COMPUTATIONS IN CLASSICAL GROUPS

A thesis

submitted in partial fulfillment of the requirements

of the degree of

Doctor of Philosophy

by

Sushil Bhunia

ID: 20123166

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH PUNE

April, 2017

Dedicated to

My Grandmother

Certificate

Certified that the work incorporated in the thesis entitled "*Computations in Classical Groups*", submitted by *Sushil Bhunia* was carried out by the candidate, under my supervision. The work presented here or any part of it has not been included in any other thesis submitted previously for the award of any degree or diploma from any other university or institution.

Date: April 21, 2017 *Dr. Anupam Kumar Singh*

Thesis Supervisor

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that violation of the above will be cause for disciplinary action by the institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Date: April 21, 2017

Sushil Bhunia

Roll Number: 20123166

Acknowledgements

To my life-coach, my late grandmother Bishnupriya Bera: because I owe it all to you.

First and foremost, I would like to express my sincere gratitude to my thesis supervisor Dr. Anupam Singh for the continuous support, for his patience, motivation, enthusiasm and encouragement. He was always ready to discuss with me. He trusted my ability and was patient enough to explain anything to me. I could not have imagined having a better guide for my Ph.D. The questions studied in this thesis are formulated by him.

Besides my supervisor, I would like to thank the rest of my research advisory committee: Prof. K. N. Raghavan and Dr. Baskar Balasubramanyam for their insightful comments and encouragement. I had the opportunity to talk mathematics with several people. I would like to thank them for their support and encouragement. In particular, I would like to thank Prof. Dipendra Prasad, Prof. Amritanshu Prasad, Prof. Maneesh Thakur and Prof. Benjamin Martin. I had very helpful mathematical discussions with Dr. Ayan Mahalanobis, Dr. Krishnendu Gongopadhyay, and Dr. Ronnie Sebastian.

I owe my understanding of mathematics to many mathematicians at IISER Pune, especially to Dr. Diganta Borah, Dr. Chandrasheel Bhagwat, Dr. Rabeya Basu, Dr. A. Raghuram, Dr. Steven Spallone, Dr. Vivek Mohan Mallick, Dr. Kaneenika Sinha, Dr. Tejas Kalelkar, Dr. Krishna

Kaipa and Dr. Amit Hogadi. I am grateful to all of them. I am thankful to CSIR for the financial support in the form of the research fellowship. I would like to acknowledge the support of the institute and its administrative staff members for their cooperation, special thanks are due to Mrs. Suvarna Bharadwaj, Mr. Tushar Kurulkar and Mr. Kalpesh Pednekar.

I am grateful to my teachers starting from my school days till date having faith in me and guiding me in right direction. Especially to Mr. Chittaranjan Chaudhuri, Mr. Suvendu Dandapat, Mr. Gautambabu in school and Prof Himadrisekhar Sarkar in Jadavpur University.

I thank all my school friends, batchmates in Jadavpur University and IISER Pune, with whom I shared good times and bad times as well. Many of you will recognize yourselves, and I hope that you will forgive me for not naming you individually. I thank my friends in Jadavpur University. In particular, Debmalya, Prahlad, Srimoyee, Simi, Mousumi, Barnali, Nirupam, Chiranjit, Dibakar, Dishari, Ibrahim, Manoranjanda, Biswajitda, and Gautamda. All the students of Mathematics at IISER Pune deserve a note of appreciation for being enthusiastic about discussing mathematics with me. I thank Rohit, Yasmeen, Hitesh, Rashmi, Sudhir, Manidipa, Pralhad, Prabhat, Makarand, Jatin, Neha, Jyotirmoy, Milan, Tathagata, Debangana, Ayesha, Girish, Advait, Chitrabhanuda, Dilpreet, Uday, Ratna, and others for their help and discussions. With a special mention to Mr. Rohit Joshi. It was fantastic to have the opportunity to discuss mathematics with him. A special acknowledgment goes to my office mate of many years: Ms. Manidipa Pal. She was a true friend ever since we began to share an office in 2012. I must thank Mr. Uday Baskar Sharma for correcting my English. I thank all the security persons in IISER and my special thanks to IISER football team.

Finally, I must express my deepest gratitude to my parents for providing me with unconditional support and constant encouragement throughout my years of study and through the process of research and write this thesis and my life in general, without whom this thesis would not have existed. I am also grateful to my other family members who have supported me along the way. Especially to my younger brother Samir, my sisters Swapna, Bandana, Gangotryi and my nephew Chunai, Munai. Last but not the least to my Kakima and Sir. Also a mention to Pramita. It is not possible to express my gratitude towards them in words.

Sushil Bhunia

Contents

Abstract

In this thesis, we develop algorithms similar to the Gaussian elimination algorithm in symplectic and split orthogonal similitude groups. As an application to this algorithm, we compute the spinor norm for split orthogonal groups. Also, we get similitude character for symplectic and split orthogonal similitude groups, as a byproduct of our algorithms.

Consider a perfect field k with $\operatorname{char} k \neq 2$, which has a non-trivial Galois automorphism of order 2. Further, suppose that the fixed field k_0 has the property that there are only finitely many field extensions of any finite degree. In this thesis, we prove that the number of z-classes in the unitary group defined over k_0 is finite. Eventually, we count the number of z-classes in the unitary group over a finite field $\mathbb{F}_q$, and prove that this number is same as that of the general linear group over $\mathbb{F}_q$ (provided $q > n$).

Notation

k : a field (char $\neq 2$)

$k^{\times}$: $k \setminus \{0\}$

$\bar{k}$: algebraic closure of k

$\mathbb{Z}$: integers

$\mathbb{Q}$: rational numbers

$\mathbb{R}$: real numbers

$\mathbb{C}$: complex numbers

$\mathbb{Q}_p$: p-adic fields

$\mathbb{F}_q$: finite fields with q elements

R : a commutative ring with 1

$R^{\times}$: units of a ring R

(V, B) : bilinear or sesquilinear form on V

β : the matrix of B relative to a basis

dV : discriminant of (V, B)

Q : a quadratic form

$\otimes$: tensor product

$\oplus$: direct sum

$\perp$: orthogonal sum

$\cong$: isomorphism

$\mathcal{Z}_G(g)$: centralizer of g in G

$\mathcal{Z}(G)$: center of G

Aut (V) : set of all automorphisms of V

$M(n, k)$: matrix algebra over k

$GL(V)$ or $GL(n, k)$: general linear group

$SL(V)$ or $SL(n, k)$: special linear group

$GSp(V, B)$ or $GSp(n, k)$: symplectic similitude group

$Sp(V, B)$ or $Sp(n, k)$: symplectic group

$GO(V, B)$ or $GO(n, k)$: orthogonal similitude group

$O(V, B)$ or $O(n, k)$: orthogonal group

$U(V, B)$ or $U(n, k)$: unitary group

Gal (L/k) : Galois group of a field L over k

$\det(g)$: determinant of a matrix g

${}^t g$: transpose of a matrix g

${}^t g^{-1}$: transpose inverse of a matrix g

$p(n)$: number of partitions of n

$\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$: diagonal matrix

italic : definition

$\square$: end of a proof

Chapter 1

Introduction

This thesis deals with the subject of classical groups. Specifically, we deal with the Gaussian elimination for some similitude groups, and conjugacy classes of centralizers for certain classical groups. We give a concrete algorithm for symplectic and split orthogonal similitude groups analogous to the usual row and column operations to solve the word problem. Also, we give structure of centralizers and classes of centralizers in unitary groups to complete the story for classical groups, at least as far as the topics we deal with are concerned.

What is the Gaussian elimination?

Gaussian elimination is a very old technique in Mathematics. It appeared in print as chapter eight in a Chinese mathematical text called, “The nine chapters of the mathematical art”. It is believed, a part of that book was written as early as 150 BCE. For a historical perspective on Gaussian elimination, we refer to a nice work by Grcar [Gc].

In computational group theory, one is always looking for algorithms that solve the word problem. Algorithms for word problem are useful in other programs in computational group theory, namely, the group recognition program and the membership problems. Extensive work on these programs are being done by several people Leedham-Green and O'Brien [LO], and Guralnick et.al. [GKKL]. Thus, one of the main objectives of this thesis is to give an algorithm, on similar lines as the row-column operations for general linear groups, to solve the word problem for similitude groups. In this thesis, we work with Chevalley generators [Ca1]. Chevalley generators for the special linear group $SL(n, k)$ are elementary transvections, which are used to do the Gaussian elimination for $GL(n, k)$. The similitude groups are thought of as an analog of what $GL(n, k)$ is for $SL(n, k)$. So, for the Gaussian elimination of symplectic and split orthogonal similitude groups, we use the Chevalley generators.

These Chevalley generators for classical groups are well-known for a very long time. However, its use in row-column operations in symplectic and split orthogonal similitude groups is new. We develop row-column operations, very similar to the Gaussian elimination algorithm for general linear groups. We call our algorithms **Gaussian elimination** in symplectic and split orthogonal similitude groups respectively.

In a nutshell, Gaussian elimination is nothing but a series of row and column operations. For details see Chapter 6. The algorithms that we develop in this thesis work for a split bilinear form B (see (4) in Example 2.2.20). First, we define elementary matrices (see Section 3.2), which give elementary operations (see 6.2) for similitude groups. We prove the following result:

Theorem 1.0.1 (Theorem 6.3.11). *Every element of the symplectic similitude group $GSp(2l, k)$ or split orthogonal similitude group $GO(n, k)$ (here $n = 2l$ or $2l + 1$), can be written as a product of elementary matrices and a diagonal matrix. Furthermore, the diagonal matrix is of the following form:*

1. *In* $GSp(2l,k)$, $\mathrm{diag}(\underbrace{1,\ldots,1}_{l},\underbrace{\mu(g),\ldots,\mu(g)}_{l})$, *where* $\mu(g)\in k^{\times}$.

2. *In* $GO(2l,k)$, $\mathrm{diag}(\underbrace{1,\ldots,1,\lambda}_{l},\underbrace{\mu(g),\ldots,\mu(g),\mu(g)\lambda^{-1}}_{l})$, *where* $\mu(g),\lambda\in k^{\times}$.

3. *In* $GO(2l+1,k)$, $\mathrm{diag}(\alpha,\underbrace{1,\ldots,1,\lambda}_{l},\underbrace{\mu(g),\ldots,\mu(g),\mu(g)\lambda^{-1}}_{l})$, *where* $\alpha^2=\mu(g)$ *and* $\mu(g),\lambda\in k^{\times}$.

What is the spinor norm and why study them?

Let k be a field with $\mathrm{char}\, k\neq 2$. The **spinor norm** is a group homomorphism $\Theta : O(n,k)\to k^{\times}/k^{\times 2}$ defined by $\Theta(g)=\prod_{i=1}^{m} Q(u_i)k^{\times 2}$, where $g=\sigma_{u_1}\sigma_{u_2}\cdots\sigma_{u_m}$ using Cartan-Dieudonne theorem (see Section 2.2.3). In the connection to group recognition project, Scott H. Murray and Colva M. Roney-Dougal [MR] studied spinor norm earlier. The definition of the spinor norm is not friendly to compute. Hahn, Wall, and Zassenhaus [Ha, Wa1, Za] developed a theory to compute the spinor norm. In this thesis, we will give an efficient algorithm to compute the spinor norm using Gaussian elimination algorithm. From Gaussian elimination algorithm, one can compute the spinor norm easily. Since the commutator subgroup of the orthogonal group is the kernel of the spinor norm restricted to the special orthogonal group, so the following theorem also gives a membership test for the commutator subgroup in the orthogonal group. We prove the following result:

Theorem 1.0.2 (Theorem 7.1.2)**.** *Let* $g\in O(n,k)$ *(here* $n=2l$ *or* $n=2l+1$*). Suppose Gaussian elimination reduces* g *to* $\mathrm{diag}(\underbrace{1,\ldots,1,\lambda}_{l\ or\ l+1},\underbrace{1,\ldots,1,\lambda^{-1}}_{l})$, *where* $\lambda\in k^{\times}$. *Then the spinor norm* $\Theta(g)=\lambda k^{\times 2}$.

What are the z-classes and why study them?

Let G be a group. The elements x and $y \in G$ are said to be z-equivalent denoted as $x \sim_z y$ if their centralizers in G are conjugate, i.e., $\mathcal{Z}_G(y) = g\mathcal{Z}_G(x)g^{-1}$ for some $g \in G$, where $\mathcal{Z}_G(x) := \{g \in G \mid gx = xg\}$ denotes centralizer of x in G. Clearly $\sim_z$ is an equivalence relation on G. The equivalence classes with respect to this relation are called **z-classes**. It is easy to see that if two elements of a group G are conjugate then their centralizers are conjugate, thus they are also z-equivalent. However, in general, the converse is not true. In fact, a group may have infinitely many conjugacy classes but finitely many z-classes (see Example 8.2.7). In this thesis, we explore the z-classes for classical groups. In [St2], R. Steinberg proved the following:

Theorem 1.0.3 (Steinberg)**.** *Let G be a reductive algebraic group defined over an algebraically closed field k of good characteristic, then the number of z-classes in G is finite.*

Question 1.0.4. *What can we say about the finiteness of z-classes for algebraic group G defined over an arbitrary field k?*

To study this we assume that the field k satisfies the following property:

Definition 1.0.5 (Property FE)**.** A perfect field k of $\operatorname{char} k \neq 2$ has the property FE if k has only finitely many field extensions of any finite degree.

Examples of such fields are, algebraically closed fields (for example, $\mathbb{C}$), real numbers $\mathbb{R}$, local fields (for example, $\mathbb{Q}_p$), and finite fields $\mathbb{F}_q$. From now on we assume that k has property FE unless stated otherwise. In [Si], A. Singh studied z-classes for real compact groups of type G_2. Ravi S. Kulkarni proved the following (see Theorem 7.4 [Ku]):

Theorem 1.0.6 (Kulkarni)**.** *Let V be an n-dimensional vector space over a field k with the property FE, then the number of z-classes in $GL(n,k)$ is finite.*

K. Gongopadhyay and Ravi S. Kulkarni proved the following (Theorem 1.1 [GK]):

Theorem 1.0.7 (Gongopadhyay-Kulkarni)**.** *Let V be an n-dimensional vector space over a field k with the property FE, equipped with a non-degenerate symmetric or skew-symmetric bilinear form B. Then, there are only finitely many z-classes in orthogonal groups $O(V,B)$ and symplectic groups $Sp(V,B)$.*

This result generalizes Steinberg's result mentioned above (Theorem 1.0.3). In this thesis, we extend this result to the unitary groups. We prove the following result:

Theorem 1.0.8 (Theorem 8.2.4)**.** *Let k be a perfect field of* $\operatorname{char} k \neq 2$ *with a non-trivial Galois automorphism of order* 2. *Let V be a finite dimensional vector space over k with a non-degenerate hermitian form B. Suppose the fixed field k_0 has the property FE, then the number of z-classes in the unitary group $U(V,B)$ is finite.*

The FE property of the field is necessary for the above theorem. For example, the field of rationals $\mathbb{Q}$ does not have property FE. We show that the above theorem is no longer true over $\mathbb{Q}$ (see Example 8.2.6).

If we look at character table of $SL(2,q)$ (for example see [B] and [Pr]), we notice conjugacy classes and irreducible characters bunched together. One observes a similar pattern in the work of Srinivasan [Sr] for $Sp(4,q)$. In [Gr], Green studied the complex representations of $GL(n,q)$ where he introduced the function $t(n)$ for the 'types of characters/classes' (towards the end of section 1 on page 407-408) which is same as the number of z-classes in $GL(n,q)$.

In Deligne-Lusztig theory, where one studies representation theory of finite groups of Lie type, z-classes of semisimple elements play an important role. In [Ca2] Carter and in [Hu2] Humphreys defined genus of an algebraic group G defined over k. Two semisimple elements have same *genus* if they are z-equivalent in $G(k)$. Thus understanding z-classes for finite groups of Lie type, especially semisimple z-classes, and their counting is of importance in representation theory (see [Fl, FG, Ca2, DM]). A. Bose, in [Bo], calculated the genus number for simply connected simple algebraic groups over an algebraically closed field, and compact simple Lie groups. In this thesis we prove the following:

Theorem 1.0.9 (Theorem 9.2.5)**.** *The number of z-classes in $U(n,q)$ is same as the number of z-classes in $GL(n,q)$ if $q > n$. Thus, the number of z-classes for either group can be read off by looking at the coefficients of the function* $\prod_{i=1}^{\infty} z(x^i)$*, where* $z(x) = \prod_{j=1}^{\infty} \frac{1}{(1-x^j)^{p(j)}}$.

Along the way, we also prove some counting results (see for example, Proposition 9.1.1, Proposition 9.1.2, Theorem 9.2.3).

A chapter wise description: A conscious effort is made to make this thesis self-contained and reader-friendly. The results in Chapters 2 to 5 are all well-known. They are preliminary in nature, and almost all basic results are recalled in the first four chapters, which are used in this thesis. After covering the preliminaries in the first four chapters, we report on author's research work in the next four chapters. Finally, in the last chapter, we give some further research problems. That pretty much summarizes the thesis giving glimpses into the main results proved in the various chapters.

Chapter 2

Classical Groups

This chapter is the most basic and at the same time most essential part of this thesis. In this chapter, we will discuss the groups that are popularly known as the classical groups, as they were named by Hermann Weyl. Let k be a field. Let V be an n-dimensional vector space over k. We denote the set of all invertible linear transformations of V by $GL(V)$. The set $GL(V)$ is a group under the multiplication defined by the composition of maps. Let us fix a basis $\{e_1, \ldots, e_n\}$ of V. Then we can identify $GL(V)$ with $GL(n, k) = \{g \in M(n, k) \mid \det(g) \neq 0\}$, the set of all $n \times n$ invertible matrices. This group is called the *general linear group*. All further groups discussed are subgroups of $GL(V)$. The *special linear group* $SL(n, k) := \{g \in GL(n, k) \mid \det(g) = 1\}$. In Weyl's words, "each group stands in its own right and does not deserve to be looked upon merely as a subgroup of something else, be it even *Her All-embracing Majesty* $GL(n)$". The exposition in this chapter is mostly based on the book by Larry C. Grove [Gv]. In Section 2.1 we describe reductive algebraic groups. Section 2.2 covers the basic definitions and some very basic properties of classical groups, especially for symplectic and orthogonal groups. Also in this section, we introduce the notion of the spinor norm. In the last section, we describe the unitary groups and some important examples, which will be useful later in this thesis.

2.1 Reductive Algebraic Groups

There are several excellent references for this topic, Borel [Br], Springer [Sp] and Humphreys [Hu1], to name a few. We fix a perfect field k ($\mathrm{char}\, k \neq 2$) for this section, and $\bar{k}$ denotes the algebraic closure of k. An *algebraic group* G defined over $\bar{k}$ is a group as well as an affine variety over $\bar{k}$ such that the maps $\mu\colon G \times G \to G$, and $i\colon G \to G$ given by $\mu(g_1, g_2) = g_1 g_2$, and $i(g) = g^{-1}$ are morphisms of varieties. An *algebraic group* G is defined over k, if the polynomials defining the underlying affine variety G are defined over k, with the maps μ and i defined over k, and the identity element e is a k-rational point of G. We denote the k-rational points of G by $G(k)$. Any algebraic group G is a closed subgroup of $GL(n)$ for some n. Hence algebraic groups are called *linear algebraic groups*.

An element in $GL(n, k)$ is called *semisimple* (respectively, *unipotent*) if it is diagonalizable over $\bar{k}$ (respectively, if all its eigenvalues are equal to 1). We have $G \hookrightarrow GL(n)$. An element $g \in G$ is said to be *semisimple* (respectively, *unipotent*) if the image of g, under the above inclusion, is semisimple (respectively, unipotent), being semisimple and unipotent is a functorial property. An algebraic group G is said to be *unipotent* if all its elements are unipotent. The *radical* of an algebraic group G over k is defined to be the largest closed, connected, solvable, normal subgroup of G, denoted by $R(G)$. We call G to be a *semisimple* algebraic group if $R(G) = \{e\}$. The *unipotent radical* of G is defined to be the closed, connected, unipotent, normal subgroup of G and denoted by $R_u(G)$. We call G to be *reductive* if $R_u(G) = \{e\}$. For example, the group $GL(n)$ is a reductive group, whereas $SL(n)$ is a semisimple group. A semisimple algebraic group is always a reductive group. In next section, we see more examples of algebraic groups, namely, classical groups.

2.1.1 Jordan decomposition

Recall that an element $g \in GL(n,k)$ can be written as $g = g_s g_u = g_u g_s$, in a unique way, where $g_s \in GL(n,k)$ is semisimple, and $g_u \in GL(n,k)$ is unipotent. This decomposition is called the *Jordan decomposition* for invertible matrices. We have the following Jordan decomposition in linear algebraic groups. We need the following (Theorem 2.4.8 [Sp]),

Theorem 2.1.1 (Jordan decomposition)**.** *Let G be a linear algebraic group defined over a perfect field k and let $g \in G$. Then there exist unique elements $g_s, g_u \in G$ such that $g = g_s g_u = g_u g_s$. Furthermore, if $\phi\colon G \to H$ is a homomorphism of linear algebraic groups, then $\phi(g_s) = \phi(g)_s$ and $\phi(g_u) = \phi(g)_u$.*

The elements g_s and g_u are called the *semisimple part* and the *unipotent part* of g respectively.

2.2 Symplectic and Orthogonal Groups

In this section, we follow Larry C. Grove [Gv], and define two important classes of groups, which preserve certain bilinear form. Let k be a field of char $k \neq 2$. Let V be an n-dimensional vector space over k.

Definition 2.2.1. A *bilinear form* on V is a function $B : V \times V \to k$ satisfying

1. $B(u+v,w) = B(u,w) + B(v,w)$
2. $B(u,v+w) = B(u,v) + B(u,w)$
3. $B(au,v) = aB(u,v) = B(u,av)$

for all $u, v, w \in V$ and all $a \in k$.

If B is a bilinear form on V and $\{e_1, e_2, \ldots, e_n\}$ is a basis for V, set $b_{ij} := B(e_i, e_j)$ for all $1 \leq i, j \leq n$. Then $\beta := (b_{ij})$ is called the matrix of B relative to $\{e_1, e_2, \ldots, e_n\}$. If $u, w \in V$, write $u = \sum_i a_i e_i$, and $w = \sum_j b_j e_j$, so that u and w are represented by column vectors $\mathbf{u} = {}^t(a_1 \cdots a_n)$ and $\mathbf{w} = {}^t(b_1 \cdots b_n)$. Then $B(u, w) = {}^t\mathbf{u}\beta\mathbf{w}$ for all $u, w \in V$, where $\mathbf{u}, \mathbf{w}$ are the column vectors with the entries being the components of u, w with respect to the given basis $\{e_1, e_2, \ldots, e_n\}$ of V. If $\{f_1, f_2, \ldots, f_n\}$ is another basis for V, write $f_j = \sum_i p_{ij} e_i$, where $p_{ij} \in k$, for all $j = 1, 2, \ldots, n$. Then $B(f_i, f_j) = \sum_{k,l} p_{ki} B(e_k, e_l) p_{lj} = \sum_{k,l} p_{ki} b_{kl} p_{lj}$, which is the (i, j)-entry of ${}^tP\beta P$, where $P = (p_{ij}) \in GL(n, k)$, is the change of basis matrix. We say two $n \times n$ matrices M, N are *congruent* if $N = {}^tPMP$, for some $P \in GL(n, k)$. So $\det N = \det P \det M \det P$. Define $k^{\times 2} := \{a^2 \mid a \in k^\times\}$. Then $k^{\times 2}$ is a subgroup of $k^\times$.

Notation 2.2.2. A vector space V having a bilinear form B will be denoted by (V, B).

Definition 2.2.3. Define the *discriminant* of (V, B) to be

$$dV := \begin{cases} 0 & \text{if } \det\beta = 0, \\ (\det\beta)k^{\times 2} & \text{otherwise.} \end{cases}$$

Observe that the discriminant dV is independent of the choice of basis.

Definition 2.2.4. The bilinear form (V, B) is said to be *non-degenerate* if $dV \neq 0$.

Definition 2.2.5. A subspace W of V is said to be *non-degenerate* if $\operatorname{rad} W := W \cap W^\perp = \{0\}$, where $W^\perp = \{v \in V \mid B(w, v) = 0 \ \forall w \in W\}$.

Unless otherwise specified, we assume from now on that (V, B) is a non-degenerate bilinear form.

Definition 2.2.6. Two bilinear forms (V_1, B_1) and (V_2, B_2) are said to be *equivalent*, denoted by $(V_1, B_1) \approx (V_2, B_2)$, if there exists a vector space isomorphism $\sigma : V_1 \to V_2$ such that $B_2(\sigma u, \sigma v) = B_1(u, v)$ for all $u, v \in V_1$.

Remark 2.2.7. We call the above σ an *isometry* with respect to B_1 and B_2.

2.2.1 Symplectic groups

Definition 2.2.8. A bilinear form B is said to be *skew-symmetric* or *alternating* if $B(u, v) = -B(v, u)$ for all $u, v \in V$.
Alternatively, this definition is equivalent to $B(u, u) = 0$ for all $u \in V$. In matrix terminology, the bilinear form B is skew-symmetric if and only if any representing matrix β is skew-symmetric, i.e., ${}^t\beta = -\beta$.

For the remainder of this section (V, B) will denote a non-degenerate alternating bilinear form.

Definition 2.2.9. A pair $\{u, v\}$ of vectors is said to be a *hyperbolic pair* if $B(u, u) = 0 = B(v, v)$ and $B(u, v) = 1 = -B(v, u)$.

The restriction of B to the subspace generated by u, v has representing matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ relative to $\{u, v\}$.

Proposition 2.2.10 (Theorem 2.10 [Gv])**.** *If B is a non-degenerate alternating bilinear form on V, then there exists a basis $\{e_1, \ldots, e_l, e_{-1}, \ldots, e_{-l}\}$ of V relative to which the representing matrix has the following form $\beta = \begin{pmatrix} 0 & I_l \\ -I_l & 0 \end{pmatrix}$, where $\{e_i, e_{-i}\}$ is a hyperbolic pair for all $i = 1, 2, \ldots, l$.*

Definition 2.2.11 (Symplectic group)**.** The *symplectic group* is denoted by $Sp(V, B) := \{T \in GL(V) \mid B(Tu, Tv) = B(u, v)\ \forall u, v \in V\}$.

In matrix terminology, the symplectic group is defined as:

$$Sp(n,k) = Sp(2l,k) := \{g \in GL(n,k) \mid {}^t g \beta g = \beta\},$$

where $\beta = \begin{pmatrix} 0 & I_l \\ -I_l & 0 \end{pmatrix}$.

Definition 2.2.12 (Symplectic similitude group)**.** The *symplectic similitude group* with respect to the matrix β as in Definition 2.2.11, is defined by $GSp(n,k) = \{g \in GL(n,k) \mid {}^t g\beta g = \mu(g)\beta, \text{for some } \mu(g) \in k^\times\}$, where $\mu : GSp(n,k) \to k^\times; g \mapsto \mu(g)$, is a group homomorphism with $\ker \mu = Sp(n,k)$.

2.2.2 Orthogonal groups

Definition 2.2.13. A bilinear form B is said to be *symmetric* if $B(u,v) = B(v,u)$ for all $u, v \in V$. In matrix terminology, the bilinear form B is symmetric if and only if any representing matrix β is symmetric, i.e., ${}^t\beta = \beta$.

Definition 2.2.14. If B is a symmetric bilinear form on V, then $Q : V \to k$ defined by $Q(v) = \frac{B(v,v)}{2}$, is called a *quadratic form* associated to B.

Thus $B(u,v) = Q(u+v) - Q(u) - Q(v)$ for all $u, v \in V$. So the bilinear form B is completely determined by the quadratic form Q and vice-versa.
For the remainder of this section (V, B) will denote a non-degenerate symmetric bilinear form.

Definition 2.2.15 (Orthogonal group)**.** The *orthogonal group* is defined by

$$\begin{aligned} O(V,B) : &= \{T \in GL(V) \mid B(Tu, Tv) = B(u,v)\ \forall u, v \in V\} \\ &= \{T \in GL(V) \mid Q(Tv) = Q(v)\ \forall v \in V\}. \end{aligned}$$

In matrix terminology, the orthogonal group is defined as:

$$O(n,k) := \{g \in GL(n,k) \mid {}^t g \beta g = \beta\}.$$

Remark 2.2.16. Equivalent forms give conjugate groups in $GL(n,k)$, i.e., if $\beta_2 = {}^t g \beta_1 g$ for some $g \in GL(n,k)$ then $O(V_2, \beta_2) = g^{-1} O(V_1, \beta_1) g$.

Definition 2.2.17. A vector $v \in V$ is called *isotropic* if $Q(v) = 0$, and *anisotropic* if $Q(v) \neq 0$. A vector space V is called *isotropic* if $Q(v) = 0$ for some $0 \neq v \in V$.

Let $u \in V$ be any non-zero anisotropic vector, and define a linear transformation σ_u via

$$\sigma_u(v) := v - \frac{2B(u,v)}{B(u,u)} u$$

for all $v \in V$. Then $\sigma_u \in O(V, B)$. We call σ_u the *reflection* along u. The following theorem is well-known, that the orthogonal group is generated by reflections. We have (see Theorem 6.6 [Gv]):

Theorem 2.2.18 (E. Cartan-Dieudonné)**.** *If V is an n-dimensional vector space, equipped with a non-degenerate symmetric bilinear form B, then every element of $O(V, B)$ is a product of at most n reflections.*

Definition 2.2.19 (Orthogonal similitude group)**.** The *orthogonal similitude group* with respect to an invertible symmetric matrix β is defined by $GO(n,k) = \{g \in GL(n,k) \mid {}^t g \beta g = \mu(g)\beta, \text{for some } \mu(g) \in k^\times\}$, where $\mu : GO(n,k) \to k^\times; g \mapsto \mu(g)$, is a group homomorphism with $\ker \mu = O(n,k)$.

Example 2.2.20. 1. Let V be an n-dimensional vector space over $\mathbb{C}$ equipped with a non-degenerate symmetric bilinear form B. It is known that any two non-degenerate symmetric bilinear forms on V are equivalent, i.e., there is a basis for V relative to which $\beta = I_n$. So the corresponding orthogonal group is denoted by

$$O(n, \mathbb{C}) = \{g \in GL(n, \mathbb{C}) \mid {}^t g g = I_n\}.$$

2. Let V be an n-dimensional vector space over $\mathbb{R}$ equipped with a non-degenerate symmetric bilinear form B. In this situation, non-degenerate symmetric bilinear forms are classified by their signature, i.e., there is a basis for V relative to which $\beta = \begin{pmatrix} I_r & 0 \\ 0 & -I_s \end{pmatrix}$. So the corresponding orthogonal groups are denoted by

$$O(r, s) := \{g \in GL(n, \mathbb{R}) \mid {}^t g \beta g = \beta\},$$

where $r + s = n$.

3. Let V be an n-dimensional vector space over $\mathbb{F}_q$ equipped with a non-degenerate symmetric bilinear form B. Then there is a basis for V relative to which $\beta = \mathrm{diag}(\underbrace{1, \dots, 1}_{n-1}, \lambda)$, where $\lambda \in \mathbb{F}_q^\times$. Thus, up to equivalence, there are two such forms corresponding to a square and non-square elements of $\mathbb{F}_q^\times$. So the corresponding orthogonal groups are denoted by

$$O(n, q) = \{g \in GL(n, q) \mid {}^t g \beta g = \beta\}.$$

4. Let V be an n-dimensional vector space over k. Up to equivalence, there is a unique non-degenerate symmetric bilinear form B of maximal Witt index over k. This is called the *split form*. More explicitly we can fix a basis $\{e_1, \dots, e_l, e_{-1}, \dots, e_{-l}\}$ for even dimension, and $\{e_0, e_1, \dots, e_l, e_{-1}, \dots, e_{-l}\}$ for odd dimension, so that the matrix of B

is as follows:

$$\beta = \begin{cases} \begin{pmatrix} 0 & I_l \\ I_l & 0 \end{pmatrix} & \text{if } n = 2l, \\ \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & I_l \\ 0 & I_l & 0 \end{pmatrix} & \text{if } n = 2l+1. \end{cases}$$

The orthogonal group corresponding to this form is called a *split orthogonal group*. In this thesis, we will work with only the split orthogonal groups, and this group will be denoted by $O(n, k)$.

2.2.3 Spinor norm

For $u \in V$ with $Q(u) \neq 0$, we defined the reflection σ_u by $\sigma_u(v) = v - 2\frac{B(u,v)}{B(u,u)}u$ along u, which is an element of the orthogonal group. We know from Theorem 2.2.18 that every element of the orthogonal group $O(n, k)$ can be written as a product of at most n reflections. Let $g \in O(n, k)$ then $g = \sigma_{u_1}\sigma_{u_2}\cdots\sigma_{u_m}$ $(m \leq n)$, where $Q(u_i) \neq 0$ for all $i = 1, 2, \ldots, m$. We are now in a position to define the spinor norm. To show that this is well-defined map, we need Clifford algebra theory (see Chapter 9 [Gv]).

Definition 2.2.21. The *spinor norm* is a group homomorphism $\Theta : O(n, k) \to k^\times/k^{\times 2}$ defined by $\Theta(g) := \prod_{i=1}^{m} Q(u_i)k^{\times 2}$, where $g = \sigma_{u_1}\cdots\sigma_{u_m}$.

Thus for a reflection, we have $\Theta(\sigma_u) = Q(u)k^{\times 2}$. However, for computational purposes, this definition is difficult to use. In Chapter 4, we will define the spinor norm using Wall's theory, and we will give an efficient algorithm in Chapter 7 to compute the spinor norm.

2.3 Unitary Groups

For the material covered here, we refer to the books [Kn] and [Gv]. Let R be a commutative ring with 1. An *involution* on R is an automorphism $J : a \mapsto \bar{a}$ of R of order 2. Thus:

$$\overline{a+b} = \bar{a} + \bar{b}, \overline{ab} = \bar{a}\bar{b}, \bar{\bar{a}} = a,$$

for all $a, b \in R$. Set $R_0 := Fix(J) = \{a \in R \mid \bar{a} = a\}$. Let V be a free R-module of rank n. In this section, we discuss the unitary groups which are also one of the classical groups. The *General Linear Group* $GL(V)$ is a group of all R-linear isomorphism of the module V over R. In matrix terminology it consists of all $n \times n$ invertible matrices and denoted as $GL(n, R)$.

Definition 2.3.1. A *sesquilinear form* on V, with respect to J, is a function $B : V \times V \to R$ satisfying

1. $B(u + v, w) = B(u, w) + B(v, w)$
2. $B(u, v + w) = B(u, v) + B(u, w)$
3. $B(au, v) = \bar{a}B(u, v) = B(u, \bar{a}v)$

for all $u, v, w \in V$ and all $a \in R$.

If B is a sesquilinear form on V and $\{e_1, e_2, \ldots, e_n\}$ is a free basis for V, set $b_{ij} := B(e_i, e_j)$ for all $1 \leq i, j \leq n$. Then $\beta := (b_{ij})$ is called the matrix of B relative to $\{e_1, e_2, \ldots, e_n\}$. If $u, w \in V$, write $u = \sum_i a_i e_i$, and $w = \sum_j b_j e_j$, so that u and w are represented by column vectors $\mathbf{u} = {}^t(a_1 \cdots a_n)$ and $\mathbf{w} = {}^t(b_1 \cdots b_n)$. Then $B(u, w) = {}^t\bar{\mathbf{u}}\beta\mathbf{w}$ for all $u, w \in V$, where $\mathbf{u}, \mathbf{w}$ are the column vectors with the entries being the components of u, w with respect to the given basis $\{e_1, e_2, \ldots, e_n\}$ of V. If $\{f_1, f_2, \ldots, f_n\}$ is another free basis for V, write $f_j = \sum_i p_{ij} e_i$, where $p_{ij} \in R$, for all $j = 1, 2, \ldots, n$. Then $B(f_i, f_j) = \sum_{k,l} \bar{p}_{ki} B(e_k, e_l) p_{lj} = \sum_{k,l} \bar{p}_{ki} b_{kl} p_{lj}$, which is the (i, j)-entry of ${}^t\bar{P}\beta P$, where $P = (p_{ij}) \in GL(n, R)$. We say two $n \times n$ matrices M, N are *congruent* if $N = {}^t\bar{P}MP$, for some $P \in GL(n, R)$. So $\det(N) = \det(P)\overline{\det(P)}\det(M)$. Define $R^{1+J} := \{a\bar{a} \mid a \in R^\times\}$ is a subgroup of $R_0^\times$.

Notation 2.3.2. A free module V having a sesquilinear form B will be denoted by (V, B).

Definition 2.3.3. Define the *discriminant* of (V, B) to be

$$dV := \begin{cases} (\det\beta)R^{1+J} & \text{if } (\det\beta) \in R^\times, \\ 0 & \text{otherwise.} \end{cases}$$

Note that dV is independent of the choice of basis. The sesquilinear form B is said to be *non-degenerate* if $dV \in R^\times$.

Another way to look at the sesquilinear form is the following. Denote the dual of V by $V^* := \mathrm{Hom}_R(V, R)$. The form B induces a map $h_B : V \to V^*, h_B(v)(w) = B(v, w)$ for all $v, w \in V$, which is R-linear. Conversely, an R-linear homomorphism $h : V \to V^*$ defines a sesquilinear form $B_h : V \times V \to R, B_h(u, v) = h(u)(v)$ for all $u, v \in V$. We call h_B the *adjoint* of B. Since $h_{B_h} = h$ and $B_{h_B} = B$, a sesquilinear form is determined by its adjoint and vice-versa. If h_B is an R-module isomorphism between V and V^* then B is non-degenerate. The above two definitions for non-degeneracy are equivalent. Let B_1 and B_2 be two sesquilinear forms on V_1 and V_2 respectively. Two forms are said to be *equivalent*, denoted by $(V_1, B_1) \approx (V_2, B_2)$, if there exists a R-module isomorphism $\sigma : V_1 \to V_2$ such that $B_2(\sigma u, \sigma v) = B_1(u, v)$ for all $u, v \in V_1$. We call σ an *isometry* with respect to B_1 and B_2.

Definition 2.3.4. A sesquilinear form B is said to be *hermitian* if $B(u, v) = \overline{B(v, u)}$ for all $u, v \in V$. In matrix terminology, the sesquilinear form B is hermitian if and only if any representing matrix β is hermitian, i.e., ${}^t\bar{\beta} = \beta$.

Definition 2.3.5. A sesquilinear form B is said to be *skew-hermitian* if

$B(u,v) = -\overline{B(v,u)}$ for all $u, v \in V$. In matrix terminology, the sesquilinear form B is skew-hermitian if and only if any representing matrix β is skew-hermitian, i.e., ${}^t\bar{\beta} = -\beta$.

Remark 2.3.6. If B is a skew-hermitian form, then $B_1 := aB$ is a hermitian form for some $a \in R^\times$ with $\bar{a} = -a$. So the corresponding isometry group will be same whether we consider hermitian or skew-hermitian form.

For the remainder of this section (V, B) will denote a non-degenerate hermitian form.

Definition 2.3.7 (Unitary group)**.** The *unitary group* is defined as follows: $U(V, B) := \{T \in GL(V) \mid B(Tu, Tv) = B(u, v)\ \forall u, v \in V\}$.

In matrix terminology, the unitary group is defined as:

$$U(n, R_0) := \{g \in GL(n, R) \mid {}^t\bar{g}\beta g = \beta\}.$$

Most of the time we will consider unitary groups over fields.

Example 2.3.8.

1. Let V be an n-dimensional vector space over $\mathbb{C}$ with $\overline{a + ib} = a - ib$. In this situation, hermitian forms are classified by signature and given by $\beta = \begin{pmatrix} I_r & 0 \\ 0 & -I_s \end{pmatrix}$. So the corresponding unitary groups are denoted by

$$U(r, s) := \{g \in GL(n, \mathbb{C}) \mid {}^t\bar{g}\beta g = \beta\},$$

where $\bar{g} := (\bar{g}_{ij})$, where $\bar{g}_{ij}$ is the usual complex conjugate and $r+s = n$.

2. Let V be an n-dimensional vector space over a finite field $\mathbb{F}_{q^2}$ with $J : a \mapsto a^q$. It is known that any two hermitian forms on V are equivalent and thus we may choose $\beta = I_n$. So the corresponding

unitary group is, unique up to conjugation, and is denoted by

$$U(n,q) := \{g \in GL(n,q^2) \mid {}^t\overline{g}g = I_n\},$$

where $\bar{g} := (g_{ij}^q)$.

3. Let V be a free module over $R = k \times k$ of rank n with $J : (a,b) \mapsto \overline{(a,b)} = (b,a)$. Then $R_0 = \{(a,b) \in R \mid (b,a) = (a,b)\} = \mathrm{diag}(k \times k) \cong k$. Then the unitary group defined over R_0 is

$$U(n,k) = \{g \in GL(n,R) \mid {}^t\overline{g}\beta g = \beta\},$$

where $g = (A,B) \in M(n,k) \times M(n,k)$ and ${}^t\overline{g} = ({}^tB, {}^tA)$, and $\beta = (\beta_1, \beta_2)$. In particular, if $\beta = (I_n, I_n)$ then $U(n,k) = \{(A,B) \in M(n,k) \times M(n,k) \mid {}^tAB = I_n\} \cong GL(n,k)$.

4. Let V be an n-dimensional vector space over k with an involution $J : a \mapsto \bar{a}$. Up to equivalence, there is a unique non-degenerate hermitian form B of maximal Witt index over k. This is called the *split form*. More explicitly we can fix a basis $\{e_1, \ldots, e_l, e_{-1}, \ldots, e_{-l}\}$ for even dimension, and $\{e_0, e_1, \ldots, e_l, e_{-1}, \ldots, e_{-l}\}$ for odd dimension, so that the matrix of B is as follows:

$$\beta = \begin{cases} \begin{pmatrix} 0 & I_l \\ I_l & 0 \end{pmatrix} & \text{if } n = 2l, \\ \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & I_l \\ 0 & I_l & 0 \end{pmatrix} & \text{if } n = 2l+1. \end{cases}$$

The unitary group corresponding to this form is called a *split unitary group*. In Section 6.4 of Chapter 6 we will work with only the split unitary groups, and this group will be denoted by $U(n, k_0)$, where k_0 is the fixed field.

Chapter 3

Chevalley Groups

This is another basic chapter of this thesis. In the present chapter, we will take another approach to define the split classical groups. For the Gaussian elimination, which we will develop in Chapter 6, we need an analog of elementary matrices. These matrices are described in Section 3.2, which come from the theory of Chevalley groups (of adjoint type). In this theory, one begins with a complex simple Lie algebra $\mathfrak{g}$, a field k, and get a group $G(k)$ (see Section 3.1). The theory was developed by Chevalley [Ch] himself, and further generalized by Robert Steinberg [St1]. In our computations, we often imitate the notation from Carter [Ca1].

3.1 Construction of Chevalley Groups (adjoint type)

Let $\mathfrak{g}$ be a complex simple Lie algebra. Since any two Cartan subalgebras of $\mathfrak{g}$ are conjugate, we fix a Cartan subalgebra $\mathfrak{h}$. Then there is the adjoint representation of $\mathfrak{g}$,

$$\mathrm{ad} : \mathfrak{g} \to \mathfrak{g}l(\mathfrak{g})$$

given by $\mathrm{ad}X(Y) = [X, Y]$. Since $\mathfrak{h}$ is Abelian, $\mathrm{ad}(\mathfrak{h})$ is a commuting family of semisimple linear transformations of $\mathfrak{g}$. Hence $\mathrm{ad}(\mathfrak{h})$ is simultaneously diagonalizable. Thus we have (see p.35 [Ca1]):

Theorem 3.1.1 (Cartan decomposition)**.** *With this notation, we have,*

$$\mathfrak{g} = \mathfrak{h} \bigoplus \sum_{\alpha \in \Phi} \mathfrak{g}_\alpha,$$

where $\mathfrak{g}_\alpha = \{X \in \mathfrak{g} \mid \mathrm{ad}H(X) = \alpha(H)X,\ \forall H \in \mathfrak{h}\}$ *are root spaces and* Φ *is a root system with respect to* $\mathfrak{h}$*.*

We call this decomposition the *Cartan decomposition* of $\mathfrak{g}$ with respect to $\mathfrak{h}$. The classification of finite dimensional complex simple Lie algebras gives four infinite families $A_l(l \geq 1), B_l(l \geq 2), C_l(l \geq 3)$ and $D_l(l \geq 4)$ called *classical types*, and five *exceptional types* G_2, F_4, E_6, E_7 and E_8. Chevalley proved that, there exists a basis of $\mathfrak{g}$ such that all the structure constants, which define $\mathfrak{g}$ as a Lie algebra, are integers. The following (Theorem 4.2.1 [Ca1]) is a key theorem to define Chevalley groups.

Theorem 3.1.2 (Chevalley basis theorem)**.** *Let* $\mathfrak{g}$ *be a simple Lie algebra over* $\mathbb{C}$*,* $\mathfrak{h}$ *be a Cartan subalgebra, and*

$$\mathfrak{g} = \mathfrak{h} \bigoplus \sum_{\alpha \in \Phi} \mathfrak{g}_\alpha$$

be a Cartan decomposition of $\mathfrak{g}$*. Let* $h_\alpha \in \mathfrak{h}$ *be the co-root corresponding to the root* α*. Then, for each root* $\alpha \in \Phi$*, an element* e_α *can be chosen in* $\mathfrak{g}_\alpha$ *such that*

$$[e_\alpha, e_{-\alpha}] = h_\alpha,$$
$$[e_\alpha, e_\beta] = \pm(r+1)e_{\alpha+\beta},$$

where r is the greatest integer for which $\beta - r\alpha \in \Phi$.

The elements $\{h_\alpha, \alpha \in \Pi; e_\alpha, \alpha \in \Phi\}$ form a basis for $\mathfrak{g}$, called a ***Chevalley basis****. The basis elements multiply together as follows:*

$$\left.\begin{aligned}
[h_\alpha, h_\beta] &= 0, \\
[h_\alpha, e_\beta] &= A_{\alpha\beta} e_\beta, \\
[e_\alpha, e_{-\alpha}] &= h_\alpha, \\
[e_\alpha, e_\beta] &= 0 && \text{if } \alpha + \beta \notin \Phi, \\
[e_\alpha, e_\beta] &= \pm(r+1) e_{\alpha+\beta} && \text{if } \alpha + \beta \in \Phi,
\end{aligned}\right\} \tag{3.1}$$

where $A_{\alpha\beta}$ are Cartan integers and Π, a simple root system fixed for Φ.

The structure constants of the algebra with respect to a Chevalley basis are all integers.

The map $\mathrm{ad} e_\alpha$ is a nilpotent linear map on $\mathfrak{g}$. Let $t \in \mathbb{C}$, then $\mathrm{ad}(te_\alpha) = t(\mathrm{ad} e_\alpha)$ is also nilpotent. Thus $\exp(t(\mathrm{ad} e_\alpha))$ is an automorphism of $\mathfrak{g}$. We denote by $\mathfrak{g}_\mathbb{Z}$ the subset of $\mathfrak{g}$ of all $\mathbb{Z}$-linear combinations of the Chevalley basis elements of $\mathfrak{g}$. By Equation (3.1), a Lie bracket can be defined for $\mathfrak{g}_\mathbb{Z}$. Thus $\mathfrak{g}_\mathbb{Z}$ is a Lie algebra over $\mathbb{Z}$. Now let k be any field. We define $\mathfrak{g}_k := \mathfrak{g}_\mathbb{Z} \otimes_\mathbb{Z} k$. Then $\mathfrak{g}_k$ is a Lie algebra over k via the Lie multiplication

$$[X \otimes 1_k, Y \otimes 1_k] := [X, Y] \otimes 1_k,$$

where X, Y are Chevalley basis elements of $\mathfrak{g}$, and 1_k denote the identity element of k.

Now everything makes sense over an arbitrary field k. So we are in a position to define the Chevalley groups of adjoint type. The Chevalley group of type $\mathfrak{g}$ over the field k, denoted by $G(k)$, is defined to be the subgroup of automorphisms of the Lie algebra $\mathfrak{g}_k$ generated by $\exp(t(\mathrm{ad} e_\alpha))$ for all $\alpha \in \Phi, t \in k$. In fact, the group $G(k)$ over k is determined up to isomorphism by the simple Lie algebra $\mathfrak{g}$ over $\mathbb{C}$ and the field k.

Observe that (see Lemma 4.5.1, p.65 [Ca1]), when $\mathfrak{g}$ is a linear Lie algebra,

$$\exp(t(\mathrm{ad}e_\alpha))X = \exp(te_\alpha)X\exp(te_\alpha)^{-1},$$

for all $X \in \mathfrak{g}_k$, for all $\alpha \in \Phi$, and for all $t \in k$. We shall abuse the notation slightly and denote the matrix of the linear map by $\exp(te_\alpha)$ itself. Define $x_\alpha(t) := \exp(te_\alpha)$. We call the $x_\alpha(t)$, *elementary matrix*. Let $\tilde{G}(k)$ be the group of matrices generated by the elements $x_\alpha(t)$ for all $\alpha \in \Phi$ and all $t \in k$. Thus there is a homomorphism from $\tilde{G}(k)$ onto $G(k)$ such that

$$\exp(te_\alpha) \mapsto \exp(t(\mathrm{ad}e_\alpha))$$

whose kernel is the center of $\tilde{G}(k)$. Hence $\frac{\tilde{G}(k)}{\mathcal{Z}(\tilde{G}(k))} \cong G(k)$. We work with $\tilde{G}(k)$ instead of the Chevalley group $G(k)$. In (see Section 11.2 [Ca1]), the classical Lie algebras and their Chevalley basis are described explicitly. Usually, row-column operations are defined by pre and post multiplication by certain elementary matrices. We are going to define the elementary matrices for symplectic and orthogonal groups, and more generally, for symplectic and orthogonal similitude groups.

Example 3.1.3 (Cartan decomposition and Chevalley basis of $\mathfrak{sp}(2l,\mathbb{C})$)**.** Let us consider the Lie algebra of type C_l:

$$\mathfrak{g} := \mathfrak{sp}(2l,\mathbb{C}) = \{X \in \mathfrak{gl}(2l,\mathbb{C}) \mid {}^tX\beta + \beta X = 0\},$$

where $\beta = \begin{pmatrix} 0 & I_l \\ -I_l & 0 \end{pmatrix}$. We can write elements of $\mathfrak{g}$ in block form. Let $X = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathfrak{g}$, where A, B, C, D are $l \times l$ matrices. We use the condition that X satisfies ${}^tX\beta + \beta X = 0$, then we get ${}^tB = B, {}^tC = C$ and $D = -{}^tA$.

The set of diagonal matrices in $\mathfrak{g}$ is a Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$. The elements of $\mathfrak{h}$ have form $H = \text{diag}(\lambda_1, \ldots, \lambda_l, -\lambda_1, \ldots, -\lambda_l)$. We index the rows and columns by $1, \ldots, l$ and $-1, \ldots, -l$. The elements $H_i = e_{ii} - e_{-i,-i}, 1 \leq i \leq l$, form a basis of $\mathfrak{h}$. Then by Theorem 3.1.1, we have,

$$\mathfrak{g} = \mathfrak{h} \oplus \sum_{\alpha \in \Phi} \mathbb{C} e_\alpha,$$

where

$$e_\alpha = \begin{cases} e_{ij} - e_{-j,-i}, & 1 \leq i \neq j \leq l, \\ e_{i,-j} + e_{j,-i}, & 1 \leq i < j \leq l, \\ e_{-i,j} + e_{-j,i}, & 1 \leq i < j \leq l, \\ e_{i,-i}, & 1 \leq i \leq l, \\ e_{-i,i}, & 1 \leq i \leq l. \end{cases} \tag{3.2}$$

The above decomposition is the Cartan decomposition of the Lie algebra $\mathfrak{g} = \mathfrak{sp}(2l, \mathbb{C})$, and a Chevalley basis for this Lie algebra is

$$\{H_i = e_{ii} - e_{-i,-i}, 1 \leq i \leq l; e_\alpha, \alpha \in \Phi\},$$

where e_α as in Equation (3.2). Observe that the above mentioned Chevalley basis is not unique, in fact, any integral multiple of it is again a Chevalley basis. Now e_α's are nilpotent endomorphisms of $\mathfrak{g}$ with $e_\alpha^2 = 0$. So $x_\alpha(t) = \exp{(te_\alpha)} = I + te_\alpha$, elementary matrix, is an automorphism of $\mathfrak{g}$. Similarly, we can do this, for orthogonal Lie algebras. For details see [Ca1]. In next section, we define these matrices explicitly.

3.2 Elementary Matrices

First of all, let us describe the elementary matrices for symplectic and split orthogonal similitude groups. The genesis of these elementary matrices lies in the Chevalley basis theorem (Theorem 3.1.2). In what follows, the scalar t varies over the field k, $n = 2l$ or $n = 2l + 1$, and $1 \leq i, j \leq l$. We define $te_{i,j}$ as the $n \times n$ matrix with t in the (i, j) position, and zero everywhere else. We simply use $e_{i,j}$ to denote $1e_{i,j}$. We often use the well-known matrix identity $e_{i,j}e_{k,l} = \delta_{j,k}e_{i,l}$, where $\delta_{j,k}$ is the Kronecker delta. For more details on elementary matrices see [Ca1].

Example 3.2.1. Elementary matrices (or elementary transvections) in $SL(n, k)$ are $x_{ij}(t) := I + te_{ij}$, where $t \in k; 1 \leq i \neq j \leq n$.

3.2.1 Elementary matrices for $GSp(2l, k)$ $(l \geq 2)$

We index rows and columns by $1, \ldots, l, -1, \ldots, -l$. The elementary matrices are as follows:

$$\begin{aligned}
x_{i,j}(t) = &\quad I + t(e_{i,j} - e_{-j,-i}) \quad \text{for } i \neq j, \\
x_{i,-j}(t) = &\quad I + t(e_{i,-j} + e_{j,-i}) \quad \text{for } i < j, \\
x_{-i,j}(t) = &\quad I + t(e_{-i,j} + e_{-j,i}) \quad \text{for } i < j, \\
x_{i,-i}(t) = &\quad I + te_{i,-i}, \\
x_{-i,i}(t) = &\quad I + te_{-i,i},
\end{aligned}$$

and in matrix format they look as follows:

$$E1 : \begin{pmatrix} R & 0 \\ 0 & {}^tR^{-1} \end{pmatrix}, \text{where } R = I + te_{i,j}; i \neq j,$$

$$E2 : \begin{pmatrix} I & R \\ 0 & I \end{pmatrix}, \text{where } R = t(e_{i,j} + e_{j,i}); \text{for } i < j \text{ or } te_{i,i},$$

$$E3 : \begin{pmatrix} I & 0 \\ R & I \end{pmatrix}, \text{where } R = t(e_{i,j} + e_{j,i}); \text{for } i < j \text{ or } te_{i,i}.$$

3.2.2 Elementary matrices for $GO(2l, k)$ $(l \geq 2)$

We index rows and columns by $1, \dots, l, -1, \dots, -l$. The elementary matrices are as follows:

$$\begin{aligned}
x_{i,j}(t) &= \quad I + t(e_{i,j} - e_{-j,-i}) \qquad \text{for } i \neq j, \\
x_{i,-j}(t) &= \quad I + t(e_{i,-j} - e_{j,-i}) \qquad \text{for } i < j, \\
x_{-i,j}(t) &= \quad I + t(e_{-i,j} - e_{-j,i}) \qquad \text{for } i < j, \\
w_l &= I - e_{l,l} - e_{-l,-l} - e_{l,-l} - e_{-l,l},
\end{aligned}$$

and in matrix format they look as follows:

$$\begin{aligned}
E1 &: \begin{pmatrix} R & 0 \\ 0 & {}^tR^{-1} \end{pmatrix}, \text{where } R = I + te_{i,j}; i \neq j, \\
E2 &: \begin{pmatrix} I & R \\ 0 & I \end{pmatrix}, \text{where } R = t(e_{i,j} - e_{j,i}); \text{for } i < j, \\
E3 &: \begin{pmatrix} I & 0 \\ R & I \end{pmatrix}, \text{where } R = t(e_{i,j} - e_{j,i}); \text{for } i < j.
\end{aligned}$$

3.2.3 Elementary matrices for $GO(2l + 1, k)$ $(l \geq 2)$

We index rows and columns by $0, 1, \dots, l, -1, \dots, -l$. The elementary matrices are as follows:

$$\begin{aligned}
x_{i,j}(t) &= \quad I + t(e_{i,j} - e_{-j,-i}) \qquad \text{for } i \neq j, \\
x_{i,-j}(t) &= \quad I + t(e_{i,-j} - e_{j,-i}) \qquad \text{for } i < j, \\
x_{-i,j}(t) &= \quad I + t(e_{-i,j} - e_{-j,i}) \qquad \text{for } i < j, \\
x_{i,0}(t) &= I + t(2e_{i,0} - e_{0,-i}) - t^2 e_{i,-i}, \\
x_{0,i}(t) &= I + t(-2e_{-i,0} + e_{0,i}) - t^2 e_{-i,i},
\end{aligned}$$

$$w_l = \quad I - e_{l,l} - e_{-l,-l} - e_{l,-l} - e_{-l,l},$$

and in matrix format they look as follows:

$$E1 : \begin{pmatrix} 1 & 0 & 0 \\ 0 & R & 0 \\ 0 & 0 & {}^tR^{-1} \end{pmatrix}, \text{where } R = I + te_{i,j}; i \neq j,$$

$$E2 : \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & R \\ 0 & 0 & I \end{pmatrix}, \text{where } R = t(e_{i,j} - e_{j,i}); \text{for } i < j,$$

$$E3 : \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & 0 \\ 0 & R & I \end{pmatrix}, \text{where } R = t(e_{i,j} - e_{j,i}); \text{for } i < j,$$

$$E4a : \begin{pmatrix} 1 & 0 & -R \\ 2R & I & -{}^tRR \\ 0 & 0 & I \end{pmatrix}, \text{where } R = te_i,$$

$$E4b : \begin{pmatrix} 1 & R & 0 \\ 0 & I & 0 \\ -2R & -{}^tRR & I \end{pmatrix}, \text{where } R = te_i.$$

Here e_i is the row vector with 1 at i^{th} place and zero elsewhere.

In [Re], Ree proved that the above defined elementary matrices generate the symplectic group $Sp(2l, k)$ and the commutator subgroups of the orthogonal groups $O(2l, k)$ and $O(2l + 1, k)$ respectively. We will give an algorithmic proof of this fact via our Gaussian elimination algorithm (see Theorem 6.3.11).

Chapter 4

Conjugacy Classes of an Isometry

G. E. Wall [Wa2], and Springer-Steinberg [SS] classified isometries up to conjugacy. They associated certain forms to an isometry. In this chapter, we define those forms associated with an element in the isometry group. In Section 4.1 we describe the Wall's form, which is associated with an orthogonal element, which will be used in Chapter 7 to compute the spinor norm. In Section 4.2, we describe the other form associated to an element of the unitary group, which will be used in Chapter 8 to prove the finiteness of z-classes in unitary group. The material in this chapter is based on the work of Wall and Springer-Steinberg, and is presented here for the sake of completeness.

4.1 Wall's Form

In [Wa2], Wall classified conjugacy classes in classical groups by associating a bilinear form and thus reducing the problem of conjugacy to the equivalence of bilinear forms. Let $g \in O(n,k)$ and define the *residual space* of g by $V_g := (1_V - g)(V)$, where 1_V denotes the identity linear map on V.

Definition 4.1.1. An element $g \in O(n,k)$ is said to be *regular* if the residual space V_g is non-degenerate.

Example 4.1.2. The reflection $\sigma_u \in O(n,k)$ is an example of a regular element, as $V_{\sigma_u} = \langle u \rangle$, which is non-degenerate.

If $g \in O(n,k)$ then we have,

$$B((1_V - g)x, y) + B(x, (1_V - g)y) = B((1_V - g)x, (1_V - g)y) \qquad (4.1)$$

for all $x, y \in V$. This defines a map

$$[,]_g : V_g \times V_g \to k \text{ by } [u,v]_g := B(u,y)$$

for all $u, v \in V_g$, where $v = (1_V - g)(y)$ for some $y \in V$. Thus to $g \in O(n,k)$ we associate $(V_g, [,]_g)$, called *Wall's form*. We have (see p.6 [Wa2]):

Proposition 4.1.3. *The map $[,]_g$ is a well-defined non-degenerate bilinear form on V_g, and g is an isometry on V_g with respect to $[,]_g$. Furthermore, we have*

1. $[u,v]_g + [v,u]_g = B(u,v)$,
2. $[u,v]_g = -[v,gu]_g$

for all $u, v \in V_g$.

Proof. Let $u = (1_V - g)x = (1_V - g)x_1$ and $v = (1_V - g)y = (1_V - g)y_1$ be in V_g for some $x, y, x_1, y_1 \in V$. Then we have

$$\begin{aligned} B((1_V - g)x, y) &= B((1_V - g)x_1, y) \\ &= B((1_V - g)x_1, (1_V - g)y) - B(x_1, (1_V - g)y) && \text{(by (4.1))} \\ &= B((1_V - g)x_1, (1_V - g)y_1) - B(x_1, (1_V - g)y_1) \\ &= B((1_v - g)x_1, y_1) && \text{(by (4.1)).} \end{aligned}$$

So the map $[,]_g$ is well-defined. Let $u \in V_g$, and if $[u,v]_g = 0$ for all $v \in V_g$, then $B(u,y) = 0$ for all $y \in V$, which implies $u = 0$, as B is nondegenerate. Hence $[,]_g$ is nondegenerate. It follows immediately that $[,]_g$ is a bilinear form on V_g, as B is so. Now $[g|_{V_g}u, g|_{V_g}v] = [g|_{V_g}u, g|_{V_g}(1_V - g)y] = B(g|_{V_g}u, g|_{V_g}y) = B(u,y) = [u,(1_V - g)y]_g = [u,v]_g$. Hence g is an isometry on V_g with respect to the new form $[,]_g$. Furthermore, let $u, v \in V_g$ then $u = (1_V - g)x$ and $v = (1_V - g)y$ for some $x, y \in V$. We have

$$\begin{aligned} B(u,v) &= B(x - gx, y - gy) \\ &= B(x,y) - B(x,gy) + B(x,y) - B(gx,y) \\ &= B(x,(1_V - g)y) + B((1_V - g)x, y) \\ &= B(v,x) + B(u,y) \\ &= [v,(1_V - g)x]_g + [u,(1_V - g)y]_g \\ &= [v,u]_g + [u,v]_g. \end{aligned}$$

Hence $[u,v]_g + [v,u]_g = B(u,v)$, which proves (1). Now we have

$$\begin{aligned} [(1_V - g)x, (1_V - g)y]_g &= B((1_V - g)x, y) \\ &= -B((1_V - g)y, gx) \\ &= -[(1_V - g)y, (1_V - g)gx]_g. \end{aligned}$$

Therefore $[u,v]_g = -[v,gu]_g$, proving (2). Hence the Proposition. □

We have seen that the Wall's form $[,]_g$ is always non-degenerate, but need not be symmetric. Here we give a criterion for the Wall's form $[,]_g$ to be symmetric. We have (see p.116 [Ha]):

Proposition 4.1.4. *The Wall's form $[,]_g$ is symmetric if and only if $g^2 = Id$.*

Proof. Suppose $[,]_g$ is symmetric, then $[u,v]_g = [v,u]_g$ for all $u, v \in V_g$.

Then by part 2 of the Proposition 4.1.3, we have $-[v, gu]_g = [v, u]_g$. So $[v, (1_V + g)u]_g = 0$ for all $u, v \in V_g$, which implies that $(1_V + g)(1_V - g)x = 0$ for all $x \in V$, where $u = (1_V - g)x$. Hence $g^2 = Id$.

Conversely, suppose that $g^2 = Id$, then we have

$$\begin{aligned}
[u, v]_g &= -[v, gu]_g && \text{(by (2) of Proposition 4.1.3)} \\
&= -[v, g(1_V - g)x]_g && \text{(where } u = (1_V - g)x \text{ for some } x \in V) \\
&= -B(v, gx) \\
&= -B(gv, x) && \text{(since } g^2 = Id) \\
&= -B(g(1_V - g)y, x) && \text{(where } v = (1_V - g)y \text{ for some } y \in V) \\
&= B((1_V - g)y, x) && \text{(since } g^2 = Id) \\
&= [(1_v - g)y, (1_V - g)x]_g \\
&= [v, u]_g.
\end{aligned}$$

Therefore the form $[,]_g$ is symmetric. $\square$

Wall developed this to classify the conjugacy class of g. We have (see Theorem 1.3.1 [Wa2]):

Proposition 4.1.5. *Let $g, h \in O(n, k)$. Then g is conjugate to h in $O(n, k)$ if and only if $(V_g, [,]_g) \approx (V_h, [,]_h)$.*

Now the residual space V_g is equipped with two bilinear forms:

1. The Wall's form $(V_g, [,]_g)$, for this we use the notation V_g.

2. Restriction of the usual form B on V_g is, denoted by (V_g, B).

4.1.1 Spinor norm using Wall's theory

We will now define the spinor norm using Wall's theory, which will be useful for our purpose.

Definition 4.1.6. The *spinor norm* is a group homomorphism $\Theta_W : O(n,k) \to k^\times/k^{\times 2}$ defined by $\Theta_W(g) = (dV_g)k^{\times 2}$, where V_g is defined as above.

Let σ_u be a reflection in $O(n,k)$. Then the residual space is $V_{\sigma_u} = \langle u \rangle$, therefore $dV_{\sigma_u} = \det([u,u]_{\sigma_u}) = Q(u)$. Hence $\Theta_W(\sigma_u) = Q(u)k^{\times 2}$, which is same as the spinor norm computed in Section 2.2.3. The following Proposition and its Corollary are due to A. J. Hahn [Ha]. We include the proof for the sake of completeness.

Proposition 4.1.7. *Let $g \in O(n,k)$ be regular with residual space V_g. Then $\Theta_W(g) = (\det(1_V - g)|_{V_g})(d(V_g, B))k^{\times 2}$.*

Proof. If $V_g = \{0\}$, then $\det((1_V - g)|_{V_g}) = 1$, since $\det(g|_{\{0\}}) = 1$, for any $g \in \mathrm{Hom}_k(V,V)$ and $dV_g = k^{\times 2}$. Hence, in this case the result follows immediately. Suppose now $V_g \neq \{0\}$. Since g is regular, $V_g \cap V_g^\perp = \{0\}$, and $\ker(1_V - g) = V_g^\perp$. So $\ker(1_V - g)|_{V_g} = V_g \cap \ker(1_V - g) = V_g \cap V_g^\perp = \{0\}$. Hence $(1_V - g)|_{V_g} \in GL(V_g)$. Therefore $[u,v]_g = B(u, (1_V - g)|_{V_g}^{-1} v)$ for all $u, v \in V_g$. Fix any basis for V_g, say $\{e_1, e_2, \ldots, e_r\}$. Let M, N be the matrices corresponding to the forms $[,]_g$ and B respectively, and let T be the matrix corresponding to the linear transformation $(1_V - g)|_{V_g}$ with respect to the above mentioned basis. Then using $[u,v]_g = B(u, (1_V - g)|_{V_g}^{-1} v)$, we get $M = NT^{-1}$. Then $\det M = \det N \det T (\det(T^{-1}))^2$. Therefore $dV_g = d(V_g, B)\det((1_V - g)|_{V_g})(\det(T^{-1}))^2$. Hence $\Theta_W(g) = (\det(1_V - g)|_{V_g})(d(V_g, B))k^{\times 2}$. □

Corollary 4.1.8. *Let $g \in O(n,k)$ be unipotent. Then $\Theta_W(g) = k^{\times 2}$.*

Proof. The fixed space of $-g$ is 0, since -1 is not an eigenvalue of g. Hence, its residual space $V_{-g} = V$, which is non-degenerate. Hence $-g$ is regular. As g is unipotent, there is a basis for V such that the matrix of g is upper triangular with diagonal entries equal to 1. Therefore by Proposition 4.1.7 we have, $\Theta_W(-g) = (2^n dV)k^{\times 2}$. Again -1_V has no fixed points (except 0), hence -1_V is regular with residual space V. Therefore $\Theta_W(-1_V) = (2^n)(dV)k^{\times 2}$. Hence $\Theta_W(g) = \Theta_W(-g)\Theta_W(-1_V) = (2^n dV)(2^n dV)k^{\times 2} = k^{\times 2}$. $\square$

4.2 Springer-Steinberg Form

Let us fix some notation and terminology. Let k be a perfect field of char $k \neq 2$ with an involution σ such that the fixed field of σ is k_0. Let V be a vector space over k, equipped with a non-degenerate hermitian form B. Let $T \in U(V, B)$ with minimal polynomial $f(x)$. We define a k-algebra $E^T := \frac{k[x]}{<f(x)>}$. Clearly, V is an E^T-module, denoted by V^T. The E^T-module structure on V^T determines $GL(n)$-conjugacy class of T. To determine conjugacy classes of T within $U(V, B)$, Springer and Steinberg defined a hermitian form H^T on V^T, called *Springer-Steinberg form*, denoted by (H^T, V^T) (see 2.6 in [SS] Chapter IV). Since $f(x)$ is self-U-reciprocal (see 5.1 for definition), there exists a unique involution α on E^T such that $\alpha(x) = x^{-1}$ and α is an extension of σ on scalars. Thus (E^T, α) is an algebra with involution. They prove that there exists a k-linear function $l^T \colon E^T \to k$ such that the symmetric bilinear form $\bar{l^T} \colon E^T \times E^T \to k$ given by $\bar{l^T}(a, b) := l^T(ab)$ is non-degenerate with $l^T(\alpha(e)) = l^T(e)$ for all $e \in E^T$. Furthermore the hermitian form H^T on E^T-module V^T (with respect to α) satisfies $B(eu, v) = l^T(eH^T(u, v))$ for all $e \in E^T$, and $u, v \in V^T$. Let $S, T \in U(V, B)$, then the following commutative diagrams clarify what we are talking about so far, which will also be useful in the following proposition (Proposition 4.2.2).

$$\begin{tikzcd} V^S \times V^S \arrow[r, "H^S"] \arrow[dr, "B"'] & E^S \arrow[d, "l^S"] \\ & k \end{tikzcd} \quad \begin{tikzcd} V^T \times V^T \arrow[r, "H^T"] \arrow[dr, "B"'] & E^T \arrow[d, "l^T"] \\ & k \end{tikzcd} \quad \begin{tikzcd} E^S \arrow[r, "f"] \arrow[dr, "l^S"'] & E^T \arrow[d, "l^T"] \\ & k \end{tikzcd}$$

Definition 4.2.1. Let (V_1, H_1) and (V_2, H_2) be two hermitian spaces over E_1 and E_2 respectively, where E_1 and E_2 are isomorphic modules over k and let $f\colon E_1 \to E_2$ be an isomorphism. Then we say (V_1, H_1) and (V_2, H_2) are *equivalent*, denoted as $(V_1, H_1) \approx (V_2, H_2)$, if there exists a k-isomorphism $\varphi\colon V_1 \to V_2$ such that

1. $\varphi(ev) = f(e)\varphi(v)$ and
2. $H_2(\varphi(u), \varphi(v)) = f(H_1(u, v))$

for all $u, v \in V_1$ and all $e \in E_1$.

We need the following (see 2.7 and 2.8 [SS] Chapter IV):

Proposition 4.2.2. *With the notation as above, let S and $T \in U(V, B)$. Then,*

1. *the elements S and T are conjugate in $U(V, B)$ if and only if (V^S, H^S) and (V^T, H^T) are equivalent.*
2. *The centralizer of T in $U(V, B)$ is $\mathcal{Z}_{U(V,B)}(T) = U(V^T, H^T)$.*

Proof. 1. Suppose S and T are conjugate in $U(V, B)$. Then there exists a $\varphi \in U(V, B)$ such that $T = \varphi S \varphi^{-1}$. Then $\varphi : V^S \to V^T$ is a k-isomorphism. Here also $f : E^S \to E^T$ is a k-isomorphism such that $f(S) = T$. Now for $v \in V^S$, $\varphi(S^m v) = \varphi \circ S^m(v) = T^m \circ \varphi(v) = f(S^m)\varphi(v)$. It then follows that $\varphi(ev) = f(e)\varphi(v)$ for all $e \in E^S$ and for all $v \in V^S$. Let $u, v \in V^S$, then $l^S(f^{-1}(H^T(\varphi u, \varphi v))) = l^T(H^T(\varphi u, \varphi v)) = B(\varphi u, \varphi v) = B(u, v) = l^S(H^S(u, v))$. Therefore $H^T(\varphi u, \varphi v) = f(H^S(u, v))$. Hence $(V^S, H^S) \approx (V^T, H^T)$.

Conversely, suppose that (V^S, H^S) and (V^T, H^T) are equivalent. Then there exists a k-isomorphism $\varphi : V^S \to V^T$ such that $H^T(\varphi u, \varphi v) = f(H^S(u, v))$ for all $u, v \in V^S$, where $f : E^S \to E^T$ is a k-isomorphism such that $f(S) = T$ and $\varphi(Sv) = f(S)\varphi(v)$ for all $v \in V^S$ and $S \in E^S$. For $v \in V^S$, $\varphi S(v) = \varphi(Sv) = f(S)\varphi(v) = T\varphi(v) = (T\varphi)(v)$, then $\varphi S = T\varphi$, i.e., $\varphi S \varphi^{-1} = T$. Now, look at $B(\varphi u, \varphi v) = l^T(H^T(\varphi u, \varphi v)) = l^T(f(H^S(u,v))) = l^S(H^S(u,v)) = B(u,v)$ for all $u, v \in V$, then φ is an isometry. Hence S and T are conjugate in $U(V,B)$.

2. Enough to show an isometry φ is in $\mathcal{Z}_{U(V,B)}(T)$ if and only if φ preserves H^T. Let $\varphi \in U(V,B)$ such that $\varphi T = T\varphi$. Then we get $H^T(\varphi u, \varphi v) = H^T(u,v)$ for all $u, v \in V^T$ (here we replace S by T and f by identity in part (1)). Conversely, suppose φ preserves H^T, then $B(\varphi u, \varphi v) = l^T(H^T(\varphi u, \varphi v)) = l^T(H^T(u,v)) = B(u,v)$. So φ is an isometry. Also as $\varphi T(v) = T\varphi(v)$ for all $v \in V$, then $\varphi T = T\varphi$. Therefore $\varphi \in \mathcal{Z}_{U(V,B)}(T)$. Hence $\mathcal{Z}_{U(V,B)}(T) = U(V^T, H^T)$.

□

We can decompose $E^T = E_1 \oplus E_2 \oplus \cdots \oplus E_r$, where E_i are indecomposable with respect to α (see section 2.2 Chapter IV of [SS]). The restriction of α to E_i is an involution on E_i denoted by α_i. Clearly, E_i's, are of one of the following forms according to the decomposition of $f(x)$ (see Equation (5.1)):

- $\frac{k[x]}{<p(x)^d>}$, where $p(x)$ is an irreducible self-U-reciprocal polynomial.

- $\frac{k[x]}{<q(x)^d>} \oplus \frac{k[x]}{<\tilde{q}(x)^d>}$, where $q(x)$ is irreducible and not self-U-reciprocal.

In the second case, the two components $\frac{k[x]}{<q(x)^d>)}$ and $\frac{k[x]}{<\tilde{q}(x)^d>}$ are isomorphic local rings, and the restriction of α is given by $\alpha(a,b) = (b,a)$ via the isomorphism. Using Wall's approximation theorem (Corollary 4.2.4) it's easy to see that all hermitian forms over such rings are equivalent. Thus to determine equivalence of H^T, we need to look at modules over rings of the first kind.

4.2.1 Wall's approximation theorem

We recall a theorem of Wall (see Theorem 2.2.1 [Wa2]), which will be useful for further analysis. Also, see Asai (Proposition 2.5 [As]) for more details. Let R be a commutative ring with 1, $\mathfrak{J}$ be its Jacobson radical, and α be an involution on R. Let (V, B) be a non-degenerate hermitian space of rank n over R. We define $\underline{V} := \frac{V}{\mathfrak{J}V}$ a module over $\underline{R} := \frac{R}{\mathfrak{J}}$. Now B induces a hermitian form $\underline{B}$ on $\underline{V}$ with respect to the involution $\underline{\alpha}$ of $\underline{R}$ induced by α. Then we have (Theorem 2.2.1 [Wa2]):

Theorem 4.2.3 (Wall's approximation theorem)**.** *With the notation as above,*

1. *any non-degenerate hermitian form over $\underline{R}$ is induced by some non-degenerate hermitian form over R.*

2. *Let (V_1, B_1) and (V_2, B_2) be non-degenerate hermitian spaces over R, and correspondingly, $(\underline{V_1}, \underline{B_1})$ and $(\underline{V_2}, \underline{B_2})$ be non-degenerate hermitian spaces over $\underline{R}$. Then (V_1, B_1) is equivalent to (V_2, B_2) if and only if $(\underline{V_1}, \underline{B_1})$ is equivalent to $(\underline{V_2}, \underline{B_2})$.*

For our purpose, we need the following,

Corollary 4.2.4. *Let V be a module over $R = \frac{k[x]}{<q(x)^d>} \oplus \frac{k[x]}{<\tilde{q}(x)^d>}$, and H_1 and H_2 be two non-degenerate hermitian forms on V with respect to the involution on R given by $\overline{(b, a)} = (a, b)$. Then H_1 and H_2 are equivalent.*

Proof. We use Wall's approximation theorem (Theorem 4.2.3). Here the Jacobson radical of R is $\mathfrak{J} = \frac{<q(x)>}{<q(x)^d>} \oplus \frac{<\tilde{q}(x)>}{<\tilde{q}(x)^d>}$. Then $\underline{R} \cong \frac{k[x]}{<q(x)>} \oplus \frac{k[x]}{<\tilde{q}(x)>} \cong K \oplus K$, where $K \cong \frac{k[x]}{<q(x)>} \cong \frac{k[x]}{<\tilde{q}(x)>}$ is a finite extension of k (thus separable). Now we have hermitian forms $\underline{H_i} \colon \underline{V} \times \underline{V} \to \underline{R}$ defined by $\underline{H_i}(u + \mathfrak{J}V, v + \mathfrak{J}V) = H_i(u, v)\mathfrak{J}$ for all $u, v \in V$. Thus it is enough to show that $\underline{H_1}$ is equivalent to $\underline{H_2}$ on $K \oplus K$-module $\underline{V}$. The norm map $N \colon (K \oplus K)^\times \to K^\times$

is $N(a,b) = \overline{(a,b)}(a,b) = (b,a)(a,b) = (ab,ab)$. Clearly, this norm map is surjective. Thus $\frac{K^\times}{Im(N)}$ is trivial. Hence the hermitian form is unique up to equivalence in this case. $\square$

Chapter 5

Conjugacy Classes and z-classes

The results in this chapter are part of [BS]. To study the z-classes, it is important to understand the conjugacy classes because z-classes are union of conjugacy classes. The problem of classifying conjugacy classes in classical groups has been studied by many mathematicians, and there is a known substantial amount of results. See, for example, Asai, Macdonald, Milnor, Springer-Steinberg, Wall, Williamson [As, Ma, Mi, SS, Wa2, Wi]. When the field is finite, Wall [Wa2] gave an explicit description of all the conjugacy classes in the unitary, symplectic and orthogonal groups, and also the order of centralizers. For some recent accounts in this direction, especially with the applications in mind, see Thiem-Vinroot [TV], and Burness and Giudici [BG] etc. The conjugacy classes in $GL(n,k)$ are given by the canonical form theory, and with the unitary group being its subgroup, one needs to begin there. We begin with recalling the notation involved in the description of conjugacy classes and z-classes. In Section 5.1 we define certain kinds of polynomials, which will be used in Section 5.2 to decompose the space with respect to a unitary linear transformation. This decomposition may be thought of as a reduction step, which will be used in Chapter 8 to prove one of the main theorems of this thesis. In Section 5.3 we describe z-classes in orthogonal and symplectic groups (for more details see [GK]).

5.1 Self-U-reciprocal Polynomials

Let k be a field with an involution given by $\bar{a} = a$ for all $a \in k$. Let $f(x) = \sum_{i=0}^{n} a_i x^i \in k[x]$. We extend the involution on k to that of $k[x]$ by $\overline{f(x)} := \sum_{i=0}^{n} \bar{a}_i x^i$. Let $f(x)$ be a polynomial with $f(0) \neq 0$. The corresponding U-reciprocal polynomial of $f(x)$ is defined by

$$\tilde{f}(x) := \overline{f(0)^{-1}}\; x^n \; \overline{f(x^{-1})}.$$

A monic polynomial $f(x)$ with a non-zero constant term is said to be *self-U-reciprocal* if $f(x) = \tilde{f}(x)$. In terms of roots, it means that for a self-U-reciprocal polynomial, whenever λ is a root, $\bar{\lambda}^{-1}$ is also a root with the same multiplicity. Note that $f(x) = \tilde{\tilde{f}}(x)$, and if $f(x) = f_1(x)f_2(x)$ then $\tilde{f}(x) = \tilde{f}_1(x)\tilde{f}_2(x)$. Also, $f(x)$ is irreducible if and only if $\tilde{f}(x)$ is irreducible. In the case of $f(x) = (x-\lambda)^n$, the polynomial $f(x)$ is self-U-reciprocal if and only if $\lambda\bar{\lambda} = 1$. A slightly more general polynomial, called self-dual polynomial will be defined in Section 5.3. Over a finite field, we have the following result due to Ennola (Lemma 2 [En]):

Proposition 5.1.1. *Let $f(x)$ be a monic, irreducible, self-U-reciprocal polynomial over a finite field $\mathbb{F}_{q^2}$. Then the degree of $f(x)$ is odd.*

Proof. Let $\deg f(x) = n$. Let α be a root of $f(x)$ in its splitting field L over $\mathbb{F}_{q^2}$. Let σ be the Frobenius automorphism of L given by $\sigma(a) = a^{q^2}$. Then $[L : \mathbb{F}_{q^2}] = \deg f(x) = n = \mathrm{order}\,(\sigma)$. Since $f(x)$ is self-U-reciprocal, so if α is a root of $f(x)$, then α^{-q} is also a root of $f(x)$ with the same multiplicity. Therefore there is an automorphism τ of L over $\mathbb{F}_{q^2}$ such that $\tau(\alpha) = \alpha^{-q}$. Then $\tau^2(\alpha) = \alpha^{q^2} = \sigma(\alpha)$, so $\tau^2 = \sigma$ since $L = \mathbb{F}_{q^2}(\alpha)$. Now

$\tau \in \langle\sigma\rangle \cong \mathbb{Z}/n\mathbb{Z} \cong \mathrm{Gal}(L/\mathbb{F}_{q^2})$, so $\tau = \sigma^t$ for some t. Therefore $\sigma = \tau^2 = \sigma^{2t}$, so $\sigma^{2t-1} = 1$. Hence n is a divisor of $2t-1$, so n is odd. $\square$

Lemma 5.1.2. *Let $T \in GL(n,k)$, and suppose $f(x)$ is the minimal polynomial of T. Then the minimal polynomial of $\bar{T}^{-1}$ is $\tilde{f}(x)$.*

Proof. Since $\tilde{f}(x) = \overline{f(0)}^{-1} x^d \overline{f(x^{-1})}$, and $f(T) = 0$, then $\tilde{f}(\bar{T}^{-1}) = \overline{f(0)}^{-1}(\bar{T}^{-1})^d \overline{f((\bar{T}^{-1})^{-1})} = \overline{f(0)}^{-1}\bar{T}^{-d}\overline{f(\bar{\bar{T}})} = \overline{f(0)}^{-1}\bar{T}^{-d}\overline{f(T)} = 0$. Thus we conclude that $\tilde{f}(x)$ is the minimal polynomial of $\bar{T}^{-1}$. $\square$

Remark 5.1.3. If $g \in U(V,B)$, then ${}^t\bar{g}\beta g = \beta$. So $\beta g \beta^{-1} = {}^t\bar{g}^{-1}$, which is conjugate to $\bar{g}^{-1}$, as g is conjugate to its transpose in $GL(n,k)$. Hence the minimal polynomials of g and $\bar{g}^{-1}$ are same, i.e., $f(x) = \tilde{f}(x)$.

If $T \in U(V,B)$ then its minimal polynomial $f(x)$ is monic with a non zero constant term, and is self-U-reciprocal. We can write it as follows:

$$f(x) = \prod_{i=1}^{k_1} p_i(x)^{r_i} \prod_{j=1}^{k_2} (q_j(x)\tilde{q_j}(x))^{s_j}, \tag{5.1}$$

where $p_i(x)$ and $q_j(x)$ are irreducible, and $p_i(x)$ is self-U-reciprocal but $q_j(x)$ is not self-U-reciprocal for all i,j.

5.2 Space Decomposition with Respect to a Unitary Transformation

Let $T \in U(V,B)$, and $f(x) \in k[x]$ satisfying $f(0) \neq 0$. Then,

Lemma 5.2.1. *For any $u, v \in V$, we have $B(u, f(T)v) = B(\overline{f(T^{-1})}u, v)$.*

Proof. Let $f(x) = \sum_{i=0}^{n} a_i x^i$, then $f(T) = \sum_{i=0}^{n} a_i T^i$. Observe that $B(T^{-1}u, v) = B(u, Tv)$ for all $u, v \in V$. Now $B(u, \sum_{i=0}^{n} a_i T^i v) = \sum_{i=0}^{n} a_i B(u, T^i v) =$

$\sum_{i=0}^{n} a_i B(T^{-i}u, v) = B(\sum_{i=0}^{n} \bar{a}_i T^{-i}u, v)$ for all $u, v \in V$. Hence $B(u, f(T)v) = B(\overline{f(T^{-1})}u, v)$. □

Lemma 5.2.2. *The subspaces* $\mathrm{Im}(f(T))$ *and* $\ker(\tilde{f}(T))$ *are mutually orthogonal.*

Proof. Let $u \in \ker(\tilde{f}(T))$ and $v \in \mathrm{Im}(f(T))$, therefore $\tilde{f}(T)u = 0$ and $v = f(T)w$ for some $w \in V$. Now $B(u, v) = B(u, f(T)w) = B(\overline{f(T^{-1})}u, w) = B(T^d\overline{f(T^{-1})}u, T^d w) = f(0)B(\overline{f(0)}^{-1}T^d\overline{f(T^{-1})}u, T^d w) = f(0)B(\tilde{f}(T)u, T^d w) = f(0)B(0, T^d w) = 0$. Hence $\mathrm{Im}(f(T)) \perp \ker(\tilde{f}(T))$. □

Let $T \in U(V, B)$ with minimal polynomial $f(x)$. Write $f(x) = \prod_i f_i(x)^{m_i}$ as in Equation (5.1), where $f_i(x) = p_i(x)$ or $q_i(x)\tilde{q}_i(x)$. Then,

Proposition 5.2.3. *The direct sum decomposition* $V = \bigoplus_i \ker(f_i(T)^{m_i})$ *is a decomposition into non-degenerate mutually orthogonal T-invariant subspaces.*

Proof. Since $f_i(x)^{m_i}$ are pairwise relatively prime, then the sum $V = \bigoplus_i \ker(f_i(T)^{m_i})$ is a direct sum. Clearly, these subspaces are T-invariant. Observe that $\mathrm{Im}(f_j(T)^{m_j}) = \bigoplus_{i \neq j} \ker(f_i(T)^{m_i})$, and $\ker(f_i(T)^{m_i}) = \ker(\tilde{f}_i(T)^{m_i})$, since $f_i(x) = \tilde{f}_i(x)$ for all i. By Lemma 5.2.2, we have $\mathrm{Im}(f_j(T)^{m_j}) \perp \ker(\tilde{f}_j(T)^{m_j})$. So we get $\bigoplus_{i \neq j} \ker(f_i(T)^{m_i}) \perp \ker(f_j(T)^{m_j})$ for all j. Hence in the sum $V = \bigoplus_i \ker(f_i(T)^{m_i})$, the subspaces are mutually orthogonal. Also mutual orthogonality implies that the restriction of the form on each subspaces are non-degenerate. □

This decomposition helps us reduce the questions about conjugacy classes and z-classes of a unitary transformation to the unitary transformations with minimal polynomial of one of the following two kinds:

Type 1. $p(x)^m$, where $p(x)$ is monic irreducible self-U-reciprocal polynomial with a non-zero constant term,

Type 2. $(q(x)\tilde{q}(x))^m$, where $q(x)$ is monic, irreducible, not self-U-reciprocal with a non-zero constant term.

Thus Proposition 5.2.3 gives us a *primary decomposition* of V into T-invariant B non-degenerate subspaces

$$V = \left(\bigoplus_{i=1}^{k_1} V_i\right) \bigoplus \left(\bigoplus_{j=1}^{k_2} V_j\right), \tag{5.2}$$

where $V_i = \ker(p_i(T)^{r_i})$ corresponds to the polynomials of Type 1, and $V_j = W_j + W_j^*$ corresponds to the polynomials of Type 2, where $W_j = \ker(q_j(T)^{s_j})$ and $W_j^* = \ker(\tilde{q}_j(T)^{s_j})$. Denote the restriction of T to each V_r by T_r. Then the minimal polynomial of T_r is one of the two types. It turns out that the centralizer of T in $U(V,B)$ is

$$\mathcal{Z}_{U(V,B)}(T) = \prod_r \mathcal{Z}_{U(V_r,B_r)}(T_r),$$

where B_r is a hermitian form obtained by restricting B to V_r. Thus the conjugacy class and the z-class of T is determined by the restriction of T to each of the primary subspaces. Hence it is enough to determine the conjugacy class and the z-class of $T \in U(V,B)$, which has the minimal polynomial of one of the types in 5.2.

5.3 z-classes in Orthogonal and Symplectic Groups

Let V be an n-dimensional vector space over k with the property FE, equipped with a non-degenerate symmetric or skew-symmetric bilinear form

B. The z-classes of orthogonal groups $O(V, B)$ and symplectic groups $Sp(V, B)$ have been discussed by Gongopadhyay and Ravi S. Kulkarni in [GK] (see Theorem 1.0.7). We will be very brief in this section to parametrize the z-classes in orthogonal and symplectic groups. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial in $k[x]$ of degree n such that $0, 1$ and -1 are not its roots. The corresponding dual polynomial of $f(x)$ is defined by

$$f^*(x) := f(0)^{-1} x^n f(x^{-1}).$$

A monic polynomial $f(x)$ with $0, 1, -1$ are not its roots is said to be *self-dual* if $f(x) = f^*(x)$. In terms of roots, it means that for a self-dual polynomial, whenever λ is a root, λ^{-1} is also a root with the same multiplicity. Suppose $T \in O(V, B)$ or $Sp(V, B)$ with the minimal polynomial $m_T(x)$. Thus an irreducible factor says $p(x)$, of the minimal polynomial, can be one of the following three types:

- $x + 1$ or $x - 1$.
- $p(x)$ is self-dual.
- $p(x)$ is not self-dual. In this case, there is an irreducible factor $p^*(x)$ will occur in the minimal polynomial.

If $T \in O(V, B)$ or $Sp(V, B)$ then its minimal polynomial $m_T(x)$ is monic with a non-zero constant term, and is self-dual. We can write it as follows

$$m_T(x) = (x+1)^e (x-1)^f \prod_{i=1}^{k_1} p_i(x)^{r_i} \prod_{j=1}^{k_2} (q_j(x) q_j^*(x))^{s_j}, \tag{5.3}$$

where $p_i(x)$ and $q_j(x)$ are irreducible, and $p_i(x)$ is self-dual but $q_j(x)$ is not self-dual for all i, j. Thus Proposition 5.2.3 gives us a *primary decomposition* of V into T-invariant B non-degenerate subspaces

$$V = \left(V_1 \bigoplus V_{-1}\right) \bigoplus \left(\bigoplus_{i=1}^{k_1} V_i\right) \bigoplus \left(\bigoplus_{j=1}^{k_2} V_j\right), \tag{5.4}$$

where $V_{-1} = \ker(T+I)^e, V_1 = \ker(T-I)^f$, and $V_i = \ker(p_i(T)^{r_i})$ corresponds to the self-dual polynomials, and $V_j = W_j + W_j^*$ corresponds to the not self-dual polynomials, where $W_j = \ker(q_j(T)^{s_j})$ and $W_j^* = \ker(q_j^*(T)^{s_j})$. Denote the restriction of T to each V_r by T_r so $T = \bigoplus_r T_r$. Then the minimal polynomial of T_r is one of the three types. It turns out that the centralizer of T in $O(V,B)$ or $Sp(V,B)$ is

$$\mathcal{Z}(T) = \prod_r \mathcal{Z}(T_r).$$

Thus the z-class of T is determined by the restriction of T to each of the primary subspaces. Then it has been proved that there are only finitely many z-classes of semisimple and unipotent elements in orthogonal and symplectic groups respectively. Thus using Jordan decomposition (Theorem 2.1.1), there are only finitely many z-classes in orthogonal groups $O(V,B)$ and symplectic groups $Sp(V,B)$.

Chapter 6

Gaussian Elimination

The results in this chapter are part of [BMS]. We improved the results on the symplectic and split orthogonal similitude groups. This chapter is one of the main chapters of this thesis. For instance, in Chapter 7 we use Gaussian elimination to compute the spinor norm as well as similitude characters. In dealing with constructive group recognition project, one needs to solve the word problem in some generating set. Thus, the main objective of this chapter is to develop a similar algorithm for symplectic and split orthogonal similitude groups to solve the word problem. In Section 6.1 we describe the classical Gaussian elimination algorithm for general linear groups. In Section 6.2 we define elementary operations for similitude groups, and describe the Gaussian elimination in similitude groups in Section 6.3. In Section 6.4 we record a result [MS] on the Gaussian elimination in the split unitary groups.

6.1 Gaussian Elimination in General Linear Groups

As we know, in the general linear group $GL(n, k)$, the word problem has an efficient solution in elementary transvections (or elementary matrices) - the

Gaussian elimination. One observes that the effect of multiplying by elementary transvections on a matrix from left or right is either a row or column operation respectively. We have the following classical Gaussian elimination algorithm for $GL(n,k)$:

Theorem 6.1.1. *Every element $g \in GL(n,k)$ can be written as a product of elementary transvections (or elementary matrices) and a diagonal matrix, the diagonal matrix is of the form* $\mathrm{diag}(1,\ldots,1,\det(g))$.

Using the above Theorem 6.1.1 one can solve the word problem in $SL(n,k)$, which can be stated as follows:

Corollary 6.1.2. *Every element of the special linear group $SL(n,k)$ can be written as a product of elementary transvections (or elementary matrices).*

Let B be a subgroup of upper triangular matrices and W be the subgroup of permutation matrices in $GL(n,k)$ respectively. In this case $W \cong S_n$, symmetric group on n letters. Then we have the following (see p.108 [Ca1]):

Theorem 6.1.3 (Bruhat decomposition). *With the notation as above,*

$$GL(n,k) = BWB = \bigsqcup_{w \in W} BwB.$$

So the above Theorem 6.1.3 says that any element $g \in GL(n,k)$ can be written as $g = b_1 w b_2$ for some $b_1, b_2 \in B$, and $w \in W$ (which is unique). Therefore $w = b_1^{-1} g b_2^{-1}$. Thus, any invertible matrix can be transformed into a permutation matrix by a series of row and column operations.

6.2 Elementary Operations

Elementary operations can be thought of as usual row-column operations for matrices. We already described the elementary matrices in Section 3.2 for the symplectic and split orthogonal similitude groups. Then multiplications of those elementary matrices on the left and right to an element of the similitude groups, for example, symplectic and split orthogonal similitude groups, are elementary operations, which we are going to describe below case by case. The Gaussian elimination algorithm is slightly different for matrices of even and odd size. We first describe it for matrices of even size and then for matrices of the odd size.

6.2.1 Elementary operations for $GSp(2l, k)$ $(l \geq 2)$

Let $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be a $2l \times 2l$ matrix written in block form of size $l \times l$. Then the row and column operations are as follows:

$$ER1: \quad \begin{pmatrix} R & 0 \\ 0 & {}^tR^{-1} \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} RA & RB \\ {}^tR^{-1}C & {}^tR^{-1}D \end{pmatrix}$$

$$EC1: \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} R & 0 \\ 0 & {}^tR^{-1} \end{pmatrix} = \begin{pmatrix} AR & B{}^tR^{-1} \\ CR & D{}^tR^{-1} \end{pmatrix}$$

$$ER2: \quad \begin{pmatrix} I & R \\ 0 & I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A + RC & B + RD \\ C & D \end{pmatrix}$$

$$EC2: \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & R \\ 0 & I \end{pmatrix} = \begin{pmatrix} A & AR + B \\ C & CR + D \end{pmatrix}$$

$$ER3: \quad \begin{pmatrix} I & 0 \\ R & I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ RA + C & RB + D \end{pmatrix}$$

$$EC3: \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & 0 \\ R & I \end{pmatrix} = \begin{pmatrix} A + BR & B \\ C + DR & D \end{pmatrix}.$$

6.2.2 Elementary operations for $GO(2l, k)$ $(l \geq 2)$

Let $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be a $2l \times 2l$ matrix written in block form of size $l \times l$. Then the row and column operations are as follows:

$$ER1: \begin{pmatrix} R & 0 \\ 0 & {}^tR^{-1} \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} RA & RB \\ {}^tR^{-1}C & {}^tR^{-1}D \end{pmatrix}$$

$$EC1: \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} R & 0 \\ 0 & {}^tR^{-1} \end{pmatrix} = \begin{pmatrix} AR & B{}^tR^{-1} \\ CR & D{}^tR^{-1} \end{pmatrix}$$

$$ER2: \begin{pmatrix} I & R \\ 0 & I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A+RC & B+RD \\ C & D \end{pmatrix}$$

$$EC2: \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & R \\ 0 & I \end{pmatrix} = \begin{pmatrix} A & AR+B \\ C & CR+D \end{pmatrix}$$

$$ER3: \begin{pmatrix} I & 0 \\ R & I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ RA+C & RB+D \end{pmatrix}$$

$$EC3: \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & 0 \\ R & I \end{pmatrix} = \begin{pmatrix} A+BR & B \\ C+DR & D \end{pmatrix}.$$

6.2.3 Elementary operations for $GO(2l+1, k)$ $(l \geq 2)$

Let $g = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix}$ be a $(2l+1)\times(2l+1)$ matrix, where A, B, C, D are $l \times l$ matrices, and $X = (X_1 X_2 \cdots X_l)$ and $Y = (Y_1 Y_2 \cdots Y_l)$ are $1 \times l$ matrices, and $E = {}^t(E_1 E_2 \cdots E_l)$ and $F = {}^t(F_1 F_2 \cdots F_l)$ are $l \times 1$ matrices. Let $\alpha \in k$.

Then the row and column operations are as follows:

$$ER1: \begin{pmatrix} 1 & 0 & 0 \\ 0 & R & 0 \\ 0 & 0 & {}^tR^{-1} \end{pmatrix} \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} = \begin{pmatrix} \alpha & X & Y \\ RE & RA & RB \\ {}^tR^{-1}F & {}^tR^{-1}C & {}^tR^{-1}D \end{pmatrix}$$

$$EC1: \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & R & 0 \\ 0 & 0 & {}^tR^{-1} \end{pmatrix} = \begin{pmatrix} \alpha & XR & Y{}^tR^{-1} \\ E & AR & B{}^tR^{-1} \\ F & CR & D{}^tR^{-1} \end{pmatrix}.$$

$$ER2: \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & R \\ 0 & 0 & I \end{pmatrix} \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} = \begin{pmatrix} \alpha & X & Y \\ E+RF & A+RC & B+RD \\ F & C & D \end{pmatrix}$$

$$EC2: \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & R \\ 0 & 0 & I \end{pmatrix} = \begin{pmatrix} \alpha & X & XR+Y \\ E & A & AR+B \\ F & C & CR+D \end{pmatrix}.$$

$$ER3: \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & 0 \\ 0 & R & I \end{pmatrix} \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ RE+F & RA+C & RB+D \end{pmatrix}$$

$$EC3: \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & 0 \\ 0 & R & I \end{pmatrix} = \begin{pmatrix} \alpha & X+YR & Y \\ E & A+BR & B \\ F & C+DR & D \end{pmatrix}.$$

For $E4$ we only write the equations which we need later.

- Let the matrix g have $C = \mathrm{diag}(d_1, \ldots, d_l)$.

$$ER4: \ [(I + t(2e_{i,0} - e_{0,-i}) - t^2 e_{i,-i})g]_{0,i} = X_i - td_i$$

- Let the matrix g have $A = \mathrm{diag}(d_1, \ldots, d_l)$.

$$ER4: \ [(I + t(-2e_{-i,0} + e_{0,i}) - t^2 e_{-i,i})g]_{0,i} = X_i + td_i$$

$$EC4: \ [g(I + t(2e_{i,0} - e_{0,-i}) - t^2 e_{i,-i})]_{i,0} = E_i + 2td_i,$$

where $1 \le i \le l$.

6.3 Gaussian Elimination in Symplectic and Orthogonal Similitude Groups

6.3.1 Some useful lemmas

To justify the steps of the Gaussian elimination algorithm we need several lemmas. So this subsection is devoted to prove these lemmas.

Lemma 6.3.1. *Let $Y = \mathrm{diag}(1, \ldots, 1, \lambda, \ldots, \lambda)$ be of size l with the number of 1s equal to $m < l$. Let X be a matrix of size l such that YX is symmetric (resp. skew-symmetric) then X is of the form $\begin{pmatrix} X_{11} & \lambda^t X_{21} \\ X_{21} & X_{22} \end{pmatrix}$, where X_{11} is symmetric (resp. skew-symmetric), and $X_{12} = \lambda^t X_{21}$ (resp. $X_{12} = -\lambda^t X_{21}$). Furthermore, if $\lambda \neq 0$ then X_{22} is symmetric (resp. skew-symmetric).*

Proof. First, observe that the matrix $YX = \begin{pmatrix} X_{11} & X_{12} \\ \lambda X_{21} & \lambda X_{22} \end{pmatrix}$. Since the matrix YX is symmetric (resp. skew-symmetric), then X_{11} is symmetric (resp. skew-symmetric), and $X_{12} = \lambda X_{21}$ (resp. $X_{12} = -\lambda X_{21}$). Also if $\lambda \neq 0$ then X_{22} is symmetric (resp. skew-symmetric). $\square$

Corollary 6.3.2. *Let $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be either in $GSp(2l, k)$ or $GO(2l, k)$.*

1. *If A is a diagonal matrix $\mathrm{diag}(1, \ldots, 1, \lambda), \lambda \in k^{\times}$, then the matrix*

C is of the form $\begin{pmatrix} C_{11} & \pm\lambda{}^tC_{21} \\ C_{21} & c_{ll} \end{pmatrix}$*, where C_{11} is an $(l-1)\times(l-1)$ symmetric if $g \in GSp(2l,k)$, and C_{11} is skew-symmetric with $c_{ll}=0$ if $g \in GO(2l,k)$.*

2. *If A is a diagonal matrix* $\mathrm{diag}(\underbrace{1,\ldots,1}_{m},\underbrace{0,\ldots,0}_{l-m})$*, then the matrix C is of the form* $\begin{pmatrix} C_{11} & 0 \\ C_{21} & C_{22} \end{pmatrix}$*, where C_{11} is an $m\times m$ symmetric matrix if $g \in GSp(2l,k)$, and is skew-symmetric if $g \in GO(2l,k)$.*

Proof. We use the condition that g satisfies ${}^tg\beta g = \mu(g)\beta$, and AC is symmetric (using ${}^tA = A$, as A is diagonal), when $g \in GSp(2l,k)$, and AC is skew-symmetric, when $g \in GO(2l,k)$. Then Lemma 6.3.1 gives the required form for C. □

Corollary 6.3.3. *Let $g = \begin{pmatrix} A & B \\ 0 & \mu(g)A^{-1} \end{pmatrix} \in GSp(2l,k)$ or $GO(2l,k)$, where $A = \mathrm{diag}(1,\ldots,1,\lambda)$, then the matrix B is of the form $\begin{pmatrix} B_{11} & \pm\lambda^{-1}{}^tB_{21} \\ B_{21} & b_{ll} \end{pmatrix}$, where B_{11} is a symmetric matrix of size $l-1$ if $g \in GSp(2l,k)$, and skew-symmetric with $b_{ll}=0$ if $g \in GO(2l,k)$.*

Proof. We use the condition that g satisfies ${}^tg\beta g = \mu(g)\beta$ and ${}^tA = A$ to get $A^{-1}B$ is symmetric if $g \in GSp(2l,k)$, and skew-symmetric if $g \in GO(2l,k)$. Again Lemma 6.3.1 gives the required form for B. □

Lemma 6.3.4. *Let $g = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in GL(2l,k)$. Then,*

1. *$g \in GSp(2l,k)$ if and only if $D = \mu(g){}^tA^{-1}$ and ${}^t(A^{-1}B) = (A^{-1}B)$, and*

2. *$g \in GO(2l,k)$ if and only if $D = \mu(g){}^tA^{-1}$ and ${}^t(A^{-1}B) = -(A^{-1}B)$.*

Proof. 1. Let $g \in GSp(2l,k)$ then g satisfies ${}^t g\beta g = \mu(g)\beta$. Then this implies $D = \mu(g){}^t A^{-1}$ and ${}^t(A^{-1}B) = (A^{-1}B)$.

Conversely, if g satisfies the given condition then clearly $g \in GSp(2l,k)$.

2. This follows by similar computation.

□

Lemma 6.3.5. *Let $Y = \operatorname{diag}(1,\dots,1,\lambda)$ be of size l, where $\lambda \in k^\times$ and $X = (x_{ij})$ be a matrix such that YX is symmetric (resp. skew-symmetric). Then $X = (R_1 + R_2 + \dots)Y$, where each R_m is of the form $t(e_{i,j} + e_{j,i})$ for some $i < j$ or of the form $te_{i,i}$ for some i (resp. each R_m is of the form $t(e_{i,j} - e_{j,i})$ for some $i < j$).*

Proof. Since the matrix YX is symmetric (resp. skew-symmetric), then the matrix X is of the form $\begin{pmatrix} X_{11} & X_{12} \\ X_{21} & x_{ll} \end{pmatrix}$, where X_{11} is symmetric (resp. skew-symmetric), $X_{12} = \lambda {}^t X_{21}$ (resp. $X_{12} = -\lambda {}^t X_{21}$) and X_{21} is a row of size $l-1$. Clearly, X is a sum of the matrices of the form $R_m Y$. □

Lemma 6.3.6. *For $1 \le i \le l$,*

1. *The element $w_{i,-i} = I + e_{i,-i} - e_{-i,i} - e_{i,i} - e_{-i,-i} \in GSp(2l,k)$ is a product of elementary matrices.*

2. *The element $w_{i,-i} = I - e_{i,-i} - e_{-i,i} - e_{i,i} - e_{-i,-i} \in GO(2l,k)$ is a product of elementary matrices.*

3. *The element $w_{i,-i} = I - 2e_{0,0} - e_{i,-i} - e_{-i,i} - e_{i,i} - e_{-i,-i} \in GO(2l+1,k)$ is a product of elementary matrices.*

Proof. 1. We have $w_{i,-i} = x_{i,-i}(1)x_{-i,i}(-1)x_{i,-i}(1)$.

2. We produce these elements inductively. First we get $w_{i,-j} = (I + e_{i,-j} - e_{j,-i})(I + e_{-i,j} - e_{-j,i})(I + e_{i,-j} - e_{j,-i}) = x_{i,-j}(1)x_{-i,j}(1)x_{i,-j}(1)$,

and $w_{i,j} = (I + e_{i,j} - e_{-j,-i})(I - e_{j,i} + e_{-i,-j})(I + e_{i,j} - e_{-j,-i}) = x_{i,j}(1)x_{j,i}(-1)x_{i,j}(1)$. Set $w_l := w_{l,-l} = I - e_{l,l} - e_{-l,-l} - e_{l,-l} - e_{-l,l}$. Then compute $w_l w_{l,l-1} w_{l,-(l-1)} = w_{(l-1),-(l-1)}$. So inductively we get $w_{i,-i}$ is a product of elementary matrices.

3. We have $w_{i,-i} = x_{0,i}(-1)x_{i,0}(1)x_{0,i}(-1)$.

□

Lemma 6.3.7. *The element* $\mathrm{diag}(1, \ldots, 1, \lambda, 1, \ldots, 1, \lambda^{-1}) \in GSp(2l, k)$ *is a product of elementary matrices.*

Proof. First we compute

$$\begin{aligned} w_{l,-l}(t) &= (I + te_{l,-l})(I - t^{-1}e_{-l,l})(I + e_{l,-l}) \\ &= I - e_{l,l} - e_{-l,-l} + te_{l,-l} - t^{-1}e_{-l,l} \\ &= x_{l,-l}(t)x_{-l,l}(-t^{-1})x_{l,-l}(t). \end{aligned}$$

Then compute

$$\begin{aligned} h_l(\lambda) &= w_{l,-l}(\lambda)w_{l,-l}(-1) \\ &= I - e_{l,l} - e_{-l,-l} + \lambda e_{l,l} + \lambda^{-1}e_{-l,-l}, \end{aligned}$$

which is the required element. □

Lemma 6.3.8. *Let* $g = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} \in GO(2l+1, k)$. *Then,*

1. *If* $A = \mathrm{diag}(1, \ldots, 1, \lambda)$ *and* $X = 0$, *then* C *is of the form* $\begin{pmatrix} C_{11} & -\lambda {}^tC_{21} \\ C_{21} & 0 \end{pmatrix}$ *with* C_{11} *skew-symmetric.*

2. If $A = \mathrm{diag}(\underbrace{1,\dots,1}_{m}, \underbrace{0,\dots,0}_{l-m})$*, and* X *with its first* m *entries* 0*, then* C *is of the form* $\begin{pmatrix} C_{11} & 0 \\ C_{21} & C_{22} \end{pmatrix}$ *with* C_{11} *skew-symmetric.*

Proof. We use the equation ${}^tg\beta g = \mu(g)\beta$, and get $2{}^tXX + {}^tAC + {}^tCA = 0$. In the first case, AC is skew-symmetric (using $X = 0$ and ${}^tA = A$). Then Lemma 6.3.1 and Corollary 6.3.2 give the required form for C. In the second case, we note that ${}^tXX$ has top-left and top-right blocks 0, and get the required form for C. □

Lemma 6.3.9. *Let* $g = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & 0 & D \end{pmatrix} \in GO(2l+1,k)$*, then* $X = 0$*, and* $D = \mu(g){}^tA^{-1}$.

Proof. We compute ${}^tg\beta g = \mu(g)\beta$, and get $2{}^tXX = 0$ and $2{}^tXY + {}^tAD = \mu(g)I$. Hence $X = 0$, and $D = \mu(g){}^tA^{-1}$. □

Lemma 6.3.10. *Let* $g = \begin{pmatrix} \alpha & 0 & Y \\ 0 & A & B \\ F & 0 & D \end{pmatrix}$*, with* A *an invertible diagonal matrix. Then* $g \in GO(2l+1,k)$ *if and only if* $\alpha^2 = \mu(g), F = 0 = Y, D = \mu(g)A^{-1}$ *and* ${}^tDB + {}^tBD = 0$*, where* $\mu(g) \in k^\times$ *is similitude of* g*.*

Proof. Let $g \in GO(2l+1,k)$ then we have ${}^tg\beta g = \mu(g)\beta$. So we get $\alpha^2 = \mu(g), F = 0 = Y, D = \mu(g)A^{-1}$ and ${}^tDB + {}^tBD = 0$.

Conversely, if g satisfies the given condition, then $g \in GO(2l+1,k)$. □

6.3.2 Gaussian elimination for $GSp(2l,k)$ and $GO(2l,k)$

The algorithm is as follows:

Step 1:

Input: A matrix $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GSp(2l, k)$ or $GO(2l, k)$.

Output: The matrix $g_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$ is one of the following kind:

a: The matrix A_1 is a diagonal matrix $\mathrm{diag}(1, \ldots, 1, \lambda)$ with $\lambda \neq 0$, and $C_1 = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & c_{ll} \end{pmatrix}$, where C_{11} is symmetric, when $g \in GSp(2l, k)$, and skew-symmetric, when $g \in GO(2l, k)$, and is of size $l-1$. Furthermore, $C_{12} = \lambda {}^t C_{21}$, when $g \in GSp(2l, k)$, and $C_{12} = -\lambda {}^t C_{21}, c_{ll} = 0$, when $g \in GO(2l, k)$.

b: The matrix A_1 is a diagonal matrix $\mathrm{diag}(\underbrace{1, \ldots, 1}_{m}, \underbrace{0, \ldots, 0}_{l-m})$, and $C_1 = \begin{pmatrix} C_{11} & 0 \\ C_{21} & C_{22} \end{pmatrix}$, where C_{11} is an $m \times m$ symmetric, when $g \in GSp(2l, k)$ and skew-symmetric, when $g \in GO(2l, k)$.

Justification: Observe the effect of ER1 and EC1 on the block A. This amounts to the classical Gaussian elimination (see Theorem 6.1.1) on a $l \times l$ matrix A. Thus we can reduce A to a diagonal matrix, and Corollary 6.3.2 makes sure that C has the required form.

Step 2:

Input: matrix $g_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$.

Output: matrix $g_2 = \begin{pmatrix} A_2 & B_2 \\ 0 & \mu(g){}^t A_2^{-1} \end{pmatrix}$; $A_2 = \mathrm{diag}(1, \ldots, 1, \lambda)$.

Justification: Observe the effect of ER3. It changes C_1 by $RA_1 + C_1$. Using Lemma 6.3.5 we can make the matrix C_1 the zero matrix in the first case, and C_{11} the zero matrix in the second case. Further, in the second case, we make use of Lemma 6.3.6 to interchange the rows, so that we get a zero matrix in place of C_1. If required, use ER1 and EC1 to make A_1 a diagonal matrix. Lemma 6.3.4 ensures that D_1 becomes $\mu(g)^t A_2^{-1}$.

Step 3:

Input: matrix $g_2 = \begin{pmatrix} A_2 & B_2 \\ 0 & \mu(g)^t A_2^{-1} \end{pmatrix}$; $A_2 = \text{diag}(1, \ldots, 1, \lambda)$.

Output: matrix $g_3 = \text{diag}(1, \ldots, 1, \lambda, \mu(g), \ldots, \mu(g), \mu(g)\lambda^{-1})$.

Justification: Using Corollary 6.3.3 we see that the matrix B_2 has a certain form. We can use ER2 to make the matrix B_2 a zero matrix because of Lemma 6.3.5.

The algorithm terminates here for $GO(2l, k)$. However for $GSp(2l, k)$ there is one more step.

Step 4:

Input: matrix $g_3 = \text{diag}(1, \ldots, 1, \lambda, \mu(g), \ldots, \mu(g), \mu(g)\lambda^{-1})$.

Output: matrix $g_4 = \text{diag}(1, \ldots, 1, \mu(g), \ldots, \mu(g))$, where $\mu(g) \in k^\times$.

Justification: Using Lemma 6.3.7.

6.3.3 Gaussian elimination for $GO(2l + 1, k)$

The algorithm is as follows:

Step 1:

Input: A matrix $g = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} \in GO(2l + 1, k)$.

Output: The matrix $g_1 = \begin{pmatrix} \alpha_1 & X_1 & Y_1 \\ E_1 & A_1 & B_1 \\ F_1 & C_1 & D_1 \end{pmatrix}$ is one of the following kind:

a: The matrix A_1 is a diagonal matrix $\mathrm{diag}(1, \ldots, 1, \lambda)$ with $\lambda \neq 0$.

b: The matrix A_1 is a diagonal matrix $\mathrm{diag}(\underbrace{1, \ldots, 1}_{m}, \underbrace{0, \ldots, 0}_{l-m})(m < l)$.

Justification: Using ER1 and EC1 we do the classical Gaussian elimination (see Theorem 6.1.1) on a $l \times l$ matrix A.

Step 2:

Input: matrix $g_1 = \begin{pmatrix} \alpha_1 & X_1 & Y_1 \\ E_1 & A_1 & B_1 \\ F_1 & C_1 & D_1 \end{pmatrix}$.

Output: matrix $g_2 = \begin{pmatrix} \alpha_2 & X_2 & Y_2 \\ E_2 & A_2 & B_2 \\ F_2 & C_2 & D_2 \end{pmatrix}$ is one of the following kind:

a: The matrix A_2 is $\mathrm{diag}(1, \ldots, 1, \lambda)$ with $\lambda \neq 0, X_2 = 0 = E_2$, and $C_2 = \begin{pmatrix} C_{11} & -\lambda {}^t C_{21} \\ C_{21} & 0 \end{pmatrix}$, where C_{11} is skew-symmetric of size $l - 1$.

b: The matrix A_2 is $\mathrm{diag}(\underbrace{1, \ldots, 1}_{m}, \underbrace{0, \ldots, 0}_{l-m})(m < l)$; X_2, E_2 have first m entries 0, and $C_2 = \begin{pmatrix} C_{11} & 0 \\ C_{21} & C_{22} \end{pmatrix}$, where C_{11} is an $m \times m$ skew-symmetric matrix.

Justification: Once we have A_1 in diagonal form, we use ER4 and EC4 to change X_1 and E_1 to the required form. Then Lemma 6.3.8 makes sure that C_1 has the required form.

Step 3:

Input: matrix $g_2 = \begin{pmatrix} \alpha_2 & X_2 & Y_2 \\ E_2 & A_2 & B_2 \\ F_2 & C_2 & D_2 \end{pmatrix}$.

Output:

a: matrix $g_3 = \begin{pmatrix} \alpha_3 & 0 & Y_3 \\ 0 & A_3 & B_3 \\ F_3 & 0 & D_3 \end{pmatrix}$; $A_3 = \mathrm{diag}(1, \ldots, 1, \lambda)$.

b: matrix $g_3 = \begin{pmatrix} \alpha_3 & X_3 & Y_3 \\ E_3 & A_3 & B_3 \\ F_3 & C_3 & D_3 \end{pmatrix}$; $A_3 = \mathrm{diag}(\underbrace{1, \ldots, 1}_{m}, \underbrace{0, \ldots, 0}_{l-m})$; X_3, E_3 have first m entries 0, and $C_3 = \begin{pmatrix} 0 & 0 \\ C_{21} & C_{22} \end{pmatrix}$.

Justification: Observe the effect of ER3, and Lemma 6.3.5 ensures the required form.

Step 4:

Input: matrix $g_3 = \begin{pmatrix} \alpha_3 & X_3 & Y_3 \\ E_3 & A_3 & B_3 \\ F_3 & C_3 & D_3 \end{pmatrix}$

Output: matrix $g_4 = \begin{pmatrix} \alpha_4 & 0 & 0 \\ 0 & A_4 & B_4 \\ 0 & 0 & \mu(g) A_4^{-1} \end{pmatrix}$ with $A_4 = \mathrm{diag}(1, \ldots, 1, \lambda), \alpha_4^2 = \mu(g)$, and $B_4 A_4 + A_4{}^t B_4 = 0$.

Justification: In the first case, Lemma 6.3.10 ensures the required form. In the second case, we interchange i with $-i$ for $m + 1 \leq i \leq l$. This will make $C_3 = 0$. Then, if needed, we use ER1 and EC1 on A_3 to make it diagonal. Then Lemma 6.3.9 ensures that A_3 has full rank. Further, we can use ER4 and EC4 to make $X_3 = 0 = E_3$. Lemma 6.3.10 gives the required form.

Step 5:

Input: matrix $g_4 = \begin{pmatrix} \alpha_4 & 0 & 0 \\ 0 & A_4 & B_4 \\ 0 & 0 & \mu(g)A_4^{-1} \end{pmatrix}; A_4 = \mathrm{diag}(1, \ldots, 1, \lambda), \alpha_4^2 = \mu(g)$.

Output: matrix $g_5 = \mathrm{diag}(\alpha_5, 1, \ldots, 1, \lambda, \mu(g), \ldots, \mu(g), \mu(g)\lambda^{-1})$ with $\alpha_5^2 = \mu(g)$.

Justification: Lemma 6.3.10 ensures that B_4 is of a certain kind. We can use ER2 to make $B_4 = 0$.

Thus the main result of this chapter is the following theorem:

Theorem 6.3.11. *Every element of symplectic similitude group $GSp(2l, k)$ or split orthogonal similitude group $GO(n, k)$ (here $n = 2l$ or $2l + 1$), can be written as a product of elementary matrices and a diagonal matrix. Furthermore, the diagonal matrix is of the following form:*

1. *In $GSp(2l, k)$, $\mathrm{diag}(\underbrace{1, \ldots, 1}_{l}, \underbrace{\mu(g), \ldots, \mu(g)}_{l})$, where $\mu(g) \in k^\times$.*
2. *In $GO(2l, k)$, $\mathrm{diag}(\underbrace{1, \ldots, 1, \lambda}_{l}, \underbrace{\mu(g), \ldots, \mu(g), \mu(g)\lambda^{-1}}_{l})$, where $\lambda, \mu(g) \in k^\times$.*
3. *In $GO(2l + 1, k)$, $\mathrm{diag}(\alpha, \underbrace{1, \ldots, 1, \lambda}_{l}, \underbrace{\mu(g), \ldots, \mu(g), \mu(g)\lambda^{-1}}_{l})$, where $\alpha^2 = \mu(g)$ and $\mu(g), \lambda \in k^\times$.*

Proof. This follows from the above algorithms 6.3.2 and 6.3.3. □

This gives us following:

Corollary 6.3.12. *Every element $g \in O(n,k)$ (here $n = 2l$ or $2l+1$) can be written as a product of elementary matrices and a diagonal matrix. Furthermore, the diagonal matrix is* $\mathrm{diag}(\underbrace{1,\ldots,1,\lambda}_{l \text{ or } l+1}, \underbrace{1,\ldots,1,\lambda^{-1}}_{l}), \lambda \in k^{\times}$.

Proof. As $g \in O(n,k)$ so $\mu(g) = 1$. In the odd dimensional orthogonal group, $\alpha = \pm 1$. In this situation, if needed we use Lemma 6.3.6 to make the first diagonal entry 1. Hence this follows from Theorem 6.3.11. □

Corollary 6.3.13. *Every element of the symplectic group $Sp(n,k)$ can be written as a product of elementary matrices.*

Proof. This follows from Theorem 6.3.11, as $\mu(g) = 1$. □

Remark 6.3.14. Corollary 6.3.12 and Corollary 6.3.13 solve the word problem in orthogonal groups $O(n,k)$ and symplectic groups $Sp(n,k)$.

6.4 Gaussian Elimination in Unitary Groups

A similar algorithm has been developed in [MS]. One can define elementary matrices and elementary operations for split unitary groups, similar to that of symplectic and split orthogonal groups. Using those elementary matrices and elementary operations, Mahalanobis and Singh solved the word problem in split unitary groups. They proved (Theorem A [MS]):

Theorem 6.4.1. *Every element of the split unitary group $U(n,k_0)$ (here $n = 2l$ or $2l+1$) can be written as a product of elementary matrices and a diagonal matrix. Furthermore, the diagonal matrix is of the following form:*

1. *In $U(2l,k_0)$,* $\mathrm{diag}(\underbrace{1,\ldots,1,\lambda}_{l}, \underbrace{1,\ldots,1,\bar{\lambda}^{-1}}_{l})$, *where $\lambda \in k^{\times}$.*
2. *In $U(2l+1,k_0)$,* $\mathrm{diag}(\alpha, \underbrace{1,\ldots,1,\lambda}_{l}, \underbrace{1,\ldots,1,\bar{\lambda}^{-1}}_{l})$, *where $\lambda, \alpha \in k^{\times}$ with $\alpha\bar{\alpha} = 1$.*

Chapter 7

Computing Spinor Norm and Similitude

This chapter reports the work done in [BMS]. In this chapter, we show how we can use Gaussian elimination developed in Chapter 6 to compute the spinor norm for split orthogonal groups. Also in this chapter, we compute similitude character for split groups using the Gaussian elimination algorithm. In this chapter, we make use of Wall's theory developed in Chapter 4.

7.1

To compute the spinor norm, we will use the following lemma.

Lemma 7.1.1. *With the notation as earlier for the group $O(n,k)$ (here $n = 2l$ or $2l+1$), we have,*

1. $\Theta(x_{i,j}(t)) = \Theta(x_{i,-j}(t)) = \Theta(x_{-i,j}(t)) = \Theta(x_{i,0}(t)) = \Theta(x_{0,i}(t)) = k^{\times 2}$.

2. $\Theta(w_l) = k^{\times 2}$.

3. $\Theta(\mathrm{diag}(\underbrace{1,\ldots,1,\lambda}_{l \text{ or } l+1},\underbrace{1,\ldots,1,\lambda^{-1}}_{l})) = \lambda k^{\times 2}$.

Proof. 1. This follows from Corollary 4.1.8, since the given elements are all unipotent.

2. Observe that w_l is a reflection along e_l+e_{-l}, and $Q(e_l+e_{-l})=1$, hence $\Theta(w_l)=Q(e_l+e_{-l})k^{\times 2}=k^{\times 2}$.

3. First observe that $\mathrm{diag}(\underbrace{1,\ldots,1,\lambda}_{l \text{ or } l+1},\underbrace{1,\ldots,1,\lambda^{-1}}_{l}) = \sigma_{e_l+e_{-l}}\sigma_{e_l+\lambda e_{-l}}$. Since $\{e_l,e_{-l}\}$ is a hyperbolic pair (see Chapter 2) then $Q(e_l+e_{-l})=1$, and $Q(e_l+\lambda e_{-l})=\lambda$. Hence

$$\Theta(\mathrm{diag}(\underbrace{1,\ldots,1,\lambda}_{l \text{ or } l+1},\underbrace{1,\ldots,1,\lambda^{-1}}_{l}))=Q(e_l+e_{-l})Q(e_l+\lambda e_{-l})k^{\times 2}=\lambda k^{\times 2}.$$

□

The main result is the following:

Theorem 7.1.2 (Spinor norm)**.** *Let $g\in O(n,k)$ (here $n=2l$ or $2l+1$). Suppose Gaussian elimination reduces g to* $\mathrm{diag}(\underbrace{1,\ldots,1,\lambda}_{l \text{ or } l+1},\underbrace{1,\ldots,1,\lambda^{-1}}_{l})$*, where $\lambda\in k^{\times}$. Then the spinor norm $\Theta(g)=\lambda k^{\times 2}$.*

Proof. Let $g\in O(n,k)$. We write g as a product of elementary matrices and a diagonal matrix of the form $\mathrm{diag}(\underbrace{1,\ldots,1,\lambda}_{l \text{ or } l+1},\underbrace{1,\ldots,1,\lambda^{-1}}_{l})$, following Corollary 6.3.12. Again from Lemma 7.1.1, we get the spinor norm for the elementary matrices and the diagonal matrix. Hence $\Theta(g)=\lambda k^{\times 2}$. □

Remark 7.1.3. The Gaussian elimination algorithm also gives us how to compute the similitude character of the symplectic and split orthogonal similitude groups (see Theorem 6.3.11).

Chapter 8

Finiteness of z-classes

The results in this chapter are part of [BS]. This chapter is devoted to the study of z-classes in unitary groups. A unitary group is an algebraic group defined over k_0. Since we are working with perfect fields, an element $T \in U(V, B)$ has a Jordan decomposition, $T = T_sT_u = T_uT_s$, where T_s is semisimple and T_u is unipotent (see Theorem 2.1.1). Further one can use this to compute the centralizer $\mathcal{Z}_{U(V,B)}(T) = \mathcal{Z}_{U(V,B)}(T_s) \cap \mathcal{Z}_{U(V,B)}(T_u)$. So the Jordan decomposition helps us reduce the study of conjugacy and computation of the centralizer of an element to the study of that of its semisimple and unipotent parts. In Section 8.1 we study the z-classes for unipotent elements. In Section 8.2 we explore the z-classes for semisimple elements, and then we prove our main theorem, which states that the number of z-classes in any unitary group is finite if k_0 has the property FE. The preliminaries for this chapter have been discussed in Chapters 2, 4 and 5.

8.1 Unipotent z-classes

We look at a special case when the minimal polynomial is $p(x)^d$, where $p(x)$ is an irreducible, self-U-reciprocal polynomial. This includes unipotent elements. The rational canonical form theory gives a decomposition of

$$V = \bigoplus_{i=1}^{r} V_{d_i}$$

with $1 \leq d_1 \leq d_2 \leq \ldots \leq d_r = d$, and each V_{d_i} is a free module over the k-algebra $\frac{k[x]}{<p(x)^{d_i}>}$ (see 2.14 Chapter IV [SS]). Thus,

Proposition 8.1.1. *Let S and T be in $U(V,B)$. Suppose the minimal polynomial of both S and T are equal, and it equals $p(x)^d$, where $p(x)$ is irreducible self-U-reciprocal. Then S and T are conjugate in $U(V,B)$ if and only if*

1. *the elementary divisors $p(x)^{d_i}$ of S and T are same for $1 \leq d_1 \leq d_2 \leq \ldots \leq d_r = d$, and*

2. *the sequence of hermitian spaces, $\left\{(V^S_{d_1}, H^S_{d_1}), \ldots, (V^S_{d_r}, H^S_{d_r})\right\}$ corresponding to S, and $\left\{(V^T_{d_1}, H^T_{d_1}), \ldots, (V^T_{d_r}, H^T_{d_r})\right\}$ corresponding to T are equivalent. Here $H^S_{d_i}$ and $H^T_{d_i}$ take values in the cyclic k-algebra $\frac{k[x]}{<p(x)^{d_i}>}$.*

Moreover, the centralizer of T, in this case, is the direct product $\mathcal{Z}_{U(V,B)}(T) = \prod_{i=1}^{r} U(V^T_{d_i}, H^T_{d_i})$.

Proof. Suppose S and T are conjugate in $U(V,B)$. Since they are conjugate they have the same set of elementary divisors which proves (1), and (2) follows from Proposition 4.2.2.

Conversely, the elementary divisors of S and T determine the orthogonal decomposition of V as follows:

$$V = V^S_{d_1} \oplus \cdots \oplus V^S_{d_r} \tag{8.1}$$

$$V = V^T_{d_1} \oplus \cdots \oplus V^T_{d_r}, \tag{8.2}$$

where $1 \leq d_1 \leq d_2 \leq \ldots \leq d_r = d$, and for each i, $V^S_{d_i}$ and $V^T_{d_i}$ are free as $E^S_{d_i}$ and $E^T_{d_i}$-module respectively. Since $E^S_{d_i}$ and $E^T_{d_i}$ are isomorphic as k-modules. We may write $E_{d_i} := E^S_{d_i} \cong E^T_{d_i} \cong \frac{k[x]}{<p(x)^{d_i}>}$. Also by (2) we have $(V^S_{d_i}, H^S_{d_i}) \approx (V^T_{d_i}, H^T_{d_i})$ for all $i = 1, 2, \ldots, r$. So by Proposition 4.2.2, we get $S|_{V^S_{d_i}}$ is conjugate to $T|_{V^T_{d_i}}$ by φ_i, then $\varphi = \varphi_1 \oplus \cdots \oplus \varphi_r$ conjugates S and T.

Moreover, we have already seen that $\mathcal{Z}_{U(V,B)}(T) = \prod_{i=1}^{r} \mathcal{Z}_{U(V_i,B_i)}(T_i)$. And by Proposition 4.2.2, we have $\mathcal{Z}_{U(V_{d_i},B_i)}(T_i) = U(V^T_{d_i}, H^T_{d_i})$ for all i. Hence $\mathcal{Z}_{U(V,B)}(T) = \prod_{i=1}^{r} U(V^T_{d_i}, H^T_{d_i})$. □

This gives us following:

Corollary 8.1.2. *Let k_0 have the property FE. Then,*

1. *the number of conjugacy classes of unipotent elements in $U(V, B)$ is finite.*

2. *The number of z-classes of unipotent elements in $U(V, B)$ is finite.*

Proof.
1. In view of Proposition 8.1.1, let the minimal polynomial be $(x - 1)^d$. Thus, we have $p(x) = x - 1$. Then the conjugacy classes correspond to a sequence $1 \leq d_1 \leq d_2 \leq \ldots \leq d_r = d$, and hermitian spaces $\{(V^T_{d_1}, H^T_{d_1}), \ldots, (V^T_{d_r}, H^T_{d_r})\}$ up to equivalence. Now $\underline{E}^T_{d_i} = \frac{k[T]}{<T-1>} \cong k$. Then, by the Wall's approximation theorem (Theorem 4.2.3), the number of non-equivalent hermitian forms (V, B) is exactly equal to the number of non-equivalent hermitian forms $(\underline{V}, \underline{B})$. However, we know that there are only finitely many non-equivalent hermitian forms over k, as k_0 has the property FE. Thus $H^T_{d_i}$ has only finitely many choices for each i. Hence the result.

2. Two elements are conjugate implies that they are also z-conjugate. Hence it follows from the previous part.

□

8.2 Semisimple z-classes

Let $T \in U(V, B)$ be a semisimple element. First, we begin with a basic case.

Lemma 8.2.1. *Let $T \in U(V, B)$ be a semisimple element such that its minimal polynomial is either $p(x)$, which is irreducible, self-U-reciprocal of degree ≥ 2, or $q(x)\tilde{q}(x)$, where $q(x)$ is irreducible not self-U-reciprocal. Let $E = \frac{k[x]}{<p(x)>}$ in the first case and $\frac{k[x]}{<q(x)>}$ in the second case. Then the z-class of T is determined by the following:*

1. *the algebra E over k, and*

2. *the equivalence class of the E-valued hermitian form H^T on V^T.*

Proof. Suppose $S, T \in U(V, B)$ are in the same z-class, then $\mathcal{Z}_{U(V,B)}(S) = g\mathcal{Z}_{U(V,B)}(T)g^{-1}$ for some $g \in U(V, B)$. We may replace T by its conjugate gTg^{-1}, so we get $\mathcal{Z}_{U(V,B)}(S) = \mathcal{Z}_{U(V,B)}(T)$, thus $U(V^S, H^S) = U(V^T, H^T)$. Hence (V^S, H^S) is equivalent to (V^T, H^T). So, in particular, E^S and E^T are isomorphic as k-algebras. The converse follows from Proposition 4.2.2. $\square$

Now for the general case, let $T \in U(V, B)$ be a semisimple element with minimal polynomial

$$m_T(x) = \prod_{i=1}^{k_1} p_i(x) \prod_{j=1}^{k_2} (q_j(x)\tilde{q}_j(x)),$$

where the $p_i(x)$ are self-U-reciprocal polynomials of degree d_i, and $q_j(x)$ not self-U-reciprocal of degree e_j. Let the characteristic polynomial of T be

$$\chi_T(x) = \prod_{i=1}^{k_1} p_i(x)^{r_i} \prod_{j=1}^{k_2} (q_j(x)\tilde{q}_j(x))^{s_j}.$$

Let us write the primary decomposition of V with respect to m_T into T-

invariant subspaces as

$$V = \bigoplus_{i=1}^{k_1} V_i \bigoplus_{j=1}^{k_2} \left(W_j + W_j^*\right). \tag{8.3}$$

Denote $E_i = \frac{k[x]}{<p_i(x)>}$ and $K_j = \frac{k[x]}{<q_j(x)>}$, the field extensions of k of degree d_i and e_j respectively.

Theorem 8.2.2. *With notation as above, let $T \in U(V, B)$ be a semisimple element. Then the z-class of T is determined by the following:*

1. *a finite sequence of integers $(d_1, \ldots, d_{k_1}; e_1, \ldots, e_{k_2})$ each $d_i, e_j \geq 0$ and $n = \sum_{i=1}^{k_1} d_i r_i + 2\sum_{j=1}^{k_2} e_j s_j$.*
2. *Finite field extensions E_i of k of degree d_i for $1 \leq i \leq k_1$ and K_j of k of degree e_j, for $1 \leq j \leq k_2$, and*
3. *equivalence classes of E_i-valued hermitian forms H_i of rank r_i, and $K_j \times K_j$-valued hermitian forms $H_j^{'}$ of rank s_j.*

Further with this notation, $\mathcal{Z}_{U(V,B)}(T) \cong \prod_{i=1}^{k_1} U_{r_i}(H_i) \times \prod_{j=1}^{k_2} GL_{s_j}(K_j)$.

Proof. Follows from Lemma 8.2.1 and Proposition 4.2.2. □

This gives us following:

Corollary 8.2.3. *Let k_0 have the property FE. Then the number of semisimple z-classes in $U(V, B)$ is finite.*

Proof. This follows if we show that there are only finitely many hermitian forms up to equivalence of any degree n. We use Jacobson's theorem (see the Theorem in [Ja]) that equivalence of hermitian forms B over k is given by equivalence of corresponding quadratic forms $Q(x) = \frac{B(x,x)+\overline{B(x,x)}}{2}$ over k_0. However, because of the FE property of k_0 it turns out that $k_0^\times/k_0^{\times 2}$ is finite, and hence there are only finitely many quadratic forms of degree n over k_0. This proves the required result. $\square$

The main result of this chapter is the following theorem:

Theorem 8.2.4. *Let k be a perfect field of $\operatorname{char} k \neq 2$ with a non-trivial Galois automorphism of order 2. Let V be a finite dimensional vector space over k with a non-degenerate hermitian form B. Suppose the fixed field k_0 has the property FE, then the number of z-classes in the unitary group $U(V,B)$ is finite.*

Proof. It follows from Corollary 8.2.3 that the number of conjugacy classes of centralizers of semisimple elements is finite. Hence, up to conjugacy, there are finitely many possibilities for $\mathcal{Z}_{U(V,B)}(s)$ for s semisimple in $U(V,B)$. Let $T \in U(V,B)$, then it has a Jordan decomposition $T = T_sT_u = T_uT_s$. Recall $\mathcal{Z}_{U(V,B)}(T) = \mathcal{Z}_{U(V,B)}(T_s) \cap \mathcal{Z}_{U(V,B)}(T_u)$, and $T_u \in \mathcal{Z}_{U(V,B)}(T_s)^{\circ}$. Now $\mathcal{Z}_{U(V,B)}(T_s)$ is a product of certain unitary groups and general linear groups possibly over a finite extension of k. Corollary 8.1.2 applied on the group $\mathcal{Z}_{U(V,B)}(T_s)$ implies that, up to conjugacy, T_u has finitely many possibilities in $\mathcal{Z}_{U(V,B)}(T_s)$. Hence, up to conjugacy, $\mathcal{Z}_{U(V,B)}(T)$ has finitely many possibilities in $U(V,B)$. Therefore the number of z-classes in $U(V,B)$ is finite. $\square$

Remark 8.2.5. The FE property of the field k_0 is necessary for the above theorem. For example, the field of rational numbers $\mathbb{Q}$ does not have the FE property. We show by an example that the above theorem is no longer true over $\mathbb{Q}$.

Example 8.2.6. Over field $\mathbb{Q}$, there could be infinitely many non-conjugate maximal tori in $GL(n)$. Since a maximal torus is centralizer of a regular semisimple element in it, we get an example of infinitely many z-classes. For the sake of clarity let us write down this concretely when $n = 2$.

The group $GL(2,\mathbb{Q})$ has infinitely many semisimple z-classes. For, if we take $f(x) \in \mathbb{Q}[x]$ any degree 2 irreducible polynomial, then the centralizer of the companion matrix $C_f \in GL(2,\mathbb{Q})$ is isomorphic to $\mathbb{Q}_f^{\times}$, where $\mathbb{Q}_f = \mathbb{Q}[x]/ < f(x) >$, a field extension. Thus non-isomorphic degree two field extensions (hence can not be conjugate) give rise to distinct z-classes (these are maximal tori in $GL(2,\mathbb{Q})$).

Consider $k = \mathbb{Q}[\sqrt{d}]$, a quadratic extension. We embed $GL(2,\mathbb{Q})$ in $U(4)$ with respect to the hermitian form $\begin{pmatrix} 0 & I_2 \\ I_2 & 0 \end{pmatrix}$ given by

$$A \mapsto \begin{pmatrix} A & 0 \\ 0 & {}^t\bar{A}^{-1} \end{pmatrix}.$$

This embedding describes maximal tori in $U(4)$ starting from that of $GL(2)$. Yet again, non-isomorphic degree 2 field extensions would give rise to distinct z-classes. In turn, this gives infinitely many z-classes (of semisimple elements) in $U(4)$.

Example 8.2.7. For $a \in k^{\times}$, consider a unipotent element $u_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ in $SL(2,k)$. Then $\mathcal{Z}_{SL(2,k)}(u_a) = \left\{ \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \mid x^2 = 1, y \in k \right\}$. Then, u_a is conjugate to u_b in $SL(2,k)$ if and only if $a \equiv b (\text{mod } (k^{\times})^2)$. Let k be a (perfect or non-perfect) field with $k^{\times}/(k^{\times 2})$ infinite. Then this would give an example, where we have infinitely many conjugacy classes of unipotents but still, they are in a single z-class.

Chapter 9

Counting z-classes

This chapter reports the work done in [BS]. In this chapter, we investigate the z-classes for classical groups. Without further ado, we shall now go into computing z-classes for $GL(n,k)$ and $U(n,k)$ for different k. In Section 9.1 we compute the number of z-classes and their generating functions for general linear groups, and in Section 9.2 we compute the same for unitary groups. The main theorem proved here is that the number of z-classes in $GL(n,q)$ is same as the number of z-classes in $U(n,q)$, when $q > n$ (Theorem 9.2.5).

9.1 z-classes in General Linear Groups

Let n be a positive integer with a partition $\lambda = (1^{k_1}2^{k_2}\dots n^{k_n})$, denoted by $\lambda \vdash n$, i.e., $n = \sum_i ik_i$, and $p(n)$ denote the number of partitions of n. Let $p(x)$ be the generating function for the partitions of integers so $p(x) = \sum_{n=0}^{\infty} p(n)x^n = \prod_{i=1}^{\infty} \frac{1}{1-x^i}$. Let $z_k(n)$ denotes the number of z-classes in $GL(n,k)$. Define $z_k(x) := \sum_{n=0}^{\infty} z_k(n)x^n$ be the generating function for the z-classes in $GL(n,k)$. If k is an algebraically closed field then we will suppress k, and simply denote them as $z(n)$ and $z(x)$ respectively.

Proposition 9.1.1. *Let k be an algebraically closed field. Then,*

1. *the number of z-classes of semisimple elements in $GL(n,k)$ is $p(n)$, which is same as the number of z-classes of unipotent elements.*

2. *The number of z-classes in $GL(n,k)$ is*

$$z(n) = \sum_{(1^{k_1}2^{k_2}\ldots n^{k_n})\vdash n} \prod_{i=1}^{n} \binom{p(i)+k_i-1}{k_i},$$

and the generating function is

$$z(x) = \prod_{i=1}^{\infty} \frac{1}{(1-x^i)^{p(i)}}.$$

Proof. Since k is an algebraically closed field then for each element $g \in GL(n,k)$ has a unique Jordan form. Suppose it has t-distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_t$. In each Jordan block corresponding to λ_i's, the entries in superdiagonal can be filled with zeros and ones. These possibilities will determine the number of z-classes. These can be said using the following argument. We know that $(1-x)^{-m} = \sum_r \binom{m+r-1}{r} x^r$. Therefore the coefficient of x^{k_i} in $(1-x)^{-p(i)}$ is $\binom{p(i)+k_i-1}{k_i}$. So for a fixed partition $\lambda = (1^{k_1}2^{k_2}\ldots n^{k_n})$ of n, the number of z-classes is $\prod_{i=1}^{n} \binom{p(i)+k_i-1}{k_i}$. Therefore the total number of z-classes in $GL(n,k)$ is $\sum_{(1^{k_1}2^{k_2}\ldots n^{k_n})\vdash n} \prod_{i=1}^{n} \binom{p(i)+k_i-1}{k_i}$. □

Proposition 9.1.2. *Let $z(x) = \prod_{i=1}^{\infty} \frac{1}{(1-x^i)^{p(i)}}$. Then,*

1. *$z_{\mathbb{C}}(x) = z(x)$.*

2. *$z_{\mathbb{R}}(x) = z(x)z(x^2)$.*

3. *If $q > n$ then $z_{\mathbb{F}_q}(x) = \prod_{n=1}^{\infty} z(x^n)$.*

Proof. 1. Here $\mathbb{C}$ can be replaced by any algebraically closed field. Since an algebraically closed field has no extension at all, $z_{\mathbb{C}}(x) = z(x)$.

2. Now $\mathbb{R}$ has two extensions, one is $\mathbb{R}$ itself of degree 1, and $\mathbb{C}$ of degree 2. Clearly the contributions to $z_{\mathbb{R}}(x)$ coming from $\mathbb{C}$ is $z_{\mathbb{C}}(x^2) = z(x^2)$. Hence $z_{\mathbb{R}}(x) = z(x)z(x^2)$.

3. For finite field $\mathbb{F}_q$, for each degree extension n, there is a unique field of that degree, namely $\mathbb{F}_{q^n}$. So the contributions to $z_{\mathbb{F}_q}(x)$ coming from $\mathbb{F}_{q^n}$ are $z_{\mathbb{C}}(x^n) = z(x^n)$. Hence $z_{\mathbb{F}_q}(x) = \prod_{n=1}^{\infty} z(x^n)$, and this product is well-defined because $\mathbb{F}_q$ has the property FE (when $q \leq n$, not all extensions will be available).

$\square$

To compare these numbers we make a table for small ranks. The last row of this table is there in the work of Green (see p.408 in [Gr]).

$z_k(n)$	z(1)	z(2)	z(3)	z(4)	z(5)	z(6)	z(7)	z(8)	z(9)	z(10)
$\mathbb{C}$	1	3	6	14	27	58	111	223	424	817
$\mathbb{R}$	1	4	7	20	36	87	162	355	666	1367
$\mathbb{F}_q, q > n$	1	4	8	22	42	103	199	441	859	1784

9.2 z-classes in Unitary Groups

The genus number of compact Lie groups has been computed in [Bo]. In this situation we have a vector space V over $\mathbb{C}$ of dimension $n+1$. The hermitian forms are classified by the signature, and the corresponding groups are denoted by $U(r,s) = \{g \in GL(n+1, \mathbb{C}) \mid {}^t\bar{g}\beta g = \beta\}$, where $\beta = \begin{pmatrix} I_r & 0 \\ 0 & -I_s \end{pmatrix}$ and $r + s = n + 1$ (see (1) of Example 2.3.8).

9.2.1 z-classes in $U(n+1,0)$

We record the result (see Theorem 3.1 [Bo]) here as follows:

Proposition 9.2.1. *The number of z-classes in $U(n+1,0)$ is $p(n+1)$.*

Proof. The group $U(n+1,0)$ is a compact Lie group. So every element is semisimple. Let $g \in U(n+1,0)$, then g is conjugate to $s := \mathrm{diag}(\lambda_1 I_{r_1}, \ldots, \lambda_t I_{r_t})$, where λ_i's are distinct complex numbers such that $\lambda_i \overline{\lambda_i} = 1$ and $r_1 + \cdots + r_t = n+1$. Hence

$$\mathcal{Z}_{U(n+1,0)}(s) = \prod_{i=1}^{t} U(r_i, 0).$$

So, up to conjugacy, $\mathcal{Z}_{U(n+1,0)}(s)$ is determined by the partitions of $n+1$. Hence the number of z-classes in $U(n+1,0)$ is $p(n+1)$. $\square$

9.2.2 z-classes in $U(n,1)$

The z-classes of $U(n,1)$ have been discussed by Cao and Gongopadhyay in [CG]. Here we present the number of z-classes in this group using the parametrization described there. Recall that the hermitian matrix used there is $\beta = \begin{pmatrix} -1 & 0 \\ 0 & I_n \end{pmatrix}$, and the unitary group is $U(n,1) = \{g \in GL(n+1,\mathbb{C}) \mid {}^t\bar{g}\beta g = \beta\}$.

Another way to look at it is the following ball model: Let V be a vector space of dimension $n+1$ over $\mathbb{C}$, i.e., $V \cong \mathbb{C}^{n+1}$ equipped with the hermitian form of *signature* $(n,1)$,

$$\langle v, w \rangle = -\bar{v}_0 w_0 + \bar{v}_1 w_1 + \cdots + \bar{v}_n w_n,$$

where $v = {}^t(v_0 v_1 \cdots v_n)$ and $w = {}^t(w_0 w_1 \cdots w_n)$ are column vectors in $\mathbb{C}^{n+1}$.

Define

$$V_0 := \{v \in V \mid \langle v, v\rangle = 0\},$$
$$V_+ := \{v \in V \mid \langle v, v\rangle > 0\},$$
$$V_- := \{v \in V \mid \langle v, v\rangle < 0\}.$$

Let $\mathbb{P}(V)$ be the complex projective space, i.e., $\mathbb{P}(V) = \frac{V \smallsetminus \{0\}}{\sim}$, where $u \sim v$ if there exists $\lambda \in \mathbb{C}^\times$ such that $u = \lambda v$. Here $\mathbb{P}(V)$ is equipped with the quotient topology, and the quotient map is $\pi : V \smallsetminus \{0\} \to \mathbb{P}(V)$. The n-dimensional complex hyperbolic space is defined to be $\mathbb{H}^n_{\mathbb{C}} := \pi(V_-)$. The boundary $\partial\mathbb{H}^n_{\mathbb{C}}$ in $\mathbb{P}(V)$ is $\pi(V_0)$. The isometry group $U(n, 1)$ of the hermitian space (V, β) acts as the isometries of $\mathbb{H}^n_{\mathbb{C}}$. The actual group of isometries of $\mathbb{H}^n_{\mathbb{C}}$ is $PU(n, 1) = \frac{U(n,1)}{\mathcal{Z}(U(n,1))}$, where $\mathcal{Z}(U(n, 1)) = \mathbb{S}^1$ is the center. Thus an isometry g of $\mathbb{H}^n_{\mathbb{C}}$ lifts to a unitary transformation $\tilde{g} \in U(n, 1)$. The fixed points of g correspond to eigenvectors of $\tilde{g}$. However, for convenience, we will mostly deal with the linear group $U(n, 1)$ rather than the projective group $PU(n, 1)$. In the following, we shall often forget the lift and use the same symbol for an isometry as well as its lifts.

Now by Brouwer's fixed point theorem, it follows that every isometry g has a fixed point on the closure $\overline{\mathbb{H}^n_{\mathbb{C}}} = \mathbb{H}^n_{\mathbb{C}} \cup \partial\mathbb{H}^n_{\mathbb{C}}$. An isometry g is called *elliptic* if it has a fixed point on $\mathbb{H}^n_{\mathbb{C}}$. It is called *parabolic* if it is not elliptic and has exactly one fixed point on the boundary $\partial\mathbb{H}^n_{\mathbb{C}}$, and is called *hyperbolic* if it is not elliptic and has exactly two fixed points on the boundary $\partial\mathbb{H}^n_{\mathbb{C}}$.

Thus the elements of this group are classified as either elliptic, hyperbolic or parabolic depending on their fixed points. Using conjugation classification [CGb] we know that if an element $g \in U(n, 1)$ is elliptic or hyperbolic, then they are always semisimple. But a parabolic element need not be semisimple. However it has a Jordan decomposition $g = g_s g_u$, where g_s is elliptic, hence semisimple, and g_u is unipotent. In particular if a parabolic isometry is unipotent, then it has minimal polynomial $(x-1)^2$ or $(x-1)^3$ and is called *vertical translation* or *non-vertical translation* respectively.

Definition 9.2.2. An eigenvalue λ (counted with multiplicities) of an element $g \in U(n,1)$ is called null, positive or negative if the corresponding λ-eigenvectors belong to V_0, V_+ or V_- respectively.

Accordingly, a similarity class of eigenvalues $[\lambda]$ is *null*, *positive* or *negative* according to its representative λ is null, positive or negative respectively.

Theorem 9.2.3. *1. The number of z-classes of hyperbolic elements in $U(n,1)$ is $p(n-1)$.*

2. The number of z-classes of elliptic elements in $U(n,1)$ is

$$\sum_{m=1}^{n+1} p(n+1-m).$$

3. The number of z-classes of parabolic elements in $U(n,1)$ is $2+p(n-1)+p(n-2)$ $(n \geq 2)$.

Proof. 1. Now, suppose $T \in U(n,1)$ is hyperbolic. Then V has an orthogonal decomposition $V = V_r \perp (\perp_{i=1}^{t} V_i)$, where $\dim(V_i) = r_i$, and V_i is the eigenspace of T corresponding to the similarity class of positive eigenvalue $[\lambda_i]$ with $|\lambda_i| = 1$. The subspace V_r is the two-dimensional T-invariant subspace spanned by the corresponding similarity class of null-eigenvalues $[re^{i\theta}], [r^{-1}e^{i\theta}]$ for $r > 1$, respectively. Then $\mathcal{Z}_{U(n,1)}(T) = \mathcal{Z}(T|_{V_r}) \times \prod_{j=1}^{t} U(r_j) = S^1 \times \mathbb{R} \times \prod_{j=1}^{t} U(r_j)$. Here $n+1 = 2 + \sum_{j=1}^{t} r_j$, i.e., $\sum_{j=1}^{t} r_j = n-1$. Thus, the number of z-classes of hyperbolic elements is $p(n-1)$.

2. Let $T \in U(n,1)$ be an elliptic element. Then T has a negative class of eigenvalue say $[\lambda]$. Let $m = \dim(V_\lambda)$, which is ≥ 1. It follows from the

conjugacy classification that all the eigenvalues have norm 1 and there is a negative eigenvalue. All other eigenvalues are of the positive type. Then $V = V_\lambda \perp V_\lambda^\perp = V_\lambda \perp (\perp_{i=1}^s V_{\lambda_i})$. Suppose $\dim(V_{\lambda_i}) = r_i$, then $\mathcal{Z}_{U(n,1)}(T) = \mathcal{Z}_{U(V_\lambda)}(T|_{V_\lambda}) \times \prod_{i=1}^{s} U(r_i)$. Now since $T|_{V_\lambda}$ is of negative type, so $\mathcal{Z}(T|_{V_\lambda}) = U(m-1,1)$. Here $n+1 = m + \sum_{i=1}^{s} r_i$, therefore $\sum_{i=1}^{s} r_i = n+1-m$. This gives that the number of z-classes of elliptic elements is $\sum_{m=1}^{n+1} p(n+1-m)$.

3. Let $T \in U(n,1)$ be parabolic. First, let T be unipotent. If the minimal polynomial of T is $(x-1)^2$, i.e., T is a vertical translation, then $\mathcal{Z}_{U(n,1)}(T) = U(n-1) \ltimes (\mathbb{C}^{n-1} \times \mathbb{R})$. If the minimal polynomial of T is $(x-1)^3$, i.e., T is non-vertical translation, then $\mathcal{Z}_{U(n,1)}(T) = (S^1 \times U(n-2)) \ltimes ((\mathbb{R} \times \mathbb{C}^{n-2}) \ltimes \mathbb{R})$. Hence there are exactly two z-classes of unipotents, one corresponds to the vertical translation and the other to the non-vertical translation. Now assume that T is not unipotent. Suppose that the similarity class of a null-eigenvalue is $[\lambda]$. Then V has a T-invariant orthogonal decomposition $V = V_\lambda \perp V_\lambda^\perp$, where V_λ is a T-indecomposable subspace of $\dim(V_\lambda) = m$, which is either 2 or 3. Then $\mathcal{Z}_{U(n,1)}(T) = \mathcal{Z}(T|_{V_\lambda}) \times \mathcal{Z}(T|_{V_\lambda^\perp})$. For each choice of λ, there is exactly one choice for the z-classes of $T|_{V_\lambda}$ in $U(m-1,1)$, i.e., $U(1,1)$ or $U(2,1)$. Note that $T|_{V_\lambda^\perp}$ can be embedded into $U(n+1-m)$. Hence it suffices to find out the number of z-classes of $T|_{V_\lambda}$ in $U(m-1,1)$. Hence the total number of z-classes of non-unipotent parabolic is $p(n-1)+p(n-2)$. Therefore the total number of z-classes of parabolic transformations is $2+p(n-1)+p(n-2)$ $(n \geq 2)$.

$\square$

9.2.3 z-classes in $U(n,q)$

Now we will focus on unitary groups over finite field $k = \mathbb{F}_{q^2}$ with σ given by $\bar{x} = x^q$ and $k_0 = \mathbb{F}_q$. It is well-known that over a finite field there is a unique non-degenerate hermitian form up to equivalence. We denote the unitary group by $U(n,q) := \{g \in GL(n,q^2) \mid {}^t\bar{g}g = I_n\}$. The groups $GL(n,q)$ and $U(n,q)$, both are subgroups of $GL(n,q^2)$. We want to count the number of z-classes, and write its generating function. In view of Ennola duality, the representation theory of both these groups are closely related. Thus it is always useful to compare any computation for $U(n,q)$ with that of $GL(n,q)$.

Lemma 9.2.4. *1. The number of z-classes of unipotent elements in $U(n,q)$ is $p(n)$, which is the number of z-classes of unipotent elements in $GL(n,q)$.*

2. The number of z-classes of semisimple elements in $U(n,q)$ is same as the number of z-classes of semisimple elements in $GL(n,q)$ if $q > n$.

Proof. 1. Let $u = [J_1^{a_1} J_2^{a_2} \dots J_n^{a_n}]$ be a unipotent element in $GL(n,q^2)$ written in Jordan block form. Wall proved the following membership test (see Case(A) on page 34 of [Wa2]): Let $A \in GL(n,q^2)$ then A is conjugate to ${}^t\bar{A}^{-1}$ in $GL(n,q^2)$ if and only if A is conjugate to an element of $U(n,q)$. Since unipotents are conjugate to their own inverse in $GL(n,q^2)$, this implies u is conjugate to ${}^t\bar{u}^{-1}$ in $GL(n,q^2)$. Hence u is conjugate to an element of $U(n,q)$. Wall also proved that two elements of $U(n,q)$ are conjugate in $U(n,q)$ if and only if they are conjugate in $GL(n,q^2)$ (see also 6.1 [Ma]). Thus, up to conjugacy, there is a one-one correspondence of unipotent elements between $GL(n,q^2)$ and $U(n,q)$. This gives that the number of unipotent conjugacy classes in $U(n,q)$ is $p(n)$, and it is same as that of $GL(n,q)$. Now, we note that $\mathcal{Z}_{U(n,q)}(u) = N\prod_{i=1}^{n} U(a_i, q)$, where $N = R_u(\mathcal{Z}_{U(n,q)}(u))$ unipotent radical, and

$$|N| = q^{\sum_{i=2}^{n}(i-1)a_i^2 + 2\sum_{i<j} i a_i a_j}$$

(see Lemma 3.3.8 [BG]). Clearly, the centralizers are distinct and hence can not be conjugate. Thus the number of unipotent z-classes in $U(n,q)$ is $p(n)$.

2. For semisimple elements, we use Theorem 8.2.2. Over a finite field (when $q > n$), we get that semisimple z-classes are characterized by simply $n = \sum_{i=1}^{k_1} d_i r_i + \sum_{j=1}^{k_2} l_j s_j$, where d_i is odd (being a degree of a monic, irreducible, self-U-reciprocal polynomial, see Proposition 5.1.1) and $l_j = 2e_j$ is even. This corresponds to the number of ways n can be written as $n = \sum_i a_i b_i$, which is same as the number of semisimple z-classes in $GL(n,q)$.

□

The main result of this chapter is the following:

Theorem 9.2.5. *The number of z-classes in $U(n,q)$ is same as the number of z-classes in $GL(n,q)$ if $q > n$. Thus, the number of z-classes for either group can be read off by looking at the coefficients of the function $\prod_{i=1}^{\infty} z(x^i)$, where $z(x) = \prod_{j=1}^{\infty} \frac{1}{(1-x^j)^{p(j)}}$.*

Proof. Recall that if $g = g_s g_u$ is the Jordan decomposition of g then $\mathcal{Z}_{U(n,q)}(g) = \mathcal{Z}_{U(n,q)}(g_s) \cap \mathcal{Z}_{U(n,q)}(g_u) = \mathcal{Z}_{\mathcal{Z}_{U(n,q)}(g_s)}(g_u)$, and the structure of $\mathcal{Z}_{U(n,q)}(g_s)$ in Theorem 8.2.2 implies that

$$\text{number of } z\text{-classes in } U(n,q) = \sum_{[s]_z} \text{ no of unipotent } z\text{-classes in } \mathcal{Z}_{U(n,q)}(s),$$

where the sum runs over semisimple z-classes. Hence the number of z-classes in $U(n,q)$ is the same as the number of z-classes in $GL(n,q)$. $\square$

However, the above Theorem 9.2.5 need not be true when $q \leq n$.

Example 9.2.6. Over a finite field $\mathbb{F}_q$, if q is not large enough we may not have as many finite extensions available as required in part 2 of Theorem 8.2.2. Thus we expect less number of z-classes. We use GAP [GAP] to calculate the number of z-classes for small order and present our findings below:

$z_{\mathbb{F}_q}(2)$	$q=2$	$q=3$	$q=4$	$q=5$	$q=7$	$q=9$
$GL(2,q)$	3	4	4	4	4	4
$U(2,q)$	3	4	4	4	4	4

$z_{\mathbb{F}_q}(3)$	$q=2$	$q=3$	$q=4$	$q=5$	$q=7$	$q=9$
$GL(3,q)$	5	7	8	8	8	8
$U(3,q)$	7	8	8	8	8	8

$z_{\mathbb{F}_q}(4)$	$q=2$	$q=3$	$q=4$	$q=5$	$q=7$
$GL(4,q)$	11	19	21	22	22
$U(4,q)$	15	22	22	22	22

Thus we demonstrate the following:

1. When $q \leq n$ the number of z-classes in $GL(n,q)$ and $U(n,q)$ are not given by the formula in Theorem 9.2.5.

2. When $q \leq n$ the number of z-classes in $GL(n,q)$ and $U(n,q)$ need not be equal.

Chapter 10

Future Plans

The groups we study here are fundamental objects in algebraic groups. Given wide interest and applications in group theory, it is interesting to compute centralizers and z-classes in algebraic groups.

10.1 Further Questions

We would like to continue our study for other groups, especially for exceptional groups. So the precise problem would be the following:

Problem 10.1.1. *Is the number of z-classes finite for the exceptional groups of type E_6, E_7, E_8, F_4, G_2 defined over k with the property FE?*

R. Steinberg proved the result all at once for reductive algebraic groups over an algebraically closed field. So one can ask the following:

Problem 10.1.2. *Is the number of z-classes finite for a reductive algebraic group defined over k with the property FE?*

This problem is hard but will be quite interesting. I believe the answer to these questions is positive. We have some ideas and preliminary results on this. Another natural question would be; what is the number of z-classes for a certain group G? We would like to address this question over finite fields $\mathbb{F}_q$. A more concrete question I would like to address in future is the following:

Problem 10.1.3. *What are the number of z-classes in $Sp(n,q)$ and $O(n,q)$?*

Problem 10.1.4. *How does it reflect on the representation theory of these groups?*

We have seen that the Bruhat decomposition (Theorem 6.1.3) for general linear groups $GL(n,k)$ has a nice connection to the classical Gaussian elimination algorithm. So one would expect the same kind of decomposition for other groups, namely, similitude groups using our Gaussian elimination algorithms developed in Section 6.3.2 and 6.3.3. So the precise problem would be the following:

Problem 10.1.5. *Do the Bruhat decomposition for the symplectic and orthogonal groups using our algorithms.*

More generally,

Problem 10.1.6. *Do the Bruhat decomposition for the symplectic and orthogonal similitude groups using our algorithms.*

Bibliography

[As] Teruaki Asai, *"The conjugacy classes in the unitary, symplectic and orthogonal groups over an algebraic number field"*, J.Math.Kyoto Univ (JMKYAZ),16-2 (1976), 325-350.

[B] Cédric Bonnafé, *"Representations of $SL_2(\mathbb{F}_q)$"*, Algebra and Applications, 13. Springer-Verlag London, Ltd., London, (2011).

[BG] Timothy C. Burness; Michael Giudici, *"Classical groups, derangements and primes"*, Australian Mathematical Society Lecture Series, 25. Cambridge University Press, Cambridge, (2016). xviii+346 pp.

[BMS] Sushil Bhunia; Ayan Mahalanobis; Anupam Singh, *"Gaussian elimination in symplectic and split orthogonal groups"*, Tech. report, https://arxiv.org/pdf/1504.03794.pdf, preprint, (2015).

[Bo] Anirban Bose, *"On the genus number of algebraic groups"*, J. Ramanujan Math. Soc. 28 (2013), no. 4, 443-482.

[Br] A. Borel, *"Linear algebraic groups"*, Graduate Texts in Mathematics, 126, Springer-Verlag, New York, (1991).

[BS] Sushil Bhunia; Anupam Singh, *"Conjugacy Classes of Centralizers in Unitary Groups"*, Tech. report, https://arxiv.org/pdf/1610.06728.pdf, preprint, (2016).

[Ca1] Roger W. Carter, *"Simple groups of Lie type"*, Pure and Applied Mathematics, vol. 28, John Wiley & Sons, (1972).

[Ca2] Roger W. Carter, *"Finite groups of Lie type. Conjugacy classes and complex characters"*, Reprint of the 1985 original. Wiley Classics Library. A Wiley-Interscience Publication. John Wiley & Sons, Ltd., Chichester, (1993).

[CG] W. S. Cao; K. Gongopadhyay, *"Commuting isometries of the complex hyperbolic space"*, Proc. Amer. Math. Soc. 139 (2011), 3317-3326.

[CGb] S. S. Chen; L. Greenberg, *"Hyperbolic spaces"*. Contribution to analysis, New York: Academic Press, (1974), 49-87.

[Ch] C. Chevalley, *"Sur certains groupes simples"*, Tohoku Math. J. 7 (1955), no. 2, 14-66.

[DM] François Digne; Jean Michel, *"Representations of finite groups of Lie type"*, London Mathematical Society Student Texts, 21. Cambridge University Press, Cambridge, (1991).

[En] Veikko Ennola, *"On the conjugacy classes of the finite unitary groups"*, Ann. Acad. Sci. Fenn. Ser. A I No. 313 (1962) 13 pp.

[FG] Jason Fulman; Robert Guralnick, *"The number of regular semisimple conjugacy classes in the finite classical groups"*, Linear Algebra Appl. 439 (2013), no. 2, 488-503.

[Fl] Peter Fleischmann, *"Finite fields, root systems, and orbit numbers of Chevalley groups"*, Finite Fields Appl. 3 (1997), no. 1, 33-47.

[GAP] The GAP Group, *"GAP-Groups, Algorithms, and Programming, Version 4.8.7"*, (2017), (`http://www.gap-system.org`).

[Gc] Joseph F. Grcar, *"Mathematicians of Gaussian elimination"*, Notices of the AMS 58 (2011), no. 6, 782-792.

[GK] K. Gongopadhyay; R. S. Kulkarni, *"The z-classes of isometries"*, J. Indian Math. Soc. (N.S.) 81 (2014),no. 3-4,245-258.

[GKKL] R. M. Guralnick; W. M. Kantor; M. Kassabov; A. Lubotzky, *"Presentations of finite simple groups: a computational approach"*, J. Eur. Math. Soc. 13 (2011), no. 2, 391-458.

[Gr] J. A. Green, *"The characters of the finite general linear groups"*, Trans. Amer. Math. Soc. 80 (1955), 402 - 447.

[Gv] Larry C. Grove, *"Classical groups and geometric algebra"*, Graduate Studies in Mathematics, 39. American Mathematical Society, Providence, RI, (2002).

[Ha] A. J. Hahn, *"Unipotent elements and the spinor norms of Wall and Zassenhaus"*, Archiv Math. (Basel) 32 (1979), 114-122.

[Hu1] James E. Humphreys, *"Linear algebraic groups"*, Graduate Texts in Mathematics, No. 21, Springer-Verlag, New York-Heidelberg, (1975).

[Hu2] James E. Humphreys, *"Conjugacy classes in semisimple algebraic groups"*, Mathematical Surveys and Monographs, 43. American Mathematical Society, Providence, RI, (1995).

[Ja] N. Jacobson, *"A note on hermitian forms"*, Bull. Amer. Math. Soc. 46 (1940) 264 - 268.

[Kn] Max-Albert Knus, *"Quadratic and hermitian forms over rings"*, Springer-Verlag, (1991).

[Ku] R. S. Kulkarni, *"Dynamics of linear and affine maps"*, Asian J. Math. 12 (2008), no.3, 321 - 344.

[LO] C. R. Leedham-Green; E. A. O'Brien, *"Constructive recognition of classical groups in odd characteristic"*, J. Algebra 322 (2009), no. 3, 833-881.

[Ma] I. G. Macdonald, *"Numbers of conjugacy classes in some finite classical groups"*, Bull. Austral. Math. Soc. 23 (1981), no. 1, 23-48.

[Mi] J. Milnor, *"On isometries of inner product spaces"*, Invent. Math. 8 (1969), 83-97.

[MR] Scott H. Murray; Colva M. Roney-Dougal, *"Constructive homomorphisms for classical groups"*, Journal of Symbolic Computation 46 (2011), 371-384.

[MS] Ayan Mahalanobis; Anupam Singh, *"Gaussian elimination in unitary groups with an application to cryptography"*, Tech. report, https://arxiv.org/pdf/1409.6136.pdf, preprint, (2015).

[Pr] Amritanshu Prasad, *"Representations of $GL_2(\mathbb{F}_q)$ and $SL_2(\mathbb{F}_q)$, and some remarks about $GL_n(\mathbb{F}_q)$"*, arXiv:0712.4051.

[Re] R. Ree, *"On some simple groups defined by C. Chevalley"*, Trans. Amer. Math. Soc., 84 (1957), 392-400.

[Si] A. Singh, *"Conjugacy Classes of Centralizers in G_2"*, J. Ramanujan Math. Soc. 23 (2008), no. 4, 327 - 336.

[Sp] T. A. Springer, *"Linear algebraic groups"*, second edition, Progress in Mathematics, no. 9, Birkhuser Boston, Inc., Boston, MA, (1998).

[Sr] Bhama Srinivasan, *"The characters of the finite symplectic group $Sp(4, q)$"*, Trans. Amer. Math. Soc. 131 (1968) 488-525.

[SS] T. A. Springer; R. Steinberg, *"Conjugacy classes"*, Seminar on Algebraic Groups and Related Finite Groups (Princeton, NJ, USA 1968/69), Lecture Notes in Mathematics 131, Springer, 167-266.

[St1] R. Steinberg, *"Lectures on Chevalley groups"*, notes prepared by John Faulkner and Robert Wilson, Yale University, (1968).

[St2] R. Steinberg, *"Conjugacy Classes in Algebraic Groups"*, notes by V. Deodhar, Lecture Notes in Mathematics 366, Springer-Verlag (1974).

[TV] Nathaniel Thiem; C. Ryan Vinroot, *"On the characteristic map of finite unitary groups"*, Adv. Math. 210 (2007), no. 2, 707-732.

[Wa1] G. E. Wall, *"The structure of a unitary factor group"*, Inst. Hautes Études Sci. Publ. Math (1959), no. 1, 23 pp.

[Wa2] G. E. Wall, *"On the conjugacy classes in the unitary, symplectic and orthogonal groups"*, J. Austral. Math. Soc. 3, 1-62 (1962).

[Wi] J. Williamson, *"Normal matrices over an arbitrary field of characteristic zero"*, Amer. J. Math 61 (1939), 335-356.

[Za] Hans Zassenhaus, *"On the spinor norm"*, Arch. Math. (1962), no. 13, 434-451.