{1, 2, ..., 2n\}, b_i > 0$ so $\sqrt{b_k} \in \mathbb{R}$.) As a result, one can replace C with $C^* = \frac{1}{(\det C)^{1/2n}} C$ to get $\frac{1}{(\det C)^{1/2n}} I_{2n}$, so by Proposition 2 J_A is conjugate to J_B.

$\boxed{3.}$ I will first prove this result for $s = 2$ on $\mathrm{SO}(2n, k)$ and then proceed inductively. The $s = 1$ case is clear because then the upper-left $s \times s$ block consists of a single entry, and if that entry of a_1 is a square one can use the "matrix" $C = (a_1^{-1/2})$ to get the desired result. Otherwise, it is in the desired form already. Let J_A be any involution on $\mathrm{SO}(2n, k)$ where $A = A_0^{-1} I_{s,t} A_0$ and the $s \times s$ upper-left corner of $A_0^T A_0 = \mathrm{diag}(a, b)$, and $s = 2$. Then by the Lemma proved before this proposition, that part of $A_0^T A_0$ is congruent to a multiple of $\mathrm{diag}(1, \alpha^2)$, where $\alpha \in \mathbb{F}_p^*$, if the diagonal components of the matrix are both squares of $\mathbb{F}_p^*$ or are equal and it is congruent to a multiple of $\mathrm{diag}(1, c^*)$ otherwise, where c^* is any non-square element of $\mathbb{F}_p^*$. Therefore, these are the two conjugacy classes of involutions of $\mathrm{SO}(2n, k)$.

Now assume the result is true for $m = 1, 2, ..., s-1$. For simplicity, let $s = m$. Working on the $s \times s$ case, I will make a proof for the $(s-1) \times (s-1)$ block in the upper-left corner, and note that the result is similar for the other part of the diagonal matrix $A_0^{-1}A_0$. In that case, let J_A be any involution on $\mathrm{SO}(2n,k)$ where $A = A_0^{-1}I_{s,t}A_0$. Also let $A_0^TA_0 = \mathrm{diag}(a_1,...,a_s)$. Then by considering the $(s-1)\times(s-1)$ block in the upper-left corner, it is assumed that $\mathrm{diag}(a_1,...,a_s) \cong \varepsilon\,\mathrm{diag}(1,...,\alpha^2,a_s^*)$ or $\mathrm{diag}(a_1,...,a_s) \cong \varepsilon\,\mathrm{diag}(1,...,c^*,a_s^*)$ where c^* is not a square of $\mathbb{F}_p$ and α and ε are elements of $\mathbb{F}_p^*$.

By abuse of notation, call a_s^* a_s. If a_s is a square, then $\varepsilon\,\mathrm{diag}(1,...,c^*,a_s) \cong \varepsilon\alpha\,\mathrm{diag}(1,\ldots,1,d^*)$, where d^* is not a square of $\mathbb{F}_p$. Also,

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & -1 \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}^T \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & c^* & 0 \\ 0 & 0 & \ldots & 0 & a_s \end{pmatrix} \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & -1 \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & a_s & 0 \\ 0 & 0 & \ldots & 0 & c^* \end{pmatrix} \cong \varepsilon \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & c^{**} \end{pmatrix}$$ by the inductive hypothesis, where c^{**} is a non-square element of $\mathbb{F}_p$.

Else if a_s is not a square, if $\mathrm{diag}(a_1,\ldots,a_s) \cong \varepsilon\,\mathrm{diag}(1,\ldots,\alpha^2,a_s)$ then I am already done because I can use the inductive hypothesis on the 2×2 lower-right corner of the matrix to get a multiple of $\mathrm{diag}(1,1,\ldots,1,a_s)$. Else if $\mathrm{diag}(a_1,...,a_s) \cong \varepsilon\,\mathrm{diag}(1,...,c^*,a_s)$ then by the inductive hypothesis taken in the lower-right $(s-1)\times(s-1)$ corner, the matrix is congruent to a multiple of $\mathrm{diag}(1,\ldots,1,c^{**})$, where c^{**} is a non-square element of $\mathbb{F}_p$, which is the desired form.

A similar result holds for the $t\times t$ block in the lower-right corner, so by Proposition 2, there are two conjugacy classes of involutions, with all the desired properties. Note that $\det(A_0A_0^T)$ equals the determinant of the upper-left $s\times s$ block times the determinant of the lower-right $t\times t$ block, and $\det(A_0A_0^T) = 1$ modulo a square, so the same must be true of each of the two blocks. To get a matrix of the desired shape, notice that one can just as well have the nonsquare entry of the lower-right $t \times t$ block be in the upper-left corner instead of the lower-right corner. Q.E.D.

The conjugacy classes of involutions over the reals can be found in Lemma 15 in a later chapter.

Chapter 4

Involution Isomorphy Classes with Respect to Conjugation Classes over $\mathrm{SO}(2n, k)$ where $k = \mathbb{Q}_p$

4.1 A Brief Introduction to $\mathbb{Q}_p$

Definition 3. *If F is a field, then a "valuation" is a mapping $|\ |: F \to \mathbb{R}$ such that for all $\alpha, \beta \in F$, the following are true:*

i. $|\alpha| \geq 0$

ii. $|\alpha| = 0 \Leftrightarrow \alpha = 0$

iii. $|\alpha\beta| = |\alpha||\beta|$

iv. $|\alpha + \beta| \leq |\alpha| + |\beta|$

This definition is taken from Gerstein, but it can be found in many other books [3, p. 51].

Given that, the p-adic numbers are defined as follows:

Definition 4. *The "p-adic valuation" $|\ |_p$ on $\mathbb{Q}$ is defined as follows: $|0|_p = 0$ and $\forall\ \alpha \in \mathbb{Q}^*$, if $\alpha = p^\ell \frac{a}{b}$ where a, b, $\ell \in \mathbb{Z}$ and $\frac{a}{b}$ is in lowest terms (so a and b are relatively prime) then*

$|\alpha|_p = p^{-\ell}$ [3, p. 52]. With that, the "p-adic numbers" $\mathbb{Q}_p$ are the completion of the rational numbers $\mathbb{Q}$ with respect to the p-adic valuation [3, p. 61]. Similarly, the "p-adic integers" are the p-adic numbers α such that $|\alpha|_p \leq 1$ [3, pp. 64, 66].

The following lemma is taken from Burton [6, pp. 27-28]. It depends on the Hilbert symbol, Legendre symbol, and Hasse symbol, and these are defined as follows:

Definition 5. *Let a be an integer and let p be a prime number. Then the Legendre symbol*

$$(a|p) \equiv \begin{cases} 0 & if\ a \equiv 0\ (mod\ p) \\ 1 & if\ a \not\equiv 0\ (mod\ p)\ and\ \exists\ x \in \mathbb{Z}\ such\ that\ x^2 \equiv a\ (mod\ p) \\ -1 & otherwise \end{cases}$$

Definition 6. *Let α and β be elements of $\mathbb{Q}_p$. Then the Hilbert symbol*

$$(\alpha, \beta)_p \equiv \begin{cases} 1, & x^2\alpha + y^2\beta = 1\ has\ a\ solution\ in\ \mathbb{Q}_p \\ -1, & otherwise \end{cases}$$

Definition 7. *The Hasse symbol over $\mathbb{Q}_p$ is defined as*

$$c_p(a_1, \ldots, a_s) \equiv (-1, -a_1 \ldots a_s)_p \prod_{i=1}^{s-1} (a_1 \ldots a_i, -a_1 \ldots a_{i+1})_p$$

The original definition actually corresponds to determinants of matrices, but all of the relevant matrices in this thesis are diagonal, so for my purposes the above one suffices. In the general definition, one takes successive determinants of blocks in the upper-left corner of the same matrix. Then by replacing every term $a_1 \ldots a_j$ with $\det A_{jj}$, where A_{jj} is the $j \times j$ upper-left block of the matrix A, one can recover the original definition from the above.

4.2 Computational Results

4.2.1 Results on the Hilbert Symbol

Lemma 2. *Let $\alpha, \beta, \gamma, \rho$, and σ be nonzero numbers in the p-adic field $\mathbb{Q}_p$. Let $(\alpha|p)$ be the value of the Legendre symbol $(\alpha_0|p)$ where α_0 is the first term in the p-adic expansion of α. Also let $(\alpha, \beta)_\infty$ be the value of the Hilbert symbol over $\mathbb{R}$ and let $(\alpha, \beta)_p$ be the value of the Hilbert symbol in $\mathbb{Q}_p$. Then we have the following:*

1. *$(\alpha,\beta)_\infty = 1$ unless $\alpha < 0$ and $\beta < 0$*

2. *$(\alpha,\beta)_p = (\beta,\alpha)_p$*

3. *$(\alpha\rho^2,\beta\sigma^2)_p = (\alpha,\beta)_p$*

4. *$(\alpha,-\alpha)_p = 1$*

5. *If $\alpha = p^n a_1$ and $\beta = p^m b_1$ with a_1 and b_1 units then:*

- ***i.*** *if p is odd then $(\alpha,\beta)_p = (-1|p)^{nm}(a_1|p)^m(b_1|p)^n$*
- ***ii.*** *else if $p = 2$, then $(\alpha,\beta)_p = (2|a_1)^m(2|b_1)^n(-1)^{\frac{(a_1-1)(b_1-1)}{4}}$*

6. *If p is prime to $2\alpha\beta$, $(\alpha,\beta)_p = 1$ for $p \neq \infty$ provided α and β are p-adic integers.*

7. *$(\alpha,\beta)_p(\alpha,\gamma)_p = (\alpha,\beta\gamma)_p$*

8. *$(\alpha,\alpha)_p = (\alpha,-1)_p$*

9. *$(\alpha\rho,\beta\rho)_p = (\alpha,\beta)_p(\rho,-\alpha\beta)_p$*

10. *If β is not a square in $\mathbb{Q}_p$ and $c = \pm 1$ then for each prime p there is an integer α such that $(\alpha,\beta)_p = c$. Furthermore, if m as defined in property 5 is odd, then such an α can be found that is prime to p.*

11. *If a and b are in $\mathbb{Q}^*$, the set of non-zero rational numbers, then*

$$\prod_{p \text{ prime and } p = \infty} (a,b)_p = 1$$

This lemma is a known result, so all proof is omitted [6, pp. 27-28].

This next lemma is helpful in the case $-1 \notin \mathbb{Q}_p^{*2}$.

Lemma 3. *If $p \neq 2$ and $-1 \notin \mathbb{Q}_p^{*2}$, $(p^{\pm 1}, p^{\pm 1})_p = -1$, $(p,p^{-1})_p = 1$, $(-p^{\pm 1}, -p^{\pm 1})_p = -1$, and $(-p,-p^{-1})_p - = 1$. Further, $(-1,-1)_p = 1$, $(p,-p^2)_p = -1$, $(p^{-1},-p^{-2}) = -1$, and $(-1,-p^2)_p = 1$.*

Proof. These results can all be verified with Lemma 2. By item 5 of Lemma 2, $(p,p)_p = (-1|p)^1(1|p)^1(1|p)^1 = -1\cdot 1\cdot 1 = -1$, $(-p,-p)_p = (-1|p)^1(-1|p)^1(-1|p)^1 = -1\cdot(-1)\cdot(-1) = -1$, $(p^{-1},p^{-1})_p = (-1|p)^1(1|p)^{-1}(1|p)^{-1} = -1\cdot 1\cdot 1 = -1$, $(-p^{-1},-p^{-1})_p = (-1|p)^1(-1|p)^{-1}(-1|p)^{-1} = -1\cdot(-1)\cdot(-1) = -1$, and $(p,p^{-1})_p = (p,p)_p = -1$ and $(-p,-p^{-1})_p = (-p,-p)_p = -1$ by item 3 of Lemma 2.

Furthermore, $(-1,-1)_p = 1$ because -1 is a p-adic integer and p is prime to $2(-1)(-1) = 2$ by assumption, so part 6 of Lemma 2 holds. Furthermore, by Lemma 2, $(p,-p^2)_p = (-1|p)^2(1|p)^2(-1|p)^1 = (-1)^2\cdot 1^1\cdot(-1)^1 = -1$. For similar reasons, $(p^{-1},-p^{-2}) = -1$. In addition, $(-1,-p^2)_p = 1$ because by property 7 of Lemma 2, $(-1,-p^2)_p = (-1,-1)_p(-1,p^2)_p = 1\cdot 1 = 1$. Q.E.D.

Similarly, the following lemma is helpful in the case $k = \mathbb{Q}_2$

Lemma 4. *Let* $k = \mathbb{Q}_2$*. Then* $(-1,-1)_2 = -1$*,* $(-1,\pm 3)_2 = \mp 1$*,* $(-1,\pm 2)_2 = \pm 1$*, and* $(-1,\pm 6)_2 = \mp 1$*. Also,* $(2,\pm 3)_2 = -1$*.*

Proof. These statements are proven using the results of Serre [10, pp. 18-20]. Specifically, he gives the following: if $a = 2^\alpha u$, $b = 2^\beta v$, where u and v are 2-adic units, then [10, p. 20]

$$(a,b)_2 = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)}$$

In the above, ε and ω are defined as follows: $\varepsilon(u) \equiv \dfrac{u-1}{2} \pmod 2$, $\omega(u) \equiv \dfrac{u^2-1}{8} \pmod 2$ [10, p. 18].

In that case, we have the following:

i. $\varepsilon(-1) \equiv \frac{-1-1}{2} \pmod 2 = 1$, $\omega(-1) \equiv \frac{(-1)^2-1}{8} \pmod 2 = 0$

ii. $\varepsilon(-3) \equiv \frac{-3-1}{2} \pmod 2 = 0$, $\omega(-3) \equiv \frac{(-3)^2-1}{8} \pmod 2 = 1$

iii. $\varepsilon(3) \equiv \frac{3-1}{2} \pmod 2 = 1$, $\omega(3) \equiv \frac{(3)^2-1}{8} \pmod 2 = 1$

Therefore, $(-1,-1)_2 = (-1)^{1\cdot 1+0\cdot 0+0\cdot 0} = -1$, $(-1,-3)_2 = (-1)^{1\cdot 0+0\cdot 1+0\cdot 0} = 1$, and $(-1,3)_2 = (-1)^{1\cdot 1+0\cdot 1+0\cdot 0} = -1$. Furthermore, $(-1,2)_2 = (-1)^{1\cdot 0+0\cdot 0+1\cdot 0} = 1$, $(-1,-2)_2 = (-1)^{1\cdot 1+0\cdot 0+1\cdot 0} = -1$, $(-1,6)_2 = (-1)^{1\cdot 1+0\cdot 1+1\cdot 0} = -1$, and $(-1,-6)_2 = (-1)^{1\cdot 0+0\cdot 1+1\cdot 0} = 1$. Lastly, $(2,3)_2 = (-1)^{0\cdot 1+1\cdot 1+0\cdot 0} = -1$ and $(2,-3)_2 = (-1)^{0\cdot 0+1\cdot 1+0\cdot 0} = -1$. Q.E.D.

4.2.2 The Classification Lemmas that Show What is Possible for $A_0A_0^T = \mathrm{diag}(\zeta_1, \ldots, \zeta_{2n})$ from Proposition 1

The above results are useful in proving what the conjugacy classes of involutions are in the case $k = \mathbb{Q}_p$. The three lemmas below are different: both of them show that there are restrictions on these conjugacy classes. Each of the conjugacy classes comes from the involution J_A, $A = A_0^{-1}I_{s,t}A_0$ and $A_0A_0^T$ is diagonal, as proved over general fields in Proposition 1.

Below there are several results that show there are restrictions on what values one can select for $A_0A_0^T$. Firstly, there is a well-known result about the square classes of $\mathbb{Q}_p$ that shows that if $p \neq 2$, there are four such square classes, and otherwise there are eight. First, a definition is needed.

Definition 8. *Over $\mathbb{Q}$, if $|x - y|_p \leq 1/g$ (so g divides $x - y$), then $x \equiv y \pmod{g}$ and we say "x is congruent to y modulo g." If x is congruent modulo g to the square of a rational integer, then x is a "quadratic residue modulo g," otherwise it is a "quadratic non-residue modulo g." This notation comes from Mahler [7, p. 67].*

It is a known fact that if $p > 2$ is prime, not all integers relatively prime to p are quadratic residues modulo p, so there is a smallest such number N_p that is a quadratic non-residue modulo p [7, p. 68]. This element will turn out to be a non-square of $\mathbb{Q}_p$, $p > 2$, and the square classes of $\mathbb{Q}_p$ are as follows:

Classification Lemma 1. *The non-squares of $\mathbb{Q}_2$ are represented by the elements -1, ± 2, ± 3, and ± 6. If $p > 2$, the non-squares of $\mathbb{Q}_p$ are represented by N_p, p, and pN_p. This means that there are seven distinct quadratic extensions of $\mathbb{Q}_2$, viz., $\mathbb{Q}_2(\sqrt{-1})$, $\mathbb{Q}_2(\sqrt{2})$, $\mathbb{Q}_2(\sqrt{-2})$, $\mathbb{Q}_2(\sqrt{3})$, $\mathbb{Q}_2(\sqrt{-3})$, $\mathbb{Q}_2(\sqrt{6})$, and $\mathbb{Q}_2(\sqrt{-6})$. Also, there are three distinct quadratic extensions of $\mathbb{Q}_p$ if $p > 2$, and they are $\mathbb{Q}_p(\sqrt{N_p})$, $\mathbb{Q}_p(\sqrt{p})$, and $\mathbb{Q}_p(\sqrt{pN_p})$. Note that if $-1 \notin \mathbb{Q}_p^{*2}$ then one can use -1 in place of N_p, as I did below.*

Proof. This result can be found in Mahler [7, Theorem 1 on p. 72]. Q.E.D.

Each remaining classification lemma below shows that there are restrictions on what diagonal elements are allowed in $A_0 A_0^T$. These restrictions vary according to whether $p \equiv 1 \pmod 4$, $p \equiv 3 \pmod 4$, or $p = 2$.

Classification Lemma 2. *Let $p \neq 2$, let $a_1, \ldots, a_s \in \mathbb{Q}_p^*$. Then if $c_p(a_1, \ldots, a_s) = -1$, in the case $-1 \in \mathbb{Q}_p^{*2}$ it is impossible that there are not at least two a_i's in distinct square classes of $\mathbb{Q}_p$. In the case $-1 \notin \mathbb{Q}_p^{*2}$, it is impossible that every non-square is in the same square class as -1.*

Proof. Assume in fact that $a_1 \ldots a_s = \xi$, where $\xi \in \mathbb{Q}_p^*$, $c_p(a_1, \ldots, a_s) = -1$, and that all non-square a_i's are in the same square class. Then by the definition of the Hasse symbol,
$c_p(a_1, \ldots, a_s) = (-1, \xi)_p \prod_{i=1}^{s-1} (a_1 \ldots a_i, -a_1 \ldots a_{i+1})_p$
$= (-1, \xi)_p (a_1, -a_1)_p (a_1, a_2)_p (a_1 a_2, -a_1 a_2)_p (a_1 a_2, a_3)_p \ldots (a_1 \ldots a_{s-1}, -a_1 \ldots a_{s-1})_p$
$(a_1 \ldots a_{s-1}, a_s)_p$
$= (-1, \xi)_p (a_1, a_2)_p (a_1 a_2, a_3)_p (a_1 a_2 a_3, a_4)_p \ldots (a_1 \ldots a_{s-1}, a_s)_p$

Now, if in any of the above terms on either side of the Hilbert symbol is a square, the value of the Hilbert symbol will be one, so such terms may be cancelled out. In the other terms, one obtains a non-square on either side of the Hilbert symbol, and these non-squares may be distinct. Assume that we have m such terms, and label these nonsquares N_{p_i} and $N_{p_i}^*$ as follows:

$$c_p(a_1, \ldots, a_s) = (-1, \xi)_p (N_{p_1}, N_{p_1}^*)_p (N_{p_2}, N_{p_2}^*)_p \ldots (N_{p_m}, N_{p_m}^*)_p$$

$\forall\ i \in \{1, \ldots, m\}$, N_{p_i} and $N_{p_i}^*$ are in the same square class by assumption so they differ by a square. Hence, $(N_{p_i}, N_{p_i}^*)_p = (N_{p_i}, N_{p_i})_p = (N_{p_1}, N_{p_1})_p$. Further, by part 8 of Lemma 2, $(-1, \xi)_p = (\xi, \xi)_p$, and ξ may or may not be a square. If it is not, then it is in the same square class as N_{p_i}. As a result, one obtains $c_p(a_1, \ldots, a_s) = (N_{p_1}, N_{p_1})_p^m$ or $c_p(a_1, \ldots, a_s) = (N_{p_1}, N_{p_1})_p^{m+1}$, and since it is of little practical significance, by abuse of notation assume $c_p(a_1, \ldots, a_s) = (N_{p_1}, N_{p_1})_p^m$.

If $-1 \in \mathbb{Q}_p^{*2}$, it follows that $c_p(a_1, \ldots, a_s) = (N_{p_1}, N_{p_1})_p^m$. But by property 8 of Lemma 2, $(N_{p_1}, N_{p_1})_p = (N_{p_1}, -1)_p = 1$ so $(N_{p_1}, N_{p_1})_p^m = 1$, but this violates my original assumption that $c_p(a_1, \ldots, a_s) = -1$.

If $-1 \notin \mathbb{Q}_p^{*2}$, then by the assumptions of the Lemma, $c_p(a_1, \ldots, a_s) = (-1,-1)_p^m$. But by Lemma 2, property 6, $(-1,-1)_p = 1 \Rightarrow (-1,-1)_p^m = 1$, but again this violates my original assumption that $c_p(a_1, \ldots, a_s) = -1$. Q.E.D.

Classification Lemma 3. *If $A_0 A_0^T = B \in \mathrm{GL}(n,k)$ then $A_0 \in \mathrm{GL}(n,k)$ is possible iff $\sqrt{\det B} \in k$. If $A_0 \notin \mathrm{GL}(n,k)$ then $A_0 \in \mathrm{GL}(n,\bar{k})$ and $A_0 \in \mathrm{GL}(n,F)$ if F is k extended quadratically to the greatest possible extent.*

Proof. $\det A_0 = \det A_0^T$ and $\det(A_0 A_0^T) = \det B \in \mathrm{GL}(n,k)$ so $\det(A_0)^2 = \det B \Rightarrow \det A_0 = \sqrt{\det B}$. Now, the formula for the determinant is a linear combination of elements in k, so if every element of A_0 is in k then $\det A_0 \in k$. Therefore, if $\det A_0 \notin k$ then not every element of A_0 is in k. As a result, if $\sqrt{\det B} \in k$ then $A_0 \in \mathrm{GL}(n,k)$ is possible, else if $\sqrt{\det B} \notin k$ then $A_0 \in \mathrm{GL}(n,\bar{k})$, $A_0 \in \mathrm{GL}(n,F)$ and $A_0 \notin \mathrm{GL}(n,k)$. Q.E.D.

4.3 The Isomorphy Classes over $\mathbb{Q}_p$

Here are the isomorphy classes. Note that Classification Lemma 2 implies there is a restriction on what elements one can and cannot put on the diagonal.

Proposition 3. *Let the field under consideration be $k = \mathbb{Q}_p$, where $-1 \in \mathbb{Q}_p^{*2}$, $p \neq 2$, and $N_p \notin \mathbb{Q}_p^{*2}$. Then the conjugacy classes of involutions J_B of $\mathrm{SO}(2n,k)$, where $B = B_0^{-1} I_{s,t} B_0$, depend on the values of $\det(\mathrm{diag}(b_1, \ldots, b_s))$, $\det(\mathrm{diag}(b_{s+1}, \ldots, b_{2n}))$, $c_p(b_1, \ldots, b_s)$, and $c_p(b_{s+1}, \ldots, b_{2n})$ in the following way: firstly, because of Classification Lemma 3, the only way in which corresponding $B_0 B_0^T$ can exist in $\mathrm{SO}(2n,k)$ as opposed to $\mathrm{SO}(2n,\bar{k})$ is if $\det(B_0 B_0^T)$ is a square. That means $\det(\mathrm{diag}(b_1, \ldots, b_s)) = \det(\mathrm{diag}(b_{s+1}, \ldots, b_{2n}))$ if they are non-squares, and they can both be set equal to one if they are squares. Then the conjugacy classes of involutions are given by Table 4.1.*

Table 4.1: The conjugacy classes of $\mathrm{SO}(2n,k)$ *where* $k=\mathbb{Q}_p$ *and* $-1\in\mathbb{Q}_p^{*2}$*. This table corresponds with Proposition 3.*

Item	$b_1\dots b_s$	$b_{s+1}\dots b_{2n}$	$c_p(b_1,\dots,b_s)$
Item	$c_p(b_{s+1},\dots,b_{2n})$	$\mathrm{diag}(b_1,\dots,b_s)$	$\mathrm{diag}(b_{s+1},\dots,b_{2n})$
1	1	1	1
1	1	I_s	I_t
2	1	1	1
2	-1	I_s	$\mathrm{diag}(1,\dots,1,p,N_p,p^{-1}N_p^{-1})$
3	1	1	-1
3	1	$\mathrm{diag}(1,\dots,1,p,N_p,p^{-1}N_p^{-1})$	I_t
4	1	1	-1
4	-1	$\mathrm{diag}(1,\dots,1,p,N_p,p^{-1}N_p^{-1})$	$\mathrm{diag}(1,\dots,1,p,N_p,p^{-1}N_p^{-1})$
5	N_p	N_p	1
5	1	$\mathrm{diag}(1,\dots,1,N_p)$	$\mathrm{diag}(1,\dots,1,N_p)$
6	N_p	N_p	1
6	-1	$\mathrm{diag}(1,\dots,1,N_p)$	$\mathrm{diag}(1,\dots,1,p,p^{-1}N_p)$
7	N_p	N_p	-1
7	1	$\mathrm{diag}(1,\dots,1,p,p^{-1}N_p)$	$\mathrm{diag}(1,\dots,1,N_p)$
8	N_p	N_p	-1
8	-1	$\mathrm{diag}(1,\dots,1,p,p^{-1}N_p)$	$\mathrm{diag}(1,\dots,1,p,p^{-1}N_p)$
9	p	p	1
9	1	$\mathrm{diag}(1,\dots,1,p)$	$\mathrm{diag}(1,\dots,1,p)$
10	p	p	1
10	-1	$\mathrm{diag}(1,\dots,1,p)$	$\mathrm{diag}(1,\dots,1,N_p,pN_p^{-1})$
11	p	p	-1

Table 4.1: Continued

Item	$b_1 \ldots b_s$	$b_{s+1} \ldots b_{2n}$	$c_p(b_1, \ldots, b_s)$
Item	$c_p(b_{s+1}, \ldots, b_{2n})$	$\mathrm{diag}(b_1, \ldots, b_s)$	$\mathrm{diag}(b_{s+1}, \ldots, b_{2n})$
11	1	$\mathrm{diag}(1, \ldots, 1, N_p, pN_p^{-1})$	$\mathrm{diag}(1, \ldots, 1, p)$
12	p	p	-1
12	-1	$\mathrm{diag}(1, \ldots, 1, N_p, pN_p^{-1})$	$\mathrm{diag}(1, \ldots, 1, N_p, pN_p^{-1})$
13	pN_p	pN_p	1
13	1	$\mathrm{diag}(1, \ldots, 1, pN_p)$	$\mathrm{diag}(1, \ldots, 1, pN_p)$
14	pN_p	pN_p	1
14	-1	$\mathrm{diag}(1, \ldots, 1, pN_p)$	$\mathrm{diag}(1, \ldots, 1, p, N_p)$
15	pN_p	pN_p	-1
15	1	$\mathrm{diag}(1, \ldots, 1, p, N_p)$	$\mathrm{diag}(1, \ldots, 1, pN_p)$
16	pN_p	pN_p	-1
16	-1	$\mathrm{diag}(1, \ldots, 1, p, N_p)$	$\mathrm{diag}(1, \ldots, 1, p, N_p)$

Proof. The proof is entirely computational, so it has been omitted. One need only check that all of my calculations are correct. And please remember, reader, whoever you are, that it is extremely easy to make typos that are hard to spot when typing something like this. Q.E.D.

Proposition 4. *Let the field under consideration be $k = \mathbb{Q}_p$, where $-1 \notin \mathbb{Q}_p^{*2}$ and $p \neq 2$. Then the conjugacy classes of involutions J_B of $\mathrm{SO}(2n, k)$, where $B = B_0^{-1} I_{s,t} B_0$, depend on the values of $\det(\mathrm{diag}(b_1, \ldots, b_s))$, $\det(\mathrm{diag}(b_{s+1}, \ldots, b_{2n}))$, $c_p(b_1, \ldots, b_s)$, and $c_p(b_{s+1}, \ldots, b_{2n})$ in the following way: firstly, because of Classification Lemma 3, the only way in which corresponding $B_0 B_0^T$ can exist in $\mathrm{SO}(2n, k)$ as opposed to $\mathrm{SO}(2n, \bar{k})$ is if $\det(B_0 B_0^T)$ is a square. That means $\det(\mathrm{diag}(b_1, \ldots, b_s)) = \det(\mathrm{diag}(b_{s+1}, \ldots, b_{2n}))$ if they are non-squares, and they can both be set equal to one if they are squares. Then the conjugacy classes of involutions are given by Table 4.2.*

Table 4.2: The conjugacy classes of $\mathrm{SO}(2n, k)$ *where* $k = \mathbb{Q}_p$ *and* $-1 \notin \mathbb{Q}_p^{*2}$. *This table corresponds with Proposition 4.*

Item	$b_1 \dots b_s$	$b_{s+1} \dots b_{2n}$	$c_p(b_1, \dots, b_s)$
Item	$c_p(b_{s+1}, \dots, b_{2n})$	$\mathrm{diag}(b_1, \dots, b_s)$	$\mathrm{diag}(b_{s+1}, \dots, b_{2n})$
1	1	1	1
1	1	I_s	I_t
2	1	1	1
2	-1	I_s	$\mathrm{diag}(1, \dots, 1, p, p^{-1})$
3	1	1	-1
3	1	$\mathrm{diag}(1, \dots, 1, p, p^{-1})$	I_t
4	1	1	-1
4	-1	$\mathrm{diag}(1, \dots, 1, p, p^{-1})$	$\mathrm{diag}(1, \dots, 1, p, p^{-1})$
5	-1	-1	1
5	1	$\mathrm{diag}(1, \dots, 1, -1)$	$\mathrm{diag}(1, \dots, 1, -1)$
6	-1	-1	1
6	-1	$\mathrm{diag}(1, \dots, 1, -1)$	$\mathrm{diag}(1, \dots, 1, p, -p^{-1})$
7	-1	-1	-1
7	1	$\mathrm{diag}(1, \dots, 1, p, -p^{-1})$	$\mathrm{diag}(1, \dots, 1, -1)$
8	-1	-1	-1
8	-1	$\mathrm{diag}(1, \dots, 1, p, -p^{-1})$	$\mathrm{diag}(1, \dots, 1, p, -p^{-1})$
9	p	p	1
9	1	$\mathrm{diag}(1, \dots, 1, -1, -p)$	$\mathrm{diag}(1, \dots, 1, -1, -p)$
10	p	p	1
10	-1	$\mathrm{diag}(1, \dots, 1, -1, -p)$	$\mathrm{diag}(1, \dots, 1, p)$
11	p	p	-1

Table 4.2: Continued

Item	$b_1 \ldots b_s$	$b_{s+1} \ldots b_{2n}$	$c_p(b_1, \ldots, b_s)$
Item	$c_p(b_{s+1}, \ldots, b_{2n})$	$\operatorname{diag}(b_1, \ldots, b_s)$	$\operatorname{diag}(b_{s+1}, \ldots, b_{2n})$
11	1	$\operatorname{diag}(1, \ldots, 1, p)$	$\operatorname{diag}(1, \ldots, 1, -1, -p)$
12	p	p	-1
12	-1	$\operatorname{diag}(1, \ldots, 1, p)$	$\operatorname{diag}(1, \ldots, 1, p)$
13	$-p$	$-p$	1
13	1	$\operatorname{diag}(1, \ldots, 1, -1, p)$	$\operatorname{diag}(1, \ldots, 1, -1, p)$
14	$-p$	$-p$	1
14	-1	$\operatorname{diag}(1, \ldots, 1, -1, p)$	$\operatorname{diag}(1, \ldots, 1, -p)$
15	$-p$	$-p$	-1
15	1	$\operatorname{diag}(1, \ldots, 1, -p)$	$\operatorname{diag}(1, \ldots, 1, -1, p)$
16	$-p$	$-p$	-1
16	-1	$\operatorname{diag}(1, \ldots, 1, -p)$	$\operatorname{diag}(1, \ldots, 1, -p)$

Proposition 5. *Let the field under consideration be $k = \mathbb{Q}_2$. Then the conjugacy classes of involutions J_B of* $\mathrm{SO}(2n, k)$*, where $B = B_0^{-1} I_{s,t} B_0$, depend on the values of* $\det(\operatorname{diag}(b_1, \ldots, b_s))$, $\det(\operatorname{diag}(b_{s+1}, \ldots, b_{2n}))$, $c_p(b_1, \ldots, b_s)$*, and* $c_p(b_{s+1}, \ldots, b_{2n})$ *in the following way: firstly, because of Classification Lemma 3, the only way in which corresponding $B_0 B_0^T$ can exist in* $\mathrm{SO}(2n, k)$ *as opposed to* $\mathrm{SO}(2n, \bar{k})$ *is if* $\det(B_0 B_0^T)$ *is a square. That means* $\det(\operatorname{diag}(b_1, \ldots, b_s)) = \det(\operatorname{diag}(b_{s+1}, \ldots, b_{2n}))$ *if they are non-squares, and they can both be set equal to one if they are squares. Then the conjugacy classes of involutions are given by Table 4.3.*

Table 4.3: The conjugacy classes of $\mathrm{SO}(2n, k)$ *where $k = \mathbb{Q}_2$. This table corresponds with Proposition 5.*

Item	$b_1 \ldots b_s$	$b_{s+1} \ldots b_{2n}$	$c_p(b_1, \ldots, b_s)$
Item	$c_p(b_{s+1}, \ldots, b_{2n})$	$\operatorname{diag}(b_1, \ldots, b_s)$	$\operatorname{diag}(b_{s+1}, \ldots, b_{2n})$
1	1	1	1

Table 4.3: Continued

Item	$b_1 \dots b_s$	$b_{s+1} \dots b_{2n}$	$c_p(b_1, \dots, b_s)$
Item	$c_p(b_{s+1}, \dots, b_{2n})$	$\mathrm{diag}(b_1, \dots, b_s)$	$\mathrm{diag}(b_{s+1}, \dots, b_{2n})$
1	1	$\mathrm{diag}(1, \dots, 1, -1, -1)$	$\mathrm{diag}(1, \dots, 1, -1, -1)$
2	1	1	1
2	-1	$\mathrm{diag}(1, \dots, 1, -1, -1)$	I_t
3	1	1	-1
3	1	I_s	$\mathrm{diag}(1, \dots, 1, -1, -1)$
4	1	1	-1
4	-1	I_s	I_t
5	-1	-1	1
5	1	$\mathrm{diag}(1, \dots, 1, -1)$	$\mathrm{diag}(1, \dots, 1, -1)$
6	-1	-1	1
6	-1	$\mathrm{diag}(1, \dots, 1, -1)$	$\mathrm{diag}(1, \dots, 1, 3, -3^{-1})$
7	-1	-1	-1
7	1	$\mathrm{diag}(1, \dots, 1, 3, -3^{-1})$	$\mathrm{diag}(1, \dots, 1, -1)$
8	-1	-1	-1
8	-1	$\mathrm{diag}(1, \dots, 1, 3, -3^{-1})$	$\mathrm{diag}(1, \dots, 1, 3, -3^{-1})$
9	2	2	1
9	1	$\mathrm{diag}(1, \dots, 1, -1, -2)$	$\mathrm{diag}(1, \dots, 1, -1, -2)$
10	2	2	1
10	-1	$\mathrm{diag}(1, \dots, 1, -1, -2)$	$\mathrm{diag}(1, \dots, 1, 2)$
11	2	2	-1
11	1	$\mathrm{diag}(1, \dots, 1, 2)$	$\mathrm{diag}(1, \dots, 1, -1, -2)$
12	2	2	-1
12	-1	$\mathrm{diag}(1, \dots, 1, 2)$	$\mathrm{diag}(1, \dots, 1, 2)$

Table 4.3: Continued

Item	$b_1 \dots b_s$	$b_{s+1} \dots b_{2n}$	$c_p(b_1, \dots, b_s)$
Item	$c_p(b_{s+1}, \dots, b_{2n})$	$\mathrm{diag}(b_1, \dots, b_s)$	$\mathrm{diag}(b_{s+1}, \dots, b_{2n})$
13	-2	-2	1
13	1	$\mathrm{diag}(1, \dots, 1, -2)$	$\mathrm{diag}(1, \dots, 1, -2)$
14	-2	-2	1
14	-1	$\mathrm{diag}(1, \dots, 1, -2)$	$\mathrm{diag}(1, \dots, 1, -1, 2)$
15	-2	-2	-1
15	1	$\mathrm{diag}(1, \dots, 1, -1, 2)$	$\mathrm{diag}(1, \dots, 1, -2)$
16	-2	-2	-1
16	-1	$\mathrm{diag}(1, \dots, 1, -1, 2)$	$\mathrm{diag}(1, \dots, 1, -1, 2)$
17	3	3	1
17	1	$\mathrm{diag}(1, \dots, 1, 3)$	$\mathrm{diag}(1, \dots, 1, 3)$
18	3	3	1
18	-1	$\mathrm{diag}(1, \dots, 1, 3)$	$\mathrm{diag}(1, \dots, 1, 2, 3 \cdot 2^{-1})$
19	3	3	-1
19	1	$\mathrm{diag}(1, \dots, 1, 2, 3 \cdot 2^{-1})$	$\mathrm{diag}(1, \dots, 1, 3)$
20	3	3	-1
20	-1	$\mathrm{diag}(1, \dots, 1, 2, 3 \cdot 2^{-1})$	$\mathrm{diag}(1, \dots, 1, 2, 3 \cdot 2^{-1})$
21	-3	-3	1
21	1	$\mathrm{diag}(1, \dots, 1, -3, 1)$	$\mathrm{diag}(1, \dots, 1, -3, 1)$
22	-3	-3	1
22	-1	$\mathrm{diag}(1, \dots, 1, -3, 1)$	$\mathrm{diag}(1, \dots, 1, -3)$
23	-3	-3	-1
23	1	$\mathrm{diag}(1, \dots, 1, -3)$	$\mathrm{diag}(1, \dots, 1, -3, 1)$
24	-3	-3	-1

Table 4.3: Continued

Item	$b_1 \ldots b_s$	$b_{s+1} \ldots b_{2n}$	$c_p(b_1, \ldots, b_s)$
Item	$c_p(b_{s+1}, \ldots, b_{2n})$	$\mathrm{diag}(b_1, \ldots, b_s)$	$\mathrm{diag}(b_{s+1}, \ldots, b_{2n})$
24	-1	$\mathrm{diag}(1, \ldots, 1, -3)$	$\mathrm{diag}(1, \ldots, 1, -3)$
25	6	6	1
25	1	$\mathrm{diag}(1, \ldots, 1, 6)$	$\mathrm{diag}(1, \ldots, 1, 6)$
26	6	6	1
26	-1	$\mathrm{diag}(1, \ldots, 1, 6)$	$\mathrm{diag}(1, \ldots, 1, 6, 1)$
27	6	6	-1
27	1	$\mathrm{diag}(1, \ldots, 1, 6, 1)$	$\mathrm{diag}(1, \ldots, 1, 6)$
28	6	6	-1
28	-1	$\mathrm{diag}(1, \ldots, 1, 6, 1)$	$\mathrm{diag}(1, \ldots, 1, 6, 1)$
29	-6	-6	1
29	1	$\mathrm{diag}(1, \ldots, 1, -1, 6)$	$\mathrm{diag}(1, \ldots, 1, -1, 6)$
30	-6	-6	1
30	-1	$\mathrm{diag}(1, \ldots, 1, -1, 6)$	$\mathrm{diag}(1, \ldots, 1, -6)$
31	-6	-6	-1
31	1	$\mathrm{diag}(1, \ldots, 1, -6)$	$\mathrm{diag}(1, \ldots, 1, -1, 6)$
32	-6	-6	-1
32	-1	$\mathrm{diag}(1, \ldots, 1, -6)$	$\mathrm{diag}(1, \ldots, 1, -6)$

Chapter 5

Fixed-Point Groups of Isomorphy Classes of Involutions over $\mathrm{SO}(2n, k)$ Where $\mathbf{k} = \mathbb{Q}_p$

5.1 Introductory Material

The fixed point group of an involution χ over a group G is defined by $G^\chi \equiv \{x \in G \mid \chi(x) = x\}$. Throughout this chapter, I will be using $\mathrm{SO}(2n, k)$ and I will assume $\mathrm{char}(k) = 0$. First a definition:

Definition 9. *If G is a semisimple algebraic group over k and $\theta \in \mathrm{Aut}(G)$, the corresponding "symmetric k-variety" is $X = \{g\theta(g)^{-1}|g \in G\}$*

For $k = \mathbb{R}$ symmetric k-varieties are also called "semisimple symmetric spaces." The real symmetric semisimple symmetric spaces for which G^χ is compact are also known as Riemannian symmetric spaces. These play an important role in Lie theory, representation theory, differential geometry, mathematical physics, and many other areas.

The symmetric k-varieties with a compact fixed-point group have many properties similar to real Riemannian symmetric spaces. For example, they consist of semisimple elements as follows from the following result due to Helminck and Wang.

Theorem 3. *Let G be a connected, reductive, algebraic k-group with* $\mathrm{char}(k) = 0$*, let χ be an involution of G, and let $X = \{x\chi(x)^{-1} \mid x \in G\}$. If $G^{\chi} \cap [G, G]$ is anisotropic over k then X_k consists of semi-simple elements [5, Proposition 10].*

According to another result of Helminck and Wang, two symmetric k-varieties related to a matrix group G are G-isomorphic iff their involutions are isomorphic with respect to conjugacy. Theorem 3 is also useful in working with symmetric k-varieties. Over $\mathbb{R}$, symmetric varieties are called "symmetric spaces" and they are studied in differential geometry, Lie groups, and representation theory. Symmetric k-varieties are generalizations of symmetric spaces.

5.2 Computational Results Used to Find the Fixed-Point Groups and Whether They are Compact

My first result of this chapter is a result giving the fixed-point group of the most basic possible involution over $\mathrm{SO}(2n, k)$.

5.2.1 The Most Basic Fixed-Point Group

Proposition 6. *Let $G = \mathrm{SO}(2n, k)$ and let $k = \mathbb{R}$ or $k = \mathbb{Q}_p$. For the matrix $A = I_{2n-i,i}$, the fixed point group G^{J_A} consists of the block matrices* $\mathrm{diag}(X_1, X_2)$ *where X_1 is $(2n-i)\times(2n-i)$, X_2 is $i \times i$, $X_1^T = X_1^{-1}$, $X_2^T = X_2^{-1}$ (so they are both invertible), and* $\det X_1 \det X_2 = 1$*. Also, G^{J_A} is not compact over $\mathbb{R}$ or $\mathbb{Q}_p$.*

Proof. Let $B \in G^{J_A}$, where $A = I_{2n-i,i}$. Let $B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$. Then by straightforward computation, $J_A(B) = \begin{pmatrix} B_{11} & -B_{12} \\ -B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$. Since $\mathrm{char}(k) \neq 2$ by assumption, $B_{21} = 0$ and $B_{12} = 0$. And inasmuch as $B \in \mathrm{SO}(2n, k)$, $B^T = B^{-1}$ so $B_{11}^T = B_{11}^{-1}$, $B_{22}^T = B_{22}^{-1}$, and $\det B = \det B_{11} \det B_{22} = 1$.

Further, because compactness on both $\mathbb{R}$ and $\mathbb{Q}_p$ is equivalent to being both closed and bounded, none of these fixed point groups are compact since $\|B\| = \|B_{11}\|\|B_{22}\|$ using the norm of either $\mathbb{R}$ or $\mathbb{Q}_p$ and the only restriction on B_{ii}, $i \in \{1,2\}$, is that $B_{ii}^{-1} = B_{ii}^T$. Therefore, the fixed point group G^{J_A}, $A = I_{2n-i,i}$, is unbounded. Q.E.D.

5.2.2 Full Results on the Possible Sums of Two Squares of P-Adic Numbers

Here are some results related to showing whether every integer $1, 2, \ldots, p$ is a sum of two squares in $\mathbb{Q}_p$. This turns out to be an important issue in determining the fixed-point groups and whether or not they are compact.

Lemma 5. *Let $n \in \mathbb{Z}$ be such that $n > 0$ and n is odd. Then there is a one-to-one correspondence between differences (not sums) of squares of integers (in $\mathbb{Z}$) that equal n and factorizations of n into two positive integers.*

Proof. This is a result of elementary number theory, and a proof can be found in Rosen [8, Lemma 3.9 on pp. 112-113]. It depends on the fact that $a^2 - b^2 = (a+b)(a-b)$. Q.E.D.

Because of this lemma, whenever $-1 \in \mathbb{Q}_p^{*2}$, there is a sum of two squares that equals p which consists of p-adic integers. If $p-1$ is a square, $(\sqrt{p-1})^2 + 1^2 = p$ so for all primes $p \equiv 1 \pmod{c}$, c a square, the result has been proven. It is below in lemma form.

Lemma 6. *For all prime numbers $p \in \mathbb{N}$, if $p \equiv 1 \pmod{c^2}$ and $c \in \mathbb{N}$ then p is the sum of two squares $p = (\sqrt{p-1})^2 + 1^2$.*

Further, because all prime numbers p where $-1 \in \mathbb{Q}_p^{*2}$ are congruent to 1 modulo 3, I have proven the following lemma.

Lemma 7. *For all p-adic fields $\mathbb{Q}_p$ such that $-1 \in \mathbb{Q}_p^{*2}$, every odd p-adic integer corresponding to a finite p-adic series is a sum of two squares. Note that $p \equiv 1 \pmod{4}$ iff $-1 \in \mathbb{Q}_p^{*2}$.*

Proof. This is a consequence of Lemma 5. Q.E.D.

Here is another lemma that is useful in proving what I want, viz., that if $p \equiv 3 \pmod 4$ then p is not the sum of two squares over $\mathbb{Q}_p$.

Lemma 8. *Over $\mathbb{Z}$, if p is a prime integer, $p \equiv 3 \pmod 4$, and $a_0, a_1, b_0, b_1 \in \{0, 1, 2, \ldots, p-1\}$ then $a_0^2 + b_0^2 \not\equiv 0 \pmod p$, $a_0^2 + b_0^2 + 2a_0a_1p + 2b_0b_1p \neq p$, and $(a_0 + pa_1)^2 + (b_0 + pb_1)^2 \neq p$.*

Proof. Assume $a_0^2 + b_0^2 + 2a_0a_1p + 2b_0b_1p = p$. Then I want to show that either a_1 or b_1 is not zero, so assume they are both zero. Then $a_0^2 + b_0^2 = p$. Therefore, $a_0^2 + b_0^2 \equiv 3 \pmod 4$. Now, any square is equivalent to 0 or 1 modulo four, so that is impossible, meaning either a_1 or b_1 is not zero, or both of them are nonzero. Further, $a_0^2 + b_0^2 \not\equiv 0 \pmod p$.

Assume without loss of generality that $a_1 \neq 0$. If $a_0 = 0$, then $b_0^2 + 2b_0b_1p = p$ so $b_0^2 = p(1 - 2b_0b_1)$ which implies that p divides b_0^2, hence b_0 (by the definition of "prime number"). That must mean that $b_0 = 0$, so $2b_0b_1p = p \Rightarrow 2b_0b_1 = 1$, but that is a contradiction because it was assumed that $b_0, b_1 \in \{0, 1, 2, \ldots, p-1\}$.

Therefore, $a_0 \neq 0$. For similar reasons, $b_0 \neq 0$. $a_0^2 + b_0^2 + 2a_0a_1p + 2b_0b_1p = p \Rightarrow a_0^2 + b_0^2 = p(1 - 2a_0a_1 - 2b_0b_1)$ so p divides $a_0^2 + b_0^2$. Thus, $a_0^2 + b_0^2 = \ell p, \ell \in \mathbb{Z}$. But $a_0, a_1, b_0, b_1 \in \{0, 1, 2, \ldots, p-1\}$ and $a_0^2 + b_0^2 + 2a_0a_1p + 2b_0b_1p = p$, so the only possibilities are that $\ell = 0$, which I proved was impossible, and $\ell = 1$, which I proved was impossible. That proves the first desired result.

Now assume $(a_0 + pa_1)^2 + (b_0 + pb_1)^2 = p$. $(a_0 + pa_1)^2 = a_0^2 + 2a_0a_1p + a_1^2p^2$, so

$$(a_0 + pa_1)^2 + (b_0 + pb_1)^2 = a_0^2 + b_0^2 + 2a_0a_1p + 2b_0b_1p + a_1^2p^2 + b_1^2p^2 = p$$

But I have shown that the first four terms above of the expansion of $(a_0 + pa_1)^2 + (b_0 + pb_1)^2$ cannot be p, or in other words, $a_0^2 + b_0^2 + 2a_0a_1p + 2b_0b_1p \neq p$. Then $a_1^2p^2 + b_1^2p^2 \neq 0$ so either $a_1 \neq 0$, $b_1 \neq 0$, or both. Assume without loss of generality that $a_1 \neq 0$. Then $a_1^2p^2 > p$, so it cannot be true that $a_0^2 + b_0^2 + 2a_0a_1p + 2b_0b_1p + a_1^2p^2 + b_1^2p^2 = p$. Q.E.D.

Proposition 7. *Over $\mathbb{Q}_p$, if $p \not\equiv 3 \pmod 4$ (so $p = 2$ or $p \equiv 1 \pmod 4$) then p is the sum of two square p-adic integers. Else if $p \equiv 3 \pmod 4$ then p is not the sum of two square p-adic integers.*

Proof. The first statement is a direct consequence of Lemmas 5 and 7. As for the second statement, let $\alpha = \sum_{i=0}^{\infty} p^i a_i$ be a p-adic integer, so all $a_i \in \{0, 1, 2, \ldots, p-1\}$. Let $\beta = \sum_{j=0}^{\infty} p^j b_j$ be another p-adic integer, which thusly has a similar condition on all b_i. Then suppose $\alpha^2 + \beta^2 = p$. In that case, $a_0^2 + b_0^2 + 2a_0a_1p + 2b_0b_1p + \ldots = p$.

In order for that to be true, it would be necessary that $a_0^2 + b_0^2 \equiv 0 \pmod{p}$, but I showed in Lemma 8 that this condition cannot be met. Q.E.D.

Lemma 9. *Let p be a prime integer. Then for any $a \in \mathbb{Z}$ there exist $b, c \in \mathbb{Z}$ such that $b^2 + c^2 \equiv a \pmod{p}$.*

Proof. There are only two square classes of the finite field $\mathbb{F}_p$, where $p \neq 2$, so the sum of any two squares has to be in one of them. In other words, each element of these square classes can be multiplied by a square to get any of the others. The result is automatic if a is a square. Since one can obtain a non-square with appropriate b and c, there is an $\alpha \in \mathbb{Z}$ such that $\alpha^2(b^2 + c^2) \equiv a \pmod{p}$, or $(\alpha b)^2 + (\alpha c)^2 \equiv a \pmod{p}$.

If $p = 2$ then $a \equiv 0 \pmod{2}$ or $a \equiv 1 \pmod{2}$, so one can set $b = 0$ or $b = 1$ and let $c = 0$ in either case to obtain the desired result. Q.E.D.

Lemma 10. *In the finite field $\mathbb{F}_p$, -1 is a square iff $p \equiv 1 \pmod{4}$.*

Proof. This result was proven by Ling Wu in his doctoral thesis. He pointed out that $\mathbb{F}_p^*$ is a cyclic group of order $p - 1$ and -1 is the only element of order two. Thus, -1 is a square iff the order of $\mathbb{F}_p^*$ is divisible (over $\mathbb{Z}$) by four, i.e., iff $p \equiv 1 \pmod{4}$ [11, Lemma 11 on p. 26]. Q.E.D.

Now here is a result from elementary number theory on the integers $\mathbb{Z}$ that is very useful in proving whether every element of $\mathbb{Q}_p$ is a square or not.

Proposition 8. *Let $a, b \in \mathbb{Z}$ be such that the greatest common divisor of a and b is d. The equation $ax + by = c$ has no solutions in $\mathbb{Z}$ if d does not divide c, i.e., if there is no integer m such that $md = c$. On the other hand, if d does divide c (so such an integer m exists) then there are infinitely many solutions to $ax + by = c$ over $\mathbb{Z}$. Furthermore, if $x = x_0$, $y = y_0$ is* *a solution to the equation then every solution is of the form* $x = x_0 + \frac{b}{d}n$, $y = y_0 - \frac{a}{d}n$, *where* $n \in \mathbb{Z}$.

Proof. This is a result of elementary number theory on linear diophantine equations in two variables. A proof can be found in Rosen [8, Theorem 3.21 on pp. 120-121]. Q.E.D.

For p-adic integers, the result is found in the next proposition.

Proposition 9. *If* $p \equiv 1 \pmod 4$ *then every p-adic integer in* $\mathbb{Q}_p$ *is the sum of the squares of two p-adic integers. If* $p \equiv 3 \pmod 4$ *or* $p = 2$ *then this is not true.*

Proof. Much of this result has already been proven by Proposition 7 and Lemma 5. In particular, the case $p \equiv 3 \pmod 4$ was proven by Proposition 7. Consider the case $p \equiv 1 \pmod 4$. By Lemma 5, every odd p-adic integer corresponding to a finite sum $\sum_{i=0}^{\ell} a_i p^i$ is in fact the sum of two squares of integers in $\mathbb{Z}$, hence in $\mathbb{Q}_p$.

Therefore, let $\alpha = \sum_{i=0}^{\infty} a_i p^i$ be a p-adic integer such that either α is even or there are an infinitely many $a_j \neq 0$, $j \in \mathbb{Z}^{\geq 0}$. Suppose $\alpha = \beta^2 + \gamma^2$, where β and γ are p-adic integers. Let $\beta = \sum_{i=0}^{\infty} b_i p^i$ and $\gamma = \sum_{i=0}^{\infty} c_i p^i$. Then $\beta^2 = \left(\sum_{i=0}^{\infty} b_i p^i\right)^2 = b_0^2 + 2b_0b_1p + (2b_0b_2 + b_1^2)p^2 + (2b_0b_3 + 2b_1b_2)p^3 + \ldots$ Thus, $\beta^2 + \gamma^2 = b_0^2 + c_0^2 + (2b_0b_1 + 2c_0c_1)p + (2b_0b_2 + b_1^2 + 2c_0c_2 + c_1^2)p^2 + (2b_0b_3 + 2b_1b_2 + 2c_0c_3 + 2c_1c_2)p^3 + \ldots$

For this to equal α, it is necessary that $b_0^2 + c_0^2 \equiv a_0 \pmod p$, and I proved in Lemma 9 that this can be done. Let $b_0^2 + c_0^2 = np + a_0$. Then it is necessary that $n + (2b_0b_1 + 2c_0c_1) \equiv a_1 \pmod p$, i.e., that $2b_0b_1 + 2c_0c_1 \equiv a_1 - n \pmod p$, so without loss of generality one may assume $n = 0$. Then $2(b_0b_1 + c_0c_1) \equiv a_1 \pmod p$. Now, b_0 and c_0 have already been determined, but b_1 and c_1 have not.

If $2(b_0b_1 + c_0c_1) = a_1 + np$ for some $n \in \mathbb{Z}$ then $2(b_0b_1 + c_0c_1) \equiv a_1 \pmod p$. Since $|\mathbb{Z}|$ is infinite, if $p \neq 2$ there is some $n \in \mathbb{Z}$ such that the greatest common divisor of $2b_0$ and $2c_0$ divides $a_1 + np$. Then by Proposition 8, there are numbers b_1 and c_1 such that $2(b_0b_1 + c_0c_1) \equiv a_1 \pmod p$. A similar result holds for the coefficients of p^2, p^3, and etc. of $\beta^2 + \gamma^2$, so inductively one can get every coefficient of every p^i to equal a_i.

On the other hand, let $p = 2$ and assume that $\alpha = \beta^2 + \gamma^2$ for all p-adic integers $\alpha \in \mathbb{Q}_2$. If a_1 is odd, $a_1 + np$ from the previous paragraph must be odd, so there is no suitable n. But that means I must solve $2(b_0b_1 + c_0c_1) \equiv 0 \pmod{2}$ or $2(b_0b_1 + c_0c_1) \equiv 1 \pmod{2}$. In the former case, let $b_1 = c_1 = 0$. The latter case is insoluble. If $a_0 = 0$, one can set $b_0^2 + c_0^2 = 2$ (if $c_0 = b_0 = 1$) and $c_1 = b_1 = 0$ to obtain 0 as the coefficient of p^0 and 1 as the coefficient of p.

However, if $a_0 = 1$ and $a_1 = 1$, one cannot solve the equations $b_0^2 + c_0^2 = a_0 = 1$ and $2(b_0b_1 + c_0c_1) = a_1 = 1$ because $a_0 = 1$ implies one of b_0 or c_0 is one and the other is zero. Assume without loss of generality that $b_0 = 1$ and $c_0 = 0$. Then in the second term one has $2(b_0b_1 + c_0c_1) = 1$ so $2b_1 = 1$, but $b_1 \in \{0, 1\}$, which is a contradiction. Ergo, the result is not true for $p = 2$, since $3 = 1 + 2^1$ is not the sum of two square p-adic integers in $\mathbb{Q}_2$. Q.E.D.

Here is the final result.

Theorem 4. *If $p \equiv 1 \pmod{4}$ then every p-adic number in $\mathbb{Q}_p$ is the sum of the squares of two p-adic numbers. If $p \equiv 3 \pmod{4}$ or $p = 2$ then this is not true.*

Proof. In the case $p \equiv 1 \pmod{4}$, a similar proof holds as was used in the previous proposition, Proposition 4. If $\alpha = \sum_{i=\ell}^{\infty} a_i p^i$, $\ell \in \mathbb{Z}$ and $\ell < 0$, one can make α the sum of two squares $\beta = \sum_{i=\ell}^{\infty} b_i p^i$ and $\gamma = \sum_{i=\ell}^{\infty} c_i p^i$ as before. In the case $p \equiv 3 \pmod{4}$, suppose $p = \beta^2 + \gamma^2$. Then let $\beta = \sum_{i=m}^{\infty} b_i p^i$ and $\gamma = \sum_{i=n}^{\infty} c_i p^i$. By Proposition 4, $m < 0$ or $n < 0$. So assume without loss of generality that $m < -2$.

$\beta^2 = b_m^2 p^{2m} + 2b_m b_{m+1} p^{2m+1} + b_{m+2}^2 p^{2m+2} + \ldots$. Furthermore, p^{2j}, $j < 0$, is larger with respect to the p-norm than p^j. As a result, in $\beta^2 + \gamma^2 = p$, the terms that are the largest with respect to the p-norm must have their coefficients cancel out or the lefthand-side of the equation will have a larger norm than the righthand-side, which is a contradiction. But $\|\beta\|_p > 1$ because $m < -2 < 0$, so, because of what has been said, $\|\beta^2\|_p > \|\beta\|_p > 1$. As a result, unless $m = n$, the biggest terms of β^2 (or γ^2 if $n > m$) will not be cancelled out, so $\|\beta^2 + \gamma^2\|_p > 1 > 1/p = \|p\|_p$ meaning $\beta^2 + \gamma^2 = p$ is impossible.

Therefore assume $m = n$. Then $\beta^2+\gamma^2 = b_m^2 p^{2m}+c_m^2 p^{2m}+2b_m b_{m+1} p^{2m+1}+2c_m c_{m+1} p^{2m+1}+ b_{m+2} p^{2m+2}+c_{m+2}^2 p^{2m+2}+\ldots$. But by Lemma 8, $b_m^2 p^{2m}+c_m^2 p^{2m} \neq p^{2m+1}$, so $b_m^2 p^{2m}+c_m^2 p^{2m} < p$ or $b_m^2 p^{2m}+c_m^2 p^{2m} > p$. In the former case, the norm of $\beta^2+\gamma^2$ is still different from the norm of p, so that cannot be true. In the latter case, there is still a coefficient of p^{2m} by Lemma 8, since neither the p^{2m} terms nor the p^{2m} and p^{2m+1} terms can cancel evenly (supposing $m < -1$). This contradicts my hypothesis that $\beta^2+\gamma^2 = p$.

Now suppose $p = 2$. Let $\beta = \sum_{i=m}^{\infty} b_i 2^i$ and $\gamma = \sum_{i=n}^{\infty} c_i 2^i$ and assume $\beta^2+\gamma^2 = 3$. Then for the same reasons as before (viz., the p-norm) $m = n$. In that case, it is impossible that $\beta^2+\gamma^2 = 3$ because the earlier terms cannot cancel out, for reasons similar to what was seen in the previous proposition. Q.E.D.

From the proof of the above, there are two corollaries found below that have been proven.

Corollary 1. *In $\mathbb{Q}_2$, 3 is not the sum of two squares. If $p \equiv 3 \pmod 4$ then p is not the sum of two squares.*

Corollary 2. *For any prime number p, in $\mathbb{Q}_p$, if $\alpha^2+\beta^2 = \gamma$, and the first term in the p-adic expansion of γ is not a square, then $\alpha = \sum_{i=m}^{\infty} a_i 2^i$ and $\beta = \sum_{i=m}^{\infty} b_i 2^i$. So both α and β start with the same index m. Furthermore, m is the first term of the p-adic expansion of γ.*

5.2.3 Computational Lemmas

The following results have to do with finding the fixed-point groups as well.

Lemma 11. *Let $\varepsilon \in k$ be such that ε^{-1} is the sum of two squares in $\mathbb{Q}_p$. Then $\mathrm{diag}(\varepsilon, \varepsilon)$ is congruent to I_2.*

Proof. Let $\varepsilon^{-1} = a^2+b^2$. Then

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \varepsilon(a^2+b^2) & 0 \\ 0 & \varepsilon(a^2+b^2) \end{pmatrix} = I_2$$

Q.E.D.

Lemma 12. *Let $0 < \ell < n$, $\ell \in \mathbb{Z}$. On $\mathbb{F}_p$ and $\mathbb{Q}_p$, if $p \equiv 1 \pmod 4$ then the block matrix $\operatorname{diag}(I_{n-\ell}, -I_\ell)$ is congruent to $\operatorname{diag}(I_{n-1}, -1)$ and I_n.*

Proof. If $p \equiv 1 \pmod 4$ then -1 is a square in both $\mathbb{F}_p$ and $\mathbb{Q}_p$, and by Lemma 10 and Proposition 9 both 1 and -1 are the sums of two squares in both $\mathbb{F}_p$ and $\mathbb{Q}_p$. Then by an inductive process, using the result of Lemma 11 as a first step, one can show that $\operatorname{diag}(I_{n-\ell}, -I_\ell)$ is congruent to I_n.

Firstly, let $n = 2$. Then $\ell = 1$. Let $a^2 + b^2 = -1$ and let $c^2 + d^2 = 1$, $c \neq 0$ (e.g., $c = 1, d = 0$). Then $\begin{pmatrix} c & \sqrt{-1}d \\ \mp d & \pm\sqrt{-1}c \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} c & \mp d \\ \sqrt{-1}d & \pm\sqrt{-1}c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

If $n = 3$ and $\ell = 1$, a similar process shows that the matrix is congruent to I_3. If $\ell = 2$, Lemma 9 shows how one can obtain I_3 with a block matrix.

Assume the result is true for all $m < n, 1 < \ell < m$. Then the matrix $\operatorname{diag}(I_{n-\ell}, -I_\ell)$ is congruent to I_n if $\ell < n - 1$ by the inductive hypothesis, and otherwise it is congruent to $\operatorname{diag}(I_{n-1}, -1)$ which is congruent to I_n. Furthermore, $\forall\ n > 1$, I_n is congruent to $\operatorname{diag}(I_{n-1}, -1)$. Q.E.D.

5.3 Fixed-Point Groups on Two Often-Used Involutions

First I have computed the fixed-point groups on a more basic set of involutions.

Proposition 10. *Let* $A = \begin{pmatrix} 0 & 1 & \dots & 0 & 0 \\ -1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & -1 & 0 \end{pmatrix}$. *Then the fixed point group of J_A over $\mathrm{GL}(2n, k)$ consists of matrices* $B = \begin{pmatrix} B_{11} & B_{12} & \dots & B_{1,n-1} & B_{1,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ B_{n1} & B_{n2} & \dots & B_{n,n-1} & B_{nn} \end{pmatrix}$ *where each $B_{i,j}$ is* *a 2×2 block, $B_{i,j} = \begin{pmatrix} \alpha_{ij} & -\beta_{ij} \\ \beta_{ij} & \alpha_{ij} \end{pmatrix}$, and (naturally) $|B| \neq 0$. Over $\mathbb{R}$ and $\mathbb{Q}_p$ it is not compact.*

Proof. Let $B \in \mathrm{SO}(2n, k)$, $B = \begin{pmatrix} B_{11} & B_{12} & \dots & B_{1,n-1} & B_{1,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ B_{n1} & B_{n2} & \dots & B_{n,n-1} & B_{nn} \end{pmatrix}$ where each $B_{i,j}$ is a 2×2 block. Let B be in the fixed point group of J_A over $\mathrm{GL}(2n, k)$. (Observe that $A^{-1} = -A = A^T$, so $A \in \mathrm{SO}(2n, k)$). Let $L_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then $J_A(B) = -ABA = -\operatorname{diag}(L_2, \dots, L_2) B \operatorname{diag}(L_2, \dots, L_2)$

$$= \begin{pmatrix} -L_2B_{11}L_2 & -L_2B_{12}L_2 & \dots & -L_2B_{1,n-1}L_2 & -L_2B_{1,n}L_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -L_2B_{n1}L_2 & -L_2B_{n2}L_2 & \dots & -L_2B_{n,n-1}L_2 & -L_2B_{nn}L_2 \end{pmatrix}$$

which must equal B.

As a result, $\forall\, i, j \in \{1, 2, \dots, n-1, n\}$, $-L_2B_{i,j}L_2 = B_{i,j}$. Let $B_{i,j} = \begin{pmatrix} \alpha_{ij} & \beta_{ij} \\ \gamma_{ij} & \delta_{ij} \end{pmatrix}$. Then $-L_2B_{i,j}L_2 = \begin{pmatrix} -\gamma_{ij} & -\delta_{ij} \\ \alpha_{ij} & \beta_{ij} \end{pmatrix} L_2 = \begin{pmatrix} \delta_{ij} & -\gamma_{ij} \\ -\beta_{ij} & \alpha_{ij} \end{pmatrix} = \begin{pmatrix} \alpha_{ij} & \beta_{ij} \\ \gamma_{ij} & \delta_{ij} \end{pmatrix}$. Therefore, $\alpha_{ij} = \delta_{ij}$ and $\beta_{ij} = -\gamma_{ij}$.

Now, $\begin{vmatrix} \alpha_{ij} & -\beta_{ij} \\ \beta_{ij} & \alpha_{ij} \end{vmatrix} = \alpha_{ij}^2 + \beta_{ij}^2$ which can be arbitrarily big. Thus, $\left\| \begin{pmatrix} \alpha_{ij} & -\beta_{ij} \\ \beta_{ij} & \alpha_{ij} \end{pmatrix} \right\|$ is infinite when using the sup norm. Ergo, because compactness on $\mathbb{R}$ and $\mathbb{Q}_p$ is equivalent to being closed and bounded, the fixed point group of A is unbounded, so it is not compact. Q.E.D.

Proposition 11. *Let $X = \begin{pmatrix} I_{s-1} & 0 & 0 & 0 \\ 0 & \alpha & -\beta & 0 \\ 0 & \beta & \alpha & 0 \\ 0 & 0 & 0 & I_{t-1} \end{pmatrix} \in \mathrm{GL}(2n, k)$, where $k = \mathbb{F}_p$ and $\alpha^2 + \beta^2$ is not a square of $\mathbb{F}_p$ (which implies $p \neq 2$). Then the fixed point group of $J_{X^{-1}I_{s,t}X}$ over $\mathrm{GL}(2n, k)$ is the subset of $\mathrm{GL}(2n, k)$ containing all matrices S of one of the following forms:*

1. *if* $\alpha = \pm\beta$, *then* $S = \begin{pmatrix} S_{11} & \mp S_{13} & S_{13} & 0 \\ \mp\Sigma_{31} & \sigma_{33} & \sigma_{32} & \pm\Sigma_{34} \\ \Sigma_{31} & \sigma_{32} & \sigma_{33} & \Sigma_{34} \\ 0 & \pm S_{43} & S_{43} & S_{44} \end{pmatrix}$ *where* S_{11} *is* $(s-1)\times(s-1)$, S_{44} *is* $(t-1)\times(t-1)$, *the* 0 *in the upper-right corner is* $(s-1)\times(t-1)$, *and the* 0 *in the lower- left corner is* $(t-1)\times(s-1)$, *all* σ_{ij} *are (one-dimensional) elements in* $\mathbb{F}_p$, Σ_{31} *is* $1\times(s-1)$, *and* Σ_{34} *is* $1\times(t-1)$.

2. *Else if* $\alpha \neq \pm\beta$, *then* $S = \begin{pmatrix} S_{11} & \frac{-\alpha}{\beta}S_{13} & S_{13} & 0 \\ \frac{-\alpha}{\beta}\Sigma_{31} & \sigma_{22} & \frac{\alpha\beta(\sigma_{33}-\sigma_{22})}{\alpha^2-\beta^2} & \frac{\beta}{\alpha}\Sigma_{34} \\ \Sigma_{31} & \frac{\alpha\beta(\sigma_{33}-\sigma_{22})}{\alpha^2-\beta^2} & \sigma_{33} & \Sigma_{34} \\ 0 & \frac{\beta}{\alpha}S_{43} & S_{43} & S_{44} \end{pmatrix}$. *The blocks of* S *have the same sizes here as in case 1.*

Proof. Let $\alpha^2+\beta^2 = \xi$. Then $X^{-1}I_{s,t}X = \begin{pmatrix} I_{s-1} & 0 & 0 & 0 \\ 0 & \frac{\alpha^2-\beta^2}{\xi} & \frac{-2\alpha\beta}{\xi} & 0 \\ 0 & \frac{-2\alpha\beta}{\xi} & \frac{\beta^2-\alpha^2}{\xi} & 0 \\ 0 & 0 & 0 & -I_{t-1} \end{pmatrix}$. Let $A = X^{-1}I_{s,t}X$ and let $S \in \mathrm{GL}(2n,k)$, $S = \begin{pmatrix} S_{11} & S_{12} & S_{13} & S_{14} \\ \Sigma_{21} & \sigma_{22} & \sigma_{23} & \Sigma_{24} \\ \Sigma_{31} & \sigma_{32} & \sigma_{33} & \Sigma_{34} \\ S_{41} & S_{42} & S_{43} & S_{44} \end{pmatrix}$ where the entries with an S are block matrices of the appropriate size to match the blocks of A and the entries with a σ are elements of $k = \mathbb{F}_p$.

By assumption, $\alpha \neq 0$ and $\beta \neq 0$ (otherwise, $\alpha^2+\beta^2$ would be a square). Since $A^{-1} = A^T = A$, $J_A(S) = ASA$ which we set equal to S. Then $AS = SA$, or $AS - SA = 0$. Hence by computation,

$$\begin{pmatrix} 0 & \frac{2\beta(S_{12}\beta+S_{13}\alpha)}{\xi} & \frac{2\alpha(S_{12}\beta+S_{13}\alpha)}{\xi} & 2S_{14} \\ \frac{-2\beta(\beta\Sigma_{21}+\alpha\Sigma_{31})}{\xi} & \frac{-2\alpha\beta(\sigma_{32}-\sigma_{23})}{\xi} & \frac{2(\alpha^2\sigma_{23}-\beta^2\sigma_{23}-\alpha\beta\sigma_{33}+\alpha\beta\sigma_{22})}{\xi} & \frac{2\alpha(\alpha\Sigma_{24}-\beta\Sigma_{34})}{\xi} \\ \frac{-2\alpha(\beta\Sigma_{21}+\alpha\Sigma_{31})}{\xi} & \frac{-2(\alpha\beta\sigma_{22}+\alpha^2\sigma_{32}-\beta^2\sigma_{32}-\alpha\beta\sigma_{33})}{\xi} & \frac{2\alpha\beta(\sigma_{32}-\sigma_{23})}{\xi} & \frac{2\beta(\alpha\Sigma_{24}-\beta\Sigma_{34})}{\xi} \\ -2S_{41} & \frac{-2\alpha(-S_{43}\beta+S_{42}\alpha)}{\xi} & \frac{-2\beta(-S_{43}\beta+S_{42}\alpha)}{\xi} & 0 \end{pmatrix} = 0$$

Therefore, $S_{12} = \frac{-\alpha}{\beta} S_{13}$, $\Sigma_{21} = \frac{-\alpha}{\beta}\Sigma_{31}$, $\sigma_{32} = \sigma_{23}$, $\Sigma_{24} = \frac{\beta}{\alpha}\Sigma_{34}$, $S_{14} = 0$, $S_{41} = 0$, and $S_{42} = \frac{\beta}{\alpha} S_{43}$. Further, one obtains the following:

1. If $\alpha = \pm\beta$, then $\sigma_{22} = \sigma_{33}$.

2. Else if $\alpha \neq \pm\beta$ then $\sigma_{23} = \sigma_{32} = \dfrac{\alpha\beta(\sigma_{33} - \sigma_{22})}{\alpha^2 - \beta^2}$.

As the result, the matrix S has one of the following two forms: if $\alpha = \pm\beta$, $S = \begin{pmatrix} S_{11} & \mp S_{13} & S_{13} & 0 \\ \mp\Sigma_{31} & \sigma_{33} & \sigma_{32} & \pm\Sigma_{34} \\ \Sigma_{31} & \sigma_{32} & \sigma_{33} & \Sigma_{34} \\ 0 & \pm S_{43} & S_{43} & S_{44} \end{pmatrix}$. Otherwise,

$$S = \begin{pmatrix} S_{11} & \frac{-\alpha}{\beta} S_{13} & S_{13} & 0 \\ \frac{-\alpha}{\beta}\Sigma_{31} & \sigma_{22} & \frac{\alpha\beta(\sigma_{33}-\sigma_{22})}{\alpha^2-\beta^2} & \frac{\beta}{\alpha}\Sigma_{34} \\ \Sigma_{31} & \frac{\alpha\beta(\sigma_{33}-\sigma_{22})}{\alpha^2-\beta^2} & \sigma_{33} & \Sigma_{34} \\ 0 & \frac{\beta}{\alpha} S_{43} & S_{43} & S_{44} \end{pmatrix}$$

Q.E.D.

Corollary 3. *Let* $X = \begin{pmatrix} I_{s-1} & 0 & 0 & 0 \\ 0 & \alpha & -\beta & 0 \\ 0 & \beta & \alpha & 0 \\ 0 & 0 & 0 & I_{t-1} \end{pmatrix} \in \mathrm{GL}(2n, k)$, *where* $k = \mathbb{F}_p$ *and* $\alpha^2 + \beta^2$ *is not a square of* $\mathbb{F}_p$ *(which implies* $p \neq 2$*). Then the fixed point group of* $J_{X^{-1}I_{s,t}X}$ *over* $\mathrm{SO}(2n, k)$ *is the fixed point group of* $J_{X^{-1}I_{s,t}X}$ *over* $\mathrm{GL}(2n, k)$ *given in the previous proposition intersected with* $\mathrm{SO}(2n, k)$*.*

5.4 Results Critical to Computing Generalized Fixed-Point Groups and Whether They are Compact

This next lemma simplifies many proofs.

Lemma 13. *Let $A \in \mathrm{GL}(2n, k)$, $\mathrm{char}(k) \neq 2$. If $A^{-1}I_{s,t}A = I_{s,t}$ then A is a block matrix of the form $A = \begin{pmatrix} W & 0 \\ 0 & X \end{pmatrix}$, where W is $s \times s$ and X is $t \times t$.*

Proof. Assume $A^{-1}I_{s,t}A = I_{s,t}$. Then $I_{s,t}A = AI_{s,t}$. Let $A = \begin{pmatrix} W & X \\ Y & Z \end{pmatrix}$, where where W is $s \times s$, X is $s \times t$, Y is $t \times s$ and Z is $t \times t$. Then $AI_{s,t} = \begin{pmatrix} W & -X \\ Y & -Z \end{pmatrix}$ and $I_{s,t}A = \begin{pmatrix} W & X \\ -Y & -Z \end{pmatrix}$. Since these two matrices are equal and $\mathrm{char}(k) \neq 2$, it follows that $X = 0$ and $Y = 0$. Q.E.D.

Theorem 5. *Let $A \in \mathrm{SO}(2n, k)$, $A = X^{-1}I_{s,t}X$, and $XX^T = \mathrm{diag}(a_1, a_2, \ldots, a_{2n})$. Let $M_s = \mathrm{diag}(a_1, \ldots, a_s)$ and $M_t = \mathrm{diag}(a_{s+1}, \ldots, a_t)$. Then the fixed point group of J_A over $\mathrm{SO}(2n, k)$ is $G^{J_A} = \left\{ X^{-1} \mathrm{diag}(N_s, N_t)X \,|\, N_sM_sN_s^T = M_s, N_tM_tN_t^T = M_t \right\}$.*

Proof. Suppose $B \in G^{J_A}$. Then $A^{-1}BA = B \Rightarrow X^{-1}I_{s,t}XBX^{-1}I_{s,t}X = B$. Therefore $I_{s,t}XBX^{-1} = XBX^{-1}I_{s,t}$. By Lemma 13, that means $XBX^{-1} = \mathrm{diag}(N_s, N_t)$ where N_s is $s \times s$ and N_t is $t \times t$. Therefore, $B = X^{-1} \mathrm{diag}(N_s, N_t)X$, and because $B \in \mathrm{SO}(2n, k)$, $BB^T = I_{2n} \Rightarrow X^{-1} \mathrm{diag}(N_s, N_t)XX^T \mathrm{diag}(N_s^T, N_t^T)(X^{-1})^T = I_{2n}$.

Therefore, $\mathrm{diag}(N_s, N_t)XX^T \mathrm{diag}(N_s^T, N_t^T) = XX^T$ so $N_sM_sN_s^T = M_s$ and $N_tM_tN_t^T = M_t$ as claimed. Note that the case in $\mathrm{SO}(2n + 1, k)$, which was proven by Ling Wu, has a very similar proof, and as such I have borrowed his notation [11, Lemma 46 on p. 63]. Q.E.D.

Fixed-Point Group Computation Lemma 1. *Let $A, B \in \mathrm{GL}(n, k)$. Let $A = (a_{ij})$ and $B = \mathrm{diag}(b_1, \ldots, b_n)$. Then $ABA^T = B$ iff for all $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, two properties hold:*

1. $\displaystyle\sum_{\ell=1}^{n} a_{i\ell}^2 b_\ell = b_i$
2. $\displaystyle\sum_{\ell=1}^{n} a_{i\ell}a_{j\ell}b_\ell = 0$

Proof. Assume $ABA^T = B$. Then by computation, $AB = \begin{bmatrix} a_{11}b_1 & a_{12}b_2 & \dots & a_{1n}b_n \\ a_{21}b_1 & a_{22}b_2 & \dots & a_{2n}b_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}b_1 & a_{n2}b_2 & \dots & a_{nn}b_n \end{bmatrix}$.

Therefore, $ABA^T =$

$$\begin{bmatrix} a_{11}^2b_1 + \ldots + a_{1n}^2b_n & a_{11}a_{21}b_1 + \ldots + a_{1n}a_{2n}b_n & \dots & a_{11}a_{n1}b_1 + \ldots + a_{1n}a_{nn}b_n \\ a_{21}a_{11}b_1 + \ldots + a_{2n}a_{1n}b_n & a_{21}^2b_1 + \ldots + a_{2n}^2b_n & \dots & a_{21}a_{n1}b_1 + \ldots + a_{2n}a_{nn}b_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}a_{11}b_1 + \ldots + a_{nn}a_{1n}b_n & a_{n1}a_{21}b_1 + \ldots + a_{nn}a_{2n}b_n & \dots & a_{21}^2b_1 + \ldots + a_{2n}^2b_n \end{bmatrix}$$

From this computation, it can be seen that if $i, j \in \{1, 2, \ldots, n\}$ and $i \neq j$ then each entry in the diagonal spot (i, i) has the form $\displaystyle\sum_{\ell=1}^{n} a_{i\ell}^2 b_\ell$, which must be equal to b_i. Similarly, each entry in the spot (i, j) has the form $\displaystyle\sum_{\ell=1}^{n} a_{i\ell}a_{j\ell}b_\ell$ and it must equal zero.

Similarly, if $ABA^T \neq B$ then either property one or property two is not true for some entry (i, j) of ABA^T. Otherwise, by property one and by computation (as above), the diagonal elements of ABA^T are the same as the diagonal elements of B, and by property two and computation, the off-diagonal elements of ABA^T are all zero, so $ABA^T = B$. Q.E.D.

The next two lemmas give two matrices, of order two and three, respectively, that can be used in blocks to obtain any diagonal matrix over $\mathrm{SO}(2n, k)$, where $k = \mathbb{Q}_p$ and $p \equiv 1 \pmod 4$, given the right conditions on a and i. The fact that they can be so used is proven subsequently.

Fixed-Point Group Computation Lemma 2. *If* $A \in \mathrm{GL}(2, k)$,

$$A = \begin{bmatrix} \pm a & \pm\sqrt{\alpha - a^2} \\ \mp\sqrt{\beta(1 - a^2/\alpha)} & \pm a\sqrt{\frac{\beta}{\alpha}} \end{bmatrix}$$

where $a \in k$ *and every root in* A *is in* k *then* $AA^T = \mathrm{diag}(\alpha, \beta)$. *Similarly, if* $B = \mathrm{diag}(I_{n-2}, A) \in \mathrm{GL}(n, k)$ *then* $BB^T = \mathrm{diag}(I_{n-2}, \alpha, \beta)$. *Furthermore, any matrix* $C \in \mathrm{GL}(2, k)$ *such that* $CC^T = \mathrm{diag}(\alpha, \beta)$ *has this form.*

Proof. $AA^T = \begin{bmatrix} a^2+(\alpha-a^2) & -a\sqrt{\beta(1-a^2/\alpha)}+\sqrt{\alpha-a^2}a\sqrt{\frac{\beta}{\alpha}} \\ -a\sqrt{\beta(1-a^2/\alpha)}+\sqrt{\alpha-a^2}a\sqrt{\frac{\beta}{\alpha}} & \beta(1-a^2/\alpha)+a^2(\beta/\alpha) \end{bmatrix}$. That simplifies to $\mathrm{diag}(\alpha,\beta)$. Based on this, the second result is automatic.

To prove the last statement, let $C=(c_{ij})$. Then assume

$$CC^T = \begin{bmatrix} c_{11}^2+c_{12}^2 & c_{11}c_{21}+c_{12}c_{22} \\ c_{11}c_{21}+c_{12}c_{22} & c_{21}^2+c_{22}^2 \end{bmatrix} = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$$

That means $c_{12} = \pm\sqrt{\alpha-c_{11}^2}$, $c_{22} = \pm\sqrt{\alpha-c_{21}^2}$, and $c_{11}c_{21}+c_{12}c_{22} = 0 \Rightarrow c_{21} = \mp\sqrt{\beta(1-c_{11}^2/\alpha)}$, whence $c_{22} = \pm c_{11}\sqrt{\frac{\beta}{\alpha}}$. By computation, only the configuration of ± signs found in the statement of the Lemma will get the right result. Q.E.D.

Fixed-Point Group Computation Lemma 3. *If $A \in \mathrm{GL}(n,k)$, $n=3$,*

$$A = \begin{bmatrix} a & \sqrt{\alpha-a^2} & 0 \\ -i\sqrt{\frac{\beta(\alpha-a^2)}{\alpha\gamma}} & ia\sqrt{\frac{\beta}{\alpha\gamma}} & -\sqrt{\frac{\beta(\gamma-i^2)}{\gamma}} \\ -\sqrt{\frac{(\gamma-i^2)(\alpha-a^2)}{\alpha}} & a\sqrt{\frac{\gamma-i^2}{\alpha}} & i \end{bmatrix}$$

where $a,i \in k$, and every root in A is in k then $AA^T = \mathrm{diag}(\alpha,\beta,\gamma)$. Similarly, if $B = \mathrm{diag}(I_{n-2},A) \in \mathrm{GL}(n,k)$ then $BB^T = \mathrm{diag}(I_{n-3},\alpha,\beta,\gamma)$.

Proof. By laborious computation, $AA^T = \mathrm{diag}(\alpha,\beta,\gamma)$, and the second result is automatic. Q.E.D.

Fixed-Point Group Computation Lemma 4. *If $p \equiv 1 \pmod 4$ and $a \in \mathbb{Q}_p$ then every root in A in both of the previous two lemmas is in $\mathbb{Q}_p$ for $\alpha=\beta=1,p,N_p$, or pN_p or $\alpha\beta=1$ for appropriate a (in the first case corresponding to Fixed-Point Group Computation Lemma 2) and $\alpha=\beta=\gamma=1$ or $\alpha\beta\gamma=1$ for appropriate a and i (in the second case corresponding to Fixed-Point Group Computation Lemma 3). Also, one can replace $1,p,N_p$ or pN_p with a square of $\mathbb{Q}_p^*$ times $1,p,N_p$ or pN_p in the above equations. The cases $\alpha\beta=p,N_p$, or pN_p and $\alpha=\beta=\gamma=p,N_p$, or pN_p do not come out.*

Proof. From Fixed-Point Group Computation Lemma 2, if $\alpha=\beta=1$, I want to show $A = \begin{bmatrix} a & \sqrt{\alpha-a^2} \\ -\sqrt{\beta(1-a^2/\alpha)} & a\sqrt{\frac{\beta}{\alpha}} \end{bmatrix} \in \mathrm{GL}(2,k)$, $k=\mathbb{Q}_p$, $p \equiv 1 \pmod 4$. $\sqrt{\alpha-a^2} = \sqrt{1-a^2}$, and this works for $a = \pm 1$. Now set $\alpha = \beta = p$. Then $\sqrt{\alpha - a^2} = \sqrt{p - a^2}$. Since -1 is a square in this case, by Lemma 6, if $p - 1$ is a square in $\mathbb{Z}$ then there is nothing to show since I can set $a = 1$, so assume otherwise. By Proposition 7, for some $\alpha, \beta \in k$, $\alpha^2 + \beta^2 = p$, so set $a = \alpha$. A similar argument holds for $\alpha = N_p$ and $\alpha = pN_p$.

$-\sqrt{\beta(1 - a^2/\alpha)} = -\sqrt{\beta - a^2\beta/\alpha}$ and $\alpha = \beta$, so we have $-\sqrt{\beta - a^2}$ again, for which the result has been proven. Similarly, since $\alpha = \beta$, $a\sqrt{\frac{\beta}{\alpha}} = a \in k$.

Now suppose $\alpha\beta = 1$. Then it is easily seen that all of the terms in the matrix A from Fixed-Point Group Computation Lemma 2 are in $\mathbb{Q}_p$. If $\alpha\beta = p$, N_p, or pN_p, the case does not come out by Classification Lemma 3. Similar arguments will work for $-A$, since the terms in the radicals are the same.

If $\alpha = \beta = \gamma = 1$, then set $a = 0, \pm 1$ and $i = 0, \pm 1$ and one has it. If $\alpha\beta\gamma = 1$, then $\beta = \alpha^{-1}\gamma^{-1}$ so $-i\sqrt{\frac{\beta(\alpha - a^2)}{\alpha\gamma}} = -i\sqrt{\beta^2(\alpha - a^2)} = -i\beta\sqrt{\alpha - a^2}$, and this case has already been dealt with. Additionally, $ia\sqrt{\frac{\beta}{\alpha\gamma}} = ia\beta$ and $-\sqrt{\frac{\beta(\gamma - i^2)}{\gamma}} = -\sqrt{\gamma - i^2}$. Further, $-\sqrt{\frac{(\gamma - i^2)(\alpha - a^2)}{\alpha}} = -\sqrt{(\gamma - i^2)(1 - \alpha^{-1}a^2)}$ which is similar to other terms that have been dealt with, and the same is true for $a\sqrt{\frac{\gamma - i^2}{\alpha}}$.

Any of the above calculations will come out if $1, p, N_p$ or pN_p is replaced by a square of $\mathbb{Q}_p^*$ times $1, p, N_p$ or pN_p. A specific proof has been omitted because the calculations are essentially the same as the above.

Now consider the last case corresponding to Fixed-Point Group Computation Lemma 3. If $\alpha = \beta = \gamma = p$ then simplifying most of the terms is similar to what has been seen. However, it cannot be done simultaneously. For $ia\sqrt{\frac{\beta}{\alpha\gamma}} = ia\sqrt{\frac{p}{p^2}} = ia\sqrt{p^{-1}} = i\sqrt{p^{-1}a^2}$ meaning that $a = 0$, or alternatively, that $i = 0$. However, if either one of them is zero then there are other terms that don't come out. The cases $\alpha = \beta = \gamma = N_p$ and $\alpha = \beta = \gamma = pN_p$ are similar. Q.E.D.

Fixed-Point Group Computation Lemma 5. *For any diagonal matrix $C \in \mathrm{GL}(n, k)$, C is congruent over $\mathrm{SO}(n, k)$ to any diagonal matrix $D \in \mathrm{GL}(n, k)$ such that the elements of D are the transposed elements of C. So there are the same number of the same entries of C in D, just in different places.*

Proof. Consider the matrix $A_{ij} = (a_{\ell m})$ where A is the same as I_n except that for some $i, j \in \{1, 2, \dots, n\}$, $i > j$, $a_{ii} = a_{jj} = 0$, $a_{ij} = -1$, and $a_{ji} = 1$. It is clear that $|A_{ij}| = 1$ because one can take the determinant successively over every row except the i^{th} and j^{th} rows to obtain $1^{n-2} \begin{vmatrix} 0 & -1 \\ 1 & 0 \end{vmatrix} = 1$. Further, $A_{ij}A_{ij}^T = I_n$, so $A_{ij} \in \mathrm{SO}(n, k)$.

Now, $A_{ij}CA_{ij}^T = C^*$, where C^* has the same entries in the same places as C except that the i^{th} and j^{th} entries (counting by rows or columns) have been transposed. By picking successive, appropriate matrices $A_{\ell_\lambda m_\lambda}$, one can obtain $A_{\ell_1 m_1} \dots A_{\ell_\iota m_\iota} C A_{\ell_\iota m_\iota}^T \dots A_{\ell_1 m_1}^T = D$. Q.E.D.

Fixed-Point Group Computation Lemma 6. *If $p \equiv 3 \pmod 4$, for the matrix in Fixed-Point Group Computation Lemma 2, if it is in $\mathrm{GL}(n, k)$ and $k = \mathbb{Q}_p$ then it is impossible that $\alpha = p$. Similarly, if $p = 2$ then it is impossible that $\alpha = 3$ and that the matrix in Fixed-Point Group Computation Lemma 2 is in $\mathrm{GL}(n, k)$, $k = \mathbb{Q}_2$.*

Proof. This is a consequence of Corollary 1. In the first case, because p is not the sum of two squares, the term $\pm\sqrt{\alpha - a^2}$ cannot be in $\mathbb{Q}_p$. The second case is similar, since Corollary 1 states that 3 is not the sum of two squares in $k = \mathbb{Q}_2$. Q.E.D.

Fixed-Point Group Computation Lemma 7. *Over any p-adic field $\mathbb{Q}_p$, $\forall\, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Q}_p^*$, $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 = 0$ has a non-trivial solution. That implies $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = a_5$ has a solution. This result can be found in Scharlau [9, Theorem 6.3 on p. 187].*

Fixed-Point Group Computation Lemma 8. *If $\mathrm{diag}(\zeta_1, \dots, \zeta_m) \in \mathrm{GL}(m, \mathbb{Q}_p)$, $\prod_{i=1}^m \zeta_i \in \mathbb{Q}_p^{*2}$, and $m \geq 4$, $\exists\, A_0 \in \mathrm{GL}(m, \mathbb{Q}_p)$ such that $A_0A_0^T = \mathrm{diag}(\zeta_1, \dots, \zeta_m) \in \mathrm{GL}(m, \mathbb{Q}_p)$.*

Proof. By Fixed-Point Group Computation Lemma 7 and because the diagonal elements of $A_0A_0^T$ have the form $\sum_{j=0}^m \eta_{ij}^2$, $\eta_{ij} \in \mathbb{Q}_p$ in the i^{th} row of $A_0A_0^T$, one can get every necessary diagonal element in $A_0A_0^T$. As for the other elements, they can be made equal to zero by linear algebra. Q.E.D.

Lemma 14. *For any $A \in \mathrm{SO}(2,k)$, A has the form $\begin{bmatrix} \pm\sqrt{1-a^2} & a \\ -a & \pm\sqrt{1-a^2} \end{bmatrix}$ for some $a \in k$. If $-1 \in k^{*2}$, a can assume any value in k.*

Proof. Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \mathrm{SO}(2,k)$. Then $A^{-1} = A^T$ and $|A| = 1$, so

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

As a result, $a_{11} = a_{22}$ and $a_{21} = -a_{12}$. Thus, $A = \begin{bmatrix} a_{11} & a_{12} \\ -a_{12} & a_{11} \end{bmatrix}$.

Now, $|A| = 1 \Rightarrow a_{11}^2 + a_{12}^2 = 1$. This means that $a_{11} = \pm\sqrt{1-a_{12}^2}$ as claimed. If $-1 \notin k^{*2}$ and the field is well ordered, then $1 - a_{12}^2 \geq 0 \Rightarrow 1 \geq a_{12}^2 \Rightarrow 1 \geq a_{12} \geq -1$. (If the field is not well ordered but $-1 \notin k^{*2}$ there will still be a restriction on a_{12}.) Otherwise, there is no restriction on a_{12}. Q.E.D.

5.5 The Generalized P-Adic Fixed-Point Groups of Involution Isomorphy Classes

Proposition 12. *Let $k = \mathbb{Q}_p$, $-1 \in \mathbb{Q}_p^{*2}$, and $N_p \notin \mathbb{Q}_p^{*2}$. Then the fixed point groups G^{J_B} of the involution conjugacy classes of $\mathrm{SO}(2n,k)$ corresponding to an involution J_B, $B = B_0^{-1} I_{s,t} B_0$, which are given by Proposition 4 are listed in Table 5.1. Their properties of compactness or non-compactness are listed below. The entries of the table correspond to α, β, γ, and δ, which fill out the following summations, which correspond to $N_s N_s^T$ and $N_t N_t^T$: i. $\sum_{\ell=1}^{s-\alpha} \mu_{i\ell}^2 = \beta$, $\sum_{\ell=s+1}^{2n-\gamma} \nu_{i\ell}^2 = \delta$ and ii. $\sum_{\ell=1}^{s-\alpha} \mu_{i\ell}\mu_{j\ell} = \beta$, $\sum_{\ell=s+1}^{2n-\gamma} \nu_{i\ell}\nu_{j\ell} = \delta$. On the chart it is assumed that $i \neq j$, $\iota \neq \lambda$, $i,j \in \{1,2,\ldots,t\}$ and $\iota,\lambda \in \{s+1, s+2, \ldots, 2n\}$. Also, $G^{J_A} = \left\{A_0^{-1}\operatorname{diag}(N_s,N_t)A_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij})\right\}$ unless otherwise specified. If $N_s \in \mathrm{O}(s,k)$ or $N_t \in \mathrm{O}(t,k)$ then I have written "n/a" for α or γ and $\in \mathrm{O}(s,k)$ or $\in \mathrm{O}(t,k)$ for β or δ, respectively. The order of the items is the same order as can be found in Proposition 3.*

Table 5.1: The table of the fixed-point groups of involutions over $\mathrm{SO}(2n,k)$ *corresponding to Proposition 3, where* $k = \mathbb{Q}_p$ *and* $-1 \in \mathbb{Q}_p^{*2}$*. This chart corresponds with Proposition 12.*

Item	$\mathrm{diag}(b_1,\ldots,b_{2n})$	β
α	γ	δ
1.i.	I_{2n}	$\in \mathrm{O}(s,k)$
n/a	*n/a*	$\in \mathrm{O}(t,k)$
1.ii.	I_{2n}	$\in \mathrm{O}(s,k)$
n/a	*n/a*	$\in \mathrm{O}(t,k)$
2.i.	$\mathrm{diag}(1,\ldots,1,p,N_p, p^{-1}N_p^{-1})$	$\in \mathrm{O}(s,k)$
n/a	3	$1+(p-1)\delta_{\iota,2n-2}+ (N_p-1)\delta_{\iota,2n-1}+(p^{-1}N_p^{-1}-1)\delta_{\iota,2n} -p\nu_{\iota,2n-2}^2-N_p\nu_{\iota,2n-1}^2-p^{-1}N_p^{-1}\nu_{\iota,2n}^2$
2.ii.	$\mathrm{diag}(1,\ldots,1,p,N_p, p^{-1}N_p^{-1})$	$\in \mathrm{O}(s,k)$
n/a	3	$-\nu_{\iota,2n-2}\nu_{\lambda,2n-2}p-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}N_p- \nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}N_p^{-1}$
3.i.	$\mathrm{diag}(1,\ldots,1,p,N_p, p^{-1}N_p^{-1},1,\ldots,1)$	$1+(p-1)\delta_{i,s-2}+ (N_p-1)\delta_{i,s-1}+(p^{-1}N_p^{-1}-1)\delta_{is} -p\mu_{i,s-2}^2-N_p\mu_{i,s-1}^2-p^{-1}N_p^{-1}\mu_{is}^2$
3	*n/a*	$\in \mathrm{O}(t,k)$
3.ii.	$\mathrm{diag}(1,\ldots,1,p,N_p, p^{-1}N_p^{-1},1,\ldots,1)$	$-\mu_{i,s-2}\mu_{j,s-2}p- \mu_{i,s-1}\mu_{j,s-1}N_p-\mu_{is}\mu_{js}p^{-1}N_p^{-1}$
3	*n/a*	$\in \mathrm{O}(t,k)$
4.i.	$\mathrm{diag}(1,\ldots,1,p,N_p,p^{-1}N_p^{-1}, 1,\ldots,1,p,N_p,p^{-1}N_p^{-1})$	$1+(p-1)\delta_{i,s-2}+ (N_p-1)\delta_{i,s-1}+(p^{-1}N_p^{-1}-1)\delta_{is} -p\mu_{i,s-2}^2-N_p\mu_{i,s-1}^2-p^{-1}N_p^{-1}\mu_{is}^2$

Table 5.1: Continued

Item	$\operatorname{diag}(b_1, \ldots, b_{2n})$	β
α	γ	δ
3	3	$1 + (p-1)\delta_{\iota,2n-2}+$ $(N_p - 1)\delta_{\iota,2n-1} + (p^{-1}N_p^{-1} - 1)\delta_{\iota,2n}$ $-p\nu^2_{\iota,2n-2} - N_p\nu^2_{\iota,2n-1} - p^{-1}N_p^{-1}\nu^2_{\iota,2n}$
4.ii.	$\operatorname{diag}(1, \ldots, 1, p, N_p, p^{-1}N_p^{-1},$ $1, \ldots, 1, p, N_p, p^{-1}N_p^{-1})$	$-\mu_{i,s-2}\mu_{j,s-2}p-$ $\mu_{i,s-1}\mu_{j,s-1}N_p - \mu_{is}\mu_{js}p^{-1}N_p^{-1}$
3	3	$-\nu_{\iota,2n-2}\nu_{\lambda,2n-2}p - \nu_{\iota,2n-1}\nu_{\lambda,2n-1}N_p-$ $\nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}N_p^{-1}$
5.i.	$\operatorname{diag}(1, \ldots, 1, N_p, 1, \ldots, 1, N_p)$	$1 + (N_p - 1)\delta_{i,s} - N_p\mu^2_{i,s}$
1	1	$1 + (N_p - 1)\delta_{\iota,2n} - N_p\nu^2_{\iota,2n}$
5.ii.	$\operatorname{diag}(1, \ldots, 1, N_p, 1, \ldots, 1, N_p)$	$-\mu_{i,s}\mu_{j,s}N_p$
1	1	$-\nu_{\iota,2n}\nu_{\lambda,2n}N_p$
6.i.	$\operatorname{diag}(1, \ldots, 1, N_p, 1, \ldots,$ $1, p, p^{-1}N_p)$	$1 + (N_p - 1)\delta_{i,s} - N_p\mu^2_{i,s}$
1	2	$1 + (p-1)\delta_{\iota,2n-1} + (p^{-1}N_p - 1)\delta_{\iota,2n}$ $-p\nu_{\iota,2n-1} - p^{-1}N_p\nu^2_{\iota,2n}$
6.ii.	$\operatorname{diag}(1, \ldots, 1, N_p, 1, \ldots,$ $1, p, p^{-1}N_p)$	$-\mu_{i,s}\mu_{j,s}N_p$
1	2	$-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p - \nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}N_p$
7.i.	$\operatorname{diag}(1, \ldots, 1, p, p^{-1}N_p,$ $1, \ldots, 1, N_p)$	$1 + (p-1)\delta_{i,s-1} + (p^{-1}N_p - 1)\delta_{i,s}$ $-p\mu_{i,s-1} - p^{-1}N_p\mu^2_{is}$
2	1	$1 + (N_p - 1)\delta_{\iota,2n} - N_p\nu^2_{\iota,2n}$
7.ii.	$\operatorname{diag}(1, \ldots, 1, p, p^{-1}N_p,$ $1, \ldots, 1, N_p)$	$-\mu_{i,s-1}\mu_{j,s-1}p - \mu_{is}\mu_{js}p^{-1}N_p$
2	1	$-\nu_{\iota,2n}\nu_{\lambda,2n}N_p$
8.i.	$\operatorname{diag}(1, \ldots, 1, p, p^{-1}N_p,$ $1, \ldots, 1, p, p^{-1}N_p)$	$1 + (p-1)\delta_{i,s-1} + (p^{-1}N_p - 1)\delta_{i,s}$ $-p\mu_{i,s-1} - p^{-1}N_p\mu^2_{is}$
2	2	$1 + (p-1)\delta_{\iota,2n-1} + (p^{-1}N_p - 1)\delta_{\iota,2n}$ $-p\nu_{\iota,2n-1} - p^{-1}N_p\nu^2_{\iota,2n}$

Table 5.1: Continued

Item	$\mathrm{diag}(b_1, \ldots, b_{2n})$	β
α	γ	δ
8.ii.	$\mathrm{diag}(1, \ldots, 1, p, p^{-1}N_p,$ $1, \ldots, 1, p, p^{-1}N_p)$	$-\mu_{i,s-1}\mu_{j,s-1}p - \mu_{is}\mu_{js}p^{-1}N_p$
2	2	$-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p - \nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}N_p$
9.i.	$\mathrm{diag}(1, \ldots, 1, p, 1, \ldots, 1, p)$	$1 + (p-1)\delta_{i,s} - p\mu_{i,s}^2$
1	1	$1 + (p-1)\delta_{\iota,2n} - p\nu_{\iota,2n}^2$
9.ii.	$\mathrm{diag}(1, \ldots, 1, p, 1, \ldots, 1, p)$	$-\mu_{i,s}\mu_{j,s}p$
1	1	$-\nu_{\iota,2n}\nu_{\lambda,2n}p$
10.i.	$\mathrm{diag}(1, \ldots, 1, p, 1, \ldots,$ $1, N_p, pN_p^{-1})$	$1 + (p-1)\delta_{i,s} - p\mu_{i,s}^2$
1	2	$1 + (N_p - 1)\delta_{\iota,2n-1} + (pN_p^{-1} - 1)\delta_{\iota,2n}$ $-N_p\nu_{\iota,2n-1} - pN_p^{-1}\nu_{\iota,2n}^2$
10.ii.	$\mathrm{diag}(1, \ldots, 1, p, 1, \ldots,$ $1, N_p, pN_p^{-1})$	$-\mu_{i,s}\mu_{j,s}p$
1	2	$-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}N_p - \nu_{\iota,2n}\nu_{\lambda,2n}pN_p^{-1}$
11.i.	$\mathrm{diag}(1, \ldots, 1, N_p, pN_p^{-1},$ $1, \ldots, 1, p)$	$1 + (N_p - 1)\delta_{i,s-1} + (pN_p^{-1} - 1)\delta_{i,s}$ $-N_p\mu_{i,s-1} - pN_p^{-1}\mu_{is}^2$
2	1	$1 + (p-1)\delta_{\iota,2n} - p\nu_{\iota,2n}^2$
11.ii.	$\mathrm{diag}(1, \ldots, 1, N_p, pN_p^{-1},$ $1, \ldots, 1, p)$	$-\mu_{i,s-1}\mu_{j,s-1}N_p - \mu_{is}\mu_{js}pN_p^{-1}$
2	1	$-\nu_{\iota,2n}\nu_{\lambda,2n}p$
12.i.	$\mathrm{diag}(1, \ldots, 1, N_p, pN_p^{-1},$ $1, \ldots, 1, N_p, pN_p^{-1})$	$1 + (N_p - 1)\delta_{i,s-1} + (pN_p^{-1} - 1)\delta_{i,s}$ $-N_p\mu_{i,s-1} - pN_p^{-1}\mu_{is}^2$
2	2	$1 + (N_p - 1)\delta_{\iota,2n-1} + (pN_p^{-1} - 1)\delta_{\iota,2n}$ $-N_p\nu_{\iota,2n-1} - pN_p^{-1}\nu_{\iota,2n}^2$
12.ii.	$\mathrm{diag}(1, \ldots, 1, N_p, pN_p^{-1},$ $1, \ldots, 1, N_p, pN_p^{-1})$	$-\mu_{i,s-1}\mu_{j,s-1}N_p - \mu_{is}\mu_{js}pN_p^{-1}$
2	2	$-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}N_p - \nu_{\iota,2n}\nu_{\lambda,2n}pN_p^{-1}$

Table 5.1: Continued

Item	$\mathrm{diag}(b_1, \ldots, b_{2n})$	β
α	γ	δ
13.i.	$\mathrm{diag}(1, \ldots, 1, pN_p, 1, \ldots, 1, pN_p)$	$1 + (pN_p - 1)\delta_{i,s} - pN_p\mu_{i,s}^2$
1	1	$1 + (pN_p - 1)\delta_{\iota,2n} - pN_p\nu_{\iota,2n}^2$
13.ii.	$\mathrm{diag}(1, \ldots, 1, pN_p, 1, \ldots, 1, pN_p)$	$-\mu_{i,s}\mu_{j,s}pN_p$
1	1	$-\nu_{\iota,2n}\nu_{\lambda,2n}pN_p$
14.i.	$\mathrm{diag}(1, \ldots, 1, pN_p, 1, \ldots,$ $1, p, N_p)$	$1 + (pN_p - 1)\delta_{i,s} - pN_p\mu_{i,s}^2$
1	2	$1 + (p - 1)\delta_{\iota,2n-1} + (N_p - 1)\delta_{\iota,2n}$ $-p\nu_{\iota,2n-1} - N_p\nu_{\iota,2n}^2$
14.ii.	$\mathrm{diag}(1, \ldots, 1, pN_p, 1, \ldots,$ $1, p, N_p)$	$-\mu_{i,s}\mu_{j,s}pN_p$
1	2	$-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p - \nu_{\iota,2n}\nu_{\lambda,2n}N_p$
15.i.	$\mathrm{diag}(1, \ldots, 1, p, N_p,$ $1, \ldots, 1, pN_p$	$1 + (p - 1)\delta_{i,s-1} + (N_p - 1)\delta_{i,s}$ $-p\mu_{i,s-1} - N_p\mu_{is}^2$
2	1	$1 + (pN_p - 1)\delta_{\iota,2n} - pN_p\nu_{\iota,2n}^2$
15.ii.	$\mathrm{diag}(1, \ldots, 1, p, N_p,$ $1, \ldots, 1, pN_p$	$-\mu_{i,s-1}\mu_{j,s-1}p - \mu_{is}\mu_{js}N_p$
2	1	$-\nu_{\iota,2n}\nu_{\lambda,2n}pN_p$
16.i.	$\mathrm{diag}(1, \ldots, 1, p, N_p,$ $1, \ldots, 1, p, N_p)$	$1 + (p - 1)\delta_{i,s-1} + (N_p - 1)\delta_{i,s}$ $-p\mu_{i,s-1} - N_p\mu_{is}^2$
2	2	$1 + (p - 1)\delta_{\iota,2n-1} + (N_p - 1)\delta_{\iota,2n}$ $-p\nu_{\iota,2n-1} - N_p\nu_{\iota,2n}^2$
16.ii.	$\mathrm{diag}(1, \ldots, 1, p, N_p,$ $1, \ldots, 1, p, N_p)$	$-\mu_{i,s-1}\mu_{j,s-1}p - \mu_{is}\mu_{js}N_p$
2	2	$-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p - \nu_{\iota,2n}\nu_{\lambda,2n}N_p$

The results on the compactness of each isomorphism class with respect to conjugacy, a.k.a. each conjugacy class by abuse of notation, are listed below.

1. *Never compact*

2. *Never compact*

3. *Never compact*

4. *Never compact*

5. *Compact iff $s = t = 1$ (which implies the group is in $\mathrm{O}(2n, k)$, not $\mathrm{SO}(2n, k)$)*

6. *Never compact*

7. *Never compact*

8. *Compact iff $s = t = 2$*

9. *Compact iff $s = t = 1$ (which implies the group is in $\mathrm{O}(2n, k)$, not $\mathrm{SO}(2n, k)$)*

10. *Never compact*

11. *Never compact*

12. *Compact iff $s = t = 2$*

13. *Compact iff $s = t = 1$ (which implies the group is in $\mathrm{O}(2n, k)$, not $\mathrm{SO}(2n, k)$)*

14. *Never compact*

15. *Never compact*

16. *Compact iff $s = t = 2$*

Proof. The results about the fixed-point groups are simple usages of Theorem 5 and Fixed-Point Group Computation Lemma 1. As for compactness, any group in $\mathrm{SO}(2n, k)$ is compact iff it is closed and bounded, and because of the form of matrices in $\mathrm{SO}(2, k)$, which can be found in Lemma 14, $\mathrm{SO}(2, k)$ is unbounded. Therefore, any group of diagonal matrices that has a block consisting of matrices in $\mathrm{SO}(2, k)$ is not compact, and by Fixed-Point Group Computation Lemma 5, it is enough for a diagonal matrix to have two diagonal entries of 1. Therefore, whenever $s + t - \alpha - \gamma \geq 2$, the fixed-point group is not compact. (Recall that $s + t = 2n$, and that s and t must both be even for the corresponding matrix to be in $\mathrm{SO}(2n, k)$ instead of $\mathrm{O}(2n, k)$.)

Every fixed-point group listed in this proposition can be formed using the matrices listed in Fixed-Point Group Computation Lemmas 2 and 3 in appropriate blocks of different matrices. That is because of Fixed-Point Group Computation Lemma 4, which states that under the right conditions (which one is free to select) they are in $\mathrm{GL}(2, k)$ or $\mathrm{GL}(3, k)$, respectively. Because $s + t = 2n$ is even, whenever $\alpha + \gamma$ is odd and greater than one, the corresponding fixed-point group will not be compact. For 1 is a square, so the equation $x^2 + y^2 + z^2 = 1$ has an unbounded solution $x = p^{-m}$, $y = \sqrt{-1}p^{-m}$, $z = 1$, where $m \in \mathbb{N}$.

Consequently, there is an unbounded matrix in the corresponding fixed-point group, making the group itself non-compact.

As a result, whenever one has a 1 in the diagonal of $B_0 B_0^T$, the corresponding fixed-point group is non-compact. However, by Fixed-Point Group Computation Lemma 2, if there is no such entry of $B_0 B_0^T$ and s and t are small enough, then the fixed-point group is indeed compact. That requires $2n = \alpha + \gamma$, so $\alpha + \gamma$ must be even. Recall that because we do not want the identity mapping to be considered an involution, $s > 0$ and $t > 0$. Thus, $\alpha > 0$ and $\gamma > 0$ are necessary conditions of compactness, and α and γ must both be odd or even.

Case four presents a special case on $\mathrm{O}(2n, k)$. Over $\mathrm{SO}(2n, k)$ it is not compact because, to be in $\mathrm{SO}(2n, k)$, t must be even, so there is a diagonal entry of 1. However, even on $\mathrm{O}(2n, k)$ it is not compact because the smallest corresponding matrix is 6×6, so one is free to select one of the thirty-six entries of the matrix in the fixed-point group as p^{-m}, $m \in \mathbb{N}$ (the positive integers). That makes the matrix unbounded, hence the fixed-point group is not compact.

Similarly, in cases eight and twelve, one can make a 4×4 matrix A such that AA^T has the appropriate form by Classification Lemma 3. It need not be bounded because there are enough independent variables for one to be p^m, $m \in \mathbb{Z}$, just as I set the entry in spot $(1, 3)$ equal to zero in the matrix in Fixed-Point Group Computation Lemma 3. Q.E.D.

Proposition 13. *Let $k = \mathbb{Q}_p$ and $-1 \notin \mathbb{Q}_p^{*2}$. Then the fixed point groups G^{J_B} of the involution conjugacy classes of* $\mathrm{SO}(2n, k)$ *corresponding to an involution J_B, $B = B_0^{-1} I_{s,t} B_0$, which are given by Proposition 5 are listed in Table 5.2. Their properties of compactness or non-compactness are listed below. They are in tabular form, and the entries α, β, γ, and δ fill out the following summations, which correspond to $N_s N_s^T$ and $N_t N_t^T$: i. $\sum_{\ell=1}^{s-\alpha} \mu_{i\ell}^2 = \beta$, $\sum_{\ell=s+1}^{2n-\gamma} \nu_{i\ell}^2 = \delta$ and ii. $\sum_{\ell=1}^{s-\alpha} \mu_{i\ell}\mu_{j\ell} = \beta$, $\sum_{\ell=s+1}^{2n-\gamma} \nu_{i\ell}\nu_{j\ell} = \delta$. On the chart it is assumed that $i \neq j$, $\iota \neq \lambda$, $i, j \in \{1, 2, \ldots, t\}$ and $\iota, \lambda \in \{s+1, s+2, \ldots, 2n\}$. Also,*

$$G^{J_A} = \left\{ A_0^{-1} \operatorname{diag}(N_s, N_t) A_0 \,|\, N_s = (\mu_{ij}), N_t = (\nu_{ij}) \right\}$$

unless otherwise specified. If $N_s \in \mathrm{O}(s, k)$ or $N_t \in \mathrm{O}(t, k)$ then I have written "n/a" for α

or γ and $\in \mathrm{O}(s,k)$ or $\in \mathrm{O}(t,k)$ for β or δ, respectively. The order of the items is the same order as can be found in Proposition 5.

Table 5.2: The fixed-point groups of involutions over $\mathrm{SO}(2n,k)$ corresponding to Proposition 4, where $k=\mathbb{Q}_p$, $-1 \notin \mathbb{Q}_p^{*2}$, and $p \neq 2$. This chart corresponds with Proposition 13.

Item	$\mathrm{diag}(b_1,\dots,b_{2n})$	β
α	γ	δ
1.i.	I_{2n}	$\in \mathrm{O}(s,k)$
n/a	*n/a*	$\in \mathrm{O}(t,k)$
1.ii.	I_{2n}	$\in \mathrm{O}(s,k)$
n/a	*n/a*	$\in \mathrm{O}(t,k)$
2.i.	$\mathrm{diag}(1,\dots,1,p,p^{-1})$	$\in \mathrm{O}(s,k)$
n/a	2	$1+(p-1)\delta_{\iota,2n-1}+(p^{-1}-1)\delta_{\iota,2n}$ $-p\nu_{\iota,2n-1}^2-p^{-1}\nu_{\iota,2n}^2$
2.ii.	$\mathrm{diag}(1,\dots,1,p,p^{-1})$	$\in \mathrm{O}(s,k)$
n/a	2	$-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p-\nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}$
3.i.	$\mathrm{diag}(1,\dots,1,p,$ $p^{-1},1,\dots,1)$	$1+(p-1)\delta_{i,s-1}+(p^{-1}-1)\delta_{is}$ $-p\mu_{i,s-1}^2-p^{-1}\mu_{is}^2$
2	*n/a*	$\in \mathrm{O}(t,k)$
3.ii.	$\mathrm{diag}(1,\dots,1,p,$ $p^{-1},1,\dots,1)$	$\mu_{i,s-1}\mu_{j,s-1}p-\mu_{is}\mu_{js}p^{-1}$
2	*n/a*	$\in \mathrm{O}(t,k)$
4.i.	$\mathrm{diag}(1,\dots,1,p,p^{-1},$ $1,\dots,1,p,p^{-1})$	$1+(p-1)\delta_{i,s-1}+(p^{-1}-1)\delta_{is}$ $-p\mu_{i,s-1}^2-p^{-1}\mu_{is}^2$
2	2	$1+(p-1)\delta_{\iota,2n-1}+(p^{-1}-1)\delta_{\iota,2n}$ $-p\nu_{\iota,2n-1}^2-p^{-1}\nu_{\iota,2n}^2$
4.ii.	$\mathrm{diag}(1,\dots,1,p,p^{-1},$ $1,\dots,1,p,p^{-1})$	$\mu_{i,s-1}\mu_{j,s-1}p-\mu_{is}\mu_{js}p^{-1}$

Table 5.2: Continued

Item	$\mathrm{diag}(b_1, \ldots, b_{2n})$	β
α	γ	δ
2	2	$-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p - \nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}$
5.i.	$\mathrm{diag}(1, \ldots, 1, -1, 1, \ldots, 1, -1)$	$1 - 2\delta_{i,s} + \mu_{i,s}^2$
1	1	$1 - 2\delta_{\iota,2n} + \nu_{\iota,2n}^2$
5.ii.	$\mathrm{diag}(1, \ldots, 1, -1, 1, \ldots, 1, -1)$	$\mu_{i,s}\mu_{j,s}$
1	1	$\nu_{\iota,2n}\nu_{\lambda,2n}$
6.i.	$\mathrm{diag}(1, \ldots, 1, -1, 1, \ldots,$ $1, p, -p^{-1})$	$1 - 2\delta_{i,s} + \mu_{i,s}^2$
1	2	$1 + (p-1)\delta_{\iota,2n-1}+$ $(-p^{-1} - 1)\delta_{\iota,2n} - p\nu_{\iota,2n-1}$ $+p^{-1}\nu_{\iota,2n}^2$
6.ii.	$\mathrm{diag}(1, \ldots, 1, -1, 1, \ldots,$ $1, p, -p^{-1})$	$\mu_{i,s}\mu_{j,s}$
1	2	$-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p + \nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}$
7.i.	$\mathrm{diag}(1, \ldots, 1, p, -p^{-1},$ $1, \ldots, 1, -1)$	$1 + (p-1)\delta_{i,s-1} + (-p^{-1} - 1)\delta_{i,s}$ $-p\mu_{i,s-1} + p^{-1}\mu_{is}^2$
2	1	$1 - 2\delta_{\iota,2n} + \nu_{\iota,2n}^2$
7.ii.	$\mathrm{diag}(1, \ldots, 1, p, -p^{-1},$ $1, \ldots, 1, -1)$	$-\mu_{i,s-1}\mu_{j,s-1}p + \mu_{is}\mu_{js}p^{-1}$
2	1	$\nu_{\iota,2n}\nu_{\lambda,2n}$
8.i.	$\mathrm{diag}(1, \ldots, 1, p, -p^{-1},$ $1, \ldots, 1, p, -p^{-1})$	$1 + (p-1)\delta_{i,s-1}+$ $(-p^{-1} - 1)\delta_{i,s} - p\mu_{i,s-1} + p^{-1}\mu_{is}^2$
2	2	$1 + (p-1)\delta_{\iota,2n-1}+$ $(-p^{-1} - 1)\delta_{\iota,2n} - p\nu_{\iota,2n-1}$ $+p^{-1}\nu_{\iota,2n}^2$
8.ii.	$\mathrm{diag}(1, \ldots, 1, p, -p^{-1},$ $1, \ldots, 1, p, -p^{-1})$	$-\mu_{i,s-1}\mu_{j,s-1}p + \mu_{is}\mu_{js}p^{-1}$
2	2	$-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p + \nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}$

Table 5.2: Continued

Item	$\mathrm{diag}(b_1, \ldots, b_{2n})$	β
α	γ	δ
9.i.	$\mathrm{diag}(1, \ldots, 1, -1, -p, 1,$ $\ldots, 1, -1, -p)$	$1 - 2\delta_{i,s-1} + (-p-1)\delta_{i,s}$ $+\mu_{i,s-1}^2 + p\mu_{is}^2$
2	2	$1 - 2\delta_{\iota,2n-1} + (-p-1)\delta_{\iota,2n}$ $+\nu_{\iota,2n-1} + p\nu_{\iota,2n}^2$
9.ii.	$\mathrm{diag}(1, \ldots, 1, -1, -p, 1,$ $\ldots, 1, -1, -p)$	$\mu_{i,s-1}\mu_{j,s-1} + \mu_{i,s}\mu_{j,s}p$
2	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1} + \nu_{\iota,2n}\nu_{\lambda,2n}p$
10.i.	$\mathrm{diag}(1, \ldots, 1, -1, -p,$ $1, \ldots, 1, p)$	$1 - 2\delta_{i,s-1} + (-p-1)\delta_{i,s}$ $+\mu_{i,s-1}^2 + p\mu_{is}^2$
2	1	$1 + (p-1)\delta_{\iota,2n} - p\nu_{\iota,2n}^2$
10.ii.	$\mathrm{diag}(1, \ldots, 1, -1, -p,$ $1, \ldots, 1, p)$	$\mu_{i,s-1}\mu_{j,s-1} + \mu_{i,s}\mu_{j,s}p$
2	1	$-\nu_{\iota,2n}\nu_{\lambda,2n}p$
11.i.	$\mathrm{diag}(1, \ldots, 1, p, 1, \ldots,$ $1, -1, -p)$	$1 + (p-1)\delta_{i,s} - p\mu_{i,s}^2$
1	2	$1 - 2\delta_{\iota,2n-1} + (-p-1)\delta_{\iota,2n}$ $+\nu_{\iota,2n-1} + p\nu_{\iota,2n}^2$
11.ii.	$\mathrm{diag}(1, \ldots, 1, p, 1, \ldots,$ $1, -1, -p)$	$-\mu_{i,s}\mu_{j,s}p$
1	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1} + \nu_{\iota,2n}\nu_{\lambda,2n}p$
12.i.	$\mathrm{diag}(1, \ldots, 1, p,$ $1, \ldots, 1, p)$	$1 + (p-1)\delta_{i,s} - p\mu_{i,s}^2$
1	1	$1 + (p-1)\delta_{\iota,2n} - p\nu_{\iota,2n}^2$
12.ii.	$\mathrm{diag}(1, \ldots, 1, p,$ $1, \ldots, 1, p,)$	$-\mu_{i,s}\mu_{j,s}p$
1	1	$-\nu_{\iota,2n}\nu_{\lambda,2n}p$
13.i.	$\mathrm{diag}(1, \ldots, 1, -1, p, 1, \ldots, 1, -1, p)$	$1 - 2\delta_{i,s-1} + (p-1)\delta_{i,s}$ $+\mu_{i,s-1}^2 - p\mu_{is}^2$
2	2	$1 - 2\delta_{\iota,2n-1} + (p-1)\delta_{\iota,2n}$ $+\nu_{\iota,2n-1} - p\nu_{\iota,2n}^2$

Table 5.2: Continued

Item	$\mathrm{diag}(b_1, \ldots, b_{2n})$	β
α	γ	δ
13.ii.	$\mathrm{diag}(1, \ldots, 1, -1, p, 1, \ldots, 1, -1, p)$	$\mu_{i,s-1}\mu_{j,s-1} - \mu_{i,s}\mu_{j,s}p$
2	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1} - \nu_{\iota,2n}\nu_{\lambda,2n}p$
14.i.	$\mathrm{diag}(1, \ldots, 1, -1, p, 1, \ldots, 1, -p)$	$1 - 2\delta_{i,s-1} + (p-1)\delta_{i,s}$ $+\mu_{i,s-1}^2 - p\mu_{is}^2$
2	1	$1 + (-p-1)\delta_{\iota,2n} + p\nu_{\iota,2n}^2$
14.ii.	$\mathrm{diag}(1, \ldots, 1, -1, p, 1, \ldots, 1, -p)$	$\mu_{i,s-1}\mu_{j,s-1} - \mu_{i,s}\mu_{j,s}p$
2	1	$\nu_{\iota,2n}\nu_{\lambda,2n}p$
15.i.	$\mathrm{diag}(1, \ldots, 1, -p, 1, \ldots, 1, -1, p)$	$1 + (-p-1)\delta_{i,s} + p\mu_{is}^2$
1	2	$1 - 2\delta_{\iota,2n-1} + (p-1)\delta_{\iota,2n}$ $+\nu_{\iota,2n-1} - p\nu_{\iota,2n}^2$
15.ii.	$\mathrm{diag}(1, \ldots, 1, -p, 1, \ldots, 1, -1, p)$	$\mu_{i,s}\mu_{j,s}p$
1	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1} - \nu_{\iota,2n}\nu_{\lambda,2n}p$
16.i.	$\mathrm{diag}(1, \ldots, 1, -p, 1, \ldots, 1, -p)$	$1 + (-p-1)\delta_{i,s} + p\mu_{is}^2$
1	1	$1 + (-p-1)\delta_{\iota,2n} + p\nu_{\iota,2n}^2$
16.ii.	$\mathrm{diag}(1, \ldots, 1, -p, 1, \ldots, 1, -p)$	$\mu_{i,s}\mu_{j,s}p$
1	1	$\nu_{\iota,2n}\nu_{\lambda,2n}p$

1. *Never compact*

2. *Never compact (since $s > 0$)*

3. *Never compact (since $t > 0$)*

4. *Compact iff $s = t = 2$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$ has no unbounded solutions in $k = \mathbb{Q}_p$*

5. *Compact iff $s = t = 1$ (which implies the group is in $\mathrm{O}(2n, k)$, not $\mathrm{SO}(2n, k)$) and -1 is the sum of two squares in $k = \mathbb{Q}_p$*

6. *Compact iff $s = t = 2$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$ has no unbounded solution in $k = \mathbb{Q}_p$*

7. *Compact iff $s = t = 2$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$ has no unbounded solution in $k = \mathbb{Q}_p$*

8. *Compact iff $s = t = 2$, and $x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2 = -p$ have no unbounded solutions in $k = \mathbb{Q}_p$*

9. *Compact iff $s = t = 2$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2 = -1$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2 = -p$ have no unbounded solutions in $k = \mathbb{Q}_p$*

10. *Compact iff $s = t = 2$ and no square class has an unbounded solution if it is the sum of four squares*

11. *Compact iff $s = t = 2$ and no square class has an unbounded solution if it is the sum of four squares*

12. *Compact iff $s = t = 2$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$ has no unbounded solutions in $k = \mathbb{Q}_p$*

13. *Compact iff $s = t = 2$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2 = -1$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$ have no unbounded solutions in $k = \mathbb{Q}_p$*

14. *Compact iff $s = t = 2$ and no square class has an unbounded solution if it is the sum of four squares*

15. *Compact iff $s = t = 2$ and no square class has an unbounded solution if it is the sum of four squares*

16. *Compact iff $s = t = 1$ (which implies the group is in $\mathrm{O}(2n, k)$, not $\mathrm{SO}(2n, k)$) and $-p$ is the sum of two squares in k*

Proof. The results about the fixed-point groups are simple usages of Theorem 5 and Fixed-Point Group Computation Lemma 1. As for compactness, any group in $\mathrm{SO}(2n, k)$ is compact iff it is closed and bounded, and because of the form of matrices in $\mathrm{SO}(2, k)$, which can be found in Lemma 14, $\mathrm{SO}(2, k)$ is unbounded. Therefore, any group of diagonal matrices that has a block consisting of matrices in $\mathrm{SO}(2, k)$ is not compact, and by Fixed-Point Group Computation Lemma 5, it is enough for a diagonal matrix to have two diagonal entries of 1. Therefore, whenever $s + t - \alpha - \gamma \geq 2$, the fixed-point group is not compact. (Recall that $s + t = 2n$, and that s and t must both be even for the corresponding matrix to be in $\mathrm{SO}(2n, k)$ instead of $\mathrm{O}(2n, k)$.)

The compactness results come from a similar process as in the previous lemma. If $s + t$ is big enough, then there will be independent variables in the corresponding matrix B_0, i.e., one will be able to make B_0 unbounded. Unlike in the previous case, p is *never* the sum of two squares by Corollary 1. When $x_1^2+x_2^2+x_3^2+x_4^2=\alpha$ has an unbounded solution in $\mathbb{Q}_p$, if α is in the diagonal of $B_0B_0^T$, the corresponding fixed-point group is not compact. Otherwise, one needs to ones in the diagonal to get a matrix with a block congruent to $\mathrm{SO}(2,k)$ in the fixed-point group. Q.E.D.

Proposition 14. *Let $k=\mathbb{Q}_2$. Then the fixed point groups G^{J_B} of the involution conjugacy classes of $\mathrm{SO}(2n,k)$ corresponding to an involution J_A, $B=B_0^{-1}I_{s,t}B_0$, which are given by Proposition 6 are listed in Table 5.3. Their properties of compactness or non-compactness are listed below. The entries α, β, γ, and δ in the tables fill out the following summations, which correspond to $N_sN_s^T$ and $N_tN_t^T$: i. $\sum\limits_{\ell=1}^{s-\alpha}\mu_{i\ell}^2=\beta$, $\sum\limits_{\ell=s+1}^{2n-\gamma}\nu_{i\ell}^2=\delta$ and ii. $\sum\limits_{\ell=1}^{s-\alpha}\mu_{i\ell}\mu_{j\ell}=\beta$, $\sum\limits_{\ell=s+1}^{2n-\gamma}\nu_{i\ell}\nu_{j\ell}=\delta$. On the chart it is assumed that $i\neq j$, $\iota\neq\lambda$, $i,j\in\{1,2,\ldots,t\}$ and $\iota,\lambda\in\{s+1,s+2,\ldots,2n\}$. Also, $G^{J_B}=\left\{B_0^{-1}\operatorname{diag}(N_s,N_t)B_0\,|N_s=(\mu_{ij}),N_t=(\nu_{ij})\right\}$ unless otherwise specified. If $N_s\in\mathrm{O}(s,k)$ or $N_t\in\mathrm{O}(t,k)$ then I have written "n/a" for α or γ and $\in\mathrm{O}(s,k)$ or $\in\mathrm{O}(t,k)$ for β or δ, respectively. The order of the items is the same order as can be found in Proposition 6.*

Table 5.3: The fixed-point groups of isomorphism classes of involutions over $\mathrm{SO}(2n,k)$ where $k=\mathbb{Q}_2$. This chart corresponds with Proposition 14 and the order of the items in it correspond with Proposition 5.

Item	$B_0B_0^T$	β
α	γ	δ
1.i.	$\mathrm{diag}(1,\ldots,1,-1,-1,1,$ $\ldots,1,-1,-1)$	$1-2\delta_{i,s-1}+\mu_{i,s-1}^2-2\delta_{is}+\mu_{is}^2$
2	2	$1-2\delta_{\iota,2n-1}+\nu_{\iota,2n-1}^2-2\delta_{\iota,2n}+\nu_{\iota,2n}^2$
1.ii.	$\mathrm{diag}(1,\ldots,1,-1,-1,1,$ $\ldots,1,-1,-1)$	$\mu_{i,s-1}\mu_{j,s-1}+\mu_{is}\mu_{js}$
2	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}+\nu_{\iota,2n}\nu_{\lambda,2n}$

Table 5.3: Continued

Item	$B_0B_0^T$	β
α	γ	δ
2.i.	$\mathrm{diag}(1,\ldots,1,-1,-1,1,\ldots,1)$	$1-2\delta_{i,s-1}-2\delta_{i,s}+\mu^2_{i,s-1}+\mu^2_{i,s}$
2	*n/a*	$\in \mathrm{O}(t,k)$
2.ii.	$\mathrm{diag}(1,\ldots,1,-1,-1,1,\ldots,1)$	$\mu_{i,s-1}\mu_{j,s-1}+\mu_{is}\mu_{js}$
2	*n/a*	$\in \mathrm{O}(t,k)$
3.i.	$\mathrm{diag}(1,\ldots,1,-1,-1)$	$\in \mathrm{O}(s,k)$
n/a	2	$1-2\delta_{\iota,2n-1}-2\delta_{\iota,2n}+\nu^2_{\iota,2n-1}+\nu^2_{\iota,2n}$
3.ii.	$\mathrm{diag}(1,\ldots,1,-1,-1)$	$\in \mathrm{O}(s,k)$
n/a	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}+\nu_{\iota,2n}\nu_{\lambda,2n}$
4.i.	I_{2n}	$\in \mathrm{O}(s,k)$
n/a	*n/a*	$\in \mathrm{O}(t,k)$
4.ii.	I_{2n}	$\in \mathrm{O}(s,k)$
n/a	*n/a*	$\in \mathrm{O}(t,k)$
5.i.	$\mathrm{diag}(1,\ldots,1,-1,1,\ldots,-1)$	$1-2\delta_{is}+\mu^2_{is}$
1	1	$1-2\delta_{\iota,2n}+\nu^2_{\iota,2n}$
5.ii.	$\mathrm{diag}(1,\ldots,1,-1,1,\ldots,-1)$	$\mu_{is}\mu_{js}$
1	1	$\nu_{\iota,2n}\nu_{\lambda,2n}$
6.i.	$\mathrm{diag}(1,\ldots,1,-1,1,\ldots,1,3,-3^{-1})$	$1-2\delta_{is}+\mu^2_{is}$
1	2	$1+2\delta_{\iota,2n-1}+(-3^{-1}-1)\delta_{\iota,2n}$ $-3\nu^2_{\iota,2n-1}+3^{-1}\nu^2_{\iota,2n}$
6.ii.	$\mathrm{diag}(1,\ldots,1,-1,1,\ldots,1,3,-3^{-1})$	$\mu_{is}\mu_{js}$
1	2	$-3\nu_{\iota,2n-1}\nu_{\lambda,2n-1}+3^{-1}\nu_{\iota,2n}\nu_{\lambda,2n}$
7.i.	$\mathrm{diag}(1,\ldots,1,3,-3^{-1},1,\ldots,1,-1)$	$1+2\delta_{i,s-1}+(-3^{-1}-1)\delta_{is}$ $-3\mu^2_{i,s-1}+3^{-1}\mu^2_{is}$
2	1	$1-2\delta_{\iota,2n}+\mu^2_{\iota,2n}$

Table 5.3: Continued

Item	$B_0B_0^T$	β
α	γ	δ
7.ii.	$\mathrm{diag}(1,\ldots,1,3,-3^{-1},1,\ldots,1,-1)$	$-3\mu_{i,s-1}\nu_{j,s-1}+3^{-1}\mu_{is}\mu_{js}$
2	1	$\nu_{\iota,2n}\nu_{\lambda,2n}$
8.i.	$\mathrm{diag}(1,\ldots,1,3,-3^{-1},$ $1,\ldots,1,3,-3^{-1})$	$1+2\delta_{i,s-1}+(-3^{-1}-1)\delta_{is}$ $-3\mu^2_{i,s-1}+3^{-1}\mu^2_{is}$
2	2	$1+2\delta_{\iota,2n-1}+(-3^{-1}-1)\delta_{\iota,2n}$ $-3\nu^2_{\iota,2n-1}+3^{-1}\nu^2_{\iota,2n}$
8.ii.	$\mathrm{diag}(1,\ldots,1,3,-3^{-1},$ $1,\ldots,1,3,-3^{-1})$	$-3\mu_{i,s-1}\nu_{j,s-1}+3^{-1}\mu_{is}\mu_{js}$
2	2	$-3\nu_{\iota,2n-1}\nu_{\lambda,2n-1}+3^{-1}\nu_{\iota,2n}\nu_{\lambda,2n}$
9.i.	$\mathrm{diag}(1,\ldots,1,-1,-2,$ $1,\ldots,1,-1,-2)$	$1-2\delta_{i,s-1}-3\delta_{is}$ $+\mu^2_{i,s-1}+2\mu^2_{is}$
2	2	$1-2\delta_{\iota,2n-1}-3\delta_{\iota,2n}$ $+\nu^2_{\iota,2n-1}+2\nu^2_{\iota,2n}$
9.ii.	$\mathrm{diag}(1,\ldots,1,-1,-2,$ $1,\ldots,1,-1,-2)$	$\mu_{is}\mu_{js}+2\mu_{is}\mu_{js}$
2	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}+2\nu_{\iota,2n}\nu_{\lambda,2n}$
10.i.	$\mathrm{diag}(1,\ldots,1,-1,-2,$ $1,\ldots,1,2)$	$1-2\delta_{i,s-1}-3\delta_{is}$ $+\mu^2_{i,s-1}+2\mu^2_{is}$
2	1	$1+\delta_{\iota,2n}-2\nu^2_{\iota,2n}$
10.ii.	$\mathrm{diag}(1,\ldots,1,-1,-2,$ $1,\ldots,1,2)$	$\mu_{is}\mu_{js}+2\mu_{is}\mu_{js}$
2	1	$-2\nu_{\iota,2n}\nu_{\lambda,2n}$
11.i.	$\mathrm{diag}(1,\ldots,1,2,$ $1,\ldots,1,-1,-2)$	$1+\delta_{is}-2\mu^2_{is}$
1	2	$1-2\delta_{\iota,2n-1}-3\delta_{\iota,2n}$ $+\nu^2_{\iota,2n-1}+2\nu^2_{\iota,2n}$
11.ii.	$\mathrm{diag}(1,\ldots,1,2,$ $1,\ldots,1,-1,-2)$	$-2\mu_{is}\mu_{js}$
1	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}+2\nu_{\iota,2n}\nu_{\lambda,2n}$

Table 5.3: Continued

Item	$B_0B_0^T$	β
α	γ	δ
12.i.	$\mathrm{diag}(1,\ldots,1,2,$ $1,\ldots,1,2)$	$1+\delta_{is}-2\mu_{is}^2$
1	1	$1+\delta_{\iota,2n}-2\nu_{\iota,2n}^2$
12.ii.	$\mathrm{diag}(1,\ldots,1,2,$ $1,\ldots,1,2)$	$-2\mu_{is}\mu_{js}$
1	1	$-2\nu_{\iota,2n}\nu_{\lambda,2n}$
13.i.	$\mathrm{diag}(1,\ldots,1,-2,$ $1,\ldots,1,-2)$	$1-3\delta_{is}+2\mu_{is}^2$
1	1	$1-3\delta_{\iota,2n}+2\nu_{\iota,2n}^2$
13.ii.	$\mathrm{diag}(1,\ldots,1,-2,$ $1,\ldots,1,-2)$	$2\mu_{is}\mu_{js}$
1	1	$2\nu_{\iota,2n}\nu_{\lambda,2n}$
14.i.	$\mathrm{diag}(1,\ldots,1,-2,$ $1,\ldots,1,-1,2)$	$1-3\delta_{is}+2\mu_{is}^2$
1	2	$1-2\delta_{\iota,2n-1}+\delta_{\iota,2n}$ $+\nu_{\iota,2n-1}^2-2\nu_{\iota,2n}^2$
14.ii.	$\mathrm{diag}(1,\ldots,1,-2,$ $1,\ldots,1,-1,2)$	$-2\mu_{is}\mu_{js}$
1	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}-2\nu_{\iota,2n}\nu_{\lambda,2n}$
15.i.	$\mathrm{diag}(1,\ldots,1,-1,2,$ $1,\ldots,1,-2)$	$1-2\delta_{i,s-1}+\delta_{is}$ $+\mu_{i,s-1}^2-2\mu_{is}^2$
2	1	$1-3\delta_{\iota,2n}+2\nu_{\iota,2n}^2$
15.ii.	$\mathrm{diag}(1,\ldots,1,-1,2,$ $1,\ldots,1,-2)$	$\mu_{is}\mu_{js}-2\mu_{is}\mu_{js}$
2	1	$2\nu_{\iota,2n}\nu_{\lambda,2n}$
16.i.	$\mathrm{diag}(1,\ldots,1,-1,2,$ $1,\ldots,1,-1,2)$	$1-2\delta_{i,s-1}+\delta_{is}$ $+\mu_{i,s-1}^2-2\mu_{is}^2$
2	2	$1-2\delta_{\iota,2n-1}+\delta_{\iota,2n}$ $+\nu_{\iota,2n-1}^2-2\nu_{\iota,2n}^2$

Table 5.3: Continued

Item	$B_0B_0^T$	β
α	γ	δ
16.ii.	diag$(1,\dots,1,-1,2,$ $1,\dots,1,-1,2)$	$\mu_{is}\mu_{js} - 2\mu_{is}\mu_{js}$
2	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1} - 2\nu_{\iota,2n}\nu_{\lambda,2n}$
17.i.	diag$(1,\dots,1,3,$ $1,\dots,1,3)$	$1+2\delta_{is}-3\mu_{is}^2$
1	1	$1+2\delta_{\iota,2n}-3\nu_{\iota,2n}^2$
17.ii.	diag$(1,\dots,1,3,$ $1,\dots,1,3)$	$-3\mu_{is}\mu_{js}$
1	1	$-3\nu_{\iota,2n}\nu_{\lambda,2n}$
18.i.	diag$(1,\dots,1,3,1,$ $\dots,1,2,3\cdot 2^{-1})$	$1+2\delta_{is}-3\mu_{is}^2$
1	2	$1+\delta_{\iota,2n-1}+(3\cdot 2^{-1}-1)\delta_{\iota,2n}$ $-2\nu_{\iota,2n-1}^2 - 3\cdot 2^{-1}\nu_{\iota,2n}^2$
18.ii.	diag$(1,\dots,1,3,1,$ $\dots,1,2,3\cdot 2^{-1})$	$-3\mu_{is}\mu_{js}$
1	2	$-2\nu_{\iota,2n-1}\nu_{\lambda,2n-1} - 3\cdot 2^{-1}\nu_{\iota,2n}\nu_{\lambda,2n}$
19.i.	diag$(1,\dots,1,2,3\cdot 2^{-1},$ $1,\dots,1,3)$	$1+\delta_{i,s-1}+(3\cdot 2^{-1}-1)\delta_{is}$ $-2\mu_{i,s-1}^2 - 3\cdot 2^{-1}\mu_{is}^2$
2	1	$1+2\delta_{\iota,2n}-3\mu_{\iota,2n}^2$
19.ii.	diag$(1,\dots,1,2,3\cdot 2^{-1},$ $1,\dots,1,3)$	$-2\mu_{i,s-1}\mu_{j,s-1} - 3\cdot 2^{-1}\mu_{is}\mu_{js}$
2	1	$-3\mu_{\iota,2n}\mu_{\lambda,2n}$
20.i.	diag$(1,\dots,1,2,3\cdot 2^{-1},$ $1,\dots,1,2,3\cdot 2^{-1})$	$1+\delta_{i,s-1}+(3\cdot 2^{-1}-1)\delta_{is}$ $-2\mu_{i,s-1}^2 - 3\cdot 2^{-1}\mu_{is}^2$
2	2	$1+\delta_{\iota,2n-1}+(3\cdot 2^{-1}-1)\delta_{\iota,2n}$ $-2\nu_{\iota,2n-1}^2 - 3\cdot 2^{-1}\nu_{\iota,2n}^2$
20.ii.	diag$(1,\dots,1,2,3\cdot 2^{-1},$ $1,\dots,1,2,3\cdot 2^{-1})$	$-2\mu_{i,s-1}\mu_{j,s-1} - 3\cdot 2^{-1}\mu_{is}\mu_{js}$
2	2	$-2\nu_{\iota,2n-1}\nu_{\lambda,2n-1} - 3\cdot 2^{-1}\nu_{\iota,2n}\nu_{\lambda,2n}$

Table 5.3: Continued

Item	$B_0B_0^T$	β
α	γ	δ
21.i.	$\mathrm{diag}(1,\ldots,-3,1,1,\ldots,1,-3,1)$	$1-4\delta_{i,s-1}+3\mu_{i,s-1}^2-\mu_{is}^2$
2	2	$1-4\delta_{\iota,2n-1}+3\nu_{\iota,2n-1}^2-\nu_{\iota,2n}^2$
21.ii.	$\mathrm{diag}(1,\ldots,-3,1,1,\ldots,1,-3,1)$	$3\mu_{i,s-1}\mu_{j,s-1}-\mu_{is}\mu_{js}$
2	2	$3\nu_{\iota,2n-1}\nu_{\lambda,2n-1}-\nu_{\iota,2n}\nu_{\lambda,2n}$
22.i.	$\mathrm{diag}(1,\ldots,-3,1,1,\ldots,1,-3)$	$1-4\delta_{i,s-1}+3\mu_{i,s-1}^2-\mu_{is}^2$
2	1	$1-4\delta_{\iota,2n}+3\nu_{\iota,2n}^2$
22.ii.	$\mathrm{diag}(1,\ldots,-3,1,1,\ldots,1,-3)$	$3\mu_{i,s-1}\mu_{j,s-1}-\mu_{is}\mu_{js}$
2	1	$3\nu_{\iota,2n}\nu_{\lambda,2n}$
23.i.	$\mathrm{diag}(1,\ldots,-3,1,\ldots,1,-3,1)$	$1-4\delta_{is}+3\mu_{is}^2$
1	2	$1-4\delta_{\iota,2n-1}+3\nu_{\iota,2n-1}^2-\nu_{\iota,2n}^2$
23.ii.	$\mathrm{diag}(1,\ldots,-3,1,\ldots,1,-3,1)$	$3\mu_{is}\mu_{js}$
1	2	$3\nu_{\iota,2n-1}\nu_{\lambda,2n-1}-\nu_{\iota,2n}\nu_{\lambda,2n}$
24.i.	$\mathrm{diag}(1,\ldots,-3,1,\ldots,1,-3)$	$1-4\delta_{is}+3\mu_{is}^2$
1	1	$1-4\delta_{\iota,2n}+3\nu_{\iota,2n}^2$
24.ii.	$\mathrm{diag}(1,\ldots,-3,1,\ldots,1,-3)$	$3\mu_{is}\mu_{js}$
1	1	$3\nu_{\iota,2n}\nu_{\lambda,2n}$
25.i.	$\mathrm{diag}(1,\ldots,1,6,1,\ldots,1,6)$	$1+5\delta_{is}-6\mu_{is}^2$
1	1	$1+5\delta_{\iota,2n}-6\nu_{\iota,2n}^2$
25.ii.	$\mathrm{diag}(1,\ldots,1,6,1,\ldots,1,6)$	$-6\mu_{is}\mu_{js}$
1	1	$-6\nu_{\iota,2n}\nu_{\lambda,2n}$
26.i.	$\mathrm{diag}(1,\ldots,1,6,1,\ldots,1,6,1)$	$1+5\delta_{is}-6\mu_{is}^2$
1	2	$1+5\delta_{\iota,2n-1}-6\nu_{\iota,2n-1}^2-\nu_{\iota,2n}^2$
26.ii.	$\mathrm{diag}(1,\ldots,1,6,1,\ldots,1,6,1)$	$-6\mu_{is}\mu_{js}$

Table 5.3: Continued

Item	$B_0B_0^T$	β
α	γ	δ
1	2	$-6\nu_{\iota,2n-1}\nu_{\lambda,2n-1}-\nu_{\iota,2n}\nu_{\lambda,2n}$
27.i.	$\mathrm{diag}(1,\ldots,1,6,1,1,\ldots,1,6)$	$1+5\delta_{i,s-1}-6\mu_{i,s-1}^2-\mu_{is}^2$
2	1	$1+5\delta_{\iota,2n}-6\nu_{\iota,2n}^2$
27.ii.	$\mathrm{diag}(1,\ldots,1,6,1,1,\ldots,1,6)$	$-6\mu_{i,s-1}\mu_{j,s-1}-\mu_{is}\mu_{js}$
2	1	$-6\nu_{\iota,2n}\nu_{\lambda,2n}$
28.i.	$\mathrm{diag}(1,\ldots,1,6,1,1,\ldots,1,6,1)$	$1+5\delta_{i,s-1}-6\mu_{i,s-1}^2-\mu_{is}^2$
2	2	$1+5\delta_{\iota,2n-1}-6\nu_{\iota,2n-1}^2-\nu_{\iota,2n}^2$
28.ii.	$\mathrm{diag}(1,\ldots,1,6,1,1,\ldots,1,6,1)$	$-6\mu_{i,s-1}\mu_{j,s-1}-\mu_{is}\mu_{js}$
2	2	$-6\nu_{\iota,2n-1}\nu_{\lambda,2n-1}-\nu_{\iota,2n}\nu_{\lambda,2n}$
29.i.	$\mathrm{diag}(1,\ldots,1,-1,6,1,\ldots,1,-1,6)$	$1-2\delta_{i,s-1}+5\delta_{is}$ $+\mu_{i,s-1}^2-6\mu_{is}^2$
2	2	$1-2\delta_{\iota,2n-1}+5\delta_{\iota,2n}$ $+\nu_{\iota,2n-1}^2-6\nu_{\iota,2n}^2$
29.ii.	$\mathrm{diag}(1,\ldots,1,-1,6,1,\ldots,1,-1,6)$	$\mu_{i,s-1}\mu_{j,s-1}-6\mu_{is}\mu_{js}$
2	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}-6\nu_{\iota,2n}\nu_{\lambda,2n}$
30.i.	$\mathrm{diag}(1,\ldots,1,-1,6,1,\ldots,1,-6)$	$1-2\delta_{i,s-1}+5\delta_{is}$ $+\mu_{i,s-1}^2-6\mu_{is}^2$
2	1	$1-7\delta_{\iota,2n}+6\nu_{\iota,2n}^2$
30.ii.	$\mathrm{diag}(1,\ldots,1,-1,6,1,\ldots,1,-6)$	$\mu_{i,s-1}\mu_{j,s-1}-6\mu_{is}\mu_{js}$
2	1	$6\nu_{\iota,2n}\nu_{\lambda,2n}$
31.i.	$\mathrm{diag}(1,\ldots,1,-6,1,\ldots,1,-1,6)$	$1-7\delta_{is}+6\mu_{is}^2$
1	2	$1-2\delta_{\iota,2n-1}+5\delta_{\iota,2n}$ $+\nu_{\iota,2n-1}^2-6\nu_{\iota,2n}^2$
31.ii.	$\mathrm{diag}(1,\ldots,1,-6,1,\ldots,1,-1,6)$	$6\mu_{is}\mu_{js}$
1	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}-6\nu_{\iota,2n}\nu_{\lambda,2n}$

Table 5.3: Continued

Item	$B_0B_0^T$	β
α	γ	δ
32.i.	$\mathrm{diag}(1,\ldots,1,-6,1,\ldots,1,-6)$	$1-7\delta_{is}+6\mu_{is}^2$
1	1	$1-7\delta_{\iota,2n}+6\nu_{\iota,2n}^2$
32.ii.	$\mathrm{diag}(1,\ldots,1,-6,1,\ldots,1,-6)$	$6\mu_{is}\mu_{js}$
1	1	$6\nu_{\iota,2n}\nu_{\lambda,2n}$

Let "$(*)$" denote the equation $x_1^2+x_2^2+x_3^2+x_4^2=\upsilon$. Then the compactness conditions on $\mathbb{Q}_2$ are as follows:

1. *Compact iff $s=t=2$ and $(*)$ has no unbounded solution for $\upsilon=1$*

2. *Never compact (since $t>0$)*

3. *Never compact (since $s>0$)*

4. *Never compact*

5. *Compact iff $s=t=1$ (which implies the group is in $\mathrm{O}(2n,k)$, not $\mathrm{SO}(2n,k)$) and -1 is the sum of two squares in $k=\mathbb{Q}_2$*

6. *Compact iff $s=t=2$ and $(*)$ has no unbounded solution for $\upsilon=\pm1,\pm3$*

7. *Compact iff $s=t=2$ and $(*)$ has no unbounded solution for $\upsilon=\pm1,\pm3$*

8. *Compact iff $s=t=2$ and $(*)$ has no unbounded solution for $\upsilon=\pm1,\pm3$*

9. *Compact iff $s=t=2$ and $(*)$ has no unbounded solutions for $\upsilon=-1,-2$*

10. *Compact iff $s=t=2$ and $(*)$ has no unbounded solution for $\upsilon=\pm1,\pm2$*

11. *Compact iff $s=t=2$ and $(*)$ has no unbounded solution for $\upsilon=\pm1,\pm2$*

12. *Compact iff $s=t=1$ (which implies the group is in $\mathrm{O}(2n,k)$, not $\mathrm{SO}(2n,k)$)*

13. *Compact iff $s=t=1$ (which implies the group is in $\mathrm{O}(2n,k)$, not $\mathrm{SO}(2n,k)$) and -2 is the sum of two squares in $k=\mathbb{Q}_2$*

14. *Compact iff $s=t=2$ and $(*)$ has no unbounded solution for $\upsilon=\pm1,\pm2$*

15. *Compact iff $s=t=2$ and $(*)$ has no unbounded solution for $\upsilon=\pm1,\pm2$*

16. *Compact iff $s=t=2$ and $(*)$ has no unbounded solution for $\upsilon=-1,2$*

17. *Compact iff $s=t=1$ (which implies the group is in $\mathrm{O}(2n,k)$, not $\mathrm{SO}(2n,k)$) and 3 is the sum of two squares in $k=\mathbb{Q}_2$*

18. *Compact iff* $s = t = 2$ *and* $(*)$ *has no unbounded solution for* $v = 1, 2, 3, 6$

19. *Compact iff* $s = t = 2$ *and* $(*)$ *has no unbounded solution for* $v = 1, 2, 3, 6$

20. *Compact iff* $s = t = 2$ *and* $(*)$ *has no unbounded solution for* $v = 2, 6$

21. *Never compact*

22. *Never compact (since* $s = t$ *as we consider* $\mathrm{SO}(2n, k)$*, not* $\mathrm{SO}(n, k)$*)*

23. *Never compact*

24. *Compact iff* $s = t = 1$ *(which implies the group is in* $\mathrm{O}(2n, k)$*, not* $\mathrm{SO}(2n, k)$*) and* -3 *is the sum of two squares in* $k = \mathbb{Q}_2$

25. *Compact iff* $s = t = 1$ *(which implies the group is in* $\mathrm{O}(2n, k)$*, not* $\mathrm{SO}(2n, k)$*) and* 6 *is the sum of two squares in* $k = \mathbb{Q}_2$

26. *Never compact (since* $s = t$ *as we consider* $\mathrm{SO}(2n, k)$*, not* $\mathrm{SO}(n, k)$*)*

27. *Never compact (since* $s = t$ *as we consider* $\mathrm{SO}(2n, k)$*, not* $\mathrm{SO}(n, k)$*)*

28. *Never compact*

29. *Compact iff* $s = t = 2$ *and* $(*)$ *has no unbounded solution for* $v = -1, 6$

30. *Compact iff* $s = t = 2$ *and* $(*)$ *has no unbounded solution for* $v = \pm 1, \pm 6$

31. *Compact iff* $s = t = 2$ *and* $(*)$ *has no unbounded solution for* $v = \pm 1, \pm 6$

32. *Compact iff* $s = t = 1$ *(which implies the group is in* $\mathrm{O}(2n, k)$*, not* $\mathrm{SO}(2n, k)$*) and* -6 *is the sum of two squares in* $k = \mathbb{Q}_2$

Proof. The proof of this result is similar to the proof of the two previous results. Q.E.D.

Chapter 6

Involution Isomorphy Classes with Respect to Conjugation Classes over $\mathrm{SO}(2n, k)$ where $k = \mathbb{Q}_p$ Extended Quadratically to the Greatest Possible Extent

6.1 The Involution Isomorphy Classes over the Greatest Quadratic Extension of $\mathbb{Q}_p$

6.1.1 A Classification Result

My first proposition below is similar to the "Classification Lemmas" of a previous chapter, except that this proposition shows how many conjugacy classes of involutions there are over $\mathbb{Q}_p$ extended quadratically instead of on $\mathbb{Q}_p$.

Proposition 15. *Suppose J_A is an involution of $\mathrm{SO}(2n, k)$, where $A = A_0^{-1} I_{s,t} A_0$ and $A_0 \in \mathrm{GL}(2n, k)$ is such that $A_0 A_0^T = \mathrm{diag}(a_1, \ldots, a_{2n})$. Let k be the greatest possible quadratic* *extension of $\mathbb{Q}_p$, which is a finite extension of $\mathbb{Q}_p$ according to Classification Lemma 1. Then for each* $\mathrm{GL}(2n,k)$ *conjugacy class of J_A there are 16 possible* $\mathrm{SO}(2n,k)$ *conjugacy classes of J_A. They correspond with the Hasse symbol of the upper-left $s \times s$ block of $A_0A_0^T$, the Hasse symbol of the lower-right $t \times t$ block of $A_0A_0^T$, and* $\det(A_0A_0^T)$.

Proof. Let J_B be an involution of $\mathrm{SO}(2n,k)$, where $B = B_0^{-1}I_{s,t}B_0$ and $B_0 \in \mathrm{GL}(2n,k)$ is such that $B_0B_0^T = \mathrm{diag}(b_1,\dots,b_{2n})$. By the fourth part of Theorem 2, J_A is conjugate to J_B iff there is a $\tau \in \mathbb{Q}_p^*$ such that $a_1a_2\dots a_{2n} = \tau^2 b_1b_2\dots b_{2n}$, $c_p(a_1,a_2,\dots,a_s) = c_p(b_1,b_2,\dots,b_s)$, and $c_p(a_{s+1},a_{s+2},\dots,a_{2n}) = c_p(b_{s+1},b_{s+2},\dots,b_{2n})$. Now, if $a_1a_2\dots a_{2n}$ and $b_1b_2\dots b_{2n}$ are in the same coset of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ (which is also called a "square class"), then $\exists\ \tau \in \mathbb{Q}_p^* \ni a_1a_2\dots a_{2n} = \tau^2 b_1b_2\dots b_{2n}$, but not otherwise. Similarly, by the definition of the Hasse symbol, $c_p(a_1,a_2,\dots,a_s) = \pm1$ and $c_p(b_1,b_2,\dots,b_s) = \pm1$. Also, $c_p(a_{s+1},a_{s+2},\dots,a_{2n}) = \pm1$ and $c_p(b_{s+1},b_{s+2},\dots,b_{2n}) = \pm1$.

So for any involution J_B there are sixteen possibilities for the values of the representatives of $b_1b_2\dots b_{2n}$ in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, for $c_p(b_1,b_2,\dots,b_s)$, and for $c_p(b_{s+1},b_{s+2},\dots,b_{2n})$ since the first term can take on the values $1, p, N_p$, and pN_p and the following two terms can each take on two values, i.e., ±1.

Note that since the terms τ_1 and τ_2 from Theorem 2 are now in the extension of $\mathbb{Q}_p$ rather than $\mathbb{Q}_p$ itself, one need only consider the determinant of the entire matrix $A_0A_0^T$ rather than the determinants of the upper-left $s \times s$ block of $A_0A_0^T$ and of the lower-right $t \times t$ block of $A_0A_0^T$. For even if $\tau_1 \neq \tau_2$, one can always make $\tau_1^2 = \tau_2^2$. Q.E.D.

6.1.2 The Isomorphy Classes

Proposition 16. *Let the field under consideration be $k = \mathbb{Q}_p(\sqrt{p}, \sqrt{N_p})$, where $-1 \in \mathbb{Q}_p^{*2}$, $p \neq 2$, and $N_p \notin \mathbb{Q}_p^{*2}$. Then the isomorphy classes of involutions J_B of* $\mathrm{SO}(2n,k)$*, where $B = B_0^{-1}I_{s,t}B_0$, depend on the values of* $\det(B_0B_0^T)$, $c_p(b_1,\dots,b_s)$*, and* $c_p(b_{s+1},\dots,b_{2n})$ *in the following way:*

1. *$\forall\ s,t \geq 1$, if* $\det(B_0B_0^T) = 1$*, $c_p(b_1,\dots,b_s) = 1$, and $c_p(b_{s+1},\dots,b_{2n}) = 1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = I_{2n}$.*

2. *$\forall\ s, t \geq 1$, if $\det(B_0B_0^T) = N_p$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \mathrm{diag}(1, 1, \ldots, 1, N_p)$.*

3. *$\forall\ s \geq 1, t > 1$, if $\det(B_0B_0^T) = pN_p$ (a nonsquare in $\mathbb{Q}_p$), $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = -1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \mathrm{diag}(1, 1, \ldots, p, N_p)$.*

4. *$\forall\ s > 1, t \geq 1$, if $\det(B_0B_0^T) = pN_p$ (a nonsquare in $\mathbb{Q}_p$), $c_p(b_1, \ldots, b_s) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_{s-1} = p$, $b_s = N_p$, and all other $b_i = 1$.*

5. *$\forall\ s, t > 1$, if $\det(B_0B_0^T) = 1$, $c_p(b_1, \ldots, b_s) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = -1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_{s-1} = p$, $b_s = N_p$, $b_{2n-1} = p^{-1}$, $b_{2n} = N_p^{-1}$, and every other $b_i = 1$.*

6. *$\forall\ s \geq 1, t > 1$, if $\det(B_0B_0^T) = 1$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = -1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_s = p^{-1}N_p^{-1}$, $b_{2n-1} = p$, $b_{2n} = N_p$, and all other $b_i = 1$.*

7. *$\forall\ s > 1, t \geq 1$, if $\det(B_0B_0^T) = 1$, $c_p(b_1, \ldots, b_s) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_{s-1} = p$, $b_s = N_p$, $b_{2n} = p^{-1}N_p^{-1}$, and all other $b_i = 1$.*

8. *$\forall\ s > 2, t > 1$ (or vice versa), if $\det(B_0B_0^T) = N_p$, $c_p(b_1, \ldots, b_s) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = -1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_{s-2} = p$, $b_{s-1} = N_p$, $b_s = p^{-1}N_p^{-1}$, $b_{2n-1} = p$, and $b_{2n} = p^{-1}N_p$ (or one can switch the s and t portions to get $s > 1$, $t > 2$).*

9. *$\forall\ s \geq 1, t > 1$, if $\det(B_0B_0^T) = N_p$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = -1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_s = p^{-1}$, $b_{2n-1} = p$, $b_{2n} = N_p$, and all other $b_i = 1$.*

10. *$\forall\ s > 1, t \geq 1$, if $\det(B_0B_0^T) = N_p$, $c_p(b_1, \ldots, b_s) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \text{diag}(b_1, \ldots, b_{2n})$ where $b_{s-1} = p, b_s = N_p$, $b_{2n} = p^{-1}$, and all other $b_i = 1$.*

11. *$\forall\ s \geq 1, t \geq 1$, if $\det(B_0B_0^T) = pN_p$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \text{diag}(1, \ldots, 1, pN_p)$.*

12. *$\forall\ s > 2, t > 1$ (or vice versa), if $\det(B_0B_0^T) = pN_p$, $c_p(b_1, \ldots, b_s) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = -1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \text{diag}(b_1, \ldots, b_{2n})$ where $b_{s-2} = p$, $b_{s-1} = N_p$, $b_s = p^{-1}N_p^{-1}$, $b_{2n-1} = p$, and $b_{2n} = N_p$ (or one can switch the s and t portions to get $s > 1$, $t > 2$).*

13. *$\forall\ s \geq 1, t \geq 1$, if $\det(B_0B_0^T) = p$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \text{diag}(b_1, \ldots, b_{2n})$ where $b_s = N_p^{-1}$, $b_{2n} = pN_p$, and all other $b_i = 1$.*

14. *$\forall\ s > 1, t \geq 1$, if $\det(B_0B_0^T) = p$, $c_p(b_1, \ldots, b_s) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \text{diag}(b_1, \ldots, b_{2n})$ where $b_{s-1} = p, b_s = N_p$, $b_{2n} = N_p^{-1}$, and all other $b_i = 1$.*

15. *$\forall\ s \geq 1, t > 1$, if $\det(B_0B_0^T) = p$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = -1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \text{diag}(b_1, \ldots, b_{2n})$ where $b_s = N_p^{-1}$, $b_{2n-1} = p$, $b_{2n} = N_p$, and all other $b_i = 1$.*

16. *$\forall\ s > 2, t > 1$ (or vice versa), if $\det(B_0B_0^T) = p$, $c_p(b_1, \ldots, b_s) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = -1$ then B corresponds to an involution J_B with the representative $B_0B_0^T = \text{diag}(b_1, \ldots, b_{2n})$ where $b_{s-2} = p$, $b_{s-1} = N_p$, $b_s = p^{-1}N_p^{-1}$, $b_{2n-1} = pN_p$, and $b_{2n} = N_p^{-1}$ (or one can switch the s and t portions to get $s > 1$, $t > 2$).*

Proof. Firstly, if $a, b \in \mathbb{Q}_p$, $a = p^{m_1}a_0$, and $b = p^{m_2}b_0$ where a_0 and b_0 are p-adic units, then $(a, b)_p = (-1|p)^{m_1m_2}(a_1|p)^{m_2}(b_1|p)^{m_1}$ by Lemma 2. So if $a = p$ and $b = N_p$, then

$(p, N_p)_p = 1 \cdot (-1)^1 \cdot (-1)^0 = -1$. Therefore, $c_p(p, N_p) = c_p(1, 1, \ldots, 1, p, N_p) = -1$. Given that, we have the following.

$\boxed{1.}$ If $B_0B_0^T = I_{2n}$, then $\det(B_0B_0^T) = 1$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$. Furthermore, any matrix $A \in \mathrm{SO}(2n, k)$ with $A = A_0^{-1}I_{s,t}A_0$ such that $\det(A_0A_0^T) = \delta \in \mathbb{Q}_p^{*2}$, $c_p(a_1, \ldots, a_s) = 1$, and $c_p(a_{s+1}, \ldots, a_{2n}) = 1$ is congruent to B by part iv of Theorem 2. A similar fact will be true for the below statements as well for the same reason, so I will not repeat the argument thereof.

$\boxed{2.}$ If $B_0B_0^T = \mathrm{diag}(1, 1, \ldots, 1, N_p)$, then $\det(B_0B_0^T) = N_p$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$.

$\boxed{3.}$ If $B_0B_0^T = \mathrm{diag}(1, 1, \ldots, p, N_p)$ then $\det(B_0B_0^T) = pN_p$ (a nonsquare in $\mathbb{Q}_p$), $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = -1$.

$\boxed{4.}$ If $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_{s-1} = p$, $b_s = N_p$, and all other $b_i = 1$ then $\det(B_0B_0^T) = pN_p$ (a nonsquare in $\mathbb{Q}_p$), $c_p(b_1, \ldots, b_s) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$.

$\boxed{5.}$ If $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_{s-1} = p$, $b_s = N_p$, $b_{2n-1} = p^{-1}$, and $b_{2n} = N_p^{-1}$ then $\det(B_0B_0^T) = 1$, $c_p(b_1, \ldots, b_s) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = -1$.

$\boxed{6.}$ If $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_s = p^{-1}N_p^{-1}$, $b_{2n-1} = p$, $b_{2n} = N_p$, and all other $b_i = 1$ then $\det(B_0B_0^T) = 1$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = -1$.

$\boxed{7.}$ If $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_{s-1} = p$, $b_s = N_p$, $b_{2n} = p^{-1}N_p^{-1}$, and all other $b_i = 1$ then $\det(B_0B_0^T) = 1$, $c_p(b_1, \ldots, b_s) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$.

$\boxed{8.}$ If $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_{s-2} = p$, $b_{s-1} = N_p$, $b_s = p^{-1}N_p^{-1}$, $b_{2n-1} = p$, $b_{2n} = p^{-1}N_p$, and all other $b_i = 1$ then $\det(B_0B_0^T) = 1$, $c_p(b_1, \ldots, b_s) = (p, pN_p)_p(pN_p, 1)_p = (p, pN_p)_p = (1|p)^1(N_p|p)^1 = 1 \cdot (-1) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = (p, N_p)_p = (1|p)^0(N_p|p)^1 = -1$ by Lemma 2.

$\boxed{9.}$ The proofs of the remaining items are very similar, so they have been omitted. Please do beware of typos, reader. Q.E.D.

Proposition 17. *Let the field under consideration be $k = \mathbb{Q}_p(\sqrt{p}, \sqrt{-1})$, where $-1 \notin \mathbb{Q}_p^{*2}$ and $p \neq 2$. Then the isomorphy classes of involutions J_B of $\mathrm{SO}(2n, k)$, where $B = B_0^{-1}I_{s,t}B_0$, depend on the values of $\det(B_0B_0^T)$, $c_p(b_1, \ldots, b_s)$, and $c_p(b_{s+1}, \ldots, b_{2n})$ in the following way:*

1. *$\forall\ s, t \geq 1$, if $\det(B_0B_0^T) = 1$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$ then B*

corresponds to an involution J_B *with the representative* $B_0B_0^T = I_{2n}$.

2. $\forall\ s,t \geq 1$, *if* $\det(B_0B_0^T) = -1$, $c_p(b_1,\ldots,b_s) = 1$, *and* $c_p(b_{s+1},\ldots,b_{2n}) = 1$ *then* B *corresponds to an involution* J_B *with the representative* $B_0B_0^T = \mathrm{diag}(1,1,\ldots,1,-1)$.

3. $\forall\ s \geq 1, t > 1$, *if* $\det(B_0B_0^T) = -1$, $c_p(b_1,\ldots,b_s) = 1$, *and* $c_p(b_{s+1},\ldots,b_{2n}) = -1$ *then* B *corresponds to an involution* J_B *with the representative* $B_0B_0^T = \mathrm{diag}(b_1,\ldots,b_{2n})$ *where* $b_s = -1$, $b_{2n-1} = p$, $b_{2n} = p^{-1}$, *and all other* $b_i = 1$.

4. $\forall\ s > 1, t \geq 1$, *if* $\det(B_0B_0^T) = -1$, $c_p(b_1,\ldots,b_s) = -1$, *and* $c_p(b_{s+1},\ldots,b_{2n}) = 1$ *then* B *corresponds to an involution* J_B *with the representative* $B_0B_0^T = \mathrm{diag}(b_1,\ldots,b_{2n})$ *where* $b_{s-1} = p$, $b_s = p^{-1}$, $b_{2n} = -1$, *and all other* $b_i = 1$.

5. $\forall\ s,t > 1$, *if* $\det(B_0B_0^T) = 1$, $c_p(b_1,\ldots,b_s) = -1$, *and* $c_p(b_{s+1},\ldots,b_{2n}) = -1$ *then* B *corresponds to an involution* J_B *with the representative* $B_0B_0^T = \mathrm{diag}(b_1,\ldots,b_{2n})$ *where* $b_{s-1} = p$, $b_s = p^{-1}$, $b_{2n-1} = p$, *and* $b_{2n} = p^{-1}$.

6. $\forall\ s > 1, t \geq 1$, *if* $\det(B_0B_0^T) = 1$, $c_p(b_1,\ldots,b_s) = -1$, *and* $c_p(b_{s+1},\ldots,b_{2n}) = 1$ *then* B *corresponds to an involution* J_B *with the representative* $B_0B_0^T = \mathrm{diag}(b_1,\ldots,b_{2n})$ *where* $b_{s-1} = p$, $b_s = p^{-1}$, *and all other* $b_i = 1$.

7. $\forall\ s \geq 1, t > 1$, *if* $\det(B_0B_0^T) = 1$, $c_p(b_1,\ldots,b_s) = 1$, *and* $c_p(b_{s+1},\ldots,b_{2n}) = -1$ *then* B *corresponds to an involution* J_B *with the representative* $B_0B_0^T = \mathrm{diag}(1,1,\ldots,1,p, p^{-1})$.

8. $\forall\ s,t \geq 1$, *if* $\det(B_0B_0^T) = -1$, $c_p(b_1,\ldots,b_s) = -1$, *and* $c_p(b_{s+1},\ldots,b_{2n}) = -1$ *then* B *corresponds to an involution* J_B *with the representative* $B_0B_0^T = \mathrm{diag}(b_1,\ldots,b_{2n})$ *where* $b_s = p$, $b_{2n} = -p^{-1}$, *and all other* $b_i = 1$.

9. $\forall\ s \geq 1, t \geq 1$, *if* $\det(B_0B_0^T) = p$, $c_p(b_1,\ldots,b_s) = 1$, *and* $c_p(b_{s+1},\ldots,b_{2n}) = 1$ *then* B *corresponds to an involution* J_B *with the representative* $B_0B_0^T = \mathrm{diag}(b_1,\ldots,b_{2n})$ *where* $b_s = -1$, $b_{2n-1} = -1$, $b_{2n} = p$, *and all other* $b_i = 1$.

10. *$\forall\ s \geq 1, t \geq 1$, if* $\det(B_0B_0^T) = -p$, $c_p(b_1, \ldots, b_s) = 1$, *and* $c_p(b_{s+1}, \ldots, b_{2n}) = 1$ *then B corresponds to an involution J_B with the representative* $B_0B_0^T = \mathrm{diag}(1, \ldots, 1, -1, p)$.

11. *$\forall\ s \geq 1, t \geq 1$, if* $\det(B_0B_0^T) = p$, $c_p(b_1, \ldots, b_s) = -1$, *and* $c_p(b_{s+1}, \ldots, b_{2n}) = 1$ *then B corresponds to an involution J_B with the representative* $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ *where, $b_s = p$, and all other $b_i = 1$.*

12. *$\forall\ s \geq 1, t > 1$ (or vice versa), if* $\det(B_0B_0^T) = p$, $c_p(b_1, \ldots, b_s) = -1$, *and* $c_p(b_{s+1}, \ldots, b_{2n}) = -1$ *then B corresponds to an involution J_B with the representative* $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ *where $b_s = p$, $b_{2n-1} = p$, and $b_{2n} = p^{-1}$ (or one can switch the s and t portions to get $s > 1$, $t \geq 2$).*

13. *$\forall\ s, t \geq 1$, if* $\det(B_0B_0^T) = p$, $c_p(b_1, \ldots, b_s) = 1$, *and* $c_p(b_{s+1}, \ldots, b_{2n}) = -1$ *then B corresponds to an involution J_B with the representative* $B_0B_0^T = \mathrm{diag}(1, \ldots, 1, p)$.

14. *$\forall\ s, t \geq 1$, if* $\det(B_0B_0^T) = -p$, $c_p(b_1, \ldots, b_s) = -1$, *and* $c_p(b_{s+1}, \ldots, b_{2n}) = 1$ *then B corresponds to an involution J_B with the representative* $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ *where $b_s = -p$ and all other $b_i = 1$.*

15. *$\forall\ s \geq 1, t > 1$, if* $\det(B_0B_0^T) = -p$, $c_p(b_1, \ldots, b_s) = 1$, *and* $c_p(b_{s+1}, \ldots, b_{2n}) = -1$ *then B corresponds to an involution J_B with the representative* $B_0B_0^T = \mathrm{diag}(1, \ldots, 1, -p)$.

16. *$\forall\ s \geq 1, t > 1$ (or vice versa), if* $\det(B_0B_0^T) = -p$, $c_p(b_1, \ldots, b_s) = -1$, *and* $c_p(b_{s+1}, \ldots, b_{2n}) = -1$ *then B corresponds to an involution J_B with the representative* $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ *where $b_s = -p$, $b_{2n-1} = p$, and $b_{2n} = p^{-1}$ (or one can switch the s and t portions to get $s > 1$, $t \geq 1$).*

Proof. It must be observed that computing the Hasse symbol is more complex in this case because, given $\alpha \in \mathbb{Q}_p$ it is no longer necessarily true that $(-1, \alpha)_p = 1$.

$\boxed{1.}$ If $B_0B_0^T = I_{2n}$, then $\det(B_0B_0^T) = 1$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$. Furthermore, any matrix $A \in \mathrm{SO}(2n, k)$ with $A = A_0^{-1}I_{s,t}A_0$ such that $\det(A_0A_0^T) = \delta \in \mathbb{Q}_p^{*2}$, $c_p(a_1, \ldots, a_s) = 1$, and $c_p(a_{s+1}, \ldots, a_{2n}) = 1$ is congruent to B by part iv of Theorem 2. A similar fact will be true for the below statements as well for the same reason, so I will not repeat the argument thereof.

$\boxed{2.}$ If $B_0B_0^T = \mathrm{diag}(1, 1, \ldots, 1, -1)$, then $\det(B_0B_0^T) = -1$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$.

$\boxed{3.}$ If $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_s = -1$, $b_{2n-1} = p$, and $b_{2n} = p^{-1}$ and all other $b_i = 1$, then $\det(B_0B_0^T) = -1$, $c_p(b_1, \ldots, b_s) = 1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = (-1, -1)_p(p, -1)_p = (p, p)_p = -1$ by Lemmas 2 and 3.

$\boxed{4.}$ If $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ where $b_{s-1} = p$, $b_s = p^{-1}$, $b_{2n} = -1$, and all other $b_i = 1$ then $\det(B_0B_0^T) = -1$, $c_p(b_1, \ldots, b_s) = -1$, and $c_p(b_{s+1}, \ldots, b_{2n}) = 1$ for similar reasons as in item 3.

$\boxed{5.}$ This case holds for similar reasons as the previous cases.

$\boxed{6.}$ The proofs of the remaining items are very similar, so they have been omitted. Q.E.D.

Proposition 18. *Let the field under consideration be $k = \mathbb{Q}_2(\sqrt{-1}, \sqrt{2}, \sqrt{3})$. Then there is at least one isomorphy class of involutions J_A of $\mathrm{SO}(2n, k)$, where $A = A_0^{-1}I_{s,t}A_0$, for every possible value of the square class of $\det(A_0A_0^T)$, the value of $c_2(a_1, \ldots, a_s)$, and the value of $c_2(a_{s+1}, \ldots, a_{2n})$. Examples of each class are listed below.*

1. *$\forall\ s, t > 1$, if $\det(A_0A_0^T) = 1$, $c_2(a_1, \ldots, a_s) = 1$, and $c_2(a_{s+1}, \ldots, a_{2n}) = 1$ then A corresponds to an involution J_A with the representative $A_0A_0^T = \mathrm{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ where $a_s = -1$, $a_{2n} = -1$, and every other $a_i = 1$.*

2. *$\forall\ s \geq 1, t > 1$, if $\det(A_0A_0^T) = 1$, $c_2(a_1, \ldots, a_s) = -1$, and $c_2(a_{s+1}, \ldots, a_{2n}) = 1$ then A corresponds to an involution J_A with the representative $A_0A_0^T = \mathrm{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ where $a_{2n-1} = -1$, $a_{2n} = -1$, and every other $a_i = 1$.*

3. *$\forall\ s > 1, t \geq 1$, if $\det(A_0A_0^T) = 1$, $c_2(a_1, \ldots, a_s) = 1$, and $c_2(a_{s+1}, \ldots, a_{2n}) = -1$ then A corresponds to an involution J_A with the representative $A_0A_0^T = \mathrm{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ where $a_{s-1} = -1$, $a_s = -1$, and every other $a_i = 1$.*

4. *$\forall\ s, t \geq 1$, if $\det(A_0A_0^T) = 1$, $c_2(a_1, \ldots, a_s) = -1$, and $c_2(a_{s+1}, \ldots, a_{2n}) = -1$ then A corresponds to an involution J_A with the representative $A_0A_0^T = I_{2n}$.*

5. $\forall\ s \geq 3, t > 1$ *or* $s > 1, t \geq 3$, *if* $\det(A_0A_0^T) = -1$, $c_2(a_1,\ldots,a_s) = 1$, *and* $c_2(a_{s+1},\ldots,a_{2n}) = 1$ *then* A *corresponds to an involution* J_A *with the representative* $A_0A_0^T = \mathrm{diag}(a_1,a_2,\ldots,a_{2n-1},a_{2n})$ *where* $a_{s-2} = -1, a_{s-1} = -1, a_s = -1$, $a_{2n-1} = -1$, $a_{2n} = -1$, *and every other* $a_i = 1$.

6. $\forall\ s > 1, t \geq 1$, *if* $\det(A_0A_0^T) = -1$, $c_2(a_1,\ldots,a_s) = 1$, *and* $c_2(a_{s+1},\ldots,a_{2n}) = -1$ *then* A *corresponds to an involution* J_A *with the representative* $A_0A_0^T = \mathrm{diag}(a_1,a_2,\ldots,$ $a_{2n-1},a_{2n})$ *where* $a_s = -1$ *and every other* $a_i = 1$.

7. $\forall\ s \geq 1, t > 1$, *if* $\det(A_0A_0^T) = -1$, $c_2(a_1,\ldots,a_s) = -1$, *and* $c_2(a_{s+1},\ldots,a_{2n}) = 1$ *then* A *corresponds to an involution* J_A *with the representative* $A_0A_0^T = \mathrm{diag}(1,1,\ldots,1,$ $-1)$.

8. $\forall\ s \geq 1, t > 1$, *if* $\det(A_0A_0^T) = -1$, $c_2(a_1,\ldots,a_s) = -1$, *and* $c_2(a_{s+1},\ldots,a_{2n}) = -1$ *then* A *corresponds to an involution* J_A *with the representative* $A_0A_0^T = \mathrm{diag}(1,1,\ldots,1,$ $3,-3^{-1})$. *Or if one wants* $s > 1, t \geq 1$, *then* A *corresponds to an involution* J_A *with the representative* $A_0A_0^T = \mathrm{diag}(a_1,a_2,\ldots,a_{2n-1},a_{2n})$ *where* $a_{s-1} = 3$, $a_s = -3^{-1}$, *and every other* $a_i = 1$.

9. $\forall\ s,t > 1$, *if* $\det(A_0A_0^T) = 3$, $c_2(a_1,\ldots,a_s) = 1$, *and* $c_2(a_{s+1},\ldots,a_{2n}) = 1$ *then* A *corresponds to an involution* J_A *with the representative* $A_0A_0^T = \mathrm{diag}(a_1,a_2,\ldots,a_{2n-1},a_{2n})$ *where* $a_s = -1$, $a_{2n-1} = -1$, $a_{2n} = 3$ *and every other* $a_i = 1$.

10. $\forall\ s,t > 1$, *if* $\det(A_0A_0^T) = 3$, $c_2(a_1,\ldots,a_s) = 1$, *and* $c_2(a_{s+1},\ldots,a_{2n}) = -1$ *then* A *corresponds to an involution* J_A *with the representative* $A_0A_0^T = \mathrm{diag}(a_1,a_2,\ldots,a_{2n-1},$ $a_{2n})$ *where* $a_s = -1$, $a_{2n} = -3$, *and every other* $a_i = 1$.

11. $\forall\ s,t > 1$, *if* $\det(A_0A_0^T) = 3$, $c_2(a_1,\ldots,a_s) = -1$, *and* $c_2(a_{s+1},\ldots,a_{2n}) = 1$ *then* A *corresponds to an involution* J_A *with the representative* $A_0A_0^T = \mathrm{diag}(a_1,a_2,\ldots,a_{2n-1},$ $a_{2n})$ *where* $a_s = -3$, $a_{2n} = -1$, *and every other* $a_i = 1$.

12. $\forall\ s \geq 1, t > 1$, *if* $\det(A_0A_0^T) = 3$, $c_2(a_1,\ldots,a_s) = -1$, *and* $c_2(a_{s+1},\ldots,a_{2n}) = -1$ *then* A *corresponds to an involution* J_A *with the representative* $A_0A_0^T = \mathrm{diag}(1,1,\ldots,2,$

$3 \cdot 2^{-1}$). *Or if one wants $s > 1, t \geq 1$, then A corresponds to an involution J_A with the representative $A_0A_0^T = \mathrm{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ where $a_{s-1} = 2$, $a_s = 3 \cdot 2^{-1}$ and every other $a_i = 1$.*

13. $\forall\ s, t > 1$, *if* $\det(A_0A_0^T) = -3$, $c_2(a_1, \ldots, a_s) = 1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = 1$ *then A corresponds to an involution J_A with the representative* $A_0A_0^T = \mathrm{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_s = 3$, $a_{2n} = -1$, and every other $a_i = 1$.*

14. $\forall\ s \geq 1, t > 1$, *if* $\det(A_0A_0^T) = -3$, $c_2(a_1, \ldots, a_s) = 1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = -1$ *then A corresponds to an involution J_A with the representative* $A_0A_0^T = \mathrm{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_{s-1} = -1$, $a_s = 3$ and every other $a_i = 1$.*

15. $\forall\ s > 1, t \geq 1$, *if* $\det(A_0A_0^T) = -3$, $c_2(a_1, \ldots, a_s) = -1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = 1$ *then A corresponds to an involution J_A with the representative* $A_0A_0^T = \mathrm{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_{2n-1} = -1$, $a_{2n} = 3$ and every other $a_i = 1$.*

16. $\forall\ s \geq 1, t > 1$, *if* $\det(A_0A_0^T) = -3$, $c_2(a_1, \ldots, a_s) = -1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = -1$ *then A corresponds to an involution J_A with the representative* $A_0A_0^T = \mathrm{diag}(1, 1, \ldots, 1, -3)$. *Or if one wants $s > 1, t \geq 1$, then A corresponds to an involution J_A with the representative $A_0A_0^T = \mathrm{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ where $a_s = -3$ and every other $a_i = 1$.*

17. $\forall\ s, t > 1$, *if* $\det(A_0A_0^T) = 2$, $c_2(a_1, \ldots, a_s) = 1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = 1$ *then A corresponds to an involution J_A with the representative* $A_0A_0^T = \mathrm{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_{s-1} = -1$, $a_s = 2$, $a_{2n} = -1$, and every other $a_i = 1$.*

18. $\forall\ s > 1, t \geq 1$, *if* $\det(A_0A_0^T) = 2$, $c_2(a_1, \ldots, a_s) = 1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = -1$ *then A corresponds to an involution J_A with the representative* $A_0A_0^T = \mathrm{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_{s-1} = -1$, $a_s = -1$, $a_{2n} = 2$, and every other $a_i = 1$.*

19. $\forall\ s \geq 1, t > 1$, *if* $\det(A_0A_0^T) = 2$, $c_2(a_1, \ldots, a_s) = -1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = 1$ *then A corresponds to an involution J_A with the representative* $A_0A_0^T = \mathrm{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_s = 2$, $a_{2n-1} = -1$, $a_{2n} = -1$, and every other $a_i = 1$.*

20. $\forall\ s \geq 1, t > 1$, *if* $\det(A_0 A_0^T) = 2$, $c_2(a_1, \ldots, a_s) = -1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = -1$ *then A corresponds to an involution J_A with the representative* $A_0 A_0^T = \operatorname{diag}(1, 1, \ldots, 2)$*. Or if one wants $s > 1, t \geq 1$, then A corresponds to an involution J_A with the representative* $A_0 A_0^T = \operatorname{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_s = 2$ and every other $a_i = 1$.*

21. $\forall\ s, t > 1$, *if* $\det(A_0 A_0^T) = -2$, $c_2(a_1, \ldots, a_s) = 1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = 1$ *then A corresponds to an involution J_A with the representative* $A_0 A_0^T = \operatorname{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_s = -2$, $a_{2n-1} = -1$, $a_{2n} = -1$, and every other $a_i = 1$.*

22. $\forall\ s \geq 1, t > 1$, *if* $\det(A_0 A_0^T) = -2$, $c_2(a_1, \ldots, a_s) = 1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = -1$ *then A corresponds to an involution J_A with the representative* $A_0 A_0^T = \operatorname{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_s = -1$, $a_{2n} = 2$ and every other $a_i = 1$.*

23. $\forall\ s > 1, t \geq 1$, *if* $\det(A_0 A_0^T) = -2$, $c_2(a_1, \ldots, a_s) = -1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = 1$ *then A corresponds to an involution J_A with the representative* $A_0 A_0^T = \operatorname{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_s = 2$, $a_{2n} = -1$, and every other $a_i = 1$.*

24. $\forall\ s \geq 1, t > 1$, *if* $\det(A_0 A_0^T) = -2$, $c_2(a_1, \ldots, a_s) = -1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = -1$ *then A corresponds to an involution J_A with the representative* $A_0 A_0^T = \operatorname{diag}(1, \ldots, -1, 2)$*. Or if one wants $s > 1, t \geq 1$, then A corresponds to an involution J_A with the representative* $A_0 A_0^T = \operatorname{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_{s-1} = -1$, $a_s = 2$ and every other $a_i = 1$.*

25. $\forall\ s, t > 1$, *if* $\det(A_0 A_0^T) = 6$, $c_2(a_1, \ldots, a_s) = 1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = 1$ *then A corresponds to an involution J_A with the representative* $A_0 A_0^T = \operatorname{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_s = 6$, $a_{2n-1} = -1$, $a_{2n} = -1$, and every other $a_i = 1$.*

26. $\forall\ s > 1, t \geq 1$, *if* $\det(A_0 A_0^T) = 6$, $c_2(a_1, \ldots, a_s) = 1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = -1$ *then A corresponds to an involution J_A with the representative* $A_0 A_0^T = \operatorname{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ *where $a_s = -1$, $a_{2n} = -6$ and every other $a_i = 1$.*

27. $\forall\ s \geq 1, t > 1$, *if* $\det(A_0 A_0^T) = 6$, $c_2(a_1, \ldots, a_s) = -1$, *and* $c_2(a_{s+1}, \ldots, a_{2n}) = 1$ *then A corresponds to an involution J_A with the representative* $A_0 A_0^T = \operatorname{diag}(a_1, a_2, \ldots,$

$a_{2n-1}, a_{2n})$ where $a_s = -6$, $a_{2n} = -1$, and every other $a_i = 1$.

28. *$\forall\ s \geq 1, t > 1$, if $\det(A_0A_0^T) = 6$, $c_2(a_1, \ldots, a_s) = -1$, and $c_2(a_{s+1}, \ldots, a_{2n}) = -1$ then A corresponds to an involution J_A with the representative $A_0A_0^T = \operatorname{diag}(1, \ldots, 1, 6, 1)$. Or if one wants $s > 1, t \geq 1$, then A corresponds to an involution J_A with the representative $A_0A_0^T = \operatorname{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ where $a_{s-1} = -6$ and every other $a_i = 1$.*

29. *$\forall\ s, t > 1$, if $\det(A_0A_0^T) = -6$, $c_2(a_1, \ldots, a_s) = 1$, and $c_2(a_{s+1}, \ldots, a_{2n}) = 1$ then A corresponds to an involution J_A with the representative $A_0A_0^T = \operatorname{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ where $a_s = -1$, $a_{2n} = 6$, and every other $a_i = 1$.*

30. *$\forall\ s \geq 1, t > 1$, if $\det(A_0A_0^T) = -6$, $c_2(a_1, \ldots, a_s) = 1$, and $c_2(a_{s+1}, \ldots, a_{2n}) = -1$ then A corresponds to an involution J_A with the representative $A_0A_0^T = \operatorname{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ where $a_{s-1} = -1$, $a_s = 6$, and every other $a_i = 1$.*

31. *$\forall\ s \geq 1, t > 1$, if $\det(A_0A_0^T) = -6$, $c_2(a_1, \ldots, a_s) = -1$, and $c_2(a_{s+1}, \ldots, a_{2n}) = 1$ then A corresponds to an involution J_A with the representative $A_0A_0^T = \operatorname{diag}(1, \ldots, 1, -1, 6)$.*

32. *$\forall\ s \geq 1, t > 1$, if $\det(A_0A_0^T) = -6$, $c_2(a_1, \ldots, a_s) = -1$, and $c_2(a_{s+1}, \ldots, a_{2n}) = -1$ then A corresponds to an involution J_A with the representative $A_0A_0^T = \operatorname{diag}(1, \ldots, 1, -6)$. Or if one wants $s > 1, t \geq 1$, then A corresponds to an involution J_A with the representative $A_0A_0^T = \operatorname{diag}(a_1, a_2, \ldots, a_{2n-1}, a_{2n})$ where $a_s = -6$ and every other $a_i = 1$.*

Proof. $\boxed{1.}$ Firstly, $\det(A_0A_0^T) = a_1 \ldots a_{2n} = -1 \cdot (-1) = 1$. Secondly, $c_2(a_1, \ldots, a_s) = (-1, a_1 \ldots a_s)_2 \prod_{i=1}^{s-1}(a_1 \ldots a_i, -a_1 \ldots a_{i+1})_2 = (-1, 1)_2 \cdot \prod_{i=1}^{s-1} 1 = 1$. Similarly, $c_2(a_{s+1}, \ldots, a_{2n}) = 1$.

$\boxed{2.}$ $c_2(a_1, \ldots, a_s) = (-1, -1)_2 = -1$,

$$\begin{aligned} c_2(a_{s+1}, \ldots, a_{2n}) &= (-1, -1)_2 \cdot \textstyle\prod_{i=s+1}^{2n-1}(a_{s+1}a_{s+2} \ldots a_i, a_{s+1}a_{s+2} \ldots a_{i+1})_2 \\ &= (-1, -1)_2 \cdot (1, -1)_2(-1, -(-1)^2)_2 \end{aligned}$$

$$
\begin{aligned}
&= -1 \cdot 1 \cdot (-1,-1)_2 \\
&= -1 \cdot (-1) \\
&= 1
\end{aligned}
$$

$\boxed{3.}$ The proof of this result is almost identical to the above proof (just change the indices).

$\boxed{4.}$ In this case, it is clear that $\det(A_0A_0^T) = 1$. Furthermore, $c_2(a_1,\dots,a_s) = (-1, a_1 \dots a_s)_2 \cdot \prod_{i=1}^{s-1}(a_1 \dots a_i, -a_1 \dots a_{i+1})_2 = (-1,-1)_2 \cdot \prod_{i=1}^{s-1} 1 = -1$ because by Lemma 4, $(-1,-1)_2 = -1$. Similarly, $c_p(a_{s+1},\dots,a_{2n}) = -1$.

$\boxed{5.}$ Since five entries in $A_0A_0^T$ are -1 and the rest are 1, it is clear that $\det(A_0A_0^T) = -1$. $c_p(1,1,\dots,-1,-1,-1) = (-1,-(-1)^2)_2 \cdot (1,1)_2(-1,-1)_2(1,1)_2 = -1 \cdot (-1) = 1$. Further, $c_p(1,\dots,-1,-1) = (-1,-1^2)_2 \cdot (1,1)_2(-1,-1)_2 = 1$.

$\boxed{6.}$ $\det(A_0A_0^T) = -1$, $c_2(a_1,\dots,a_s) = -1$ as before, and $c_2(a_{s+1},\dots,a_{2n}) = 1$ as before.

$\boxed{7.}$ The proof of this result is similar to the previous one.

$\boxed{8.}$ $c_2(\mathrm{diag}(1,\dots,1,3,-3^{-1})) = (-1,1)_2(3,-1)_2 = -1$ by Lemma 4. Also, $\det(\mathrm{diag}(1,\dots,1,3,-3^{-1})) = -1$ and $c_2(1,\dots,1) = -1$.

$\boxed{9.}$ $c_2(\mathrm{diag}(a_1,\dots,a_s)) = 1$, $c_2(\mathrm{diag}(a_{s+1},\dots,a_{2n})) = (-1,-3)_2(1,3)_2 = 1$, and clearly $\det(A_0A_0^T) = 3$. Since these proofs are becoming highly repetitive, I have left it to the reader to verify the rest of them. Q.E.D.

6.2 The Fixed-Point Groups over $\mathbb{Q}_p$ Extended Quadratically as Much as Possible

Proposition 19. *Let $k = \mathbb{Q}_p(\sqrt{p}, \sqrt{N_p})$, $-1 \in \mathbb{Q}_p^{*2}$, and $N_p \notin \mathbb{Q}_p^{*2}$. Then the fixed point groups G^{J_B} of the involution conjugacy classes of* $\mathrm{SO}(2n,k)$ *corresponding to an involution J_B, $B = B_0^{-1}I_{s,t}B_0$, which are given by Proposition 16 are listed below, and none of them is compact. (Note that the size conditions on s and t and the conditions on* $\det(B_0B_0^T)$, *$c_p(b_1,\dots,b_s)$ and $c_p(b_{s+1},\dots,b_{2n})$ have been omitted from the items for the sake of brevity. The enumeration of them corresponds with their order in the list in Proposition 16 and all* *of these conditions can be found there.)*

1. *If* $B_0 B_0^T = I_{2n}$ *then*

$$G^{J_B} = \left\{ B_0^{-1} \operatorname{diag}(N_s, N_t) B_0 \middle| N_s \in \mathrm{O}(s,k), N_t \in \mathrm{O}(t,k), \det(N_s) = \det(N_t) = \pm 1 \right\}$$

2. *If* $B_0 B_0^T = \operatorname{diag}(1, 1, \ldots, 1, N_p)$ *then*

$$G^{J_B} = \left\{ B_0^{-1} \operatorname{diag}(N_s, N_t) B_0 \, | N_s \in \mathrm{O}(s,k), N_t = (\nu_{ij}) \right\}$$

where $\forall\ i, j \in \{s+1, s+2, \ldots, 2n\}$, $i \neq j$, $\det(N_s) = \det(N_t) = \pm 1$ *and the following are true:*

i. $\displaystyle\sum_{\ell=s+1}^{2n-1} \nu_{i1}^2 = 1 + (N_p - 1)\delta_{i,2n} - N_p \nu_{i,2n}^2$

ii. $\displaystyle\sum_{\ell=s+1}^{2n-1} \nu_{i\ell}\nu_{j\ell} = -\nu_{i,2n}\nu_{j,2n} N_p.$

3. *If* $B_0 B_0^T = \operatorname{diag}(1, 1, \ldots, p, N_p)$ *then*

$$G^{J_B} = \left\{ B_0^{-1} \operatorname{diag}(N_s, N_t) B_0 \, | N_s \in \mathrm{O}(s,k), N_t = (\nu_{ij}) \right\}$$

where $\forall\ i, j \in \{s+1, s+2, \ldots, 2n\}$, $i \neq j$, $\det(N_s) = \det(N_t) = \pm 1$ *and the following are true:*

i. $\displaystyle\sum_{\ell=s+1}^{2n-2} \nu_{i1}^2 = 1 + (p-1)\delta_{i,2n-1} + (N_p - 1)\delta_{i,2n} - p\nu_{i,2n-1}^2 - N_p \nu_{i,2n}^2$

ii. $\displaystyle\sum_{\ell=s+1}^{2n-2} \nu_{i\ell}\nu_{j\ell} = -\nu_{i,2n-1}\nu_{j,2n-1} p - \nu_{i,2n}\nu_{j,2n} N_p.$

4. *If* $B_0 B_0^T = \operatorname{diag}(b_1, \ldots, b_{2n})$ *where* $b_{s-1} = p$, $b_s = N_p$, *and all other* $b_i = 1$ *then*

$$G^{J_B} = \left\{ B_0^{-1} \operatorname{diag}(N_s, N_t) B_0 \, | N_s = (\nu_{ij}), N_t \in \mathrm{O}(t,k) \right\}$$

where $\forall\ i, j \in \{1, 2, \ldots, t\}$, $i \neq j$, $\det(N_s) = \det(N_t) = \pm 1$ *and the following are true:*

i. $\sum_{\ell=1}^{s-2} \nu_{i1}^2 = 1 + (p-1)\delta_{i,s-1} + (N_p - 1)\delta_{is} - p\nu_{i,s-1}^2 - N_p\nu_{is}^2$

ii. $\sum_{\ell=1}^{s-2} \nu_{i\ell}\nu_{j\ell} = -\nu_{i,s-1}\nu_{j,s-1}p - \nu_{is}\nu_{js}N_p.$

5. *If* $B_0B_0^T = \operatorname{diag}(b_1, \ldots, b_{2n})$ *where* $b_{s-1} = p$, $b_s = N_p$, $b_{2n-1} = p^{-1}$, $b_{2n} = N_p^{-1}$, *and every other* $b_i = 1$ *then*

$$G^{J_B} = \left\{B_0^{-1}\operatorname{diag}(N_s, N_t)B_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij})\right\}$$

where $\forall\, i, j \in \{1, 2, \ldots, t\}$, $i \neq j$, *and* $\forall\, \iota, \lambda \in \{s{+}1, s{+}2, \ldots, 2n\}$, $\iota \neq \lambda$, *the following are true:*

i. $\sum_{\ell=1}^{s-2} \mu_{i1}^2 = 1 + (p-1)\delta_{i,s-1} + (N_p - 1)\delta_{is} - p\mu_{i,s-1}^2 - N_p\mu_{is}^2$, $\sum_{\ell=s+1}^{2n-2} \nu_{\iota1}^2 = 1 + (p^{-1} - 1)\delta_{\iota,2n-1} + (N_p^{-1} - 1)\delta_{\iota,2n} - p^{-1}\nu_{\iota,2n-1}^2 - N_p^{-1}\nu_{\iota,2n}^2$

ii. $\sum_{\ell=1}^{s-2} \mu_{i\ell}\mu_{j\ell} = -\mu_{i,s-1}\mu_{j,s-1}p - \mu_{is}\mu_{js}N_p$, $\sum_{\ell=s+1}^{2n-2} \mu_{\iota\ell}\mu_{\lambda\ell} = -\mu_{\iota,2n-1}\mu_{\lambda,2n-1}p^{-1} - \mu_{\iota,2n}\mu_{\lambda,2n} N_p^{-1}$

6. *If* $B_0B_0^T = \operatorname{diag}(b_1, \ldots, b_{2n})$ *where* $b_s = p^{-1}N_p^{-1}$, $b_{2n-1} = p$, $b_{2n} = N_p$, *and all other* $b_i = 1$ *then*

$$G^{J_B} = \left\{B_0^{-1}\operatorname{diag}(N_s, N_t)B_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij})\right\}$$

where $\forall\, i, j \in \{1, 2, \ldots, t\}$, $i \neq j$, *and* $\forall\, \iota, \lambda \in \{s{+}1, s{+}2, \ldots, 2n\}$, $\iota \neq \lambda$, *the following are true:*

i. $\sum_{\ell=1}^{s-1} \mu_{i1}^2 = 1 + (p^{-1}N_p^{-1} - 1)\delta_{is} - p^{-1}N_p^{-1}\mu_{is}^2$, $\sum_{\ell=s+1}^{2n-2} \nu_{\iota1}^2 = 1 + (p-1)\delta_{\iota,2n-1} + (N_p - 1)\delta_{\iota,2n} - p\nu_{\iota,2n-1}^2 - N_p\nu_{\iota,2n}^2$

ii. $\sum_{\ell=1}^{s-1} \mu_{i\ell}\mu_{j\ell} = -\mu_{is}\mu_{js}p^{-1}N_p^{-1}$, $\sum_{\ell=s+1}^{2n-2} \nu_{\iota\ell}\nu_{\lambda\ell} = -\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p - \nu_{\iota,2n}\nu_{\lambda,2n}N_p$

7. *If* $B_0B_0^T = \operatorname{diag}(b_1, \ldots, b_{2n})$ *where* $b_{s-1} = p$, $b_s = N_p$, $b_{2n} = p^{-1}N_p^{-1}$, *and all other* $b_i = 1$ *then*

$$G^{J_B} = \left\{B_0^{-1}\operatorname{diag}(N_s, N_t)B_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij})\right\}$$

where $\forall\ i, j \in \{1, 2, \ldots, t\}$, $i \neq j$, *and* $\forall\ \iota, \lambda \in \{s+1, s+2, \ldots, 2n\}$, $\iota \neq \lambda$, *the following are true:*

i. $\displaystyle\sum_{\ell=1}^{s-2} \mu_{i1}^2 = 1+(p-1)\delta_{i,s-1}+(N_p-1)\delta_{i,s}-p\mu_{i,s-1}^2-N_p\mu_{i,s}^2$, $\displaystyle\sum_{\ell=s+1}^{2n-1} \nu_{\iota 1}^2 = 1+(p^{-1}N_p^{-1}-1)\delta_{\iota,2n} - p^{-1}N_p^{-1}\nu_{\iota,2n}^2$

ii. $\displaystyle\sum_{\ell=1}^{s-2} \mu_{i\ell}\mu_{j\ell} = -\mu_{i,s-1}\mu_{j,s-1}p - \mu_{is}\mu_{js}N_p$, $\displaystyle\sum_{\ell=s+1}^{2n-1} \nu_{\iota\ell}\nu_{\lambda\ell} = -\nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}N_p^{-1}$

8. *If* $B_0B_0^T = \operatorname{diag}(b_1, \ldots, b_{2n})$ *where* $b_{s-2} = p$, $b_{s-1} = N_p$, $b_s = p^{-1}N_p^{-1}$, $b_{2n-1} = p$, *and* $b_{2n} = p^{-1}N_p$ *then*

$$G^{J_B} = \left\{B_0^{-1}\operatorname{diag}(N_s, N_t)B_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij})\right\}$$

where $\forall\ i, j \in \{1, 2, \ldots, t\}$, $i \neq j$, *and* $\forall\ \iota, \lambda \in \{s+1, s+2, \ldots, 2n\}$, $\iota \neq \lambda$, *the following are true:*

i. $\displaystyle\sum_{\ell=1}^{s-3} \mu_{i1}^2 = 1+(p-1)\delta_{i,s-2}+(N_p-1)\delta_{i,s-1}+(p^{-1}N_p^{-1}-1)\delta_{is}-p\mu_{i,s-2}^2-N_p\mu_{i,s-1}^2 - p^{-1}N_p^{-1}\mu_{is}^2$, $\displaystyle\sum_{\ell=s+1}^{2n-2} \nu_{\iota 1}^2 = 1+(p-1)\delta_{\iota,2n-1}+(p^{-1}N_p-1)\delta_{\iota,2n} - p\nu_{\iota,2n-1} - p^{-1}N_p\nu_{\iota,2n}^2$

ii. $\displaystyle\sum_{\ell=1}^{s-3} \mu_{i\ell}\mu_{j\ell} = -\mu_{i,s-2}\mu_{j,s-2}p-\mu_{i,s-1}\mu_{j,s-1}N_p-\mu_{is}\mu_{js}p^{-1}N_p^{-1}$, $\displaystyle\sum_{\ell=s+1}^{2n-2} \nu_{\iota\ell}\nu_{\lambda\ell} = -\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p - \nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}N_p$

9. *If* $B_0B_0^T = \operatorname{diag}(b_1, \ldots, b_{2n})$ *where* $b_s = p^{-1}$, $b_{2n-1} = p$, $b_{2n} = N_p$, *and all other* $b_i = 1$ *then*

$$G^{J_B} = \left\{B_0^{-1}\operatorname{diag}(N_s, N_t)B_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij})\right\}$$

where $\forall\ i, j \in \{1, 2, \ldots, t\}$, $i \neq j$, *and* $\forall\ \iota, \lambda \in \{s+1, s+2, \ldots, 2n\}$, $\iota \neq \lambda$, *the following are true:*

i. $\sum_{\ell=1}^{s-1} \mu_{i1}^2 = 1 + (p^{-1} - 1)\delta_{is} - p^{-1}\mu_{is}^2$, $\sum_{\ell=s+1}^{2n-2} \nu_{\iota 1}^2 = 1 + (p-1)\delta_{\iota,2n-1} + (N_p - 1)\delta_{\iota,2n} - p\nu_{\iota,2n-1}^2 - N_p\nu_{\iota,2n}^2$

ii. $\sum_{\ell=1}^{s-1} \mu_{i\ell}\mu_{j\ell} = -\mu_{is}\mu_{js}p$, $\sum_{\ell=s+1}^{2n-2} \nu_{\iota\ell}\nu_{\lambda\ell} = -\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p - \nu_{\iota,2n}\nu_{\lambda,2n}N_p$

10. *If* $B_0 B_0^T = \operatorname{diag}(b_1, \ldots, b_{2n})$ *where* $b_{s-1} = p, b_s = N_p$, $b_{2n} = p^{-1}$, *and all other* $b_i = 1$ *then*

$$G^{J_B} = \left\{ B_0^{-1} \operatorname{diag}(N_s, N_t) B_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij}) \right\}$$

where $\forall\ i, j \in \{1, 2, \ldots, t\}$, $i \neq j$, *and* $\forall\ \iota, \lambda \in \{s{+}1, s{+}2, \ldots, 2n\}$, $\iota \neq \lambda$, *the following are true:*

i. $\sum_{\ell=1}^{s-2} \mu_{i1}^2 = 1 + (p-1)\delta_{i,s-1} + (N_p - 1)\delta_{i,s} - p\mu_{i,s-1}^2 - N_p\mu_{i,s}^2$, $\sum_{\ell=s+1}^{2n-1} \nu_{\iota 1}^2 = 1 + (p^{-1} - 1)\delta_{\iota,2n} - p^{-1}\nu_{\iota,2n}^2$

ii. $\sum_{\ell=1}^{s-2} \mu_{i\ell}\mu_{j\ell} = -\mu_{i,s-1}\mu_{j,s-1}p - \mu_{is}\mu_{js}N_p$, $\sum_{\ell=s+1}^{2n-1} \nu_{\iota\ell}\nu_{\lambda\ell} = -\nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}$

11. *If* $B_0 B_0^T = \operatorname{diag}(1, 1, \ldots, 1, pN_p)$ *then*

$$G^{J_B} = \left\{ B_0^{-1} \operatorname{diag}(N_s, N_t) B_0 \,|N_s \in \mathrm{O}(s, k), N_t = (\nu_{ij}) \right\}$$

where $\forall\ i, j \in \{s+1, s+2, \ldots, 2n\}$, $i \neq j$, $\det(N_s) = \det(N_t) = \pm 1$ *and the following are true:*

i. $\sum_{\ell=s+1}^{2n-1} \nu_{i1}^2 = 1 + (pN_p - 1)\delta_{i,2n} - pN_p\nu_{i,2n}^2$

ii. $\sum_{\ell=s+1}^{2n-1} \nu_{i\ell}\nu_{j\ell} = -\nu_{i,2n}\nu_{j,2n}pN_p.$

12. *If* $B_0 B_0^T = \operatorname{diag}(b_1, \ldots, b_{2n})$ *where* $b_{s-2} = p$, $b_{s-1} = N_p$, $b_s = p^{-1}N_p^{-1}$, $b_{2n-1} = p$, *and* $b_{2n} = N_p$ *then*

$$G^{J_B} = \left\{ B_0^{-1} \operatorname{diag}(N_s, N_t) B_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij}) \right\}$$

where $\forall\ i,j \in \{1,2,\dots,t\}$, $i \neq j$, *and* $\forall\ \iota,\lambda \in \{s+1, s+2, \dots, 2n\}$, $\iota \neq \lambda$, *the following are true:*

i. $\displaystyle\sum_{\ell=1}^{s-3} \mu_{i1}^2 = 1 + (p-1)\delta_{i,s-2} + (N_p - 1)\delta_{i,s-1} + (p^{-1}N_p^{-1} - 1)\delta_{is} - p\mu_{i,s-2}^2 - N_p\mu_{i,s-1}^2 - p^{-1}N_p^{-1}\mu_{is}^2$, $\displaystyle\sum_{\ell=s+1}^{2n-2} \nu_{\iota 1}^2 = 1 + (p-1)\delta_{\iota,2n-1} + (N_p - 1)\delta_{\iota,2n} - p\nu_{\iota,2n-1} - N_p\nu_{\iota,2n}^2$

ii. $\displaystyle\sum_{\ell=1}^{s-3} \mu_{i\ell}\mu_{j\ell} = -\mu_{i,s-2}\mu_{j,s-2}p - \mu_{i,s-1}\mu_{j,s-1}N_p - \mu_{is}\mu_{js}p^{-1}N_p^{-1}$, $\displaystyle\sum_{\ell=s+1}^{2n-2} \nu_{\iota\ell}\nu_{\lambda\ell} = -\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p - \nu_{\iota,2n}\nu_{\lambda,2n}N_p$

13. *If* $B_0B_0^T = \mathrm{diag}(b_1,\dots,b_{2n})$ *where* $b_s = N_p^{-1}$, $b_{2n} = pN_p$, *and all other* $b_i = 1$ *then*

$$G^{J_B} = \left\{ B_0^{-1}\,\mathrm{diag}(N_s, N_t)B_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij}) \right\}$$

where $\forall\ i,j \in \{1,2,\dots,t\}$, $i \neq j$, *and* $\forall\ \iota,\lambda \in \{s+1, s+2, \dots, 2n\}$, $\iota \neq \lambda$, *the following are true:*

i. $\displaystyle\sum_{\ell=1}^{s-1} \mu_{i1}^2 = 1 + (N_p^{-1} - 1)\delta_{i,s} - N_p^{-1}\mu_{i,s}^2$, $\displaystyle\sum_{\ell=s+1}^{2n-1} \nu_{\iota 1}^2 = 1 + (pN_p - 1)\delta_{\iota,2n} - pN_p\nu_{\iota,2n}^2$

ii. $\displaystyle\sum_{\ell=1}^{s-1} \mu_{i\ell}\mu_{j\ell} = -\mu_{is}\mu_{js}N_p^{-1}$, $\displaystyle\sum_{\ell=s+1}^{2n-1} \nu_{\iota\ell}\nu_{\lambda\ell} = -\nu_{\iota,2n}\nu_{\lambda,2n}pN_p$

14. *If* $B_0B_0^T = \mathrm{diag}(b_1,\dots,b_{2n})$ *where* $b_{s-1} = p, b_s = N_p$, $b_{2n} = N_p^{-1}$, *and all other* $b_i = 1$ *then*

$$G^{J_B} = \left\{ B_0^{-1}\,\mathrm{diag}(N_s, N_t)B_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij}) \right\}$$

where $\forall\ i,j \in \{1,2,\dots,t\}$, $i \neq j$, *and* $\forall\ \iota,\lambda \in \{s+1, s+2, \dots, 2n\}$, $\iota \neq \lambda$, *the following are true:*

i. $\displaystyle\sum_{\ell=1}^{s-2} \mu_{i1}^2 = 1 + (p-1)\delta_{i,s-1} + (N_p - 1)\delta_{i,s} - p\mu_{i,s-1}^2 - N_p\mu_{i,s}^2$, $\displaystyle\sum_{\ell=s+1}^{2n-1} \nu_{\iota 1}^2 = 1 + (N_p^{-1} - 1)\delta_{\iota,2n} - N_p^{-1}\nu_{\iota,2n}^2$

ii. $\displaystyle\sum_{\ell=1}^{s-2} \mu_{i\ell}\mu_{j\ell} = -\mu_{i,s-1}\mu_{j,s-1}p - \mu_{is}\mu_{js}N_p$, $\displaystyle\sum_{\ell=s+1}^{2n-1} \nu_{\iota\ell}\nu_{\lambda\ell} = -\nu_{\iota,2n}\nu_{\lambda,2n}N_p^{-1}$

15. *If* $B_0B_0^T = \operatorname{diag}(b_1, \ldots, b_{2n})$ *where* $b_s = N_p^{-1}$, $b_{2n-1} = p$, $b_{2n} = N_p$, *and all other* $b_i = 1$ *then*

$$G^{J_B} = \left\{ B_0^{-1} \operatorname{diag}(N_s, N_t) B_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij}) \right\}$$

where $\forall\ i, j \in \{1, 2, \ldots, t\}$, $i \neq j$, *and* $\forall\ \iota, \lambda \in \{s{+}1, s{+}2, \ldots, 2n\}$, $\iota \neq \lambda$, *the following are true:*

i. $\sum\limits_{\ell=1}^{s-1} \mu_{i1}^2 = 1 + (N_p^{-1} - 1)\delta_{is} - N_p^{-1}\mu_{is}^2$, $\sum\limits_{\ell=s+1}^{2n-2} \nu_{\iota 1}^2 = 1 + (p-1)\delta_{\iota,2n-1} + (N_p - 1)\delta_{\iota,2n} - p\nu_{\iota,2n-1}^2 - N_p\nu_{\iota,2n}^2$

ii. $\sum\limits_{\ell=1}^{s-1} \mu_{i\ell}\mu_{j\ell} = -\mu_{is}\mu_{js}N_p^{-1}$, $\sum\limits_{\ell=s+1}^{2n-2} \nu_{\iota\ell}\nu_{\lambda\ell} = -\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p - \nu_{\iota,2n}\nu_{\lambda,2n}N_p$

16. *If* $B_0B_0^T = \operatorname{diag}(b_1, \ldots, b_{2n})$ *where* $b_{s-2} = p$, $b_{s-1} = N_p$, $b_s = p^{-1}N_p^{-1}$, $b_{2n-1} = pN_p$, *and* $b_{2n} = N_p^{-1}$ *then*

$$G^{J_B} = \left\{ B_0^{-1} \operatorname{diag}(N_s, N_t) B_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij}) \right\}$$

where $\forall\ i, j \in \{1, 2, \ldots, t\}$, $i \neq j$, *and* $\forall\ \iota, \lambda \in \{s{+}1, s{+}2, \ldots, 2n\}$, $\iota \neq \lambda$, *the following are true:*

i. $\sum\limits_{\ell=1}^{s-3} \mu_{i1}^2 = 1 + (p-1)\delta_{i,s-2} + (N_p - 1)\delta_{i,s-1} + (p^{-1}N_p^{-1} - 1)\delta_{is} - p\mu_{i,s-2}^2 - N_p\mu_{i,s-1}^2 - p^{-1}N_p^{-1}\mu_{is}^2$, $\sum\limits_{\ell=s+1}^{2n-2} \nu_{\iota 1}^2 = 1 + (pN_p - 1)\delta_{\iota,2n-1} + (N_p^{-1} - 1)\delta_{\iota,2n} - pN_p\nu_{\iota,2n-1} - N_p^{-1}\nu_{\iota,2n}^2$

ii. $\sum\limits_{\ell=1}^{s-3} \mu_{i\ell}\mu_{j\ell} = -\mu_{i,s-2}\mu_{j,s-2}p - \mu_{i,s-1}\mu_{j,s-1}N_p - \mu_{is}\mu_{js}p^{-1}N_p^{-1}$, $\sum\limits_{\ell=s+1}^{2n-2} \nu_{\iota\ell}\nu_{\lambda\ell} = -\nu_{\iota,2n-1}\nu_{\lambda,2n-1}pN_p - \nu_{\iota,2n}\nu_{\lambda,2n}N_p^{-1}$

Proof. $\boxed{1.}$ This immediately follows from Proposition 26, which states that

$$G^{J_B} = \left\{ X^{-1} \operatorname{diag}(N_s, N_t) X \,\middle|\, N_sN_s^T = I_s, N_tN_t^T = I_t \right\}$$

This is the same as the given set. Note that if $\det(N_s) = \det(N_t) = -1$, $\det(X^{-1} \operatorname{diag}(N_s, N_t)\, X) = \det(N_s)\det(N_t) = 1$.

$\boxed{2.}$ This follows from Proposition 26 and Lemma 20. (Of course, I used the δ_{it} notation so I could write one formula corresponding to the diagonal elements of $N_t \operatorname{diag}(1, \dots, 1, N_p) N_t^T$ instead of two.)

The proofs of the remaining items are similar, and they have been omitted for brevity. As for compactness, every square root of every element in $\mathbb{Q}_p$ is in this quadratic extension field by Classification Lemma 1. Therefore, the matrices in Fixed-Point Group Computation Lemma 2 and Fixed-Point Group Computation Lemma 3 are in $\mathrm{SO}(2n, k)$ for every value of a and i. Recall that these matrices have the form $\begin{bmatrix} \pm a & \pm\sqrt{\alpha - a^2} \\ \mp\sqrt{\beta(1 - a^2/\alpha)} & \pm a\sqrt{\frac{\beta}{\alpha}} \end{bmatrix}$ and $\begin{bmatrix} a & \sqrt{\alpha - a^2} & 0 \\ -i\sqrt{\frac{\beta(\alpha-a^2)}{\alpha\gamma}} & ia\sqrt{\frac{\beta}{\alpha\gamma}} & -\sqrt{\frac{\beta(\gamma-i^2)}{\gamma}} \\ -\sqrt{\frac{(\gamma-i^2)(\alpha-a^2)}{\alpha}} & a\sqrt{\frac{\gamma-i^2}{\alpha}} & i \end{bmatrix}$. Therefore, one can *always* make the matrices corresponding to each fixed-point group unbounded, so none of them is compact. Q.E.D.

Proposition 20. *Let $k = \mathbb{Q}_p(\sqrt{p}, \sqrt{-1})$, where $-1 \notin \mathbb{Q}_p^{*2}$ and $p \neq 2$. Then the fixed point groups G^{J_B} of the involution conjugacy classes of* $\mathrm{SO}(2n, k)$ *corresponding to an involution J_B, $B = B_0^{-1} I_{s,t} B_0$, which are given by Proposition 17 are listed below, and none of them is compact. This time they are in tabular form, and the entries α, β, γ, and δ fill out the following summations, which correspond to $N_s N_s^T$ and $N_t N_t^T$: i.* $\sum_{\ell=1}^{s-\alpha} \mu_{i\ell}^2 = \beta$, $\sum_{\ell=s+1}^{2n-\gamma} \nu_{i\ell}^2 = \delta$ *and ii.* $\sum_{\ell=1}^{s-\alpha} \mu_{i\ell}\mu_{j\ell} = \beta$, $\sum_{\ell=s+1}^{2n-\gamma} \nu_{i\ell}\nu_{j\ell} = \delta$. *On the charts (but not elsewhere) it is assumed that $i \neq j$, $\iota \neq \lambda$, $i, j \in \{1, 2, \dots, t\}$ and $\iota, \lambda \in \{s+1, s+2, \dots, 2n\}$. Also, $G^{J_B} = \left\{B_0^{-1} \operatorname{diag}(N_s, N_t) B_0 \,|N_s = (\mu_{ij}), N_t = (\nu_{ij})\right\}$ unless otherwise specified. The order of the items is the same order as can be found in Proposition 17.*

1. *If $B_0 B_0^T = I_{2n}$ then*

$$G^{J_B} = \left\{B_0^{-1} \operatorname{diag}(N_s, N_t) B_0 \middle| N_s \in \mathrm{O}(s, k), N_t \in \mathrm{O}(t, k), \det(N_s) = \det(N_t) = \pm 1\right\}$$

2. *If $B_0 B_0^T = \operatorname{diag}(1, 1, \dots, 1, -1)$ then*

$$G^{J_B} = \left\{B_0^{-1} \operatorname{diag}(N_s, N_t) B_0 \,|N_s \in \mathrm{O}(s, k), N_t = (\nu_{ij})\right\}$$

where $\forall\ i, j \in \{s+1, s+2, \ldots, 2n\}$, $i \neq j$, $\det(N_s) = \det(N_t) = \pm 1$ *and the following are true:*

i. $\displaystyle\sum_{\ell=s+1}^{2n-1} \nu_{i1}^2 = 1 - 2\delta_{i,2n} + \nu_{i,2n}^2$

ii. $\displaystyle\sum_{\ell=s+1}^{2n-1} \nu_{i\ell}\nu_{j\ell} = \nu_{i,2n}\nu_{j,2n}.$

Tables listing the remaining fixed point groups in summarized form follow, together with full, unabbreviated items whenever $N_s \in \mathrm{O}(s,k)$ *or* $N_t \in \mathrm{O}(t,k)$. *The tables include the conditions on* $B_0B_0^T$ *in abbreviated form, the full versions of which can be found in Proposition 17. Note that the* δ *at the head of the last column is not the Krönecker delta function* $\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$*, but that this delta function is found in the summations.*

6. *If* $B_0B_0^T = \mathrm{diag}(b_1, \ldots, b_{2n})$ *where* $b_{s-1} = p$, $b_s = p^{-1}$, *and all other* $b_i = 1$ *then*

$$G^{J_B} = \left\{B_0^{-1}\,\mathrm{diag}(N_s, N_t)B_0\,|N_s = (\mu_{ij}), N_t \in \mathrm{O}(t,k)\right\}$$

where $\forall\ i, j \in \{1, 2, \ldots, s\}$, $i \neq j$, $\det(N_s) = \det(N_t) = \pm 1$ *and the following are true:*

i. $\displaystyle\sum_{\ell=1}^{s-2} \mu_{i1}^2 = 1 + (p-1)\delta_{i,s-1} + (p^{-1}-1)\delta_{i,s} - p\mu_{i,s-1}^2 - p^{-1}\mu_{i,s}^2$

ii. $\displaystyle\sum_{\ell=1}^{s-2} \mu_{i\ell}\mu_{j\ell} = -p\mu_{i,s-1}\mu_{j,s-1} - p^{-1}\mu_{is}\mu_{js}.$

7. *If* $B_0B_0^T = \mathrm{diag}(1, 1, \ldots, 1, p, p^{-1})$ *then*

$$G^{J_B} = \left\{B_0^{-1}\,\mathrm{diag}(N_s, N_t)B_0\,|N_s \in \mathrm{O}(s,k), N_t = (\nu_{ij}),\right\}$$

where $\forall\ i, j \in \{s+1, s+2, \ldots, 2n\}$, $i \neq j$, $\det(N_s) = \det(N_t) = \pm 1$ *and the following are true:*

i. $\displaystyle\sum_{\ell=s+1}^{2n-2} \nu_{i1}^2 = 1 + (p-1)\delta_{i,2n-1} + (p^{-1}-1)\delta_{i,2n} - p\nu_{i,2n-1}^2 - p^{-1}\nu_{i,2n}^2$

Table 6.1: The fixed-point groups of conjugacy classes three through five of involutions over $\mathrm{SO}(2n,k)$ where $k = \mathbb{Q}_p(\sqrt{p},\sqrt{-1})$, $-1 \notin \mathbb{Q}_p^{*2}$, and $p \neq 2$. The order corresponds with Proposition 17.

Item	$B_0B_0^T$	β
α	γ	δ
3.i.	$\operatorname{diag}(1,\ldots,-1,1,\ldots,p,p^{-1})$	$1-2\delta_{is}+\mu_{is}^2$
1	2	$1+(p-1)\delta_{\iota,2n-1}+(p^{-1}-1)\delta_{\iota,2n}$ $-p\nu_{\iota,2n-1}^2-p^{-1}\nu_{\iota,2n}^2$
3.ii.	$\operatorname{diag}(1,\ldots,-1,1,\ldots,p,p^{-1})$	$\mu_{is}\mu_{js}$
1	2	$-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p-\nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}$
4.i.	$\operatorname{diag}(1,\ldots,p,p^{-1},1,\ldots,-1)$	$1+(p-1)\delta_{i,s-1}+(p^{-1}-1)\delta_{is}$ $-p\mu_{i,s-1}^2-p^{-1}\mu_{is}^2$
2	1	$1-2\delta_{\iota,2n}+\nu_{\iota,2n}^2$
4.ii.	$\operatorname{diag}(1,\ldots,p,p^{-1},1,\ldots,-1)$	$\mu_{i,s-1}\mu_{j,s-1}p+\mu_{is}\mu_{js}p^{-1}$
2	1	$\nu_{\iota,2n}\nu_{\lambda,2n}$
5.i.	$\operatorname{diag}(1,\ldots,p,p^{-1},1,\ldots,p,p^{-1})$	$1+(p-1)\delta_{i,s-1}+(p^{-1}-1)\delta_{is}$ $-p\mu_{i,s-1}^2-p^{-1}\mu_{is}^2$
2	2	$1+(p-1)\delta_{\iota,2n-1}+(p^{-1}-1)\delta_{\iota,2n}$ $-p\nu_{\iota,2n-1}^2-p^{-1}\nu_{\iota,2n}^2$
5.ii.	$\operatorname{diag}(1,\ldots,p,p^{-1},1,\ldots,p,p^{-1})$	$\mu_{i,s-1}\mu_{j,s-1}p+\mu_{is}\mu_{js}p^{-1}$
2	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p+\nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}$

ii. $\displaystyle\sum_{\ell=s+1}^{2n-2}\nu_{i\ell}\nu_{j\ell} = -p\nu_{i,2n-1}\nu_{j,2n-1}-p^{-1}\nu_{i,2n}\nu_{j,2n}.$

10. *If* $B_0B_0^T = \operatorname{diag}(1,1,\ldots,1,-1,p)$ *then*

$$G^{J_B} = \left\{B_0^{-1}\operatorname{diag}(N_s,N_t)B_0 \,|\, N_s \in \mathrm{O}(s,k), N_t = (\nu_{ij}),\right\}$$

where $\forall\ i,j \in \{s+1,s+2,\ldots,2n\}$, $i \neq j$, $\det(N_s) = \det(N_t) = \pm 1$ *and the following are true:*

i. $\displaystyle\sum_{\ell=s+1}^{2n-1}\nu_{i1}^2 = 1-2\delta_{i,2n-1}+(p-1)\delta_{i,2n}+\nu_{i,2n-1}^2-p\nu_{i,2n}^2$

Table 6.2: The fixed-point groups of conjugacy classes eight and nine of involutions over $\mathrm{SO}(2n,k)$ where $k=\mathbb{Q}_p(\sqrt{p},\sqrt{-1})$, $-1\notin\mathbb{Q}_p^{*2}$, and $p\neq 2$

Item	$B_0B_0^T$	α
β	γ	δ
8.i.	$\mathrm{diag}(1,\ldots,p,1,\ldots,1,-p^{-1})$	1
$1+(p-1)\delta_{is}-p\mu_{is}^2$	1	$1+(-p^{-1}-1)\delta_{\iota,2n}+p^{-1}\nu_{\iota,2n}^2$
8.ii.	$\mathrm{diag}(1,\ldots,p,1,\ldots,1,-p^{-1})$	1
$-p\mu_{\iota s}\mu_{\lambda s}$	1	$p^{-1}\nu_{\iota,2n}\nu_{\lambda,2n}$
9.i.	$\mathrm{diag}(1,\ldots,-1,1,\ldots,-1,p)$	1
$1-2\delta_{is}+\mu_{is}^2$	2	$1-2\delta_{\iota,2n-1}+(p-1)\delta_{\iota,2n}$ $+\nu_{\iota,2n-1}^2-p\nu_{\iota,2n}^2$
9.ii.	$\mathrm{diag}(1,\ldots,-1,1,\ldots,-1,p)$	1
$\mu_{is}\mu_{js}$	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}-\nu_{\iota,2n}\nu_{\lambda,2n}p$

ii. $\displaystyle\sum_{\ell=s+1}^{2n-1}\nu_{i\ell}\nu_{j\ell}=\nu_{i,2n-1}\nu_{j,2n-1}-p\nu_{i,2n}\nu_{j,2n}.$

11. *If* $B_0B_0^T=\mathrm{diag}(b_1,\ldots,b_{2n})$ *where,* $b_s=p$*, and all other* $b_i=1$ *then*

$$G^{J_B}=\left\{B_0^{-1}\,\mathrm{diag}(N_s,N_t)B_0\,|N_s=(\mu_{ij}),N_t\in\mathrm{O}(t,k)\right\}$$

where $\forall\ i,j\in\{1,2,\ldots,s\}$*,* $i\neq j$*,* $\det(N_s)=\det(N_t)=\pm1$ *and the following are true:*

i. $\displaystyle\sum_{\ell=1}^{s-1}\mu_{i1}^2=1+(p-1)\delta_{is}-p\mu_{is}^2$

ii. $\displaystyle\sum_{\ell=1}^{s-1}\mu_{i\ell}\mu_{j\ell}=-p\mu_{is}\mu_{js}.$

13. *If* $B_0B_0^T=\mathrm{diag}(1,1,\ldots,1,p)$ *then*

$$G^{J_B}=\left\{B_0^{-1}\,\mathrm{diag}(N_s,N_t)B_0\,|N_s\in\mathrm{O}(s,k),N_t=(\nu_{ij})\right\}$$

where $\forall\ i,j\in\{s+1,s+2,\ldots,2n\}$*,* $i\neq j$*,* $\det(N_s)=\det(N_t)=\pm1$ *and the following are true:*

Table 6.3: The fixed-point group of conjugacy class twelve of involutions over $\mathrm{SO}(2n,k)$ where $k=\mathbb{Q}_p(\sqrt{p},\sqrt{-1})$, $-1\notin\mathbb{Q}_p^{*2}$, and $p\neq 2$. The order corresponds with Proposition 17.

Item	$B_0B_0^T$	α
β	γ	δ
12.i.	$\mathrm{diag}(1,\dots,p,1,\dots,p,p^{-1})$	1
$1+(p-1)\delta_{is}+\mu_{is}^2$	2	$1+(p-1)\delta_{\iota,2n-1}+(p^{-1}-1)\delta_{\iota,2n}$ $-p\nu_{\iota,2n-1}^2-p^{-1}\nu_{\iota,2n}^2$
12.ii.	$\mathrm{diag}(1,\dots,p,1,\dots,p,p^{-1})$	1
$-p\mu_{is}\mu_{js}$	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p+\nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}$

i. $\displaystyle\sum_{\ell=s+1}^{2n-1}\nu_{i1}^2=1+(p-1)\delta_{i,2n}-p\nu_{i,2n}^2$

ii. $\displaystyle\sum_{\ell=s+1}^{2n-1}\nu_{i\ell}\nu_{j\ell}=-p\nu_{i,2n}\nu_{j,2n}.$

14. *If* $B_0B_0^T=\mathrm{diag}(b_1,\dots,b_{2n})$ *where,* $b_s=-p$, *and all other* $b_i=1$ *then*

$$G^{J_B}=\left\{B_0^{-1}\,\mathrm{diag}(N_s,N_t)B_0\,|N_s=(\mu_{ij}),N_t\in\mathrm{O}(t,k)\right\}$$

where $\forall\ i,j\in\{1,2,\dots,s\}$, $i\neq j$, $\det(N_s)=\det(N_t)=\pm1$ *and the following are true:*

i. $\displaystyle\sum_{\ell=1}^{s-1}\mu_{i1}^2=1+(-p-1)\delta_{is}+p\mu_{is}^2$

ii. $\displaystyle\sum_{\ell=1}^{s-1}\mu_{i\ell}\mu_{j\ell}=p\mu_{is}\mu_{js}.$

15. *If* $B_0B_0^T=\mathrm{diag}(1,1,\dots,1,-p)$ *then*

$$G^{J_B}=\left\{B_0^{-1}\,\mathrm{diag}(N_s,N_t)B_0\,|N_s\in\mathrm{O}(s,k),N_t=(\nu_{ij}),\right\}$$

where $\forall\ i,j\in\{s+1,s+2,\dots,2n\}$, $i\neq j$, $\det(N_s)=\det(N_t)=\pm1$ *and the following are true:*

i. $\displaystyle\sum_{\ell=s+1}^{2n-1}\nu_{i1}^2=1+(-p-1)\delta_{i,2n}+p\nu_{i,2n}^2$

ii. $\displaystyle\sum_{\ell=s+1}^{2n-1} \nu_{i\ell}\nu_{j\ell} = p\nu_{i,2n}\nu_{j,2n}$.

Table 6.4: The fixed-point group of conjugacy class sixteen of involutions over $\mathrm{SO}(2n,k)$ where $k=\mathbb{Q}_p(\sqrt{p},\sqrt{-1})$, $-1\notin\mathbb{Q}_p^{*2}$, and $p\neq 2$. The order corresponds with Proposition 17.

Item	$B_0B_0^T$	α
β	γ	δ
16.i.	$\mathrm{diag}(1,\dots,-p,1,\dots,p,p^{-1})$	1
$1+(-p-1)\delta_{is}+\mu_{is}^2$	2	$1+(p-1)\delta_{\iota,2n-1}+(p^{-1}-1)\delta_{\iota,2n}$ $-p\nu_{\iota,2n-1}^2-p^{-1}\nu_{\iota,2n}^2$
16.ii.	$\mathrm{diag}(1,\dots,-p,1,\dots,p,p^{-1})$	1
$p\mu_{is}\mu_{js}$	2	$-\nu_{\iota,2n-1}\nu_{\lambda,2n-1}p-\nu_{\iota,2n}\nu_{\lambda,2n}p^{-1}$

Proof. The proof of this proposition is very similar to the proof of the previous one, and it has been omitted for the sake of brevity. Q.E.D.

Proposition 21. *Let $k=\mathbb{Q}_2(\sqrt{-1},\sqrt{2},\sqrt{3})$. Then the fixed point groups G^{J_A} of the involution conjugacy classes of $\mathrm{SO}(2n,k)$ corresponding to an involution J_A, $A=A_0^{-1}I_{s,t}A_0$, which are given by Proposition 18 are listed below, and none of them is compact. This time they are in tabular form, and the entries α, β, γ, and δ fill out the following summations, which correspond to $N_sN_s^T$ and $N_tN_t^T$: i.* $\displaystyle\sum_{\ell=1}^{s-\alpha}\mu_{i\ell}^2=\beta$, $\displaystyle\sum_{\ell=s+1}^{2n-\gamma}\nu_{i\ell}^2=\delta$ *and ii.* $\displaystyle\sum_{\ell=1}^{s-\alpha}\mu_{i\ell}\mu_{j\ell}=\beta$, $\displaystyle\sum_{\ell=s+1}^{2n-\gamma}\nu_{i\ell}\nu_{j\ell}=\delta$. *On the chart it is assumed that $i\neq j$, $\iota\neq\lambda$, $i,j\in\{1,2,\dots,t\}$ and $\iota,\lambda\in\{s+1,s+2,\dots,2n\}$. Also, $G^{J_A}=\left\{A_0^{-1}\,\mathrm{diag}(N_s,N_t)A_0\,|N_s=(\mu_{ij}),N_t=(\nu_{ij})\right\}$ unless otherwise specified. In this case, unlike the last case, if $N_s\in\mathrm{O}(s,k)$ or $N_t\in\mathrm{O}(t,k)$ then I have written ”n/a” for α or γ and $\in\mathrm{O}(s,k)$ or $\in\mathrm{O}(t,k)$ for β or δ, respectively. The order of the items is the same order as can be found in Proposition 18.*

Table 6.5: The fixed-point groups of isomorphy classes of involutions over $\mathrm{SO}(2n,k)$ *where* $k=\mathbb{Q}_2(\sqrt{-1},\sqrt{2},\sqrt{3})$*. This chart corresponds with Proposition 21. The order corresponds with Proposition 18.*

Item	$A_0A_0^T$	β
α	γ	δ
1.i.	$\mathrm{diag}(1,\dots,1,-1,1,\dots,-1)$	$1-2\delta_{is}+\mu_{is}^2$
1	1	$1-2\delta_{\iota,2n}+\nu_{\iota,2n}^2$
1.ii.	$\mathrm{diag}(1,\dots,1,-1,1,\dots,-1)$	$\mu_{is}\mu_{js}$
1	1	$\nu_{\iota,2n}\nu_{\lambda,2n}$
2.i.	$\mathrm{diag}(1,\dots,1,-1,-1)$	$\in \mathrm{O}(s,k)$
n/a	2	$1-2\delta_{\iota,2n-1}-2\delta_{\iota,2n}+\nu_{\iota,2n-1}^2+\nu_{\iota,2n}^2$
2.ii.	$\mathrm{diag}(1,\dots,1,-1,-1)$	$\in \mathrm{O}(s,k)$
n/a	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}+\nu_{\iota,2n}\nu_{\lambda,2n}$
3.i.	$\mathrm{diag}(1,\dots,1,-1,-1,1,\dots,1)$	$1-2\delta_{i,s-1}-2\delta_{i,s}+\mu_{i,s-1}^2+\mu_{i,s}^2$
2	*n/a*	$\in \mathrm{O}(t,k)$
3.ii.	$\mathrm{diag}(1,\dots,1,-1,-1,1,\dots,1)$	$\mu_{i,s-1}\mu_{j,s-1}+\mu_{is}\mu_{js}$
2	*n/a*	$\in \mathrm{O}(t,k)$
4.i.	I_{2n}	$\in \mathrm{O}(s,k)$
n/a	*n/a*	$\in \mathrm{O}(t,k)$
4.ii.	I_{2n}	$\in \mathrm{O}(s,k)$
n/a	*n/a*	$\in \mathrm{O}(t,k)$
5.i.	$\mathrm{diag}(1,\dots,1,-1,-1,$ $-1,1\dots,-1,-1)$	$1-2\delta_{i,s-2}-2\delta_{i,s-1}-2\delta_{is}$ $+\mu_{i,s-2}^2+\mu_{i,s-1}^2+\mu_{is}^2$
3	2	$1-2\delta_{\iota,2n-1}-2\delta_{\iota,2n}+\nu_{\iota,2n-1}^2+\nu_{\iota,2n}^2$
5.ii.	$\mathrm{diag}(1,\dots,1,-1,-1,$ $-1,1\dots,-1,-1)$	$\mu_{i,s-2}\mu_{j,s-2}+\mu_{i,s-1}\mu_{j,s-1}$ $+\mu_{is}\mu_{js}$

Table 6.5: Continued

Item	$A_0A_0^T$	β
α	γ	δ
3	2	$\nu_{\iota,2n-2}\nu_{\lambda,2n-2} + \nu_{\iota,2n-1}\nu_{\lambda,2n-1}$ $+\nu_{\iota,2n}\nu_{\lambda,2n}$
6.i.	$\text{diag}(1,\dots,-1,1,\dots,1)$	$1 - 2\delta_{is} + \mu_{is}^2$
1	*n/a*	$\in \text{O}(t,k)$
6.ii.	$\text{diag}(1,\dots,-1,1,\dots,1)$	$\mu_{is}\mu_{js}$
1	*n/a*	$\in \text{O}(t,k)$
7.i.	$\text{diag}(1,\dots,1,-1)$	$\in \text{O}(s,k)$
n/a	1	$1 - 2\delta_{\iota,2n} + \nu_{\iota,2n}^2$
7.ii.	$\text{diag}(1,\dots,1,-1)$	$\in \text{O}(s,k)$
n/a	1	$\nu_{\iota,2n}\nu_{\lambda,2n}$
8.i.	$\text{diag}(1,\dots,1,3,-3^{-1},1,\dots,1)$	$1 + 2\delta_{i,s-1} + (-3^{-1} - 1)\delta_{is}$ $-3\mu_{i,s-1}^2 + 3^{-1}\mu_{is}^2$
2	*n/a*	$\in \text{O}(t,k)$
8.ii.	$\text{diag}(1,\dots,1,3,-3^{-1},1,\dots,1)$	$-3\mu_{i,s-1}\mu_{j,s-1} + 3^{-1}\mu_{is}\mu_{js}$
2	*n/a*	$\in \text{O}(t,k)$
9.i.	$\text{diag}(1,\dots,-1,1,\dots,-1,3)$	$1 - 2\delta_{is} + \mu_{is}^2$
1	2	$1 - 2\delta_{\iota,2n-1} + 2\delta_{\iota,2n} + \nu_{\iota,2n-1}^2 - 3\nu_{\iota,2n}^2$
9.ii.	$\text{diag}(1,\dots,-1,1,\dots,-1,3)$	$\mu_{is}\mu_{js}$
1	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1} - 3\nu_{\iota,2n}\nu_{\lambda,2n}$
10.i.	$\text{diag}(1,\dots,-1,1,\dots,-3)$	$1 - 2\delta_{is} + \mu_{is}^2$
1	1	$1 - 4\delta_{\iota,2n} + 3\nu_{\iota,2n}^2$
10.ii.	$\text{diag}(1,\dots,-1,1,\dots,-3)$	$\mu_{is}\mu_{js}$
1	1	$3\nu_{\iota,2n}\nu_{\lambda,2n}$
11.i.	$\text{diag}(1,\dots,-3,1,\dots,-1)$	$1 - 4\delta_{is} + 3\mu_{is}^2$

Table 6.5: Continued

Item	$A_0A_0^T$	β
α	γ	δ
1	1	$1-2\delta_{\iota,2n}+\nu_{\iota,2n}^2$
11.ii.	$\mathrm{diag}(1,\ldots,-3,1,\ldots,-1)$	$3\mu_{is}\mu_{js}$
1	1	$\nu_{\iota,2n}\nu_{\lambda,2n}$
12.i.	$\mathrm{diag}(1,\ldots,1,2,3\cdot 2^{-1})$	$\in \mathrm{O}(s,k)$
n/a	2	$1+\delta_{\iota,2n-1}+(3\cdot 2^{-1}-1)\delta_{\iota,2n}$ $-2\nu_{\iota,2n-1}^2-3\cdot 2^{-1}\nu_{\iota,2n}^2$
12.ii.	$\mathrm{diag}(1,\ldots,1,2,3\cdot 2^{-1})$	$\in \mathrm{O}(s,k)$
n/a	2	$-2\nu_{\iota,2n-1}\nu_{\lambda,2n-1}-3\cdot 2^{-1}\nu_{\iota,2n}\nu_{\lambda,2n}$
13.i.	$\mathrm{diag}(1,\ldots,1,3,1,\ldots,-1)$	$1+2\delta_{is}-3\mu_{is}^2$
1	1	$1-2\delta_{\iota,2n}+\nu_{\iota,2n}^2$
13.ii.	$\mathrm{diag}(1,\ldots,1,3,1,\ldots,-1)$	$-3\mu_{is}\mu_{js}$
1	1	$\nu_{\iota,2n}\nu_{\lambda,2n}$
14.i.	$\mathrm{diag}(1,\ldots,1,-1,3,1,\ldots,1)$	$1-2\delta_{i,s-1}+2\delta_{i,s}+\mu_{i,s-1}^2-3\mu_{i,s}^2$
2	*n/a*	$\in \mathrm{O}(t,k)$
14.ii.	$\mathrm{diag}(1,\ldots,1,-1,3,1,\ldots,1)$	$\mu_{i,s-1}\mu_{j,s-1}-3\mu_{is}\mu_{js}$
2	*n/a*	$\in \mathrm{O}(t,k)$
15.i.	$\mathrm{diag}(1,\ldots,1,-1,3)$	$\in \mathrm{O}(s,k)$
n/a	2	$1-2\delta_{\iota,2n-1}+2\delta_{\iota,2n}+\nu_{\iota,2n-1}^2-3\nu_{\iota,2n}^2$
15.ii.	$\mathrm{diag}(1,\ldots,1,-1,3)$	$\in \mathrm{O}(s,k)$
n/a	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}-3\nu_{\iota,2n}\nu_{\lambda,2n}$
16.i.	$\mathrm{diag}(1,\ldots,1,-3)$	$\in \mathrm{O}(s,k)$
n/a	1	$1+2\delta_{\iota,2n}+3\nu_{\iota,2n}^2$
16.ii.	$\mathrm{diag}(1,\ldots,1,-3)$	$\in \mathrm{O}(s,k)$
n/a	1	$3\nu_{\iota,2n}\nu_{\lambda,2n}$

Table 6.5: Continued

Item	$A_0A_0^T$	β
α	γ	δ
17.i.	$\mathrm{diag}(1,\dots,1,-1,2,1,\dots,-1)$	$1-2\delta_{i,s-1}+\delta_{is}+\mu_{i,s-1}^2-2\mu_{is}^2$
2	1	$1-2\delta_{\iota,2n}+\nu_{\iota,2n}^2$
17.ii.	$\mathrm{diag}(1,\dots,1,-1,2,1,\dots,-1)$	$\mu_{i,s-1}\mu_{j,s-1}-2\mu_{is}\mu_{js}$
2	1	$\nu_{\iota,2n}\nu_{\lambda,2n}$
18.i.	$\mathrm{diag}(1,\dots,1,-1,-1,1,\dots,2)$	$1-2\delta_{i,s-1}-2\delta_{is}+\mu_{i,s-1}^2+\mu_{is}^2$
2	1	$1+\delta_{\iota,2n}-2\nu_{\iota,2n}^2$
18.ii.	$\mathrm{diag}(1,\dots,1,-1,-1,1,\dots,2)$	$\mu_{i,s-1}\mu_{j,s-1}+\mu_{is}\mu_{js}$
2	1	$-2\nu_{\iota,2n}\nu_{\lambda,2n}$
19.i.	$\mathrm{diag}(1,\dots,2,1,\dots,-1,-1)$	$1+\delta_{is}-2\mu_{is}^2$
1	2	$1-2\delta_{\iota,2n-1}-2\delta_{\iota,2n}+\nu_{\iota,2n-1}^2+\nu_{\iota,2n}^2$
19.ii.	$\mathrm{diag}(1,\dots,2,1,\dots,-1,-1)$	$-2\mu_{is}\mu_{js}$
1	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}+\nu_{\iota,2n}\nu_{\lambda,2n}$
20.i.	$\mathrm{diag}(1,\dots,1,2)$	$\in \mathrm{O}(s,k)$
n/a	1	$1+\delta_{\iota,2n}-2\nu_{\iota,2n}^2$
20.ii.	$\mathrm{diag}(1,\dots,1,2)$	$\in \mathrm{O}(s,k)$
n/a	1	$-2\nu_{\iota,2n}\nu_{\lambda,2n}$
21.i.	$\mathrm{diag}(1,\dots,-2,1,\dots,-1,-1)$	$1-3\delta_{is}+2\mu_{is}^2$
1	2	$1-2\delta_{\iota,2n-1}-2\delta_{\iota,2n}+\nu_{\iota,2n-1}^2+\nu_{\iota,2n}^2$
21.ii.	$\mathrm{diag}(1,\dots,-2,1,\dots,-1,-1)$	$2\mu_{is}\mu_{js}$
1	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}+\nu_{\iota,2n}\nu_{\lambda,2n}$
22.i.	$\mathrm{diag}(1,\dots,-1,1,\dots,2)$	$1-2\delta_{is}+\mu_{is}^2$
1	1	$1+\delta_{\iota,2n}-2\nu_{\iota,2n}^2$
22.ii.	$\mathrm{diag}(1,\dots,-1,1,\dots,2)$	$\mu_{is}\mu_{js}$

Table 6.5: Continued

Item	$A_0A_0^T$	β
α	γ	δ
1	1	$-2\nu_{\iota,2n}\nu_{\lambda,2n}$
23.i.	$\mathrm{diag}(1,\ldots,1,2,1,\ldots,-1)$	$1+\delta_{is}-2\mu_{is}^2$
1	1	$1-2\delta_{\iota,2n}+\nu_{\iota,2n}^2$
23.ii.	$\mathrm{diag}(1,\ldots,1,2,1,\ldots,-1)$	$-2\mu_{is}\mu_{js}$
1	1	$\nu_{\iota,2n}\nu_{\lambda,2n}$
24.i.	$\mathrm{diag}(1,\ldots,1,-1,2)$	$\in \mathrm{O}(s,k)$
n/a	2	$1-2\delta_{\iota,2n-1}+\delta_{\iota,2n}+\nu_{\iota,2n-1}^2-2\nu_{\iota,2n}^2$
24.ii.	$\mathrm{diag}(1,\ldots,1,-1,2)$	$\in \mathrm{O}(s,k)$
n/a	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}-2\nu_{\iota,2n}\nu_{\lambda,2n}$
25.i.	$\mathrm{diag}(1,\ldots,1,6,1,\ldots,-1,-1)$	$1+5\delta_{is}-6\mu_{is}^2$
1	2	$1-2\delta_{\iota,2n-1}-2\delta_{\iota,2n}+\nu_{\iota,2n-1}^2+\nu_{\iota,2n}^2$
25.ii.	$\mathrm{diag}(1,\ldots,1,6,1,\ldots,-1,-1)$	$-6\mu_{is}\mu_{js}$
1	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1}+\nu_{\iota,2n}\nu_{\lambda,2n}$
26.i.	$\mathrm{diag}(1,\ldots,-1,1,\ldots,-6)$	$1-2\delta_{is}+\mu_{is}^2$
1	1	$1-7\delta_{\iota,2n}+6\nu_{\iota,2n}^2$
26.ii.	$\mathrm{diag}(1,\ldots,-1,1,\ldots,-6)$	$\mu_{is}\mu_{js}$
1	1	$6\nu_{\iota,2n}\nu_{\lambda,2n}$
27.i.	$\mathrm{diag}(1,\ldots,1,-6,1,\ldots,-1)$	$1-7\delta_{is}+6\mu_{is}^2$
1	1	$1-2\delta_{\iota,2n}+\nu_{\iota,2n}^2$
27.ii.	$\mathrm{diag}(1,\ldots,1,-6,1,\ldots,-1)$	$6\mu_{is}\mu_{js}$
1	1	$\nu_{\iota,2n}\nu_{\lambda,2n}$
28.i.	$\mathrm{diag}(1,\ldots,1,6,1)$	$\in \mathrm{O}(s,k)$
n/a	2	$1+5\delta_{\iota,2n-1}-6\nu_{\iota,2n-1}^2-\nu_{\iota,2n}^2$

Table 6.5: Continued

Item	$A_0A_0^T$	β
α	γ	δ
28.ii.	$\mathrm{diag}(1,\ldots,1,6,1)$	$\in \mathrm{O}(s,k)$
n/a	2	$-6\nu_{\iota,2n-1}\nu_{\lambda,2n-1} - \nu_{\iota,2n}\nu_{\lambda,2n}$
29.i.	$\mathrm{diag}(1,\ldots,-1,1,\ldots,6)$	$1 - 2\delta_{is} + \mu_{is}^2$
1	1	$1 + 5\delta_{\iota,2n} - 6\nu_{\iota,2n}^2$
29.ii.	$\mathrm{diag}(1,\ldots,-1,1,\ldots,6)$	$\mu_{is}\mu_{js}$
1	1	$-6\nu_{\iota,2n}\nu_{\lambda,2n}$
30.i.	$\mathrm{diag}(1,\ldots,1,-1,6,1,\ldots,1)$	$1 - 2\delta_{i,s-1} + 5\delta_{i,s} + \mu_{i,s-1}^2 - 6\mu_{is}^2$
2	*n/a*	$\in \mathrm{O}(t,k)$
30.ii.	$\mathrm{diag}(1,\ldots,1,-1,6,1,\ldots,1)$	$\mu_{i,s-1}\mu_{j,s-1} - 6\mu_{is}\mu_{js}$
2	*n/a*	$\in \mathrm{O}(t,k)$
31.i.	$\mathrm{diag}(1,\ldots,1,-1,6)$	$\in \mathrm{O}(s,k)$
n/a	2	$1 - 2\delta_{\iota,2n-1} + 5\delta_{\iota,2n} + \nu_{\iota,2n-1}^2 - 6\nu_{\iota,2n}^2$
31.ii.	$\mathrm{diag}(1,\ldots,1,-1,6)$	$\in \mathrm{O}(s,k)$
n/a	2	$\nu_{\iota,2n-1}\nu_{\lambda,2n-1} - 6\nu_{\iota,2n}\nu_{\lambda,2n}$
32.i.	$\mathrm{diag}(1,\ldots,1,-6)$	$\in \mathrm{O}(s,k)$
n/a	1	$1 - 7\delta_{\iota,2n} + 6\nu_{\iota,2n}^2$
32.ii.	$\mathrm{diag}(1,\ldots,1,-6)$	$\in \mathrm{O}(s,k)$
n/a	1	$6\nu_{\iota,2n}\nu_{\lambda,2n}$

Chapter 7

Diagram Automorphisms of D_ℓ and Two Maximal Tori of $\mathrm{SO}(2n,k)$ that Can Be Used to Compute Quadratic Elements, and Information About the Quadratic Elements

7.1 Introductory Results

7.1.1 Preliminaries and Recollections

In this chapter, it is assumed that a torus T of the group $G \equiv \mathrm{SO}(2n,k)$ is a maximal (σ,k)-split torus of G, where σ is an involution of G and $K = \mathbb{R}$. In other words, it is assumed that, firstly, T is a torus such that there is a $g \in G$ where gTg^{-1} is a group consisting of diagonal matrices. Secondly, it is assumed that $T = T^{-1} \equiv \{t \in T | \sigma(t) = t^{-1}\}$.

Notation: define J_n as $J_n \equiv \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$ and define $K_{p,q} \equiv \begin{pmatrix} -I_p & 0 & 0 & 0 \\ 0 & I_q & 0 & 0 \\ 0 & 0 & -I_p & 0 \\ 0 & 0 & 0 & I_q \end{pmatrix}$ as in Helgason [4, p. 444]. Note that $J_n^{-1} = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} = -J_n$ and $K_{p,q}^{-1} = K_{p,q}$.

Define an involution $\theta : G \to G$, $\theta : x \mapsto (x^T)^{-1}$. The following lemma is taken from Helgason [4, pp. 451-455].

Lemma 15. *For any $X \in \mathrm{GL}(2n, k)$, $k = \mathbb{R}$, the involution conjugacy classes of $\mathrm{GL}(2n, k)$ are as follows:*

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

2. $\sigma(X) = J_n(X^T)^{-1}J_n^{-1}$

3. $\sigma(X) = I_{p,q}XI_{p,q}$

4. $\sigma(X) = J_nXJ_n^{-1}$

5. $\sigma(X) = K_{p,q}XK_{p,q}$

7.1.2 The Maximal (σ, k)-Split Tori Stemming from Lemma 15

It is now necessary to investigate the maximal (σ, k)-split tori generated on $\mathrm{SO}(2n, k)$ by these conjugacy classes of involutions, and that is done in the following proposition. Recall that there is a one-to-one correspondence between the conjugacy classes (i.e., the isomorphism classes) of $\mathrm{SO}(2n, k)$ and $\mathrm{GL}(2n, k)$ according to Proposition 2.

Proposition 22. *The maximal (σ, k)-split tori T generated on $\mathrm{SO}(2n, k)$ by the conjugacy classes of involutions in the above lemma are as follows:*

1. *If $\sigma(X) = (X^T)^{-1}$, $T = \{X \in \mathrm{SO}(2n, k) | X^2 = I_{2n}\}$*

2. *If* $\sigma(X) = J_n(X^T)^{-1}J_n^{-1}$*,* $T = \left\{ X \in \mathrm{SO}(2n,k) \middle| X = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \right\}$ *where* $D = A^T, C = -C^T, B = -B^T$

3. *If* $\sigma(X) = I_{p,q}XI_{p,q}$*,* $T = \left\{ X \in \mathrm{SO}(2n,k) \middle| X = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \right\}$ *where* $A = A^T, B = -C^T, D = D^T$

4. *If* $\sigma(X) = J_nXJ_n^{-1}$*,* $T = \left\{ X \in \mathrm{SO}(2n,k) \middle| X = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \right\}$ *where* $D = A^T, C = -C^T, B = -B^T$

5. *If* $\sigma(X) = K_{p,q}XK_{p,q}$*,* $T = \left\{ X \in \mathrm{SO}(2n,k) \middle| X = \begin{pmatrix} A & B & C & D \\ E & F & G & H \\ I & J & K & L \\ M & N & O & P \end{pmatrix} \right\}$ *where* $A = A^T, B = -E^T, C = I^T, D = -M^T, F = F^T, G = -J^T, H = N^T, K = K^T, L = -O^T, P = P^T$

Proof. These items will be proven in order.

1. Define an involution σ on $\mathrm{SO}(2n,k)$ such that $\sigma : X \mapsto (X^T)^{-1}$. Then we need all $X \in \mathrm{SO}(2n,k)$ such that $\sigma(X) = X^{-1}$. On $\mathrm{SO}(2n,k)$, $X^{-1} = X^T$ so $\sigma(X) = (X^T)^{-1} = (X^T)^T = X$ so we need $X = X^T$. Then the maximal torus is $T = \{X \in \mathrm{SO}(2n,k) | X = X^T\}$.

2. Now define $\sigma : X \mapsto J_n(X^T)^{-1}J_n^{-1}$. Set $J_n(X^T)^{-1}J_n^{-1} = X^{-1} = X^T$. Then $J_nXJ_n^{-1} = X^T$. Let $X = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, where A, B, C, and D are all $n \times n$ blocks. Then $J_nXJ_n^{-1} = -J_nXJ_n = \begin{pmatrix} D & -C \\ -B & A \end{pmatrix} = \begin{pmatrix} A^T & C^T \\ B^T & D^T \end{pmatrix}$.
$\therefore D = A^T$, $C = -C^T$, and $B = -B^T$.

3. Set $\sigma : X \mapsto I_{p,q}XI_{p,q}$, where p and q are arbitrary. Let $X = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ as before, except that now A is a $p \times p$ block, B is a $p \times q$ block, C is a $q \times p$ block, and D is a $q \times q$ block. $I_{p,q}XI_{p,q} = \begin{pmatrix} A & -B \\ -C & D \end{pmatrix}$ and we set this equal to $X^T = \begin{pmatrix} A^T & C^T \\ B^T & D^T \end{pmatrix}$. That means that $A = A^T$, $D = D^T$, and $C = -B^T$.

4. If we set $\sigma : X \mapsto J_nXJ_n^{-1}$, we get the same result as in item 2.

5. Lastly, set $\sigma : X \mapsto K_{p,q}XK_{p,q}$, where $K_{p,q} = \text{diag}(-I_p, I_q, -I_p, I_q)$. Let $X = \begin{pmatrix} A & B & C & D \\ E & F & G & H \\ I & J & K & L \\ M & N & O & P \end{pmatrix}$. Then by computation, $K_{p,q}XK_{p,q} = \begin{pmatrix} A & -B & C & -D \\ -E & F & -G & H \\ I & -J & K & -L \\ -M & N & -O & P \end{pmatrix}$. If we set this equal to $X^T = \begin{pmatrix} A^T & E^T & I^T & M^T \\ B^T & F^T & J^T & N^T \\ C^T & G^T & K^T & O^T \\ D^T & H^T & L^T & P^T \end{pmatrix}$, then it is clear that $A = A^T, B = -E^T, C = I^T, D = -M^T, F = F^T, G = -J^T, H = N^T, K = K^T, L = -O^T$, and $P = P^T$.

The maximality of these tori follows from the fact that all possible matrices meeting the necessary criteria are contained within each one. Q.E.D.

7.2 Diagram Automorphisms

Now consider the following root system D_4, where the black dots here and afterwards signify fixed points in the diagram automorphism.

Lemma 16. *In the root system D_4 shown above, the longest element of the Weyl group with respect to the basis, which I will call $w_0(\theta)$, acts on α_1 as follows: $w_0(\theta)(\alpha_1) = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$.*

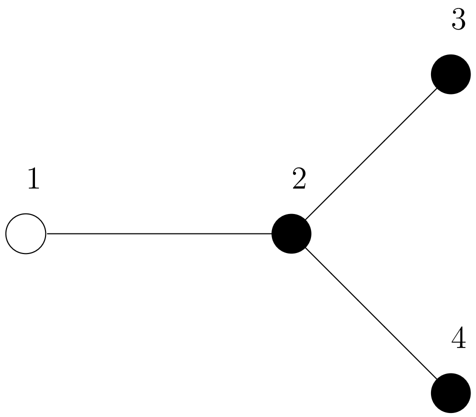

Figure 7.1: The Root System D_4

Proof. Let S_{α_i} be the reflection of α_i to $-\alpha_i$ $\forall$ $i \in \{1,2,3.4\}$. Then $w_0(\theta)(\alpha_1) = S_{\alpha_2}S_{\alpha_4}S_{\alpha_2}S_{\alpha_3}S_{\alpha_2}S_{\alpha_4}(\alpha_1)$. As a result,

$$\begin{aligned}
w_0(\theta)(\alpha_1) &= S_{\alpha_4}S_{\alpha_3}S_{\alpha_2}S_{\alpha_3}(\alpha_1) \\
&= S_{\alpha_2}S_{\alpha_4}S_{\alpha_2}S_{\alpha_3}S_{\alpha_2}(\alpha_1) \\
&= S_{\alpha_2}S_{\alpha_4}S_{\alpha_2}S_{\alpha_3}(\alpha_1+\alpha_2) \\
&= S_{\alpha_2}S_{\alpha_4}S_{\alpha_2}(\alpha_1+\alpha_2+\alpha_3) \\
&= S_{\alpha_2}S_{\alpha_4}(\alpha_1+\alpha_2-\alpha_2+\alpha_3-\alpha_2) \\
&= S_{\alpha_2}S_{\alpha_4}(\alpha_1+\alpha_2+\alpha_3) \\
&= S_{\alpha_2}(\alpha_1+\alpha_2+\alpha_3+\alpha_4) \\
&= (\alpha_1+\alpha_2)-\alpha_2+(\alpha_3+\alpha_2)+\alpha_4 \\
&= \alpha_1+\alpha_2+\alpha_3+\alpha_4
\end{aligned}$$

Note that S_{α_4} acts non-trivially on α_2 instead of α_3.

Q.E.D.

Here is a much more general but related result to the above lemma.

Proposition 23. *This proposition will prove the following results.*

1. *In the root system D_ℓ (or DI_b) shown below,*

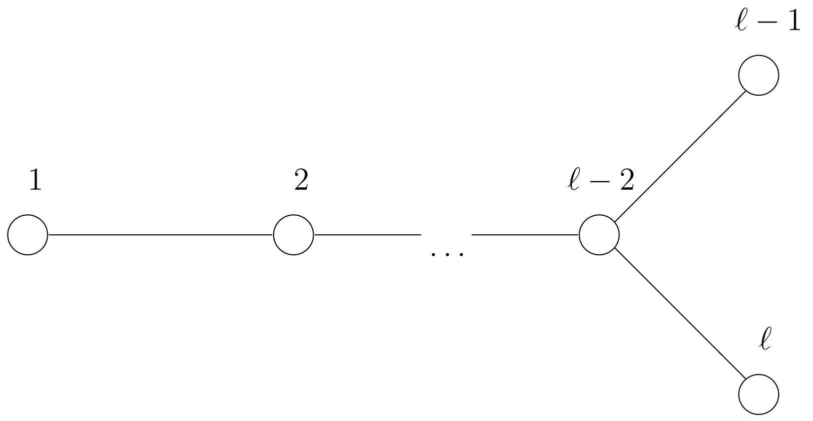

Figure 7.2: The Root System $D\mathrm{I}_b$ (or D_ℓ)

$w_0(\theta) = \mathrm{id}$ *since there are no black dots. That means the diagram automorphism* $\theta = -\,\mathrm{id}$.

2. *In the root system $DIII_a$ shown below,*

$w_0(\theta) = S_{\alpha_1} \circ S_{\alpha_3} \circ \ldots \circ S_{\alpha_{\ell-3}} \circ S_{\alpha_\ell}$. *That means the diagram automorphism* $\theta = -\left(\prod_{i=0}^{\lceil\frac{\ell-4}{2}\rceil} S_{\alpha_{2i+1}}\right) \circ S_{\alpha_\ell}$, *where the multiplication is understood as the composition of functions, which is the group action on the automorphism group, and $\lceil\ \rceil$ denotes the "ceiling" function which sends any real number ξ to the next integer greater than or equal to ξ.*

3. *In the root system $DIII_b$ shown below,*

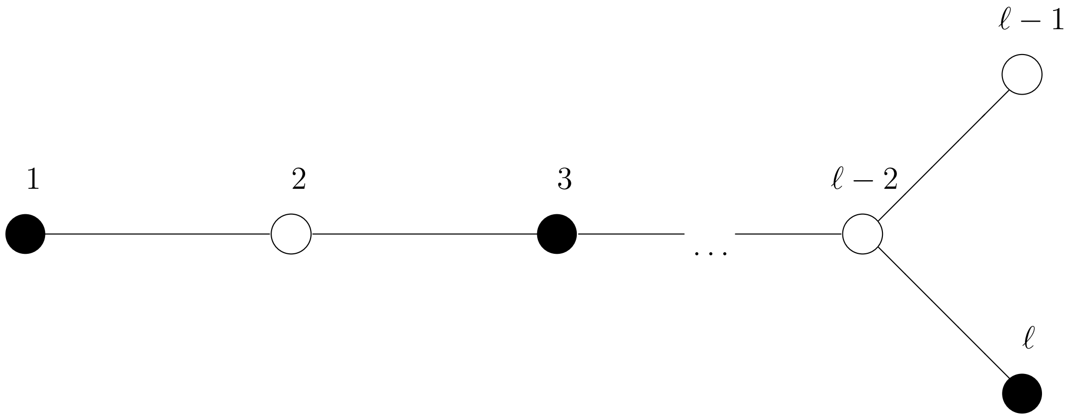

Figure 7.3: The Root System $D\mathrm{III}_a$

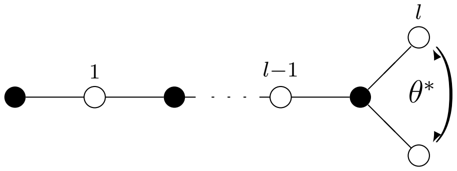

Figure 7.4: The Root System $D\mathrm{III}_b$

$w_0(\theta) = \left(\prod_{i=0}^{\lceil \frac{\ell-3}{2} \rceil} S_{\alpha_{2i+1}}\right)$ *so that the diagram automorphism* $\theta = -\theta^* \cdot \left(\prod_{i=0}^{\lceil \frac{\ell-3}{2} \rceil} S_{\alpha_{2i+1}}\right)$.

4. *In the root system* DI_a *shown below,*

$w_0(\theta) = -\operatorname{id}$ *on the black dots and* $w_0(\theta) = \operatorname{id}$ *on all of the white dots except for* s. *On* s, $w_0(\theta) = \begin{cases} -\operatorname{id}, & \ell \text{ even} \\ -\varepsilon, & \ell \text{ odd} \end{cases}$, *where "$\varepsilon$ is the automorphism which permutes* $\alpha_{\ell-1}$ *and* α_ℓ *and leaves the others fixed" [1, p. 257]. So the diagram automorphism* $\theta = -w_0(\theta)$.

Proof. $\boxed{1.}$ There are no fixed points, denoted by black dots, for $w_0(\theta)$ to act on and $\theta^* = \operatorname{id}$ here, since it is not present. Therefore, the diagram automorphism $\theta = -\operatorname{id} \circ \theta^* \circ w_0(\theta) =$

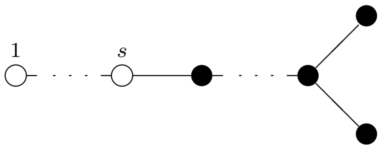

Figure 7.5: The Root System DI_a

$-\operatorname{id}$.

$\boxed{2.}$ None of the fixed points are adjacent, so $w_0(\theta) = S_{\alpha_1} \circ S_{\alpha_3} \circ \ldots \circ S_{\alpha_{\ell-3}} \circ S_{\alpha_\ell}$. Therefore, the diagram automorphism $\theta = -\left(\prod_{i=0}^{\lceil\frac{\ell-4}{2}\rceil} S_{\alpha_{2i+1}}\right) \circ S_{\alpha_\ell}$.

$\boxed{3.}$ For the same reason as in case 2, $w_0(\theta) = S_{\alpha_1} \circ S_{\alpha_3} \circ \ldots \circ S_{\alpha_{\ell-2}}$ so $\theta = -\theta^* \cdot \left(\prod_{i=0}^{\lceil\frac{\ell-3}{2}\rceil} S_{\alpha_{2i+1}}\right)$, since θ^* is not trivial in this case.

$\boxed{4.}$ On every fixed point (denoted by black dots), $w_0(\theta) = -\operatorname{id}$ and on the white dots except for s, $w_0(\theta) = \operatorname{id}$. On α_s, $w_0(\theta) = \begin{cases} -\operatorname{id}, & \ell \textit{ even} \\ -\varepsilon, & \ell \textit{ odd} \end{cases}$ [1, p. 257]. So the diagram automorphism $\theta = -\operatorname{id} \circ \theta^* \circ w_0(\theta) = -w_0(\theta)$. Q.E.D.

7.3 Maximal Tori in the Case $p \equiv 1 \pmod 4$, in the Other Cases k-Anisotropic Tori

7.3.1 Preliminary Results and Definitions

Definition 10. *A torus T is "k-split" if the minimum polynomial of its elements factors completely over k. (That would imply that these minimum polynomials have the same number of roots in k as their degree.) On the other hand, a torus T is "k-anisotropic" if the minimum polynomial of each of its elements has no roots in k at all.*

This next lemma will simplify the proof of Proposition 24.

Lemma 17. $T = \left\{ \left(\begin{array}{cc} a & b \\ -b & a \end{array} \right) \middle| a^2 + b^2 = 1 \ \forall \ i = 1, 2, \ldots, n \right\}$ *is a maximal k-split torus of* $\mathrm{SO}(2,k)$ *iff* $-1 \in k^{*2}$. *If* $-1 \notin k^{*2}$ *then* T *is a k-anisotropic torus of* $\mathrm{SO}(2,k)$.

Proof. Let $A \equiv \left(\begin{array}{cc} a & b \\ -b & a \end{array} \right)$, $C \equiv \left(\begin{array}{cc} c & d \\ -d & c \end{array} \right)$ be elements of T. Then

$$AC = \left(\begin{array}{cc} ac - bd & ad + bc \\ -bc - ad & ac - bd \end{array} \right) = CA$$

and $\det(CA) = (ac - bd)^2 + (ad + bc)^2 = a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 = c^2(a^2 + b^2) + d^2(a^2 + b^2) = c^2 + d^2 = 1$ so $AC = CA \in T$. That means that T is a torus.

Further, $\det(A) = 1$ so T has the same dimention as $\mathrm{SO}(2,k)$, and $A^T = \left(\begin{array}{cc} a & -b \\ b & a \end{array} \right)$, so that $AA^T = \left(\begin{array}{cc} a^2 + b^2 & -ab + ab \\ -ab + ab & a^2 + b^2 \end{array} \right) = I_2$ so $A \in \mathrm{SO}(2,k)$.

The minimum polynomial of A is $\left| \begin{array}{cc} a - \lambda & b \\ -b & a - \lambda \end{array} \right| = \lambda^2 - 2a\lambda + (a^2 + b^2)$. Therefore, the eigenvalues are

$$\frac{2a \pm \sqrt{4a^2 - 4a^2 - 4b^2}}{2} = a \pm b\sqrt{-1}$$

That means that T is a k-split torus of $\mathrm{SO}(2,k)$ (where $n = 1$) iff $-1 \in k^{*2}$. It is clear that if $-1 \notin k^{*2}$ then T is a k-anisotropic torus of $\mathrm{SO}(2,k)$. Q.E.D.

7.3.2 The First Torus

Proposition 24. *The set*

$$T = \left\{ \left(\begin{array}{ccccc} a_1 & b_1 & \ldots & 0 & 0 \\ -b_1 & a_1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & a_n & b_n \\ 0 & 0 & \ldots & -b_n & a_n \end{array} \right) \middle| a_i^2 + b_i^2 = 1 \ \forall \ i = 1, 2, \ldots, n \right\}$$

is a maximal k-split torus of $\mathrm{SO}(2n,k)$ *iff* $-1 \in k^{*2}$. *If* $-1 \notin k^{*2}$ *then* T *is a k-anisotropic torus of* $\mathrm{SO}(2n,k)$.

Proof. This proof will be inductive. The case where $n = 1$ has been taken care of by Lemma 17 above so assume the result is true $\forall\ n \leq \ell$. Now let $n = \ell + 1$. Let $A = \begin{pmatrix} a_1 & b_1 & \dots & 0 & 0 \\ -b_1 & a_1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_n & b_n \\ 0 & 0 & \dots & -b_n & a_n \end{pmatrix} \in T$ and let $C = \begin{pmatrix} c_1 & d_1 & \dots & 0 & 0 \\ -d_1 & c_1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & c_n & d_n \\ 0 & 0 & \dots & -d_n & c_n \end{pmatrix} \in T$. Then

$$AC = CA = \begin{pmatrix} a_1c_1 - b_1d_1 & a_1d_1 + b_1c_1 & \dots & 0 & 0 \\ -b_1c_1 - a_1d_1 & a_1c_1 - b_1d_1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_nc_n - b_nd_n & a_nd_n + b_nc_n \\ 0 & 0 & \dots & -b_nc_n - a_nd_n & a_nc_n - b_nd_n \end{pmatrix}$$

and $\det(CA) = 1$ because the determinant of the $(n-2) \times (n-2)$ block in the upper left is 1 by the inductive hypothesis and the determinant of the 2×2 block in the bottom left is 1 because it is identical to the matrices considered in Lemma 17. As in Lemma 17, this shows that $AC = CA \in T$. That means that T is a torus.

Similarly, $\det(A) = 1$ so T has the same dimention as $\mathrm{SO}(2n,k)$, and

$$AA^T = \begin{pmatrix} a_1^2 + b_1^2 & -a_1b_1 + a_1b_1 & \dots & 0 & 0 \\ -a_1b_1 + a_1b_1 & a_1^2 + b_1^2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_n^2 + b_n^2 & -a_nb_n + a_nb_n \\ 0 & 0 & \dots & -a_nb_n + a_nb_n & a_n^2 + b_n^2 \end{pmatrix} = I_n$$

so $A \in \mathrm{SO}(2n,k)$.

The minimum polynomial of A is equal to $\begin{vmatrix} a_1-\lambda & b_1 & \dots & 0 & 0 \\ -b_1 & a_1-\lambda & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_n-\lambda & b_n \\ 0 & 0 & \dots & -b_n & a_n-\lambda \end{vmatrix}$. By the properties of determinants,

$$|A-\lambda I_n| = \begin{vmatrix} a_1-\lambda & b_1 & \dots & 0 & 0 \\ -b_1 & a_1-\lambda & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{vmatrix} \begin{vmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_n-\lambda & b_n \\ 0 & 0 & \dots & -b_n & a_n-\lambda \end{vmatrix}$$

Define $\xi(\lambda) = \begin{vmatrix} a_1-\lambda & b_1 & \dots & 0 & 0 \\ -b_1 & a_1-\lambda & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_{n-1}-\lambda & b_{n-1} \\ 0 & 0 & \dots & -b_{n-1} & a_{n-1}-\lambda \end{vmatrix}$, which factors over k iff $-1 \in k^{*2}$ by the inductive hypothesis. $\begin{vmatrix} a_1-\lambda & b_1 & \dots & 0 & 0 \\ -b_1 & a_1-\lambda & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{vmatrix} = \begin{vmatrix} a_1-\lambda & b_1 & \dots & 0 \\ -b_1 & a_1-\lambda & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{vmatrix} =$

$$\begin{vmatrix} a_1-\lambda & b_1 & \dots & 0 & 0 \\ -b_1 & a_1-\lambda & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_{n-1}-\lambda & b_{n-1} \\ 0 & 0 & \dots & -b_{n-1} & a_{n-1}-\lambda \end{vmatrix} = \xi(\lambda).\text{ Therefore,}$$

$$|A-\lambda I_n| = \xi(\lambda)\begin{vmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_n-\lambda & b_n \\ 0 & 0 & \dots & -b_n & a_n-\lambda \end{vmatrix} = \xi(\lambda)[\lambda_n^2 - 2a_n\lambda + (a_n^2+b_n^2)]$$

The roots of this polynomial are equal to the roots of $\xi(\lambda)$ and $a_n \pm b_n\sqrt{-1}$ which are in k iff $-1 \in k^{*2}$. This proves the result. Q.E.D.

7.3.3 More Useful Results

Lemma 18. *All matrices of the form* $\begin{pmatrix} a_1 & \dots & 0 & 0 & \dots & b_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & a_t & b_t & \dots & 0 \\ 0 & \dots & -b_t & a_t & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_1 & \dots & 0 & 0 & \dots & a_1 \end{pmatrix}$ *have eigenvalues of the form* $a_i \pm b_i\sqrt{-1}$ *for all* $i \in \{1,2,\dots,t\}$.

Proof. This proof will be inductive. In the $t=1$ case, the determinant of $\begin{vmatrix} a_1-\lambda & b_1 \\ -b_1 & a_1-\lambda \end{vmatrix} = \lambda^2 - 2a_1\lambda + a_1^2 + b_1^2$ which has roots $a_1 \pm b_1\sqrt{-1}$ as claimed.

Now assume the result is true for $t = 1, 2, \dots, n-1$. In that case, we are assuming that $\begin{vmatrix} a_1-\lambda & \dots & 0 & 0 & \dots & b_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & a_{n-1}-\lambda & b_{n-1} & \dots & 0 \\ 0 & \dots & -b_{n-1} & a_{n-1}-\lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_1 & \dots & 0 & 0 & \dots & a_1-\lambda \end{vmatrix}$ has the roots $a_i \pm b_i\sqrt{-1}$ for all $i = 1, 2, \ldots, n-1$. Now consider the case where $t = n$.

$$\begin{vmatrix} a_1-\lambda & \dots & 0 & 0 & \dots & b_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & a_t-\lambda & b_t & \dots & 0 \\ 0 & \dots & -b_t & a_t-\lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_1 & \dots & 0 & 0 & \dots & a_1-\lambda \end{vmatrix}$$

$$= (a_1-\lambda)\begin{vmatrix} a_2-\lambda & \dots & 0 & 0 & \dots & b_2 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & a_t-\lambda & b_t & \dots & 0 & 0 \\ 0 & \dots & -b_t & a_t-\lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_2 & \dots & 0 & 0 & \dots & a_2-\lambda & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & a_1-\lambda \end{vmatrix}$$

$$-b_1\begin{vmatrix} 0 & a_2-\lambda & \dots & 0 & 0 & \dots & b_2 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & a_t-\lambda & b_t & \dots & 0 \\ 0 & 0 & \dots & -b_t & a_t-\lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -b_2 & \dots & 0 & 0 & \dots & a_1-\lambda \\ -b_1 & 0 & 0 & 0 & 0 & 0 & 0 \end{vmatrix}$$

$$= [\lambda^2 - 2a_1\lambda + a_1^2 + b_1^2] \begin{vmatrix} a_2 - \lambda & \dots & 0 & 0 & \dots & b_2 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & a_t - \lambda & b_t & \dots & 0 \\ 0 & \dots & -b_t & a_t - \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_2 & \dots & 0 & 0 & \dots & a_2 - \lambda \end{vmatrix}$$

Now, inductively, we assumed the polynomial resulting from the last matrix above has only roots in the desired form, since it is $(n-1) \times (n-1)$, and the roots of the polynomial on the left are again $a_1 \pm b_1\sqrt{-1}$. This proves the result. Q.E.D.

Lemma 19. *Any matrix in* $\mathrm{SO}(2n, k)$ *can be row-reduced to* I_{2n} *by using row operations corresponding to matrices in* $\mathrm{SO}(2n, k)$*. Further, one can also row-reduce a matrix in* $\mathrm{SO}(2n, k)$ *that has a block in* $\mathrm{SO}(2m, k)$ *on the main diagonal,* $m < n$*, that is otherwise diagonal and whose diagonal entries outside of the block have the product of one.*

Proof. The proof will be inductive. Let $A \in \mathrm{SO}(2, k)$. Then by Lemma 14, $A = \begin{bmatrix} \pm\sqrt{1-a^2} & a \\ -a & \pm\sqrt{1-a^2} \end{bmatrix}$ for some $a \in k$. It follows that $A^{-1} = \begin{bmatrix} \pm\sqrt{1-a^2} & -a \\ a & \pm\sqrt{1-a^2} \end{bmatrix}$ $= A^T$. Then if one takes the first row of A, multiplies it by $\pm\sqrt{1-a^2}$ and adds $-a$ times the second row to the first row, the first row will be the same as the first row of I_2. Similarly, one can multiply the second row by $\pm\sqrt{1-a^2}$ and add a times the first row to it to render the second row identical to the second row of I_2. This corresponds to multiplying A by A^{-1}, and these operations are both a combination of elementary row operations.

Now assume the result is true on $\mathrm{SO}(2n, k)$ for $n \in \{1, 2, \dots, m-1\}$, using the same method. Let $n = m$ and let $A \in \mathrm{SO}(2n, k)$. If $B \in \mathrm{SO}(2n-2, k)$, the result is true on B. That means that a combination of elementary row operations takes one from B to I_{2n-2}. Specifically, $B^{-1} = B^T$ so, by multiplying the first row of B by b_{11}, e.g., and adding the second row of B multiplied by b_{21} to it, adding the third row of B multiplied by b_{31} to it, and etc. down to adding the last row of B multiplied by $b_{2n-2,1}$ to the first row will make the first row the same as the first row of I_{2n-2}. By the inductive hypothesis, a similar process will work for the other rows.

Thus, one can do the same thing to row-reduce A to I_{2n}, considering the fact that $A^{-1} = A^T$ since $A \in \mathrm{SO}(2n, k)$.

If one considers the matrix $C = \begin{bmatrix} \alpha_1 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & \ddots & 0 & 0 & 0 & \dots & 0 \\ 0 & \dots & \alpha_i & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & D & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \alpha_{i+1} & \dots & 0 \\ 0 & \ddots & 0 & 0 & 0 & \ddots & 0 \\ 0 & \dots & 0 & 0 & 0 & \dots & \alpha_{2n-2m} \end{bmatrix}$, $D \in \mathrm{SO}(2m, k)$, all $\alpha_j \in \; k$, and $m < n$, one can use a similar simultaneous row-reduction to obtain the identity. This row reduction will correspond to the matrix

$$\begin{bmatrix} \alpha_1 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & \ddots & 0 & 0 & 0 & \dots & 0 \\ 0 & \dots & \alpha_i & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & D^{-1} & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \alpha_{i+1} & \dots & 0 \\ 0 & \ddots & 0 & 0 & 0 & \ddots & 0 \\ 0 & \dots & 0 & 0 & 0 & \dots & \alpha_{2n-2m} \end{bmatrix}$$

where $D \in \mathrm{SO}(2m, k)$ and all $\alpha_j \in \; k$. Q.E.D.

7.3.4 The Second Torus

Proposition 25. *For $\sigma = J_{I_{s,t}}$ where $t \in \{1, 2, \ldots, n\}$ and $s + t = 2n$, assuming $-1 \in k^{*2}$, the maximal (σ, k)-split torus of $\mathrm{SO}(2n, k)$ can be chosen as*

$$T = \left\{ \left(\begin{array}{ccccccc} a_1 & \ldots & 0 & \ldots & 0 & \ldots & b_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & a_t & \ldots & b_t & \ldots & 0 \\ \vdots & \vdots & \vdots & I_{2n-2t} & \vdots & \vdots & \vdots \\ 0 & \ldots & -b_t & \ldots & a_t & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_1 & \ldots & 0 & \ldots & 0 & \ldots & a_1 \end{array} \right) \middle| \, a_i^2 + b_i^2 = 1 \ \forall \ i = 1, 2, \ldots, t \right\}$$

The dimension of the above torus is t.

Proof. Let $A = \left(\begin{array}{ccccccc} a_1 & \ldots & 0 & \ldots & 0 & \ldots & b_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & a_t & \ldots & b_t & \ldots & 0 \\ \vdots & \vdots & \vdots & I_{2n-2t} & \vdots & \vdots & \vdots \\ 0 & \ldots & -b_t & \ldots & a_t & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_1 & \ldots & 0 & \ldots & 0 & \ldots & a_1 \end{array} \right) \in T$, let

$C = \left(\begin{array}{ccccccc} c_1 & \ldots & 0 & \ldots & 0 & \ldots & d_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & c_t & \ldots & d_t & \ldots & 0 \\ \vdots & \vdots & \vdots & I_{2n-2t} & \vdots & \vdots & \vdots \\ 0 & \ldots & -d_t & \ldots & c_t & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -d_1 & \ldots & 0 & \ldots & 0 & \ldots & c_1 \end{array} \right) \in T$. Then

$$AC = \begin{pmatrix} a_1c_1 - b_1d_1 & \dots & 0 & \dots & 0 & \dots & a_1d_1 + b_1c_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & a_tc_t - b_td_t & \dots & a_td_t + b_tc_t & \dots & 0 \\ \vdots & \vdots & \vdots & I_{2n-2t} & \vdots & \vdots & \vdots \\ 0 & \dots & -a_td_t - b_tc_t & \dots & a_tc_t - b_td_t & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_1d_1 - b_1c_1 & \dots & 0 & \dots & 0 & \dots & a_1c_1 - b_1d_1 \end{pmatrix} = CA \text{ so}$$

T is commutative.

Let $B = J_{I_{s,t}}(A) = \begin{pmatrix} a_1 & \dots & 0 & \dots & 0 & \dots & -b_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & a_t & \dots & -b_t & \dots & 0 \\ \vdots & \vdots & \vdots & I_{2n-2t} & \vdots & \vdots & \vdots \\ 0 & \dots & b_t & \dots & a_t & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_1 & \dots & 0 & \dots & 0 & \dots & a_1 \end{pmatrix}$. Then $AB = I_{2n}$ so B is the inverse of A. That means that T is σ-split.

The minimum polynomial of A is

$$\begin{vmatrix} a_1 - \lambda & \dots & 0 & \dots & 0 & \dots & b_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & a_t - \lambda & \dots & b_t & \dots & 0 \\ \vdots & \vdots & \vdots & I_{2n-2t}(1-\lambda) & \vdots & \vdots & \vdots \\ 0 & \dots & -b_t & \dots & a_t - \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_1 & \dots & 0 & \dots & 0 & \dots & a_1 - \lambda \end{vmatrix}$$

$$= (1-\lambda)^{2n-2t} \begin{vmatrix} a_1-\lambda & \dots & 0 & 0 & \dots & b_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & a_t-\lambda & b_t & \dots & 0 \\ 0 & \dots & -b_t & a_t-\lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_1 & \dots & 0 & 0 & \dots & a_1-\lambda \end{vmatrix}$$

By Lemma 18, the roots of the above are 1 and $a_i \pm b_i\sqrt{-1}$ for all $i = 1, 2, \dots, t$. That means that T is indeed k-split.

All that is left to show is maximality of the torus T. Given the above eigenvalues, the corresponding eigenvectors of A are as follows: the vector $x_i = (0, 0, \dots, 0, 1, 0, \dots, 0)^T$, where only the i^{th} row is nonzero, corresponds to the eigenvalue 1 $\forall\ i \in \{t+1, t+2, \dots, 2n-2t\}$. $A - (a_i + b_i\sqrt{-1})I_{2n} =$

$$\begin{pmatrix} a_1-a_i-b_i\sqrt{-1} & \dots & 0 & \dots & 0 & \dots & 0 & \dots & b_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & -b_i\sqrt{-1} & 0 & \dots & 0 & -b_i & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & a_t-a_i-b_i\sqrt{-1} & \dots & b_t & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & I_{2n-2t} & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & -b_t & \dots & a_t-a_i-b_i\sqrt{-1} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \dots & b_i & 0 & \dots & 0 & -b_i\sqrt{-1} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_1 & \dots & 0 & \dots & 0 & 0 & 0 & \dots & a_1-a_i-b_i\sqrt{-1} \end{pmatrix}$$

The eigenvector y_i such that $(A-(a_i+b_i\sqrt{-1})I_{2n})y_i = 0$ is $y_i = (0, \dots, 0, \sqrt{-1}, 0, \dots, 0, 1, 0, \dots, 0)^T$ where $\sqrt{-1}$ is in the i^{th} spot, 1 is in the $(2n-i)^{th}$ spot, and the other entries are zero. Note that in the case $b_i = 0$ this is still an eigenvector of A.

For similar reasons, the eigenvector z_i corresponding to the eigenvalue $a_i - b_i\sqrt{-1}$ is $y_i = (0, \dots, 0, -\sqrt{-1}, 0, \dots, 1, 0, \dots, 0)^T$ where $-\sqrt{-1}$ is in the i^{th} spot, 1 is in the $(2n-i)^{th}$ spot, and the other entries are zero. Thus, the matrix of eigenvectors B (the one which I chose to use) looks like this:

$$B = \begin{pmatrix} \sqrt{-1} & -\sqrt{-1} & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \sqrt{-1} & -\sqrt{-1} & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & \sqrt{-1} & -\sqrt{-1} & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

In that case, $B^{-1}AB = \mathrm{diag}(a_1+b_1\sqrt{-1}, a_1-b_1\sqrt{-1}, \dots, a_i+b_i\sqrt{-1}, a_i-b_i\sqrt{-1}, \dots, a_t+b_t\sqrt{-1}, a_t-b_t\sqrt{-1}, 1, \dots, 1)$. In $\mathrm{SO}(2n,k)$, only diagonal matrices commute with $B^{-1}AB$, *except* that the bottom-right corner can be any special orthogonal $(2n-2t)\times(2n-2t)$ matrix. However, since the entries to the left of that block in the matrix will all be 0, by Lemma 19 that block can be row-reduced over $\mathrm{SO}(2n,k)$ to I_{2n-2t}. (Observe that the product of all of the eigenvalues is one.) That means that the diagonal matrix is *maximal.* That implies that any matrix conjugate to it is maximal as well.

Let C be such a matrix, i.e., a matrix commutative with $B^{-1}AB$. Then C has the block form $C = \begin{pmatrix} c_1 & \dots & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & \dots & c_t & 0 \\ 0 & \dots & 0 & D \end{pmatrix}$ where D is a special orthogonal matrix of size $(2n-2t)\times$

$(2n-2t)$. Then $BCB^{-1} =$

$$\begin{pmatrix} \frac{1}{2}c_1+\frac{1}{2}c_2 & \dots & 0 & 0 & 0 & \dots & \frac{\sqrt{-1}}{2}c_1-\frac{\sqrt{-1}}{2}c_2 \\ 0 & \ddots & 0 & 0 & 0 & \vdots & 0 \\ 0 & \dots & \frac{1}{2}c_{t-1}+\frac{1}{2}c_t & 0 & \frac{\sqrt{-1}}{2}c_{t-1}-\frac{\sqrt{-1}}{2}c_t & \dots & 0 \\ 0 & \dots & 0 & D & 0 & \dots & 0 \\ 0 & \dots & \frac{\sqrt{-1}}{2}c_{t-1}-\frac{\sqrt{-1}}{2}c_t & 0 & \frac{1}{2}c_{t-1}+\frac{1}{2}c_t & \dots & 0 \\ 0 & \vdots & 0 & 0 & 0 & \ddots & 0 \\ \frac{\sqrt{-1}}{2}c_1-\frac{\sqrt{-1}}{2}c_2 & \dots & 0 & 0 & 0 & \dots & \frac{1}{2}c_1+\frac{1}{2}c_2 \end{pmatrix}$$

which is of the desired form. Q.E.D.

7.4 Results Related to Quadratic Elements

7.4.1 A Preliminary Result and a Definition

Proposition 26. *The matrices* $A = \begin{pmatrix} -a & b \\ b & a \end{pmatrix}$ *and* $B = \begin{pmatrix} -c & d \\ d & c \end{pmatrix}$*, where* $a^2+b^2 = c^2+d^2 = 1$ *and* $a \neq 1$*,* $c \neq 1$*, are conjugate over* $\mathrm{SO}(2,k)$ *. Further,* $a+1 = e^2(c+1)$ *for some* $e \in k$*.*

Proof. Assume $a^2+b^2 = 1$ and $c^2+d^2 = 1$. Let $A = X^{-1}I_{1,1}X$ and $B = Y^{-1}I_{1,1}Y$ where $X = \begin{pmatrix} b & a+1 \\ a+1 & -b \end{pmatrix}$, $Y = \begin{pmatrix} d & c+1 \\ c+1 & -d \end{pmatrix}$, and A and B are conjugate over $\mathrm{SO}(2,k)$. Note that A and B both have a determinant of minus one, which means that they are not in $\mathrm{SO}(2,k)$. Let $D = |X^{-1}|^{-1/2}|Y|^{-1/2}X^{-1}Y$. Then $D \in \mathrm{SO}(2,k) \subset \mathrm{O}(2,k)$ because its determinant is one and $D^{-1}AD = Y^{-1}XX^{-1}I_{1,1}XX^{-1}Y = Y^{-1}I_{1,1}Y = B$.

So A is conjugate to B over $\mathrm{SO}(2,k)$, since there is the matrix $D \in \mathrm{SO}(2,k)$ such that $D^{-1}AD = B$. That means $D^{-1}X^{-1}I_{1,1}XD = Y^{-1}I_{1,1}Y \Rightarrow I_{1,1}XD = XDY^{-1}I_{1,1}Y \Rightarrow I_{1,1}XDY^{-1} = XDY^{-1}I_{1,1}$. Thus, XDY^{-1} is diagonal.

Let $XDY^{-1} = \mathrm{diag}(e,f)$, so that $XD = \mathrm{diag}(e,f)Y$. Since $D \in \mathrm{O}(2,k)$, $D^T = D^{-1}$ so $XX^T = XDD^TX^T = \mathrm{diag}(e,f)Y \cdot (Y\,\mathrm{diag}(e,f))^T = \mathrm{diag}(e,f)Y \cdot Y^T\,\mathrm{diag}(e,f)$ so $\mathrm{diag}(b^2+(a+1)^2, b^2+(a+1)^2) = \mathrm{diag}(e^2[d^2+(c+1)^2], f^2[(c+1)^2+d^2])$.

Since $b^2 + (a+1)^2 = b^2 + a^2 + 2a + 1 = 2(a+1)$, $e^2[d^2 + (c+1)^2] = 2e^2(c+1)$, and $f^2[(c+1)^2+d^2]) = 2f^2(c+1)$, one obtains $\operatorname{diag}(2(a+1), 2(a+1)) = \operatorname{diag}(2e^2(c+1), 2f^2(c+1))$. Thus, $a + 1 = e^2(c+1) = f^2(c+1)$ which proves the result. Q.E.D.

Definition 11. *The set of "quadratic elements" of a maximal (σ, k)-split torus T are the $a \in T$ such that $\sigma \operatorname{Inn}(a)$ is an involution of the group G. Quadratic elements are also called "k-inner elements."*

7.4.2 The Big Result on Quadratic Elements

Proposition 27. *All the quadratic elements (or k-inner elements) for $\mathrm{SO}(2n, k)$ are conjugate to J_A over $\mathrm{SO}(2n, k)$ with* $A = \begin{pmatrix} -a_1 & b_1 & \dots & 0 & 0 & 0 \\ b_1 & a_1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & -a_t & b_t & 0 \\ 0 & 0 & \dots & b_t & a_t & 0 \\ 0 & 0 & \dots & 0 & 0 & I_{2n-2t} \end{pmatrix}$, *and where $\forall\ i \in \{1, 2, \dots, t\}$, $a_i^2 + b_i^2 = 1$ and $a_i \neq -1$.*

Proof. By Proposition 24 a maximal (σ, k)-split torus (to which the others are conjugate) is

$$T = \left\{ \begin{pmatrix} a_1 & \dots & 0 & \dots & 0 & \dots & b_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & a_t & \dots & b_t & \dots & 0 \\ \vdots & \vdots & \vdots & I_{2n-2t} & \vdots & \vdots & \vdots \\ 0 & \dots & -b_t & \dots & a_t & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_1 & \dots & 0 & \dots & 0 & \dots & a_1 \end{pmatrix} \middle| \, a_i^2 + b_i^2 = 1 \forall\ i = 1, 2, \dots, t \right\}$$

Therefore, if $E \in T$, the quadratic elements are of the form $J_{I_{s,t}} J_E = J_{I_{s,t}E}$. Let $B \equiv I_{s,t}E =$

$$\begin{pmatrix} a_1 & \dots & 0 & \dots & 0 & \dots & b_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & a_t & \dots & b_t & \dots & 0 \\ \vdots & \vdots & \vdots & I_{2n-2t} & \vdots & \vdots & \vdots \\ 0 & \dots & b_t & \dots & -a_t & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_1 & \dots & 0 & \dots & 0 & \dots & -a_1 \end{pmatrix}$$. Assume that $\forall\ i \in \{1, 2, \dots, t\}$, $a_i \neq -1$.

B has eigenvalues of 1 and -1 with multiplicities of $2n - t$ and t, respectively. The corresponding matrix of eigenvectors is S below:

$$S \equiv \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \frac{-b_1}{a_1+1} & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \frac{-b_2}{a_2+1} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & 0 & \dots & 0 & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & \frac{-b_t}{a_t+1} \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \ddots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & \frac{b_t}{a_t+1} & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 \\ \vdots & \vdots & \dots & \vdots & 0 & 0 & \dots & 0 & \vdots & \vdots & \dots & \vdots \\ 0 & \frac{b_2}{a_2+1} & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ \frac{b_1}{a_1+1} & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \end{pmatrix}$$

Thus, $S^{-1}BS = I_{s,t}$.

Let $A = \begin{pmatrix} -a_1 & b_1 & \dots & 0 & 0 & 0 \\ b_1 & a_1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & -a_t & b_t & 0 \\ 0 & 0 & \dots & b_t & a_t & 0 \\ 0 & 0 & \dots & 0 & 0 & I_{2n-2t} \end{pmatrix}$. Then A can be diagonalized as well. It also has eigenvalues of 1 and -1 with the same multiplicities as B ($2n - t$ and t, respectively).

The matrix of eigenvectors of A is R below:

$$R \equiv \begin{pmatrix} \frac{b_1}{a_1+1} & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & \frac{-b_1}{a_1+1} & 0 & \ldots & 0 \\ 0 & \frac{b_2}{a_2+1} & \ldots & 0 & 0 & 0 & \ldots & 0 & 0 & 1 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & 0 & 0 & \ldots & 0 & 0 & \frac{-b_2}{a_2+1} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & 0 & \ldots & 0 & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \frac{b_t}{a_t+1} & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & \ldots & 1 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & \frac{-b_t}{a_t+1} \\ 0 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & 1 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & 0 & \ddots & 0 & 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 1 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Thus, $R^{-1}AR = I_{s,t}$.

As a result, $S^{-1}BS = R^{-1}AR = I_{s,t}$ so $RS^{-1}BSR^{-1} = A \Rightarrow \left(SR^{-1}\right)^{-1} B \left(SR^{-1}\right) = A$. $\left(SR^{-1}\right)^{-1} = \left(SR^{-1}\right)^{T}$ and $\det(SR^{-1}) = 1$ iff t is even, that is, iff $I_{s,t} \in \mathrm{SO}(2n, k)$, so the result has been proven by Theorem 2. Q.E.D.

7.4.3 How to Use the Big Result on Quadratic Elements

Proposition 28. *The matrices* $A = \begin{pmatrix} -a_1 & b_1 & \dots & 0 & 0 & 0 \\ b_1 & a_1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & -a_t & b_t & 0 \\ 0 & 0 & \dots & b_t & a_t & 0 \\ 0 & 0 & \dots & 0 & 0 & I_{2n-2t} \end{pmatrix}$ *and*

$B = \begin{pmatrix} -c_1 & d_1 & \dots & 0 & 0 & 0 \\ d_1 & c_1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & -c_t & d_t & 0 \\ 0 & 0 & \dots & d_t & c_t & 0 \\ 0 & 0 & \dots & 0 & 0 & I_{2n-2t} \end{pmatrix}$*, where it is assumed that all* $a_i^2 + b_i^2 = c_i^2 + d_i^2 = 1$ *and all* $a_i \neq -1$ *and all* $c_i \neq -1$*, are conjugate over* $\mathrm{SO}(2n, k)$ *iff* $\mathrm{diag}(a_1+1, a_2+1, \dots, a_t+1)$ *is congruent to* $\mathrm{diag}(c_1+1, c_2+1, \dots, c_t+1)$*.*

Proof. A is the same as it was in the previous proposition, so it still has eigenvalues ± 1 and matrix of eigenvectors

$$R \equiv \begin{pmatrix} \frac{b_1}{a_1+1} & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \frac{-b_1}{a_1+1} & 0 & \dots & 0 \\ 0 & \frac{b_2}{a_2+1} & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \frac{-b_2}{a_2+1} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & 0 & \dots & 0 & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \frac{b_t}{a_t+1} & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & \frac{-b_t}{a_t+1} \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \ddots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Similarly, B has the same eigenvalues with the same multiplicities and a matrix of eigenvectors

$$S \equiv \begin{pmatrix} \frac{d_1}{c_1+1} & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \frac{-d_1}{c_1+1} & 0 & \dots & 0 \\ 0 & \frac{d_2}{c_2+1} & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \frac{-d_2}{c_2+1} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & 0 & \dots & 0 & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \frac{d_t}{c_t+1} & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & \frac{-d_t}{c_t+1} \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \ddots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Thus, $R^{-1}AR = S^{-1}BS = I_{s,t}$. Consequently, $A = RI_{s,t}R^{-1}$ and $B = SI_{s,t}S^{-1}$.

Assume A and B are conjugate over $\mathrm{SO}(2n,k)$. My claim is that $\mathrm{diag}(a_1+1, a_2+1, \dots, a_t+1)$ is congruent to $\mathrm{diag}(c_1+1, c_2+1, \dots, c_t+1)$. Given my assumption, $\exists\ C \in \mathrm{SO}(2n,k) \ni CAC^{-1} = B$. Then $CRI_{s,t}R^{-1}C^{-1} = SI_{s,t}S^{-1}$ which implies that $S^{-1}CRI_{s,t} = I_{s,t}S^{-1}CR$ so $S^{-1}CR = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$, where A_1 is $t \times t$ and A_2 is $(2n-t) \times (2n-t)$.

Thus, $CR = S \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$ so $RR^T = R^TC^TCR = \begin{pmatrix} A_1^T & 0 \\ 0 & A_2^T \end{pmatrix} S^TS \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$. Hence $\mathrm{diag}(a_1+1, a_2+1, \dots, a_t+1, 1, 1, \dots, 1, a_1+1, a_2+1, \dots, a_t+1)^{-1} = \begin{pmatrix} A_1^T & 0 \\ 0 & A_2^T \end{pmatrix}$ $\mathrm{diag}(c_1+1, c_2+1, \dots, c_t+1, 1, 1, \dots, 1, c_1+1, c_2+1, \dots, c_t+1)^{-1} \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$ which implies the desired result, since it means $\mathrm{diag}(a_1+1, a_2+1, \dots, a_t+1, 1, 1, \dots, 1, a_1+1, a_2+1, \dots, a_t+1) = \begin{pmatrix} A_1^{-1} & 0 \\ 0 & A_2^{-1} \end{pmatrix} \mathrm{diag}(c_1+1, c_2+1, \dots, c_t+1, 1, 1, \dots, 1, c_1+1, c_2+1, \dots, c_t+1)$

$\begin{pmatrix} (A_1^{-1})^T & 0 \\ 0 & (A_2^{-1})^T \end{pmatrix}$. That means that the $t \times t$ upper-left blocks of the diagonal matrices are also congruent to each other.

Now assume that $\mathrm{diag}(a_1{+}1, a_2{+}1, \ldots, a_t{+}1)$ is congruent to $\mathrm{diag}(c_1{+}1, c_2{+}1, \ldots, c_t{+}1)$ over $\mathrm{SO}(2n, k)$. Then $\mathrm{diag}(a_1 + 1, a_2 + 1, \ldots, a_t + 1, 1, 1, \ldots, 1, a_1 + 1, a_2 + 1, \ldots, a_t + 1)$ is congruent to $\mathrm{diag}(c_1{+}1, c_2{+}1, \ldots, c_t{+}1, 1, 1, \ldots, 1, c_1{+}1, c_2{+}1, \ldots, c_t{+}1)$ via a block diagonal matrix $L \equiv \begin{pmatrix} L_1 & 0 \\ 0 & L_2 \end{pmatrix}$, where $L \in \mathrm{SO}(2n, k)$, L_1 is $t{\times}t$, and L_2 is $(2n{-}t){\times}(2n{-}t)$. In other words, $L^T R^T R L = S^T S$. Let $M \equiv RLS^{-1}$. Then $M^{-1}AM = SL^{-1}R^{-1}RI_{s,t}R^{-1}RLS^{-1} = SL^{-1}I_{s,t}LS^{-1} = SI_{s,t}S^{-1} = B$. Q.E.D.

Bibliography

[1] N. Bourbaki. *Groups et Algèbres de Lie.* Hermann, Paris, France, 1968.

[2] Christopher Dometrius. *Relationship Between Symmetric and Skew-Symmetric Bilinear Forms on $V = K^N$ and Involutions of* and $\mathrm{SO}(N, K, \beta)$. PhD thesis, NCSU, Raleigh, NC, 2003.

[3] Larry J. Gerstein. *Basic Quadratic Forms.* The American Mathematical Society, Providence, RI, 2008.

[4] Sigurdur Helgason. *Differential Geometry, Lie Groups, and Symmetric Spaces.* Academic Press, Inc., New York, NY, 1978.

[5] A.G. Helminck and S.P. Wang. On rationality properties of involutions of reductive groups. *Advances in Mathematics*, 99:26–96, 1993.

[6] Burton W. Jones. *The Arithmetic Theory of Quadratic Forms.* The Waverly Press, Baltimore, MD, 1950.

[7] Kurt Mahler. *P-Adic Numbers and Their Functions.* Press Syndicate of the University of Cambridge, New York, NY, 1981.

[8] Kenneth H. Rosen. *Elementary Number Theory and Its Applications.* AT&T Laboratories, New York, NY, 2000.

[9] Winfried Scharlau. *Quadratic and Hermitian Forms.* Springer-Verlag, Berlin, Germany, 1985.

[10] Jean-Pierre Serre. *A Course in Arithmetic*. Springer-Verlag New York Inc., New York, NY, 1973.

[11] Ling Wu. *Classification of Involutions of SL(n,k) and SO(2n+1,k)*. PhD thesis, NCSU, Raleigh, NC, 2002.

APPENDIX

Appendix A

Extraneous Results

This proposition is true, but I didn't need it for anything.

Proposition 29. *A sequence in $\mathbb{Q}_p$ that is bounded both above and below has a limit superior and a limit inferior.*

Proof. Let $\Phi = \{\phi_1, \phi_2, \ldots\}$ be a bounded sequence in $\mathbb{Q}_p$ that is bounded above and below. Then there are real numbers δ and ε such that, $\forall\ i \in \mathbb{N}$, $\delta \leq |\phi_i|_p \leq \varepsilon$. Now, the p-norm gives discrete values for the norms of points in $\mathbb{Q}_p$, so there can only be a finite number of p-norm values that come from the terms ϕ_i of the sequence Φ. By the pigeonhole principle, that means at least one of the values p^k of the norm, where $k \in \mathbb{Z}$ and $\delta \leq p^k \leq \varepsilon$, must be repeated an infinite number of times.

If there is only one norm value p^k such that for an infinite number of ϕ_i, $|\phi_i|_p = p^k$, then any $\alpha \in \mathbb{Q}_p$ such that $|\alpha|_p = p^k$ will be both the limit superior and the limit inferior of the terms of Φ. (That means that the limit of the norm of the terms of Φ exists, and $\underset{t\to\infty}{lim} |\phi_t|_p = p^k$.)

Otherwise, let p^{k_1} and p^{k_2} be two distinct p-norm values of the terms of Φ such that for an infinite number of $i, j \in \mathbb{N}$, $|\phi_i|_p = p^{k_1}$ and $|\phi_j|_p = p^{k_2}$. Assume without loss of generality that $p^{k_1} < p^{k_2}$, that p^{k_2} is the biggest such infinitely repeated p-norm value, and that p^{k_1} is the smallest such infinitely repeated p-norm value. Then $\underset{t\to\infty}{\overline{lim}}\ \phi_t = p^{k_2}$ and $\underset{t\to\infty}{\underline{lim}}\ \phi_t = p^{k_1}$. The reason is that there can only be a finite number of ϕ_i with a bigger norm value than

p^{k_2} and there can only be a finite number of ϕ_i with a smaller norm value than p^{k_1}, by my assumptions at the top of this paragraph. Q.E.D.

I think the lemma below is redundant with Classification Lemma 2.

Lemma 20. *Let* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}(2,k)$*, let* $k = \mathbb{Q}_p$ *and let* N_p *be a nonsquare of* k*. Then it cannot be true that* $AA^T = \mathrm{diag}(1, N_p)$*.*

Proof. Assume otherwise, i.e., assume $AA^T = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{bmatrix} = \mathrm{diag}(1, N_p)$. Then $a^2 + b^2 = 1 \Rightarrow b = \pm\sqrt{1-a^2}$ and $c^2 + d^2 = N_p$, which is always possible if $-1 \in \mathbb{Q}_p^{*2}$ but might not be otherwise. However, in the other case, N_p could be picked so that it is the sum of two squares. Suppose for the sake of argument that that has been done. Then $d = \pm\sqrt{N_p - c^2}$, so

$$ac + bd = 0$$

$$ac \pm \sqrt{1-a^2}\sqrt{N_p - c^2} = 0$$

$$ac = \mp\sqrt{1-a^2}\sqrt{N_p - c^2}$$

Since N_p is not a square, $c \neq 0$. Assume $a \neq \pm 1$. Then $\frac{a}{\sqrt{1-a^2}} = \mp\frac{\sqrt{N_p-c^2}}{c}$ so $\frac{a^2}{1-a^2} = \frac{N_p-c^2}{c^2}$ so $-1 + \frac{1}{1-a^2} = \frac{N_p-c^2}{c^2} \Rightarrow \frac{1}{1-a^2} = \frac{N_p}{c^2} \Rightarrow c^2 = N_p(1-a^2)$. But $c^2 + d^2 = N_p$ so $N_p - N_p a^2 + d^2 = N_p \Rightarrow d^2 = N_p a^2$ or $(d/a)^2 = N_p$, which is a paradox because N_p is not a square.

Now assume $a = \pm 1$. Then $b = 0$ and $ac = \mp\sqrt{1-a^2}\sqrt{N_p - c^2} = 0$ implies $c = 0$ so $d^2 = N_p$, but again, that is a paradox. Q.E.D.

These two guys might be useful in computing examples of fixed-point groups over $\mathbb{Q}_p$.

Lemma 21. *If* v *is a square over* $\mathbb{Z}$*, then* $v \not\equiv 2 \pmod{4}$*.*

Proof. If any number is congruent to two modulo four, then it is even but not divisible by four. Therefore, its prime factorization contains an odd power of two, so it cannot be a perfect square over $\mathbb{Z}$. Q.E.D.

Lemma 22. *In $\mathbb{Q}_3$, -1 and -3 are not the sums of two squares.*

Proof. Generally speaking, $-1 = \sum_{i=0}^{\infty}(p-1)p^i$ and $-p = \sum_{i=1}^{\infty}(p-1)p^i$. Assume the desired result is not true for -1. Therefore, by Corollary 2, if $\beta^2 + \gamma^2 = -1$, then $\beta = \sum_{i=0}^{\infty} b_i 2^i$ and $\gamma = \sum_{i=0}^{\infty} c_i 2^i$.

Then $\beta^2 + \gamma^2 = b_0^2 + c_0^2 + (2b_0b_1 + 2c_0c_1)p + (2b_0b_2 + b_1^2 + 2c_0c_2 + c_1^2)p^2 + (2b_0b_3 + 2b_1b_2 + 2c_0c_3 + 2c_1c_2)p^3 + \ldots$ By Corollary 1, p is not the sum of two squares, and if $p-1$ were a square then that would not be the case. So $p-1$ is not a square, not only in this case, but in $\mathbb{Q}_p$ ($p \equiv 3 \pmod 4$).

Therefore if $b_0^2 + c_0^2 = p - 1$, $b_0 \neq 0$ and $c_0 \neq 0$. That can sometimes happen, and it happens if $p = 3$, e.g., let $b_0 = c_0 = 1$. So consider $p = 3$. In the second term, one can set $b_1 = 1$ and $c_1 = 0$ so consider the third term. $2b_0b_2 + b_1^2 + 2c_0c_2 + c_1^2 = 2b_2 + 2c_2 + 1 = 2$, which has no solution over $\mathbb{Z}$. If instead one sets $2b_2 + 2c_2 + 1 = 2 + 2^\ell$, $\ell \in \mathbb{N}$, there is still no solution because the righthand-side is even and the lefthand-side is odd. That is a paradox. However, if $b_0 = 2$ and $c_0 = 1$, then $b_0^2 + c_0^2 = 5 = 2 + 3$, so the 3 can be added to the next term. But that also causes a paradox, because then $1 + 2b_0b_1 + 2c_0c_1 = 2 + 2^\ell$ and again one side of the equation is odd and the other is even. No other combination of $b_0 = 1, 2$ and $c_0 = 1, 2$ can get the first term to be 2, so that proves the result. The case $\beta^2 + \gamma^2 = -3$ is similar. Q.E.D.

The last result below is redundant with (in fact, is superseded by) Fixed-Point Computation Lemma 7, which comes from Scharlau.

Fixed-Point Group Computation Lemma 9. *For sufficiently large $m \in \mathbb{N}$, $x_1^2 + \ldots + x_m^2 = p$, $x_1^2 + \ldots + x_m^2 = -1$, and $x_1^2 + \ldots + x_m^2 = -p$ have solutions in $\mathbb{Q}_p$, where $p \equiv 3 \pmod 4$. One can always select $m = p$ to obtain a solution for each equation.*

Proof. There's not much to the first one. If $m = p$ let $x_i = \pm 1\ \forall\ i \in \{1, 2, 3, \ldots, m-1, m\}$.

In $\mathbb{Q}_p$, $-1 = \sum_{i=0}^{\infty}(p-1)p^i$. Let $x_j = \sum_{i=0}^{\infty}\xi_{ij}p^i$. Then $x_j^2 = \left(\sum_{i=0}^{\infty}\xi_{ij}p^i\right)^2 = \xi_{0j}^2 + 2\xi_{0j}\xi_{1j}p + (2\xi_{0j}\xi_{2j} + \xi_{1j}^2)p^2 + (2\xi_{0j}\xi_{3j} + 2\xi_{1j}\xi_{2j})p^3 + \ldots$ A sum of p of these terms can get what is desired.

Specifically, let $m = p$. Then $\forall\ j \in \{1, 2, 3, \ldots, m-1, m\}$, set $\xi_{0j} = \pm 1$ if $j < m$ and set $\xi_{0m} = 0$ to get the first term. Then one is free to set each term ξ_{0j} equal to one or minus one later. For the second term, set $\xi_{1j} = \xi_{0j}$ for all $j \leq \frac{p-1}{2}$ and set $\xi_{1m} = 1$. For the third term, there are a number of ξ_{1j}^2 terms whose sum is equal to $\frac{p+1}{2}$. Then set $\xi_{2j} = \xi_{0j}$ if $j \leq \frac{p-3}{4}$ and set $\xi_{2j} = 0$ if $j < m$ otherwise to get the third term. (Observe that if $p = 3$, $\frac{p-3}{4} = 0$.) Note that no selection has been made for ξ_{2m}.

One continues in this vein to get -1. In the fourth term, based on the selections already made, we have $\left(\sum_{i=1}^{m-1} 2\xi_{0i}\xi_{3i}\right) + \dfrac{p-3}{4} + \xi_{2m}$. (Recall $\xi_{0m} = 0$, so the top index of the sum is $m-1$, not m.) So if $p \neq 3$, one must solve $\left(\sum_{i=1}^{m-1} 2\xi_{0i}\xi_{3i}\right) + \xi_{2m} = \dfrac{p-5}{2}$. This leaves one with many options, such as setting $\xi_{3i} = 0\ \forall\ i \in \{1, 2, \ldots, m-1\}$ and setting $\xi_{2m} = \frac{p-5}{2}$, which is necessary if $p = 7$. Or, one could have $\xi_{31} = \xi_{01}$ and the other $\xi_{3i} = 0$, so $\xi_{2m} = \frac{p-7}{2}$. There are many more such options too, depending on what p is.

To get the fourth term if $p = 3$, one must solve $\left(\sum_{i=1}^{m-1} 2\xi_{0i}\xi_{3i}\right) + \xi_{2m} = 2$, and that is just as easy. The following terms are similar (indeed, note that no selection has been made for ξ_{3m}), and since there are an infinite number of them they have been left to the reader. This process works, and inductively it goes on ad infinitum.

Lastly, in $\mathbb{Q}_p$, $-p = \sum_{i=1}^{\infty}(p-1)p^i$. One can obtain a sum of p squares to equal this series in the exact same way as was done in the previous equation. Just start with terms $x_j = \sum_{i=1}^{\infty}\xi_{ij}p^i$ instead of $x_j = \sum_{i=0}^{\infty}\xi_{ij}p^i$ and one has it. Q.E.D.