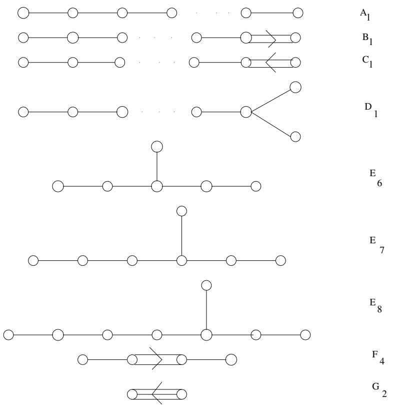
Reality Properties of Conjugacy Classes in Algebraic Groups

Anupam Kumar Singh

Thesis Supervisor : Prof. Maneesh Thakur

A thesis in Mathematics submitted to the
Indian Statistical Institute
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
April 2006



Stat Math Unit, Indian Statistical Institute
8th Mile Mysore Road, RVC Post, Bangalore 560059, India
email : anupamk18@gmail.com

"Mathematics is always a continuum, linked to its history, the past - nothing comes out of zero........ A theorem is never arrived at in the way that logical thought would lead you to believe or that posterity thinks. It is usually much more accidental, some chance discovery in answer to some kind of question. Eventually you can rationalize it and say that this is how it fits. Discoveries never happen as neatly as that. You can rewrite history and make it look much more logical, but actually it happens quite differently....."

Sir Michael Atiyah

Source : Interview with Michael Atiyah and Isadore Singer
http://www.abelprisen.no/en/prisvinnere/2004/interview_2004_1.html

Acknowledgments

It gives me immense pleasure to acknowledge the support of many of my friends, colleagues, family members and teachers, without whom I could not have imagined the existence of this thesis. A large part of the work in this thesis was done at Harish-Chandra Research Institute during my stay there. I wish to acknowledge the support of the institute and its staff members for providing me with excellent facilities and highly competitive work environment.

First, I would like to thank Prof. Maneesh Thakur, my thesis supervisor, for his help and encouragement. He has been understanding, supportive, patient and passionate throughout my association with him. I am indebted for my views and knowledge of Mathematics to him which grew out of numerous discussions over the years. I deeply appreciate his way of working, start from basics, and must say that it has had a great influence on me. The questions in this thesis were suggested to me by him.

At Harish-Chandra Research Institute, I had the opportunity to talk Mathematics with several people. I give credit to Prof. Dipendra Prasad for growing my interest in algebra. It was his graduate course and other courses on Algebraic Number Theory and Algebraic Groups which fascinated me to choose the subject for my research. My association with him dates back to the summers of my undergraduate years when I was a visiting student at HRI. Even, till date, I do not let go in vain any opportunity to discuss Mathematics with him. I also thank him for his remarks on my thesis which helped to improve it tremendously. I owe my understanding of Mathematics to many mathematicians at HRI, specially to Prof. S.D. Adhikari, Prof. Suryaramana, Prof. C. S. Dalawat, Prof. SatyaDeo, Prof. I.B.S. Passi, Prof. Ravi Kulkarni, Prof. E. K. Narayanan, Dr. Shripad Garge, Dr. Ritumoni Sarma, Dr. Manoj Keshari and Dr. A. V. Jayanthan. I learned mathematics from them and had influence on my working style as well. I thank them for always being there to help me out with even silly doubts. All of the students of School of Mathematics at HRI deserve a note of appreciation for being enthusiastic about discussing mathematics with me. Mrs. Seema Agrawal and Dr. Archana Tandon deserve salute from me. At times, I derived motivation from their infinite energy to be patient and hard working. I also thank Yashpal, Ajay Srivastava and Amit Roy for helping me in all kind of non-academic matters which made life a lot easier. It will never be enough to thank the library staff and their help in providing the state-of-the-art facility and always being eager to help out.

I had opportunity to discuss Mathematics with Prof. Mikhail Borovoi and Prof. Boris Kunyavskii. My thanks are due to Prof. Borovoi and his family for being helpful to me during my visit to Israel. I thank Prof. T. A. Springer for making positive comments and showing interest in my thesis questions over emails. I thank Prof. Eric Ellers for showing interest in my thesis and making several comments which made it much more readable.

I discussed Mathematics with many people in Indian Statistical Institute, Bangalore and I thank them for all their support. My thanks are due to Prof. B. Sury, Prof. S. Inamdar and other members of the unit for having good deal of discussions on Mathematics with them. Prof. N. S. N. Sastry and Prof. G. Misra have been very helpful throughout my stay in ISI. I appreciate enthusiasm of department secretary Ms. Asha to whom I have troubled very often.

I take this opportunity to thank many of my teachers starting from my early school days till date for having faith in my ability and guiding me in right direction. Mr. Alagu, Mr. S.B. Singh, (Late) Mr. H.S. Singh, (who taught me in schools), Prof. Sobha Madan, Prof. R.K.S. Rathore, Prof. Shunmugaraj (during undergraduation) deserve my thanks and regards for helping me to fight out my obscure version of Mathematics. Mathematics, for me, would not have been same without their patience with me. Their faith has been a guiding principal in my career. The Department of Mathematics, IIT Kanpur, deserves a note for shaping my career in Mathematics. I have very fond memories of the department and I wish the department will continue to be very active and helpful in guiding students in the right direction.

In my life I have had great influence on my character of many of my friends. My thanks to all of my school friends, batch-mates in college and graduation. I thank Pooja, Alok, Manna and Neena, who were my batch mates in M.Sc., for always being there to help me out with all kind of problems. They always made me feel like a member of a family. Even now I trouble them quite often. For a long time I shared office in HRI with Sanjeev who was senior to me and a good friend. On many occasions we had competition to outwork each other. Thanks! I enjoyed that. I enjoyed my several years of stay at HRI with Sanjeev, Partha, Swapan, Sourin, Suryadeep and

had all kind of discussions from life to academics and from politics to philosophy. With many friends at HRI, Punita, Thanga, Kalyan, Sanoli, Purusottam, Siddhartha, Aarti, Anupama, Sahu, Vikram, Supriya, Tanusree, Archana, Nishikant, Bindusar, Manoj, Anamitra, Rajeev, Kalpataru, Arijit, I had a nice time. All badminton, football and cricket players in HRI (and in ISI) deserve special thanks because sports is the next best thing I love. As it goes with a great saying that 'A healthy mind lives in a healthy body' all of the players have played a great part in shaping my life and making me a better person. I have fond memories of my little friends (most of the kids in HRI), specially Rishabh and Rupam, having played with them. I hope they will not forget me. Many friends at ISI, Bangalore, specially Dishant, Suhas, Tejas and Binod deserve my thanks for being helpful and making my life comfortable.

Finally this endeavor would not have existed without support from my parents and my brother. There can not be any substitute for the unconditional support and love of my parents, who have given me complete freedom over the years. My brother, Anish, who is a good friend and with whom I have shared/discussed every event of my life, needs to be mentioned here for always being there.

I dedicate this thesis to my school teachers.

The comments of referees has been very useful to improve this thesis.

Contents

Notation

In this thesis we denote a field by k. We consider fields of characteristic not 2 unless stated otherwise. The notation $\bar{k}$ and k_s denotes an algebraic closure and separable closure of k respectively. The symbols $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ will denote fields of rational, real, complex numbers respectively. The symbol $\mathbb{Z}$ will denote the set of integers. We denote by $cd(k)$ the cohomological dimension of k.

We use G to denote an algebraic group and $G(k)$ to denote the group of k-rational points of G. Sometimes we abuse notation and denote the group of $\bar{k}$ points of G by G. An algebraic group always means a linear algebraic group unless stated otherwise. The connected component of G is denoted by G^0. The Lie algebra of G is denoted by $\mathfrak{g}$. An element $g \in G(k)$ is k-real if there exists $t \in G(k)$ such that $tgt^{-1} = g^{-1}$. Let H be a subgroup of G. We denote the centralizer of H in G by $\mathcal{Z}_G(H) = \{g \in G \mid gh = hg \ \forall h \in H\}$ and the normalizer of H in G by $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. The center of G is denoted by $\mathcal{Z}(G)$. The general linear group is denoted by $GL_n(k)$ and special linear group by $SL_n(k)$. Orthogonal groups are denoted as $O(V, \mathfrak{b}), O_n(\mathfrak{b})$ or $O(\mathfrak{q})$ where $\mathfrak{b}$ or $\mathfrak{q}$ indicates the form. Note that we use $Sp_{2n}(\mathfrak{b})$ or $Sp_{2n}(k)$ to denote the symplectic group and $U(V, \mathfrak{h})$ to denote the unitary group with hermitian form $\mathfrak{h}$.

The matrix algebra over field k is denoted by $M_n(k)$. We use the symbol $\mathfrak{C}$ to denote octonion (Cayley) algebras in chapters where we deal with groups of type G_2.

The symbols $\otimes, \oplus$ are used to denote tensor and direct sum respectively. The end of a proof is denoted with symbol $\Box$. **Bold face** word means the word appears for the first time and we give definition for that or a possible reference for the definition.

The notation $\det(A), \mathrm{Hom}(M, N), \mathrm{Aut}(V), \mathrm{Gal}(K/k)$ denotes the determinant of a matrix A, the set of all homomorphisms from M to N, the set of all automorphisms of V and the Galois group of field K over k respectively. The symbol $\mathrm{diag}(A, B, \ldots, D)$ denotes the diagonal matrix where A, B and D themselves are matrices (possibly 1×1) sitting on the diagonal. Transpose of a matrix A is written as ${}^{t}\!A$ and transpose inverse is written as ${}^{t}\!A^{-1}$.

CHAPTER 0

Prologue

Group theory is ubiquitous in nature and it arises via symmetry aspects of objects. The most common groups are the set of linear transformations which preserve symmetry of some object. The way platonic solids are related to finite subgroups of 3-dimensional orthogonal group has mesmerized us for a long time. It is a striking fact, but not surprising, that algebraic groups have their origin in differential equations. It was imagination of S. Lie and later some papers written by Kolchin, to develop Galois theory for differential equations which gave birth to algebraic groups. To start with, linear algebraic groups are defined over algebraically closed fields. In many ways they have properties similar to Lie groups. It is a credit to the great mathematicians Chevalley, Kolchin, Borel and others, who extensively studied the theory of algebraic groups. They also brought in the picture of algebraic groups defined over an arbitrary base field k. In studying algebraic groups over algebraically closed fields one has a lot of facilities and nice theorems. However studying groups over an arbitrary base field is equally important from the point of view of group theory and its representations. In this thesis we deal with the subject of algebraic groups and try to look into the structure of some of the groups. We hope this thesis adds to the understanding of algebraic groups.

We now describe the organization of this thesis. The question of determining real elements in an algebraic group is of great importance from the point of view of representation theory. A reader who is just interested in looking up the results proved in this thesis, should go straightaway to Chapter 6 and then move on to Chapter 10 for connections with representation theory. Since there is no general theory to describe the main results in answer to our questions we study the question of reality for various groups case by case. We have mainly dealt with classical groups case by case and groups of type G_2. Indeed we see that the results are coherent and follow a pattern which guides us towards asking the question in broader sense, i.e., for all algebraic groups (see Section 10.2). Some general results in Chapter 9 further strengthen our claim.

Chapters 1 to 5 are preliminary in nature and are intended to introduce most of the basic concepts used in this thesis. We do not aim to give a complete account of these topics but try to give most of the definitions and results used later and provide appropriate references for these results. In Chapter 1 we describe the classical groups with which we deal in this thesis. There are excellent references ([**A**], [**G**] to mention a few) available on this topic and the subject is usually referred in literature as "Geometric Algebra". The modern theory, from the point of view of algebraic groups, is treated very well in [**KMRT**].

In Chapter 2 we give a brief account of the theory of algebraic groups. In this chapter, we introduce some definitions and terminologies which we keep using throughout this thesis. For a detailed study of the theory of algebraic groups, we refer the reader to [**S3**], [**Sp**], [**Hu**], [**Bo**].

In this thesis we also deal with exceptional groups of type G_2. In Chapter 3 we describe how to obtain all groups of type G_2 over k. The book [**SV**] is an excellent reference for the subject. We develop the theory to suit our needs and describe results from some of the papers, specifically from [**J**] and [**W2**], which we use while proving our results.

Galois cohomology is introduced in Chapter 4. We describe how Galois cohomology describes forms of certain algebraic groups. The book [**Se**] is a good source for this topic.

In Chapter 5 we give a description of maximal tori in SU_n. Though a description of maximal tori in classical groups is available in [**Ka**] and [**R**], for our work we need details of this description for SU_n. We also describe how decomposability of tori is related to representations.

Chapter 6 collects together all main results. Here we describe all the results obtained in this thesis and known results in that direction. Chapters 7, 8 and 9 are devoted to the proofs of the results.

For number theoretic preliminaries (e.g. local and global field, ramification theory, division algebra etc.), we refer the reader to the excellent text [**CF**].

The problem which we have dealt with is closely related to representation theory. In Chapter 10 we describe this connection and try to put forward our question in general theory of representations of algebraic groups. We also take this opportunity to describe some of the questions that remain to be answered. We hope the results in this thesis will contribute to the understanding of the subject.

CHAPTER 1

Classical Groups

In this chapter we give a brief introduction to classical groups. For the classical theory of forms and their isometry groups, we refer the reader to the books by E. Artin ([**A**]) and L. C. Grove ([**G**]) on the subject. For a modern account of the subject, we refer to the book [**KMRT**]. Let k be a field. Let V be a vector space of dimension n over k. We denote the set of all linear automorphisms of V by $GL(V)$. The set $GL(V)$ is a group under the multiplication defined by composition of maps. Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be a basis of V. Then we can identify $GL(V)$ with $GL_n(k) = \{A \in M_n(k) \mid \det(A) \neq 0\}$, the set of all $n \times n$ invertible matrices. This group is called the **general linear group**. The linear automorphisms, which have determinant 1, constitute a subgroup of $GL(V)$, denoted by $SL(V)$. The corresponding matrix group is denoted by $SL_n(k) = \{A \in M_n(k) \mid \det(A) = 1\}$. This group is called the **special linear group** .

1.1. Bilinear Forms and Hermitian Forms

Let V be a vector space of dimension n over a field k. A map $\mathfrak{b} \colon V \times V \to k$ is called a **bilinear form** if

$$\begin{array}{rcl} \mathfrak{b}(ax+by,z) & = & a\mathfrak{b}(x,z) + b\mathfrak{b}(y,z) \\ \mathfrak{b}(x,ay+bz) & = & a\mathfrak{b}(x,y) + b\mathfrak{b}(x,z) \end{array}$$

for all $x, y, z \in V$ and $a, b \in k$.

Definition 1.1.1. A bilinear form $\mathfrak{b}$ is called **symmetric** if $\mathfrak{b}(x,y) = \mathfrak{b}(y,x)$ for all $x, y \in V$. A bilinear form $\mathfrak{b}$ is called **skew-symmetric** or **symplectic** if $\mathfrak{b}(x,x) = 0$ for all $x \in V$.

Let $\mathfrak{b}$ be a bilinear form on V. Let $\{e_1, \ldots, e_n\}$ be a basis of V over k. Then there exists a matrix B such that $\mathfrak{b}(x,y) = {}^t xBy$. The matrix B has $\mathfrak{b}(e_i, e_j)$ as its ij^{th} entry. Note that a bilinear form $\mathfrak{b}$ is symmetric (respectively skew-symmetric) if and only if the corresponding matrix B is symmetric, i.e., $B = {}^tB$ (respectively skew-symmetric, i.e., ${}^tB = -B$), with respect to any fixed basis of V.

Let V be a vector space of dimension n over k. A map $\mathfrak{q}\colon V \to k$ is called a **quadratic form** if

(i) $\mathfrak{q}(ax) = a^2\mathfrak{q}(x)$, for all $a \in k$ and $x \in V$,

(ii) the map $\mathfrak{b}_\mathfrak{q}\colon V \times V \to k$ defined by $\mathfrak{b}_\mathfrak{q}(x,y) = \mathfrak{q}(x+y) - \mathfrak{q}(x) - \mathfrak{q}(y)$ is bilinear.

We note that the bilinear form associated to $\mathfrak{q}$ is symmetric. Given a symmetric bilinear form $\mathfrak{b}$, we can define the associated quadratic form as $\mathfrak{q}(x) = \mathfrak{b}(x,x)$. If characteristic of $k \neq 2$, this gives a one-one correspondence between symmetric bilinear forms and quadratic forms.

Let k be a quadratic field extension of a field k_0. Let σ be the nontrivial field automorphism of k over k_0. We write $\sigma(a) = \bar{a}$ for $a \in k$. Let V be a vector space of dimension n over field k. A map $\mathfrak{b}\colon V \times V \to k$ is called a **sesquilinear** if

$$\begin{aligned} \mathfrak{b}(ax+by,z) &= a\mathfrak{b}(x,z) + b\mathfrak{b}(y,z) \\ \mathfrak{b}(x,ay+bz) &= \bar{a}\mathfrak{b}(x,y) + \bar{b}\mathfrak{b}(x,z) \end{aligned}$$

for all $x,y,z \in V$ and $a,b \in k$.

Definition 1.1.2. A sesquilinear form is called **hermitian** if $\mathfrak{b}(x,y) = \overline{\mathfrak{b}(y,x)}$ for all $x,y \in V$.

Let $\{e_1,\ldots,e_n\}$ be a basis of V over k. Then there exists a matrix B such that $\mathfrak{b}(x,y) = {}^t\!xB\bar{y}$. The matrix B has $\mathfrak{b}(e_i,e_j)$ as its ij^{th} entry. Note that the form $\mathfrak{b}$ is hermitian if and only if the corresponding matrix B is hermitian, i.e., ${}^t\bar{B} = B$.

Let V be a vector space of dimension n over k. Let σ be an automorphism of field k such that $\sigma^2 = 1$ (identity or non-identity). We denote by k_0 the fixed subfield of k under σ when σ is non-identity. We call $(V,\mathfrak{b})$ a **symmetric** or **quadratic (symplectic, hermitian) space** if the form $\mathfrak{b}$ is symmetric (skew-symmetric, hermitian) on V. Let $(V,\mathfrak{b})$ be a space with a form $\mathfrak{b}$ of one of the above types. Then the form $\mathfrak{b}$ is called **nondegenerate** if one of the following equivalent conditions is true:

(i) the subspace $\{x \in V \mid \mathfrak{b}(x,y) = 0,\ \forall y \in V\} = 0$,

(ii) the subspace $\{y \in V \mid \mathfrak{b}(x,y) = 0,\ \forall x \in V\} = 0$,

(iii) the corresponding matrix B to the form is nonsingular.

A quadratic form $\mathfrak{q}$ on V is called nondegenerate if the corresponding bilinear form $\mathfrak{b}_\mathfrak{q}$ is nondegenerate on V. A vector $v \in V$ is called **isotropic** if $\mathfrak{b}(v,v) = 0$ otherwise it is called **anisotropic**. Let W be a subspace of V. We define $W^\perp = \{y \in V \mid \mathfrak{b}(x,y) = 0\ \forall x \in W\}$. A subspace W of V is called **isotropic** if $W \cap W^\perp \neq \{0\}$ and is called **totally isotropic** if $W = W^\perp$. A subspace W is nondegenerate if the form $\mathfrak{b}$ restricted to W is nondegenerate.

Lemma 1.1.3. *Let $(V, \mathfrak{b})$ be a symmetric, symplectic or a hermitian space. Let W be a subspace. Then,*

(1) $\dim(V) = \dim(W) + \dim(W^\perp)$ *and*
(2) $V = W \oplus W^\perp$ *if and only if the form $\mathfrak{b}$ restricted to W is nondegenerate.*

This Lemma is useful in determining whether a subspace is nondegenerate. Let W_1 and W_2 be two subspaces of V. We call V is orthogonal sum of W_1 and W_2 if $V = W_1 \oplus W_2$ and $\mathfrak{b}(w_1, w_2) = 0$ $\forall w_1 \in W_1$ and $w_2 \in W_2$. We denote it by $V = W_1 \bigoplus W_2$.

We will need the notion of **tensor product of bilinear forms**. Let $(V_1, \mathfrak{b}_1)$ and $(V_2, \mathfrak{b}_2)$ be vector spaces over k with bilinear forms. We define $\mathfrak{b}_1 \otimes \mathfrak{b}_2$, a bilinear form on $V_1 \otimes V_2$, by

$$\mathfrak{b}_1 \otimes \mathfrak{b}_2(v_1 \otimes v_2, w_1 \otimes w_2) = \mathfrak{b}_1(v_1, w_1)\mathfrak{b}_2(v_2, w_2).$$

If $\mathfrak{b}_1$ and $\mathfrak{b}_2$ both are symmetric then the form $\mathfrak{b}_1 \otimes \mathfrak{b}_2$ is symmetric. Hence we have notion of tensor product of quadratic forms. Let $(V_1, \mathfrak{q}_1)$ and $(V_2, \mathfrak{q}_2)$ be quadratic spaces over k. Then $(V_1 \otimes V_2, \mathfrak{q}_1 \otimes \mathfrak{q}_2)$ is a quadratic space where $\mathfrak{q}_1 \otimes \mathfrak{q}_2(v_1 \otimes v_2) = \mathfrak{q}_1(v_1)\mathfrak{q}_2(v_2)$.

1.2. Isometry Groups

Let $(V, \mathfrak{b})$ be a space with form $\mathfrak{b}$ which is either symmetric, skew symmetric or hermitian. An element $T \in GL(V)$ is called an **isometry** if $\mathfrak{b}(Tx, Ty) = \mathfrak{b}(x, y)$ for all $x, y \in V$. If the form $\mathfrak{b}$ is symmetric (respectively skew-symmetric or hermitian) the group of isometries is called **orthogonal** (respectively **symplectic or unitary**) group of $(V, \mathfrak{b})$ denoted by $O(V, \mathfrak{b})$ (respectively $Sp(V, \mathfrak{b}), U(V, \mathfrak{b})$). Let $\mathfrak{b}$ be a skew-symmetric form on V. An element $T \in GL(V)$ is called a **skew-symplectic isometry** if $\mathfrak{b}(Tx, Ty) = -\mathfrak{b}(x, y)$ for all $x, y \in V$. The orthogonal group is also denoted by $O(V, \mathfrak{q})$, where $\mathfrak{q}$ is the corresponding quadratic form. The group $SO(V, \mathfrak{b}) = \{T \in O(V, \mathfrak{b}) \mid \det(T) = 1\}$ is called the **special orthogonal** group and the group $SU(V, \mathfrak{b}) = \{T \in U(V, \mathfrak{b}) \mid \det(T) = 1\}$ is called the **special unitary** group.

In the matrix notation, we fix a basis of V and denote the matrix of $\mathfrak{b}$ by B. The matrix groups corresponding to the orthogonal group, symplectic group and the unitary group are denoted as $O_n(\mathfrak{b})$ (or $O_n(\mathfrak{q})$), $Sp_{2n}(\mathfrak{b})$ and $U_n(\mathfrak{b})$ respectively. We have,

$$\begin{aligned} O_n(\mathfrak{b}) &= \{A \in GL_n(k) \mid {}^tABA = B\} \\ Sp_{2n}(\mathfrak{b}) &= \{A \in GL_{2n}(k) \mid {}^tABA = B\} \\ U_n(\mathfrak{b}) &= \{A \in GL_n(k) \mid {}^tAB\bar{A} = B\}. \end{aligned}$$

where $\bar{A}$ is the matrix having entries $\bar{a}_{ij}$ where a_{ij} is the ij^{th} entry of A.

Let us first analyze the structure of orthogonal and unitary groups. Let V be a vector space over k with a nondegenerate symmetric bilinear form or a hermitian form B on it. Then we have,

Proposition 1.2.1. *Let $(V, \mathfrak{b})$ be as above. Then there exists a basis $\{e_1, \ldots, e_n\}$ of V such that $\mathfrak{b}(e_i, e_j) = 0$ for all $i \neq j$.*

We call such a basis an **orthogonal basis** for V. Then the matrix of the form is $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ where $\lambda_i = \mathfrak{b}(e_i, e_i) \in k^*$ if $\mathfrak{b}$ is symmetric and $\lambda_i \in k_0^*$ if $\mathfrak{b}$ is hermitian. Over an algebraically closed field, one can choose an orthonormal basis in the first case and the orthogonal group is $O_n(\mathfrak{b}) = \{A \in GL_n(k) \mid {}^tAA = I\}$.

A transformation $\tau \in O(V, \mathfrak{q})$ is called a **reflection** if there exist an element $v \in V$ with $\mathfrak{q}(v) \neq 0$ such that $\tau(v) = -v$ and τ fixes every vector orthogonal to v. We also denote τ by τ_v. In fact, we have

$$\tau_v(x) = x - 2\frac{\mathfrak{b}(x, v)}{\mathfrak{q}(v)}v.$$

Theorem 1.2.2 (Cartan, Dieudonne). *Let V be a vector space of dimension n over a field k. Let $\mathfrak{q}$ be a nondegenerate quadratic form on it. Then every element in $O(V, \mathfrak{q})$ is a product of at most n reflections.*

The group $SO(V, \mathfrak{q})$ is of index 2 in $O(V, \mathfrak{q})$. An element in $O(V, \mathfrak{q})$ is called a **proper isometry** if it belongs to $SO(V, \mathfrak{q})$ otherwise it is **improper**.

Corollary 1.2.3. *With hypothesis as above, if n is odd and $\tau \in O(V, \mathfrak{q})$ is a proper isometry then τ has a non zero fixed point in V.*

Study of involutions in the orthogonal group is of great importance. An involution in this group corresponds to a nondegenerate subspace of V (see [**G**], Proposition 6.11).

Proposition 1.2.4. *With notation as above, let $\tau \in O(V, \mathfrak{q})$ be an involution, i.e., $\tau^2 = 1$. Then there exists a nondegenerate subspace U of V such that $\tau = -1|_U \oplus 1|_{U^\perp}$.*

Now we include a discussion about symplectic groups. Let V be a vector space with a nondegenerate skew-symmetric form $\mathfrak{b}$ on it. Since the corresponding matrix is skew-symmetric it follows that the dimension of V is even. Let the dimension of V be $n = 2m$.

Proposition 1.2.5. *With notation as above, there exists a basis $\{u_1, v_1, \ldots, u_m, v_m\}$ of V such that $\mathfrak{b}(u_i, v_i) = 1, \mathfrak{b}(u_i, v_j) = 0, \mathfrak{b}(u_i, u_i) = 0$ and $\mathfrak{b}(u_i, u_j) = 0$ for all i, j with $i \neq j$.*

Such a basis is called a **symplectic basis** for V. The corresponding matrix of the form with respect to a symplectic basis is $B = \operatorname{diag}(N, \ldots, N)$ where $N = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. For a symplectic basis, the matrix B does not depend on k hence we denote the symplectic group by $Sp_{2n}(k)$. When $n = 2$, the group $Sp_2(k) = SL_2(k)$. The center of $Sp(V, \mathfrak{b})$ is $\{I, -I\}$ and every element of the symplectic group has determinant 1.

1.3. Algebras with Involutions and Classical Groups

We refer to the book [**KMRT**] for detailed treatment of topics covered in this section. Let k be a field and A an associative k algebra with identity. An **involution** on A is a map (not necessarily k-linear) $\sigma\colon A \to A$ such that

$$\sigma(x + y) = \sigma(x) + \sigma(y), \ \sigma(xy) = \sigma(y)\sigma(x) \ \forall x, y \in A$$

and $\sigma^2 = 1$. For an algebra A with involution σ, the group $\operatorname{Aut}(A, \sigma)$ of k-linear automorphisms of A commuting with σ, is an algebraic group defined over k.

We describe here how classical groups arise this way from matrix algebras. Let V be a finite dimensional vector space over k with a nondegenerate bilinear form $\mathfrak{b}$. Then $\tilde{\mathfrak{b}}\colon V \to V^*$ defined by $\tilde{\mathfrak{b}}(x)(y) = \mathfrak{b}(x, y)$ is an isomorphism. This defines a map $\sigma_{\mathfrak{b}}\colon \operatorname{End}_k(V) \to \operatorname{End}_k(V)$ by $\sigma_{\mathfrak{b}}(T) = \tilde{\mathfrak{b}}^{-1\,t}T\tilde{\mathfrak{b}}$ where ${}^tT \in \operatorname{End}_k(V^*)$. The map $\sigma_{\mathfrak{b}}$ is an anti-automorphism of the k-algebra $\operatorname{End}_k(V)$. We call $\sigma_{\mathfrak{b}}$ the **adjoint** anti-automorphism of $\operatorname{End}_k(V)$ with respect to $\mathfrak{b}$.

Theorem 1.3.1. *The map $\mathfrak{b} \mapsto \sigma_{\mathfrak{b}}$ gives a one-one correspondence between equivalence classes of nondegenerate bilinear forms on V modulo k^* and k-linear anti-automorphisms of the algebra $\operatorname{End}_k(V)$. Under this map a k-linear involution on $\operatorname{End}_k(V)$ corresponds to a bilinear form on V which is either symmetric or skew-symmetric.*

An adjoint anti-automorphism $\sigma_{\mathfrak{b}}$ which is k-linear, is called the **adjoint involution**.

The idea above could be generalized to central simple algebras with involutions to get forms of classical groups over field k. A **central simple algebra** of degree n over k is a k-algebra A such that $A \otimes_k \bar{k} \cong M_n(\bar{k})$ as $\bar{k}$-algebras. Note that for a central simple algebra A we have $\dim_k(A) = n^2$ and the center $\mathcal{Z}(A) = k$. An involution $\sigma \colon A \to A$ maps k to k. Hence $\sigma|_k = Id$ or an automorphism of order 2.

Definition 1.3.2. We call σ an **involution of** 1**st kind** if $\sigma|_k = Id$ and of 2**nd kind** if $\sigma|_k$ is an automorphism of order 2.

An involution σ of the first kind is said to be of **symplectic type** if for any splitting field L and any isomorphism $(A_L = A \otimes_k L, \sigma_L) \cong (\mathrm{End}_L(V), \sigma_{\mathfrak{b}})$, the bilinear form $\mathfrak{b}$ is skew-symmetric; otherwise it is called of **orthogonal type**. We note that ([**KMRT**], Corollary 2.8),

Proposition 1.3.3. *Let A be a central simple k-algebra with an involution σ of the first kind. If degree of A is odd, then A is split and σ is necessarily of orthogonal type. If degree of A is even, then the index of A is power of* 2 *and A has involutions of both type.*

An involution of second kind is said to be of **unitary type**. Let (A, σ) be a central simple k-algebra with involution. A **similitude** of (A, σ) is an element $g \in A$ such that $\sigma(g)g \in k^*$. The scalar $\sigma(g)g$ is called the **multiplier** of g and is denoted by $\mu(g)$. The set of all similitudes of (A, σ) is a subgroup of $A^\times$, the set of all invertible elements of A, which we denote by $Sim(A, \sigma)$. The group $\mathrm{Aut}_k(A, \sigma) = \{\theta \in \mathrm{Aut}_k(A) \mid \sigma\theta = \theta\sigma\}$ is a group defined over k which is a form of one of the classical groups defined in the previous section depending on the type of $\sigma \otimes 1$ on $A \otimes \bar{k}$ over $\bar{k}$. Similitudes with multiplier 1 are called isometries and form a group $\mathrm{Iso}(A, \sigma)$:

$$\mathrm{Iso}(A, \sigma) = \{g \in A^\times \mid \sigma(g)g = 1\}.$$

Let $(V, \mathfrak{b})$ be a nondegenerate symmetric or skew-symmetric space. Consider the central simple k-algebra $A = \mathrm{End}_k(V)$ with adjoint involution $\sigma_{\mathfrak{b}}$. Then,

$$Sim(\mathrm{End}_k(V), \sigma_{\mathfrak{b}}) = \{T \in \mathrm{End}_k(V) \mid \mathfrak{b}(T(v), T(w)) = \alpha\mathfrak{b}(v, w)\ \alpha \in k^*, \forall v, w \in V\}.$$

The group $\mathrm{Iso}(\mathrm{End}_k(V), \sigma_{\mathfrak{b}})$ is $O(V, \mathfrak{b})$ if $\mathfrak{b}$ is symmetric and is $Sp(V, \mathfrak{b})$ if $\mathfrak{b}$ is skew-symmetric. When $\mathfrak{b}$ is skew-symmetric we denote the group $Sim(\mathrm{End}_k(V), \sigma_{\mathfrak{b}})$ by $GSp(V, \mathfrak{b})$ or $GSp(2n, k)$.

One can define adjoint involutions corresponding to hermitian forms as well. Let E be a central simple algebra over a field k and let V be a finitely generated left E module. Let $\theta\colon E \to E$ be an involution on E.

Definition 1.3.4. A **hermitian form** on V is a bi-additive map

$$\mathfrak{h}\colon V \times V \to E$$

such that

(i) $\mathfrak{h}(\alpha x, \beta y) = \alpha\mathfrak{h}(x,y)\theta(\beta)$ for all $x, y \in V$ and $\alpha, \beta \in E$,
(ii) $\mathfrak{h}(y,x) = \theta(\mathfrak{h}(x,y))$ for all $x, y \in V$.

The hermitian form $\mathfrak{h}$ on the left E-module V is called nondegenerate if the only element $x \in V$ such that $\mathfrak{h}(x,y) = 0$ for all $y \in V$ is $x = 0$. For every nondegenerate hermitian form $\mathfrak{h}$ on V, there exists a unique involution $\sigma_{\mathfrak{h}}$ on $\mathrm{End}_E(V)$ such that $\sigma_{\mathfrak{h}}(\alpha) = \theta(\alpha)$ for all $\alpha \in k$ and

$$h(x, f(y)) = h(\sigma_{\mathfrak{h}}(f)(x), y) \ \ for\ x, y \in V.$$

The involution $\sigma_{\mathfrak{h}}$ is called the **adjoint** involution with respect to $\mathfrak{h}$. In this case the isometry group $\mathrm{Iso}(\mathrm{End}_E(V), \mathfrak{h})$ is denoted by $U(V, \mathfrak{h})$.

For more discussion on the forms of classical groups over a field k see Section 4.3.

CHAPTER 2

Linear Algebraic Groups

In this chapter we give a brief account of the theory of algebraic groups. For the material covered here, we refer the books [**S3**], [**Sp**], [**Hu**] and [**Bo**], written by some of the masters of the subject.

2.1. Definition and Examples

Let $\bar{k}$ be an algebraically closed field. An **algebraic group** G is a variety over $\bar{k}$ with a group structure on it such that the maps $m\colon G\times G \to G$ defined by $(x, y) \mapsto xy$ and $i\colon G \to G$ defined by $x \mapsto x^{-1}$ are maps of varieties. If the underlying variety of G is an affine variety over $\bar{k}$ then the group is called an **affine algebraic group**. We give some examples below.

Examples :

(1) The multiplicative group $\mathbb{G}_m$ and the additive group $\mathbb{G}_a$ of $\bar{k}$ are algebraic groups.

(2) The general linear group GL_n is an algebraic group. Following subgroups of GL_n are examples of algebraic group: a finite subgroup, D_n (diagonal matrices in GL_n), T_n (upper triangular matrices in GL_n), U_n (unipotent upper triangular matrices in GL_n), SL_n (special linear group i.e. matrices of determinant 1), O_n (orthogonal group), SO_n (special orthogonal group), Sp_{2n} (symplectic group).

(3) Elliptic curves are example of algebraic groups which are not affine.

Any affine algebraic group G is a closed subgroup of some GL_n. Hence often affine algebraic groups are called **linear algebraic groups**. In this thesis we will only deal with linear algebraic groups and hence we will drop the adjective affine (or linear) occasionally.

Let k be a field and $\bar{k}$ be an algebraic closure of k. An algebraic group G is defined over k (or G is a k-group) if the polynomials defining the underlying variety G are defined over k, with the group maps m and i defined over k and the identity element $e \in G$ is a k-rational point. We denote the k-points of G by $G(k)$.

Let V be a finite dimensional vector space over $\bar{k}$. A **rational representation** of an algebraic group G in V is a homomorphism of algebraic groups $r\colon G \to GL(V)$. For a group G defined over k we say that a rational representation r is defined over k if the map is defined over k. We denote by $\bar{k}[G]$ the coordinate algebra of the algebraic group G. The right translation map of G defined by $(g, x) \mapsto xg^{-1}$ gives rise to a representation ρ of G:

$$\rho\colon G \to GL(\bar{k}[G]) \ , \ (\rho(g)f)(x) = f(xg)$$

where $f \in \bar{k}[G]$.

2.2. Jordan Decomposition

We now describe the Jordan decomposition of an element in an algebraic group. First we recall Jordan decomposition from linear algebra. Let V be a finite dimensional vector space over $\bar{k}$. An endomorphism T of V is called **semisimple** if there is a basis of V consisting of eigenvectors of T. We say that an endomorphism T is **nilpotent** if $T^s = 0$ for some integer $s \geq 1$ and T is **unipotent** if $T - 1$ is nilpotent. For any element $t \in \mathrm{End}(V)$ there are unique $t_s, t_n \in \mathrm{End}(V)$ such that t_s is semisimple, t_n is nilpotent, $t_s t_n = t_n t_s$ and $t = t_s + t_n$. This is called the additive Jordan decomposition. Let $t \in GL(V)$. There are unique elements $t_s, t_u \in GL(V)$ such that t_s is semisimple and t_u is unipotent and $t = t_s t_u = t_u t_s$ (multiplicative Jordan decomposition).

Jordan decomposition generalises to infinite dimensional vector space for locally finite endomorphisms. Let V be a vector space (not necessarily finite dimensional) over k. An element $t \in \mathrm{End}(V)$ is locally finite if V is a union of finite dimensional t-stable subspaces. Let G be an algebraic group. We have for an element $g \in G$ ([**Sp**], Theorem 2.4.8),

Theorem 2.2.1 (Jordan decomposition)**.** *Let $g \in G$. There exist unique elements $g_s, g_u \in G$ such that $g = g_s g_u = g_u g_s$ and for any rational representation $\phi\colon G \to GL(V)$ the element $\phi(g_s) = \phi(g)_s$ is semisimple and $\phi(g_u) = \phi(g)_u$ is unipotent.*

The element g_s is called the semisimple part of g and g_u is called the unipotent part of g.

Let G be an algebraic group defined over k. Let $g \in G(k)$. Then g_s and g_u need not belong to $G(k)$. But if the field k is perfect, the elements g_s and g_u belong to $G(k)$ and we have the Jordan decomposition for g over k.

2.3. Semisimple Algebraic Groups

In this section we briefly recall the structure theory of semisimple algebraic groups. A linear algebraic group G is **diagonalizable** if it is isomorphic to a closed subgroup of some group D_n of diagonal matrices. A group T is a **torus** if it is isomorphic to some D_n. Equivalently a torus is a connected commutative algebraic group consisting of semisimple elements alone. A torus T is a k-torus if T is a group defined over k and is a torus. A k-torus T is called k-split if T is k-isomorphic to some D_n. Tori play an important role in the study of algebraic groups.

Let G be a connected linear algebraic group. A **maximal torus** of G is a torus in G that is not strictly contained in another torus contained in G. We record some important results here regarding tori in an algebraic group. Any two maximal tori of G are conjugate ([**Sp**], Theorem 6.4.1). The dimension of a maximal torus in G is called the **rank** of G. Also every semisimple element of G lies in a maximal torus ([**Sp**], Theorem 6.4.5). Now let G be a connected linear algebraic group defined over a field k. Then G contains maximal tori defined over k ([**Sp**], Theorem 13.3.6) and every semisimple element of $G(k)$ lies in a maximal k-torus ([**Sp**], Corollary 13.3.8). However, conjugacy of all maximal tori in $G(k)$ is no longer true.

Let G be a connected linear algebraic group. A maximal closed, connected, solvable normal subgroup of G is called the **radical**, denoted as $R(G)$, of G. We call a group G **semisimple** if $R(G) = (e)$. A maximal closed, connected, unipotent normal subgroup of G is called the **unipotent radical**, denoted as $R_u(G)$, of G. In fact, the maximal, closed, unipotent normal subgroup of $R(G)$ is $R(G)_u = R_u(G)$. The group G is called **reductive** if the unipotent part of $R(G)$ is trivial. For example the group GL_n is a reductive group with $R(GL_n) = D_n$, the diagonal torus, whereas SL_n is a semisimple group. A torus is a reductive group which is not semisimple. Let G be a reductive group defined over k. We say that G is **split over** k or k-split if G contains a maximal k-torus which is k split. The group G is **quasi-split** if there exists a Borel subgroup of G defined over k and **anisotropic** if none of its proper parabolic subgroups is defined over k.

Let T be a maximal torus in G. Then the group $W = W(G,T) = N_G(T)/\mathcal{Z}_G(T)$ is finite and is called the **Weyl group** of G with respect to a fixed maximal torus T. If the group G is reductive then $\mathcal{Z}_G(T) = T$ ([**Sp**], Corollary 7.6.4) and in this case the Weyl group $W = N_G(T)/T$. This group plays important role in the study of structure of semisimple groups.

The next proposition reduces the study of structure of reductive groups to that of tori and semisimple groups ([**Sp**], Corollary 8.1.6).

Proposition 2.3.1. *Let G be a connected reductive group. Let $G' = [G, G]$ be the commutator subgroup of G. Then, $G = G'.Z^0$ where Z^0 is the connected component of the center of G.*

In this decomposition G' is a semisimple group and Z^0 is a torus. Moreover, this decomposition is an almost direct product, i.e., the intersection of G' and Z^0 is a finite group (or equivalently the connected component of this intersection is trivial). An example of this decomposition is $GL_n(\bar{k}) = SL_n(\bar{k}).\mathcal{Z}(GL_n(\bar{k}))^0$ where $\mathcal{Z}(GL_n(\bar{k})) = \mathcal{Z}(GL_n(\bar{k}))^0 = \bar{k}^*$. The intersection of the components is scalar matrices λI of determinant 1, i.e., $\lambda^n = 1$, which is a finite group.

Let G be a connected semisimple group. We can decompose such a group as an almost direct product of simple groups. Recall that a group G is a **simple** (also called **quasi-simple**) algebraic group if any proper normal subgroup of G is finite and lies in the center of G. Some examples of simple groups are SL_n, SO_n, Sp_{2n}, G_2 (all these groups have been introduced in this thesis) et cetra. We have ([**Sp**], Theorem 8.1.5),

Proposition 2.3.2. *Let G be a connected semisimple group. Then G has a finite set of closed normal subgroups $G_1, \dots, G_k$ such that:*

(i) *each G_i is simple,*
(ii) *$[G_i, G_j] = 1$ if $i \neq j$,*
(iii) *$G = G_1 G_2 \cdots G_k$,*
(iv) *$G_i \cap G_1 \cdots G_{i-1} G_{i+1} \cdots G_k$ is finite for each i.*

The G_i are uniquely determined by these conditions. They are called simple components of the semisimple group G. Simple groups can be classified via root system which we recall briefly in next section.

2.4. Root Datum and Reductive Groups

Let G be a connected reductive group over $\bar{k}$. Let $\mathfrak{g}$ be the Lie algebra of G. Then G acts via the Ad representation on the Lie algebra $\mathfrak{g}$, i.e., we have a rational representation $\mathrm{Ad}\colon G \to GL(\mathfrak{g})$. We fix a maximal torus T in G and denote the **character group of** T by $X(T) = \mathrm{Hom}(T, \mathbb{G}_m)$. If the rank of the group G is r then the group X is isomorphic to $\mathbb{Z}^r$. The torus T acts on $\mathfrak{g}$ via the Ad representation. Since T is a commuting set of semisimple elements, it acts diagonally on $\mathfrak{g}$ ([**Sp**], Section 7.1). That is, we have

$$\mathfrak{g} = \bigoplus_{\alpha \in X} \mathfrak{g}_\alpha$$

where

$$\mathfrak{g}_\alpha = \{x \in \mathfrak{g} \mid \mathrm{Ad}(t)(x) = \alpha(t)x \ \forall t \in T\}.$$

The subspaces $\mathfrak{g}_\alpha$ are called weight spaces and any non-zero vector in it is called weight vector. The zero weight space is exactly the Lie algebra $\mathfrak{t}$ of T. We write $\Phi = \{\alpha \in X(T) \mid \mathfrak{g}_\alpha \neq 0\}$ and denote the lattice (subgroup) generated by Φ in $X(T)$ by Q. We list some properties here and refer to [**Sp**], Corollary 8.1.2 for the proofs. We have,

(1) Each $\mathfrak{g}_\alpha$ for $\alpha \in \Phi$ is one-dimensional and $\alpha \in \Phi$ if and only if $-\alpha \in \Phi$.
(2) The group W, Weyl group, acts naturally on $X(T)$ and leaves Φ invariant.
(3) Let $E = \mathbb{R} \otimes_{\mathbb{Z}} Q$. Then (E, Φ) is an abstract root system (see [**Sp**], Section 7.4).

A semisimple group can be determined by its root system (E, Φ) and the **fundamental group** X/Q. In view of Proposition 2.3.2 it is enough to classify simple groups. Simple groups correspond to irreducible root systems which eventually can be classified as one of the following types:

$$A_n (n \geq 1), B_n (n \geq 2), C_n (n \geq 3), D_n (n \geq 4), E_6, E_7, E_8, F_4, G_2.$$

The groups $SL_n(\bar{k})$ for $n \geq 1$, $SO_{2n+1}(\mathfrak{q})$ for $n \geq 2$, $Sp_{2n}(\bar{k})$ for $n \geq 3$ and $SO_{2n}(\mathfrak{q})$ for $n \geq 4$ over $\bar{k}$, introduced in the Chapter 1, are the groups of type $A_n(n \geq 1), B_n(n \geq 2), C_n(n \geq 3), D_n(n \geq 4)$ respectively. To determine reductive groups one needs more data which we describe below.

Let us consider the **Borel subgroups** (a maximal connected closed solvable subgroup) of G containing a fixed maximal torus T. They are all conjugate under the action of $N(T)$ and in fact, W acts simply transitively on this set ([**Sp**], Corollary 6.4.12). Let B be a Borel subgroup of G containing T. Then $B = U \rtimes T$ where $U = R_u(B)$. The group G has a unique Borel subgroup B^-, called opposite Borel, containing T such that $B \cap B^- = T$. We have $B^- = U^- T$ where $U^- = R_u(B^-)$ ([**Sp**], Lemma 8.1.4). The subgroups U and U^- are connected unipotent groups normalized by T (in fact, maximal unipotent subgroups of G) and $U \cap U^- = 1$. Let us denote the **cocharacter group** $\mathrm{Hom}(\mathbb{G}_m, T)$ of T by $Y(T)$. Then $Y(T) \cong \mathbb{Z}^r$ where r is the rank of G. We get a pairing:

$$X \times Y \to \mathbb{Z}$$

defined using $\mathrm{Aut}(\mathbb{G}_m) \cong \mathbb{Z}$. For each $\alpha \in \Phi$ there exists a unique (up to scalars) homomorphism $u_\alpha \colon \mathbb{G}_a \to G$ such that $tu_\alpha(x)t^{-1} = u_\alpha(\alpha(t)x)$ for all $x \in \mathbb{G}_a$ and $t \in T$. The image of u_α is denoted as U_α, called the **root subgroup** of G corresponding to α ([**Sp**], Proposition 8.1.1). The root subgroups are minimal proper subgroups of U and U^-. Moreover, the u_α can be chosen such that there is a homomorphism $\phi_\alpha \colon SL_2 \to G$ such that

$$\phi_\alpha \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = u_\alpha(x), \phi_\alpha \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = u_{-\alpha}(x).$$

We define $\alpha^\vee \colon \mathbb{G}_m \to T$ by $\alpha^\vee(x) = \phi_\alpha \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$. Then $\alpha^\vee \in Y$ and is called the **coroot** associated to $\alpha \in \Phi$. We denote the set of coroots by $\Phi^\vee$.

We have associated a root datum $(X(T), \Phi, Y(T), \Phi^\vee)$ to a reductive group G with respect to a fixed maximal torus T in G. One can prove that this data does not depend on the choice of a maximal torus. Every reductive group is classified by its root datum ([**Sp**], Theorem 10.1.1). One can give an abstract definition of root datum and we have a reductive group corresponding to each root datum. We briefly describe how the Weyl group W can be defined from root datum. We let Φ^+ be the set of roots arising from root subgroups of U and Φ^- be those coming from U^-. Roots in Φ^+, Φ^- are called positive and negative roots respectively. Let Δ be the set of positive roots which can not be written as sum of two positive roots. Roots in Δ are called **simple** roots. The group $W(\Delta)$ generated by simple reflections, i.e., reflections with respect to simple roots, is the Weyl group ([**SV**], Theorem 8.3.4). There is an element $w_0 \in W$ such that $w_0(\Phi^+) = \Phi^-$. This element w_0 is unique and is of order 2 called the **longest element**.

Let G be a semisimple algebraic group. Let $Q \subset X$ be its root lattice. Then the fundamental group X/Q is a finite group. Let P be the dual lattice of Q. One can identify P with the weight lattice and we have $Q \subset X \subset P$. A semisimple group G is called **simply connected** if $X = P$ and **adjoint** if $X = Q$.

CHAPTER 3

Groups of Type G_2

In this chapter we describe the groups of type G_2 over a field k. The fact that all groups of type G_2 can be described this way follows from the computation of Galois Cohomology for G_2 in the next chapter (see Corollary 4.3.5). We shall discuss Galois Cohomology in the next chapter. For the exposition in this chapter we follow the book [**SV**]. Results in this chapter are used later in the proof of one of the main theorems. Several results are taken from [**J**], [**W2**] and [**L**] and modified suitably to fulfil our requirements.

3.1. The Group G_2 and Octonions

We begin by a brief introduction to the group G_2. Any group G of type G_2 over a given field k can be realized as the group of k-automorphisms of an octonion algebra over k, determined uniquely by G. We will need the notion of a composition algebra over a field k.

Definition 3.1.1. A composition algebra $\mathfrak{C}$ over a field k is an algebra over k, not necessarily associative, with an identity element 1 together with a nondegenerate quadratic form N on $\mathfrak{C}$, permitting composition, i.e., $N(xy) = N(x)N(y) \ \ \forall\, x, y \in \mathfrak{C}$.

The quadratic form N is called the **norm** on $\mathfrak{C}$. The associated bilinear form N is given by : $N(x, y) = N(x + y) - N(x) - N(y)$. Every element x of $\mathfrak{C}$ satisfies the equation $x^2 - N(x, 1)x + N(x)1 = 0$. There is an involution (anti automorphism of order 2) on $\mathfrak{C}$ defined by $\bar{x} = N(x, 1)1 - x$. We call $N(x, 1)1 = x + \overline{x}$, the **trace** of x. The possible dimensions of a composition algebra over k are $1, 2, 4, 8$. Composition algebras of dimension 1 or 2 are commutative and associative, those of dimension 4 are associative but not commutative (called **quaternion** algebras), and those of dimension 8 are neither commutative nor associative (called **octonion** algebras or **Cayley** algebra).

Let $\mathfrak{C}$ be an octonion algebra and $G = \mathrm{Aut}(\mathfrak{C})$ be the automorphism group of $\mathfrak{C}$. Since any automorphism of an octonion algebra leaves the norm invariant, $\mathrm{Aut}(\mathfrak{C})$ is a subgroup of the orthogonal group $O(\mathfrak{C}, N)$. In fact, the automorphism group G is a subgroup of the rotation group $SO(N)$ and is contained in $SO(N_1) = \{t \in SO(N) \mid t(1) = 1\}$, where $N_1 = N|_{1^\perp}$. We have ([**SV**], Theorem 2.3.5),

Proposition 3.1.2. *The algebraic group $\mathfrak{G} = \mathrm{Aut}(\mathfrak{C}_{\bar{k}})$, where $\mathfrak{C}_{\bar{k}} = \mathfrak{C} \otimes \bar{k}$ and $\bar{k}$ is an algebraic closure of k, is the split, connected, simple algebraic group of type G_2. Moreover, $\mathfrak{G}$ is defined over k.*

In fact, any simple group of type G_2 over a field k is isomorphic to the automorphism group of an octonion algebra $\mathfrak{C}$ over k ([**Se**], Chapter III, Proposition 5, Corollary; see Corollary 4.3.5). There is a dichotomy with respect to the norm of octonion algebras (in general, for composition algebras). The norm N is a **Pfister** form (tensor product of norm forms of quadratic extensions) and hence is either anisotropic or hyperbolic. If N is anisotropic, every nonzero element of $\mathfrak{C}$ has an inverse in $\mathfrak{C}$. We then call $\mathfrak{C}$ a **division** octonion algebra. If N is hyperbolic, up to isomorphism, there is only one octonion algebra with N as its norm, called the **split** octonion algebra. We give below a model for the split octonion algebra over a field k. Let

$$\mathfrak{C} = \left\{ \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} \mid \alpha, \beta \in k; v, w \in k^3 \right\},$$

where k^3 is the three-dimensional vector space over k with standard basis. On k^3 we have a nondegenerate bilinear form, given by $\langle v, w \rangle = \sum_{i=1}^{3} v_i w_i$, where $v = (v_1, v_2, v_3)$ and $w = (w_1, w_2, w_3)$ in k^3 and the wedge product on k^3 is given by $v \wedge w \in k^3$ where $\langle v \wedge w, u \rangle = \det(v, w, u)$ for $u, v, w \in k^3$. Addition on $\mathfrak{C}$ is entry-wise and the multiplication on $\mathfrak{C}$ is given by,

$$\begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} \begin{pmatrix} \alpha' & v' \\ w' & \beta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' - \langle v, w' \rangle & \alpha v' + \beta' v + w \wedge w' \\ \beta w' + \alpha' w + v \wedge v' & \beta\beta' - \langle w, v' \rangle \end{pmatrix}.$$

The quadratic form N, the norm on $\mathfrak{C}$, is given by

$$N \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} = \alpha\beta + \langle v, w \rangle.$$

An octonion algebra over a field k can be defined as an algebra over k which, after changing base to a separable closure k_s of k, becomes isomorphic to the split octonion algebra over k_s (see [**T**]).

3.1.1. Octonions from Rank 3 Hermitian Spaces. We briefly recall here from [**T**], a construction of octonion algebras from rank 3 hermitian spaces over a quadratic étale algebra over k. First we recall ([**KMRT**], Proposition 18.3),

Definition 3.1.3. Let $\mathcal{E}$ be a finite dimensional k-algebra. Then $\mathcal{E}$ is called an étale algebra if $\mathcal{E} \otimes_k k_s \cong k_s \times \ldots \times k_s$, where k_s is a separable closure of k.

Let L be a quadratic étale algebra over k with $x \mapsto \overline{x}$ as its standard involution. Let $(V, \mathfrak{h})$ be a rank 3 nondegenerate hermitian space over L (see Definition 1.3.4). Assume that the discriminant of $(V, \mathfrak{h})$ is trivial, i.e., $\bigwedge^3(V, \mathfrak{h}) \cong (L, < 1 >)$, where $< 1 >$ denotes the hermitian form $(x, y) \mapsto x\overline{y}$ on L. Fixing a trivialization $\psi \colon \bigwedge^3(V, \mathfrak{h}) \cong (L, < 1 >)$, we define a vector product $\times \colon V \times V \longrightarrow V$ by the identity,

$$\mathfrak{h}(u, v \times w) = \psi(u \wedge v \wedge w),$$

for $u, v, w \in V$. Let $\mathfrak{C}$ be the 8-dimensional k-vector space $\mathfrak{C} = C(L; V, \mathfrak{h}, \psi) = L \oplus V$. We define a multiplication on $\mathfrak{C}$ by,

$$(a, v)(b, w) = (ab - \mathfrak{h}(v, w),\ aw + \overline{b}v + v \times w),\ a, b \in L,\ v, w \in V.$$

With this multiplication, $\mathfrak{C}$ is an octonion algebra over k with norm $N(a, v) = N_{L/k}(a) + \mathfrak{h}(v, v)$. Note that L embeds in $\mathfrak{C}$ as a composition subalgebra. The isomorphism class of $\mathfrak{C}$, thus obtained, does not depend on ψ. One can show that all octonion algebras arise this way. We need the following ([**T**], Theorem 2.2),

Proposition 3.1.4. *Let $(V, \mathfrak{h})$ and $(V', \mathfrak{h}')$ be isometric hermitian spaces with trivial discriminant, over a quadratic étale algebra L. Then the octonion algebras $C(L; V, \mathfrak{h})$ and $C(L; V', \mathfrak{h}')$ are isomorphic, under an isomorphism restricting to the identity map on the subalgebra L.*

We also need the following,

Lemma 3.1.5. *Let L be a quadratic field extension of k. Let $(V, \mathfrak{h})$ be a rank three hermitian space over L with trivial discriminant. For any trivialization ψ of the discriminant, the octonion algebra $\mathfrak{C}(L; v, \mathfrak{h}, \psi)$ is a division algebra, if and only if the k-quadratic form on V, given by $\mathfrak{q}(x) = \mathfrak{h}(x, x)$, is anisotropic.*

3.1.2. Quaternions from Rank 3 Quadratic Spaces. We note that a similar construction for quaternion algebras can be done, starting from a rank 3 quadratic space V over k, with trivial discriminant. Let $\mathfrak{b} \colon V \times V \longrightarrow k$ be a nondegenerate bilinear form. Assume that the discriminant of $(V, \mathfrak{b})$ is trivial, i.e., $\bigwedge^3(V, \mathfrak{b}) \cong (k, <$

$1>$), where $<1>$ denotes the bilinear form $(x,y)\mapsto xy$ on k. Fixing a trivialization $\psi\colon\ \bigwedge^3(V,\mathfrak{b})\cong(k,<1>)$, we define a vector product $\times\colon V\times V\longrightarrow V$ by the identity, $\mathfrak{b}(u,v\times w)=\psi(u\wedge v\wedge w)$, for $u,v,w\in V$. Let Q be the 4-dimensional k-vector space $Q=Q(k;V,\mathfrak{b},\psi)=k\oplus V$. We define a multiplication on Q by,

$$(a,v)(b,w)=(ab-\mathfrak{b}(v,w),\ aw+bv+v\times w),\ a,b\in k,\ v,w\in V.$$

With this multiplication, Q is a quaternion algebra over k, with norm $N(a,v)=a^2+\mathfrak{b}(v,v)$. The isomorphism class of Q thus obtained, does not depend on ψ. One can show that all quaternion algebras arise this way.

Proposition 3.1.6. *Let $(V,\mathfrak{b})$ and $(V',\mathfrak{b}')$ be isometric quadratic spaces with trivial discriminants, over a field k. Then the quaternion algebras $Q(k;V,\mathfrak{b})$ and $Q(k;V',\mathfrak{b}')$ are isomorphic.*

3.2. Some Subgroups of G_2

Let $\mathfrak{C}$ be an octonion algebra over a field k (of characteristic $\neq 2$). Let L be a composition subalgebra of $\mathfrak{C}$. In this section, we describe subgroups of $G=\mathrm{Aut}(\mathfrak{C})$, consisting of automorphisms leaving L pointwise fixed or invariant. We define

$$G(\mathfrak{C}/L)=\{t\in\mathrm{Aut}(\mathfrak{C})\mid t(x)=x\ \forall\ x\in L\}$$

and

$$G(\mathfrak{C},L)=\{t\in\mathrm{Aut}(\mathfrak{C})\mid t(x)\in L\ \forall\ x\in L\}\,.$$

Jacobson studied $G(\mathfrak{C}/L)$ in his paper ([**J**]). We mention the descriptions of these subgroups here. One knows that the two dimensional composition algebras over k are precisely the quadratic étale algebras over k ([**KMRT**], Theorem 33.17). Let L be a two dimensional composition subalgebra of $\mathfrak{C}$. Then L is either a quadratic field extension of k or $L\cong k\times k$. Let us assume first that L is a quadratic field extension of k and $L=k(\gamma)$, where $\gamma^2=c.1\neq 0$. Then $L^\perp$ is a left L vector space via the octonion multiplication. Also,

$$\mathfrak{h}\colon L^\perp\times L^\perp\longrightarrow L$$

$$\mathfrak{h}(x,y)=N(x,y)+\gamma^{-1}N(\gamma x,y),$$

is a nondegenerate hermitian form on $L^\perp$ over L. Any automorphism t of $\mathfrak{C}$, fixing L pointwise, induces an L-linear map $t|_{L^\perp}\colon L^\perp\longrightarrow L^\perp$. Then we have ([**J**], Theorem 3),

Proposition 3.2.1. *Let the notation be as fixed above. Let L be a quadratic field extension of k as above. Then the subgroup $G(\mathfrak{C}/L)$ of G is isomorphic to the unimodular (special) unitary group $SU(L^{\perp}, \mathfrak{h})$ of the three dimensional space $L^{\perp}$ over L relative to the hermitian form $\mathfrak{h}$, via the isomorphism,*

$$\begin{aligned} \psi\colon G(\mathfrak{C}/L) &\longrightarrow SU(L^{\perp}, \mathfrak{h}) \\ t &\longmapsto t|_{L^{\perp}}. \end{aligned}$$

Now, let us assume that L is a split two dimensional étale subalgebra of $\mathfrak{C}$. Then $\mathfrak{C}$ is necessarily split and L contains a nontrivial idempotent e. There exists a basis $\mathcal{B} = \{1, u_1, u_2, u_3, e, w_1, w_2, w_3\}$ of $\mathfrak{C}$, called the **Peirce basis** with respect to e, such that the subspaces $U = \text{span}\{u_1, u_2, u_3\}$ and $W = \text{span}\{w_1, w_2, w_3\}$ satisfy $U = \{x \in \mathfrak{C} \mid ex = 0,\ xe = x\}$ and $W = \{x \in \mathfrak{C} \mid xe = 0,\ ex = x\}$. We have, for $\eta \in G(\mathfrak{C}/L),\ x \in U$,

$$0 = \eta(ex) = \eta(e)\eta(x) = e\eta(x),\ \eta(x)e = \eta(x)\eta(e) = \eta(xe) = \eta(x).$$

Hence $\eta(U) = U$. Similarly, $\eta(W) = W$. Then we have ([**J**], Theorem 4),

Proposition 3.2.2. *Let the notation be as fixed above. Let L be a split quadratic étale subalgebra of $\mathfrak{C}$. Then $G(\mathfrak{C}/L)$ is isomorphic to the unimodular (special) linear group $SL(U)$, via the isomorphism given by,*

$$\begin{aligned} \phi\colon G(\mathfrak{C}/L) &\longrightarrow SL(U) \\ \eta &\longmapsto \eta|_U. \end{aligned}$$

Moreover, if we denote the matrix of $\eta|_U$ by A and that of $\eta|_W$ by A_1, with respect to the Peirce basis as above, then ${}^{t}\!A_1 = A^{-1}$.

In the model of the split octonion algebra as in the previous section, with respect to the diagonal subalgebra L, the subspaces U and W are respectively the space of strictly upper triangular and strictly lower triangular matrices. The above action is then given by,

$$\eta\begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} = \begin{pmatrix} \alpha & Av \\ {}^{t}\!A^{-1}w & \beta \end{pmatrix}.$$

We now compute the subgroup $G(\mathfrak{C}, L)$ of automorphisms of the split octonion algebra, leaving invariant a split quadratic étale subalgebra. We work with the matrix model for split octonions. Up to conjugacy by an automorphism, we may assume that the split subalgebra is the diagonal subalgebra. We consider the map ρ on $\mathfrak{C}$ given by

$$\begin{array}{rcl}\rho\colon \mathfrak{C} & \longrightarrow & \mathfrak{C}\\ \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} & \mapsto & \begin{pmatrix} \beta & w \\ v & \alpha \end{pmatrix}.\end{array}$$

Then ρ leaves the two dimensional subalgebra $L = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \mid \alpha, \beta \in k \right\}$ invariant and it is an automorphism of $\mathfrak{C}$, with $\rho^2 = 1$.

Proposition 3.2.3. *Let $\mathfrak{C}$ be the split octonion algebra as above and let L be the diagonal split quadratic étale subalgebra. Then we have,*

$$G(\mathfrak{C}, L) \cong G(\mathfrak{C}/L) \rtimes H,$$

where H is the order two group generated by ρ.

Proof. Let $h \in G(\mathfrak{C}, L)$. Then $h|_L = 1$ or the nontrivial k-automorphism of L. In the first case, $h \in G(\mathfrak{C}/L)$ and, in the second, $h\rho \in G(\mathfrak{C}/L)$. Hence $h = g\rho$ for some $g \in G(\mathfrak{C}/L)$. Moreover, it is clear that H normalizes $G(\mathfrak{C}/L)$ in $\mathrm{Aut}(\mathfrak{C})$. Since $H \cap G(\mathfrak{C}/L) = \{1\}$, we get the required result. □

We now give a general construction of the automorphism ρ of an octonion algebra $\mathfrak{C}$, not necessarily split, as above. We first recall the Cayley-Dickson Doubling for composition algebras :

Proposition 3.2.4. *Let $\mathfrak{C}$ be a composition algebra and $\mathfrak{D} \subset \mathfrak{C}$ a composition subalgebra, $\mathfrak{D} \neq \mathfrak{C}$. Let $a \in \mathfrak{D}^\perp$ with $N(a) = -\lambda \neq 0$. Then $\mathfrak{D}_1 = \mathfrak{D} \oplus \mathfrak{D}a$ is a composition subalgebra of $\mathfrak{C}$ of dimension $2\dim(\mathfrak{D})$. The product on $\mathfrak{D}_1$ is given by:*

$$(x + ya)(u + va) = (xu + \lambda\overline{v}y) + (vx + y\overline{u})a, \;\; x, y, u, v \in \mathfrak{D},$$

where $x \mapsto \overline{x}$ is the involution on $\mathfrak{D}$. The norm on $\mathfrak{D}_1$ is given by $N(x + ya) = N(x) - \lambda N(y)$.

Let $\mathfrak{C}$ be an octonion algebra and $L \subset \mathfrak{C}$, a quadratic composition subalgebra of $\mathfrak{C}$. Let $a \in L^\perp$ with $N(a) \neq 0$. Let $\mathfrak{D} = L \oplus La$ be the double as described above. Then $\mathfrak{D}$ is a quaternion subalgebra of $\mathfrak{C}$. Define $\rho_1\colon \mathfrak{D} \to \mathfrak{D}$ by $\rho_1(x + ya) = \sigma(x) + \sigma(y)a$, where σ denotes the nontrivial automorphism of L. Then ρ_1 is an automorphism of $\mathfrak{D}$, and clearly $\rho_1^2 = 1$ and $\rho_1|_L = \sigma$. We now repeat this construction with respect to $\mathfrak{D}$ and ρ_1. Write $\mathfrak{C} = \mathfrak{D} \oplus \mathfrak{D}b$ for some $b \in \mathfrak{D}^\perp$, $N(b) \neq 0$. Define $\rho\colon \mathfrak{C} \to \mathfrak{C}$ by,

$$\rho(x + yb) = \rho_1(x) + \rho_1(y)b.$$

Then $\rho^2 = 1$ and $\rho|_L = \sigma$ and ρ is an automorphism of $\mathfrak{C}$. One can prove that this construction yields the one given above for the split octonion algebra and its diagonal subalgebra. We have,

Proposition 3.2.5. *Let $\mathfrak{C}$ be an octonion algebra, possibly division, and $L \subset \mathfrak{C}$ a quadratic composition subalgebra. Then $G(\mathfrak{C}, L) \cong G(\mathfrak{C}/L) \rtimes H$, where H is the subgroup generated by ρ and ρ is an automorphism of $\mathfrak{C}$ with $\rho^2 = 1$ and ρ restricted to L is the nontrivial k-automorphism of L.*

We mention a few more subgroups of $\mathrm{Aut}(\mathfrak{C})$. Let $\mathfrak{D} \subset \mathfrak{C}$ be a quaternion subalgebra. Then we have, by Cayley-Dickson doubling, $\mathfrak{C} = \mathfrak{D} \oplus \mathfrak{D}a$ for some $a \in \mathfrak{D}^{\perp}$ with $N(a) \neq 0$. Let $\phi \in \mathrm{Aut}(\mathfrak{C})$ be such that $\phi(x) = x$ for all $x \in \mathfrak{D}$. Then for $z = x + ya \in \mathfrak{C}$, we have, $\phi(z) = \phi(x) + \phi(y)\phi(a)$. But $a \in \mathfrak{D}^{\perp}$ implies $\phi(a) \in \mathfrak{D}^{\perp} = \mathfrak{D}a$. Therefore $\phi(a) = pa$ for some $p \in \mathfrak{D}$ and, by taking norms, we see that $p \in SL_1(\mathfrak{D})$. In fact, we have ([**SV**], Proposition 2.2.1),

Proposition 3.2.6. *The group of automorphisms of $\mathfrak{C}$, leaving $\mathfrak{D}$ pointwise fixed, is isomorphic to $SL_1(\mathfrak{D})$, the group of elements of $\mathfrak{D}$ whose norm is 1. In the above notation, $G(\mathfrak{C}/\mathfrak{D}) \cong SL_1(\mathfrak{D})$.*

We describe yet another subgroup of $\mathrm{Aut}(\mathfrak{C})$. Let $\mathfrak{D}$ be as above and $\phi \in \mathrm{Aut}(\mathfrak{D})$. We can write $\mathfrak{C} = \mathfrak{D} \oplus \mathfrak{D}a$ as above. Define $\widetilde{\phi} \in \mathrm{Aut}(\mathfrak{C})$ by $\widetilde{\phi}(x + ya) = \phi(x) + \phi(y)a$. Then one checks easily that $\widetilde{\phi}$ is an automorphism of $\mathfrak{C}$ that extends ϕ on $\mathfrak{D}$. These automorphisms form a subgroup of $\mathrm{Aut}(\mathfrak{C})$, which we shall abuse notation and continue to denote by $\mathrm{Aut}(\mathfrak{D})$.

Proposition 3.2.7. *With notation as fixed, we have $G(\mathfrak{C}, \mathfrak{D}) \cong G(\mathfrak{C}/\mathfrak{D}) \rtimes \mathrm{Aut}(\mathfrak{D})$.*

Proof. Clearly $\mathrm{Aut}(\mathfrak{D}) \cap G(\mathfrak{C}/\mathfrak{D}) = \{1\}$ and $\mathrm{Aut}(\mathfrak{D})$ normalizes $G(\mathfrak{C}/\mathfrak{D})$. Now, for $\psi \in G(\mathfrak{C}, \mathfrak{D})$, consider the automorphism $\phi = \psi\widetilde{\psi}^{-1}$. Then ϕ fixes elements of H pointwise and we have $\psi = \phi\widetilde{\psi} \in G(\mathfrak{C}/\mathfrak{D}) \rtimes \mathrm{Aut}(\mathfrak{D})$. □

Some of these subgroups are conjugate in the group G. We have a Skolem-Noether type theorem for composition algebras ([**SV**], Corollary 1.7.3) which can be used to describe conjugacy of some of these subgroups.

Theorem 3.2.8. *Let $\mathfrak{C}$ be a composition algebra and let $\mathfrak{D}$ and $\mathfrak{D}'$ be composition subalgebras of the same dimension. Then, every linear isomorphism from $\mathfrak{D}$ onto $\mathfrak{D}'$ can be extended to an automorphism of $\mathfrak{C}$.*

We use this theorem to get following,

Proposition 3.2.9. *Let $\mathfrak{C}$ be an octonion algebra over k and $G = \mathrm{Aut}(\mathfrak{C})$. Let $\mathfrak{D}$ and $\mathfrak{D}'$ be two composition subalgebras of $\mathfrak{C}$. Suppose $\mathfrak{D}$ and $\mathfrak{D}'$ are isomorphic composition subalgebras. Then the subgroups $G(\mathfrak{C}/\mathfrak{D})$ and $G(\mathfrak{C}/\mathfrak{D}')$ are conjugate in the group G. Also the subgroups $G(\mathfrak{C}, \mathfrak{D})$ and $G(\mathfrak{C}, \mathfrak{D}')$ are conjugate in the group G.*

Proof. Let $\tilde{\phi}$ be the isomorphism of $\mathfrak{D}$ to $\mathfrak{D}'$. By Theorem 3.2.8 $\tilde{\phi}$ can be extended to an automorphism of $\mathfrak{C}$, say ϕ. Then, it is easy to check $\phi G(\mathfrak{C}/\mathfrak{D})\phi^{-1} = G(\mathfrak{C}/\mathfrak{D}')$ and $\phi G(\mathfrak{C}, \mathfrak{D})\phi^{-1} = G(\mathfrak{C}, \mathfrak{D}')$. □

Using these results we calculate centralizers of elements in the groups of type G_2 (Theorem 8.5.1) and it turns out that they are contained in one of the subgroups described above.

3.3. Involutions in G_2

In this section, we discuss the structure of involutions in G_2. Let G be a group of type G_2 over k and $\mathfrak{C}$ be an octonion algebra over k with $G = \mathrm{Aut}(\mathfrak{C})$. We call an element $g \in G(k)$ an **involution** if $g^2 = 1$. Hence nontrivial involutions in $G(k)$ are precisely the automorphisms of $\mathfrak{C}$ of order 2. Let g be an involution in $\mathrm{Aut}(\mathfrak{C})$. The eigenspace corresponding to the eigenvalue 1 of $g \in \mathrm{Aut}(\mathfrak{C})$ is the subalgebra $\mathfrak{D}$ of $\mathfrak{C}$ of fixed points of g and is a quaternion subalgebra of $\mathfrak{C}$ ([**J**], section 4, there it is called a reflection). The orthogonal complement $\mathfrak{D}^{\perp}$ of $\mathfrak{D}$ in $\mathfrak{C}$ is the eigenspace corresponding to the eigenvalue -1. Conversely, the linear automorphism of $\mathfrak{C}$, leaving a quaternion subalgebra $\mathfrak{D}$ of $\mathfrak{C}$ pointwise fixed and, acting as multiplication by -1 on $\mathfrak{D}^{\perp}$, is an involutorial automorphism of $\mathfrak{C}$ (see Proposition 3.2.6). Let ρ be an involution in $G(k)$ and let $\mathfrak{D}$ be the quaternion subalgebra of $\mathfrak{C}$, fixed pointwise by ρ. Let $\rho' = g\rho g^{-1}$ be a conjugate of ρ by an element $g \in G(k)$. Then, the quaternion subalgebra $\mathfrak{D}' = g(\mathfrak{D})$ of $\mathfrak{C}$ is fixed pointwise by ρ'. Conversely, suppose the quaternion subalgebra $\mathfrak{D}$ of $\mathfrak{C}$ is isomorphic to the quaternion subalgebra $\mathfrak{D}'$ of $\mathfrak{C}$. Then, by Theorem 3.2.8 there exists an automorphism g of $\mathfrak{C}$ such that $g(\mathfrak{D}) = \mathfrak{D}'$. If ρ denotes the involution leaving $\mathfrak{D}$ fixed pointwise, $\rho' = g\rho g^{-1}$ fixes $\mathfrak{D}'$ pointwise. Therefore, we have,

Proposition 3.3.1. *Let $\mathfrak{C}$ be an octonion algebra over k. Then the conjugacy classes of involutions in $G = \mathrm{Aut}(\mathfrak{C})$ are in bijection with the isomorphism classes of quaternion subalgebras of $\mathfrak{C}$.*

Corollary 3.3.2. *Assume that ${}_2Br(k)$, the 2-torsion in the Brauer group of k, is trivial, i.e., all quaternion algebras over k are split (for example, $cd(k) \leq 1$ fields). Then all involutions in $G(k)$ are conjugates.*

We need a refinement of a theorem of Jacobson ([**J**], Theorem 2), due to Wonenburger ([**W1**], Theorem 5) and Neumann ([**N**]),

Proposition 3.3.3. *Let $\mathfrak{C}$ be an octonion algebra over a field k of characteristic different from 2. Then every element of G is a product of 3 involutions.*

We will study in Chapter 8, the structure of real elements in $G(k)$, in terms of involutions. We will show that a semisimple element $g \in G(k)$ is real, i.e., conjugate to g^{-1} in $G(k)$, if and only if g is a product of 2 involutions in $G(k)$ (Theorem 6.2.2).

CHAPTER 4

Galois Cohomology

In this chapter we give a brief introduction to Galois Cohomology. The book by Serre ([**Se**]) is an excellent reference for the subject and the exposition here is drawn from that book. Another good reference is the notes by Kneser ([**K**]). Occasionally we also need the theory of central simple algebras for which we refer to [**P**]. To understand the theory of algebraic groups over base field k it is very important to understand Galois Cohomology.

4.1. Commutative Cohomology and Central Simple Algebra

Let G be a group and let A be a set on which G acts. We denote the action by $s(a) = {}^s a$ for $s \in G$ and $a \in A$. We call A a G-set. If A is a group and the action of G is via automorphisms then we call A a G-group. Let A be an Abelian G-group. We define $\mathcal{C}^0(G, A) = A$ and $\mathcal{C}^i(G, A) = \{a \colon \underbrace{G \times \ldots \times G}_{i} \to A\}$ which is the set of all maps from $\underbrace{G \times \ldots \times G}_{i}$ to A. We also write $a(s_1, \ldots, s_i)$ as $a_{s_1,\ldots,s_i}$. We define maps $\delta^0 \colon \mathcal{C}^0 \to \mathcal{C}^1$ by $\delta^0(a)(s) = {}^s a - a$ and

$$\begin{aligned}
\delta^i \quad &: \quad \mathcal{C}^i \to \mathcal{C}^{i+1} \text{ for } i \geq 1 \\
\delta^i(a)(s_1, \ldots, s_{i+1}) \quad &= \quad {}^{s_1}a(s_2, \ldots, s_{i+1}) \\
&+ \quad \sum_{j=1}^{i} (-1)^j a(s_1, \ldots, s_j s_{j+1}, \ldots, s_{i+1}) + (-1)^{i+1} a(s_1, \ldots, s_i)
\end{aligned}$$

Then

$$0 \to \mathcal{C}^0 \xrightarrow{\delta^0} \mathcal{C}^1 \xrightarrow{\delta^1} \mathcal{C}^2 \xrightarrow{\delta^2} \ldots \xrightarrow{\delta^{i-1}} \mathcal{C}^i \xrightarrow{\delta^i} \mathcal{C}^{i+1} \xrightarrow{\delta^{i+1}} \ldots$$

is a chain-complex. We define $\mathcal{Z}^i(G, A) = ker(\delta^i)$, the group of **cocycles** and $\mathcal{B}^i(G, A) = Im(\delta^{i-1})$, the group of **coboundaries**. Then $\mathcal{B}^i(G, A) \subset \mathcal{Z}^i(G, A)$ and we define $H^i(G, A) = \frac{\mathcal{Z}^i(G,A)}{\mathcal{B}^i(G,A)}$, called ***i*-th cohomology group**. The cohomology groups are Abelian groups. We write down first few cohomology groups explicitly.

(1) $H^0(G, A) = A^G = \{a \in A \mid {}^s a = a \ \forall s \in G\}$, the set of fixed points of A by the action of G.

(2) $H^1(G,A) = \dfrac{\{a\colon G \to A \mid a_{st} = a_s + {}^s a_t\}}{\{a\colon G \to A \mid a_s = {}^s c - c \text{ for some } c \in A\}}$.

(3) $H^2(G,A) = \dfrac{\{a\colon G\times G \to A \mid a_{s_1 s_2, s_3} = {}^{s_1} a_{s_2,s_3} + a_{s_1, s_2 s_3} - a_{s_1,s_2}\}}{\{a\colon G\times G \to A \mid a_{s,t} = {}^s b_t - b_{st} + b_s \text{ for some map } b\colon G \to A\}}$.

Example 1: Let K be a finite Galois extension of a field k. Let $G = \mathrm{Gal}(K/k)$ be the Galois group. Then G acts on the additive group K by evaluation. Then $H^0(G,K) = k$ and $H^i(G,K) = 0$ for all $i \geq 1$.

Example 2: Let K be a Galois extension of a field k. Let G denote the Galois group $\mathrm{Gal}(K/k)$. Then G acts on the Abelian group K^* by evaluation. Then the cohomology groups are :

(1) $H^0(G,K^*) = k^*$.
(2) $H^1(G,K^*) = 1$ (Hilbert's theorem 90).
(3) $H^2(G,K^*) = \mathrm{Br}(K/k)$.

The group $\mathrm{Br}(K/k)$ is the relative Brauer group which we introduce below.

4.1.1. Central Simple Algebras and the Brauer Group. Let k be a field. Let A be a finite dimensional algebra over k. Then A is called **simple** if it has no two sided ideals other than 0 and A. A finite dimensional algebra is called a **central simple algebra** if it is simple and $\mathcal{Z}(A) = k$. From Wedderburn's structure theorem ([**P**], Theorem, Section 3.5) it follows that a central simple algebra A is isomorphic to $M_r(D)$ where D is a central division algebra over k. Equivalently, a central simple algebra of degree n over k is a k-algebra A such that $A \otimes_k \bar{k} \cong M_n(\bar{k})$ as $\bar{k}$-algebras. We define an equivalence relation on the set of finite dimensional central simple algebras over field k as follows. We call A and B equivalent if one of the following equivalent conditions is satisfied:

(i) If $A \cong M_n(D)$ and $B \cong M_m(D')$ then $D \cong D'$.
(ii) There exist m, n such that $A \otimes M_m(k) \cong B \otimes M_n(k)$.

The **Brauer group** of k ([**P**], Proposition a, Section 12.5) is the set of equivalence classes of finite dimensional central simple algebras over k with multiplication defined by tensor product. It is denoted as $\mathrm{Br}(k)$. Brauer group of a field is an Abelian group. We give few examples here.

(1) $\mathrm{Br}(\mathbb{F}) = \{0\}$, for any finite field $\mathbb{F}$.
(2) $\mathrm{Br}(k) = \{0\}$, for any algebraically closed field k. In fact, $\mathrm{Br}(k) = \{0\}$, for any field k of transcendence degree one over an algebraically closed field.
(3) $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$.

(4) $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$, where $\mathbb{Q}_p$ is the field of p-adic numbers.

Let K/k be a field extension. Then we have a map $\mathrm{Br}(k) \to \mathrm{Br}(K)$ defined by $A \mapsto A \otimes K$. The kernel of this map is called the **relative Brauer group**, denoted as $\mathrm{Br}(K/k)$. Let A be a central simple algebra. Let $K \subset A$ be a subfield containing k such that $\mathcal{Z}_A(K) = K$, then K is called a **maximal subfield** of A.

Theorem 4.1.1. *Let A be a central simple algebra over field k of dimension n^2. Then any maximal subfield K of A is a splitting field of A and $[K : k] = [A : K] = n$. Conversely, given any finite field extension K of k of degree n, any element of* $\mathrm{Br}(K/k)$ *has a unique representative A of degree n^2 which contains K as a maximal subfield.*

For the proof of this theorem we refer to [**P**], Section 13.2 and 14.2. If D is a central division algebra over k of dimension n^2 then there exists a finite Galois extension K of k which is a splitting field for D. Hence

$$\mathrm{Br}(k) = \bigcup_K \mathrm{Br}(K/k)$$

where union is taken over all finite Galois extensions of k. Here we determine the structure of any central simple algebra in the context of the Brauer group ([**P**], Section 14.2).

Proposition 4.1.2. *Let K/k be a Galois extension of fields with Galois group G. Let n be the degree of field extension K/k. Let A be a central simple algebra over k containing K as its maximal subfield. Then there exists $x_\sigma \in A, \forall \sigma \in G$ and $a \colon G \times G \to K^*$, a 2-cocycle, such that $A = \bigoplus_{\sigma \in G} K x_\sigma$ and the multiplication is given by*

$$\alpha x_\sigma . \beta x_\tau = \alpha \sigma(\beta) a_{\sigma,\tau} x_{\sigma\tau}.$$

Conversely we have,

Proposition 4.1.3. *Let K/k be a Galois extension of fields with Galois group G. Let n be the degree of field extension K/k. Let $a \colon G \times G \to K^*$ be a 2-cocycle. We put $A = \bigoplus_{\sigma \in G} K x_\sigma$ and define multiplication as follows :*

$$\alpha x_\sigma . \beta x_\tau = \alpha \sigma(\beta) a_{\sigma,\tau} x_{\sigma\tau}.$$

Then A is a central simple algebra over k containing K as a maximal subfield.

The algebra obtained in this proposition is denoted by $[K, G, a]$. Proposition 4.1.3 provides a surjective map form $\mathscr{Z}^2(G, K^*) \to \mathrm{Br}(K/k)$ defined by $a \mapsto [K, G, a]$. This map induces a group isomorphism of $H^2(G, K^*)$ and $\mathrm{Br}(K/k)$.

Let k be a field. We say k has **cohomological dimension** ≤ 1 (written as $cd(k) \leq 1$) if $\mathrm{Br}(K) = 0$ for every algebraic extension K of k. For k with $cd(k) \leq 1$, let L/K be a finite Galois extension with K algebraic over k, then the norm $N_{L/K} \colon L^* \to K^*$ is surjective ([**Se**], Chapter II, Section 3.1, Proposition 5).

A field k is a C_1 field if every equation $f(x_1, \ldots, x_n) = 0$, where f is a homogeneous polynomial of degree $d \geq 1$, with coefficients in k, has a nontrivial solution in k^n if $n > d$. Let k be a C_1 field. Then every algebraic extension K of k is C_1 and $cd(k) \leq 1$ ([**Se**], Chapter II, Section 3.2, Corollary). A finite field, an extension of transcendence degree 1 of an algebraically closed field are examples of C_1 field. For the notion of C_r fields see [**Se**], Chapter II, Section 4.5.

4.2. Non-Commutative Cohomology

Let G be a group and A a set on which G acts. We denote $s(a) = {}^s a$ for $s \in G$ and $a \in A$. We call A a G-set. If A is a group and the action of G is via automorphisms then we say A is a G-group. We define cohomology groups as follows. Let A be a G-set. Then $H^0(G, A) = A^G = \{a \in A \mid {}^s a = a \ \forall s \in G\}$, set of fixed points of A under the action of G.

A map $a \colon G \to A$ is called a 1-cocycle if

$$a_{st} = a_s {}^s a_t \ (s, t \in G).$$

Two 1-cocycles a and b are equivalent if there exists $c \in A$ such that $b_s = c^{-1} a_s {}^s c$. This is an equivalence relation on the set of 1-cocycles and the quotient group is denoted as $H^1(G, A)$. The set $H^1(G, A)$ need not be a group but it has a distinguished element, namely, the class of 1-cocycles of the form $b^{-1} {}^s b$ for $b \in A$ called the **neutral element or trivial cocycle**.

If A is commutative group we can define higher cohomology groups as defined in Section 4.1.

Example : Let K be a finite Galois extension of k with Galois group $G = \mathrm{Gal}(K/k)$. Let G act on the group $GL_n(K)$ entry wise. Then $H^0(G, GL_n(K)) = GL_n(k)$ and $H^1(G, GL_n(K)) = \{1\}$.

Let A be a G-group. A **principal homogeneous space** or **torsor** for G over A is a non-empty G-set P, on which A acts on the right (compatible with the action of

G) such that $\forall x, y \in P$, there exists a unique $a \in A$ such that $y = x.a$. Then ([**Se**], Chapter I, Section 5.2, Proposition 33),

Proposition 4.2.1. *Let A be a G-group. There is a bijection between the set of classes of principal homogeneous spaces over A and the set $H^1(G, A)$.*

Next we describe the cohomology exact sequence associated to a subgroup. Let A be a subgroup of B which are G-groups. The homogeneous space B/A of left A-cosets of B is a G-set. Then we have ([**Se**], Chapter I, Section 5.4, Proposition 36),

Proposition 4.2.2. *The sequence of pointed sets :*

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, B/A) \xrightarrow{\delta} H^1(G, A) \to H^1(G, B)$$

is exact.

If A is normal in B then the above exact sequence can be extended on its right up to $H^1(G, B/A)$.

4.3. Forms of Algebraic Groups

Let V be a vector space over a field k. Let x be a tensor (1-tensor) on V. Let K be a Galois extension of the field k and G be the Galois group. Then the tensor x can be extended to x_K over $V_K = V \otimes K$. We call (V, x) and (V', x') are **K-isomorphic** if (V_K, x_K) and (V'_K, x'_K) are isomorphic. Let (V, x) be a pair and $E_{(V,x)}(K/k)$ be the set of k isomorphism classes of (V', x') which are K isomorphic to (V, x). Let $A_K = \mathrm{Aut}_K(V_K, x_K)$. Then G acts on V_K by $s.(x \otimes \lambda) = x \otimes s(\lambda)$ for any $s \in G$. The group G acts on A_K as follows:

$$s(f)(x) = s.f(s^{-1}(x)), \quad i.e., \; s(f) = sfs^{-1}.$$

This action on $GL_n(K)$ is same as the entry wise action.

Let us fix (V, x). We compare $E(K/k) = E_{(V,x)}(K/k)$ to $H^1(G, A_K)$. Let $(V', x') \in E(K/k)$ and $f \colon V_K \to V'_K$ be the map giving isomorphism of (V_K, x_K) and (V'_K, x'_K). We define a map $p \colon G \to A_K$ by $s \mapsto f^{-1}s(f) = f^{-1}sfs^{-1}$. It is easy to check that p is a 1-cocycle. We define a map $\theta \colon E(K/k) \to H^1(G, A_K)$ by $\theta(V', x') \mapsto p$ ([**Se**], Chapter III, Section 1.1, Proposition 1).

Proposition 4.3.1. *The map θ is bijective.*

Let us consider a nondegenerate quadratic form $\mathfrak{q}$ as a tensor. Then the set $E(K/k)$ is the set of quadratic forms that are K-isomorphic to $\mathfrak{q}$. The group $A_K =$

$O_K(\mathfrak{q})$, is the orthogonal group of the form over K. We have ([**Se**], Chapter III, Section 1.2, Proposition 4),

Corollary 4.3.2. *The set $H^1(G, O_K(\mathfrak{q}))$ is in bijective correspondence with the set of classes of quadratic k-forms that are K-isomorphic to $\mathfrak{q}$.*

If we take $\mathfrak{b}$ a nondegenerate alternating (symplectic) form as a tensor then we get ([**Se**], Chapter III, Section 1.2, Proposition 3),

Corollary 4.3.3. $H^1(G, Sp_{2n}(\mathfrak{b})) = \{1\}$.

Now we choose V an algebraic variety (e.g. an algebraic group) defined over k. As before we take K an extension of k and denote by A_K the group of K-automorphisms of V_K. Now let K/k be a Galois extension and let V' be a K/k-form of V. The set P of K-isomorphisms of V'_K over V_K is obviously a principal homogeneous space over the Gal(K/k)-group $A(K) = \mathrm{Aut}_V(K)$. Hence we get a canonical map as before ([**Se**], Chapter III, Section 1.3, Proposition 5 and Corollary):

$$\theta \colon E(K/k) \to H^1(K/k, \mathrm{Aut}_V).$$

Proposition 4.3.4. *The map θ is injective. If V is a quasiprojective, it is bijective. Hence if V is an algebraic group, the map θ is bijective.*

Corollary 4.3.5. *The K/k-forms of simple groups of type G_2 is in one-one correspondence with K/k-forms of octonion algebras. Also, K/k-forms of classical groups with trivial center is in one-one correspondence with K/k-forms of semisimple algebras with involution.*

Let Q be a quaternion algebra over k. We associate a group $SL_1(Q)$ to it which is a k-form of SL_2 and the rational points of this group can be identified with the elements of Q with reduced norm 1.

We mention here a theorem about an algebraic group over field with $cd(k) \leq 1$. This theorem is due to Steinberg ([**S1**], Theorem 1.9; [**Se**], Chapter III, Section 2.3, Theorem 1').

Theorem 4.3.6 (Steinberg). *Let k be a perfect field with $cd(k) \leq 1$. Then, $H^1(k, L) = 0$ for every connected linear group L.*

If L is connected reductive group then the assumption that k is a perfect field is not needed in this theorem.

CHAPTER 5

Maximal Tori in SU_n

We need an explicit description of maximal tori in the special unitary group of a nondegenerate hermitian space for our work, we discuss it in this chapter (cf. [**R**], Section 3.4). In fact maximal tori in any classical group can be described in this way. The general theory is known to experts hence we restrict ourself to the specific case. We refer to [**Ka**] for the description of maximal tori in classical groups, in general.

5.1. Description of Maximal Tori

Let k be a field (of characteristic different from 2) and L a quadratic field extension of k. Let V be a vector space of dimension n over L. We denote by k_s a separable closure of k containing L. Let $\mathfrak{h}$ be a nondegenerate hermitian form on V (see Definition 1.1.2). Let $\mathcal{E}$ be an étale algebra (see Definition 3.1.3) over k. It then follows that the bilinear form $T\colon \mathcal{E}\times\mathcal{E}\longrightarrow k$, induced by the trace : $T(x,y)=tr_{\mathcal{E}/k}(xy)$ for $x,y\in\mathcal{E}$, is nondegenerate.

Lemma 5.1.1. *Let L be a quadratic field extension of k. Let $\mathcal{E}$ be an étale algebra over k containing L, equipped with an involution σ, restricting to the non-trivial k-automorphism of L. Let $\mathcal{F}=\mathcal{E}^\sigma=\{x\in\mathcal{E}\mid\sigma(x)=x\}$. Let $\dim_L(\mathcal{E})=n$. For $u\in\mathcal{F}^*$, define*

$$\begin{aligned}\mathfrak{h}^{(u)} &: \mathcal{E}\times\mathcal{E}\longrightarrow L\\ \mathfrak{h}^{(u)}(x,y) &= tr_{\mathcal{E}/L}(ux\sigma(y)).\end{aligned}$$

Then $\mathfrak{h}^{(u)}$ is a nondegenerate σ-hermitian form on $\mathcal{E}$, left invariant by $T_{(\mathcal{E},\sigma)}=\{\alpha\in\mathcal{E}^*\mid\alpha\sigma(\alpha)=1\}$, under the action by left multiplication.

Proof. That $\mathfrak{h}^{(u)}$ is a hermitian form is clear. To check non-degeneracy, let $\mathfrak{h}^{(u)}(x,y)=0\ \forall y\in\mathcal{E}$. Then, $tr_{\mathcal{E}/L}(ux\sigma(y))=0\ \forall y\in\mathcal{E}$, i.e., $tr_{\mathcal{E}/L}(xy')=0\ \forall y'\in\mathcal{E}$. Since $\mathcal{E}$ is étale, it follows that $x=0$. Therefore $\mathfrak{h}^{(u)}$ is nondegenerate. Now let $\alpha\in T_{(\mathcal{E},\sigma)}$. We have,

$$\mathfrak{h}^{(u)}(\alpha x,\alpha y)=tr_{\mathcal{E}/L}(u\alpha x\sigma(\alpha y))=tr_{\mathcal{E}/L}(ux\sigma(y))=\mathfrak{h}^{(u)}(x,y).$$

Hence the last assertion. $\square$

Remark 5.1.2. We note that $\mathcal{E} = \mathcal{F} \otimes_k L$. If we put $\mathcal{F}' = \{x \in \mathcal{E} \mid \sigma(x) = -x\}$ then $\mathcal{E} = \mathcal{F} \oplus \mathcal{F}'$. Further, if $L = k(\gamma)$ with $\gamma^2 \in k^*$, then $\mathcal{F}' = \mathcal{F}\gamma$.

Notation : In what follows, we shall often deal with situations when, for an algebraic group G defined over k, and for any extension K of k, the group $G(K)$ of K-rational points in G coincides with $G(k) \otimes_k K$. When no confusion is likely to arise, we shall abuse notation and use G to denote both the algebraic group, as well as its group of k-points. We shall identify $T_{(\mathcal{E},\sigma)}$ with its image in $U(\mathcal{E}, \mathfrak{h}^{(u)})$, under the embedding via left homotheties.

Lemma 5.1.3. *With notation as in the previous lemma, $T_{(\mathcal{E},\sigma)}$ is a maximal k-torus in $U(\mathcal{E}, \mathfrak{h}^{(u)})$, the unitary group of the hermitian space $(\mathcal{E}, \mathfrak{h}^{(u)})$.*

Corollary 5.1.4. *Let $T^1_{(\mathcal{E},\sigma)} = \{\alpha \in \mathcal{E}^* \mid \alpha\sigma(\alpha) = 1, \det(\alpha) = 1\}$. Then $T^1_{(\mathcal{E},\sigma)} \subset SU(\mathcal{E}, \mathfrak{h}^{(u)})$ is a maximal k-torus.*

Theorem 5.1.5. *Let k be a field and L a quadratic field extension of k. We denote by σ the nontrivial k-automorphism of L. Let V be a L-vector space of dimension n with a nondegenerate σ-hermitian form $\mathfrak{h}$. Let $T \subset U(V, \mathfrak{h})$ be a maximal k-torus. Then there exists $\mathcal{E}_T$, an étale L-algebra of dimension n over L, with an involution $\sigma_{\mathfrak{h}}$ restricting to the nontrivial k-automorphism of L, such that*

$$T = T_{(\mathcal{E}_T,\sigma_{\mathfrak{h}})}.$$

Moreover, if $\mathcal{E}_T$ is a field, there exists $u \in \mathcal{F}^*$ such that $(V, \mathfrak{h})$ is isomorphic to $(\mathcal{E}_T, \mathfrak{h}^{(u)})$ as a hermitian space.

Proof. Let $A = \mathrm{End}_L(V)$. Then A is a central simple L-algebra. Let $\mathcal{E}_T = \mathcal{Z}_A(T)$, the centralizer of T in A. Note that $T \subset \mathcal{E}_T$. The hermitian form $\mathfrak{h}$ defines the adjoint involution $\sigma_{\mathfrak{h}}$ on A (see Section 1.3),

$$\begin{aligned} \sigma_{\mathfrak{h}} \colon A \ &\longrightarrow \ A \\ \mathfrak{h}(\sigma_{\mathfrak{h}}(f)(x), y) \ &= \ \mathfrak{h}(x, f(y)) \end{aligned}$$

for all $x, y \in V$. Then $\sigma_{\mathfrak{h}}$ is an involution of second kind over L/k on A (Definition 1.3.2). We claim that $\sigma_{\mathfrak{h}}$ restricts to $\mathcal{E}_T$: Let $f \in \mathcal{E}_T$, we need to show $\sigma_{\mathfrak{h}}(f) \in \mathcal{E}_T$, i.e., $\sigma_{\mathfrak{h}}(f)t = t\sigma_{\mathfrak{h}}(f) \ \ \forall\, t \in T$. This follows from,

$$\begin{aligned} \mathfrak{h}(\sigma_{\mathfrak{h}}(f)t(x), y) &= \mathfrak{h}(t(x), f(y)) = \mathfrak{h}(x, t^{-1}f(y)) = \mathfrak{h}(x, ft^{-1}(y)) \\ &= \mathfrak{h}(\sigma_{\mathfrak{h}}(f)(x), t^{-1}y) = \mathfrak{h}(t\sigma_{\mathfrak{h}}(f)(x), y). \end{aligned}$$

We have $T \subset U(V, \mathfrak{h}) \subset \mathrm{End}_L(V)$ and $\sigma_{\mathfrak{h}}$ is an involution on $\mathrm{End}_L(V)$, restricting to the nontrivial k-automorphism of L. There is a canonical isomorphism of algebras with involutions ([**KMRT**], Chapter I, Proposition 2.15),

$$(\mathrm{End}_L(V) \otimes_k k_s, \sigma_{\mathfrak{h}}) \cong (\mathrm{End}_{k_s}(V) \times \mathrm{End}_{k_s}(V), \epsilon),$$

where $\epsilon(A, B) = (B, A)$. Since $U(V, \mathfrak{h}) = \{A \in \mathrm{End}_L(V) \mid A\sigma_{\mathfrak{h}}(A) = 1\}$, we have,

$$\begin{aligned} U(V, \mathfrak{h}) \otimes_k k_s &\cong \{(A, B) \in \mathrm{End}_L(V) \otimes_k k_s \mid (A, B).\epsilon(A, B) = 1\} \\ &= \{(A, A^{-1}) \mid A \in \mathrm{End}_{k_s}(V)\}. \end{aligned}$$

We thus have an embedding

$$T \otimes_k k_s \longrightarrow \mathrm{End}_{k_s}(V) \times \mathrm{End}_{k_s}(V), \ A \mapsto (A, A^{-1}).$$

To prove $\mathcal{E}_T$ is étale, we may conjugate $T \otimes k_s$ to the diagonal torus in $GL_n(k_s)$. The embedding then becomes,

$$T \otimes_k k_s \cong (k_s^*)^n \longrightarrow M_n(k_s) \times M_n(k_s),$$

$$(t_1, \ldots, t_n) \mapsto (\mathrm{diag}(t_1, \ldots, t_n), \mathrm{diag}(t_1^{-1}, \ldots, t_n^{-1})).$$

Now, we have,

$$\begin{aligned} \mathcal{E}_T \otimes_k k_s = \mathcal{Z}_A(T) \otimes_k k_s &= \mathcal{Z}_{A \otimes_k k_s}(T \otimes_k k_s) \\ \cong \mathcal{Z}_{M_n(k_s) \times M_n(k_s)}\big(\{(\mathrm{diag}(t_1, \ldots, t_n), \mathrm{diag}(t_1^{-1}, \ldots, t_n^{-1})) &\mid t_i \in k_s^*\}\big) = k_s^{2n}. \end{aligned}$$

Hence $\mathcal{E}_T$ is an étale algebra of k-dimension $2n$ and L-dimension n. We have, $T \subset T_{(\mathcal{E}_T, \sigma_{\mathfrak{h}})}$ and, by dimension count, $T = T_{(\mathcal{E}_T, \sigma_{\mathfrak{h}})}$. We have on V, the natural left $\mathrm{End}_L(V)$-module structure. Since $\mathcal{E}_T$ is a subalgebra of $\mathrm{End}_L(V)$ and a field, V is a left $\mathcal{E}_T$-vector space of dimension 1. Let $V = \mathcal{E}_T.v$ for $v \neq 0$. Let us consider the dual $V^* = \mathrm{Hom}_L(V, L)$, which is a left-$\mathcal{E}_T$-vector space of dimension 1 via the action: $(\alpha.f)(x) = f(\alpha(x)), \ \alpha \in \mathcal{E}_T, \ x \in V$. We consider the following elements in V^*:

$$\begin{aligned} \phi_1 \quad : \quad & V = \mathcal{E}_T.v \longrightarrow L \\ & fv \mapsto \mathfrak{h}(f(v), v) \\ \phi_2 \quad : \quad & V = \mathcal{E}_T.v \longrightarrow L \\ & fv \mapsto tr(f). \end{aligned}$$

Since $\mathcal{E}_T$ is separable, both these are nonzero elements of V^*. Hence there exists $u \in \mathcal{E}_T^*$ such that $\mathfrak{h}(f(v), v) = tr(uf) \ \forall f \in \mathcal{E}_T$. We have,

$$\mathfrak{h}(f.v, g.v) = \mathfrak{h}(f(v), g(v)) = \mathfrak{h}(\sigma_{\mathfrak{h}}(g)f(v), v) = tr(u\sigma_{\mathfrak{h}}(g)f) \ \forall f, g \in \mathcal{E}_T.$$

This will prove the theorem provided we show $u \in F$. For any $f \in \mathcal{E}_T$ we have,

$$tr(\sigma_{\mathfrak{h}}(u)f) = tr(\sigma_{\mathfrak{h}}(u).\sigma_{\mathfrak{h}}(\sigma_{\mathfrak{h}}(f))) = \sigma_{\mathfrak{h}}(tr(u\sigma_{\mathfrak{h}}(f)))$$
$$= \sigma_{\mathfrak{h}}(\mathfrak{h}(\sigma_{\mathfrak{h}}(f)(v), v)) = \mathfrak{h}(v, \sigma_{\mathfrak{h}}(f)(v)) = \mathfrak{h}(f(v), v) = tr(uf).$$

Since $\mathcal{E}_T$ is separable, the trace form is nondegenerate and hence $\sigma_{\mathfrak{h}}(u) = u$. The map

$$\Phi\colon (V, \mathfrak{h}) \longrightarrow (\mathcal{E}_T, \mathfrak{h}^{(u)}),\ fv \mapsto f$$

is an isometry:

$$\mathfrak{h}^{(u)}(\Phi(fv), \Phi(gv)) = tr(u\sigma_{\mathfrak{h}}(g)f) = \mathfrak{h}(fv, gv)$$

by the computation done above. □

Corollary 5.1.6. *Let the notation be as fixed above. Let T be a maximal torus in $SU(V, \mathfrak{h})$. Then there exists an étale algebra $\mathcal{E}_T$ over L of dimension n, such that $T \cong T^1_{(\mathcal{E}_T, \sigma_{\mathfrak{h}})}$.*

Remark 5.1.7. The hypothesis in the last assertion in Theorem 5.1.5, that $\mathcal{E}_T$ be a field, is only a simplifying assumption. The result holds good even when $\mathcal{E}_T$ is not a field.

Let $T \subset SU(V, \mathfrak{h})$ be a maximal torus. Then from the proof of Theorem 5.1.5 we see that $\mathcal{E}_T = \mathcal{Z}_{\mathrm{End}(V)}(T')$ is an étale algebra with involution $\sigma_{\mathfrak{h}}$ such that $T = T^1_{(\mathcal{E}_T, \sigma_{\mathfrak{h}})}$, here T' is a maximal torus in $U(V, \mathfrak{h})$.

5.2. Tori and Representations

We continue here with notation introduced in the previous section.

Lemma 5.2.1. *With notation as above, V is an irreducible representation of T if and only if $\mathcal{E}_T$ is a field.*

Proof. Suppose $\mathcal{E}_T$ is not a field. Then $\exists 0 \neq f \in \mathcal{E}_T$ such that $V \neq ker(f) \neq 0$. Put $W = ker(f) \subset V$, which is a L-vector subspace. We claim that W is a T invariant subspace. Let $x \in W, t \in T$.

$$f(x) = 0 \Rightarrow t(f(x)) = 0 \Rightarrow f(t(x)) = 0 \Rightarrow t(x) \in W.$$

Hence, $T(W) = W$.

Conversely, let $\mathcal{E}_T$ be a field and $0 \neq W \subset V$ be a T-invariant L-subspace of V. We shall show that $V = W$. We know that V is a one dimensional $\mathcal{E}_T$ vector space. Thus, it suffices to show that W is an $\mathcal{E}_T$ subspace of V. Suppose first that k is infinite. Let $t \in T(k)$ be a regular element (see [**Bo**], Proposition 8.8 and the Remark on Page 116). Then $\mathcal{E}_T = L[t]$ and we have, for $f(t) \in \mathcal{E}_T$, $f(t)(W) = W$, since W is T-invariant. Now let k be finite. Then $\mathcal{E}_T$ is a finite field and its multiplicative group $\mathcal{E}_T^*$ is cyclic. The group $T(k)$, being a subgroup of $\mathcal{E}_T^*$, is cyclic. Then a cyclic generator t of $T(k)$ is a regular element and arguing as above, we are done in this case too. □

We call a torus **indecomposable** if it can not be written as a direct product of subtori.

Corollary 5.2.2. *Let T be a maximal torus in $SU(V, \mathfrak{h})$. Then T is indecomposable if and only if V is an irreducible representation of T. That is if and only if $\mathcal{E}_T$ is a field.*

Proof. By the above lemma, if V is reducible as a representation of T, $\mathcal{E}_T$ is not a field. Hence it must be a product of at least two (separable) field extensions of L, say $\mathcal{E}_T = E_1 \times \ldots \times E_r$. Then from Corollary 5.1.6, $T = T^1_{\mathcal{E}_T} = T^1_{E_1} \times \ldots \times T^1_{E_r}$. Hence T is decomposable. Conversely, suppose V is irreducible as a representation of T. Then, by the above lemma, $\mathcal{E}_T$ is a field. Suppose the torus T decomposes as $T = T_1 \times T_2$ into a direct product of two proper subtori. Suppose first that k is infinite. Let $t \in T(k)$ be a regular element (see [**Bo**], Proposition 8.8 and the Remark on Page 116). Then the minimal polynomial (= characteristic polynomial) $\chi(X)$ of t factorizes over k, as can be seen by base changing to k_s and conjugating T to the diagonal torus in $SL(n)$. Therefore $\mathcal{E}_T = L[X]/\chi(X)$ is not a field, a contradiction. Hence T is indecomposable. When k is finite, the multiplicative group $\mathcal{E}_T^*$ of $\mathcal{E}_T$ is cyclic and hence $T(k)$ is cyclic. A cyclic generator t of $T(k)$ is then regular and we repeat the above argument to reach a contradiction. Hence T is indecomposable. □

With this we move on to pose the main question of the thesis and describe the results proved in this thesis along with known results.

CHAPTER 6

Main Results

In this chapter we discuss the main problem addressed in this thesis. We mention known results and theorems proved in this thesis. Proof of the theorems will follow in later chapters. The results proved in this thesis are titled "Theorem" in this chapter. Results which were known are attributed to the respective author(s) with label "Proposition". I appologise for this convention, though limited to this chapter only.

Let G be an algebraic group defined over a field k. It is desirable, from the representation theoretic point of view, to study conjugacy classes of elements in G. We call an element $g \in G$ **real** if there exists $h \in G$ such that $hgh^{-1} = g^{-1}$. An element $g \in G(k)$ is called **k-real** if there exists $h \in G(k)$ such that $hgh^{-1} = g^{-1}$. We address the following problem in this thesis:

Problem: Characterize real elements of the group $G(k)$.

An **involution** in G is an element g with $g^2 = 1$. Note that with our convention the identity element is also an involution. An element in G is called **strongly real** if it is a product of two involutions in G. We raise the following question here.

Problem: Let $g \in G(k)$ be a k-real element. Is g strongly k-real in $G(k)$?

Note that a strongly k-real element in $G(k)$ is always k-real in $G(k)$. Conversely, a real element $g \in G(k)$ is strongly k-real if and only if there exists a conjugating element in $G(k)$ which is an involution, i.e., there exists $t \in G(k)$ with $t^2 = 1$ such that $tgt^{-1} = g^{-1}$. This remark is very useful in investigating the structure of real elements.

It is worth mentioning that the characterization of real elements depends on the base field. We will give examples of elements in a group G of type G_2 which are not k-real but are strongly real over $\bar{k}$. We note that every element of a conjugacy class which contains a real element is real. Such a conjugacy class is called a **real conjugacy class**. For finite groups, the number of real conjugacy classes is same as the number of real irreducible characters. Let G be a finite group. A complex representation of G is realizable if it is defined over $\mathbb{R}$. It is obvious that a character corresponding to a realizable representation is real. An irreducible character χ is real if and only if there is a non-zero G-invariant bilinear form on the representation space V. A representation V of G is called **orthogonal (symplectic)** if there exists a non-zero symmetric (skew-symmetric) bilinear form on V which is G-invariant. In fact, an irreducible real character comes from a realizable representation if and only if the representation V is orthogonal ([**JL**], Theorem 23.16). Hence our problem seems to be directly related to the representation theory of G. For a semisimple algebraic group, there exists an involution h in the center, which acts by 1 in an irreducible self-dual representation if and only if the representation is orthogonal. For most of the groups studied in this thesis, we prove that real semisimple elements are strongly real. If one compares these results to the results proved in [**Pr1**] and [**Pr2**], these are exactly the groups for which irreducible, self dual representations are orthogonal. For more discussion and explicit references on the connection to representation theory we refer the reader to Section 10.1.

6.1. Results in Classical Groups

Reality for classical groups over fields of characteristic not 2 has been studied in [**MVW**] by Moeglin, Vignéras and Waldspurger.

The following result is due to Wonenburger ([**W1**], Theorem 1).

Proposition 6.1.1. *An element of $GL_n(k)$ is real if and only if it is strongly real in $GL_n(k)$.*

However, a similar result is false for matrices over division algebras. In [**El1**] (Lemma 2 and Lemma 3) Ellers constructs an example of a simple transformation of a vector space V over the real quaternion division algebra $\mathbb{H}$, which is conjugate to its inverse but is not strongly real. This is also evident by looking at the real quaternion division algebra $\mathbb{H} = \mathbb{R}.1 \oplus \mathbb{R}.i \oplus \mathbb{R}.j \oplus \mathbb{R}.ij$ where i, j, k have usual meanings. In the group $GL_1(\mathbb{H})$, the element i is conjugate to its inverse by j which satisfies $j^2 = -1$. The only nontrivial element of $GL_1(\mathbb{H})$ which is an involution is -1 and hence i is not a product of two involution in $GL_1(\mathbb{H})$. For $SL_n(k)$, we prove,

Theorem 6.1.2. *Let V be a vector space of dimension n over k. Let $t \in SL(V)$. Suppose $n \not\equiv 2 \pmod 4$. Then t is real in $SL(V)$ if and only if t is strongly real in $SL(V)$.*

We show by examples that the result fails when $n \equiv 2 \pmod 4$.

We now consider the group $SL_1(Q) = \{x \in Q^* \mid \mathrm{Nrd}(x) = 1\}$, for a quaternion algebra Q over k. A quaternion algebra Q is a central simple algebra over k of degree 2. We note that $SL_1(Q)$ is a form of SL_2 over k in the sense defined in Section 4.3. We denote the group $SL_1(Q)/\mathcal{Z}(SL_1(Q))$ by $PSL_1(Q)$.

Theorem 6.1.3. *With notation as above, let $G = PSL_1(Q)$ and $t \in G$ be a semisimple element. Then, t is real in $PSL_1(Q)$ if and only if t is strongly real in $PSL_1(Q)$. Furthermore, $SL_1(Q)$ has real elements which are not strongly real.*

One can consider the matrix algebra $M_2(k)$ as a quaternion algebra and the group under consideration in this case is $G = PSL_2(k)$. Hence we see that a semisimple element $t_0 \in PSL_2(k)$ is real in $PSL_2(k)$ if and only if t_0 is a product of two involutions in $PSL_2(k)$.

We continue our investigation for D, a central division algebra of odd degree n over a field k. Let $G = D^*$ or $G = SL_1(D) = \{x \in D^* \mid \mathrm{Nrd}(x) = 1\}$. Then,

Theorem 6.1.4. *Let G be as above. Then the only real elements in G are ± 1.*

In fact, using this theorem we prove that $\mathrm{Iso}(D, \sigma)$ has no nontrivial real elements. For σ of the first kind, $\mathrm{Iso}(D, \sigma)$ is a form of orthogonal group and for σ of the second kind, it is a form of unitary group.

Let V be a vector space over k with a nondegenerate quadratic form $\mathfrak{q}$. We denote the orthogonal group by $O(\mathfrak{q})$. Then Wonenburger proved ([**W1**], Theorem 2),

Proposition 6.1.5. *Any element of the orthogonal group $O(\mathfrak{q})$ is a product of two involutions, i.e., the group $O(\mathfrak{q})$ is bireflectional. Hence every element of $O(\mathfrak{q})$ is strongly real.*

Djoković extended this result ([**D**], Theorem 1) to fields of characteristic 2. However, Knüppel and Nielsen proved ([**KN**], Theorem A),

Proposition 6.1.6. *The group $SO(\mathfrak{q})$ is trireflectional. It is bireflectional if* $\dim(V) \not\equiv 2 \pmod 4$ *and hence every element is strongly real in that case.*

They give necessary and sufficient condition for an element in the special orthogonal group to be a product of two involutions ([**KN**], Proposition 3.3). However, we classify semisimple real elements in $SO(\mathfrak{q})$ without any restriction on dimension.

Theorem 6.1.7. *Let $t \in SO(\mathfrak{q})$ be a semisimple element. Then, t is real in $SO(\mathfrak{q})$ if and only if t is strongly real in $SO(\mathfrak{q})$.*

Feit and Zuckermann discuss reality for spin groups in [**FZ**] (Corollary D). They prove,

Proposition 6.1.8. *Let F be an algebraically closed field. Let $(V, \mathfrak{q})$ be an n-dimensional quadratic space. Suppose n is odd. Then, every element in $Spin(\mathfrak{q})$ is real in $Spin(\mathfrak{q})$.*

Let V be a vector space of dimension $2n$ with a symplectic form. We denote the corresponding symplectic group by $Sp(2n, k)$. Let $Sp^{\pm}(2n, q)$ be the group consisting of symplectic and skew-symplectic isometries. Feit and Zuckermann proved ([**FZ**], Theorem E).

Proposition 6.1.9. *Let $F = \mathbb{F}_q$ be a finite field. Then,*

(i) *If $q \equiv 1 \pmod 4$ then every element of $Sp(2n, q)$ is real.*
(ii) *If $q \equiv 3 \pmod 4$ then every element of $Sp(2n, q)$ is real in $Sp^{\pm}(2n, q)$.*

Wonenburger proved ([**W1**], Theorem 2),

Proposition 6.1.10. *Any element of $Sp(2n, k)$ is a product of two skew-symplectic involutions.*

That every element of a symplectic group over fields of characteristic 2 is a product of two involutions is settled in [**Ni**]. Recently Vinroot ([**V**], Theorem 2) proved for $GSp(2n, k)$ over k with characteristic $\neq 2$,

Proposition 6.1.11. *Let $g \in GSp(2n, k)$ with similitude factor $\mu(g) = \beta$. Then $g = t_1 t_2$, where t_1 is a skew-symplectic involution and t_2 is such that $\mu(t_2) = -\beta$ with $t_2^2 = \beta I$.*

The center of $Sp(2n, k)$ is $\mathcal{Z}(Sp(2n, k)) = \{\pm 1\}$. We denote the projective symplectic group by $PSp(2n, k) = Sp(2n, k)/\mathcal{Z}(Sp(2n, k))$. We prove,

Theorem 6.1.12. *Let $t \in Sp(2n, k)$ be a semisimple element. Suppose t is either conjugate to t^{-1} or $-t^{-1}$. Then the conjugation can be achieved by an element $s \in Sp(2n, k)$ such that $s^2 = -1$. Hence a semisimple element of $PSp(2n, k)$ is real if and only if it is strongly real in $PSp(2n, k)$.*

We give an example of a symplectic transformation which can not be written as a product of two involution but is a real element.

We now determine real semisimple elements in unitary groups. Let K be a quadratic extension of k.

Theorem 6.1.13. *Let $(V, \mathfrak{h})$ be a hermitian space over K. Let $t \in U(V, \mathfrak{h})$ be a semisimple element. Then, t is real in $U(V, \mathfrak{h})$ if and only if it is strongly real.*

We also prove similar results for special unitary groups.

Theorem 6.1.14. *Let $t \in SU(V, \mathfrak{h})$ be semisimple. Suppose $n \not\equiv 2 \pmod 4$. Then t is real in $SU(V, \mathfrak{h})$ if and only if it is strongly real.*

Remark 6.1.15. We exhibit real unipotent elements in $SU(V, \mathfrak{h})$ which are not strongly real in $U(V, \mathfrak{h})$.

6.2. Results in Exceptional Groups

We now begin the study of reality properties for exceptional groups. In this thesis, we have tackled groups of type G_2 over fields of characteristic different from 2. We prove reality implies strong reality for all elements in these groups except for unipotent elements over fields of characteristic 3. One expects similar results for exceptional groups of type E_8 and F_4 as well, which is evident from Theorem 6.3.2 and Theorem 6.3.3. By consulting the character table of G_2 over finite fields in [**CR**], one sees that reality is not true for arbitrary elements of G_2 (see also Theorem 8.4.6 and Theorem 8.4.7, in this thesis). Let G be a group of type G_2 over a field k of characteristic $\neq 2$. We prove,

Theorem 6.2.1. *In addition, if $char(k) \neq 3$, every unipotent element in $G(k)$ is strongly real in $G(k)$.*

For a general element in $G(k)$, we prove,

Theorem 6.2.2. *Let characteristic $k \neq 2, 3$. Then, an element $t \in G(k)$ is real in $G(k)$ if and only if t is strongly real in $G(k)$.*

The assumption $char(k) \neq 3$ is needed only for the case of unipotents. Real semisimple elements are strongly real in $G(k)$ for any field k, $char(k) \neq 2$. We call a torus in G **indecomposable** if it can not be written as a direct product of two subtori, **decomposable** otherwise. We show that semisimple elements in decomposable tori are always real (Theorem 8.1.9). We construct examples of indecomposable tori in G containing non-real elements (Proposition 8.4.2 and Theorem 8.4.5).

We work with an explicit realization of a group of type G_2 as the automorphism group of an octonion algebra. It is known ([**Se**], Chapter III, Proposition 5, Corollary) that for a group G of type G_2 over k, there exists an octonion algebra $\mathfrak{C}$ over k, unique up to a k-isomorphism, such that $G \cong \mathrm{Aut}(\mathfrak{C})$, the group of k-algebra automorphisms of $\mathfrak{C}$. The group G is k-split if and only if the octonion algebra $\mathfrak{C}$ is split, otherwise G is anisotropic and $\mathfrak{C}$ is necessarily a division algebra. We prove,

Theorem 6.2.3. *Any element which is not unipotent in $G(k)$ either leaves invariant a quaternion subalgebra or fixes a quadratic étale subalgebra of $\mathfrak{C}$ pointwise.*

This is Lemma 8.1.3 in the thesis. We discuss reality for G_2 over special fields (Proposition 8.4.2, Theorem 8.4.5 and Theorem 8.4.6). We show that nonreal elements exists in G_2 over k finite, with characteristic k not 2 or 3 (compare with [**CR**]), these are neither semisimple nor unipotent.

As a result of our investigation for groups of type G_2 we also get information about conjugacy classes in such groups. We put this in general frame work of algebraic groups and describe the results obtained. Let G be an algebraic group defined over a field k. Let X be a G-space. Two elements $x, y \in X$ are said to have **same orbit type** if the isotropy subgroups G_x and G_y are conjugate. Let G be a compact Lie group acting on a compact manifold M. It was conjectured by Montgomery ([**Ei**], Problem 45) that there are only finitely many orbit types. Floyd proved that if G is a torus acting on a compact orientable manifold then there are only a finite number of distinct isotropy subgroups ([**F**], 4.5). Using the results of Floyd, Mostow ([**M**], Theorem) proved that when G is a compact Lie group acting on a compact manifold M then there are at most a finite number of inequivalent orbits. One can consider the action of a group G on itself by conjugation and ask for orbit types. Rony Gouraige studied conjugacy classes of centralizers in $M_n(D)$ (the algebra of endomorphisms of a finite dimensional vector space over a central division algebra) in his thesis submitted at City University of New York in 2004.

In this thesis we calculate conjugacy classes of centralizers of elements for anisotropic groups of type G_2 over a field of characteristic $\neq 2$. Anisotropic groups of type G_2 over k are given by automorphisms of octonion division algebras over k. We specifically calculate conjugacy classes of centralizers for compact G_2 (anisotropic G_2 over $\mathbb{R}$) and prove,

Theorem 6.2.4. *Let G be the anisotropic group of type G_2 over $\mathbb{R}$. Then there are exactly five orbit types (conjugacy classes of centralizers).*

6.3. Results in Algebraic Groups

Motivated by several results obtained above we have investigated the structure of real elements in general algebraic groups. We would like to mention the work of Tiep and Zalesski (refer [**TiZ**]) in this connection. They look at a slightly different question. They were interested in classifying groups in which all elements are real. They have successfully classified ([**TiZ**], Theorem 1.2) finite quasi-simple groups in which all elements are real. They also look at the question of all unipotent elements being real in simple, simply connected algebraic group over a finite field. However, it is worth mentioning a theorem about simple algebraic group proved in that paper.

Proposition 6.3.1. *Let G be a simple algebraic group over an algebraically closed field of characteristic $p \neq 0$. All elements of G are real if and only if G is of type B_n, C_n, D_{2n}, G_2, F_4, E_7 or E_8.*

We look to characterize real elements in somewhat the same class of groups considered by Tiep and Zalesskii but over an arbitrary base field k (not just over algebraically closed field). An element t in a connected linear algebraic group G is called **regular** if its centralizer $\mathcal{Z}_G(t)$ has minimal dimension among all centralizers. An element is called **strongly regular** if its centralizer in G is a maximal torus. We prove,

Theorem 6.3.2. *Let G be a connected simple group of adjoint type defined over k. Suppose the longest element w_0 of the Weyl group W of G with respect to a maximal k-torus T acts by -1 on the roots. Let $t \in G(k)$ be a strongly regular element. Then t is k-real in $G(k)$ if and only if t is strongly k-real in $G(k)$. Moreover, if $T(k)$ contains a strongly regular element, then every element of $T(k)$ is strongly real in $G(k)$.*

We study the question for semisimple elements in groups over fields of $cd(k) \leq 1$ and prove,

Theorem 6.3.3. *Let k be a field with $cd(k) \leq 1$. Let G be a simple adjoint group defined over k. Suppose that the longest element w_0 in the Weyl group of G with respect to a maximal torus T acts as -1 on the roots. Then every semisimple element in $G(k)$ is strongly real in $G(k)$.*

We devote next three chapters for the proofs of the theorems mentioned here.

CHAPTER 7

Reality in Classical Groups

In this chapter we discuss structure of real elements in classical groups. These groups have been described in Chapter 1. We prove the results mentioned in Section 6.1. The results in this section are part of [**ST2**].

7.1. The Groups $GL_n(k)$ and $SL_n(k)$

We begin by recording a theorem of Wonenburger ([**W1**], Theorem 1) for GL_n, which, in fact, is the motivating example for our results.

Proposition 7.1.1. *An element of $GL_n(k)$ is real if and only if it is strongly real in $GL_n(k)$.*

In this section we explore the structure of real elements in $SL_n(k)$. We follow the proof of Wonenburger for $GL_n(k)$ ([**W1**], Theorem 1) and modify it for our purpose.

Theorem 7.1.2. *Let V be a vector space of dimension n over k. Let $t \in SL(V)$. Suppose $n \not\equiv 2 \pmod 4$. Then t is real in $SL(V)$ if and only if t is strongly real in $SL(V)$.*

Proof. Let $\delta_1(X), \ldots, \delta_n(X)$ be the invariant factors of t in $k[X]$. Since t is real, each $\delta_i(X)$ is self-reciprocal. The space V decomposes as $V = \oplus_{i=1}^n V_i$, where each V_i is a cyclic, t invariant subspace of V and the minimal polynomial of $t_i = t|_{V_i}$ is the self-reciprocal polynomial $\delta_i(X)$. We shall construct involutions H_i in $GL(V_i)$, conjugating t_i to t_i^{-1}, with $\det(H_i) = (-1)^m$ if dimension of $V_i = 2m$ and $\det(H_i) = (-1)^m$ or $(-1)^{m+1}$ when dimension of $V_i = 2m+1$. We then take $H = \oplus_{i=1}^n H_i$. Then H is an involution conjugating t to t^{-1} and $\det(H) = 1$ if $\dim(V) \not\equiv 2 \pmod 4$.

Now t_i is a cyclic linear transformation on the vector space V_i with characteristic polynomial $\chi_{t_i}(X) = \delta_i(X)$ self-reciprocal. We can write $\chi_{t_i}(X) = (X-1)^r(X+1)^s f(X)$ where $f(\pm 1) \neq 0$ and $V_i = W_{-1} \oplus W_1 \oplus W_0$, where W_{-1}, W_1 and W_0 are the kernels of $(t_i - 1)^r, (t_i+1)^s$ and $f(t_i)$ respectively. To produce the involution H_i on V_i as above, it suffices to do so on each of W_{-1}, W_1 and W_0. Hence it is enough to consider the following cases. Let S be a cyclic linear transformation on a vector space W with self reciprocal characteristic polynomial $\chi_S(X)$, of the following two kinds;

(1) the degree of $\chi_S(X)$ is even, say $2m$,
(2) $\chi_S(X) = (X-1)^{2m+1}$ or $(X+1)^{2m+1}$.

We claim that in the first case S is conjugate to S^{-1} by an involution whose determinant is $(-1)^m$. And in the second case there are involutions with determinant $(-1)^m$ or $(-1)^{m+1}$ conjugating S to S^{-1}.

Case 1. Since W is cyclic, there is a vector $u \in W$ such that $\mathcal{E} = \{u, Su, \ldots, S^{2m-1}u\}$ is a basis of W. By substituting $S^m u = y$ we get $\mathcal{E} = \{S^{-m}y, \ldots, y, \ldots, S^{m-1}y\}$. Let

$$\mathcal{B} = \{y, (S+S^{-1})y, \ldots, (S^{m-1}+S^{-m+1})y, (S-S^{-1})y, \ldots, (S^m - S^{-m})y\}.$$

Then $\mathcal{B}$ is a basis of W. We denote the subspace generated by the first m vectors of $\mathcal{B}$ by P and the latter m vectors by Q. Then $S+S^{-1}$ leaves P as well as Q invariant. Also $(S-S^{-1})(P) = Q$ and $(S-S^{-1})(Q) \subset P$. Let $H = 1|_P \oplus -1|_Q$. Then H is an involution which conjugates S to S^{-1} and has determinant $(-1)^m$.

Case 2. In this case, we have the characteristic polynomial $\chi_S(X) = (X-\epsilon)^{2m+1}$ where $\epsilon = \pm 1$. Since W is cyclic, there is a vector $u \in W$ such that $\mathcal{E} = \{u, Su, \ldots, S^{2m}u\}$ is a basis. By substituting $S^m u = y$ we get $\mathcal{E} = \{S^{-m}y, \ldots, y, \ldots, S^m y\}$. As in the previous case, we consider the basis

$$\mathcal{B} = \{y, (S+S^{-1})y, \ldots, (S^m+S^{-m})y, (S-S^{-1})y, \ldots, (S^m - S^{-m})y\}.$$

We denote the subspace generated by the first $m+1$ vectors of $\mathcal{B}$ by P and the latter m vectors by Q. Then $S+S^{-1}$ leaves P as well as Q invariant. Also $(S-S^{-1})(P) \subset Q$ and $(S-S^{-1})(Q) \subset P$. We consider $H_1 = 1|_P \oplus -1|_Q$ and $H_2 = -1|_P \oplus 1|_Q$. Then H_1 and H_2 both are involutions which conjugate S to S^{-1} and have determinants $(-1)^m$ and $(-1)^{m+1}$ respectively. □

Remarks 7.1.3. 1. An element $S = \mathrm{diag}(\alpha, \alpha^{-1}, \beta, \beta^{-1}, \gamma, \gamma^{-1}) \in SL_6(k)$ such that all the diagonal entries are distinct, can be conjugated to its inverse by

$$H = \mathrm{diag}\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) \in SL_6(k)$$

where $H^2 = -1$. In fact any element $T \in SL_6(k)$ such that $TST^{-1} = S^{-1}$ is of the form:

$$T = \mathrm{diag}\left(\begin{pmatrix} 0 & a \\ \tilde{a} & 0 \end{pmatrix}, \begin{pmatrix} 0 & b \\ \tilde{b} & 0 \end{pmatrix}, \begin{pmatrix} 0 & c \\ \tilde{c} & 0 \end{pmatrix}\right)$$

where $a\tilde{a}b\tilde{b}c\tilde{c} = -1$. Suppose $T^2 = 1$. Then $a\tilde{a} = 1, b\tilde{b} = 1, c\tilde{c} = 1$. This implies that $a\tilde{a}b\tilde{b}c\tilde{c} = 1$, a contradiction. Hence there is no involution in $SL_6(k)$ conjugating S to S^{-1}, i.e., S is real semisimple but not strongly real in $SL_6(k)$.

2. Let us take $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, a unipotent element in $SL_2(k)$. Then any element $X \in GL_2(k)$ such that $XAX^{-1} = A^{-1}$ has the form $X = \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix}$. Then, A is conjugate to A^{-1} in $SL_2(k)$ if and only if -1 is a square in k. In that case (-1 is a square in k) the element X which conjugates A to its inverse satisfies $X^2 = -1$, not an involution, and hence A is not strongly real in $SL_2(k)$.

7.2. Groups of Type A_1

In this section we study real semisimple elements in $SL_2(k)$ and $PSL_2(k) = SL_2(k)/\mathcal{Z}(SL_2(k))$. We fix an algebraic closure $\bar{k}$ of k. Let $G = SL_2(\bar{k})$. We fix the maximal torus $T = \{\text{diag}(\alpha, \alpha^{-1}) \mid \alpha \in \bar{k}^*\}$ in G.

Lemma 7.2.1. *With notation as above, every semisimple element of $G = SL_2(\bar{k})$ is real in G. The only involutions in G are $\{I, -I\}$, hence non-central semisimple elements are not a product of involutions. Moreover, every semisimple element of G is conjugate to its inverse by an involution in $GL_2(\bar{k})$, hence is strongly real in $GL_2(\bar{k})$.*

Proof. Let $t \in SL_2(\bar{k})$ be semisimple. First, assume that $t = \text{diag}(\alpha, \alpha^{-1}) \in T$. Let $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\bar{k})$. Then $g^2 = -1$ and

$$gtg^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} = t^{-1}.$$

Hence, for any $t \in T$, $gtg^{-1} = t^{-1}$.

Now let $n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then we have, for any $t \in T$, $ntn^{-1} = t^{-1}$ and n is an involution with $\det(n) = -1$. Hence, for any $t \in T$, we have $t = n.nt$, a product of two involutions in $GL_2(\bar{k})$. Now, if $s \in SL_2(\bar{k})$ is semisimple then $gsg^{-1} \in T$ for some $g \in SL_2(\bar{k})$. If $gsg^{-1} = \rho_1\rho_2$, $\rho_i \in GL_2(\bar{k}), \rho_i^2 = 1$, then $s = g^{-1}\rho_1 g.g^{-1}\rho_2 g$, and $g^{-1}\rho_i g$ are involutions in $GL_2(\bar{k})$. □

Corollary 7.2.2. *Let $G = PSL_2(\bar{k})$ and t be a semisimple element in G. Then t is real in G if and only if t is strongly real in G.*

Proof. Let $t \in PSL_2(\bar{k})$ be a real semisimple element. Let $t_0 \in SL_2(\bar{k})$ be a representative of t. Then t_0 is either conjugate to t_0^{-1} or $-t_0^{-1}$ in $SL_2(\bar{k})$. When t_0 is conjugate to t_0^{-1}, it follows from the previous lemma that there exists an element $s \in SL_2(\bar{k})$ with $s^2 = -1$ such that $st_0s^{-1} = t_0^{-1}$. Hence we can write $t_0 = (-s).(st_0)$, which writes t as a product of two involutions in $PSL_2(\bar{k})$.

Now suppose t_0 is conjugate to $-t_0^{-1}$ in $SL_2(\bar{k})$. Then the characteristic polynomial of t_0 is $X^2 + 1$. In this case t itself is an involution in $PSL_2(\bar{k})$. □

We record an interesting fact about semisimple elements in $SL_2(k)$.

Lemma 7.2.3. *Let $t \in SL_2(k)$ be a semisimple element. Then t is either strongly regular or central in $SL_2(k)$.*

Proof. It is enough to prove this over $\bar{k}$. Let $t \in SL_2(\bar{k})$ be a semisimple element. If t is central then t is either I or $-I$. Hence we may assume t is a non-central element. Then, up to conjugation in $SL_2(\bar{k})$, we have $t = \mathrm{diag}(\alpha, \alpha^{-1})$, where $\alpha^2 \neq 1$. Then $\mathcal{Z}_{SL_2(\bar{k})}(t) = \{\mathrm{diag}(\gamma, \gamma^{-1}) \mid \gamma \in \bar{k}^*\}$, a maximal torus in $SL_2(\bar{k})$. Hence t is strongly regular (i.e. centralizer of t is equal to the maximal torus containing it). □

Hence we can produce real elements in $SL_2(k)$, as in Lemma 7.2.1, which are not a product of two involutions in $SL_2(k)$.

Proposition 7.2.4. *Let $t_0 \in PSL_2(k)$ be a semisimple element. Then t_0 is real in $PSL_2(k)$ if and only if t_0 is strongly real in $PSL_2(k)$.*

Proof. Let $t \in SL_2(k)$ be a representative of t_0. Since t_0 is real in $PSL_2(k)$, it follows that t is either conjugate to t^{-1} or $-t^{-1}$ in $SL_2(k)$. In the second case, the characteristic polynomial of t must be $X^2 + 1$ and hence $t^2 = -1$. For the first case we prove that there exists $s \in SL_2(k)$ with $s^2 = -1$ such that $sts^{-1} = t^{-1}$.

If t is central, it is either I or $-I$. Hence we may assume that the element t is conjugate to the matrix $t_1 = \mathrm{diag}(\alpha, \alpha^{-1})$ in $SL_2(\bar{k})$, for some $\alpha \in \bar{k}$ with $\alpha^2 \neq 1$. Let $n = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\bar{k})$. Then $nt_1n^{-1} = t_1^{-1}$ and $n^2 = -1$. In fact n conjugates every element of the torus $T_1 = \{\mathrm{diag}(\gamma, \gamma^{-1}) \mid \gamma \in \bar{k}^*\}$ to its inverse. Hence there exists $h \in SL_2(\bar{k})$ such that $hth^{-1} = t^{-1}$ and $h^2 = -I$. Moreover, h conjugates every element of the maximal torus T containing t, to its inverse. Since t is real in $SL_2(k)$, there exists $g \in SL_2(k)$ such that $gtg^{-1} = t^{-1}$. Then $g \in h\mathcal{Z}_{SL_2(\bar{k})}(t)$. Since t is not central (by Lemma 7.2.3) we have $\mathcal{Z}_{SL_2(\bar{k})}(t) = T$, a maximal torus. We write $g = hx$

where $x \in T$. Then $g^2 = hxhx = -hxh^{-1}x = -x^{-1}x = -I$ and this proves the required result. □

We now consider Q, a quaternion algebra over k. It is a central simple algebra over k of degree 2. We note that $SL_1(Q) = \{x \in Q^* \mid \mathrm{Nrd}(x) = 1\}$ is a form of SL_2 over k. We denote the group $SL_1(Q)/\mathcal{Z}(SL_1(Q))$ by $PSL_1(Q)$.

Proposition 7.2.5. *With notation as above, let $G = PSL_1(Q)$ and $t \in G$ be a semisimple element. Then, t is real in $PSL_1(Q)$ if and only if t is strongly real in $PSL_1(Q)$. Furthermore, $G = SL_1(Q)$ has real elements which are not strongly real.*

Proof. We first observe that an element $t \in Q^*$ is either strongly regular or central. Proof of this fact and the rest of the proposition is on similar lines as in Lemma 7.2.3 and Proposition 7.2.4. □

7.3. $SL_1(D)$, deg(D) Odd

We now consider anisotropic simple groups of type A_n, for n even. These are the groups $SL_1(D)$ for central division algebras of degree $n+1$. Let D be a central division algebra over a field k, with degree D odd. Let $G = D^*$ or $G = SL_1(D) = \{x \in D^* \mid \mathrm{Nrd}(x) = 1\}$. We have,

Theorem 7.3.1. *Let G be as above. Then the only real elements in $G = D^*$ are ± 1. In $G = SL_1(D)$, there are no nontrivial real elements.*

Proof. We first prove that there are no non-central real element in G and there are no non-central involutions in G. Let $t \in G$ be a real element which is not in the center of D. Then $k(t)$ is a subfield $\neq k$ contained in D and has a field automorphism defined by $t \mapsto t^{-1}$ of order two. Hence the degree of $k(t)$ over k is even. But degree of D being odd, D can not contain a field extension of even degree. Hence there are no real elements which are not in the center of G.

Now let $t \in G$ is a non-central involution. Then $k(t)$ is a field extension over k of even degree. Following similar argument as in the previous paragraph, we get a contradiction. Hence any involution in G is in the center of G. Since D is central and degree D is odd, any such involution is trivial. This completes the proof. □

Corollary 7.3.2. *Let D be a central division algebra over a field k, with degree D odd. Let σ be an involution on D. Then the group* $\mathrm{Iso}(D, \sigma)$ *has no nontrivial real elements.*

Proof. We note that $\mathrm{Iso}(D,\sigma)=\{x\in D\mid x\sigma(x)=1\}\subset D^*$. Hence the result follows from previous theorem. $\square$

We remark that in view of Proposition 1.3.3 the group $\mathrm{Iso}(D,\sigma)$, for σ of the first kind, is a form of orthogonal group. The group $\mathrm{Iso}(D,\sigma)$, for σ of the second kind, is a form of unitary group.

7.4. Orthogonal Groups

Let V be a vector space over k with a nondegenerate quadratic form Q. We denote the orthogonal group by $O(Q)$. Wonenburger proved ([**W1**], Theorem 2; see also [**El2**] and [**El3**]),

Proposition 7.4.1. *Any element of the orthogonal group $O(Q)$ is strongly real, i.e., the group $O(Q)$ is bireflectional. Hence every element of $O(Q)$ is real.*

Djoković extended this result ([**D**], Theorem 1) to fields of characteristic 2. However, Knüppel and Nielsen proved ([**KN**], Theorem A),

Proposition 7.4.2. *The group $SO(Q)$ is trireflectional, except when $\dim(V)=2$ and $V\neq\mathcal{H}_3$, where $\mathcal{H}_3$ is the hyperbolic plane over $\mathbb{F}_3$. The group $SO(Q)$ is bireflectional if and only if $\dim(V)\not\equiv 2\pmod 4$ or $V=\mathcal{H}_3$, and hence in this case every element is real.*

They give necessary and sufficient condition for an element in special orthogonal group to be strongly real ([**KN**], Proposition 3.3).

Proposition 7.4.3. *Let $t\in SO(Q)$. Then t is strongly real in $SO(Q)$ if and only if $\dim(V)\not\equiv 2\pmod 4$ or an orthogonal decomposition of V into orthogonally indecomposable t-modules contains an odd dimensional summand.*

In the case $\dim(V)\equiv 2\pmod 4$, we explore reality for semisimple elements in $SO(Q)$. First we prove,

Lemma 7.4.4. *Let $t\in SO(Q)$ where $\dim(V)\equiv 2\pmod 4$. Let t be a semisimple element which has only two distinct eigenvalues λ and λ^{-1} (hence $\lambda\neq\pm1$) over $\bar{k}$. Then t is not real in $SO(Q)$.*

Proof. We prove that the element t is not real over $\bar{k}$. Let $\dim(V)=2m$ where m is odd. The element t over $\bar{k}$ is conjugate to $A=\mathrm{diag}(\underbrace{\lambda,\ldots,\lambda}_{m},\underbrace{\lambda^{-1},\ldots,\lambda^{-1}}_{m})$

with $\lambda \neq \pm 1$ in $SO(J)$ where J is the matrix of the quadratic form over $\bar{k}$ given by $J = \begin{pmatrix} 0 & S \\ S & 0 \end{pmatrix}$ where $S = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \vdots & & & & \vdots \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}$, an $m \times m$ matrix. Now suppose A is real in $SO(J)$, i.e., there exists $T \in SO(J)$ such that $TAT^{-1} = A^{-1}$. Then T maps the λ-eigen subspace of A to the λ^{-1}-eigen subspace of A and vice-versa. Hence T has the following form:

$$T = \begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix}$$

for $m \times m$ matrices B and C. Since T is orthogonal, it satisfies ${}^tTJT = J$, which gives ${}^tBSC = S$. That is, $\det(B)\det(C) = 1$. Hence $\det(T) = (-1)^m \det(B)\det(C) = -\det(B)\det(C) = -1$ since m is odd. This contradicts that $T \in SO(J)$. Hence A is not real in $SO(J)$ and hence t is not real in $SO(Q)$. □

Lemma 7.4.5. *Let* $\dim(V) \equiv 0 \pmod 4$ *and* $t \in SO(Q)$ *be semisimple. Suppose* t *has only two distinct eigenvalues* λ *and* λ^{-1}*(hence* $\lambda \neq \pm 1$*) over* $\bar{k}$*. Then, any element* $g \in O(Q)$ *such that* $gtg^{-1} = t^{-1}$ *belongs to* $SO(Q)$*, i.e.,* $\det(g) = 1$.

Proof. We follow the notation in the previous lemma. Let $\dim(V) = 2m$, where m is even. As in the proof of the previous lemma, we may assume t is diagonal. Then any element T that conjugates t to t^{-1} over $\bar{k}$, is of the form $T = \begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix}$. We have $\det(T) = (-1)^m \det(B)\det(C) = \det(B)\det(C) = 1$. Since g is a conjugate of T, the claim follows. □

Now we state the main theorem about special orthogonal groups.

Theorem 7.4.6. *Let* $t \in SO(Q)$ *be a semisimple element. Then,* t *is real in* $SO(Q)$ *if and only if* t *is strongly real in* $SO(Q)$*.*

Proof. If $\dim(V) \not\equiv 2 \pmod 4$ then the theorem follows from Propositions 7.4.2 and 7.4.3. Hence let us assume that $\dim(V) \equiv 2 \pmod 4$. Let $\dim(V) = 2m$ where m is odd. In this case we will prove that the element t is real in $SO(Q)$ if and only if 1 or -1 is an eigenvalue of t.

First we prove that if 1 and -1 are not eigenvalues then t is not real. It is enough to prove this statement over $\bar{k}$. We write $\bar{V} = V \otimes_k \bar{k}$ and continue to denote t over

$\bar{k}$ by t itself. We have a t-invariant orthogonal decomposition of $\bar{V}$;

$$\bar{V} = \bar{V}_1 \oplus \bar{V}_{-1} \oplus \bar{V}_{\lambda_1^{\pm 1}} \oplus \cdots \oplus \bar{V}_{\lambda_r^{\pm 1}}$$

where $\bar{V}_1$ and $\bar{V}_{-1}$ are the eigenspaces of t corresponding to 1 and -1 respectively and $\bar{V}_{\lambda_j^{\pm 1}} = \bar{V}_{\lambda_j} \oplus \bar{V}_{\lambda_j^{-1}}$ where $\bar{V}_{\lambda_j}$ is the eigenspace corresponding to λ_j for $\lambda_j^2 \neq 1$. Since 1 and -1 are not eigenvalues for t, we have $\bar{V}_1 = 0$ and $\bar{V}_{-1} = 0$. If $r = 1$ it follows from Lemma 7.4.4 that t is not real. Hence we may assume $r \geq 2$. We denote the restriction of t on $\bar{V}_{\lambda_j^{\pm 1}}$ by t_j. Let the dimension of $\bar{V}_{\lambda_j^{\pm 1}}$ be n_j. Since $\lambda_j \neq \pm 1$, n_j is even and is either $0 \pmod 4$ or $2 \pmod 4$. Let the number of subspaces $\bar{V}_{\lambda_j^{\pm 1}}$ such that n_j is $2 \pmod 4$ be s. Then s is odd, since $\dim(V) \equiv 2 \pmod 4$. Let $g \in SO(Q)$ such that $gtg^{-1} = t^{-1}$. Then g leaves $\bar{V}_{\lambda_j^{\pm 1}}$ invariant for all j. We denote the restriction of g on $\bar{V}_{\lambda_j^{\pm 1}}$ by g_j. Then $g_j \in O(\bar{V}_{\lambda_j^{\pm 1}})$ and $g_j t_j g_j^{-1} = t_j^{-1}$. From the previous lemma, determinant of g_j is 1 whenever $n_j \equiv 0 \pmod 4$ and the determinant of g_j is -1 whenever $n_j \equiv 2 \pmod 4$. Hence the determinant of g is $(-1)^s = -1$, which contradicts $g \in SO(Q)$. Hence t can not be real in $SO(Q)$.

Conversely, if 1 or -1 is an eigenvalue then the subspace $\bar{V}_1$ or $\bar{V}_{-1}$ is non-zero. These subspaces are defined over k. Let us denote their descents by V_1 and V_{-1} over k. The dimension of V_1 and V_{-1} is always even. But the matrix I and $-I$ can be written as a product of two involutions, each having determinant 1 or -1. Hence in this case t can be always written as a product of two involutions in $SO(Q)$. □

7.5. Symplectic Groups

Now we consider the symplectic group. Let V be a vector space of dimension $2n$ with a nondegenerate symplectic form. We denote the symplectic group by $Sp(2n, k)$. The center of this group $\mathcal{Z}(Sp(2n, k)) = \{\pm 1\}$ and we denote the projective symplectic group by $PSp(2n, k) = Sp(2n, k)/\mathcal{Z}(Sp(2n, k))$.

Lemma 7.5.1. *Let $t \in Sp(2, \bar{k})$ be a semisimple element. Suppose that t is either conjugate to t^{-1} or $-t^{-1}$. Then the conjugation can be achieved by an element $s \in Sp(2, \bar{k})$ such that $s^2 = -1$. Hence a semisimple element of $PSp(2, \bar{k})$ is real if and only if it is strongly real in $PSp(2, \bar{k})$.*

Proof. We note that $Sp(2, \bar{k}) = SL(2, \bar{k})$. Hence proof follows from Corollary 7.2.2. □

Lemma 7.5.2. *Let $t \in Sp(4, \bar{k})$ be a semisimple element. Suppose that t is either conjugate to t^{-1} or $-t^{-1}$. Then the conjugation can be achieved by an element*

$s \in Sp(4,\bar{k})$ such that $s^2 = -1$. Hence a semisimple element of $PSp(4,\bar{k})$ is real if and only if it is strongly real in $PSp(4,\bar{k})$.

Proof. Let $J = \operatorname{diag}\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right)$. Then $Sp(4,\bar{k}) = \{A \in GL(4,\bar{k}) \mid {}^tAJA = J\}$. We first assume t is conjugate to t^{-1}. We may assume $t = \operatorname{diag}(\lambda, \lambda^{-1}, \mu, \mu^{-1})$. We let

$$g = \operatorname{diag}\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) \in Sp(4,\bar{k}).$$

Then $g^2 = -1$ and $gtg^{-1} = t^{-1}$.

Now let t be conjugate to $-t^{-1}$. Then we may assume $t = \operatorname{diag}(\lambda, \lambda^{-1}, -\lambda, -\lambda^{-1})$. Let $g = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$. Then g belongs to $Sp(4,\bar{k})$ with $g^2 = -1$ and $gtg^{-1} = -t^{-1}$. □

Theorem 7.5.3. *Let $t \in Sp(2n,k)$ be a semisimple element. Suppose t is either conjugate to t^{-1} or $-t^{-1}$. Then the conjugation can be achieved by an element $s \in Sp(2n,k)$ such that $s^2 = -1$. Hence a semisimple element of $PSp(2n,k)$ is real if and only if it is strongly real in $PSp(2n,k)$.*

Proof. First we consider semisimple elements in $Sp(2n,\bar{k})$. Let $t \in Sp(2n,\bar{k})$ be semisimple with t conjugate to t^{-1}. Then t can be conjugated to $\operatorname{diag}(\lambda_1, \lambda_1^{-1}, \ldots, \lambda_n, \lambda_n^{-1})$ and this diagonal element can be conjugated to its inverse by $s = \operatorname{diag}(\underbrace{N, \ldots, N}_{n})$ where $N = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Clearly $s^2 = -1$. A conjugate of s then does the job.

Now let us assume t is conjugate to $-t^{-1}$ in $Sp(2n,\bar{k})$. Then t can be conjugated to

$$\operatorname{diag}(\lambda_1, \lambda_1^{-1}, -\lambda_1, -\lambda_1^{-1}, \ldots, \lambda_r, \lambda_r^{-1}, -\lambda_r, -\lambda_r^{-1}, \mu_1, \mu_1^{-1}, \ldots, \mu_s, \mu_s^{-1})$$

in $Sp(2n, \bar{k})$ where $\mu_i^2 = \pm 1$. Such an element t can be conjugated to $-t^{-1}$ by $s = \mathrm{diag}(\underbrace{M, \dots, M}_{r}, \underbrace{N, \dots, N}_{s}) \in Sp(2n, \bar{k})$ where

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

and $s^2 = -1$. This concludes the proof of the theorem over $\bar{k}$.

We now complete the proof over k. Let $t \in Sp(V)$, where V is a $2n$-dimensional vector space over k. We first assume t is real in $Sp(V)$.

First note that if $t_1 \in Sp(V_1)$ and $t_2 \in Sp(V_2)$, where V_1 and V_2 are vector space over k of dimension $2n_1$ and $2n_2$ respectively, and if there exist $g_1 \in Sp(V_1)$ and $g_2 \in Sp(V_2)$ such that $g_i t_i g_i^{-1} = t_i^{-1}$ and $g_i^2 = -1$, then $t_1 \oplus t_2$ is conjugate to its inverse $t_1^{-1} \oplus t_2^{-1}$ by $g = g_1 \oplus g_2$ in $Sp(V_1 \oplus V_2)$ and $g^2 = -1$.

Now let $t \in Sp(V)$ be real. We write $\bar{V}$ for $V \otimes \bar{k}$ and $\bar{V}_\alpha = \{x \in \bar{V} \mid t(x) = \alpha x\}$, where $\alpha \in \bar{k}^*$. Both $\bar{V}_1$ and $\bar{V}_{-1}$ are defined over k. Let the subspaces V_1 and V_{-1} of V be the descents of $\bar{V}_1$ and $\bar{V}_{-1}$ respectively. We note that the dimension of V_{-1} is even, since the determinant of t is 1. We now assume $\alpha \neq \pm 1$. We write $\bar{W}_\alpha = \bar{V}_\alpha \oplus \bar{V}_{\alpha^{-1}}$, which is a nondegenerate subspace of $\bar{V}$. The subspace $\bar{W}_\alpha$ is defined over the subfield k_α of $\bar{k}$, where k_α is the fixed field of the subgroup of $\Gamma = \mathrm{Gal}(\bar{k}/k)$ fixing the unordered pair $\{\alpha, \alpha^{-1}\}$. We denote the descent subspace of $\bar{W}_\alpha$ over k_α by W_α. Then W_α is a direct sum of m_α two-dimensional subspaces over k_α, which are stable under t and t restricted to each of these 2-dimensional subspace is conjugate to $\mathrm{diag}\{\alpha, \alpha^{-1}\}$.

By Lemma 7.5.1, there exists $g_\alpha \in Sp(W_\alpha)$ with $g_\alpha^2 = -1$ such that $g_\alpha t|_{W_\alpha} g_\alpha^{-1} = t|_{W_\alpha}^{-1}$. The subspace $W_{\Gamma\alpha} = \oplus_{\sigma \in \Gamma} W_{\sigma\alpha}$ is defined over k and we denote the restriction of t to this subspace by $t_{\Gamma\alpha}$ (which is $\oplus_{\sigma\in\Gamma} t_{\sigma\alpha}$). Also $g_{\Gamma\alpha} = \oplus g_{\sigma\alpha}$ is defined over k and conjugates t to t^{-1} on the subspace $W_{\Gamma\alpha}$. We note that the $g_{\Gamma\alpha}^2 = -1$.

Now we write $V = V_1 \oplus V_{-1} \oplus_{\alpha \in \bar{k}^*} W_{\Gamma\alpha}$. Since the dimension of V_{-1} is even, we may take g_{-1} as the direct sum of $N = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ on this subspace, $\frac{1}{2}\dim(V_{-1})$ times. Since n is even, dimension of V_1 is even and we may take g_1 as the direct sum of N, $\frac{1}{2}\dim(V_1)$ times, on this subspace. Finally we take $g = g_1 \oplus g_{-1} \oplus_{\alpha \in \bar{k}^*} g_{\Gamma\alpha} \in Sp(2n, k)$. We have $g^2 = -1$ and $gtg^{-1} = t^{-1}$.

Now let us assume that t is conjugate to $-t^{-1}$. We follow the same proof as above except that we consider $\bar{W}_\alpha = \bar{V}_\alpha \oplus \bar{V}_{\alpha^{-1}} \oplus \bar{V}_{-\alpha} \oplus \bar{V}_{-\alpha^{-1}}$ when $\alpha^2 \neq \pm 1$. We construct $g_{\Gamma\alpha}$ using Lemma 7.5.2 in this case. The rest of the proof is along similar lines as above. □

Remark 7.5.4. We give an example to show that there are semisimple real elements in $Sp(4,k)$ which are not a product of two involutions. Let

$$J = \operatorname{diag}\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right)$$

be the matrix of the skew-symmetric (symplectic) form. Then $Sp(4,k) = \{A \in GL(4,k) \mid {}^tAJA = J\}$. Let $S = \operatorname{diag}(\lambda, \lambda^{-1}, \mu, \mu^{-1}) \in Sp(4,k)$ with all diagonal entries distinct. Then any element $T \in Sp(4,k)$, such that $TST^{-1} = S^{-1}$, is of the following type:

$$T = \operatorname{diag}\left(\begin{pmatrix} 0 & -a \\ a^{-1} & 0 \end{pmatrix}, \begin{pmatrix} 0 & -b \\ b^{-1} & 0 \end{pmatrix}\right)$$

such that $T^2 = -1$. Hence A is real semisimple but not a product of two involutions.

7.6. Unitary Groups

In this section we deal with unitary groups. Let K be a quadratic field extension of k. Let V be an n-dimensional vector space with a nondegenerate hermitian form $\mathfrak{h}$. Then

$$U(V,\mathfrak{h}) = \{t \in GL(V) \mid \mathfrak{h}(t(v), t(w)) = \mathfrak{h}(v,w)\ \forall v, w \in V\}$$

is a k-group. Let $\bar{k}$ be an algebraic closure of k. We denote $\bar{V} = V \otimes_k \bar{k}$, a module over $K \otimes_k \bar{k}$. We define $\bar{\mathfrak{h}}$ on $\bar{V}$ by base change of $\mathfrak{h}$ to $\bar{k}$. Then $U(\bar{V}, \bar{\mathfrak{h}})$ is an algebraic group defined over k and $U(V,\mathfrak{h})$ is the group of k-points of $U(\bar{V},\bar{\mathfrak{h}})$. Let $\{e_1, \ldots, e_n\}$ be an orthogonal basis of V with respect to $\mathfrak{h}$. Let $\mathfrak{h}(e_i, e_i) = \alpha_i \in k$ and let $H = \operatorname{diag}(\alpha_1, \ldots, \alpha_n)$. Then $U(V,\mathfrak{h}) \cong U(H) = \{A \in GL_n(K) \mid {}^tAH\bar{A} = H\}$.

Lemma 7.6.1. *Let V be a two dimensional vector space over K with a nondegenerate hermitian form $\mathfrak{h}$. Let e_1, e_2 be an orthogonal basis of V with $\mathfrak{h}(e_i, e_i) = h_i$ and $H = \begin{pmatrix} h_1 & 0 \\ 0 & h_2 \end{pmatrix}$. Let A be any diagonal matrix in $U(H)$. Then A is real in $U(H)$ if and only if $h_1h_2 \in N_{K/k}(K^*)$ and, in that case, it is strongly real.*

Proof. Let $A = \begin{pmatrix} \xi & 0 \\ 0 & \bar{\xi} \end{pmatrix} \in U(H)$. Let T be an element such that $TAT^{-1} = A^{-1}$. Then T has following form: $T = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$ where $h_1 b\bar{b} = h_2$ and $h_2 c\bar{c} = h_1$. Hence A is real in $U(H)$ if and only if $h_1 h_2 \in N_{K/k}(K^*)$. And, if the condition holds, we can take $T = \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix}$. This proves the result. □

Theorem 7.6.2. *Let $(V, \mathfrak{h})$ be a hermitian space over K. Let $t \in U(V, \mathfrak{h})$ be a semisimple element. Then, t is real in $U(V, \mathfrak{h})$ if and only if t is strongly real.*

Proof. Let $t \in U(V, h)$ be a real semisimple element. Let $g \in U(V, h)$ be such that $gtg^{-1} = t^{-1}$. We base change to $\bar{k}$ and argue. Since t is real semisimple, we have a decomposition of $\bar{V}$ as follows:

$$\bar{V} = \bar{V}_1 \obot \bar{V}_{-1} \obot_{\lambda\bar{\lambda}=1} (\bar{V}_\lambda \obot \bar{V}_{\lambda^{-1}}) \obot_{\lambda \neq \bar{\lambda}^{-1}} ((\bar{V}_\lambda \oplus \bar{V}_{\bar{\lambda}^{-1}}) \obot (\bar{V}_{\lambda^{-1}} \oplus \bar{V}_{\bar{\lambda}}))$$

where $\bar{V}_1, \bar{V}_{-1}$ and $\bar{V}_\lambda$ are eigenspaces corresponding to eigenvalues $1, -1$ and λ respectively. Since t is unitary, whenever λ is an eigen value $\bar{\lambda}^{-1}$ is also an eigen value. To verify the orthogonality in the decomposition we take $x \in \bar{V}_\lambda$ and $y \in \bar{V}_\mu$ and note that

$$h(x, y) = h(t(x), t(y)) = h(\lambda x, \mu y) = \lambda\bar{\mu} h(x, y).$$

Hence $\bar{V}_\lambda$ and $\bar{V}_\mu$ are orthogonal if $\lambda\bar{\mu} \neq 1$. We denote the subspace $\bar{V}_\lambda \obot \bar{V}_{\lambda^{-1}}$ by $\bar{W}_\lambda$ when $\lambda\bar{\lambda} = 1$ and $(\bar{V}_\lambda \oplus \bar{V}_{\bar{\lambda}^{-1}}) \obot (\bar{V}_{\lambda^{-1}} \oplus \bar{V}_{\bar{\lambda}})$ as $\bar{W}_\lambda$ in other cases. In the first case, for $x \in \bar{W}_\lambda$ we have $t(x) = \lambda^{\pm 1} x$ and since $gtg^{-1} = t^{-1}$ we get $t(g(x)) = \lambda^{\mp 1} g(x)$. This implies that $g(x) \in \bar{W}_\lambda$ which means the conjugating element g leaves $\bar{W}_\lambda$ invariant. Similarly one can verify that g leaves $\bar{W}_\lambda$ invariant in the other case also. Since $\bar{V}_\lambda$ ($\bar{V}_\lambda \oplus \bar{V}_{\bar{\lambda}^{-1}}$ in the second case) is nondegenerate (because it is an orthogonal sum), we can choose an orthogonal basis $\{e_1, \ldots, e_r\}$ for $\bar{V}_\lambda$ ($\bar{V}_\lambda \oplus \bar{V}_{\bar{\lambda}^{-1}}$ in the other case). We decompose $\bar{W}_\lambda$ in t invariant planes as follows. Let P_i be the subspace generated by $\{e_i, g(e_i)\}$. Then $\bar{W}_\lambda = P_1 \oplus \ldots \oplus P_r$ is an orthogonal decomposition. Moreover, t leaves each of the P_i invariant. The element n_i which maps e_i to $g(e_i)$ and $g(e_i)$ to e_i, is a unitary involution conjugating $t|_{P_i}$ to its inverse. The element $\bar{s} = n_1 \oplus \ldots \oplus n_r$ conjugates $t|_{\bar{W}_\lambda}$ to its inverse and is a unitary involution.

Let W_λ be the sum of all Galois conjugates of $\bar{W}_\lambda$ and s be the sum of all Galois conjugates of $\bar{s}$. Then W_λ is defined over k and $t|_{W_\lambda}$ is conjugate to its inverse by the involution s defined over k. This gives the decomposition of V as $V = V_1 \oplus V_{-1} \oplus_\lambda W_\lambda$

and we have proved that t is a product of two involutions on each component. Hence t is strongly real. □

Corollary 7.6.3. *Let $t \in SU(V, \mathfrak{h})$ be semisimple. Suppose $n \not\equiv 2 \pmod 4$. Then t is real in $SU(V, \mathfrak{h})$ if and only if it is strongly real.*

Proof. The result follows by keeping track of the determinant of the conjugating element in the proof of Theorem 7.6.2. □

Remarks 7.6.4. 1. Let K be a quadratic extension of k. Let V be a two dimensional vector space over a field K with a nondegenerate hermitian form $\mathfrak{h}$ defined as follows. Let $\{e_1, e_2\}$ be a basis of V such that $\mathfrak{h}(e_1, e_1) = 1, \mathfrak{h}(e_2, e_2) = -1$ and $\mathfrak{h}(e_1, e_2) = 0$. In the matrix notation, the matrix of the form is $H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $U(H) = \{X \in GL_2(K) \mid {}^tXH\bar{X} = H\}$. Let $A = \begin{pmatrix} \xi & 0 \\ 0 & \bar{\xi} \end{pmatrix} \in SU(H)$ where $\xi \neq \bar{\xi}$. Then A is semisimple. Let $T \in GL_2(K)$ such that $TAT^{-1} = A^{-1}$. Then T is of the form $T = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$. Note that A is real in $U(H)$ if and only if there exists $T = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$ with $b\bar{b} = -1$ and $c\bar{c} = -1$. The element A is not strongly real in $SU(H)$. For T to be in $SU(H)$ we need $bc = -1$ and this implies $T^2 = -1$. Hence no involution conjugates A to its inverse. But if K has an element b such that $b\bar{b} = -1$, then A can be conjugated to A^{-1} by T such that $T^2 = -1$. For example one can take $K = \mathbb{Q}(\sqrt{5})$ and $k = \mathbb{Q}$.

2. Let V be a two dimensional vector space over K with a hermitian form $\mathfrak{h}$ on it. Let $K = k(\gamma)$. Let $\{e_1, e_2\}$ be a basis of V such that $\mathfrak{h}(e_1, e_1) = 0, \mathfrak{h}(e_2, e_2) = 0$ and $\mathfrak{h}(e_1, e_2) = \gamma = -\mathfrak{h}(e_2, e_1)$. In the matrix notation, the matrix of the form is $H = \begin{pmatrix} 0 & \gamma \\ -\gamma & 0 \end{pmatrix}$ and $U(H) = \{X \in GL_2(K) \mid {}^tXH\bar{X} = H\}$. Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SU(H)$. Then A is a unipotent element. Let $T \in GL_2(K)$ be such that $TAT^{-1} = A^{-1}$. Then T is of the form $T = \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix}$. Note that A is real in $U(H)$ if and only if there exists $T = \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix}$ with $a\bar{a} = -1$ and $a\bar{b} - \bar{a}b = 0$. Here $T^2 = a^2I$. The element A is not strongly real in $SU(H)$. For if so, we would have $a^2 = 1$ and $a\bar{a} = -1$, which would imply that γ is a square in k. Hence no involution conjugates

A to its inverse. But if k has an element a such that $a^2 = -1$, then A is conjugate to its inverse by T such that $T^2 = -1$. For example one can take $K = \mathbb{Q}(\sqrt{-1}, \sqrt{5})$ and $k = \mathbb{Q}(\sqrt{-1})$.

CHAPTER 8

Reality in Groups of Type G_2

This whole chapter is devoted to the study of reality properties in groups of type G_2. We give proofs to results mentioned in the Section 6.2. We also obtain results on conjugacy classes and centralizers in groups of type G_2 which we use to calculate conjugacy classes of centralizers in Section 8.5. The preliminaries for this chapter have been discussed in Chapter 3. The results in Sections 8.1, 8.2, 8.3 and 8.4 have appeared in [**ST1**] and the results in 8.5 are the part of [**Si**].

8.1. Reality in G_2

Let G be a group of type G_2 defined over a field k (of characteristic $\neq 2$). Then, there exists an octonion algebra $\mathfrak{C}$ over k such that $G \cong \mathrm{Aut}(\mathfrak{C})$ ([**Se**], Chapter III, Proposition 5, Corollary). Let t_0 be an element of $G(k)$. We will also denote the image of t_0 in $\mathrm{Aut}(\mathfrak{C})$ by t_0. We write $\mathfrak{C}_0$ for the subspace of trace 0 elements of $\mathfrak{C}$. In this section, we explore the condition so that t_0 is conjugate to t_0^{-1} in $G(k)$. We prove the following,

Theorem 8.1.1. *Let G be a group of type G_2 over a field k of characteristic not 2 and 3. Let $t_0 \in G(k)$. Then, t_0 is real in $G(k)$ if and only if t_0 is strongly real in $G(k)$.*

In fact the result is true in characteristic 3 also except for unipotent elements. We let $V_{t_0} = ker(t_0 - 1)^8$. Then V_{t_0} is a composition subalgebra of $\mathfrak{C}$ with norm as the restriction of the norm on $\mathfrak{C}$ ([**W2**]). Let $r_{t_0} = \dim(V_{t_0} \cap \mathfrak{C}_0)$. Then r_{t_0} is $1, 3$ or 7. We note that if $r_{t_0} = 7$, the characteristic polynomial of t_0 is $(X-1)^8$ and t_0 is unipotent. We have,

Lemma 8.1.2. *Let $t_0 \in G(k)$ be a unipotent element. In addition, we assume $char(k) \neq 3$. Then t_0 is strongly real in $G(k)$.*

Proof. Since t_0 is unipotent, we have $r_{t_0} = 7$. In this case, the characteristic polynomial of t_0 on $\mathfrak{C}_0$ is $(X-1)^7$. The assertion follows from a theorem of Wonenburger ([**W2**], Theorem 4), which states that if $char(k) \neq 3$ and the characteristic polynomial of $t \in \mathrm{Aut}(\mathfrak{C})$ is divisible by $(x-1)^3$, t is a product of two involutory automorphisms of $\mathfrak{C}$. Hence t_0 is strongly real in $G(k)$. □

Lemma 8.1.3. *Let the notation be as fixed above and let $t_0 \in G(k)$ be an element which is not unipotent (e.g. a semisimple element). Then, either t_0 leaves a quaternion subalgebra invariant or fixes a quadratic étale subalgebra L of $\mathfrak{C}$ pointwise. In the latter case, $t_0 \in SU(V, \mathfrak{h}) \subset G(k)$ for a rank 3 hermitian space V over a quadratic field extension L of k or $t_0 \in SL(3) \subset G(k)$.*

Proof. Since t_0 is not unipotent, from the above discussion, we see that r_{t_0} is 1 or 3. If $r_{t_0} = 3$, t_0 leaves a quaternion subalgebra $\mathfrak{D}$ of $\mathfrak{C}$ invariant. In the case $r_{t_0} = 1$, $L = V_{t_0}$ is a two dimensional composition subalgebra and has the form $V_{t_0} = k.1 \oplus (V_{t_0} \cap \mathfrak{C}_0)$, an orthogonal direct sum. Let $L \cap \mathfrak{C}_0 = k.\gamma$ with $N(\gamma) \neq 0$. Since t_0 leaves $\mathfrak{C}_0$ and V_{t_0} invariant, we have, $t_0(\gamma) = \gamma$ and hence $t_0(x) = x \ \forall x \in L$, so that $t_0 \in G(\mathfrak{C}/L)$. The result now follows from Proposition 3.2.1 and Proposition 3.2.2. □

If t_0 leaves a quaternion subalgebra invariant, t_0 is strongly real in $G(k)$. This follows from the following theorem (see [**W2**], Theorem 4).

Theorem 8.1.4. *Let $\mathfrak{C}$ be an octonion algebra. If g is an automorphism of $\mathfrak{C}$ which maps a quaternion subalgebra $\mathfrak{D}$ into itself, then g is a product of two involutory automorphisms.*

Corollary 8.1.5. *If an automorphism g of $\mathfrak{C}$ leaves a nondegenerate plane of $\mathfrak{C}_0$ invariant, then it is a product of two involutory automorphisms.*

We discuss the other cases here, i.e., the fixed points of t_0 form a quadratic étale subalgebra L of $\mathfrak{C}$.

(1) The fixed subalgebra L is a quadratic field extension of k and
(2) the fixed subalgebra is split, i.e., $L \cong k \times k$.

By the discussion in Section 3.2, in the first case, t_0 belongs to $G(\mathfrak{C}/L) \cong SU(L^{\perp}, \mathfrak{h})$ (Proposition 3.2.1) and in the second case t_0 belongs to $G(\mathfrak{C}/L) \cong SL(3)$ (Proposition 3.2.2). We denote the image of t_0 by A in both of these cases. We analyze further the cases depending on the characteristic polynomial of A. We mention a result of Neumann here ([**N**], Satz 6 and Satz 8).

Proposition 8.1.6. *Let t_0 be an element in $G(k)$ and suppose t_0 exactly fixes a quadratic étale subalgebra L of $\mathfrak{C}$ pointwise. Let us denote the image of t_0 by A in $SU(L^{\perp}, \mathfrak{h})$ or in $SL(3)$ as the case may be. Also assume that the characteristic* *polynomial of A over L in the first case and over k in the second, is reducible and the minimal polynomial of A is not of the form $(X-\alpha)^3$, for $\alpha \in L$ in the first case and for $\alpha \in k$ in the second case. Then t_0 is strongly real.*

We have the following,

Theorem 8.1.7. *Let G be a group of type G_2 over a field k of characteristic not 2. Let $t_0 \in G(k)$ be an element which is not unipotent. Then, t_0 is real in $G(k)$ if and only if t_0 is strongly real in $G(k)$. In addition, if $char(k) \neq 3$ then every unipotent element in $G(k)$ is strongly real in $G(k)$.*

Proof. The assertion about unipotents in $G(k)$ follows from Lemma 8.1.2. In view of Lemma 8.1.3 and discussion following the lemma, we need to consider the case when $t_0 \in SU(L^{\perp}, \mathfrak{h})$ or $t_0 \in SL(3)$. In these cases, we look at the characteristic polynomial $\chi_A(X)$ and the minimal polynomial $m_A(X)$ of A. We first assume that $\chi_A(X) \neq m_A(X)$. Hence degree of $m_A(X) \leq 2$ and $\chi_A(X)$ is reducible. The conditions in Proposition 8.1.6 are satisfied in this case. Hence t_0 is strongly real. We take up the case of A with $\chi_A(X) = m_A(X)$ below. □

The result follows from the following theorem.

Theorem 8.1.8. *Let t_0 be an element in $G(k)$ and suppose t_0 fixes exactly a quadratic étale subalgebra L of $\mathfrak{C}$ pointwise. Let us denote the image of t_0 by A in $SU(L^{\perp}, \mathfrak{h})$ or in $SL(3)$ as the case may be. Also assume that the characteristic polynomial of A over L in the first case and over k in the second, is equal to the minimal polynomial of A. Then t_0 is conjugate to t_0^{-1} in $G(k)$ if and only if t_0 is strongly real in $G(k)$.*

Proof. We distinguish the cases of both these subgroups below and complete the proof in the next two sections, see Theorem 8.2.8 and Theorem 8.3.5. □

We record the theorem about semisimple elements separately.

Theorem 8.1.9. *Let t_0 be a semisimple element in $G(k)$ and suppose t_0 fixes the quadratic étale subalgebra L of $\mathfrak{C}$ pointwise. Let us denote the image of t_0 by A in $SU(L^{\perp}, \mathfrak{h})$ or in $SL(3)$ as the case may be. If the characteristic polynomial of A over L in the first case and over k in the second, is reducible then t_0 is strongly real in $G(k)$. If the characteristic polynomial is irreducible then t_0 is real if and only if t_0 is strongly real.*

Proof. Let us assume first that the characteristic polynomial of A over L in the first case and over k in the second, is irreducible. This case follows from Theorem 8.1.8. Since the characteristic polynomial of A is irreducible, it equals the minimal polynomial of A. Hence let us consider the case when characteristic polynomial is reducible. First, let us take the case when L is a field extension. Let T be a maximal torus in $SU(L^{\perp}, \mathfrak{h})$ containing t_0. By Corollary 5.1.6, there exists an étale L-algebra $\mathcal{E}_T$ with an involution σ and $u \in \mathcal{F}^*$ such that $(L^{\perp}, \mathfrak{h}) \cong (\mathcal{E}_T, \mathfrak{h}^{(u)})$, here $\mathcal{F}$ is the fixed point subalgebra of σ in $\mathcal{E}_T$. Since the characteristic polynomial of A is reducible, we see that $L^{\perp}$ is a reducible representation of T. From Corollary 5.2.2 we see that $\mathcal{E}_T$ is not a field. We can write $\mathcal{E}_T \cong \mathcal{F} \otimes L$ where $\mathcal{F}$ is a cubic étale k-algebra but not a field. Let $\mathcal{F} = k \times \Delta$, for some quadratic étale k-algebra Δ. Hence $\mathcal{E}_T \cong L \times (\Delta \otimes L)$ and σ is given by $(\alpha, f \otimes \beta) \mapsto (\bar{\alpha}, f \otimes \bar{\beta})$. Writing $u = (u_1, u_2)$ where $u_1 \in k$, the hermitian form $\mathfrak{h}^{(u)}$ is given by $\mathfrak{h}^{(u)}((l, \delta), (l', \delta')) = tr_{L/L}(lu_1l') + tr_{\Delta\otimes L/L}(\delta u_2 \delta') = lu_1l' + tr_{\Delta\otimes L/L}(\delta u_2\delta')$. Hence $L \times \{0\}$ is a nondegenerate subspace left invariant by the action of $t_0 \in T^1_{(\mathcal{E}_T,\sigma_{\mathfrak{h}})} \cong T^1_L \times T^1_{\Delta\otimes L}$, which acts by left multiplication. Therefore t_0 leaves invariant a two dimensional nondegenerate k-plane in $\mathfrak{C}_0$. The result now follows from Corollary to Theorem 8.1.4. The proof in the case when L is split proceeds on similar lines. □

8.2. $SU(V, \mathfrak{h}) \subset G$

We continue with notation introduced in the last section. We assume that L is a quadratic field extension of k. Let t_0 be an element in $G(\mathfrak{C}/L)$ with characteristic polynomial of the restriction to $V = L^{\perp}$, equal to its minimal polynomial over L. We write $\mathfrak{C} = L \bigoplus V$, where V is an L-vector space with hermitian form $\mathfrak{h}$ induced by the norm on $\mathfrak{C}$. Then we have seen that $G(\mathfrak{C}/L) \cong SU(V, \mathfrak{h})$ (Theorem 3.2.1).

Lemma 8.2.1. *Let the notation be as fixed above. Let t_0 be an element in $G(\mathfrak{C}/L)$ which does not have a nonzero fixed point outside L. Suppose that $\exists g \in G(k)$ such that $gt_0g^{-1} = t_0^{-1}$. Then $g(L) = L$.*

Proof. Suppose that $g(L) \not\subset L$. Then we claim that $\exists x \in L \cap \mathfrak{C}_0$ such that $g(x) \notin L$. For this, let $y \in L$ be such that $g(y) \notin L$. Let $x = y - \frac{1}{2}tr(y)1$. Then $tr(x) = 0$ and if $g(x) \in L$ then $g(y) \in L$, a contradiction. Hence we have $x \in L \cap \mathfrak{C}_0$ with $g(x) \notin L$. Also since $t_0(x) = x$, we have,

$$t_0(g(x)) = gt_0^{-1}(x) = g(x).$$

Therefore t_0 fixes $g(x) \notin L$, a contradiction. Hence, $g(L) = L$. □

We recall a construction from Proposition 3.2.5. Let $a \in L^\perp$ with $N(a) \neq 0$. Let $\mathfrak{D} = L \oplus La$ and $\rho_1 \colon \mathfrak{D} \to \mathfrak{D}$ be defined by $\rho_1(x + ya) = \sigma(x) + \sigma(y)a$. Write again $\mathfrak{C} = \mathfrak{D} \oplus \mathfrak{D}b$, for $b \in \mathfrak{D}^\perp$ with $N(b) \neq 0$ and define $\rho \colon \mathfrak{C} \to \mathfrak{C}$ by $\rho(x + yb) = \sigma(x) + \sigma(y)b$. Then ρ is an automorphism of $\mathfrak{C}$ of order 2 which restricts to L to the nontrivial automorphism of L. The basis

$$\{f_1 = a, f_2 = b, f_3 = ab\}$$

of $V = L^\perp$ over L is an orthogonal basis for $\mathfrak{h}$. **We fix this basis throughout this section**. Let us denote the matrix of $\mathfrak{h}$ with respect to this basis by $H = \mathrm{diag}(\lambda_1, \lambda_2, \lambda_3)$ where $\lambda_i = \mathfrak{h}(f_i, f_i) \in k^*$. Then $SU(V,\mathfrak{h})$ is isomorphic to $SU(H) = \{A \in SL(3,L) \mid {}^t\!AH\bar{A} = H\}$.

Theorem 8.2.2. *With notation fixed as above, let A be the matrix of t_0 in $SU(H)$ with respect to the fixed basis described above. Suppose that t_0 does not have a nonzero fixed point outside L. Then t_0 is conjugate to t_0^{-1} in $G(k)$, if and only if $\bar{A}$ is conjugate to A^{-1} in $SU(H)$, where the entries of $\bar{A}$ are obtained by applying σ on the entries of A.*

Proof. Let $g \in G(k)$ be such that $gt_0g^{-1} = t_0^{-1}$. In view of Lemma 8.2.1, we have $g(L) = L$. We have (Proposition 3.2.5) $G(\mathfrak{C}, L) \cong G(\mathfrak{C}/L) \rtimes N$ where $N =< \rho >$ and ρ is an automorphism of $\mathfrak{C}$, described above. Clearly g does not belong to $G(\mathfrak{C}/L)$. For if so, we can conjugate t_0 to t_0^{-1} in $G(\mathfrak{C}/L) \cong SU(H)$. But then the characteristic polynomial $\chi(X) = X^3 - \bar{a}X^2 + aX - 1$, where $a \in L$, and $\bar{a} = a$. Hence $\chi(X) = (X-1)(X^2 + (1-a)X + 1)$ and t_0 has a nonzero fixed point in $L^\perp$, a contradiction. We write $g = g'\rho$ where $g' \in G(\mathfrak{C}/L)$. Let B be the matrix of g' in $SU(H)$. Then, by a direct computation, it follows that,

$$gt_0g^{-1}(\alpha_0.1 + \alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3)$$

$$= \alpha_0.1 + \alpha_1 B\bar{A}B^{-1} f_1 + \alpha_2 B\bar{A}B^{-1} f_2 + \alpha_3 B\bar{A}B^{-1} f_3.$$

Also,

$$t_0^{-1}(\alpha_0.1 + \alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3) = (\alpha_0.1 + \alpha_1 A^{-1} f_1 + \alpha_2 A^{-1} f_2 + \alpha_3 A^{-1} f_3).$$

Therefore, if t_0 is conjugate to t_0^{-1} in $G = \mathrm{Aut}(\mathfrak{C})$, then $\bar{A}$ is conjugate to A^{-1} in $SU(H)$. Conversely, let $B\bar{A}B^{-1} = A^{-1}$ for some $B \in SU(H)$. Let $g' \in G(\mathfrak{C}/L)$ be the element corresponding to B. Then $g'\rho$ conjugates t_0 to t_0^{-1}. □

Let V be a vector space over L of dimension n with a nondegenerate hermitian form $\mathfrak{h}$. Let H denote the diagonal matrix of $\mathfrak{h}$ with respect to some fixed orthogonal basis. Then, for any $A \in U(H)$, we have ${}^{t}AH\bar{A} = H$. Let $A \in SU(H)$ with characteristic polynomial $\chi_A(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + (-1)^n$. Then $(-1)^n a_i = \bar{a}_{n-i}$ for $i = 1, \ldots, n-1$.

Lemma 8.2.3. *With notation as above, let $A \in SU(H)$ with its characteristic polynomial over L be the same as its minimal polynomial. Suppose $A = A_1A_2$ with $A_1, A_2 \in GL(n, L)$ and $\bar{A}_1A_1 = I = \bar{A}_2A_2$. Then, $A_1, A_2 \in U(H)$.*

Proof. Let $H = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$, where $\lambda_1, \ldots, \lambda_n \in k$. We have ${}^{t}AH\bar{A} = H$. Then,

$$(HA_1^{-1})A(HA_1^{-1})^{-1} = HA_1^{-1}A_1A_2A_1H^{-1} = H\bar{A}^{-1}H^{-1} = {}^{t}A.$$

Since the characteristic polynomial of A equals its minimal polynomial, by ([**TaZ**], Theorem 2) HA_1^{-1} is symmetric, i.e., $HA_1^{-1} = {}^{t}(HA_1^{-1}) = {}^{t}A_1^{-1}H$. This implies, $H = {}^{t}A_1HA_1^{-1} = {}^{t}A_1H\bar{A}_1$. Hence, $A_1 \in U(H)$. By similar analysis we see that $A_2 \in U(H)$. □

Lemma 8.2.4. *With notation as above, let $A \in SU(H)$ with characteristic polynomial $\chi_A(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + (-1)^n$ over L, equal to its minimal polynomial. Then, $A = B_1B_2$ with $B_1, B_2 \in GL(n, L)$ and $\overline{B}_1B_1 = I = \overline{B}_2B_2$.*

Proof. Let A_χ denote the companion matrix of A, namely

$$A_\chi = \begin{pmatrix} 0 & 0 & \ldots & 0 & -(-1)^n \\ 1 & 0 & \ldots & 0 & -a_{n-1} \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & \ldots & 1 & -a_1 \end{pmatrix}.$$

We have,

$$A_\chi = \begin{pmatrix} (-1)^n & 0 & \ldots & 0 & 0 \\ a_{n-1} & 0 & \ldots & 0 & -1 \\ \vdots & \vdots & & & \vdots \\ a_1 & -1 & \ldots & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & \ldots & 0 & -1 \\ 0 & 0 & \ldots & -1 & 0 \\ \vdots & \vdots & & & \vdots \\ -1 & 0 & \ldots & 0 & 0 \end{pmatrix} = A_1A_2,$$

and $\bar{A}_1A_1 = I = \bar{A}_2A_2$, using $(-1)^n a_i = \bar{a}_{n-i}$ for $i = 1, \ldots, n-1$. Since the characteristic polynomial of A equals its minimal polynomial, there exists $T \in GL(n, L)$ such that $A = TA_\chi T^{-1}$. We put $B_1 = TA_1\bar{T}^{-1}, B_2 = \bar{T}A_2T^{-1}$. Then $A = B_1B_2$, where $\bar{B}_1B_1 = I = \bar{B}_2B_2$. □

Corollary 8.2.5. *Let $A \in SU(H)$ with characteristic polynomial $\chi_A(X)$ over L same as its minimal polynomial. Then, $A = B_1B_2$ with $B_1, B_2 \in U(H)$ and $\overline{B}_1B_1 = I = \overline{B}_2B_2$.*

From this corollary, we get the following,

Lemma 8.2.6. *Let $A \in SU(H)$, with characteristic polynomial over L equal to its minimal polynomial. Then,*

(1) *$\bar{A}$ is conjugate to A^{-1} in $U(H)$, if and only if $A = A_1A_2$ with $A_1, A_2 \in U(H)$ and $\bar{A}_1A_1 = I = \bar{A}_2A_2$.*
(2) *$\bar{A}$ is conjugate to A^{-1} in $SU(H)$, if and only if $A = A_1A_2$ with $A_1, A_2 \in SU(H)$ and $\bar{A}_1A_1 = I = \bar{A}_2A_2$.*

The following proposition is due to Neumann ([**N**], Lemma 5). Recall that we have fixed a basis $\{f_1, f_2, f_3\}$ for $V = L^{\perp}$ over L in Theorem 8.2.2.

Proposition 8.2.7. *Let $\mathfrak{C}$ be an octonion algebra over k and let L be a quadratic field extension of k, which is a subalgebra of $\mathfrak{C}$. An element $t \in G(\mathfrak{C}/L)$ is a product of two involutions in $\mathrm{Aut}(\mathfrak{C})$, if and only if, the corresponding matrix $A \in SU(H)$ is a product of two matrices $A_1, A_2 \in SU(H)$, satisfying $\bar{A}_1A_1 = \bar{A}_2A_2 = I$.*

We now have,

Theorem 8.2.8. *Let t_0 be an element in $G(\mathfrak{C}/L)$ which does not have a fixed point outside L and let A denote the image of t_0 in $SU(H)$. Suppose the characteristic polynomial of A is equal to its minimal polynomial over L. Then t_0 is conjugate to t_0^{-1}, if and only if t_0 is a product of two involutions in $G(k)$.*

Proof. From Theorem 8.2.2 we have, t_0 is conjugate to t_0^{-1}, if and only if $\bar{A}$ is conjugate to A^{-1} in $SU(H)$. From Lemma 8.2.6 above, $\bar{A}$ is conjugate to A^{-1} in $SU(H)$ if and only if $A = A_1A_2$ with $A_1, A_2 \in SU(H)$ and $\bar{A}_1A_1 = I = \bar{A}_2A_2$. Now, from Proposition 8.2.7, it follows that t_0 is a product of two involutions. □

In [**W2**] and [**L**] examples of elements in $G(k)$, for G of type G_2, are constructed, which are not product of two involutions. These examples are neither semisimple nor unipotent. However, we continue our analysis to produce examples of semisimple elements which are not real. Let V be a vector space over L of dimension n together with a nondegenerate hermitian form h. Let $A \in SU(H)$. Let us denote the conjugacy class of A in $U(H)$ by C and the centralizer of A in $U(H)$ by $\mathcal{Z}$ and let

$$L_A = \{\det(X) \mid X \in \mathcal{Z}\}.$$

Lemma 8.2.9. *With notation as fixed above, for $X, Y \in U(H)$, XAX^{-1} is conjugate to YAY^{-1} in $SU(H)$ if and only if* $\det(X) \equiv \det(Y)(modL_A)$.

Proof. Suppose there exists $S \in SU(H)$ such that $SXAX^{-1}S^{-1} = YAY^{-1}$. Then, $Y^{-1}SX \in \mathcal{Z}$ and $\det(X) \equiv \det(Y)(modL_A)$.

Conversely, let $\det(XY^{-1}) = \det(B)$ for $B \in \mathcal{Z}$. Put $S = YBX^{-1}$. Then $\det(S) = 1$, $S \in SU(H)$ and $Y^{-1}SX = B \in \mathcal{Z}$. Then, $Y^{-1}SXA = AY^{-1}SX$ gives $SXAX^{-1}S^{-1} = YAY^{-1}$. □

Lemma 8.2.10. *Let t_0 be an element in $G(\mathfrak{C}/L)$ for L a quadratic field extension of k and A be the corresponding element in $SU(H)$. Suppose the characteristic polynomial of A is irreducible over L. Then, t_0 is conjugate to t_0^{-1} in $G(k)$, if and only if for every $X \in U(H)$ such that $X\bar{A}X^{-1} = A^{-1}$, $\det(X) \in L_{\bar{A}}$.*

Proof. We have, by Theorem 8.2.2, t_0 is conjugate to t_0^{-1} in $G(k)$ if and only if $\bar{A}$ is conjugate to A^{-1} in $SU(H)$. Let $X \in U(H)$ be such that $X\bar{A}X^{-1} = A^{-1}$. Then from the above lemma, $\bar{A}$ is conjugate to A^{-1} in $SU(H)$ if and only if $\det(X) \in L_{\bar{A}}$. □

Corollary 8.2.11. *With notation as fixed above, whenever $L^1/L_{\bar{A}}$ is trivial, t_0 is conjugate to t_0^{-1} in $G(k)$, where $L^1 = \{\alpha \in L | \alpha\bar{\alpha} = 1\}$.*

Proof. We have $L^1 = \{\alpha \in L \mid \alpha\bar{\alpha} = 1\} = \{\det(X) | X \in U(H)\}$. Now let us fix $X_0 \in U(H)$ such that $X_0\bar{A}X_0^{-1} = A^{-1}$. Then, for any $X \in U(H)$ such that $X\bar{A}X^{-1} = A^{-1}$, we have $X_0^{-1}X \in \mathcal{Z}_{U(H)}(\bar{A})$. Hence $\det(X) \in \det(X_0)L_{\bar{A}}$. But since $L^1/L_{\bar{A}}$ is trivial, we have $\det(X) \in L_{\bar{A}}$. From the above lemma, it now follows that t_0 is conjugate to t_0^{-1} in $G(k)$. □

Remark 8.2.12. From the proof above, for any $X \in U(H)$ such that $X\bar{A}X^{-1} = A^{-1}$, we get $X \in X_0\mathcal{Z}_{U(H)}(\bar{A})$. Since the characteristic polynomial of A is irreducible, that of $\bar{A}$ is irreducible as well. Therefore $\mathcal{Z}_{U(H)}(\bar{A}) \subset \mathcal{Z}_{\mathrm{End}_L(V)}(\bar{A}) = L[\bar{A}] \cong L[T]/ < \chi_{\bar{A}}(T) >$. In fact, $\mathcal{Z}_{U(H)}(\bar{A}) = \{x \in \mathcal{Z}_{\mathrm{End}_L(V)}(\bar{A}) \mid x\sigma_h(x) = 1\}$. Hence we can write $X = X_0 f(\bar{A})$ for some polynomial $f(T) \in L[T]$.

Lemma 8.2.13. *Let $A \in SU(H)$ and its characteristic polynomial $\chi_A(X)$ be irreducible over L. Let $\mathcal{E} = L[X]/\chi_{\bar{A}}(X)$, a degree three field extension of L. Then $L^1/L_{\bar{A}} \hookrightarrow L^*/N(\mathcal{E}^*)$.*

Proof. Define a map $\phi\colon L^1 \longrightarrow L^*/N(\mathcal{E}^*)$ by $x \mapsto xN(\mathcal{E}^*)$. We claim that $ker(\phi) = \{x \in L^1 \mid x \in N(\mathcal{E}^*)\} = L_{\bar{A}} = \{N(x) \mid x \in \mathcal{E}^*, x\sigma(x) = 1\}$. Let $x \in ker(\phi)$, i.e., $x = N(y)$ for some $y \in \mathcal{E}^*$ and $x\sigma(x) = 1$. Let $\tilde{y} = xy^{-1}\sigma(y) \in \mathcal{E}^*$ then

$N(\tilde{y}) = x, \tilde{y}\sigma(\tilde{y}) = 1$. Hence $x \in L_{\bar{A}}$. Conversely, if $N(x) \in L_{\bar{A}}$ for some $x \in \mathcal{E}^*$ such that $x\sigma(x) = 1$ then $N(x) \in ker(\phi)$. □

Hence if the field k is C_1 (for example, finite field) or it does not admit degree three extensions (real closed fields, algebraically closed fields etc.), $L^*/N(E^*)$ is trivial. From Corollary 8.2.11, it follows that every element in $G(\mathfrak{C}/L)$, with irreducible characteristic polynomial, is conjugate to its inverse. In particular, combining with Theorem 8.1.9, it follows that every semisimple element in $G(k)$ is conjugate to its inverse.

Proposition 8.2.14. *With notation as above, let L be a quadratic field extension of k and let $S \in SU(H)$ be an element with irreducible characteristic polynomial over L, satisfying $\bar{S} = S^{-1}$. Let $\mathcal{E} = L[X]/\chi_S(X)$, a degree three field extension of L, and assume $L^1/N(\mathcal{E}^1)$ is nontrivial, where $L^1 = \{x \in L \mid x\sigma(x) = 1\}$, $\mathcal{E}^1 = \{x \in \mathcal{E} \mid x\sigma(x) = 1\}$ and σ is the extension of the nontrivial automorphism of L to $\mathcal{E}$. Then there exists an element $A \in SU(H)$ with characteristic polynomial same as the characteristic polynomial of S, which can not be written as $A = A_1A_2$ where $\bar{A}_i = A_i^{-1}$ and $A_i \in SU(H)$. The corresponding element t in $G(\mathfrak{C}/L)$ is not a product of two involutions in $G = \mathrm{Aut}(\mathfrak{C})$ and hence not real in G.*

Proof. Let $b \in L^1$ such that $b^2 \notin N(\mathcal{E}^1)$. Put $D = \mathrm{diag}(b, 1, 1)$ and $A = DSD^{-1}$, then A belongs to $SU(H)$. Now suppose $A = A_1A_2$ with $\bar{A}_i = A_i^{-1}$ and $A_i \in SU(H)$. Then $A = A_1A_2 = DSD^{-1} = DSDD^{-2}$. Put $T_1 = DSD$ and $T_2 = D^{-2}$, then $\bar{T}_i = T_i^{-1}$. Since $A_2AA_2^{-1} = \bar{A}^{-1}$ and $T_2AT_2^{-1} = \bar{A}^{-1}$, we have $T_2^{-1}A_2 \in \mathcal{Z}_{U(V,\mathfrak{h})}(A)$, i.e., $T_2^{-1}A_2 = f(A)$ for some $f(X) \in L[X]$ (see the Remark after Corollary 8.2.11). Then $b^2 = \det(T_2^{-1}) = \det(T_2^{-1}A_2) = \det(f(A)) \in N(\mathcal{E}^*)$, a contradiction. □

Remark 8.2.15. If we choose S in the theorem above with characteristic polynomial separable, then the element A, constructed in the proof, is a semisimple element in an indecomposable maximal torus, contained in $SU(H)$, which is not real.

We recall that any central division algebra of degree three is cyclic ([**P**], Theorem, Section 15.6). Let L be a quadratic field extension of k. Let F be a degree three cyclic extension of k and we denote $E = F.L$. Let us denote the generator of the Galois group of F over k by τ. Let $A = F \oplus Fu \oplus Fu^2$ with $udu^{-1} = \tau(d)$ for all $d \in F$ and $u^3 = a \in k^*$. Then A, denoted by (F, τ, a), is a cyclic algebra of degree three over k. Recall also that (F, τ, a) is a division algebra if and only if $a \notin N_{F/k}(F^*)$. We denote the relative Brauer group of F over k by $B(F/k)$, i.e., the group of Brauer classes of central simple algebras over k, which split over F. We define a map $\phi\colon B(F/k) \longrightarrow B(E/L)$ by $[(F,\tau,a)] \mapsto [(E,\tau,a)]$ (which is the same as the map $[D] \mapsto [D \otimes L]$). This map is well defined ([**P**], Section 15.1, Corollary c) and is an injective map since $ker(\phi) = \{[(F,\tau,a)] \in B(F/k) \mid a \in k^*, a \in N_{E/L}(E^*)\} = \{[(F,\tau,a)] \in B(F/k) \mid a \in N_{F/k}(F^*)\}$. We have a commutative diagram,

$$\begin{tikzcd}
k^*/N_{F/k}(F^*) \arrow[r, "\cong"] \arrow[d] & B(F/k) \arrow[d, "\phi"] \\
L^*/N_{E/L}(E^*) \arrow[r, "\cong"] & B(E/L)
\end{tikzcd}$$

The vertical maps are injective in the above diagram. We have the following exact sequence,

$$1 \longrightarrow (N_{E/L}(E^*)k^*)/N_{E/L}(E^*) \longrightarrow L^*/N_{E/L}(E^*) \longrightarrow L^1/N_{E/L}(E^1) \longrightarrow 1$$

where $(N_{E/L}(E^*)k^*)/N_{E/L}(E^*) \cong k^*/N_{F/k}(F^*)$. Hence, from the commutativity of the above diagram, we get $B(E/L)/\phi(B(F/k)) \cong L^1/N_{E/L}(E^1)$.

This shows $L^1/N_{E/L}(E^1)$ is nontrivial, if and only if there exists a central division algebra D over L which splits over E and it does not come from a central division algebra over k, split by F. Over number field for such a construction we refer to [**K**] (Chapter V, Proposition 1).

8.3. $SL(3) \subset G$

We continue here with proof of the Theorem 8.1.8. Let us assume now that $L \cong k \times k$. We have seen in Section 3.2 that $G(\mathfrak{C}/L) \cong SL(U) \cong SL(3)$. Let t_0 be an element in $G(\mathfrak{C}/L)$ and denote its image in $SL(3)$ by A. We assume that the characteristic polynomial of $A \in SL(3)$ is equal to its minimal polynomial over k.

Lemma 8.3.1. *Let the notation be fixed as above. Let t_0 be an element in $G(\mathfrak{C}/L)$ which does not have a fixed point outside L. Suppose that $\exists h \in G = \mathrm{Aut}(\mathfrak{C})$, such that $ht_0h^{-1} = t_0^{-1}$. Then $h(L) = L$.*

Proof. Suppose that $h(L) \not\subset L$. Then we claim that $\exists x \in L \cap \mathfrak{C}_0$ such that $h(x) \notin L$. For this, let $y \in L$ be such that $h(y) \notin L$. Let $x = y - \frac{1}{2}tr(y)1$. Then $tr(x) = 0$ and if $h(x) \in L$ then $h(y) \in L$, a contradiction. Hence we have $x \in L \cap \mathfrak{C}_0$ with $h(x) \notin L$. Also since $t_0(x) = x$, we have,

$$t_0(h(x)) = ht_0^{-1}(x) = h(x).$$

Therefore, t_0 fixes $h(x) \in \mathfrak{C}_0$ and $h(x) \notin L$, a contradiction. Hence any $h \in \mathrm{Aut}(\mathfrak{C})$, conjugating t_0 to t_0^{-1} in G, leaves L invariant. □

From Theorem 7.1.2 it follows that if t_0 is conjugate to t_0^{-1} in $G(\mathfrak{C}/L) \cong SL(3)$ then t_0 is strongly real. Hence we may assume that A is not real in $SL(3)$.

Theorem 8.3.2. *With notation fixed as above, let A be the matrix of t_0 in $SL(3)$. Let A be not real in $SL(3)$. Then t_0 is conjugate to t_0^{-1} in $G = \mathrm{Aut}(\mathfrak{C})$, if and only if A is conjugate to ${}^tA$ in $SL(3)$.*

Proof. Let $h \in G$ be such that $ht_0h^{-1} = t_0^{-1}$. In view of the lemma above, we have $h(L) = L$. We may, without loss of generality (up to conjugacy by an automorphism), assume that

$$\mathfrak{C} = \left\{ \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} \mid \alpha, \beta \in k; v, w \in k^3 \right\} \text{ with L} = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \mid \alpha, \beta \in \mathrm{k} \right\}$$

By Proposition 3.2.3, h belongs to $G(\mathfrak{C}/L) \rtimes H$. Clearly h does not belong to $G(\mathfrak{C}/L)$ since we have assumed A is not real in $SL(3)$. Hence $h = g\rho$ for some $g \in G(\mathfrak{C}/L)$. Let A denote the matrix of t_0 on U in $SL(3)$ and B that of g. Then, a direct computation gives,

$$ht_0h^{-1} \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} = \begin{pmatrix} \alpha & B{}^tA^{-1}B^{-1}v \\ {}^tB^{-1}A{}^tBw & \beta \end{pmatrix},$$

and

$$t_0^{-1} \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} = \begin{pmatrix} \alpha & A^{-1}v \\ {}^tAw & \beta \end{pmatrix}.$$

Therefore,

$$ht_0h^{-1} = t_0^{-1} \Leftrightarrow A = B{}^tAB^{-1}.$$

Hence, t_0 is conjugate to t_0^{-1} in $G(k)$ if and only if A is conjugate to ${}^tA$ in $SL(3)$. □

Lemma 8.3.3. *Let A be a matrix in $SL(n)$ with its characteristic polynomial equal to its minimal polynomial. Then A is conjugate to ${}^tA$ in $SL(n)$ if and only if A is a product of two symmetric matrices in $SL(n)$.*

Proof. Any matrix conjugating A to ${}^tA$ is necessarily symmetric ([**TaZ**], Theorem 2). Let S be a symmetric matrix which conjugates A to ${}^tA$ in $SL(n)$, i.e., $SAS^{-1} = {}^tA$. Let $B = SA = {}^tAS$. Then B is symmetric and belongs to $SL(n)$. Hence $A = S^{-1}B$ is a product of two symmetric matrices in $SL(n)$. Conversely, let A be a product of two symmetric matrices from $SL(n)$, say $A = S_1S_2$. Then S_2 conjugates A to ${}^tA$. □

We need the following result from ([**W1**]), (cf. also [**L**]),

Proposition 8.3.4. *Let $\mathfrak{C}$ be a (split) octonion algebra over a field k of characteristic not 2. Let L be a split two-dimensional subalgebra of $\mathfrak{C}$. An element $\eta \in G(\mathfrak{C}/L)$ is a product of two involutory automorphisms if and only if the corresponding matrix in $SL(3)$ can be decomposed into a product of two symmetric matrices in $SL(3)$.*

We have,

Theorem 8.3.5. *Let t_0 be an element in $G(\mathfrak{C}/L)$, with notation as in this section. Let us assume that the matrix A of t_0 in $SL(3)$ has characteristic polynomial equal to its minimal polynomial. Then, t_0 can be conjugated to t_0^{-1} in $G = Aut(\mathfrak{C})$, if and only if t_0 is a product of two involutions in $G(k)$.*

Proof. First, let t_0 be real in $G(\mathfrak{C}/L)$. Then, A is real in $SL(3)$ and hence it is strongly real (see Theorem 7.1.2). Thus the element t_0 is strongly real in $G(k)$. Now we assume t_0 is not real in $G(\mathfrak{C}/L)$, i.e., A is not real in $SL(3)$. In this case, the element t_0 can be conjugated to t_0^{-1} in $G(k)$ if and only if, A can be conjugated to ${}^tA$ in $SL(3)$ (Theorem 8.3.2). This is if and only if, A is a product of two symmetric matrices in $SL(3)$ (Lemma 8.3.3). By Proposition 8.3.4, this is if and only if t_0 is a product of two involutions in $\mathrm{Aut}(\mathfrak{C})$. □

We continue our analysis and produce examples of nonreal semisimple elements. We derive a necessary and sufficient condition that a matrix A in $SL(3)$, with irreducible characteristic polynomial, be conjugate to ${}^tA$ in $SL(3)$. We have, more generally,

Theorem 8.3.6. *Let A be a matrix in $SL(n)$ with characteristic polynomial $\chi_A(X)$ irreducible. Let $E = k[X]/\chi_A(X) \cong k[A]$ be the field extension of k of degree n given by $\chi_A(X)$. Then A is conjugate to ${}^tA$ in $SL(n)$, if and only if, for every $T \in GL(n)$ with $TAT^{-1} = {}^tA$,* $\det(T)$ *is a norm from E.*

Proof. Fix a $T_0 \in GL(n)$ such that $T_0AT_0^{-1} = {}^tA$ and define a map,

$$\begin{array}{rcl}\{T \in M_n(k) \mid TA = {}^tAT\} & \longrightarrow & k[A] \\ T & \mapsto & T_0^{-1}T\end{array}$$

This map is an isomorphism of vector spaces. Since if $T \in M_n(k)$ is such that $TA = {}^tAT$ then $T_0^{-1}T$ belongs to $\mathcal{Z}(A)$ $(= k[A]$, as the characteristic polynomial of A is the same as its minimal polynomial). To prove the assertion, suppose $T_0 \in SL(n)$

conjugates A to ${}^tA$. But with the above bijection, $T_0^{-1}T = p(A)$ for some $p(A) \in k[A]$, $p(X) \in k[X]$. Hence $\det(p(A)) = \det(T)$, i.e. $\det T$ is a norm from E.

Conversely suppose there exists $T \in GL(n)$ with $TAT^{-1} = {}^tA$ and $\det(T)$ is a norm from E. Then there exists $p(X) \in k[X]$ such that $\det(p(A)) = \det(T)^{-1}$. Thus $\det(Tp(A)) = 1$ and
$(Tp(A))A(p(A)^{-1}T^{-1}) = TAT^{-1} = {}^tA$. □

In the case under discussion, $A \in SL(3)$ has irreducible characteristic polynomial. Hence, $E \cong k[A] \cong \mathcal{Z}_{M_3(k)}(A)$ is a cubic field extension of k . We combine the previous two theorems to get,

Corollary 8.3.7. *Let A be a matrix in $SL(3)$ with irreducible characteristic polynomial. With notation as above, suppose $k^*/N(E^*)$ is trivial. Then A can be conjugated to ${}^tA$ in $SL(3)$ and hence t_0 can be conjugated to t_0^{-1} in* $\mathrm{Aut}(\mathfrak{C})$.

If k a C_1 field (e.g., a finite field) or k does not admit cubic field extensions (e.g., k real closed, algebraically closed), the above criterion is satisfied automatically. Hence every element in $G(\mathfrak{C}/L)$, for $L = k \times k$, with irreducible characteristic polynomial over k, is conjugate to its inverse in $G(k)$. In particular, combining this with Theorem 8.1.9, we see that every semisimple element in $G(k)$ is real.

We shall give a cohomological proof of reality for G_2 (and other groups with appropriate hypothesis) over fields k with $cd(k) \leq 1$ (see the Theorem 9.3.3).

In view of these results, to produce an example of a semisimple element of $G = \mathrm{Aut}(\mathfrak{C})$ that is not conjugate to its inverse in $\mathrm{Aut}(\mathfrak{C})$, we need to produce a semisimple element which is a product of three involutions but not a product of two involutions. We shall show that, for the split form G of G_2 over $k = \mathbb{Q}$ or $k = \mathbb{Q}_p$, there are semisimple elements in $G(k)$ which are not conjugate to their inverses in $G(k)$. We shall do this in next section by exhibiting explicit elements in G_2 over a finite field, which are not real. These necessarily are not semisimple or unipotent (see the Remark 8.4.8). We adapt a slight variant of an example in ([**W2**], [**L**]) for our purpose, there the issue is bireflectionality of G_2. The following lemma will be used to produce nonreal elements in G_2 in next section.

Lemma 8.3.8. *Let k be a field and let S be a symmetric matrix in $SL(3)$ whose characteristic polynomial $p(X)$ is irreducible over k. Let $E = k[X]/ < p(X) >$, the degree three field extension of k given by $p(X)$. Further suppose that $k^*/N(E^*)$ is not trivial. Then there exists a matrix in $SL(3)$, with characteristic polynomial $p(X)$, which is not a product of two symmetric matrices in $SL(3)$.*

Proof. Let $b \in k^*$ such that $b^2 \notin N(E^*)$. Consider $D = \mathrm{diag}(b, 1, 1)$, a diagonal matrix and put $A = DSD^{-1}$. Then $A \in SL(3)$. We claim that A is not a product of two symmetric matrices from $SL(3)$. Assume the contrary. Suppose $A = DSD^{-1} = S_1S_2$ where $S_1, S_2 \in SL(3)$ and symmetric. Then

$$A = DSD^{-1} = (DSD)D^{-2} = S_1S_2.$$

Let $T_1 = DSD,\ T_2 = D^{-2}$. Then ${}^tT_i = T_i,\ i = 1, 2$ and $A = T_1T_2 = S_1S_2$. Therefore,

$${}^tA = T_2T_1 = T_2AT_2^{-1} = S_2S_1 = S_2AS_2^{-1}.$$

Since the characteristic polynomial of A is irreducible, by the proof of Theorem 8.3.6, $D^2S_2 = T_2^{-1}S_2 \in \mathcal{Z}(A) = k[A] \cong E$. Which implies $S_2 = D^{-2}f(A)$ for some polynomial $f(X) \in k[X]$. Taking determinants, we get

$$1 = \det S_2 = \det D^{-2} \det(f(A)),$$

i.e., $b^2 = \det(f(A)) \in N(E^*)$, contradicting the choice of $b \in k$. Hence A can not be written as a product of two symmetric matrices from $SL(3)$. □

8.4. Examples of Nonreal Elements

In this section we produce examples of nonreal semisimple elements in groups of type G_2. In [**W2**] and [**L**], there are examples of elements which are product of three involutions but not two. These are examples of nonreal elements. First we produce nonreal semisimple elements which are product of three involutions but not two in G_2 over number fields and over fields $\mathbb{Q}$ and $\mathbb{Q}_p$. In the view of Theorem 8.1.7 these elements are not real. We also produce examples of nonreal elements in G_2 over finite fields. Note that over finite fields every semisimple as well as unipotent element is real. Hence the elements produced are of mixed kind, i.e., neither semisimple nor unipotent.

8.4.1. Nonreal Elements in G_2 over Number Fields.

We use Proposition 8.2.14 to construct non-real elements in G_2 over number fields and use the notation introduced there.

Lemma 8.4.1. *Let k be a number field and L a quadratic field extension of k. Let F be a cyclic extension of degree 3 over k. Let us denote $E = F.L$. Then $L^1/N_{E/L}(E^1)$ is nontrivial.*

Proof. The proof follows by looking at a place of E over L which is unramified of degree 3. □

We proceed to construct an example of the situation required in Proposition 8.2.14.

Proposition 8.4.2. *Let k be a number field. There exist octonion algebras $\mathfrak{C}$ over k such that not every (semisimple) element in* $\mathrm{Aut}(\mathfrak{C})$ *is real.*

Proof. We use Proposition 8.2.14 here. Let L be a quadratic field extension of k. Let F be a degree three cyclic extension of k. Then we have $E = F.L$, a degree three cyclic extension of L. We denote the extension of the nontrivial automorphism of L over k to E over L by σ, which is the identity automorphism when restricted to F. Sometimes we write $\bar{x} = \sigma(x)$ for $x \in E$. Let us consider E as a vector space over L. We consider the trace hermitian form on E defined as follows:

$$\begin{array}{rcl} tr\colon E \times E & \longrightarrow & L \\ tr(x, y) & = & tr_{E/L}(x\bar{y}). \end{array}$$

The restriction of this form to F is the trace form $tr\colon F \times F \longrightarrow k$, given by $tr(x, y) = tr_{F/k}(xy)$. We choose an orthogonal basis of F over k, say $\{f_1, f_2, f_3\}$, with respect to the trace form, and extend it to a basis of E/L. Then the bilinear form tr with respect to this basis has diagonalization $< 1, 2, 2 >$ ([**KMRT**], Section 18.31). We have $disc(tr) = 4 \in N_{L/k}(L^*)$. Hence (E, tr) is a rank 3 hermitian space over L with trivial discriminant and $SU(E, tr)$ is isomorphic to $SU(H)$ where $H = \mathrm{diag}(1, 2, 2)$. We choose an element $1 \neq a \in T^1 - L^1$, where $T^1 = \{x \in E \mid x\bar{x} = 1, N_{E/L}(x) = 1\}$. Let us consider the left homothety map,

$$\begin{array}{rcl} l_a\colon E & \longrightarrow & E \\ l_a(x) & = & ax \end{array}$$

Since $a \in T^1 - L^1$, the characteristic polynomial $\chi(X)$ of l_a is the minimal polynomial of a over L, which is irreducible of degree 3 over L. Next we prove that $l_a \in SU(E, tr)$. This is so since,

$$tr(l_a(x), l_a(y)) = tr(ax, ay) = tr_{E/L}(ax\bar{a}\bar{y}) = tr_{E/L}(x\bar{y}) = tr(x, y).$$

Let $S = (s_{ij})$ denote the matrix of l_a with respect to the chosen basis $\{f_1, f_2, f_3\}$ of F over k. Then the matrix of $l_{\bar{a}}$ is $\bar{S} = (\bar{s_{ij}})$. Also, since $a\bar{a} = 1$, we have $S\bar{S} = 1$. Thus we have a matrix S in $SU(H)$, for $H =< 1, 2, 2 >$, satisfying the conditions of Proposition 8.2.14.

Now, let $L = k(\gamma)$ with $\gamma^2 = c \in k^*$. We write $Q = k \oplus F$. Since (F, tr) is a quadratic space with trivial discriminant, we can define a quaternionic multiplication on Q (Proposition 3.1.6), denote its norm by N_Q. We double Q with $\gamma^2 = c \in k^*$ to get an octonion algebra $\mathfrak{C} = Q \oplus Q$ with multiplication,

$$(x, y)(u, v) = (xu + c\bar{v}y, vx + y\bar{u})$$

and the norm $N((x, y)) = N_Q(x) - cN_Q(y)$. We choose a basis $\{1, a, b, ab\}$ of Q, orthogonal for N_Q, so that N_Q has diagonalization $< 1, 1, 2, 2 >$ with respect to this basis. This gives a basis $\{(1, 0), (a, 0), (b, 0), (ab, 0), (0, 1), (0, a), (0, b), (0, ab)\}$ of $\mathfrak{C}$ and the diagonalization of N with respect to this basis is $< 1, 1, 2, 2, -c, -c, -2c, -2c >$. We observe that the subalgebra $k \oplus k \subset \mathfrak{C}$ is isomorphic to L and $L^\perp = F \times F$ is a 3 dimensional vector space over L with hermitian form $< 1, 2, 2 >$. Hence $SU(L^\perp, \mathfrak{h})$, with respect to the basis $\{(a, 0), (b, 0), (ab, 0)\}$ of $L^\perp$, is $SU(H)$ for $H =< 1, 2, 2 >$. Hence, from the discussion in previous paragraph, we have an element of required type in $SU(L^\perp, \mathfrak{h})$.

By Lemma 8.4.1, $L^1/N(E^1)$ is nontrivial. It follows from Proposition 8.2.7 and Proposition 8.2.14 that not all (semisimple) elements in Aut($\mathfrak{C}$), which are contained in the subgroup $SU(E, tr)$, are real. □

Corollary 8.4.3. *Let k be a totally real number field. Then there exists an octonion division algebra $\mathfrak{C}$ over k such that not every element in* Aut($\mathfrak{C}$) *is real. Hence there exist (semisimple) elements in* Aut($\mathfrak{C}$)*, which are the product of three involutions but not the product of two involutions.*

Proof. We recall from Lemma 3.1.5 that if the k-quadratic form $\mathfrak{q}_{\mathfrak{b}}$, corresponding to the bilinear form $\mathfrak{b}\colon E \times E \longrightarrow k$, defined by $\mathfrak{b}(x, y) = tr_{E/L}(x\bar{y}) + tr_{E/L}(\bar{x}y)$, is anisotropic then the octonion algebra $\mathfrak{C}$, as constructed in the proof of the above proposition, is a division algebra. In case when k is a totally real number field and $L = k(i)$, the diagonalization of $\mathfrak{q}_{\mathfrak{b}}$ is $< 1, 2, 2, 1, 2, 2 >$, which is clearly anisotropic over k. □

Remarks 8.4.4. **1.** We note that the quadratic form $\mathfrak{q}_{\mathfrak{b}}$ as above, can be isotropic for imaginary quadratic number fields. For example if $k = \mathbb{Q}(\sqrt{-2})$, $\mathfrak{q}_{\mathfrak{b}}$ has diagonalization $< 1, -1, -1, -c, c, c >$, which is isotropic. Hence the octonion algebra $\mathfrak{C}$ in this case is split. Therefore, indecomposable tori in subgroups $SU(V, \mathfrak{h}) \subset$ Aut($\mathfrak{C}$) exist in all situations, whether $\mathfrak{C}$ is division or not. And in either case, there are nonreal elements.

2. It seems likely that existence of nonreal elements in $G(k)$ for k a number field should follow from existence of such elements in $G(k)$ for k local.

8.4.2. Nonreal Elements in Split G_2 over $\mathbb{Q}$ and $\mathbb{Q}_p$. In view of Theorem 8.3.5 and its proof, the element A corresponds to an element in $\mathrm{Aut}(\mathfrak{C})$ which can not be conjugated to its inverse. If we choose the matrix S as in the statement of the Lemma 8.3.8, to have separable characteristic polynomial, the matrix A, as constructed in the proof, corresponds to a semisimple element in an indecomposable torus contained in $SL(3) \subset G = \mathrm{Aut}(\mathfrak{C})$, which is not real.

Theorem 8.4.5. *Let G be a split group of type G_2 over $k = \mathbb{Q}$ or $\mathbb{Q}_p$. Then there exists a semisimple element in $G_2(k)$ which is not conjugate to its inverse.*

Proof. Reality over $\mathbb{Q}_p$: Let $k = \mathbb{Q}_p,\ p \neq 2$. Let $p(X)$ be an irreducible monic polynomial of degree n, with coefficients in $\mathbb{Q}_p$. By a theorem of Bender ([**Be1**]), there exists a symmetric matrix with $p(X)$ as its characteristic polynomial, if and only if, for the field extension $E = \mathbb{Q}_p[X]/(p(X))$, there exists α in E^* such that $(-1)^{\frac{n(n-1)}{2}}N(\alpha)$ belongs to $(\mathbb{Q}_p^*)^2$. We choose E as the (unique) unramified extension of $\mathbb{Q}_p$ of degree 3. Then, E is a cyclic extension of $\mathbb{Q}_p$. We choose $\beta \in E^*,\ N(\beta) = 1$ so that $E = \mathbb{Q}_p(\beta)$. Let $p(X)$ be the minimal polynomial of β over $\mathbb{Q}_p$. Then, applying Bender's result, there is a symmetric matrix A over $\mathbb{Q}_p$, with characteristic polynomial $p(X)$. Since $N(\beta) = 1$, A belongs to $SL(3, \mathbb{Q}_p)$. We have, $\mathbb{Q}_p^*/N(E^*) \cong \mathcal{Z}/3\mathcal{Z}$ (see [**P**], Section 17.9), hence $(\mathbb{Q}_p^*)^2 \not\subset N(E)$. Therefore we are done by Lemma 8.3.8, combined with Proposition 8.3.4 and Theorem 8.3.5.

This example shows that there exist semisimple elements in $G = \mathrm{Aut}(\mathfrak{C})$ over $k = \mathbb{Q}_p$, which are not a product of two involutions and hence must be product of three involutions, by ([**W2**]). In particular, reality for G_2 fails over $\mathbb{Q}_p$ (Theorem 8.1.7).

Reality over $\mathbb{Q}$: A polynomial $p(X) \in K[X]$ is called K-real if every real closure of K contains the splitting field of $p(X)$ over K. Bender ([**Be2**], Theorem 1) proves that whenever we have K, an algebraic number field, and $p(X)$ a monic K-polynomial with an odd degree factor over K, then $p(X)$ is K-real if and only if it is the characteristic polynomial of a symmetric K-matrix.

Let $p(X) = X^3 - 3X - 1$. Then all roots of this polynomial are real but not rational. This polynomial is therefore irreducible over $\mathbb{Q}$ and by Bender's theorem stated above, $p(X)$ is the characteristic polynomial of a symmetric matrix. Note that $K = \mathbb{Q}[X]/ < p(X) >$ is a degree 3 cyclic extension of $\mathbb{Q}$.

We recall that for a cyclic field extension K of k, the relative Brauer group $B(K/k) \cong k^*/N_{K/k}(K^*)$ (refer [**P**], Section 15.1, Proposition b). It is known that if K/k is a nontrivial extension of global fields, then $B(K/k)$ is infinite (refer [**FKS**], Corollary 4). Therefore, for K chosen as above, $\mathbb{Q}^*/N(K^*)$ is not trivial. Hence all conditions required by Lemma 8.3.8 are satisfied by the polynomial $p(X)$ and we get a semisimple element $t_0 \in G_2(\mathbb{Q})$ which is not conjugate to its inverse, using Lemma 8.3.8, Proposition 8.3.4 and Theorem 8.3.5. □

8.4.3. Nonreal Elements in G_2 over Finite Fields. Let $k = \mathcal{F}_q$ be a finite field. We have shown (Theorem 8.1.7) that semisimple elements and unipotent elements in $G(k)$ are real in $G(k)$. We now construct an element in $G(k)$ which is not conjugate to its inverse. Let $\mathfrak{C}$ be the split octonion algebra over k, assume that the characteristic of k is not 2 or 3. We use the matrix model for the split octonions, as introduced in the Section 3.1. Let L be the split diagonal subalgebra of $\mathfrak{C}$. We assume that k contains primitive third roots of unity. We have, $G(\mathfrak{C}/L) \cong SL(3)$. Let ω be a primitive third root of unity in k. Let

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

Then $A \in SL(3)$ and the minimal polynomial (=characteristic polynomial) of A is $p(X) = (X - \omega)^3$. Let $b \in k$ be such that the polynomial $X^3 - b^2$ is irreducible over k (this is possible due to characteristic assumptions). Let $D = \mathrm{diag}(b, 1, 1)$ and $B = DAD^{-1}$. Then $B \in SL(3)$ and has the same minimal polynomial as A. Note that B is neither semisimple, nor unipotent. Let $t \in G(\mathfrak{C}/L)$ be the automorphism of $\mathfrak{C}$ corresponding to B. It is clear that the fixed point subalgebra of t is precisely L.

Theorem 8.4.6. *The element $t \in G(\mathfrak{C}/L)$ as above, is not real.*

Proof. If not, suppose for $h \in G(k)$, $hth^{-1} = t^{-1}$. Then, since t fixes precisely L pointwise, we have $h(L) = L$. Therefore $h \in G(\mathfrak{C}, L) \cong G(\mathfrak{C}/L) \rtimes H$, where $H =< \rho >$ is as in Proposition 3.2.3. If $h \in G(\mathfrak{C}/L)$, conjugacy of t and t^{-1} by h would imply conjugacy of B and B^{-1} in $SL(3)$. But this can not be, since ω is the only root of $p(X)$. Thus $h = g\rho$ for $g \in G(\mathfrak{C}/L)$. Now, by exactly the same calculation as in the proof of Theorem 8.3.2, conjugacy of t and t^{-1} in $G(k)$ is equivalent to conjugacy of B and ${}^tB$ in $SL(3)$. Let $CBC^{-1} = {}^tB$ with $C \in SL(3)$. Let

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

Then $T \in SL(3)$ is symmetric and $TAT^{-1} = {}^tA$. Hence A is a product of two symmetric matrices in $SL(3)$, say $A = T_1T_2$ with $T_i \in SL(3)$, symmetric (see the proof of Lemma 8.3.3). But $CBC^{-1} = {}^tB$ gives $(DCD)A = {}^tA(DCD)$. Therefore, by an argument used in the proof of Theorem 8.3.6, using the fact that the characteristic polynomial is equal to the minimal polynomial of A, we have, $DCD = T_2f(A)$ for some polynomial $f \in k[X]$. Taking determinants, we get $b^2 = \det(f(A)) = f(\omega)^3$. But this contradicts the choice of b. Hence t is not real. □

A similar construction can be done for the subgroup $SU(V, \mathfrak{h}) \subset G$. We continue to assume that k is a finite field with characteristic different from $2, 3$. We first note that the (split) octonion algebra contains all quadratic extensions of k. We assume that 2 is a square in k and that k contains no primitive cube roots of unity. Let L be a quadratic extension of k containing a primitive cube root of unity ω. Let $b \in L$ with $N_{L/k}(b) = 1$ such that the polynomial $X^3 - b^2$ is irreducible over L. Let $\alpha \in L$ with $N_{L/k}(\alpha) = -1$. Let

$$A = \begin{pmatrix} \omega + \frac{1}{4} & \frac{1}{2} & -\frac{1}{4}\alpha \\ -\frac{1}{2}\omega^2 & \omega & \frac{1}{2}\alpha\omega^2 \\ -\frac{1}{4}\overline{\alpha} & -\frac{1}{2}\overline{\alpha} & \omega - \frac{1}{4} \end{pmatrix},$$

then $A \in SU(3)$ and the minimal polynomial (= characteristic polynomial) of A over L is $(X - \omega)^3$. Let F be a cubic extension of k and $E = F.L$. Then E is a cyclic extension of L and we have the trace hermitian form as defined in Proposition 8.4.2, on E. We fix an orthogonal basis for F over k for the trace bilinear form and extend it to a basis of E over L. Then the trace hermitian form has diagonalization $< 1, 1, 1 >$. We construct $\mathfrak{C} = L \oplus E$ with respect to the hermitian space (E, tr), as in Section 3. Then $SU(L^{\perp}, h) \cong SU(3)$. Let $D = \mathrm{diag}(b, 1, 1)$ and $B = DAD^{-1}$. Then $B \in SU(3)$ and has the same minimal polynomial as A. Note that B is neither semisimple, nor unipotent. Let t denote the automorphism of $\mathfrak{C}$ corresponding to B. Then the fixed point subalgebra of t in $\mathfrak{C}$ is precisely L. We have,

Theorem 8.4.7. *The element $t \in G(\mathfrak{C}/L)$ as above, is not real.*

Proof. Suppose t is real in $G(k)$. Then there is $h \in G(k)$ such that $hth^{-1} = t^{-1}$. Since the fixed point subalgebra of t is L, we have $h(L) = L$. Thus, by Proposition 3.2.5, $h \in G(\mathfrak{C}, L) \cong G(\mathfrak{C}/L) \rtimes H$, where $H =< \rho >$ is as in Proposition 3.2.5. If $h \in G(\mathfrak{C}/L)$, then B and B^{-1} would be conjugate in $SU(3)$, but that can not be since ω is the only eigenvalue for B. Hence $h = g\rho$ for $g \in G(\mathfrak{C}/L)$. Then, conjugacy of t and t^{-1} in $G(k)$ is equivalent to conjugacy of $\overline{B}$ and B^{-1} in $SU(3)$, by the same calculation as in the proof of Th. 6.5. By Lemma 8.2.6, this is if and only if $B = B_1B_2$ with $B_i \in SU(3)$ and $\overline{B_i}B_i = 1$. But then $B = DAD^{-1} = B_1B_2$ and hence $A = (D^{-1}B_1D^{-1})(DB_2D) = A_1A_2$, say. Then $A_i \in U(3)$ and $\overline{A_i}A_i = 1$. Let $C \in SU(3)$ be such that $C\overline{B}C^{-1} = B^{-1}$. Then $C\overline{DAD^{-1}}C^{-1} = DA^{-1}D^{-1}$. This gives, $(D^{-1}CD^{-1})\overline{A}(DC^{-1}D) = A^{-1}$. Hence, by Lemma 8.2.6, $A = T_1T_2$ with $T_i \in SU(3)$, $\overline{T_i}T_i = 1$. Therefore, by a similar argument as in the remark following Corollary 8.2.11, we must have, $T_1A_1^{-1} = f(A)$ for a polynomial $f(X) \in L[X]$. Taking determinants, we get $b^{-2} = f(\omega)^3$, contradicting the choice of b. Therefore t is not real in $G(k)$. □

Remarks 8.4.8. 1. Our results in fact show that if an element in $G(k)$, for a group G of type G_2, is conjugate to its inverse in $G(k)$, the conjugating element can be chosen to be an involution. The same is true for unipotents (these are always conjugate to their inverses).

2. The obstruction : From our results, we see that semisimple elements belonging to decomposable tori are always product of two involutions and hence real in $G(k)$. For semisimple elements belonging to an indecomposable maximal torus T, the obstruction to reality is measured by $L^1/N(\mathcal{E}^1)$, where $T \subset SU(V, \mathfrak{h}) \cong SU(\mathcal{E}, \mathfrak{h}^{(u)})$ is given by $T = \mathcal{E}^1$ and $\mathcal{E}$ is a cubic field extension of L. In the other case, when $T \subset SL(3)$, the obstruction is measured by $k^*/N(\mathcal{F}^*)$, where $\mathcal{F}$ is a cubic field extension of k. In both cases, the obstruction has a Brauer group interpretation. When $T \subset SL(3) \subset G$ is an indecomposable maximal torus, coming from a cyclic cubic field extension $\mathcal{F}$ of k, the obstruction to reality for elements in $T(k)$, is the relative Brauer group $B(\mathcal{F}/k)$. For an indecomposable torus $T \subset SU(\mathcal{E}, \mathfrak{h}^u) \subset G$, where $\mathcal{E}$ is a cubic cyclic field extension of L, the obstruction is the quotient $B(\mathcal{E}/L)/\phi(B(\mathcal{F}/k)$, where $\mathcal{F}$ is the subfield of $\mathcal{E}$, fixed by the involution σ on $\mathcal{E}$ and ϕ is the base change map $B(\mathcal{F}/k) \longrightarrow B(\mathcal{E}/L)$.

8.5. Centralizers in Anisotropic G_2

In this section, we compute conjugacy classes of centralizers in compact G_2. Let G be an anisotropic group of type G_2 over a field k. Then there exists $\mathfrak{C}$, an octonion division algebra over k, such that $G \cong \mathrm{Aut}(\mathfrak{C})$. By abuse of notation we write $G = \mathrm{Aut}(\mathfrak{C})$. We fix these notation for this section. First, we calculate centralizer of an element in G. Let $t \in G$. We denote the centralizer of t in G by $\mathcal{Z}_G(t) = \{g \in G \mid gt = tg\}$. Since G is anisotropic, every element in G is semisimple and leaves a subalgebra of $\mathfrak{C}$ fixed pointwise (Lemma 8.1.3). We denote the subalgebra of fixed points of t by $\mathfrak{C}^t = \{x \in \mathfrak{C} \mid t(x) = x\}$.

Proposition 8.5.1. *Let G be an anisotropic group of type G_2 over k. Let $\mathfrak{C}$ be the octonion division algebra over k such that $G = \mathrm{Aut}(\mathfrak{C})$. Let $t \in G$. Then $\mathfrak{C}^t$ is a composition subalgebra of $\mathfrak{C}$ and the centralizer $\mathcal{Z}_G(t) \subset G(\mathfrak{C}, \mathfrak{C}^t)$.*

Proof. The subalgebra $\mathfrak{C}^t \subset \mathfrak{C}$ is a composition subalgebra as $\mathfrak{C}$ is division. Let $g \in \mathcal{Z}_G(t)$. Then,

$$t(g(x)) = g(x), \ \forall x \in \mathfrak{C}^t.$$

Hence $g(x) \in \mathfrak{C}^t$, $\forall x \in \mathfrak{C}^t$. This shows that $g \in G(\mathfrak{C}, \mathfrak{C}^t)$ and $\mathcal{Z}_G(t) \subset G(\mathfrak{C}, \mathfrak{C}^t)$. □

We note that t restricted to $\mathfrak{C}_0$, trace zero space of $\mathfrak{C}$, is an element of special orthogonal group of an odd dimensional space ([**SV**], Proposition 2.2.2), hence t has a fixed point in $\mathfrak{C}_0$ by Cartan-Dieudonne theorem. This implies that the dimension of $\mathfrak{C}^t$ is ≥ 2. As the dimension of a composition subalgebra can be $2, 4$ or 8 the subalgebra $\mathfrak{C}^t$ is either a quadratic field extension of k, a quaternion subalgebra or $t = I$. Hence we need to calculate centralizers of elements which are contained in a subgroup $G(\mathfrak{C}/L)$ where L is a quadratic field extension or $G(\mathfrak{C}/Q)$ where Q is a quaternion subalgebra.

Let Q be a quaternion subalgebra of the octonion division algebra $\mathfrak{C}$, hence Q itself is division.

Lemma 8.5.2. *Let $\mathfrak{C}$ be an octonion division algebra and $G = \mathrm{Aut}(\mathfrak{C})$. Let Q be a quaternion subalgebra of $\mathfrak{C}$. Let $t = \mathfrak{R}_p \in G(\mathfrak{C}/Q)$ for some $p \in SL_1(Q)$ with $p \notin k$. Then $\mathcal{Z}_G(t) = \{\mathfrak{R}_{p_1}\mathfrak{I}_{c_1} \in G(\mathfrak{C}, Q) \mid p_1c_1 \in L\}$ where $L = k(p)$, a quadratic field extension of k.*

Proof. We have $t = \mathfrak{R}_p \in G(\mathfrak{C}/Q)$ with $p \notin k$. We write $\mathfrak{C} = Q \oplus Qb$ for some $b \in Q^{\perp}$. Then $t(x + yb) = x + (py)b$. From Proposition 8.5.1 we get, $\mathcal{Z}_G(t) \subset G(\mathfrak{C}, Q) = \{\mathfrak{R}_{p_1}\mathfrak{I}_{c_1} \mid p_1 \in SL_1(Q), c_1 \in Q^*\}$. Let $g \in \mathcal{Z}_G(t)$ and let $g = \mathfrak{R}_{p_1}\mathfrak{I}_{c_1}$. Then

$$gt = tg \Rightarrow \mathfrak{R}_{p_1}\mathfrak{I}_{c_1}R_p = \mathfrak{R}_p\mathfrak{R}_{p_1}\mathfrak{I}_{c_1} \Rightarrow \mathfrak{R}_{p_1c_1pc_1^{-1}}\mathfrak{I}_{c_1} = \mathfrak{R}_{pp_1}\mathfrak{I}_{c_1}$$

and we get, $p_1c_1p = pp_1c_1$, i.e., $p_1c_1 \in \mathcal{Z}_Q(p) = L$ where $L = k(p)$ is a quadratic field extension of k. Hence $\mathcal{Z}_G(t) = \{\mathfrak{R}_{p_1}\mathfrak{I}_{c_1} \mid p_1c_1 \in L, c_1 \in Q^*, p_1 \in SL_1(Q)\}$. □

Now we consider conjugacy classes of centralizers of these elements in G.

Lemma 8.5.3. *Let $t, t' \in G = \mathrm{Aut}(\mathfrak{C})$. Let t and t' leave quaternion subalgebra Q and Q' fixed pointwise, respectively. Suppose Q and Q' are isomorphic. Let $t = \mathfrak{R}_p$*

and $t' = \mathfrak{R}'_p$ where $p \in SL_1(Q)$ and $p' \in SL_1(Q')$ and both $p, p' \notin k$. Suppose $L = k(p)$ and $L' = k(p')$ are isomorphic field extensions of k. Then $\mathcal{Z}_G(t)$ is conjugate to $\mathcal{Z}_G(t')$ in G.

Proof. As Q and Q' are isomorphic, by Theorem 3.2.8 we have an automorphism ϕ of $\mathfrak{C}$ such that $\phi|_Q$ is the given isomorphism of Q to Q'. By conjugating the element t' by ϕ we may assume t and t' both belong to $G(\mathfrak{C}/Q)$. Let L and L' be isomorphic. Then there exists an isomorphism $\psi = \mathfrak{I}_c$, conjugation by $c \in Q$, which gives the isomorphism of L to L'. Let $g \in \mathcal{Z}_G(\mathfrak{R}_p)$. From previous lemma $g = \mathfrak{R}_{p_1}\mathfrak{I}_{c_1}$ with $p_1 c_1 \in L$. Then,

$$\psi g \psi^{-1} = \mathfrak{I}_c \mathfrak{R}_{p_1}\mathfrak{I}_{c_1}\mathfrak{I}_{c^{-1}} = \mathfrak{R}_{cp_1c^{-1}}\mathfrak{I}_{cc_1c^{-1}}.$$

We note that $cp_1c^{-1}cc_1c^{-1} = cp_1c_1c^{-1} \in L'$. This implies $\psi g \psi^{-1} \in \mathcal{Z}_G(t')$ and hence $\mathcal{Z}_G(t)$ is conjugate to $\mathcal{Z}_G(t')$ in G. □

Remark 8.5.4. In similar way one can calculate centralizers of elements of $G(\mathfrak{C}, Q)$. Let $t \in G(\mathfrak{C}, Q)$. Let $t = \mathfrak{R}_p\mathfrak{I}_c$ where $p \in SL_1(Q)$ and $c \in Q - k$. Then $\mathcal{Z}_G(t) = \{\mathfrak{R}_{p_1}\mathfrak{I}_{c_1} \mid c_1 \in k(c), p_1c_1 \in k(pc)\}$.

We note that the center of $SL_1(Q)$ is $\{1, -1\}$ and the element t in $\mathrm{Aut}(\mathfrak{C})$ corresponding to -1 is a non-trivial involution (i.e. $t^2 = 1$). By a similar calculation as above it is easy to see that $\mathcal{Z}_G(t) = G(\mathfrak{C}, Q)$ for $1 \neq t$ an involution. In fact any non-trivial involution in $\mathrm{Aut}(\mathfrak{C})$ correspond to a quaternion subalgebra in this fashion. Two involutions are conjugate if and only if the corresponding fixed quaternion subalgebras are isomorphic (see Section 3.3). From Proposition 3.2.9, two involutions have their centralizers conjugate if and only if the corresponding fixed quaternion subalgebras are isomorphic. We observe that the centralizers corresponding to involutions and other type of elements in Lemma 8.5.3 are not isomorphic hence they can not be conjugate in the group G.

Let $t \in G = \mathrm{Aut}(\mathfrak{C})$ where $\mathfrak{C}$ is a division octonion algebra. Then t fixes a quadratic subfield L pointwise as the dimension of $\mathfrak{C}^t$ is ≥ 2. Moreover we can find $a, b \in \mathfrak{C}$ such that $Q = L \oplus La$ is a quaternion subalgebra and $\mathfrak{C} = Q \oplus Qb$. Then $L^{\perp}$ is a hermitian space over L. With respect to the basis $\{a, b, ab\}$ we write the subgroup $SU(L^{\perp}, \mathfrak{h})$ of G as $SU(H) = \{A \in SL(3, L) \mid {}^t\!AH\bar{A} = H\}$ where $H = \mathrm{diag}\{\mathfrak{h}(a, a), \mathfrak{h}(b, b), \mathfrak{h}(ab, ab)\}$. We denote the matrix of t as A with respect to this basis. We observe that t leaves a quaternion subalgebra fixed pointwise if and only if 1 is an eigenvalue of A, i.e., $X - 1$ is a factor of the characteristic polynomial $\chi_A(X)$. The conjugacy classes of centralizers of such elements have been already discussed in previous paragraph and in Lemma 8.5.3 hence we assume that $X-1$ is not a factor of $\chi_A(X)$. For other elements we have,

Lemma 8.5.5. *With notation as above, let $t \in G(\mathfrak{C}/L)$. Suppose 1 is not a root of $\chi_A(X)$. Then, $\mathcal{Z}_G(t) \subset G(\mathfrak{C}/L)$.*

Proof. Let $t \in G(\mathfrak{C}/L)$ be such that t does not fix any point in $L^{\perp}$. Let $g \in \mathcal{Z}_G(t)$ then $g \in G(\mathfrak{C}, L) \cong SU(L^{\perp}, \mathfrak{h}) \rtimes < \rho >$ where ρ is an extension of conjugation on L (Proposition 3.2.5). We denote the matrix of t in $SU(H)$ by A. Then, either $g \in SU(L^{\perp}, \mathfrak{h})$ or $g = h\rho$ for some $h \in SU(L^{\perp}, \mathfrak{h})$. When $g \in SU(L^{\perp}, \mathfrak{h})$ we denote the matrix of g by C. Then $g \in \mathcal{Z}_G(t)$ implies $AC = CA$ in $SU(H)$. When $g = h\rho$ we denote the matrix of h by B and we denote the action of ρ on elements of L by $\alpha \mapsto \bar{\alpha}$. Then,

$$\begin{aligned} gt(\alpha_1 a + \alpha_2 b + \alpha_3 c) &= h\rho t(\alpha_1 a + \alpha_2 b + \alpha_3 c) = h\rho(\alpha_1 Aa + \alpha_2 Ab + \alpha_3 Ac) \\ &= h(\bar{\alpha}_1 \bar{A}a + \bar{\alpha}_2 \bar{A}b + \bar{\alpha}_3 \bar{A}c) = \bar{\alpha}_1 B\bar{A}a + \bar{\alpha}_2 B\bar{A}b + \bar{\alpha}_3 B\bar{A}c \end{aligned}$$

and

$$\begin{aligned} tg(\alpha_1 a + \alpha_2 b + \alpha_3 c) &= th\rho(\alpha_1 a + \alpha_2 b + \alpha_3 c) = th(\bar{\alpha}_1 a + \bar{\alpha}_2 b + \bar{\alpha}_3 c) \\ &= t(\bar{\alpha}_1 Ba + \bar{\alpha}_2 Bb + \bar{\alpha}_3 Bc) = \bar{\alpha}_1 ABa + \bar{\alpha}_2 ABb + \bar{\alpha}_3 ABc. \end{aligned}$$

As $g \in \mathcal{Z}_G(t)$, above calculation implies $AB = B\bar{A}$ where $B \in SU(H)$. Suppose $\mathcal{Z}_G(t)$ is not contained in $G(\mathfrak{C}/L)$. Then there exist $g = h\rho \in G(\mathfrak{C}, L)$ such that $gt = tg$. With calculations above if we denote the matrix of h by B in $SU(H)$, we get $AB = B\bar{A}$ in $SU(H)$. In this case the characteristic polynomial $\chi_A(X) = X^3 - aX^2 + \bar{a}X - 1$ will have $a = \bar{a}$. But $\chi_A(X) = X^3 - aX^2 + aX - 1 = (X-1)(X^2 + (1-a)X + 1)$ is reducible and A has 1 as an eigenvalue. Which contradicts the assumption that 1 is not a root of $\chi_A(X)$. Hence $\mathcal{Z}_G(t) \subset G(\mathfrak{C}/L)$. □

Remark 8.5.6. In view of above calculations we observe that the centralizer of $t \in G(\mathfrak{C}/L)$ in G is isomorphic to $\{B \in SU(H) \mid AB = BA\} \cup \{B \in SU(H) \mid AB = B\bar{A}\}$.

Let $t \in G(\mathfrak{C}/L)$ and let $A \in SU(H)$ be the corresponding matrix. Moreover we assume that 1 is not a root of $\chi_A(X)$. Let K be an algebraic closure of k containing L. As t is semisimple we have following cases:

(1) The characteristic polynomial of A has distinct roots over K.
(2) The characteristic polynomial of A has two distinct roots over K which belong to k.

We calculate centralizers in these cases. We observe that whenever H is a connected subgroup of a connected algebraic group G and $t \in H$ such that $\mathcal{Z}_G(t) \subset H$ then t is regular in G if and only if it is so in H. Hence $t \in G(\mathfrak{C}/L)$ is regular in $G(\mathfrak{C}/L)$ if and only if it is regular in G (Lemma 8.5.5). This implies that any element of $G(\mathfrak{C}/L)$ (which does not have 1 as an eigenvalue) is either a regular element in G or its characteristic polynomial is $(X-\alpha)(X-\beta)^2$ where α, β are in $L-k$. We calculate centralizers of these elements here.

Lemma 8.5.7. *Let $t \in G = \mathrm{Aut}(\mathfrak{C})$. With notation as above let $t \in G(\mathfrak{C}/L)$ and A be the corresponding element in $SU(H)$. Suppose 1 is not an eigenvalue of A. Then the centralizer of t is a maximal torus in G or it is isomorphic to a subgroup $\left\{\begin{pmatrix} \det(S)^{-1} & 0 \\ 0 & S \end{pmatrix} \in SU(H) \mid S \in U(W, \mathfrak{h}|_W)\right\}$ for some 2-dimensional nondegenerate L-subspace W of $L^{\perp}$.*

Proof. When the element t is regular the centralizer is a maximal torus in G and hence the conjugacy of centralizers of these elements correspond to conjugacy classes of maximal tori of G over k. Now suppose the characteristic polynomial $\chi_A(X)$ has multiple roots, i.e., $\chi_A(X) = (X-\alpha)(X-\beta)^2$ where $\alpha, \beta \in L$ both not equal to 1 and the minimal polynomial is $(X-\alpha)(X-\beta)$. Then we can choose a basis of $L^{\perp}$ consisting of eigenvectors v_1, v_2, v_3 corresponding to eigenvalues α, β, β of t. We denote the subspace generated by v_2, v_3 as W. The matrix of t is diagonal with respect to this basis, $A = \mathrm{diag}\{\alpha, \beta, \beta\}$. As 1 is not a root of $\chi_A(X)$ the centralizer $\mathcal{Z}_G(t) \cong \mathcal{Z}_{SU(H)}(A)$ which is isomorphic to $\mathcal{Z}_{GL_3(L)}(A) \cap SU(H) = \left\{\begin{pmatrix} \det(S)^{-1} & 0 \\ 0 & S \end{pmatrix} \mid S \in U(W, \mathfrak{h}|_W)\right\}$. □

8.5.1. Conjugacy Classes of Centralizers in Compact G_2. Let G be the compact real group of type G_2. We note that for the base field $k = \mathbb{R}$ there is a unique anisotropic form of G_2. As there is a unique nondegenerate anisotropic quadratic form over $\mathbb{R}$ of dimension 8, there is a unique octonion division algebra (up to isomorphism) $\mathfrak{C}$ over $\mathbb{R}$ and $G \cong \mathrm{Aut}(\mathfrak{C})$. We calculate centralizers of elements and there conjugacy classes in this case. Let $\mathfrak{C}$ be the octonion division algebra over $\mathbb{R}$ and $G = \mathrm{Aut}(\mathfrak{C})$. Let $t \in G$. Let L be a quadratic field extension of $\mathbb{R}$ left fixed pointwise by t (which is isomorphic to $\mathbb{C}$). Then $t \in SU(L^{\perp}, \mathfrak{h}) \cong SU(3) = \{A \in GL_3(\mathbb{C}) \mid {}^t\!A\bar{A} = 1\}$. We also note that all quadratic field extensions of $\mathbb{R}$ contained in $\mathfrak{C}$ are isomorphic hence all subgroups of type $SU(L^{\perp}, \mathfrak{h})$ are conjugate (Proposition 3.2.9) in G. But every element of $SU(3)$ can be diagonalized in $SU(3)$. Hence characteristic polynomial of A over L is either $(X-\alpha)(X-\beta)(X-\gamma)$ or $(X-\alpha)(X-\beta)^2$.

If A has three distinct roots and none of them is 1 then the element t is regular in G and the centralizer is a maximal torus in G (ref. Lemma 8.5.7). In this case centralizer is contained in the subgroup $SU(3)$ and is a maximal torus of $SU(3)$. As all maximal tori of G are conjugate we have one conjugacy class of centralizers of these elements. Now suppose t has repeated roots then with respect to some basis $A = \text{diag}\{\alpha, \beta, \beta\}$ where neither of α, β is 1 and the centralizer (ref. Lemma 8.5.7)

$$\mathcal{Z}_G(t) \cong \mathcal{Z}_{SU(3)}(A) \cong \left\{ \begin{pmatrix} \det(S)^{-1} & 0 \\ 0 & S \end{pmatrix} \mid S \in U(2) \right\}.$$

If t leaves a quaternion subalgebra Q fixed (i.e. the characteristic polynomial of t has 1 as a root) then A is either $\text{diag}\{1,-1,-1\}$, an involution in G, or $\text{diag}\{1, \alpha, \bar{\alpha}\}$ for some $\alpha \in L$ of norm 1. If t is an involution the centralizer is whole of the subgroup $G(\mathfrak{C}/L) \cong SU(3)$ (from remark following Lemma 8.5.5). And when t is not an involution the centralizer $\mathcal{Z}_G(t) \cong \mathcal{Z}_{SU(3)}(A) \cup \{B \in SU(3) \mid AB = B\bar{A}\}$.

Lemma 8.5.8. *Let $\mathfrak{C}$ be the octonion division algebra over $\mathbb{R}$ and $G = \text{Aut}(\mathfrak{C})$. Let $t \in G$ and $L \subset \mathfrak{C}$ be the quadratic field extension of $\mathbb{R}$ left pointwise fixed by t, i.e., $t \in G(\mathfrak{C}/L)$. Suppose t is not an involution. Then, $\mathcal{Z}_G(t) \subset G(\mathfrak{C}/L)$ if and only if t does not leave any quaternion subalgebra fixed pointwise.*

Proof. If $t \in G(\mathfrak{C}/L)$ does not leave any quaternion subalgebra fixed pointwise then the characteristic polynomial of t does not have 1 as a root. Hence from Lemma 8.5.5 it follows that $\mathcal{Z}_G(t) \subset G(\mathfrak{C}/L)$. Now suppose $t \in G(\mathfrak{C}/L)$ leaves a quaternion subalgebra Q fixed pointwise. By using Theorem 3.2.8 we may assume Q contains L. As $t \in G(\mathfrak{C}/L) \cong SU(3)$ the corresponding matrix A can be diagonalized in the subgroup $SU(3)$. We write the matrix of t as $A = \text{diag}\{1, \alpha, \bar{\alpha}\}$ for some $\alpha \in L$ with $\alpha\bar{\alpha} = 1$. We claim that there exists an element $B \in SU(3)$ such that $AB = B\bar{A}$. We take $B = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ and check that $B \in SU(3)$ and $AB = B\bar{A}$. From remark following Lemma 8.5.5 we see that $\mathcal{Z}_G(t)$ is not contained in $G(\mathfrak{C}/L)$. □

In this case the centralizer is not contained in the subgroup $G(\mathfrak{C}/L) \cong SU(3)$. As all quaternion division algebras over $\mathbb{R}$ are isomorphic and all quadratic field extensions contained in any of the quaternion algebras are isomorphic, we have one conjugacy class of centralizers of non-involutions.

Hence we have proved,

Theorem 8.5.9. *Let G be the anisotropic group of type G_2 over $\mathbb{R}$. Then the total number of orbit types (conjugacy classes of centralizers) are five, corresponding to elements*

$$I, \mathrm{diag}\{\alpha,\beta,\gamma\}, \mathrm{diag}\{\alpha,\beta,\beta\}, \mathrm{diag}\{1,-1,-1\}, \mathrm{diag}\{1,\alpha,\bar{\alpha}\}$$

where none of α,β,γ are 1 or -1.

CHAPTER 9

Reality in Algebraic Groups

In this chapter we investigate the reality question for algebraic groups in general. We mainly prove the theorems mentioned in Section 6.3. First we look at the structure of strongly regular real elements in simple groups of adjoint type which have -1 in the Weyl group and prove that it is real if and only if it is strongly real. This we do in Section 9.1. Later in Section 9.3 we look at the structure of semisimple real elements over fields of $cd(k) \leq 1$. The results in this section are part of [**ST2**].

9.1. Strongly Regular Real Elements

In this section we discuss structure of a strongly regular real element. An element t in a connected linear algebraic group G is called **regular** if its centralizer $\mathcal{Z}_G(t)$ has minimal dimension among all centralizers. An element is called **strongly regular** if its centralizer in G is a maximal torus. We note that a semisimple element in a connected reductive group is regular if and only if the connected component of its centralizer is a maximal torus. Let G be a connected, simple algebraic group defined over k of adjoint type such that the longest element w_0 in the Weyl group W of G with respect to a maximal torus T acts by -1 on the roots. The adjoint groups of type $A_1, B_l, C_l, D_{2l}(l > 2), E_7, E_8, F_4, G_2$ are precisely the simple groups which satisfy the above hypothesis. For the groups of the above type we mention here a theorem of Richardson and Springer ([**RS**], Proposition 8.22) which plays an important role in our investigation.

Proposition 9.1.1 (Richardson, Springer)**.** *Let G be a simple group of adjoint type, let T' be a maximal torus of G and let $c \in W(T')$ be an involution. Then there exists an involution $n \in N(T')$ which represents c.*

Then we have,

Theorem 9.1.2. *Let G be a connected simple group of adjoint type defined over k. Suppose the longest element w_0 of the Weyl group W of G with respect to a maximal torus T acts by -1 on the roots. Let $t \in G(k)$ be a strongly regular element. Then*

t is real in $G(k)$ if and only if t is strongly real in $G(k)$. Moreover, every element of a maximal torus, which contains a strongly regular real element, is strongly real in $G(k)$.

Proof. Let $t \in G(k)$ be a strongly regular real element and let $g \in G(k)$ be such that $gtg^{-1} = t^{-1}$. Let T be a maximal torus in G defined over k which contains t. We use a theorem of Richardson and Springer ([**RS**], Proposition 8.22; Proposition 9.1.1) here. With the hypothesis we have assumed, this theorem implies that any involution in W is represented by an involution $n \in N(T)$. The longest element w_0 acts as -1 on the roots and is an involution. Hence there exists $n \in N(T)$, an involution, such that $nsn^{-1} = s^{-1}$ for all $s \in T$. Thus $ntn = t^{-1}$ and $g \in n\mathcal{Z}_G(t) = nT$. Let $g = ns_0$, for $s_0 \in T$. Then $g^2 = ns_0ns_0 = s_0^{-1}s_0 = 1$. Hence g is an involution and the element t is a product of two involutions g and gt.

Suppose now T is a maximal torus in G defined over k and $T(k)$ contains a strongly regular real element t. Let $s \in T(k)$. Suppose $g \in G(k)$ conjugates t to t^{-1}. Then we have proved that $g^2 = 1$. We claim that g conjugates s to s^{-1}. From calculations in the paragraph above, we have $g = ns_0$ for some $s_0 \in T$. Then $gsg^{-1} = ns_0ss_0^{-1}n^{-1} = nsn^{-1} = s^{-1}$. But since g is an involution in $G(k)$, s is a product of two involutions. □

We note that in groups G satisfying the hypothesis of the theorem, there are strongly regular elements in $G(k)$ which are not real in $G(k)$. We have proved that for a group G of type G_2 defined over k, a semisimple element in $G(k)$ is real if and only if it is a product of two involutions in $G(k)$ (Theorem 6.2.2). Examples of semisimple elements which are not real are also constructed in the Chapter 8.4. Hence in a maximal torus containing such an element no strongly regular element is real.

9.2. Cohomological Obstruction to Reality

The results in this subsection are known to the experts ([**Se**], Chapter III, section 2.3). However, we include some with proofs for the sake of completeness. Let G be a connected linear algebraic group defined over a field k. We have,

Lemma 9.2.1. *Let $g \in G$. Let $g = g_sg_u$ be the Jordan decomposition of g in G. Let H be the centralizer of g_s in G. Then, g is real in G if and only if g_s is real and g_u^{-1}, xg_ux^{-1} are conjugate in H, where $xg_sx^{-1} = g_s^{-1}$.*

Proof. Let g be real in G, i.e., there exists $x \in G$ such that $xgx^{-1} = g^{-1}$. Then x conjugates g_s and g_u to g_s^{-1} and g_u^{-1} respectively.

Conversely let $h \in H$ such that $hg_u^{-1}h^{-1} = xg_ux^{-1}$. Then,

$$\begin{aligned} h^{-1}xg(h^{-1}x)^{-1} &= h^{-1}xgx^{-1}h = h^{-1}xg_sx^{-1}xg_ux^{-1}h = h^{-1}g_s^{-1}xg_ux^{-1}h \\ &= g_s^{-1}h^{-1}xg_ux^{-1}h = g_s^{-1}g_u^{-1} = g^{-1}. \end{aligned}$$

Hence g is real in G. □

It is not true that g is real if and only if g_s real and g_u real. We give examples of this situation.

Example 1: Let $G = GL_4(k)$. We take $s = \mathrm{diag}(\lambda, \lambda, \lambda^{-1}, \lambda^{-1})$ with $\lambda^2 \neq 1$, $u = \mathrm{diag}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)$ and $g = su$. Then $g_s = s, g_u = u$ and the centralizer of s in G is $\mathcal{Z}_{GL_4(k)}(s) = \{\mathrm{diag}(A, B) \mid A, B \in GL_2(k)\}$. The elements s and u are real but g is not real. In fact $xsx^{-1} = s^{-1}$ where

$$x = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

The elements u^{-1} and $xux^{-1} = \mathrm{diag}\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)$ are not conjugate in $\mathcal{Z}_{GL_4(k)}(s)$ hence g is not real by Lemma 9.2.1.

Example 2: In G_2 over a finite field, all semisimple as well as unipotent elements are real but still there are nonreal elements (see Section 8.4.3).

Next we derive a cohomological obstruction to reality over the base field k. Let G be a connected linear algebraic group defined over k. Let $t \in G(k)$ be real in G. We put $H = \mathcal{Z}_G(t)$, the centralizer of t in G. Let $X = \{x \in G \mid xtx^{-1} = t^{-1}\}$. Then X is an H-torsor defined over k with H-action given by $h.x = xh$ for $h \in H$ and $x \in X$.

Since t is real over $\bar{k}$, we have $X \neq \phi$. The torsor X corresponds to an element of $H^1(k, H)$ ([**Se**], Chapter 1, section 5.2, Proposition 33). Let $x \in X$ and γ be the cocycle corresponding to X. Then γ is given by $\gamma(\sigma) = x^{-1}\sigma(x)$ for all $\sigma \in \Gamma = \mathrm{Gal}(\bar{k}/k)$. Now we look for a condition which determines when t is k-real.

Proposition 9.2.2. *Let G be a connected algebraic group defined over k. Let $t \in G(k)$ be real over $\bar{k}$. Then t is real in $G(k)$ if and only γ, as above, represents a trivial cocycle in $H^1(k, H)$ where H is the centralizer of t in G.*

Proof. Let t be real in $G(k)$. Then there exists $g' \in G(k)$ such that $g'tg'^{-1} = t^{-1}$. Then $g'^{-1}g \in H$. Write $g = g'h$ for some $h \in H$. Then,

$$\gamma(\sigma) = g^{-1}\sigma(g) = h^{-1}g'^{-1}\sigma(g')\sigma(h) = h^{-1}\sigma(h).$$

This implies that γ is equivalent to the trivial cocycle.

Conversely, let γ be the trivial cocycle. Then there exists $h \in H$ such that $\gamma(\sigma) = h^{-1}\sigma(h)$. That is, $g^{-1}\sigma(g) = h^{-1}\sigma(h)$, then $\sigma(gh) = gh$. Hence $gh \in G(k)$ and $ght(gh)^{-1} = ghth^{-1}g^{-1} = gtg^{-1} = t^{-1}$. Hence the element t is real in $G(k)$. □

Corollary 9.2.3. *With notation as above, t is real in $G(k)$ if and only if the H-torsor X has a k-point or, equivalently the cocycle γ is trivial in $H^1(k, H)$.*

Note that if $H^1(k, H)$ is trivial then t is real in $G(k)$. By a theorem of Steinberg ([**S1**] Theorem 1.9; also see [**Se**], Chapter III, section 2.3) if H is a connected reductive group and $cd(k) \leq 1$ or H is connected with k perfect of $cd(k) \leq 1$, we have $H^1(k, H) = 0$. In these situations t is real.

Proposition 9.2.4. *Let G be a split connected semisimple adjoint group defined over an arbitrary field k and suppose -1 belongs to the Weyl group of G. Let T be a k-split maximal torus in G. Then every element of $T(k)$ is strongly real.*

Proof : By Theorem 9.1.1, there exists $n_0 \in N(T)(\bar{k})$ such that ${n_0}^2 = 1$ and $n_0 s {n_0}^{-1} = s^{-1}$ for all $s \in T$. Consider the Galois cocycle $\gamma(\sigma) = n_0\sigma(n_0)$ for $\sigma \in \Gamma = \mathrm{Gal}(\bar{k}/k)$. Since T is defined over k, we have, for $s \in T$ and $\sigma \in \Gamma$,

$$\sigma(n_0)s\sigma(n_0)^{-1} = \sigma(n_0\sigma^{-1}(s)n_0) = \sigma(\sigma^{-1}(s^{-1})) = s^{-1}.$$

Hence, we must have, in the Weyl group $W = N(T)/T$, $n_0T = \sigma(n_0)T$. Therefore $\gamma(\sigma) = n_0\sigma(n_0) \in T$. Hence γ is a 1-cocycle in $H^1(k, T)$. But since T is k-split, $H^1(k, T) = 0$. Hence there is $s \in T$ such that

$$\gamma(\sigma) = n_0\sigma(n_0) = s^{-1}\sigma(s).$$

This gives $sn_0 = \sigma(sn_0)$ for all $\sigma \in \Gamma$. Hence $sn_0 \in T(k)$. Also

$$(sn_0)^2 = sn_0sn_0 = ss^{-1} = 1.$$

Therefore $g = sn_0$ is an involution in $T(k)$ and for any $t \in T(k)$, we have,

$$gtg^{-1} = gtg = sn_0tn_0s^{-1} = st^{-1}s^{-1} = t^{-1}.$$

Thus $(gt)^2 = 1$ and $t = g.gt$. Hence t is strongly real. □

9.3. Reality over Fields of $cd(k) \leq 1$

In this section we discuss reality for semisimple elements over fields of $cd(k) \leq 1$. We have,

Theorem 9.3.1. *Let k be a field with $cd(k) \leq 1$. Let G be a connected reductive group defined over k with -1 in its Weyl group. Then every semisimple element in $G(k)$ is real in $G(k)$.*

Proof. Let $t \in G(k)$ be semisimple. Let T be a maximal torus defined over k with $t \in T(k)$. Then the Weyl group $W = N(T)/T$, where $N(T)$ is the normalizer of T in G. We have the exact sequence

$$1 \to T \to N(T) \to W \to 1.$$

The corresponding Galois cohomology sequence is

$$1 \to T(k) \to N(T)(k) \to W(k) \to H^1(k,T) \to \cdots .$$

Since $cd(k) \leq 1$, by Steinberg's theorem ([**S1**], Theorem 1.9), $H^1(k,T) = 0$. Hence the longest element w_0 in the Weyl group, which acts by -1 on the set of roots, lifts to an element $h \in N(T)(k)$. Hence $hth^{-1} = t^{-1}$ with $h \in G(k)$ and t is real in $G(k)$. □

Corollary 9.3.2. *Let G and k be as in the above theorem. Then every regular element of G is real.*

Proof. Let $g \in G$ be regular and $g = g_s g_u$ be the Jordan decomposition of g in G with g_s semisimple and g_u unipotent. Then, by the above theorem, $hg_sh^{-1} = g_s^{-1}$ for some $h \in G$. Then hg_uh^{-1} and g_u^{-1} are regular unipotents in $\mathcal{Z}_G(g_s)^0$ and hence there is $x \in \mathcal{Z}_G(g_s)$ such that $xhg_uh^{-1}x^{-1} = g_u^{-1}$. Then $(xh)g(xh)^{-1} = g^{-1}$ and hence g is real (see [**SS**], Corollary 1.9, Chapter III). □

Theorem 9.3.3. *Let k be a field with $cd(k) \leq 1$ (e.g. algebraically closed fields and finite fields etc.). Let G be a simple adjoint group defined over k. Suppose that the longest element w_0 in the Weyl group of G with respect to a maximal torus T acts as -1 on the roots. Then every semisimple element in $G(k)$ is strongly real in $G(k)$.*

Proof. Let $t \in G(k)$ be a semisimple element. Let T be a torus in G defined over k which contains t, i.e., $t \in T(k)$. From a theorem of Richardson and Springer ([**RS**], Proposition 8.22), as $-1 \in W$, there exists $n_0 \in N(T)$ with $n_0^2 = 1$ which represents

-1 in W. That is, we have $n_0 s n_0^{-1} = s^{-1}$ for all $s \in T$. We claim that the coset $n_0 T$ is Γ-stable. We note that for $\sigma \in \Gamma = \mathrm{Gal}(\bar{k}/k)$,

$$\sigma(n_0) s \sigma(n_0)^{-1} = \sigma(n_0 \sigma^{-1}(s) n_0^{-1}) = \sigma(\sigma^{-1}(s^{-1})) = s^{-1}$$

for all $s \in T$ and $\sigma \in \Gamma$. Hence $\sigma(n_0) \in N(T)$ also represents -1 in W. Thus we have $\sigma(n_0)T = n_0 T$ and so $n_0 \sigma(n_0) \in T$.

We look at the cocycle defined by $\sigma \mapsto n_0 \sigma(n_0)$. Then the image of this cocycle lands in T. Since $cd(k) \leq 1$, from a theorem of Steinberg ([**S1**], Theorem 1.9) we have $H^1(k, T) = 0$ and hence the cocycle defined above is a trivial cocycle. That is, there exists $t_0 \in T$ such that $n_0 \sigma(n_0) = t_0 \sigma(t_0^{-1})$ for all $\sigma \in \Gamma$. This implies $\sigma(n_0 t_0) = n_0 t_0$ for all $\sigma \in \Gamma$ and hence $n_0 t_0 \in G(k)$. We check that $n_0 t_0$ is an involution and conjugates every element of T to its inverse.

$$(n_0 t_0)^2 = n_0 t_0 n_0 t_0 = t_0^{-1} t_0 = 1$$

and

$$n_0 t_0 s (n_0 t_0)^{-1} = n_0 t_0 s t_0^{-1} n_0 = n_0 s n_0 = s^{-1}.$$

Hence every semisimple element of $G(k)$ is real in $G(k)$. □

CHAPTER 10

Epilogue

In this chapter, we address the question of reality in the frame work of representation theory. We start with a discussion of the question for finite groups. We do not define some of the terminology used in this chapter, however we give appropriate references.

10.1. Reality Question and Representation Theory

First we discuss real representations of a finite group and its relation to real elements in the group. For the theory here we refer to the book [**JL**] chapter 23. Let G be a finite group. We consider representations of G over $\mathbb{C}$. A character χ of G is called **real** if $\chi(g) \in \mathbb{R}$, for all $g \in G$. Then we have (see [**JL**], Theorem 23.1),

Proposition 10.1.1. *Let G be a finite group. The number of real irreducible characters of G is equal to the number of real conjugacy classes of G.*

Note that if an element g is real then all conjugates of g are real and we call the conjugacy class of g, a real conjugacy class. A representation $\phi\colon G \to GL(V)$ is realizable if it is defined over $\mathbb{R}$, i.e. with respect to some basis of V the $\phi(G) \subset GL_n(\mathbb{R})$. It is obvious that a character corresponding to a realizable representation is real. This brings us to the question of determining representations which give rise to real characters.

Proposition 10.1.2. *Let G be a finite group and χ be an irreducible character of a representation V. Then, χ is real if and only if there is a non-zero G-invariant bilinear form on the representation space V.*

A representation (ϕ, V) of G is called **orthogonal (symplectic)** if there exists a non-zero symmetric (skew-symmetric) bilinear form on V which is G-invariant. That is, $\phi(G) \subset O_n(\mathbb{C})$ if the representation is orthogonal and $\phi(G) \subset Sp_{2m}(\mathbb{C})$ if the representation is symplectic. The next proposition determines which real characters come from realizable representations.

Proposition 10.1.3. *An irreducible real character comes from a realizable representation if and only if the representation V is orthogonal. And an irreducible real character does not come from a realizable representation if and only if the representation V is symplectic.*

A question of independent interest is to directly relate orthogonal and symplectic representations to real elements in G. Results proved in this thesis suggest that orthogonal representations should be related to strongly real elements, i.e., the one which are a product of two involutions. It also seems likely that for a large class of finite groups, real elements in $G/\mathcal{Z}(G)$ are strongly real. There does not seem to be any known result in this direction.

The question of determining a finite group of which all elements are real has been extensively studied. We would like to mention the work of [**TiZ**] where they classify finite quasi simple groups in which all elements are real. They also give some examples of nonreal elements. Study of real element has been used in the proof of Thompson and Ore conjectures in the case of finite Chevalley groups. Here we quote a Theorem from [**EG**] (Theorem 1).

Theorem 10.1.4. *Let G be a Chevalley group. Let h_1 and h_2 be two regular semisimple elements in G from a maximal split torus and let C_1 and C_2 be the conjugacy classes of h_1 and h_2, respectively. Then $C_1C_2 \supset G/\mathcal{Z}(G)$.*

This theorem immediately implies the Ore conjecture for any simple group G containing a regular semisimple element h in a maximal split torus, and the Thompson conjecture, if this element is, in addition, real (see [**EG**]).

Now we turn our attention to representations of algebraic groups. We have seen that for finite groups real elements are related to real representations which in turn to orthogonal and symplectic representations. Now we would like to bring in the connection of a representation being self-dual to being orthogonal or symplectic. Steinberg studied this question for Chevalley groups. Here we refer to Lemma 78 and Lemma 79 from [**S4**]. Let G be an indecomposable (i.e. corresponds to an indecomposable root system) infinite Chevalley group, V an irreducible rational G-module and λ be its highest weight. Then,

Lemma 10.1.5 (Steinberg)**.** *The following conditions are equivalent.*

(1) *There exists a nonzero invariant bilinear form on V.*

(2) *V and its dual V^* are isomorphic as representations of G.*

(3) $-w_0\lambda = \lambda$, *where* w_0 *is the longest element in the Weyl group of* G.

Moreover if there exists an invariant bilinear form on V then it is unique up to multiplication by a scalar and is either symmetric or skew-symmetric. Next lemma determines when the representation is orthogonal.

Lemma 10.1.6 (Steinberg)**.** *With notation as above, there exists an element* h *in the center of* G *with* $h^2 = 1$ *such that, if* V *possesses an invariant bilinear form, then it is symmetric if* $\lambda(h) = 1$ *and skew-symmetric if* $\lambda(h) = -1$.

One can summarise the results above by saying that, for a semisimple algebraic group, there exists an involution h in the center, which acts by 1 on an irreducible self-dual representation if and only if the representation is orthogonal. In particular, any self dual representation of an adjoint semisimple group is orthogonal. This question has been extensively studied in the literature. We mention here the works of Prasad ([**Pr1**], [**Pr2**]) where he studies self dual representations of finite groups of Lie type and p-adic groups.

10.2. Programme and Further Questions

Nevertheless, in the end we would like to point out some questions to which this thesis has contributed partially. Some of these questions are of independent interest and answers to these questions will help in understanding algebraic groups.

1. Reality in classical groups: The determination of real elements in an algebraic group G, defined over a field k, is far from being satisfactory. We need to determine suitable criteria for real elements for the k-forms of classical groups which are defined using algebras with involutions (see [**KMRT**], chapter III, section 12). Let (A, σ) be a central simple k-algebra with involution. Determine real elements in the groups $Sim(A, \sigma), PSim(A, \sigma)$ and $\mathrm{Iso}(A, \sigma)$. More specifically, we would like to ask whether real semisimple elements in these groups are strongly real. In this thesis we have given a partial answer to this question. For example when $A = \mathrm{End}_k(V)$ and σ is the adjoint involution $\sigma_{\mathfrak{b}}$ corresponding to a nondegenerate symmetric or skew-symmetric form $\mathfrak{b}$, we have answered this question for the group $\mathrm{Iso}(A, \sigma)$ (see the theorems mentioned in Section 6.1 and Section 7.3).

2. Reality in exceptional groups: The programme for exceptional groups needs delicate care. In this thesis, among exceptional groups we have tackled the groups of type G_2 and classify real elements as strongly real. There are known forms of F_4 in which there are no k-rational involutions. Our results suggest that in such forms of F_4 (which are necessarily anisotropic), there are no nontrivial real elements.

3. Real elements and orthogonal representations: In view of the connection to representation theory described in the previous section it would be of interest to directly relate self-dual representations to real elements, at least for groups with suitable hypothesis. Even in the case of finite groups there seem to be no satisfactory answer. We are lead to the following question: Let G be a finite group. Is the number of strongly real conjugacy classes of $G/\mathcal{Z}(G)$ equal to the number of orthogonal characters of $G/\mathcal{Z}(G)$?

4. Reality in linear algebraic groups: A lot of results, Theorem 9.1.2 and Theorem 9.3.3, suggest stronger results should be true. For example one should be able to generalise Theorem 9.1.2 for all semisimple elements not just for strongly regular elements. In the analysis in Chapter 9, the result of Wonenburger about $GL_n(k)$, which is a reductive group but not semisimple, is left out. One should modify the hypothesis suitably for reductive groups and bring in the results about $GL_n(k)$ into the picture. Perhaps, a suitable notion of Weyl group associated to an element will do. We would like to mention here a few questions raised by T. A. Springer. Let G be a connected reductive group.

(i) Do the real elements in G form a Zariski closed subset of G?
(ii) If so, what are the dimension of its components?
(iii) Do the real semisimple elements form a dense subset?

5. Obstruction to reality: We have hardly dealt with the arithmetic aspect of reality property in this thesis, though it is very much in the scheme of things to deal with the local-global behavior of reality of an element in these groups. We specify the question more clearly here. Let G a group defined over a global field k. Let $g \in G(k)$ be a real element. Is it true that g is real in $G(k)$ if and only if g is real in $G(k_p)$, $\forall p$ and in $G(\mathbb{R})$? One can ask another related question to compute obstruction to reality for a particular group. We explain it here. Let G be a group defined over k. Let $g \in G(k)$. Suppose g is real in $G(\bar{k})$, where $\bar{k}$ is an algebraic closure of k. Calculate the obstruction to g being real in $G(k)$. We have calculated this for the groups of type G_2 in this thesis (see Corollary 8.2.11 and 8.3.7 and Section 9.2). For a local-global principle for conjugacy classes in classical groups, we refer to [**Fl**].

6. Centralizers and their conjugacy classes: Conjugacy classes and centralizers have been studied extensively in the literature and are very important in understanding the structure of a group. With several results about groups of type

G_2 in hand, we calculated conjugacy classes of centralizers in groups of type G_2 (see Section 8.5). It would be of interest to calculate the conjugacy classes of centralizers in classical groups and parameterize them using Galois cohomology.

We thank you for showing interest in this thesis.

Bibliography

[A] E. Artin, *"Geometric algebra"*, Reprint of the 1957 original, Wiley Classics Library, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, **1988**.

[B] N. Bourbaki, *"Lie Groups and Lie Algebras"*, Chapters $4-6$, Springer-Verlag, **2000**.

[Be1] E. A. Bender, *"Symmetric matrices, characteristic polynomials and Hilbert symbols over local number fields"*, Bulletin of the American Mathematical Society **79 (1973)**, 518-520.

[Be2] E. A. Bender, *"Characteristic polynomial of symmetric matrices"*, Pacific Journal of Mathematics **25 No. 3 (1968)**, 433-441.

[Bo] A. Borel, *"Linear algebraic groups"*, GTM 126, Springer-Verlag, **1991**.

[CF] J. W. S. Cassels and A. Fröhlich (editor), *"Algebraic number theory"* Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union, Academic Press, London; Thompson Book Co., Inc., Washington, D.C. **1967**.

[CR] B. Chang and R. Ree, *"The characters of $G_2(q)$"*, Symposia Mathematica, Vol. XIII (Convegno di Gruppi e loro Rappresentazioni, INDAM, Rome,1972), Academic Press, London, **1974**, 395-413.

[D] D. Ž. Djoković, *"Product of two involutions"*, Arch. Math. (Basel) **18 (1967)**, 582-584.

[Ei] S. Eilenberg, *"On the problems of topology"*, Ann. of Math. **(2) 50 (1949)**, 247-260.

[El1] Erich W. Ellers, *"Products of two involutory matrices over skewfields"*, Linear Algebra Appl. **26 (1979)**, 59-63.

[El2] Erich W. Ellers, *"Decomposition of orthogonal, symplectic, and unitary isometries into simple isometries"*, Abh. Math. Sem. Univ. Hamburg **46 (1977)**, 97-127.

[El3] Erich W. Ellers, *"Bireflectionality in classical groups"*, Canad. J. Math. **29 (1977) no. 6**, 1157-1162.

[El4] Erich W. Ellers, *"Products of involutions in simple Chevalley groups"*, J. Geom. **69 (2000) no. 1-2**, 68-72.

[EG] Erich W. Ellers, N. Gordeev, *"On the conjectures of J. Thompson and O. Ore"*, Trans. Amer. Math. Soc. **350 (1998) no. 9**, 3657-3671.

[F] E. E. Floyd, *"Orbits of torus groups operating on manifolds"*, Ann. of Math. **(2) 65 (1957)**, 505-512.

[FKS] B. Fein, W. Kantor and M. Schacher, *"Relative Brauer groups II"*, Journal für die reine und angewandte Mathematik **328 (1981)**, 39-57.

[Fl] Y. Z. Flicker, *"A remark on local-global principles for conjugacy classes"*, Ark. Mat. **40 (2002) no. 1**, 47-53.

[FZ] W. Feit and G. J. Zuckermann, *"Reality properties of conjugacy classes in spin groups and symplectic groups"*, Algebraists' Homage: Papers in Ring Theory and Related Topics (S. A. Amitsur, D. J. Saltman and G. B. Seligman, eds.), Contemporary Mathematics **13 (1982)**, 239-253.

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

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

[J] N. Jacobson, *"Composition algebras and their automorphisms"*, Rendiconti del Circolo Matematico Palermo **(2) 7 (1958)**, 55-80.

[JL] G. James and M. Liebeck, *"Representations and characters of groups"*, Second edition, Cambridge University Press, New York, **2001**.

[K] M. Kneser, *"Lectures on Galois cohomology of classical groups, With an appendix by T. A. Springer, Notes by P. Jothilingam"*, Tata Institute of Fundamental Research Lectures on Mathematics, No. 47, Tata Institute of Fundamental Research, Bombay, **1969**.

[Ka] K. Kariyama, *"On conjugacy classes of maximal tori in classical groups"*, J. Algebra **125 (1989), no. 1**, 133-149.

[KMRT] M. A. Knus, A. Merkurjev, M. Rost and J. P. Tignol, *"The book of involutions"*, American Mathematical Society Colloquium Publications, vol. 44, The American Mathematical Society, Providence, RI, **1998**.

[KN] F. Knüppel and K. Nielsen, *"Products of involutions in* $\mathrm{O}^+(V)$*"*, Linear Algebra Appl. **94 (1987)**, 217-222.

[L] H. Lausch, *"Generators of automorphism groups of Cayley algebras"*, in Generators and relations in groups and geometries (Lucca, 1990), Kluwer Academic Publication, Dordrecht **1991**, pp. 69-94.

[M] G. D. Mostow, *"On a conjecture of Montgomery"*, Ann. of Math. **(2) 65 (1957)**, 513-516.

[MVW] C. Mœglin, M.-F. Vignéras and J.-L. Waldspurger, *"Correspondences de Howe sur un corps $p-$adique"*, Lecture Notes in Mathematics 1291, Springer-Verlag, Berlin, **1987**.

[N] A. Neumann, *"Bedingungen für die Zweispiegeligkeit der Automorphismengruppen von Cayleyalgebren"*, Geometriae Dedicata **34 (1990) no. 2**, 145-159.

[Ni] K. Nielsen, *"On bireflectionality and trireflectionality of orthogonal groups"*, Linear Algebra and its Application **94 (1987)**, 197-208.

[P] Richard S. Pierce, *"Associative algebras"*, Graduate Texts in Mathematics 88 Springer-Verlag, New York-Berlin, **1982**.

[Pr1] D. Prasad, *"On the self-dual representations of finite groups of Lie type"*, J. Algebra **210 (1998) no. 1**, 298-310.

[Pr2] D. Prasad, *"On the self-dual representations of a p-adic group"*, Internat. Math. Res. Notices **(1999) no. 8**, 443-452.

[R] J. D. Rogawski, *"Automorphisc representations of unitary groups in three variable"*, Annals of Math. Studies 123, Princeton University Press, **(1990)**.

[RS] R. W. Richardson and T. A. Springer, *" The Bruhat order on symmetric varieties"*, Geom. Dedicata **35 (1990) no. 1-3**, 389-436.

[S1] R. Steinberg, *"Regular elements of semisimple algebraic groups"*, Inst. Hautes tudes Sci. Publ. Math. **No. 25 (1965)**, 49-80.

[S2] R. Steinberg, *"On Galois cohomology of linear algebraic groups"*, Proceedings of an International Conference on the Theory of Groups, Canberra (1965), Gordon and Breach, London, **(1967)**, 315-319.

[S3] R. Steinberg, *"Conjugacy classes in algebraic groups"*, Notes by Vinay V. Deodhar, Lecture Notes in Mathematics, 366, Springer-Verlag, Berlin-New York, **(1974)**.

[S4] R. Steinberg, *"Lectures on Chevalley groups"*, Notes prepared by John Faulkner and Robert Wilson, Yale University, New Haven, Conn., **(1968)**.

[Se] J. P. Serre, *"Galois cohomology"*, Springer-Verlag, Berlin, **(1997)**.

[Si] A. Singh, *"Conjugacy classes of centralizers in G_2"*, preprint.

[Sp] T. A. Springer, *"Linear algebraic groups"*, second edition, Progress in Mathematics 9, Birkhäuser Boston, Boston, MA, **(1998)**.

[SS] T. A. Springer, R. Steinberg, *"Conjugacy classes"*, 1970 Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69), pp. 167-266 Lecture Notes in Mathematics, **Vol. 131** Springer, Berlin.

[ST1] A. Singh and M. Thakur, *"Reality properties of conjugacy classes in G_2"*, Israel Journal of Mathematics **145 (2005)**, 157-192.

[ST2] A. Singh and M. Thakur, *"Reality properties of conjugacy classes in algebraic groups"*, preprint.

[SV] T. A. Springer and F. D. Veldkamp, *"Octonions, Jordan algebras and exceptional groups"*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, **(2000)**.

[T] M. Thakur, *"Cayley algebra bundles on $\mathbb{A}^2_K$ revisited"*, Communications in Algebra **23 (1995) no. 13**, 5119-5130.

[TaZ] O. Taussky and H. Zassenhaus, *"On the similarity transformation between a matrix and its transpose"*, Pacific Journal of Mathematics **9 (1959)**, 893-896.

[TiZ] P. H. Tiep, A. E. Zalesski, *"Real conjugacy classes in algebraic groups and finite groups of Lie type"*, J. Group Theory **8 (2005) no. 3**, 291-315.

[V] C.R. Vinroot, *"A factorization in* $\mathrm{GSp}(V)$*"*, Linear Multilinear Algebra **52 (2004) no. 6**, 385-403.

[W1] M. J. Wonenburger, *"Transformations which are products of two involutions"*, Journal of Mathematics and Mechanics **16 (1966)**, 327-338.

[W2] M. J. Wonenburger, *"Automorphisms of Cayley algebras"*, Journal of Algebra **12 (1969)**, 441-452.

[Wa] G. E. Wall, *"On the conjugacy classes in the unitary, symplectic and orthogonal groups"*, Journal of the Australian Mathematical Society **3 (1963)**, 1-63.