University of Alberta

Lower Bounds for Essential Dimension of Algebraic Groups in the Characteristic 2 Case

by

Antonio Babic

A thesis submitted to the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Mathematics

Department of Mathematical and Statistical Sciences

Fall 2013
Edmonton, Alberta

Abstract

When computing the essential dimension of an algebraic group G defined over a field k, finding lower bounds is generally a much more difficult problem than finding upper bounds. For simple algebraic groups G of adjoint type, Chernousov-Serre developed a general method for computing lower bounds of G via an orthogonal representation. Their work did not cover the case when $char(k) = 2$, but they did note their belief that the method could be extended to this case. We will show that the method developed by Chernousov-Serre does indeed work in the characteristic 2 case. As an application, we employ the method to assist with the computation of the essential dimension of the orthogonal group O_n and simple adjoint groups of type G_2 in the characteristic 2 case.

Acknowledgements

Although this dissertation is an individual endeavour, it could not have been completed without the assistance, guidance and support of many people.

First I would like to thank my supervisor Dr. Vladimir Chernousov. He has a tremendous amount of knowledge and insight and I am humbled that he was willing to share some of this with me. His congenial disposition always made me feel invited in his office and fostered an environment of learning. If not for his support and genuine interest in my learning I may have missed out on the incredible learning experience that has been my PhD work.

I would like to thank the members of my supervisory committee Dr. Arturo Pianzola, Dr. Jochen Kuttler, Dr. Stefan Gille and Dr. Vakhtang Putkaradze for their time and insightful comments.

I would like to thank my fellow graduate students at the University of Alberta for creating such an enjoyable environment to learn in. I would like extend a special thank you to my office mate Uladzimir Yahorau. I always enjoyed our long math related discussions and they were invaluable in my growth as a mathematician.

I would like to thank my parents, Marija and Branko, for their emphasis on and commitment to my education, as well as for all the sacrifices they made to give me a chance to pursue my dreams. I would also like to thank my brother Marko for his proofreading work and constant encouragement.

Finally I would like to thank the most important person in my life, my

wife Stephanie. The magnitude of her love and support both inside and outside my academic career are beyond words. No matter how difficult or frustrating things became, she could always put a smile on my face and provided me with the motivation to work harder. I could not ask for a more perfect person with whom to share my achievement.

Contents

List of Tables

Chapter 1

Introduction

1.1 An Introduction to Essential Dimension

The essential dimension of an algebraic object can be thought of as the minimal number of independent parameters needed to define it. Essential dimension assigns a numerical invariant (a non-negative integer) to algebraic objects and allows us to compare their relative complexity. Naturally, the fewer parameters needed for definition, the simpler the object is.

The notion of essential dimension is relatively new and first appeared in a 1997 paper by J. Buhler and Z. Reichstein [BuRe] within the context of finite groups. A. Merkrujev later extended this notion to arbitrary covariant functors; see [BF03]. Before we examine how essential dimension first appeared in [BuRe], let us see some simple examples (taken from [Re]) to get an idea for what is going on.

Example 1:

Let q be a non-degenerate quadratic form on K^n where K/k is a field extension of a field k with $char(k) \neq 2$. Let b denote the bilinear form associated to q. We would like to know whether q can be "defined over" a smaller field $k \subset K_0 \subset K$, i.e. is there a K-basis $e_1, ..., e_n$ of K^n such that

$b_{ij} = b(e_i, e_j) \in K_0$ for all $i, j = 1, 2, ..., n$? Equivalently, this means that in this basis

$$q(x_1, ..., x_n) = \sum_{i=1}^{n} b_{ij} x_i x_j$$

has all of its coefficients in K_0.

It now makes sense to ask the question: "Is there a minimal field K_0 which q can be defined over?" In general, the answer to this question is no. However, in a similar vein, we can inquire: "Can we find a field K_0 of minimal transcendence degree over k such that q is defined over K_0?" This question is much more tractable and often has a positive response and so leads us to the following definition. The smallest possible value of $tr.deg_k(K_0)$ such that q is defined over K_0 is called the essential dimension of q and is denoted $ed(q)$ or $ed_k(q)$.

Example 2:

Again, let k be an arbitrary field, K/k a field extension and consider a linear transformation $T\colon K^n \to K^n$. We say that two linear transformations are equivalent if their corresponding transformation matrices are conjugates over K. If the transformation matrix of T is (a_{ij}), then we say that T descends to K_0 for $k \subset K_0 \subset K$ if $a_{ij} \in K_0$ for all $i, j = 1, 2, ..., n$. We define the essential dimension of T to be the smallest possible value of $tr.deg_k(K_0)$ and write $ed(T)$ or $ed_k(T)$ for this value. Clearly, T descends to $k(a_{ij} \mid i, j = 1, 2, ..., n)$, so $ed(T) \leq n^2$.

However, we can improve dramatically upon this upper bound. By considering the rational canonical form R of the transformation matrix of T, we obtain an equivalent linear transformation whose matrix has at most n entries which are not 0 or 1. Thus, using this argument we see that $ed(T) \leq n$.

We have now seen two very concrete examples of essential dimension. Let us proceed with a more formal definition of essential dimension and see how our two examples fit into this context.

Let k be our base field, $Fields_k$ the category of field extensions over k and

$$\mathcal{F}\colon Fields_k \longrightarrow Sets$$

a covariant functor.

For K/k a field extension, we say that $a \in \mathcal{F}(K)$ *descends* to K_0 if $k \subset K_0 \subset K$ and a is in the image of $\mathcal{F}(K_0) \to \mathcal{F}(K)$. The *essential dimension* of $a \in \mathcal{F}(K)$ is defined as

$$ed(a) = min\{tr.deg_k K_0\},$$

where the minimum is taken over all subfields K_0 such that a descends to K_0. If $ed(a) = tr.deg_k K$, we say that a is *incompressible*. The *essential dimension* of the functor $\mathcal{F}$ is defined as the supremum of $ed(a)$ taken over all $a \in \mathcal{F}(K)$ and over all field extensions K/k.

In Example 1, $\mathcal{F}(K)$ is the set of K-isomorphism classes of non-degenerate quadratic forms on K^n. In Example 2, $\mathcal{F}(K)$ is the set of equivalence classes of linear transformations $K^n \to K^n$. We saw in both of these examples that $ed(\mathcal{F}) \leq n$ and in fact it is possible to show $ed(\mathcal{F}) = n$ for each of these examples.

Related to the definition of essential dimension we also have the following notion. The *essential dimension at p* (where p is a prime number) of $a \in \mathcal{F}(L)$ is defined as

$$ed(a; p) = min\{ed(a_K)\},$$

where a_K is the image of a in $\mathcal{F}(K)$ and the minimum is taken over all field extensions K such that $[K\colon L]$ is finite and prime to p. The *essential dimension at p* of $\mathcal{F}$ is

$$ed(\mathcal{F}; p) = max\{ed(a; p)\}$$

where the maximum is taken over all (L, a) with $a \in \mathcal{F}(L)$.

To give some historical perspective, we will explain where the idea of essential dimension first came from. Consider the following age-old problem: We would like to find a "radical formula" for the roots of a polynomial $x^n + a_1x^{n-1} + ... + a_n$ over some field k. By radical formula we mean a formula involving only addition, subtraction, multiplication, division and n-th roots. Let us start by examining the case $n = 2$.

Let $f(x) = x^2 + ax + b$ and define $L = k[x]/\langle f(x)\rangle$. Thus L is the field attained from k by adjoining a root of $f(x)$. We know that we can choose an element $\alpha \in L$ whose minimal polynomial g_α depends on a smaller number of parameters than f. For example, if we choose α with trace 0, then g_α is of the form $x^2 - d$. Here we can easily find a radical formula $\alpha = \sqrt{d}$. But then we have a formula for any element of L, including for the roots of our minimal polynomial $f(x)$, because any element of L can be written as $l_1 + l_2\alpha$ for $l_1, l_2 \in k$. From this process we can derive the well known quadratic formula

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

We can develop similar formulas for $n = 3, n = 4$, but Galois proved that no such formula exists for $n \geq 5$.

Now consider the situation where $K = k(t_1, ..., t_n)$, the generic polynomial $f = x^n + t_1x^{n-1} + ... + t_n$ and the field extension $L = K[x]/\langle f\rangle$. Let $\alpha \in L$ and write its minimal polynomial as $g_\alpha = x^n + f_1x^{n-1} + ... + f_n$ where $f_i \in K$. As before we can choose $\alpha \in L$ so that the field generated by the coefficients of its minimal polynomial $k(f_1, ..., f_n) = E \subset K$ is a proper subfield (e.g. take α with trace 0). If we define $F = E[x]/\langle g_\alpha\rangle$ then we have that $F \otimes_E K = L$ because, similarly to the case $n = 2$ from above, the powers of α will form a K-basis for L. In this case we say that L *descends* to F. We would like to choose α so that the corresponding field E has the smallest possible transcendence degree over k, because this field would be simpler than our original field L.

Note that L in the previous paragraph was a separable algebra, and it is

known that its twisted forms can be described by the Galois cohomology functor $H^1(-, S_n)\colon E/k \to H^1(E, S_n)$. It was for this functor that Z. Reichstein and J. Buhler first introduced the notion of essential dimension; see [BuRe]. It turns out that the consideration of these Galois cohomology functors is very natural and leads us to the following definition.

Let G be a smooth linear algebraic group over a field k and consider the covariant functor

$$\begin{aligned} \mathcal{F}\colon Fields_k &\longrightarrow Sets \\ K &\longmapsto H^1(K, G). \end{aligned}$$

We define the *essential dimension (at p)* of G to be the essential dimension (at p) of this functor $\mathcal{F}$. Thus, by definition, if G is an algebraic group, the essential dimension of G is the minimal number of parameters needed to define all G-torsors.

Related to the notion of essential dimension is that of compressibility. In Example 1 above we saw the definition of the essential dimension of a quadratic form when the base field did not have characteristic 2. We will extend this notion to arbitrary fields. Let K/k be a field extension of an arbitrary field k and f a quadratic form over K. Then, if there exists another quadratic form g defined over a field L/k satisfying

- $k \subset L \subset K$;
- $tr.deg_k L < tr.deg_k K$; and
- $g \otimes_L K \simeq f$

we say that f is *compressible*. Otherwise, it is *incompressible*. Then, as in Example 1, we can define the essential dimension of f to be the smallest possible value of $tr.deg_k(L)$ such that f "compresses" to L.

Since the area of essential dimension is still relatively new there are many open questions. For example, even the essential dimension of the group that spawned the notion of essential dimension, S_n, is still unknown. As of right

now, it is known that if $char(k) = 0$, then

$$[n/2] \leq ed(S_n) \leq n - 3.$$

The precise values are known for some small values of n. Most recently A. Duncan, in [Du], proved $ed(S_7) = 4$, but for higher values of n this remains an open problem.

Despite only being in its infancy, the study of essential dimension has become very popular and many mathematicians have contributed results to this area. Most notably, Brosnan, Reichstein and Vistoli computed the essential dimension of spin groups through the use of stacks [BRV] and Merkurjev and Karpenko found the essential dimension of p-groups, in good characteristic, by employing K-theory [KM]. In an upcoming paper A. Merkurjev gives an overview of essential dimension, its connection to other areas of mathematics and the current state of open problems; see [Me].

We now will turn our attention to the heart of this dissertation. In general, computing lower bounds for essential dimension is more difficult than computing upper bounds. If G is an algebraic group and $G \to \mathrm{GL}(V)$ is a generically free representation, then a result from [Re2] says $ed(G) \leq \dim(V) - \dim(G)$. To get an upper bound we take a generically free representation of smallest possible dimension and then subtract the dimension of the group from this value. There is no method for computing lower bounds which works quite so easily as the one for upper bounds. However, a general method of computing lower bounds of essential dimensions of algebraic groups over fields of characteristic $\neq 2$ via orthogonal representations was proposed in a 2006 paper [ChSe] by V. Chernousov and J.-P. Serre.

In this paper, regarding their method for computing lower bounds, the authors remarked

It seems likely that a similar method can also be applied in characteristic 2 ...

The goal of this dissertation is to extend this method for computing lower

bounds of essential dimension to the characteristic 2 case. Results regarding essential dimension in the characteristic 2 case can vary wildly from their non-characteristic 2 counterparts. For example, if $char(k) \neq 2$ it is known that for the orthogonal group $\mathcal{O}_n$ we have $ed(\mathcal{O}_n) = n$. However, as will be seen in Theorem 1.2.2, the essential dimension of the orthogonal group in the characteristic 2 case is quite different.

In attempting to extend the method for computing lower bounds in [ChSe] to the characteristic 2 case many roadblocks arise. The primary difficulties when working in characteristic 2 are related to the definition and manipulation of quadratic forms and an object known as the Witt group which will be described in Section 2.2. We will now proceed to state the main Theorem and results of this dissertation.

1.2 The Main Theorem and Results

In what follows, we will be assuming that $\text{char}(k) = 2$ and k is algebraically closed. Let $K = k(t_1, ..., t_r, u)$ where $t_1, ..., t_r, u$ are algebraically independent indeterminates. Let G° be a simple algebraic group over k of adjoint type and let T be a maximal torus of G° of rank r. Let $c \in \text{Aut}(G^\circ)$ be such that $c^2 = 1$ and $c(t) = t^{-1}$ for each $t \in T$ (it is known that such an automorphism exists, see e.g. [DeGr, Exp. XXIV, Prop. 3.16.2, p. 355]. This automorphism is inner (i.e. belongs to G°) if and only if -1 belongs to $W_G(T)$, the Weyl group of (G, T). When this is the case we put $G = G^\circ$. If not, we define G to be the subgroup of $\text{Aut}(G^\circ)$ generated by G° and c. We have

- $G = G^\circ$ for types A_1, B_r, C_r, D_r (r even), G_2, F_4, E_7, E_8; and
- $(G\colon G^\circ) = 2$ and $G = \text{Aut}(G^\circ)$ for types $A_r (r \geq 2), D_r$ (r odd), E_6.

Theorem 1.2.1. *If G is as above, then we have $ed(G; 2) \geq r + 1$.*

We will prove the Theorem in two steps:

1. We construct a particular cocycle θ_G in $H^1(K, G)$ for K defined as above and depending on $r + 1$ parameters.

2. We construct an orthogonal representation for G and show that the twisted quadratic form associated to the image of θ_G under this representation is incompressible.

Of course, the last property implies that the cocycle θ_G is incompressible and the Theorem follows.

In order to construct this orthogonal representation we will need to know explicitly the Killing forms of split simple Lie algebras of simply connected groups defined over $\mathbb{Z}$. The computation of these is done in Chapter 3. Next, in Chapter 4 we construct our desired orthogonal representation. In Chapter 5 we describe our particular cocycle and determine explicitly the types of quadratic forms associated to this cocycle. In Chapter 6 we show that these associated quadratic forms are incompressible and then in Chapter 7 we put everything together to complete the proof of Theorem 1.2.1.

This approach must be modified for groups of type B_r and F_4. For B_r we will not use the orthogonal representation constructed in Chapter 4, but instead will use the standard representation. This special case will be discussed in Section 5.2. To deal with F_4 we will use a totally different approach relying on the theory of cohomological invariants. This special case will be discussed in Section 7.2. The reason for treating these cases separately is that the process detailed in the previous paragraph produces a weaker lower bound than Theorem 1.2.1 asks for.

We will now state two more Theorems whose proofs are based on the main Theorem.

Theorem 1.2.2. *Let $\mathcal{O}_m$ denote the smooth orthogonal group of dimension m defined over a field k of characteristic 2. Then,*

- $ed(\mathcal{O}_{2n}) = n + 1$;
- $ed(\mathcal{O}_{2n+1}) = n + 2$.

Theorem 1.2.3. *Let $\mathbf{G}_2$ be a split simple algebraic group of type G_2 defined over a field k of characteristic 2. Then*

$$ed(\mathbf{G}_2) = 3.$$

In Chapter 7, these two results will be proven by relying on Theorem 1.2.1.

Chapter 2

Background Information

2.1 Quadratic Forms

In this Section we will briefly recall the definition of a quadratic form and explain some associated concepts/definitions, which will be used throughout. Note that all the definitions in this Section make the assumption that the characteristic of the field we work over is 2. The definitions and results below are taken from [EKM].

Let F be an arbitrary field and V a finite dimensional vector space over F. A *quadratic form* is a map $q\colon V \to F$ satisfying:

1. $q(av) = a^2 q(v)$ for all $v \in V$ and $a \in F$; and
2. (Polar Identity) $b_q\colon V \times V \to F$ defined by

$$b_q(v, w) = q(v + w) - q(v) - q(w)$$

is a bilinear form.

We call the pair (V, q) a *quadratic space*.

There is a standard notation for certain types of quadratic forms. If $a \in F$, we denote the quadratic form on a one-dimensional vector space $V = F$

defined as $q(v) = av^2$, by $\langle a \rangle$. We will denote the direct sum $\langle a_1 \rangle \oplus \langle a_2 \rangle \oplus ... \oplus \langle a_n \rangle$ as $\langle a_1, ..., a_n \rangle$. As well, the form $\langle a, a, ..., a \rangle$ will be denoted $r\langle a \rangle$ where r is the number of times a appears. Finally, if $a, b \in F$, the 2-dimensional quadratic form on $V = F^2$ given by $q(v, w) = av^2 + vw + bw^2$ will be denoted $[a, b]$.

If $(V, q), (W, p)$ are two quadratic spaces, we say that a map $\varphi \colon V \to W$ is an *isometry* if

- φ is a linear isomorphism; and
- $p(\varphi(v)) = q(v)$ for all $v \in V$.

If an isometry exsits between two quadratic spaces, we say that they are *isometric*.

Let V be a finite dimensional vector space over an arbitrary field F. We define the *hyperbolic form* of V to be the form on the vector space $V \oplus V^*$ given by

$$\begin{aligned} \mathbb{H}(V) \colon \ V \oplus V^* &\longrightarrow F \\ (v, f) &\longrightarrow f(v). \end{aligned}$$

Note that any such form is isometric to a quadratic form of the shape

$$[0, 0] \oplus [0, 0] \oplus ... \oplus [0, 0].$$

If q is a quadratic form which is isometric to $\mathbb{H}(W)$ for some vector space W, then we say q is a *hyperbolic form*. Also, the form $\mathbb{H}(F)$ is called the *hyperbolic plane* and denoted simply by $\mathbb{H}$.

Let $b \colon V \times V \to F$ be a bilinear form. The *radical* of b is defined as

$$\mathrm{rad}(b) = \{v \in V \mid b(v, w) = 0 \ \forall \ w \in V\}.$$

Let $q\colon V \to F$ be a quadratic form. The *quadratic radical* of q is defined as

$$\mathrm{rad}(q) = \{v \in \mathrm{rad}(b_q) \mid q(v) = 0\}.$$

We say that q is *regular* if $\mathrm{rad}(q) = 0$.

If $\mathfrak{b}\colon V \times V \to F$ is a bilinear form and L/F is a field extension, then $\mathfrak{b}_L$ is a bilinear form on $L \otimes_F V := V_L$ given by

$$\mathfrak{b}_L(a \otimes v, c \otimes w) = ac\ \mathfrak{b}(v, w).$$

Similarly, if $q\colon V \to F$ is a quadratic form and L/F is a field extension, then we can define a quadratic form

$$q_L\colon V_L = L \otimes_F V \to L, \quad q_L(a \otimes v) = a^2 q(v).$$

With these definitions in hand consider the following result:

Lemma 2.1.1. *Let q be a quadratic form over F. Then the following are equivalent:*

1. *q_L is regular for every field extension L/F.*
2. *q_L is regular over an algebraically closed field L containing F.*
3. *q is regular and $\dim(\mathrm{rad}(b_q)) \leq 1$.*

Proof. See [EKM, Lemma 7.1.6]. □

A quadratic form q over F satisfying any of above three equivalent conditions is called *nondegenerate*. We have the following results on nondegeneracy:

Lemma 2.1.2. *Let F be an arbitrary field. Then*

1. *the form $\langle a \rangle$ is nondegenerate if and only if $a \in F^\times$;*
2. *the form $[a, b]$ is nondegenerate.*

Proof. See [EKM, Proposition 7.19]. □

Lemma 2.1.3. *If φ and ψ are nondegenerate quadratic forms over F and at least one of them is even-dimensional, then $\varphi \oplus \psi$ is nondegenerate.*

Proof. See [EKM, Remark 7.2.1 (3)] □

The next two results provide a sort of analog of the diagonalization of quadratic forms in the characteristic 2 case.

Lemma 2.1.4. *Let φ be a quadratic form on V over F. Then there exists 2-dimensional subspaces $V_i \subset V$, $1 \leq i \leq n$ for some n, a subspace $W \subset \mathrm{rad}(b_\varphi)$, and an orthogonal decomposition*

$$\varphi = \varphi|_{rad(\varphi)} \oplus \varphi|_W \oplus \varphi|_{V_1} \oplus ... \oplus \varphi|_{V_n},$$

with $\varphi_{V_i} \simeq [a_i, b_i]$, nondegenerate, $a_i, b_i \in F$ for all $i = 1, ..., n$. In particular,

$$\varphi \simeq r\langle 0\rangle \oplus \langle c_1, c_2, ...c_s\rangle \oplus [a_1, b_1] \oplus ... \oplus [a_n, b_n],$$

where $r = \dim(\mathrm{rad}(\varphi))$ and $s = \dim(W), c_i \in F^\times$ for $i = 1, ..., s$.

Proof. See [EKM, Proposition 7.3.1] □

When the form we begin with is nondegenerate, we have a stronger version of this Lemma:

Lemma 2.1.5. *Let φ be a nondegenerate quadratic form over F.*

1. *If $\dim \varphi = 2n$, then*

$$\varphi \simeq \oplus_{i=1}^n [a_i, b_i]$$

   for some $a_i, b_i \in F$.

2. *If $\dim \varphi = 2n + 1$, then*

$$\varphi \simeq \oplus_{i=1}^n [a_i, b_i] \oplus \langle c\rangle$$

for some $a_i, b_i \in F$ and $c \in F^\times$ unique up to $(F^\times)^2$.

Proof. See [EKM, Corollary 7.3.2]. □

Let $q\colon V \to F$ be a quadratic form. Let $\overline{V} := V/\mathrm{rad}(q)$ and let $\pi\colon V \to \overline{V}$ be the canonical epimorphism. Consider the mapping $\overline{q}\colon \overline{V} \to F$ given by $\overline{q}(\overline{v}) = q(v)$ where v is any lift of $\overline{v}$. We first claim that this map is well defined.

Indeed, let $\overline{v} \in \overline{V}$ and let v_1, v_2 be two liftings of $\overline{v}$. We must show that $q(v_1) = q(v_2)$. By definition we can write $v_2 = v_1 + u$ where $u \in \mathrm{rad}(q)$. Since $u \in \mathrm{rad}(q) \subset \mathrm{rad}(b_q)$ we know that $0 = b_q(v_2, u)$. From this we get

$$0 = b_q(v_2, u) = q(v_2 + u) + q(v_2) + \underbrace{q(u)}_{=0} = q(v_2 + u) + q(v_2)$$
$$\Rightarrow q(v_2) = q(v_2 + u) = q(v_1).$$

Moreover, this mapping defines a quadratic form because

- $\overline{q}(a\overline{r}) = \overline{q}(\overline{ar}) = q(ar) = a^2 q(r) = a^2 \overline{q}(\overline{r})$; and
- $b_{\overline{q}}(v, w) = \overline{q}(\overline{v+w}) - \overline{q}(\overline{v}) - \overline{q}(\overline{w}) = q(v+w) - q(v) - q(w) = b_q(v, w)$.

We will call $\overline{q}$ the *normalization* of q.

For the remainder of this Section consider the general situation where we have a quadratic form q defined over an algebraically closed field F. Since F is algebraically closed we know that in the decomposition given by Lemma 2.1.4 we can choose the c_i to be 0 or 1. Thus we may write our form as

$$q = [a_1, b_1] \oplus ... \oplus [a_n, b_n] \oplus \langle c_1, ..., c_n \rangle, \;\; c_i \in \{0, 1\}.$$

Moreover, we claim that if at least one of the $c_i = 1$, then we may assume without loss of generality that exactly one of the $c_i = 1$. Indeed, consider the quadratic form $\widetilde{q} = \langle 1 \rangle \oplus \langle 1 \rangle$ defined over a vector space V with basis

e_1, e_2. Consider a new basis $e_1' = e_1 + e_2, e_2' = e_2$. Then we have

$$\begin{aligned}\widetilde{q}(xe_1' + ye_2') &= \widetilde{q}(xe_1 + (x+y)e_2) = x^2 + (x+y)^2 = x^2 + x^2 + y^2 \\ &= 0x^2 + 1y^2 \simeq \langle 0\rangle \oplus \langle 1\rangle.\end{aligned}$$

Then by induction our claim follows.

We can also show that in the case of an algebraically closed field $[a, b] \simeq [0, 0]$ for any $a, b \in F$. Indeed, by [EKM, 7.19] in characteristic 2 every binary isotropic nondegenerate form is isometric to $\mathbb{H} = [0, 0]$. So to prove our claim, we only need to show that $[a, b]$ is isotropic. We first consider the case where one of a or b equals 0. Without loss of generality consider $[a, 0]$. Then $[a, 0](0, 1) = a \cdot 0^2 + 0 \cdot 1 + 0 \cdot 1^2 = 0$, so $[a, 0]$ is isotropic and therefore isometric to $[0, 0]$.

Now consider the case where neither a nor b equals 0. Note that

$$ax^2 + xy + by^2 = 0 \Leftrightarrow x^2 + x\frac{y}{a} + ab\left(\frac{y}{a}\right)^2 = 0$$

so we can consider the form $[1, ab]$ instead. Then, by 7.6 in [EKM] this form is isotropic if and only if $z^2 + z + ab$ has a root in F. However, since F is algebraically closed a root exists and hence $[a, b] \simeq [0, 0]$, as desired.

With the two previous results in hand we know that an arbitrary quadratic form q can be expressed in one of the following two forms:

$$q \simeq [0, 0] \oplus .... \oplus [0, 0] \oplus \langle 1\rangle \oplus (m-1)\langle 0\rangle \quad \text{(type 1)}$$

or

$$q \simeq [0, 0] \oplus .... \oplus [0, 0] \oplus m\langle 0\rangle \quad \text{(type 2)}.$$

For either type, we will make the convention that our quadratic form q is defined over a vector space V with fixed basis $\{e_1, ..., e_{2n}, e_{2n+1}, ..., e_{2n+m}\}$. This means that we have n summands of the form $[0, 0]$ for both types, $m - 1$ $\langle 0\rangle$ summands for forms of type 1 and m $\langle 0\rangle$ summands for forms of

type 2.

Next, we would like to describe the radical of q for each type. In general, if we can write a quadratic form as $\widetilde{q} = \widetilde{q}_1 \oplus \widetilde{q}_2$, then by examining definitions its easy to see $b_{\widetilde{q}} = b_{\widetilde{q}_1} \oplus b_{\widetilde{q}_2}$. Then, by combining induction and this fact its easy to see that for forms of type 1 we have

$$b_q = \bigoplus_{i=1}^{n} b_{[0,0]} \oplus \bigoplus_{j=1}^{m} b_{\langle c_j \rangle}$$

and a similar decomposition exists for forms of type 2. Then note,

$$\begin{aligned} b_{\langle c_i \rangle}(x,y) &= \langle c_i \rangle(x+y) + \langle c_i \rangle(x) + \langle c_i \rangle(y) = c_i(x+y)^2 + c_i x^2 + c_i y^2 \\ &= c_i x^2 + c_i y^2 + c_i x^2 + c_i y^2 = 0. \end{aligned}$$

and

$$\begin{aligned} b_{[0,0]}((x_1,y_1),(x_2,y_2)) &= [0,0]((x_1+y_1, x_2+y_2)) + [0,0]((x_1,x_2)) + [0,0]((y_1,y_2)) \\ &= 0(x_1+y_1)^2 + (x_1+y_1)(x_2+y_2) + 0(x_2+y_2)^2 \\ &+ 0x_1^2 + x_1x_2 + 0x_2^2 + 0y_1^2 + y_1y_2 + 0y_2^2 \\ &= x_1x_2 + x_1y_2 + y_1x_2 + y_1y_2 + x_1x_2 + y_1y_2 \\ &= x_1y_2 + y_1x_2. \end{aligned}$$

It follows that for both types of forms we get

$$\mathrm{rad}(b_q) = span\{e_{2n+1}, ..., e_{2n+m}\}.$$

Furthermore we get

$$\mathrm{rad}(q) = span\{e_{2n+2}, ..., e_{2n+m}\} \quad \text{for forms of type 1}$$

and

$$\mathrm{rad}(q) = span\{e_{2n+1}, ..., e_{2n+m}\} \quad \text{for forms of type 2.}$$

Knowing this we can say precisely what the normalization of each of these

forms looks like. For forms of type 1 the normalization looks like

$$\overline{q} \simeq \bigoplus_{i=1}^{n} [0,0] \oplus \langle 1 \rangle$$

and for forms of type 2 the normalization looks like

$$\overline{q} \simeq \bigoplus_{i=1}^{n} [0,0].$$

Note that for either type, each summand in the normalization is nondegenerate by Lemma 2.1.2 and then by Lemma 2.1.3 so is their orthogonal sum. Thus the normalization of an arbitrary quadratic form is nondegenerate, a result which we will record as a Lemma.

Lemma 2.1.6. *Given an arbitrary quadratic form q defined on a vector space V over F, its normalization $\overline{q}\colon \overline{V} = V/\mathrm{rad}(q) \to F$ is nondegenerate.*

We also need the following result from [EKM, Theorem 8.4], known as the "Witt Cancellation Theorem", for later use:

Lemma 2.1.7. *Let φ, φ' be quadratic forms on V and V' respectively and ψ, ψ' quadratic forms on W and W' respectively, with $\mathrm{rad}\, b_\psi = 0 = \mathrm{rad}\, b_{\psi'}$. If*

$$\varphi \oplus \psi \simeq \varphi' \oplus \psi' \quad \textit{and} \quad \psi \simeq \psi',$$

then $\varphi \simeq \varphi'$.

The last goal we would like to achieve in this Section is to relate the orthogonal group of a quadratic form to that of its normalization. Recall that given a quadratic space (V, q) we defined the *orthogonal group* related to this space to be

$$\mathcal{O}(V,q) = \{x \in \mathrm{GL}(V) \mid q(x(v)) = q(v) \ \forall\ v \in V\}.$$

We would like to define

$$\lambda\colon \mathcal{O}(V,q) \longrightarrow \mathcal{O}(\overline{V},\overline{q}).$$

First note that the canonical epimorphism $\pi\colon V \to \overline{V}$ preserves length, i.e. $\overline{q}(\pi(v)) = \overline{q}(\overline{v}) = q(v)$.

Next, given $x \in \mathcal{O}(V,q)$ define $\lambda(x) = \overline{x}\colon \overline{V} \to \overline{V}$ by $\overline{x}(\overline{v}) = \overline{x(v)}$. First we claim this mapping is well defined, for which we must show $x(\mathrm{rad}(q)) \subset \mathrm{rad}(q)$. To prove this claim we first need to show that $x(v) \in \mathrm{rad}(b_q)$ for $v \in \mathrm{rad}(q)$. Let $w_0 \in V$. Since x is invertible we have $x(w) = w_0$ for some $w \in V$. Then

$$\begin{aligned} b_q(x(v), w_0) &= q(x(v) + w_0) + q(x(v)) + q(w_0) \\ &= q(x(v) + x(w)) + q(x(v)) + q(x(w)) \\ &= q(x(v+w)) + q(x(v)) + q(x(w)) \\ &= q(v+w) + q(v) + q(w) = b_q(v,w) = 0 \end{aligned}$$

because $v \in \mathrm{rad}(q) \subset \mathrm{rad}(b_q)$. We also have $q(x(v)) = q(v) = 0$. Thus, $x(v) \in \mathrm{rad}(q)$.

It remains to see that $\overline{x} \in \mathcal{O}(\overline{V},\overline{q})$. However, $\overline{q}(\overline{x}(\overline{v})) = \overline{q}\left(\overline{x(v)}\right) = q(x(v)) = q(v) = \overline{q}(\overline{v})$. Thus we have the following result:

Lemma 2.1.8. *A canonical mapping $V \to \overline{V}$ induces a natural morphism*

$$\lambda\colon \mathcal{O}(V,q) \longrightarrow \mathcal{O}(\overline{V},\overline{q}).$$

2.2 The Witt Group in Characteristic 2

In this Section we will introduce the notion of the Witt group, discuss a structure Theorem of the Witt group in characteristic 2 for certain fields due to Arason and conclude by giving some simple tools used to manipulate elements of the Witt group.

Given two quadratic forms $q\colon V \to F$ and $p\colon W \to F$ we can define their orthogonal sum as $q \oplus p\colon V \oplus W \to F, (v, w) \to q(v) + p(w)$. This is again a quadratic form. By Lemma 2.1.3 if p, q are two even-dimensional, nondegenerate quadratic forms over a field F, then their orthogonal sum is again nondegenerate. Thus, the isometry classes of even-dimensional nondegenerate quadratic forms over F form a monoid under orthogonal sum.

In general, if M is any monoid, we have an associated construction called the *Grothendieck group*, which turns any monoid into a group. On $M \times M$ we define a coordinate-wise addition $(m_1, m_2) + (n_1, n_2) = (m_1 + n_1, m_2 + n_2)$. Then we can define an equivalence relation where $(m_1, m_2) \sim (n_1, n_2)$ if there exists $k \in M$ such that $m_1 + n_2 + k = m_2 + n_1 + k$. If we mod out $M \times M$ by this equivalence relation, it will produce a group, known as the Grothendieck group. Note that in this group the identity element is the class of any element of the form (m, m) and the inverse of (m_1, m_2) is (m_2, m_1).

Now we return to our situation where we have the monoid consisting of isometry classes of even-dimensional, nondegenerate quadratic forms over a field F. The *quadratic Witt group* or just *Witt group* is the quotient of the Grothendieck group of this monoid by the subgroup generated by the image of the hyperbolic plane. We will denote this group by $W_q(F)$.

Next we will summarize the results of [Ar1] related to the structure of the Witt group over complete fields in characteristic 2. Let K be a field of characteristic 2, s an indeterminate over K and let $K((s))$ be the field of formal Laurent series over K. If f is a quadratic form over $K((s))$, we will denote its image in $W_q(K((s)))$ by f_W.

Theorem 2.2.1. *$W_q(K((s)))$ is the additive group generated by the elements $[\alpha, \beta s^{-k}]_W$ and $[\alpha s^{-1}, \beta s^{-k+1}]_W$ where $k \in \mathbb{Z}$, $k \geq 0$ and $\alpha, \beta \in K$, with the condition that $[\alpha, \beta s^{-k}]_W$ and $[\alpha s^{-1}, \beta s^{-k+1}]_W$ are biadditive as*

functions of α, β and satisfy the following sets of relations:

$$[\alpha, \beta\rho^2 s^{-k}]_W + [\beta, \alpha\rho^2 s^{-k}]_W = 0 \text{ if } k \text{ is even} \tag{2.1a}$$

$$[\alpha s^{-1}, \beta\rho^2 s^{-k+1}]_W + [\beta s^{-1}, \alpha\rho^2 s^{-k+1}]_W = 0 \text{ if } k \text{ is even} \tag{2.1b}$$

$$[\alpha, \beta\rho^2 s^{-k}]_W + [\beta s^{-1}, \alpha\rho^2 s^{-k+1}]_W = 0 \text{ if } k \text{ is odd} \tag{2.1c}$$

$$[\alpha, \alpha\rho^2 s^{-2k}]_W + [\alpha, \rho s^{-k}]_W = 0 \tag{2.2a}$$

$$[\alpha s^{-1}, \alpha\rho^2 s^{-2k+1}]_W + [\alpha s^{-1}, \rho s^{-k+1}]_W = 0 \tag{2.2b}$$

Here k runs through the non-negative integers and α, β and ρ run through K.

Theorem 2.2.2. *For $m \geq 0$ let $W_q(K((s)))_m$ be the subgroup of $W_q(K((s)))$ generated by the $[\alpha, \beta s^{-k}]_W$ and $[\alpha s^{-1}, \beta s^{-k+1}]_W$ where $k \in \mathbb{Z}, 0 \leq k \leq m$ and $\alpha, \beta \in K$. Then:*

- *$W_q(K((s)))_0$ is isomorphic to $W_q(K) \oplus W_q(K)$. A generator $[\alpha, \beta]_W$ of $W_q(K((s)))_0$ is sent to $[\alpha, \beta]_W$ in the first summand $W_q(K)$, but a generator $[\alpha s^{-1}, \beta s]_W$ corresponds to $[\alpha, \beta]_W$ in the second summand.*
- *If $n > 0$ then $W_q(K((s)))_{2n}/W_q(K((s)))_{2n-1}$ is isomorphic to $K \wedge_{K^2} K \oplus K \wedge_{K^2} K$. The class of a generator $[\alpha, \beta s^{-2n}]_W$ corresponds to $\alpha \wedge \beta$ in the first summand, but the class of a generator $[\alpha s^{-1}, \beta s^{-2n+1}]_W$ corresponds to $\alpha \wedge \beta$ in the second summand.*
- *If $n \geq 0$ then $W_q(K((s)))_{2n+1}/W_q(K((s)))_{2n}$ is isomorphic to $K \otimes_{K^2} K$. The class of a generator $[\alpha, \beta s^{-2n+1}]_W$ corresponds to $\alpha \otimes \beta$, but the class of a generator $[\alpha s^{-1}, \beta s^{-2n}]_W$ corresponds to $\beta \otimes \alpha$.*

We conclude this Section by providing some simple Lemmas related to quadratic forms and the Witt group in characteristic 2. We will make use of these results in Chapter 6 to prove the incompressibility of so-called canonical monomial forms which will be defined later.

Lemma 2.2.3. *Let $a, b \in K((s))$ be such that $ab \in sK[[s]]$. Then $[a, b]$ is hyperbolic, i.e. $[a, b]_W$ is zero in the Witt group $W_q(K((s)))$.*

Proof. See [Ar1, Lemma 3]. □

Lemma 2.2.4. *Over a field of characteristic 2 every binary isotropic non-degenerate quadratic form is isomorphic to the hyperbolic plane.*

Proof. See [EKM, 7.19 (4)]. □

Lemma 2.2.5. *Let $a, b \in F^\times$, where F is a field of characteristic 2. Then, $a[1, b] \simeq [a^{-1}, ab]$*

Proof. Given $a[1, b] = ax^2+axy+aby^2$ consider the linear change of variables $\widetilde{x} = ax, \widetilde{y} = y$. Then our form becomes $a^{-1}\widetilde{x}^2 + \widetilde{x}\widetilde{y} + ab\widetilde{y}^2 = [a^{-1}, ab]$. □

Lemma 2.2.6. *Let $[a, b]$ be a binary quadratic form over a field F of characteristic 2. Then, $[a, b]$ is hyperbolic $\iff ab = f + f^2$ for some $f \in F$.*

Proof. See [EKM, 7.6] and apply Lemma 2.2.4. □

Lemma 2.2.7. *$[1, \alpha^2 s^{-2n}]_W = [1, \alpha s^{-n}]_W$ for any $\alpha \in K$ and any nonegative integer n.*

Proof. Follows directly from equality (2.2a). □

Lemma 2.2.8. *Let K be an arbitrary field of characteristic 2, $K((s))$ the field of formal Laurent series over K and let $u, v, p, q \in K$ be arbitrary. Then*

$$[u^2 p, v^2 q s^{-n}] \simeq [p, v^2 u^2 q s^{-n}] \tag{2.3a}$$

$$[u^2 p s^{-1}, v^2 q s^{-n+1}] \simeq [p s^{-1}, v^2 u^2 q s^{-n+1}] \tag{2.3b}$$

Proof.

$$[u^2 p, v^2 q s^{-n}] = u^2 p x^2 + xy + v^2 q s^{-n} y^2.$$

Consider the change of variables $\widetilde{x} = ux, \widetilde{y} = y/u$ to get:

$$p\widetilde{x}^2 + \widetilde{x}\widetilde{y} + v^2 q s^{-n} y^2 \frac{u^2}{u^2} = p\widetilde{x} + \widetilde{x}\widetilde{y} + v^2 u^2 q s^{-n} \widetilde{y}^2 = [p, v^2 u^2 q s^{-n}].$$

A virtually identical argument will give equality (2.3b). □

2.3 Galois and Faithfully Flat Cohomology

Later on we will make heavy use of both Galois cohomology and faithfully flat cohomology. We will give a brief introduction of both cohomologies and also explain how to twist quadratic forms with respect to cocycles in each of these cohomologies. We begin with the notion of non-Abelian Galois cohomology. The discussion below is taken from [Se02].

Let G/k be an algebraic group over an arbitrary field, k_s its separable closure and define $\Gamma := \mathrm{Gal}(k_s/k)$. We define the 0-th Galois cohomology set as:

$$H^0(k, G) = G(k).$$

To define the 1st Galois cohomology set we need some preliminary definitions. A *cocycle* is a continuous mapping:

$$\begin{aligned} \zeta \colon \Gamma &\to G(k_s) \\ \sigma &\mapsto (g_\sigma) \end{aligned}$$

such that for all $\sigma, \tau \in \Gamma$, $g_{\sigma\tau} = g_\sigma \sigma(g_\tau)$. In the above definition, continuity means with respect to the profinite topology on Γ and the discrete topology on $G(k_s)$. We denote the set of all cocyles by $Z^1(k, G)$. We say that two cocycles are equivalent and write $(g'_\sigma) \sim (g_\sigma)$ if there exists $x \in G(k_s)$ such that $(g'_\sigma) = x^{-1}(g_\sigma)\sigma(x)$. We can then define the first Galois cohomology set as

$$H^1(k, G) = Z^1(k, G)/\sim .$$

Note that if G is commutative then G induces a natural group structure on $H^1(k, G)$. As well, if we have a k-morphism of algebraic groups $\varphi \colon G \longrightarrow G'$,

it induces a mapping

$$H^1(k, G) \longrightarrow H^1(k, G').$$

Indeed, let $[(g_\sigma)] \in H^1(k, G)$ and by abuse of notation let us write

$$\varphi = \varphi(k_s)\colon G(k_s) \longrightarrow G'(k_s).$$

Then,

$$\varphi(g_\sigma)\sigma(\varphi(g_\tau)) = \varphi(g_\sigma)\varphi(\sigma(g_\tau)) = \varphi(g_\sigma\sigma(g_\tau)) = \varphi(g_{\sigma\tau}).$$

Note that φ commutes with σ, because φ was defined to be a k-morphism and $\sigma \in Gal(k_s/k)$.

We will now present some key results about the first Galois cohomology sets of certain algebraic groups.

Theorem 2.3.1. *We have:*

- $H^1(k, \mathrm{G}_m) = 1$*;*
- $H^1(k, \mathrm{G}_a) = 1$*;*
- $H^1(k, \mu_n) = k^\times/(k^\times)^n$*; and*
- $H^1(k, \mathbb{Z}/p) = k/\wp(k)$*,* $char(k) = p$*,* $\wp(k) = \{x^p - x \mid x \in k\}$.

We will now explain the process of twisting a quadratic form with respect to a Galois cocycle. Let k be an arbitrary field, L/k a field extension and G/k an algebraic group. Assume we have an orthogonal representation $\rho\colon G \to \mathcal{O}(V, q)$ where V is a finite dimensional vector space over k with basis $\{e_1, ..., e_n\}$ and q is a nondegenerate quadratic form on V. The orthogonal representation ρ induces a natural morphism

$$\widetilde{\rho}\colon H^1(L, G) \longrightarrow H^1(L, \mathcal{O}(V, q)), \quad \zeta \mapsto \zeta.$$

It is known that $H^1(L, \mathcal{O}(V, q)) \simeq \{$isomorphism classes of nondegenerate,

n-dimensional quadratic forms$\}$. So to each cocycle ζ in $Z^1(L, \mathcal{O}(V,q))$ we can associate a quadratic form, namely the twisting of q by the cocycle ζ, a process which we describe below.

Let L_s be a separable closure of L and let $\Gamma = \mathrm{Gal}(L_s/L)$. Let $\zeta = (a_\sigma)$. We have $a_\sigma \in \mathcal{O}(V,q)(L_s) \subseteq \mathrm{GL}(V_s)$ where $V_s = V \otimes_L L_s$. We now define two actions of Γ on V_s. Let $v \in V_s$ be arbitrary, and write $v = \sum_{i=1}^n v_i e_i$ where $v_i \in L_s$. Also, let $\gamma \in \Gamma$. Then

$$\gamma \cdot v = \sum_{i=1}^n \gamma(v_i) e_i$$

is called the standard action of the Galois group on V_s. We next define the *twisted action* by

$$\gamma^* \cdot v = a_\gamma \left(\sum_{i=1}^n \gamma(v_i) e_i \right).$$

Note that $a_\gamma \in \mathrm{GL}(V_s)$ and $v \in V_s$ so this action makes sense and one can check easily that the twisted action really is a group action.

Now define

$$W := V_s^{\Gamma^*} = \{ v \in V_s \mid \gamma^* \cdot v = v \ \ \forall \ \ \gamma \in \Gamma \}.$$

One can easily see that W is a k-subspace of V_s. According to Galois descent [Wa, Ch.17] we know $W \otimes_L L_s \simeq V_s$ so it follows that $\dim(V) = \dim(W)$. By assumption we have a quadratic form $q \colon V \to L$ and by scalar extension we get a quadratic form $q_s \colon V_s \to L \otimes_L L_s = L_s$. Let us show that if we restrict q_s to W, then $q_s(W) \subset L$. Indeed, suppose $w \in W$, so we know that $w = \gamma^* \cdot w = a_\gamma(\gamma \cdot w)$. Now, since $a_\gamma \in \mathcal{O}(V,q)(L_s)$ it preserves length, i.e.

$$q_s(w) = q_s(a_\gamma(\gamma \cdot w)) = q_s(\gamma \cdot w).$$

Now since q was defined on a vector space V/k, its coefficients live in k and then so do those of q_s by definition. Because of this, we get q_s commutes

with the Galois action. Thus

$$q_s(w) = q_s(\gamma \cdot w) = \gamma \cdot (q_s(w)).$$

It follows that $q_s(w) \in L_s$ is stable with respect to the Galois action and this implies $q_s(w) \in L$, as was desired.

So we define $p = q_s|_W \colon W \to L$, a quadratic form over L, which we call the twisting of q with respect to the cocycle ζ. We say p is the *twisted form* of q with respect to ζ. So in order to explicitly compute the twisted form p, we need to find a basis for W, that is, a set of $n = \dim(V)$ linearly independent vectors in V_s which are invariant under the twisted action.

We now move on to describing faithfully flat cohomology and twisting with respect to a faithfully flat cocycle. The discussion below is taken from [Wa].

Let G/K be an algebraic group and consider an algebraic closure $\overline{K}$ of K. The *zeroeth faithfully flat cohomology set* is defined as $H^0(K, G) = G(K)$. To describe the first faithfully flat cohomology set we need some preliminary definitions. Consider two natural maps

$$\pi_i \colon \overline{K} \to \overline{K} \otimes \overline{K}, \quad x \longmapsto \begin{cases} x \otimes 1 & i = 1 \\ 1 \otimes x & i = 2 \end{cases}.$$

These give rise to two maps $G(\overline{K}) \to G(\overline{K} \otimes \overline{K})$ which we will call π_1^*, π_2^*. If we fix an embedding $G \hookrightarrow \mathrm{GL}_n$ then one can view elements in $G(\overline{K})$ as matrices and then π_i^* corresponds to applying π_i to each entry of $x \in G(\overline{K}) \subseteq \mathrm{GL}_n(\overline{K})$. For example, if $x = (a_{ij})$, then $\pi_1^*((a_{ij})) = (a_{ij} \otimes 1)$ and $\pi_2^*((a_{ij})) = (1 \otimes a_{ij})$. Further, we can also consider the embeddings

$$s_{12}, s_{13}, s_{23} \colon \overline{K} \otimes \overline{K} \to \overline{K} \otimes \overline{K} \otimes \overline{K}, \quad a \otimes b \mapsto \begin{cases} a \otimes b \otimes 1 & \text{for } s_{12} \\ a \otimes 1 \otimes b & \text{for } s_{13} \\ 1 \otimes a \otimes b & \text{for } s_{23} \end{cases}.$$

These induce 3 maps

$$s_{12}^*, s_{13}^*, s_{23}^* \colon G(\overline{K} \otimes \overline{K}) \longrightarrow G(\overline{K} \otimes \overline{K} \otimes \overline{K}).$$

Then we say that $g \in G(\overline{K} \otimes \overline{K})$ is a *faithfully flat cocycle* if $s_{12}^*(g)s_{23}^*(g) = s_{13}^*(g)$ and denote the set of all cocycles by $Z^1(K, G)$. We can introduce an equivalence relation on cocycles, where $g_1 \sim g_2 \Leftrightarrow \ \exists\ x \in G(\overline{K})$ such that $g_2 = \pi_1^*(x)g_1\pi_2^*(x^{-1})$. Then we define the *first faithfully flat cohomology set* as $H^1(K, G) = Z^1(K, G)/\sim$. It is possible to show that this construction is a generalization of Galois cohomology [Wa, Section 17.7].

Next, suppose G, G_1, G_2 are affine algebraic groups over a field K. Then we explain what it means for the sequence

$$1 \longrightarrow G_1 \xrightarrow{\varphi} G \xrightarrow{\psi} G_2 \longrightarrow 1$$

to be exact in the faithfully flat topology. The definitions of exactness at G_1 and G are as expected. That is, the sequence is exact at G_1 if for every K-algebra R, the induced map $\varphi(R) \colon G_1(R) \to G(R)$ is an injection. The sequence is exact at G if for all K-algebras R one has $\operatorname{Ker}\psi = \operatorname{Im}\phi$. However, exactness at G_2 is a little bit different. We say the sequence is exact at G_2 if for all K-algebras R and $\beta \in G_2(R)$ there is a faithfully flat extension $R \subset S$ and $\alpha \in G(S)$ such that $\psi(\alpha)$ equals the image of β under the induced map $G_2(R) \to G_2(S)$. Recall that an extension of rings $\lambda \colon R \to S$ is called *faithfully flat* if λ is a flat morphism and for any R-module M, $M \otimes_R S = 0 \Rightarrow M = 0$. Note that since K is a field to check exactness at G_2 it suffices to show that $G(\overline{K}) \to G_2(\overline{K})$ is surjective where $\overline{K}$ is an algebraic closure of K.

When the above sequence is exact, it produces a long exact sequence in faithfully flat cohomology:

$$\begin{aligned} &1 \to G_1(K) \to G(K) \to G_2(K) \to H^1(K, G_1) \\ &\to H^1(K, G) \to H^1(K, G_2). \end{aligned}$$

For later use, we would like to describe in detail the connecting morphism $G_2(K) = H^0(K, G_2) \to H^1(K, G_1)$. Let $\alpha \in G_2(K)$. Now over an algebraic closure $\overline{K}$ we have a surjection $G(\overline{K}) \to G_2(\overline{K})$, so let $\widetilde{\alpha}$ be a lifting of α in $G(\overline{K})$. Then it can be shown that if we let $\beta = \pi_1^*(\widetilde{\alpha}) \cdot (\pi_2^*(\widetilde{\alpha}))^{-1}$, not only does β live in $G(\overline{K} \otimes \overline{K})$, it actually takes image in the subgroup $G_1(\overline{K} \otimes \overline{K})$. Moreover, β is a cocycle in the sense of faithfully flat cohomology. Thus the connecting morphism is given by

$$G_2(K) \longrightarrow H^1(K, G_1), \quad \alpha \mapsto \beta = \pi_1^*(\widetilde{\alpha})(\pi_2^*(\widetilde{\alpha}))^{-1}.$$

In general, let G be an algebraic group acting on a finite dimensional K-vector space V with basis $\{e_1, ..., e_n\}$. Let $\alpha \in Z^1(K, G) \subset G(L \otimes L)$ where $L = K(\sqrt{\alpha})$. Suppose further that we have a quadratic form $q \colon V \to K$ and that G preserves it. We will now explain how to twist this form with respect to the cocycle α. We first consider the vector space $V \otimes L = V_L$ and we can naturally extend our quadratic form to this space as seen in Section 2.1. Any $x \in V_L$ can be written as $\sum_{i=1}^{n}(a_i + b_i\sqrt{\alpha})e_i = x$ where $a_i, b_i \in K$.

Now to compute the twisting of q we have to find a basis for

$$Y = {}^{\alpha}V_L := \{x \in V_L \mid \pi_1(x) = \alpha(\pi_2(x))\}.$$

By faithfully flat descent $\dim(Y) = \dim(V) = n$, so it is enough to find n linearly independent elements of V_L which satisfy the given condition. Once we have this we can restrict our form q_L to Y and it is known that such a restriction takes an image not only in L, but more importantly in K. Thus $q_L|_Y$ is a quadratic form over K, called the *twisted form of q with respect to the cocycle α*.

Chapter 3

Killing Forms of Simple Lie Algebras over $\mathbb{Z}$

3.1 Preliminary Results

To construct the required orthogonal representations of the algebraic groups described in Section 1.2 we need to know explicitly how the Killing form $\mathcal{K}$ of Lie algebras of split, simple, simply connected groups defined over a field k looks like. Since our main field has characteristic 2, we begin by computing $\mathcal{K}$ in a Chevalley basis of the Lie algebra $\mathcal{L} = \mathcal{L}(G)$ of a split simple simply connected algebraic group G defined over $\mathbb{Z}$ and then we pass to k by applying the base change $\mathbb{Z} \to \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} \hookrightarrow k$.

Recall that a Chevalley basis is a canonical basis of $\mathcal{L}$ which arises from a decomposition of

$$\mathcal{L} = \mathcal{L}_0 \oplus (\coprod_{\alpha \neq 0} \mathcal{L}_\alpha)$$

into a direct sum of the weight subspaces $\mathcal{L}_\alpha$ with respect to a split maximal toral subalgebra $\mathcal{H} = \mathcal{L}_0 \subset \mathcal{L}$. Note that the set of all nontrivial weights in the above decomposition forms a root system and that for every root α we have $\dim(\mathcal{L}_\alpha) = 1$.

In what follows Φ will denote the set of all roots of $\mathcal{L}$ with respect to $\mathcal{H}$, $\Delta \subset \Phi$ its basis and Φ^+ (resp. Φ^-) positive (resp. negative) roots. By [Hu, Theorem 25.2] there exist elements $\{H_{\alpha_i} |\, \alpha_i \in \Delta\}$ in $\mathcal{H}$ and $X_\alpha \in \mathcal{L}_\alpha,\ \alpha \in \Phi$ such that the set

$$\{H_{\alpha_i} |\, \alpha_i \in \Delta\ \} \cup \{X_\alpha |\, \alpha \in \Phi^+\} \cup \{X_{-\alpha} |\, \alpha \in \Phi^+\}$$

forms a basis for $\mathcal{L}$, known as a *Chevalley basis*, and these generators are subject to the following relations:

- $[H_{\alpha_i}, H_{\alpha_j}] = 0$;
- $[H_{\alpha_i}, X_\alpha] = \langle \alpha, \alpha_i \rangle X_\alpha$;
- $H_\alpha := [X_\alpha, X_{-\alpha}] = \sum_{\alpha_i \in \Delta} n_i H_{\alpha_i}$ where $n_i \in \mathbb{Z}$; and
- $[X_\alpha, X_\beta] = \begin{cases} 0 & \text{if } \alpha + \beta \notin \Phi \\ \pm(p+1) X_{\alpha+\beta} & \text{otherwise} \end{cases}$,

  where p is the greatest positive integer such that $\alpha - p\beta \in \Phi$.

Here for two arbitrary roots $\alpha, \beta \in \Phi$ the scalar $\langle \alpha, \beta \rangle$ is given by

$$\langle \alpha, \beta \rangle = \frac{2(\alpha, \beta)}{(\beta, \beta)}\ ,$$

where $(-,-)$ denotes the standard inner product on the root lattice. It is in this Chevalley basis that we will compute the Killing form $\mathcal{K}$ of $\mathcal{L}$.

Recall that for any $X, Y \in \mathcal{L}$ one has

$$\mathcal{K}(X, Y) = \mathrm{Tr}(\mathrm{ad}(X) \circ \mathrm{ad}(Y))\ ,$$

where $\mathrm{ad}\colon \mathcal{L} \to \mathrm{End}(\mathcal{L})$ is the adjoint representation of $\mathcal{L}$ and it is straightforward to check that

$$\mathcal{K}(H_{\alpha_i}, X_\alpha) = 0,\ \mathcal{K}(X_\alpha, X_\beta) = 0$$

for all i and all roots $\alpha, \beta \in \Phi$ such that $\alpha + \beta \neq 0$; in particular,

$\mathcal{K}(X_\alpha, X_\alpha) = 0$. Thus as a vector space $\mathcal{L}$ is decomposed into an orthogonal sum of subspaces $\mathcal{H}$ and $\langle X_\alpha, X_{-\alpha} \rangle$, $\alpha \in \Phi^+$. Before proceeding with the computation we require some more preliminary results. The most important of these is [Ma, Lemma 3.4.2] which we state below:

Lemma 3.1.1. *Let $\mathcal{L}$ be as above with a Chevalley basis*

$$\{H_{\alpha_i} |\, \alpha_i \in \Delta\} \cup \{X_\alpha |\, \alpha \in \Phi^+\} \cup \{X_{-\alpha} |\, \alpha \in \Phi^+\}.$$

The restriction $\mathcal{K}|_{\mathcal{L}_\alpha \oplus \mathcal{L}_{-\alpha}}$ is of the form $m_\alpha xy$ where m_α is an integer and

$$\mathcal{K}(H_{\alpha_i}, H_{\alpha_j}) = 2\check{h}(\check{\alpha}_i, \check{\alpha}_j) \ ,$$

where $\check{h}$ is the dual Coxeter number of $\mathcal{L}$, $\check{\alpha}_i = \frac{2\alpha_i}{(\alpha_i, \alpha_i)}$ and $(\check{\alpha}, \check{\beta})$ is the Weyl-invariant inner product with $(\check{\alpha}, \check{\alpha}) = 2$ for a long root α.

Note that the formula given by Lemma 3.1.1 requires $(\check{\alpha}, \check{\alpha}) = 2$ for a long root α. As will be seen, for groups of type C_n and G_2 we will have to multiply the standard inner product by an appropriate scalar to match this condition. We will also make use of some results due to Steinberg and Springer [SpSt]. The first of these is that for any long root $\alpha \in \Phi$ we have

$$\mathcal{K}(H_\alpha, H_\alpha) = \mathrm{Tr}(\mathrm{ad}(H_\alpha) \circ \mathrm{ad}(H_\alpha)) = 4\check{h} \ , \tag{3.1}$$

where $\check{h}$ is the dual Coxeter number of the given Lie algebra. They also showed that for any root $\alpha \in \Phi$ we have

$$\mathcal{K}(X_\alpha, X_{-\alpha}) = \mathrm{Tr}(\mathrm{ad}(X_\alpha) \circ \mathrm{ad}(X_{-\alpha})) = \frac{1}{2}\mathrm{Tr}(\mathrm{ad}(H_\alpha) \circ \mathrm{ad}(H_\alpha)). \tag{3.2}$$

Combining these results we see that to compute the Killing form of $\mathcal{L}$ we really only need to know how this form looks on the Cartan subalgebra $\mathcal{H}$. On each subspace $\mathcal{L}_\alpha \oplus \mathcal{L}_{-\alpha}$, Lemma 3.1.1 tells us that the Killing form is of the form $m_\alpha xy$. Then, the coefficient m_α of this binary quadratic form can be determined by equation (3.2) if we know the Killing form on the Cartan subalgebra. Further, for each long root α we know by equation (3.1) that

$\mathcal{K}(H_\alpha, H_\alpha) = 4\check{h}$. Similarly, by using the formula given in Lemma 3.1.1 and the fact that the Killing form is W-invariant, where W is the corresponding Weyl group, we see that $\mathcal{K}(H_\beta, H_\beta)$ is a constant value for all short roots β, but this value will depend on the type of Φ.

Also, again using the formula in Lemma 3.1.1, we see that if $\alpha_i, \alpha_j \in \Delta \subset \Phi$ are non adjacent roots, then

$$\mathcal{K}(H_{\alpha_i}, H_{\alpha_j}) = \mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_j})) = 0.$$

Indeed this is equivalent to saying that $(\alpha_i, \alpha_j) = 0$ which is true for non adjacent roots.

We will make use of the explicit description of the root systems found in [Bo02] to help us with the computations needed to determine the Killing forms. In all of these explicit descriptions we make the convention that ϵ_i denotes the vector in $\mathbb{R}^n$ with a 1 in the ith position and 0s elsewhere. We now proceed with the computation of the Killing forms of simple Lie algebras.

3.2 Type A_n

The basis of the root system is given by:

$$\alpha_i = \epsilon_i - \epsilon_{i+1} \quad \text{for all} \quad i = 1, ..., n.$$

Then we have:

$$\begin{aligned}
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_i})) &= 4\check{h} \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_{i+1}})) &= 2\check{h}\left(\frac{2(\epsilon_i - \epsilon_{i+1})}{(\epsilon_i - \epsilon_{i+1}, \epsilon_i - \epsilon_{i+1})}, \frac{2(\epsilon_{i+1} - \epsilon_{i+2})}{(\epsilon_{i+1} - \epsilon_{i+2}, \epsilon_{i+1} - \epsilon_{i+2})}\right) \\
&= 2\check{h}\left(\frac{2(\epsilon_i - \epsilon_{i+1})}{2}, \frac{2(\epsilon_{i+1}, \epsilon_{i+2})}{2}\right) = 2\check{h}(\epsilon_i - \epsilon_{i+1}, \epsilon_{i+1} - \epsilon_{i+2}) \\
&= -2\check{h}
\end{aligned}$$

Thus we can conclude that the Killing form $\mathcal{K}$ restricted to the Cartan subalgebra $\mathcal{H}$ of the Lie algebra $\mathcal{L}$ of type A_n is of the form:

$$\mathcal{K}|_{\mathcal{H}} = 4\check{h}\left(\sum_{i=1}^{n} x_i^2\right) - 4\check{h}\left(\sum_{i=1}^{n-1} x_i x_{i+1}\right).$$

Therefore it follows that the Killing form on all of $\mathcal{L}$ is:

$$\mathcal{K} = \mathcal{K}|_{\mathcal{H}} + 4\check{h}\left(\sum_{|\Phi^+|} y_i y_{i+1}\right).$$

This is because for each positive root $\alpha \in \Phi^+$ we know that $\mathcal{K}$ restricted to the 2-dimensional subspace $\mathcal{L}_\alpha \oplus \mathcal{L}_{-\alpha}$ is of the form $m_\alpha y_i y_{i+1}$. Since all roots have the same length it follows from equation (3.2) that

$$\mathrm{Tr}(\mathrm{ad}(X_\alpha) \circ \mathrm{ad}(X_{-\alpha})) = \frac{1}{2}\mathrm{Tr}(\mathrm{ad}(H_\alpha) \circ \mathrm{ad}(H_\alpha)) = \frac{1}{2} \cdot 4\check{h} = 2\check{h}.$$

The coefficient m_α is then 2 times this number, or $2 \cdot 2\check{h} = 4\check{h}$, which is precisely the number that appears above.

To pass to the main field k we first modify $\mathcal{K}$ by dividing all coefficients of $\mathcal{K}$ by $4\check{h}$. After doing so our modified Killing form (still denoted by $\mathcal{K}$) becomes

$$\mathcal{K} = \sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n-1} x_i x_{i+1} + \sum_{|\Phi^+|} y_i y_{i+1}.$$

Passing from $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, which is a field of characteristic 2, we finally would like to "diagonalize" our form. Recall that (unlike in fields of characteristic not 2) it is not true that every quadratic form is diagonalizable over a field of characteristic 2. However, we saw in Lemma 2.1.4 that we have an analog of diagonalization and using this we would like to write the above form $\mathcal{K}$ in a similar way.

Lemma 3.2.1. *We have*

$$\mathcal{K} \simeq \bigoplus_{i=1}^{(n-1)/2} [0,0] \oplus \langle c \rangle \oplus \bigoplus_{|\Phi^+|} [0,0], \text{ if } n \text{ is odd; } c \in \{0,1\}$$

and

$$\mathcal{K} \simeq \bigoplus_{i=1}^{(n-1)/2} [0,0] \oplus \bigoplus_{|\Phi^+|} [0,0], \text{ if } n \text{ is even}$$

Before proving this assertion we make the following trivial observation. For the part of the Killing form outside of the Cartan subalgebra it is obvious that it is a direct sum of hyperbolic planes, so is of the shape $\bigoplus [0,0]$. Therefore, to prove the above result and a similar result for all subsequent simple Lie algebras, it is enough to provide a "diagonalization" for the restriction of the Killing form to the Cartan subalgebra.

Also, recall in Section 2.1 we observed that over an algebraically closed field $[a,b] \simeq [0,0]$ for arbitrary a, b. In the proof of Lemma 3.2.1, binary quadratic forms of the shape $[1,0], [0,1]$ and $[1,1]$ will appear, but using the observation from Section 2.1 we can immediately conclude these forms are isometric to $[0,0]$ over k. To avoid excessive explanation in the proof of Lemma 3.2.1 and in the computation of Killing forms for all subsequent types, we will not repeat this result each time. Just always keep in mind that if we have a quadratic form of the shape

$$\bigoplus_{i=1}^{n} [a_i, b_i] \quad \text{or} \quad \bigoplus_{i=1}^{n} [a_i, b_i] \oplus \langle c \rangle$$

then, by this observation, they are (respectively) automatically isometric to

$$\bigoplus_{i=1}^{n} [0,0] \quad \text{or} \quad \bigoplus_{i=1}^{n} [0,0] \oplus \langle c \rangle.$$

Proof. We will proceed by induction on odd and then even rank n. First we explicitly compute the Killing form restricted to the Cartan subalgebra for types A_1 to A_5.

- A_1**:** $x_1^2 \simeq \langle 1 \rangle$;
- A_2**:** $x_1^2 + x_1x_2 + x_2^2 \simeq [1,1]$;
- A_3**:** $x_1^2+x_1x_2+x_2^2+x_2x_3+x_3^2 = x_2^2+x_2(x_1+x_3)+(x_1+x_3)^2 \simeq [1,1]\oplus\langle 0\rangle$;
- A_4**:** $x_1^2 + x_1x_2 + x_2^2 + x_2x_3 + x_3^2 + x_3x_4 + x_4^2 = (x_2^2 + x_2(x_1 + x_3) + (x_1 + x_3)^2) + (x_4^2 + x_3x_4) \simeq [1,1] \oplus [1,0]$; and
- A_5**:** $x_1^2 + x_1x_2 + x_2^2 + x_2x_3 + x_3^2 + x_3x_4 + x_4^2 + x_4x_5 + x_5^2 = (x_2^2 + x_2(x_1 + x_3)+(x_1+x_3)^2)+(x_4^2+x_4(x_3+x_5)+(x_3+x_5)^2)+x_3^2 \simeq [1,1]\oplus[1,1]\oplus\langle 1\rangle$.

Case A_{2n+1}. We proceed by induction on n. We know that the Killing form restricted to the Cartan subalgebra is

$\sum_{i-1}^{2n+1} x_i^2 + \sum_{i=1}^{2n} x_ix_{i+1} =$
$x_1^2 + x_1x_2 + x_2^2 + x_2x_3 + x_3^2 + x_3x_4 + x_4^2 + x_4x_5 + (\sum_{i=5}^{2n+1} x_i^2 + \sum_{i=5}^{2n} x_ix_{i+1}) =$
$(x_2^2 + x_2(x_1 + x_3) + (x_1 + x_3)^2) + (x_3x_4 + x_4^2 + x_4x_5)+$
$(\sum_{i=5}^{2n+1} x_i^2 + \sum_{i=5}^{2n} x_ix_{i+1})$.

Note that $(\sum_{i=5}^{2n+1} x_i^2 + \sum_{i=5}^{2n} x_ix_{i+1})$ is the Killing form of the Lie algebra of type $A_{2n+1-4} = A_{2n-3}$ restricted to the Cartan subalgebra, so by induction is of the required form. The remaining terms $(x_2^2+x_2(x_1+x_3)+(x_1+x_3)^2)+$ $(x_3x_4 + x_4^2 + x_4x_5)$ are isometric to $[1,1] \oplus [1,0]$, so the claim is proven.

The case of even rank A_{2n} follows by using an identical argument as in the odd case. □

3.3 Type B_n

As mentioned at the end of Chapter 2, we will not use the Killing form to get an orthogonal representation for groups of type B_n, but we inlcude its computation for completeness.

The basis of the root system is given by

$$\alpha_i = \epsilon_i - \epsilon_{i+1} \ \forall \ i = 1, ..., n-1; \ and$$
$$\alpha_n = \epsilon_n.$$

So here $\alpha_1, ..., \alpha_{n-1}$ are long roots and α_n is a short root. Note that for the standard bilinear form on the root lattice one has $(\check{\alpha}, \check{\alpha}) = 2$ for any long root α. Then we compute:

$$\begin{aligned}
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_i})) &= 4\check{h} \quad \forall \ i = 1, ..., n-1; \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_n}) \circ \mathrm{ad}(H_{\alpha_n})) &= 2\check{h}\left(\frac{2\epsilon_n}{(\epsilon_n, \epsilon_n)}, \frac{2\epsilon_n}{(\epsilon_n, \epsilon_n)}\right) = 2\check{h}(2\epsilon_n, 2\epsilon_n) = 8\check{h}; \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_{i+1}})) &= -2\check{h} \ \forall \ i = 1, ..., n-2 \text{ (identical to computation in Section 3.2)}; \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_{n-1}}) \circ \mathrm{ad}(H_{\alpha_n})) &= 2\check{h}\left(\frac{2(\epsilon_{n-1} - \epsilon_n)}{2}, \frac{2\epsilon_n}{1}\right) = -4\check{h}.
\end{aligned}$$

Thus we can conclude that the Killing form $\mathcal{K}$ restricted to the Cartan subalgebra $\mathcal{H}$ of B_n is of the form

$$\mathcal{K}|_{\mathcal{H}} = 4\check{h}\left(\sum_{i=1}^{n-1} x_i^2\right) + 8\check{h}x_n^2 - 4\check{h}\left(\sum_{i=1}^{n-2} x_i x_{i+1}\right) - 8\check{h}x_{n-1}x_n.$$

Therefore it follows that the Killing form on all of B_n is:

$$\mathcal{K} = \mathcal{K}|_{\mathcal{H}} + 4\check{h}\left(\sum_{|\Phi^+_{long}|} y_i y_{i+1}\right) + 8\check{h}\left(\sum_{|\Phi^+_{short}|} z_i z_{i+1}\right).$$

Each $y_i y_{i+1}$ corresponds to the restriction of the Killing form to the two

dimensional subalgebra $\mathcal{L}_\alpha \oplus \mathcal{L}_{-\alpha}$ where α is a long root. The coefficient appearing in front of the $y_i y_{i+1}$ was computed in the exact same way as in Section 3.2, i.e. by employing equation (3.2). The coefficient appearing in front of the $z_i z_{i+1}$ is computed similarly; namely, it was noted in Section 3.1 that $\mathrm{Tr}(\mathrm{ad}(H_\beta) \circ \mathrm{ad}(H_\beta))$ was constant for all short roots β. In the B_n case this constant value is $8\check{h} = \mathrm{Tr}(\mathrm{ad}(H_{\alpha_n}) \circ \mathrm{ad}(H_{\alpha_n}))$ because α_n is a short root. Then, in the same way we did for long roots, we make use of equation (3.2) to conclude that this is the coefficient appearing in front of the restriction to the Killing form on $\mathcal{L}_\beta \oplus \mathcal{L}_{-\beta}$ where β is a short root.

As we did for the Killing form on A_n, we can modify this form by dividing out by the highest power appearing in all terms, which once again is $4\check{h}$. After doing so and passing to $\mathbb{Z}/2\mathbb{Z}$ we get

$$\begin{aligned}\mathcal{K} &= \left(\sum_{i=1}^{n-1} x_i^2\right) - \left(\sum_{i=1}^{n-2} x_i x_{i+1}\right) + \left(\sum_{|\Phi^+_{long}|} y_i y_{i+1}\right) \\ &\quad + 2\left(x_n^2 - x_{n-1}x_n + \sum_{|\Phi^+_{short}|} z_i z_{i+1}\right) \\ &= \left(\sum_{i=1}^{n-1} x_i^2\right) - \left(\sum_{i=1}^{n-2} x_i x_{i+1}\right) + \left(\sum_{|\Phi^+_{long}|} y_i y_{i+1}\right) + m * \langle\, 0 \,\rangle.\end{aligned}$$

where $m = 2|\Phi^+_{short}| + 1$. We would now like to "diagonalize" our Killing form as we did for A_n. As noted in that computation, all we need to do is to "diagonalize" the restriction of the Killing form to the Cartan subalgebra. After simplification the Killing form restricted to the Cartan subalgebra of B_n is

$$\mathcal{K}|_{\mathcal{H}} = \left(\sum_{i=1}^{n-1} x_i^2\right) - \left(\sum_{i=1}^{n-2} x_i x_{i+1}\right) + \langle\, 0 \,\rangle,$$

which is clearly isometric to the Killing form restricted to the Cartan subalgebra of type A_{n-1}. So the next result follows immediately from the proof of Lemma 3.2.1.

Lemma 3.3.1. *We have*

$$\mathcal{K} \simeq \bigoplus_{i=1}^{(n-2)/2} [0,0] \oplus \bigoplus_{|\Phi^+_{long}|} [0,0] \oplus \langle c \rangle \oplus m\langle 0 \rangle, \text{ if } n \text{ is even; } c \in \{0,1\}$$

and

$$\mathcal{K} \simeq \bigoplus_{i=1}^{(n-1)/2} [0,0] \oplus \bigoplus_{|\Phi^+_{long}|} [0,0] \oplus m\langle 0 \rangle, \text{ if } n \text{ is odd,}$$

where $m = 2|\Phi^+_{short}| + 1$.

3.4 Type C_n

The basis of the root system is given by

$$\alpha_i = \epsilon_i - \epsilon_{i+1} \ \forall \ i = 1, ..., n-1; \text{ and}$$
$$\alpha_n = 2\epsilon_n.$$

So here $\alpha_1, ..., \alpha_{n-1}$ are short roots and α_n is a long root. Note that for α_n we have

$$\check{\alpha}_n = \frac{2(2\epsilon_n)}{(2\epsilon_n, 2\epsilon_n)} = \frac{4\epsilon_n}{4} = \epsilon_n$$

and so we get $(\check{\alpha}_n, \check{\alpha}_n) = (\epsilon_n, \epsilon_n) = 1$. However, in order to apply the Theorems of Section 3.1, we need this value to be 2. In order to achieve this we will consider the standard inner product multiplied by $\frac{1}{2}$. If we do this we get

$$\check{\alpha}_n = \frac{2(2\epsilon_n)}{(2\epsilon_n, 2\epsilon_n)} = \frac{4\epsilon_n}{4 * \frac{1}{2}} = 2\epsilon_n$$

and it follows $(\check{\alpha}_n, \check{\alpha}_n) = (2\epsilon_n, 2\epsilon_n) = 4 * \frac{1}{2} = 2$, as desired. So using this modified inner product we compute:

$$\begin{aligned}
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_i})) &= 2\check{h}\left(\frac{2(\epsilon_i - \epsilon_{i+1})}{(\epsilon_i - \epsilon_{i+1}, \epsilon_i - \epsilon_{i+1})}, \frac{2(\epsilon_i - \epsilon_{i+1})}{(\epsilon_i - \epsilon_{i+1}, \epsilon_i - \epsilon_{i+1})}\right) \\
&= 2\check{h}\left(\frac{2(\epsilon_i - \epsilon_{i+1})}{2 * \frac{1}{2}}, \frac{2(\epsilon_i - \epsilon_{i+1})}{2 * \frac{1}{2}}\right) \\
&= 8\check{h}(\epsilon_i - \epsilon_{i+1}, \epsilon_i - \epsilon_{i+1}) = 8\check{h} \ \ \forall \ i = 1, ..., n-1 \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_n}) \circ \mathrm{ad}(H_{\alpha_n})) &= 4\check{h} \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_{i+1}})) &= 2\check{h}(2(\epsilon_i - \epsilon_{i+1}), 2(\epsilon_{i+1} - \epsilon_{i+2})) \\
&= 8\check{h}(\epsilon_i - \epsilon_{i+1}, \epsilon_{i+1} - \epsilon_{i+2}) \\
&= -4\check{h} \ \ \forall \ i = 1, ..., n-2 \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_{n-1}}) \circ \mathrm{ad}(H_{\alpha_n})) &= 2\check{h}(2(\epsilon_{n-1} - \epsilon_n), 2\epsilon_n) = 8\check{h}(\epsilon_{n-1} - \epsilon_n, \epsilon_n) = -4\check{h}
\end{aligned}$$

We can now conclude that the Killing form $\mathcal{K}$ restricted to the Cartan subalgebra $\mathcal{H}$ of C_n is of the form

$$\mathcal{K}|_{\mathcal{H}} = 8\check{h}\left(\sum_{i=1}^{n-1} x_i^2 - \sum_{i=1}^{n-1} x_i x_{i+1}\right) + 4\check{h}\, x_n^2 \,.$$

Therefore, arguing as in Section 3.3, we get that the Killing form on all of C_n is:

$$\mathcal{K} = \mathcal{K}|_{\mathcal{H}} + 8\check{h}\left(\sum_{|\Phi^+_{short}|} y_i y_{i+1}\right) + 4\check{h}\left(\sum_{|\Phi^+_{long}|} z_i z_{i+1}\right) \,.$$

Again, after dividing it by $4\check{h}$ our Killing form becomes

$$\mathcal{K} = x_n^2 + \sum_{|\Phi^+_{long}|} z_i z_{i+1} + m * 0.$$

where $m = (n-1) + 2|\Phi^+_{short}|$. Then, the "diagonalization" of this form is obvious. We summarize it in the following Lemma:

Lemma 3.4.1. *We have*

$$\mathcal{K} \simeq \langle 1 \rangle \oplus \bigoplus_{|\Phi^+_{long}|} [0,0] \oplus m\langle 0 \rangle.$$

3.5 Type D_n

The basis of the root system is given by

$$\begin{aligned} &\alpha_i = \epsilon_i - \epsilon_{i+1} \ \forall \ i = 1, 2, ..., n-1; \ \textit{and} \\ &\alpha_n = \epsilon_{n-1} + \epsilon_n. \end{aligned}$$

Note that α_{n-2} is adjacent to α_n, but α_{n-1} is not. Then we compute:

$$\begin{aligned} \mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_i})) &= 4\check{h} \ \ \forall \ i = 1, ..., n; \\ \mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_{i+1}})) &= -2\check{h} \ \forall \ i = 1, ..., n-2 \text{ (identical to computation in Section 3.2);} \\ \mathrm{Tr}(\mathrm{ad}(H_{\alpha_{n-2}}) \circ \mathrm{ad}(H_{\alpha_n})) &= 2\check{h}(\epsilon_{n-2} - \epsilon_{n-1}, \epsilon_{n-1} + \epsilon_n) = -2\check{h}. \end{aligned}$$

Thus we may conclude that the Killing form $\mathcal{K}$ restricted to the Cartan subalgebra $\mathcal{H}$ of D_n is of the form:

$$\mathcal{K}|_{\mathcal{H}} = 4\check{h} \left(\sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n-2} x_i x_{i+1} - x_{n-2} x_n \right).$$

Therefore, arguing as in Section 3.2, we get that the Killing form on all of D_n is:

$$\mathcal{K} = \mathcal{K}|_{\mathcal{H}} + 4\check{h} \left(\sum_{|\Phi^+|} y_i y_{i+1} \right).$$

As before, after dividing this form by $4\check{h}$ it becomes

$$\mathcal{K} = \sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n-2} x_i x_{i+1} - x_{n-2} x_n + \sum_{|\Phi^+|} y_i y_{i+1}.$$

Passing to $\mathbb{Z}/2\mathbb{Z}$ we would like to "diagonalize" this form as we did in previous Sections.

Lemma 3.5.1. *We have*

$$\mathcal{K} \simeq \bigoplus_{i=1}^{(n-1)/2} [0,0] \oplus \langle 0 \rangle \oplus \bigoplus_{|\Phi^+|} [0,0], \text{ if } n \text{ is odd;}$$

and

$$\mathcal{K} \simeq \bigoplus_{i=1}^{(n-2)/2} [0,0] \oplus \langle c_1 \rangle \oplus \langle c_2 \rangle \oplus \bigoplus_{|\Phi^+|} [0,0], \text{ if } n \text{ is even; } c_1, c_2 \in \{0,1\}.$$

where one of c_1 or c_2 equals 0.

Proof. As discussed in the proof of Lemma 3.2.1 it is enough to see what happens to $\mathcal{K}|_{\mathcal{H}}$. For this we will proceed by induction on rank, but first we need explicit computations for some small values of n.

- D_3: $x_1^2+x_2^2+x_3^2+x_1x_3+x_1x_2 = x_1^2+x_1(x_2+x_3)+(x_2+x_3)^2 \simeq [1,1]\oplus\langle 0\rangle$;
- D_4: $x_1^2 + x_1x_2 + x_2^2 + x_2x_3 + x_3^2 + x_2x_4 + x_4^2 = x_2^2 + x_2(x_1 + x_3 + x_4) + (x_1 + x_3 + x_4)^2 \simeq [1,1] \oplus \langle 0\rangle \oplus \langle 0\rangle$;
- D_5: $x_1^2 + x_1x_2 + x_2^2 + x_2x_3 + x_3^2 + x_3x_4 + x_4^2 + x_3x_5 + x_5^2 = (x_1^2 + x_1x_2) + (x_3^2 + x_3(x_2 + x_4 + x_5) + (x_2 + x_4 + x_5)^2) \simeq [1,0] \oplus [1,1] \oplus \langle 0\rangle$; and
- D_6: $x_1^2 + x_1x_2 + x_2^2 + x_2x_3 + x_3^2 + x_3x_4 + x_4^2 + x_4x_5 + x_5^2 + x_4x_6 + x_6^2 = (x_2^2 + x_2(x_1 + x_3) + (x_1 + x_3)^2) + (x_4^2 + x_4(x_3 + x_5 + x_6) + (x_3 + x_5 + x_6)^2) + x_3^2 \simeq [1,1] \oplus [1,1] \oplus \langle 1\rangle \oplus \langle 0\rangle$.

We first assume that $n = 2k + 1$ is odd and proceed by induction on k. We know that on D_{2k+1} the Killing form restricted to the Cartan subalgebra is

$$\begin{aligned}
\mathcal{K}|_{\mathcal{H}} &= \sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n-2} x_i x_{i+1} - x_{n-2}x_n \\
&= x_1^2 + x_1x_2 + x_2^2 + x_2x_3 + x_3^2 + x_3x_4 + x_4^2 + x_4x_5 + \\
&\left(\sum_{i=5}^{n} x_i^2 - \sum_{i=5}^{n-2} x_i x_{i+1} - x_{n-2}x_n\right) \\
&= (x_2^2 + x_2(x_1+x_3) + (x_1+x_3)^2) + (x_4^2 + x_4(x_3+x_5)) + \\
&\left(\sum_{i=5}^{n} x_i^2 - \sum_{i=5}^{n-2} x_i x_{i+1} - x_{n-2}x_n\right).
\end{aligned}$$

Then note

$$(x_2^2 + x_2(x_1+x_3) + (x_1+x_3)^2) + (x_4^2 + x_4(x_3+x_5)) \simeq [1,1] \oplus [1,0]$$

and the remaining terms

$$\left(\sum_{i=5}^{n} x_i^2 - \sum_{i=5}^{n-2} x_i x_{i+1} - x_{n-2}x_n\right)$$

give the Killing form restricted to the Cartan subalgebra of $D_{2k+1-4} = D_{2k-3}$, which by induction has the desired form. Thus, the result follows.

The case of even $n = 2k$ can be treated in exactly the same way and so we omit this portion of the proof. □

3.6 Type E_6, E_7, E_8

Type E_6 A basis for the root system is given by

$$\begin{aligned}
\alpha_1 &= \frac{1}{2}(\epsilon_1 - \epsilon_2 - \epsilon_3 - \epsilon_4 - \epsilon_5 - \epsilon_6 - \epsilon_7 + \epsilon_8);\\
\alpha_2 &= \epsilon_1 + \epsilon_2;\\
\alpha_3 &= \epsilon_2 - \epsilon_1;\\
\alpha_4 &= \epsilon_3 - \epsilon_2;\\
\alpha_5 &= \epsilon_4 - \epsilon_3;\ \textit{and}\\
\alpha_6 &= \epsilon_5 - \epsilon_4.
\end{aligned}$$

We have

$$(\alpha_i, \alpha_j) = \begin{cases} 2 & \text{if } i = j \\ -1 & \text{if } \alpha_i, \alpha_j \text{ are adjacent} \\ 0 & \text{otherwise} \end{cases}.$$

Note that α_i, α_j are adjacent for the pairs $(i,j) = (1,3), (2,4), (3,4), (4,5), (5,6)$. Now again using the formula in Lemma 3.1.1 it is easy to see that

$$\begin{aligned}
&\mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_i})) = 4\check{h} \ \ \forall\ i = 1, ..., 6\\
&\mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_j})) = -2\check{h} \text{ for all adjacent } \alpha_i, \alpha_j
\end{aligned}$$

Thus the Killing form of E_6 restricted to the Cartan subalgebra $\mathcal{H}$ is:

$$\mathcal{K}|_{\mathcal{H}} = 4\check{h}\left(\sum_{i=1}^{6} x_i^2 - x_1x_3 - x_2x_4 - x_3x_4 - x_4x_5 - x_5x_6\right).$$

It follows then that the Killing form for E_6 is:

$$\mathcal{K} = \mathcal{K}|_{\mathcal{H}} + 4\check{h}\left(\sum_{|\Phi^+|} y_i y_{i+1}\right).$$

We can simplify this form by dividing through by $4\check{h}$. Doing so we get

$$\mathcal{K} = \sum_{i=1}^{6} x_i^2 - x_1x_3 - x_2x_4 - x_3x_4 - x_4x_5 - x_5x_6 + \sum_{|\Phi^+|} y_iy_{i+1}.$$

Now we would like to "diagonalize" this form. As before, it is enough to do so for the part related to the Cartan subalgebra. We have

$$\begin{aligned}\mathcal{K}|_{\mathcal{H}} &= \sum_{i=1}^{6} x_i^2 + x_1x_3 + x_2x_4 + x_3x_4 + x_4x_5 + x_5x_6 \\ &= (x_3^2 + x_3(x_1 + x_4) + (x_1 + x_4)^2) + (x_5^2 + x_5(x_4 + x_6) \\ &+ (x_4 + x_6)^2) + (x_2^2 + x_2x_4).\end{aligned}$$

Now consider the linear change of variables

$$\tilde{x}_1 = x_1 + x_4, \tilde{x}_2 = x_2, \tilde{x}_3 = x_3, \tilde{x}_4 = x_4, \tilde{x}_5 = x_5, \tilde{x}_6 = x_4 + x_6.$$

After this change our form becomes

$$(\tilde{x}_3^2 + \tilde{x}_3\tilde{x}_1 + \tilde{x}_1^2) + (\tilde{x}_5^2 + \tilde{x}_5\tilde{x}_6 + \tilde{x}_6^2) + (\tilde{x}_2^2 + \tilde{x}_2\tilde{x}_4),$$

which is clearly isometric to $[1,1] \oplus [1,1] \oplus [1,0]$. Thus the "diagonalization" of our simplified Killing form on E_6 is

$$\begin{aligned}\mathcal{K} &= [1,1] \oplus [1,1] \oplus [1,0] \oplus \bigoplus_{|\Phi^+|} [0,0] \\ &\simeq [0,0] \oplus [0,0] \oplus [0,0] \oplus \bigoplus_{|\Phi^+|} [0,0].\end{aligned}$$

Type E_7 A basis for the root system is the same as for E_6 along with the following additional vector:

$$\alpha_7 = \epsilon_6 - \epsilon_5.$$

Then,

$$(\alpha_i, \alpha_7) = \begin{cases} 0 & \text{if } i = 1,2,3,4,5 \\ -1 & \text{if } i = 6 \\ 2 & \text{if } i = 7 \end{cases}.$$

and hence

$$\begin{aligned} \mathrm{Tr}(\mathrm{ad}(H_{\alpha_7}) \circ \mathrm{ad}(H_{\alpha_7})) &= 4\check{h} \\ \mathrm{Tr}(\mathrm{ad}(H_{\alpha_6}) \circ \mathrm{ad}(H_{\alpha_7})) &= -2\check{h} \end{aligned}$$

Thus the Killing form of E_7 restricted to the Cartan subalgebra $\mathcal{H}$ is:

$$\mathcal{K}|_{\mathcal{H}} = 4\check{h}\left(\sum_{i=1}^{7} x_i^2 - x_1x_3 - x_2x_4 - x_3x_4 - x_4x_5 - x_5x_6 - x_6x_7\right).$$

It follows then that the Killing form for E_7 is:

$$\mathcal{K} = \mathcal{K}|_{\mathcal{H}} + 4\check{h}\left(\sum_{|\Phi^+|} y_i y_{i+1}\right).$$

We can simplify this form by dividing through by $4\check{h}$. Doing so we get

$$\mathcal{K} = \sum_{i=1}^{7} x_i^2 - x_1x_3 - x_2x_4 - x_3x_4 - x_4x_5 - x_5x_6 - x_6x_7 + \sum_{|\Phi^+|} y_i y_{i+1}.$$

Now we would like to "diagonalize" this form. As before, it is enough to do so for the part related to the Cartan subalgebra. We have

$$\begin{aligned} \mathcal{K}|_{\mathcal{H}} &= \sum_{i=1}^{7} x_i^2 + x_1x_3 + x_2x_4 + x_3x_4 + x_4x_5 + x_5x_6 + x_6x_7 \\ &= (x_4^2 + x_4(x_2 + x_3) + (x_2 + x_3)^2) + (x_6^2 + x_6(x_5 + x_7) \\ &+ (x_5 + x_7)^2) + (x_1^2 + x_1x_3) + (x_4x_5). \end{aligned}$$

Now consider the linear change of variables

$$\tilde{x}_1 = x_1, \tilde{x}_2 = x_2 + x_3, \tilde{x}_3 = x_3, \tilde{x}_4 = x_4, \tilde{x}_5 = x_5, \tilde{x}_6 = x_6, \tilde{x}_7 = x_5 + x_7.$$

After this change our form becomes

$$\begin{aligned}
&= (\tilde{x}_4^2 + \tilde{x}_4\tilde{x}_2 + \tilde{x}_2^2) + (\tilde{x}_6^2 + \tilde{x}_6\tilde{x}_7 + \tilde{x}_7^2) + (\tilde{x}_1^2 + \tilde{x}_1\tilde{x}_3) + (\tilde{x}_4\tilde{x}_5) \\
&= (\tilde{x}_4^2 + \tilde{x}_4(\tilde{x}_2 + \tilde{x}_5) + (\tilde{x}_2 + \tilde{x}_5)^2) + (\tilde{x}_6^2 + \tilde{x}_6\tilde{x}_7 + \tilde{x}_7^2) + (\tilde{x}_1^2 + \tilde{x}_1\tilde{x}_3) + \tilde{x}_5^2 \\
&\simeq [1,1] \oplus [1,1] \oplus [1,0] \oplus \langle 1 \rangle.
\end{aligned}$$

Thus the "diagonalization" of our simplified Killing form on E_7 is

$$\begin{aligned}
\mathcal{K} &= [1,1] \oplus [1,1] \oplus [1,0] \oplus \langle 1 \rangle \oplus \bigoplus_{|\Phi^+|} [0,0] \\
&\simeq [0,0] \oplus [0,0] \oplus [0,0] \oplus \langle 1 \rangle \oplus \bigoplus_{|\Phi^+|} [0,0].
\end{aligned}$$

Type E_8 A basis for the root system is the same as for E_7 along with the following additional vector:

$$\alpha_8 = \epsilon_7 - \epsilon_6.$$

Then,

$$(\alpha_i, \alpha_8) = \begin{cases} 0 & \text{if } i = 1,2,3,4,5,6 \\ -1 & \text{if } i = 7 \\ 2 & \text{if } i = 8 \end{cases}.$$

and hence

$$\begin{aligned}
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_8}) \circ \mathrm{ad}(H_{\alpha_8})) &= 4\check{h} \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_7}) \circ \mathrm{ad}(H_{\alpha_8})) &= -2\check{h}
\end{aligned}$$

Thus the Killing form of E_8 restricted to the Cartan subalgebra $\mathcal{H}$ is:

$$\mathcal{K}|_{\mathcal{H}} = 4\check{h}\left(\sum_{i=1}^{8} x_i^2 - x_1x_3 - x_2x_4 - x_3x_4 - x_4x_5 - x_5x_6 - x_6x_7 - x_7x_8\right).$$

It follows then that the Killing form for E_8 is:

$$\mathcal{K} = \mathcal{K}|_{\mathcal{H}} + 4\check{h}\left(\sum_{|\Phi^+|} y_i y_{i+1}\right).$$

We can simplify this form by dividing through by $4\check{h}$. Doing so we get

$$\mathcal{K} = \sum_{i=1}^{8} x_i^2 - x_1x_3 - x_2x_4 - x_3x_4 - x_4x_5 - x_5x_6 - x_6x_7 - x_7x_8 + \sum_{|\Phi^+|} y_i y_{i+1}.$$

Now we would like to "diagonalize" this form. As before, it is enough to do so for the part related to the Cartan subalgebra. We have

$$\begin{aligned}\mathcal{K}|_{\mathcal{H}} &= \sum_{i=1}^{8} x_i^2 + x_1x_3 + x_2x_4 + x_3x_4 + x_4x_5 + x_5x_6 + x_6x_7 + x_7x_8 \\ &= (x_4^2 + x_4(x_2+x_3) + (x_2+x_3)^2) + (x_7^2 + x_7(x_6+x_8) + (x_6+x_8)^2) \\ &+ (x_1^2 + x_1x_3) + (x_5^2 + x_5(x_4+x_6)).\end{aligned}$$

Now consider the linear change of variables

$$\begin{aligned}&\tilde{x}_1 = x_1, \tilde{x}_2 = x_2 + x_3, \tilde{x}_3 = x_3, \tilde{x}_4 = x_4, \\ &\tilde{x}_5 = x_5, \tilde{x}_6 = x_4 + x_6, \tilde{x}_7 = x_5 + x_7, \tilde{x}_8 = x_6 + x_8.\end{aligned}$$

After this change our form becomes

$$\begin{aligned}&= (\tilde{x}_4^2 + \tilde{x}_4\tilde{x}_2 + \tilde{x}_2^2) + (\tilde{x}_7^2 + \tilde{x}_7\tilde{x}_8 + \tilde{x}_8^2) + (\tilde{x}_1^2 + \tilde{x}_1\tilde{x}_3) + (\tilde{x}_5^2 + \tilde{x}_5\tilde{x}_6) \\ &\simeq [1,1] \oplus [1,1] \oplus [1,0] \oplus [1,0].\end{aligned}$$

Thus the "diagonalization" of our simplified Killing form on E_8 is

$$\begin{aligned}\mathcal{K} &= [1,1] \oplus [1,1] \oplus [1,0] \oplus [1,0] \oplus \bigoplus_{|\Phi^+|} [0,0] \\ &\simeq [0,0] \oplus [0,0] \oplus [0,0] \oplus [0,0] \oplus \bigoplus_{|\Phi^+|} [0,0].\end{aligned}$$

3.7 Type F_4

As with type B_n, we will not need the Killing form for groups of type F_4, but we include the computation for completeness.

A basis for the root system is given by

$$\begin{aligned}\alpha_1 &= \epsilon_2 - \epsilon_3; \\ \alpha_2 &= \epsilon_3 - \epsilon_4; \\ \alpha_3 &= \epsilon_4; \\ \alpha_4 &= \frac{1}{2}(\epsilon_1 - \epsilon_2 - \epsilon_3 - \epsilon_4).\end{aligned}$$

Next we compute

$$\begin{aligned}&(\alpha_1, \alpha_1) = 2; (\alpha_1, \alpha_2) = -1; (\alpha_1, \alpha_3) = 0; (\alpha_1, \alpha_4) = 0; (\alpha_2, \alpha_2) = 2, \\ &(\alpha_2, \alpha_3) = -1; (\alpha_2, \alpha_4) = 0; (\alpha_3, \alpha_3) = 1; (\alpha_3, \alpha_4) = -\frac{1}{2}; (\alpha_4, \alpha_4) = 1.\end{aligned}$$

Also, recall the definition $\check{\alpha} = \frac{2\alpha}{(\alpha,\alpha)}$ from Lemma 3.1.1. For the roots in the basis of F_4 we have

$$\check{\alpha}_i = \begin{cases} \alpha_i & \text{for } i = 1, 2 \\ 2\alpha_i & \text{for } i = 3, 4 \end{cases}.$$

Knowing this, we compute:

$$\begin{aligned}
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_1}) \circ \mathrm{ad}(H_{\alpha_1})) &= 2\check{h}(\alpha_1, \alpha_1) = 4\check{h} \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_1}) \circ \mathrm{ad}(H_{\alpha_2})) &= 2\check{h}(\alpha_1, \alpha_2) = -2\check{h} \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_2}) \circ \mathrm{ad}(H_{\alpha_2})) &= 2\check{h}(\alpha_2, \alpha_2) = 4\check{h} \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_2}) \circ \mathrm{ad}(H_{\alpha_3})) &= 2\check{h}(\alpha_2, 2\alpha_3) = -4\check{h} \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_3}) \circ \mathrm{ad}(H_{\alpha_3})) &= 2\check{h}(2\alpha_3, 2\alpha_3) = 8\check{h} \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_3}) \circ \mathrm{ad}(H_{\alpha_4})) &= 2\check{h}(2\alpha_3, 2\alpha_4) = -4\check{h} \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_4}) \circ \mathrm{ad}(H_{\alpha_4})) &= 2\check{h}(2\alpha_4, 2\alpha_4) = 8\check{h}
\end{aligned}$$

Thus the Killing form of F_4 restricted to the Cartan subalgebra $\mathcal{H}$ is:

$$\mathcal{K}|_{\mathcal{H}} = 4\check{h}(x_1^2 - x_1x_2 + x_2^2) + 8\check{h}(-x_2x_3 + x_3^2 - x_3x_4 + x_4^2).$$

It follows then that the Killing form for F_4 is:

$$\mathcal{K} = \mathcal{K}|_{\mathcal{H}} + 4\check{h}\left(\sum_{|\Phi^+_{long}|} y_iy_{i+1}\right) + 8\check{h}\left(\sum_{|\Phi^+_{short}|} z_iz_{i+1}\right).$$

We can simplify this form by dividing through by $4\check{h}$. Doing so, and noting all terms multiplied by 2 go to 0, gives us

$$\mathcal{K} = x_1^2 + x_1x_2 + x_2^2 + \sum_{|\Phi^+_{long}|} y_iy_{i+1} + m * \langle\, 0 \,\rangle,$$

where $m = 2 + |\Phi^+_{short}|$. Clearly a "diagonalization" of this form is given by

$$\begin{aligned}
\mathcal{K} &= [1,1] \oplus \bigoplus_{|\Phi^+_{long}|} [0,0] \oplus m\langle 0 \rangle \\
&\simeq [0,0] \oplus \bigoplus_{|\Phi^+_{long}|} [0,0] \oplus m\langle 0 \rangle
\end{aligned}$$

3.8 Type G_2

A basis for the root system is given by

$$\alpha_1 = \epsilon_1 - \epsilon_2;$$
$$\alpha_2 = -2\epsilon_1 + \epsilon_2 + \epsilon_3.$$

Next we compute

$$(\alpha_1, \alpha_1) = 2; (\alpha_1, \alpha_2) = -3; (\alpha_2, \alpha_2) = 6.$$

Also, recall the definition $\check{\alpha} = \frac{2\alpha}{(\alpha,\alpha)}$ from Lemma 3.1.1. For the roots in the basis of G_2 we have

$$\check{\alpha}_1 = \alpha_1 \text{ and } \check{\alpha}_2 = \frac{1}{3}\alpha_2.$$

Note that α_2 is the long root and $(\check{\alpha}_2, \check{\alpha}_2) = (\frac{1}{3}\alpha_2, \frac{1}{3}\alpha_2) = \frac{1}{9} * 6 = \frac{2}{3}$, but in order to use the formula of Section 3.1 this value should be 2. In order to achieve we will consider the standard inner product multiplied by $\frac{1}{3}$. If we do this we get

$$\check{\alpha}_2 = \frac{2\alpha_2}{(\alpha_2, \alpha_2)} = \frac{2\alpha_2}{6 * \frac{1}{3}} = \alpha_2$$

and then it follows $(\check{\alpha}_2, \check{\alpha}_2) = (\alpha_2, \alpha_2) = 6 * \frac{1}{3} = 2$, as desired. So using this modified inner product we compute:

$$\begin{aligned}
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_1}) \circ \mathrm{ad}(H_{\alpha_1})) &= 2\check{h}\left(\frac{2\alpha_1}{(\alpha_1, \alpha_1)}, \frac{2\alpha_1}{(\alpha_1, \alpha_1)}\right) = 2\check{h}\left(\frac{2\alpha_1}{2 * \frac{1}{3}}, \frac{2\alpha_1}{2 * \frac{1}{3}}\right) \\
&= 2\check{h}(3\alpha_1, 3\alpha_1) = 18\check{h}\left(2 * \frac{1}{3}\right) = 12\check{h} \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_1}) \circ \mathrm{ad}(H_{\alpha_2})) &= 2\check{h}(3\alpha_1, \alpha_2) = 6\check{h}\left(-3 * \frac{1}{3}\right) = -6\check{h} \\
\mathrm{Tr}(\mathrm{ad}(H_{\alpha_2}) \circ \mathrm{ad}(H_{\alpha_2})) &= 2\check{h}(\frac{1}{3}\alpha_2, \frac{1}{3}\alpha_2) = 4\check{h}
\end{aligned}$$

From the above calculations it follows that the Killing form of G_2 restricted to the Cartan subalgebra $\mathcal{H}$ is:

$$\mathcal{K}|_{\mathcal{H}} = 4\check{h}(3x_1^2 + x_2^2 - 3x_1x_2).$$

Thus the Killing form on all of G_2 is

$$\mathcal{K} = \mathcal{K}|_{\mathcal{H}} + 12\check{h}\left(\sum_{|\Phi^+_{short}|} y_i y_{i+1}\right) + 4\check{h}\left(\sum_{|\Phi^+_{long}|} z_i z_{i+1}\right).$$

Then we may simplify this form by dividing through by $4\check{h}$ and making use of the fact that we work in characteristic 2. After simplification we get

$$\mathcal{K} = x_1^2 + x_1x_2 + x_2^2 + \sum_{|\Phi^+|} y_i y_{i+1}.$$

An obvious "diagonalization" of this form is

$$\begin{aligned}\mathcal{K} &= [1,1] \oplus \bigoplus_{|\Phi^+|} [0,0] \\ &\simeq [0,0] \oplus \bigoplus_{|\Phi^+|} [0,0]\end{aligned}$$

3.9 Dimension Lemma

Later on we will need the following result.

Lemma 3.9.1. *The dimension of the normalization of the portion of the Killing forms not related to the Cartan subalgebra for all simple algebraic groups G is greater than or equal to $2 \cdot \mathrm{rank}(G)$.*

Proof. To simplify terminology, in the remainder of the proof we will refer to the portion of the Killing forms not related to the Cartan subalgebra as the "non-Cartan form". We will now proceed to verify the result on a

case-by-case basis.

- $\mathbf{A_n}$: The dimension of the non-Cartan form is $2|\Phi^+| = 2\frac{n(n+1)}{2} = n^2 + n \geq 2n$ for all $n \geq 1$.
- $\mathbf{B_n}$: Since root systems of type B_1 and A_1 are isomorphic, we only need to consider the case $n \geq 2$. The dimension of the non-Cartan form is then $2|\Phi^+_{long}| = 2(n^2 - n) = 2n^2 - 2n = 2n(n-1) \geq 2n$ for all $n \geq 2$.
- $\mathbf{C_n}$: Since root systems of type B_n and C_n are isomorphic for $n = 1, 2$ we only need consider the case $n \geq 3$. The dimension of the non-Cartan form is $2|\Phi^+_{long}| = 2n \geq 2n$ for all $n \geq 3$.
- $\mathbf{D_n}$: Here we only need to consider the case $n \geq 4$, because for lower values of n the result follows for root systems of type A_n. The dimension of the non-Cartan form is $2|\Phi^+| = 2(n^2 - n) = 2n^2 - 2n = 2n(n-1) \geq 2n$ for all $n \geq 4$.
- $\mathbf{E_6}$: The dimension of the non-Cartan form is $2|\Phi^+| = 72 \geq 6 \cdot 2 = 12$.
- $\mathbf{E_7}$: The dimension of the non-Cartan form is $2|\Phi^+| = 126 \geq 7 \cdot 2 = 14$.
- $\mathbf{E_8}$: The dimension of the non-Cartan form is $2|\Phi^+| = 240 \geq 8 \cdot 2 = 16$.
- $\mathbf{F_4}$: The dimension of the non-Cartan form is $2|\Phi^+_{long}| = 24 \geq 4 \cdot 2 = 8$.
- $\mathbf{G_2}$: The dimension of the non-Cartan form is $2|\Phi^+| = 12 \geq 2 \cdot 2 = 4$.

□

Chapter 4

Constructing an Orthogonal Representation

4.1 A Preliminary Lemma

Letting G be an algebraic group as defined for Theorem 1.2.1, we will construct a very explicit orthogonal representation, which we will call the "non-degenerate Killing" representation. Before doing so we need a small preliminary Lemma.

Lemma 4.1.1. *Let $\mathfrak{g}$ be a simple Lie algebra. The Killing form $\mathcal{K}$ of $\mathfrak{g}$ is invariant under any automorphism of $\mathfrak{g}$.*

Proof. Let $\rho \in \mathrm{Aut}(\mathfrak{g})$. The equation $\rho([x,y]) = [\rho(x), \rho(y)]$ for $z = \rho(y)$ is $\rho([x, \rho^{-1}(z)]) = [\rho(x), z]$, which can be written as $\mathrm{ad}(\rho(x)) = \rho \circ \mathrm{ad}(x) \circ \rho^{-1}$. Thus,

$$\begin{aligned}\mathcal{K}(\rho(x), \rho(y)) &= \mathrm{Tr}(\mathrm{ad}(\rho(x)) \circ \mathrm{ad}(\rho(y))) = \mathrm{Tr}(\rho \circ \mathrm{ad}(x) \circ \mathrm{ad}(y) \circ \rho^{-1}) \\ &= \mathrm{Tr}(\mathrm{ad}(x) \circ \mathrm{ad}(y)) = \mathcal{K}(x,y)\,. \quad \square\end{aligned}$$

4.2 An Orthogonal Representation

We will construct the "non-degenerate Killing" representation by relying on the explicit computations of Killing forms of simple Lie algebras done in Chapter 3.

Let G^{ad} be a simple algebraic group of adjoint type over a field k of characteristic 2 and let $\varphi\colon G^{sc} \to G^{ad}$ be its universal covering. Here G^{sc} is the corresponding simply connected group. Let $\mu = \mathrm{Ker}(\varphi)$. It is the center of G^{sc} and hence μ is contained in any maximal torus $\widetilde{T}$ of G^{sc}. Related to φ we also have the associated differential map

$$d\varphi\colon \mathfrak{g}^{sc} := \mathrm{Lie}(G^{sc}) \longrightarrow \mathrm{Lie}(G^{ad}) := \mathfrak{g}^{ad},$$

which is a morphism of Lie algebras. Before proceeding we would like to get a little more information on $\mathrm{Ker}(d\varphi)$. In particular we want the following result:

Lemma 4.2.1. $\mathrm{Ker}(d\varphi) \subset C$ *where* C *is a Cartan subalgebra of* $\mathfrak{g}^{sc}$.

Note that $\mathrm{Ker}(d\varphi)$ is nontrivial in the following cases: A_n for odd n, B_n, C_n, D_n and E_7. For completeness, at the end of this Section we will provide a summary of the kernel of φ for each type of simple algebraic group and then $\mathrm{Ker}(d\varphi)$ can be viewed as the Lie algebra of these kernels.

Proof. Proof of Lemma 4.2.1 Recall the definition of the ring of dual numbers:

$$k[\epsilon] = \{x + y\epsilon \mid x, y \in k\}$$

where $\epsilon^2 = 0$. We define a ring homomorphism

$$k[\epsilon] \longrightarrow k; \quad a + b\epsilon \mapsto a.$$

If G is an algebraic group over k, then this morphism induces another morphism

$$\lambda\colon G(k[\epsilon]) \longrightarrow G(k).$$

We can view G as living inside GL_n for some n and after making such an identification we get that

$$\mathrm{Ker}(\lambda) = \left\{ (g_{ij}) \in G(k[\epsilon]) \;\middle|\; g_{ij} = \begin{cases} 1 + b_{ij}\epsilon & \text{if } i = j \\ b_{ij}\epsilon & \text{if } i \neq j \end{cases} \text{ for } b_{ij} \in k \right\}.$$

It is then a well-known fact that the matrix (b_{ij}) is contained in the Lie algebra of G and hence $\mathrm{Lie}(G) = \mathfrak{g}$ can be identified with $\mathrm{Ker}(\lambda)$. In this way we have $\mathrm{Lie}(G) = \mathrm{Ker}(\lambda) \subset G(k[\epsilon])$. Now, let us apply this general result to our situation.

For any ring R our universal covering map φ induces

$$\varphi_R \colon G^{sc}(R) \to G^{ad}(R)$$

and by a general result $\mathrm{Ker}(\varphi_R) = Z(G^{sc})(R)$ where Z denotes the center. Letting $R = k[\epsilon]$ we get a map

$$\varphi_{k[\epsilon]} \colon G^{sc}(k[\epsilon]) \longrightarrow G^{ad}(k[\epsilon]).$$

By the above identification we know $\mathfrak{g}^{sc} \subset G^{sc}(k[\epsilon])$ and it is also true that

$$\varphi_{k[\epsilon]}|_{\mathfrak{g}^{sc}} = d\varphi \colon \mathfrak{g}^{sc} \to \mathfrak{g}^{ad} \subset G^{ad}(k[\epsilon]).$$

Again, working with an arbitrary algebraic group G, it is known that

$$G(k[\epsilon]) \simeq G(k) \rtimes \mathrm{Lie}(G).$$

Hence, applying this decomposition to $Z(G^{sc})$ we get

$$Z(G^{sc})(k[\epsilon]) = Z(G^{sc})(k) \rtimes \mathrm{Lie}(Z(G^{sc})).$$

Putting everything together we have

$$\mathrm{Ker}(d\varphi) \subset \mathrm{Ker}(\varphi_{k[\epsilon]}) = Z(G^{sc})(k[\epsilon]) = Z(G^{sc})(k) \rtimes \mathrm{Lie}(Z(G^{sc})).$$

This implies that

$$\mathrm{Ker}(d\varphi) = \mathrm{Lie}(Z(G^{sc}) \subset C$$

as desired. The last inclusion follows because $Z(G^{sc}) \subset \widetilde{T}$ for any maximal torus $\widetilde{T}$ and therefore $\mathrm{Lie}(Z(G^{sc})) \subset \mathrm{Lie}(\widetilde{T}) = C$. □

Define $W := d\varphi(\mathfrak{g}^{sc})$ and note that this is a Lie subalgebra of $\mathfrak{g}^{ad}$; in particular it is a vector subspace of $\mathfrak{g}^{ad}$. Also, since we have seen that $\mathrm{Ker}(d\varphi) \subset C$ where C was a Cartan subalgebra of $\mathfrak{g}^{sc}$ we obtain the following result:

Corollary 4.2.2.

$$W \simeq C/\mathrm{Ker}(d\varphi) \oplus \Lambda,$$

where Λ represents the components of the root space decomposition of $\mathfrak{g}^{ad}$ other than its Cartan subalgebra.

Let $\mathcal{K}$ be the Killing form on $\mathfrak{g}^{sc}$, which we computed in the previous Chapter. Let $\mathrm{Ad}\colon G^{sc} \to \mathrm{GL}(\mathfrak{g}^{sc})$ be the adjoint representation. Then for any $g \in G^{sc}(k)$ and $v \in \mathfrak{g}^{sc}$ we have

$$\mathcal{K}(\mathrm{Ad}(g)(v)) = \mathcal{K}(gvg^{-1}) = K(v)$$

by Lemma 4.1.1. Thus, we can view the adjoint mapping as going from

$$G^{sc} \to \mathcal{O}(\mathfrak{g}^{sc}, \mathcal{K}) \subset \mathrm{GL}(\mathfrak{g}^{sc}).$$

Similar considerations are applied to the adjoint representation $\mathrm{Ad}\colon G^{ad} \to \mathrm{GL}(\mathfrak{g}^{ad})$ of G^{ad}. We would now like to show the following:

Lemma 4.2.3. *$W \subset \mathfrak{g}^{ad}$ is stable with respect to $\mathrm{Ad}(G^{ad})$, i.e. for every $g \in G^{ad}(k)$ and $v \in \mathfrak{g}^{sc}$ we have $g(d\varphi(v)) = d\varphi(w)$ for some $w \in \mathfrak{g}^{sc}$.*

Proof. Since k is algebraically closed we have a surjection $G^{sc}(k) \to G^{ad}(k)$. Thus, given $g \in G^{ad}(k)$, we can choose a lifting $\widetilde{g} \in G^{sc}(k)$.

It is known that the following diagram is commutative by [Hu2]:

$$\begin{array}{ccc|ccc} G^{sc}\times\mathfrak{g}^{sc} & \xrightarrow{Ad} & \mathfrak{g}^{sc} & (\widetilde{g},v) & \longmapsto & \widetilde{g}(v) \\ \varphi\downarrow\, d\varphi & \circlearrowleft & \downarrow d\varphi & \downarrow & & \downarrow \\ G^{ad}\times\mathfrak{g}^{ad} & \xrightarrow{Ad} & \mathfrak{g}^{ad} & (g,d\varphi(v)) & \longmapsto & g(d\varphi(v))=d\varphi(\widetilde{g}(v)) \end{array}$$

So setting $w=\widetilde{g}(v)$ the claim follows. □

As a result we get a representation $G^{ad}\to \mathrm{GL}(W)$ via the restriction of the adjoint representation of G^{ad}, i.e. for $g\in G^{ad}(k)$ we get

$$\mathrm{Ad}(g)|_W\colon W\to W.$$

Our next goal is to show that the Killing form $\mathcal{K}$ on $\mathfrak{g}^{sc}$ produces one on $W=d\varphi(\mathfrak{g}^{sc})$. Namely, we define a form $\mathcal{K}_W$ (and by abusing terminology we still call it the Killing form) on W by $\mathcal{K}_W(w)=\mathcal{K}(v)$ where $v\in\mathfrak{g}^{sc}$ is any lifting of $w\in W$. Note that such a lifting exists because $d\varphi$ is a surjection of $\mathfrak{g}^{sc}$ onto W. The only thing we must now check is that this definition is well defined, i.e. does not depend on the choice of lifting.

Suppose v_1,v_2 are two liftings of $w\in W$ under $d\varphi$. Then

$$v_1-v_2:=u\in\mathrm{Ker}(d\varphi)\subset\mathrm{Lie}(Z(G^{sc}))\subset Z(\mathfrak{g}^{sc}).$$

Hence

$$\begin{aligned}\mathcal{K}(v_2)&=\mathcal{K}(v_1+u)=\mathcal{K}(v_1+u,v_1+u)\\&=\mathcal{K}(v_1,v_1)+\mathcal{K}(v_1,u)+\mathcal{K}(u,v_1)+\mathcal{K}(u,u)\\&=\mathcal{K}(v_1,v_1)=\mathcal{K}(v_1).\end{aligned}$$

These equalities follow because $u\in Z(\mathfrak{g}^{sc})$, which implies $ad(u)=0$.

Having shown that $\mathcal{K}_W$ is well defined in all cases we next claim that we have the following result:

Lemma 4.2.4. *There is an orthogonal representation* $\eta\colon G^{ad} \to \mathcal{O}(W, \mathcal{K}_W)$.

Proof. We know already that we have a mapping $G^{ad} \to \mathrm{GL}(W)$, but to prove our claim we must show that for every $w \in W$ and $g \in G^{ad}(k)$ we have $\mathcal{K}_W(g(w)) = \mathcal{K}_W(w)$. Let $v \in \mathfrak{g}^{sc}$, $\widetilde{g} \in G^{sc}(k)$ be any liftings of w and g respectively. Then,

$$\mathcal{K}_W(g(w)) = \mathcal{K}(\widetilde{g}(v)) = \mathcal{K}(v) = \mathcal{K}_W(w),$$

so our claim is proven. □

Note that $\mathcal{K}_W$ may be degenerate, but we know its normalization $\overline{\mathcal{K}}_W$ is nondegenerate by Lemma 2.1.6. Also, by Lemma 2.1.8 we have a natural morphism $\lambda\colon \mathcal{O}(W, \mathcal{K}_W) \to \mathcal{O}(\overline{W}, \overline{\mathcal{K}}_W)$ where $\overline{W} = W/\mathrm{rad}(\mathcal{K}_W)$. Thus $\lambda \circ \eta$ gives us the desired orthogonal representation, which we call the "non-degenerate Killing" representation

We would also like to get a handle on the dimension of $\overline{W}$. In Chapter 3 we explicitly computed Killing forms on $\mathfrak{g}^{sc}$ which we have denoted by $\mathcal{K}$. We then saw that we had an associated Killing form $\mathcal{K}_W$ on $W \simeq C/\mathrm{Ker}(d\varphi) \oplus \Lambda$.

From this decomposition of W and the definition of $\mathcal{K}_W$ it follows that $\mathcal{K}_W$ is isometric to $\mathcal{K}$, except that some terms of $\mathcal{K}$ related to the Cartan subalgebra of $\mathfrak{g}^{sc}$ may be missing in $\mathcal{K}_W$. Note that the terms of $\mathcal{K}$ not related to the Cartan subalgebra are not modified at all when we pass to $\mathcal{K}_W$. Then, since the portion of $\mathcal{K}$ not related to the Cartan subalgebra is nondegenerate, when we pass to the normalization $\overline{\mathcal{K}}_W$ this portion again remains unaffected.

What this tells us is that the dimension of $\overline{\mathcal{K}}_W$ is at least as great as the dimension of the portion of $\mathcal{K}$ not related to the Cartan subalgebra. In Lemma 3.9.1, we saw that this lower bound on the dimension of $\overline{\mathcal{K}}_W$ was greater than $2 \cdot rank(G)$ for all types of simple groups G.

To complete our construction we need an orthogonal representation not

only for G^{ad}, but also for the subgroup of $\mathrm{Aut}(G^{ad})$ generated by G^{ad} and c, where $c \in \mathrm{Aut}(G^{ad})$ was defined in Section 1.2 to have the property $c^2 = 1$ and $c(t) = t^{-1}$ for all t in a maximal torus T of G^{ad}. However, as discussed in [ChSe], c preserves $\mathfrak{g}^{sc}$ and its Killing form. Then arguing as for Ad above, we can conclude c preserves W and $\mathcal{K}_W$. Then again, arguing as above, we get an orthogonal representation which we will also call the "non-degenerate Killing" representation.

We conclude the Chapter by providing a table of $\mathrm{Ker}(\varphi)$ for each type of simple algebraic group. We also indicate whether or not this kernel is smooth over a field of characteristic 2.

Table 4.1: Kernel of φ

Type	**Kernel**	**Smooth?**
A_n - n odd	μ_{n+1}	no
A_n - n even	μ_{n+1}	yes
$B_n; C_n$	μ_2	no
D_n - n even	$\mu_2 \times \mu_2$	no
D_n - n odd	μ_4	no
E_6	μ_3	yes
E_7	μ_2	no
remaining types	1	yes

Chapter 5

Twisting of Killing Forms

5.1 Twisting of Killing Forms

Let G be an algebraic group as described in Section 1.2 . Let Φ be the root system of G with respect to a maximal torus T^{ad} of rank r and let $\Omega = \{\alpha_1, ..., \alpha_r\}$ be a basis of Φ. We use the notation T^{ad} to indicate that this is a maximal torus in a group G of adjoint type. It follows by definition that Ω is a basis for the character group $X(T^{ad})$. Now consider the co-character group $Y(T^{ad}) = \mathrm{Hom}(\mathrm{G}_m, T^{ad})$. There is a natural bilinear pairing

$$(-,-)\colon Y(T^{ad}) \times X(T^{ad}) \longrightarrow \mathbb{Z}$$

which is defined as follows. If $\varphi \in X(T^{ad})$ and $\psi \in Y(T^{ad})$, then $\varphi \circ \psi\colon \mathrm{G}_m \to \mathrm{G}_m$ is a homomorphism, hence it is given by exponentiation to an integral power, say $a = a_{\varphi\,\psi} \in \mathbb{Z}$. Then, by definition $(\psi, \varphi) = a$.

Having fixed our basis $\alpha_1, ..., \alpha_r$ of $X(T^{ad})$ we can choose a basis for $Y(T^{ad})$ dual to this one with respect to the pairing $(-,-)$, say $\delta_1, ..., \delta_r$. What this means is that $\delta_1, ..., \delta_r$ is a basis of $Y(T^{ad})$ such that

$$(\delta_i, \alpha_j) = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases} .$$

Then if S is any k-algebra and $t \in T^{ad}(S)$ we can write t uniquely as $t = \delta_1(s_1)\delta_2(s_2)\cdots\delta_r(s_r)$ for some $s_i \in S^\times$. Thus we can view elements of the group $T^{ad}(S)$ as r-tuples $t = (\delta_1(s_1), ..., \delta_r(s_r))$ and in this way we fix a decomposition $T^{ad} \simeq \mathrm{G}_m \times \mathrm{G}_m \times ... \times \mathrm{G}_m$.

Let A_0 be the kernel of squaring on T^{ad} and let $A = A_0 \times \{1, c\}$ be the subgroup of G generated by A_0 and c, where c is the automorphism described in Section 1.2. The group A is isomorphic to $\mu_2 \times ... \times \mu_2 \times \mathbb{Z}/2$.

Let $K = k(t_1, .., t_r, x)$ where $t_1, ..., t_r, x$ are algebraically independent indeterminates. Then

$$H^1(K, A) = H^1(K, \mu_2) \times ... \times H^1(K, \mu_2) \times H^1(K, \mathbb{Z}/2)$$

where here we work with faithfully flat cohomology. Note that in characteristic 2 the constant group scheme $\mathbb{Z}/2$ is smooth so we can think of $H^1(K, \mathbb{Z}/2)$ in terms of Galois cohomology. Then using standard results from cohomology theory [Se02] we get that

$$H^1(K, A) \simeq K^\times/(K^\times)^2 \times ... \times (K^\times)/(K^\times)^2 \times K/\wp(K)\,,$$

where $\wp(K) = \{y^2 + y \mid y \in K\}$. The t_i define elements $(t_i) \in K^\times/(K^\times)^2$ and x defines an element $(x) \in K/\wp K$. Let θ_A be the element of $H^1(K, A)$ with components $((t_1), ..., (t_r), (x))$.

Now let $\lambda(\theta_A) := \theta_0$ be the image of θ_A in $H^1(K, \mathcal{O}(V, q))$ where $\lambda\colon A \to \mathcal{O}(V, q)$ is the restriction of the orthogonal representation constructed in Chapter 4. Note that θ_0 can be interpreted as a quadratic form, namely the twist of q by θ_0. We will compute this form explicitly.

Before beginning to compute the twisting, we want to make clear precisely which forms will be twisted. In Chapter 3 we computed Killing forms for the simply connected case and then in Chapter 4, via $d\varphi$, the differential of the universal covering $\varphi\colon G^{sc} \to G^{ad}$, we obtained a corresponding Killing

form on

$$W = d\varphi(\text{Lie}(G^{sc})) \subset \text{Lie}(G^{ad}) = \mathfrak{g}^{ad}.$$

It is for these Killing forms that we will be computing the twisting.

We know we can decompose $\text{Lie}(G^{sc}) = \mathfrak{g}^{sc}$ as

$$\mathfrak{g}^{sc} = C^{sc} \oplus \bigoplus_{\alpha \in \Phi^+} (X_\alpha \oplus X_{-\alpha}) = C^{sc} \oplus \Lambda^{sc}$$

where C^{sc} is the Cartan subalgebra corresponding to the maximal torus T^{sc} and Λ^{sc} corresponds to the remainder of the root space decomposition. We saw in Chapter 4 that the kernel of $d\varphi \colon \mathfrak{g}^{sc} \to \mathfrak{g}^{ad}$ was contained entirely in C^{sc}. Thus if decompose $\mathfrak{g}^{ad}$ as

$$\mathfrak{g}^{ad} = C^{ad} \oplus \bigoplus_{\alpha \in \Phi^+} (X_\alpha \oplus X_{-\alpha}) = C^{ad} \oplus \Lambda^{ad}$$

we know that $d\varphi|_{\Lambda^{sc}} \colon \Lambda^{sc} \xrightarrow{\sim} \Lambda^{ad}$ is an isomorphism. Thus, the portion of the Killing forms not related to C^{sc} computed in Chapter 3 is the same for $\mathfrak{g}^{sc}$ and $\mathfrak{g}^{ad}$. Since $Ker(d\varphi)$ was contained in C^{sc}, some portion of the Killing forms related to C^{sc} computed in Chapter 3 may vanish, but we will see this will be of no consequence.

We begin the computations of the twisted quadratic forms by noting that our cocycle θ_A is really the product of two cocycles $((t_1), ..., (t_r))$ and (x). Since these two cocycles take values in a commutative group, their product really gives a cocycle which we call θ_A. So to twist we can proceed in 2 steps. First we will twist by (x) with respect to Galois cohomology and then twist the resulting form by $((t_1), ..., (t_r))$ with respect to faithfully flat cohomology. This process would be the same as if we twisted by θ_0 all in one step.

We will further break down each of these steps into two substeps. Since C^{ad} and Λ^{ad} are orthogonal with respect to the Killing form and our cocycle stabilizes each of C^{ad} and Λ^{ad}, we will twist separately the portion of the

Killing forms related to the Cartan subalgebra and those which are not related to the Cartan subalgebra.

This observation is useful for two reasons. First of all it simplifies computations. Secondly, in Chapter 4 we computed an orthogonal representation not for $\mathfrak{g}^{ad}$, but rather for the normalization of $W = d\varphi(\mathfrak{g}^{sc})$, which we denoted $\overline{W}$. So what we would really like is to know what the twisting of the Killing form we defined on $\overline{W}$ looks like.

Let us decompose W as $W = W_{Cartan} \oplus W_{roots}$. We know that $W_{roots} \simeq \Lambda^{ad}$, so after we compute the twisting of the portion of the Killing form related to Λ^{ad}, we will know exactly what the portion of the twisting of the Killing form related to W_{roots} is. This form will be non-degenerate, so when we pass from W to $\overline{W}$ this portion of the Killing form will remain unaffected. Now, let's see what happens to the Cartan part of the Killing form.

As mentioned, we only know that the Killing form on W_{Cartan} is the same as that of C^{sc} with some terms potentially missing. Based on our computations in Chapter 3 we would thus know that the Killing form on W_{Cartan} looks like

$$\bigoplus_i [0,0] \oplus m\langle 0\rangle \oplus n\langle 1\rangle \quad (\dagger)$$

where m may be zero and $n = 0$ or 1. When we move from W to $\overline{W}$, the only change to the portion of the Killing form related to W_{Cartan} would be that any copies of $\langle 0\rangle$ would disappear.

The discussion in the previous paragraph tells us, to a degree, what the portion of the Killing form related to W_{Cartan} will look like when we pass to $\overline{W}$. However, what we really want to know is what happens to the twisting of the portion of the Killing form related to W_{Cartan} when we pass to $\overline{W}$. Well, as we will see shortly, the portion of the Killing form related to W_{Cartan} remains totally unaffected when we twist. Thus we know that after twisting and after passing to $\overline{W}$, the portion of our Killing form related to W_{Cartan} will be given by $(\dagger)$.

As mentioned above, we will twist with respect to the cocyles (x) and $((t_1), ..., (t_r))$ separately. To compute the twisting by (x) we begin by considering the portion of the Killing form not related to the Cartan subalgebra, which is a direct sum of binary quadratic forms $[0, 0]$ stable with respect to c for all types of simple Lie algebras. So to compute the twisting, it will be enough to consider how to twist just one of these binary quadratic forms. Let

$$V = \mathcal{L}_\alpha \oplus \mathcal{L}_{-\alpha} = \langle X_\alpha, X_{-\alpha} \rangle$$

be the 2-dimensional vector space over K on which our quadratic form $[0, 0]$ is defined. Now let L/K be a Galois extension of degree 2, i.e. $L = K(\theta)$ where θ is a root of the irreducible polynomial $y^2 + y + x$. We know that $\Gamma = \mathrm{Gal}(L/K) = \{1, \sigma\}$ where $\sigma(\theta) = \theta + 1$. Define $V_L = L \otimes_K V$ and let $v = (v_1 + v_2\theta)X_\alpha + (v_1' + v_2'\theta)X_{-\alpha} \in V_L$ be an arbitrary element.

Since 1 is the identity automorphism, clearly $\lambda(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and since c permutes X_α and $X_{-\alpha}$ we get $\lambda(c) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. We will now describe explicitly what the twisted actions of the automorphism $1, \sigma$ are on an arbitrary element v of V_L. We get,

$$\begin{aligned} 1^* \cdot v &= \lambda(1)id((v_1 + v_2\theta)X_\alpha + (v_1' + v_2'\theta)X_{-\alpha})) = v \text{ ; and} \\ \sigma^* \cdot v &= \lambda(c)\sigma((v_1 + v_2\theta)X_\alpha + (v_1' + v_2'\theta)X_{-\alpha}) \\ &= \lambda(c)((v_1 + v_2(\theta + 1))X_\alpha + (v_1' + v_2'(\theta + 1)X_{-\alpha}) \\ &= (v_1' + v_2'(\theta + 1))X_\alpha + (v_1 + v_2(\theta + 1))X_{-\alpha}\,. \end{aligned}$$

In order to compute the twisting of our Killing forms by (x) we must find a basis for

$$U = V_L^{\Gamma^*} = \{v \in V_L \mid \gamma^* \cdot v = v \ \forall\ \gamma \in \Gamma\}.$$

By Galois descent, the dimension of this vector space is the same as that of V, namely 2. So in order to find a basis we must find 2 linearly independent elements of U. Note that 1 fixes every element of V under the twisted action,

so to see whether or not an element of V_L belongs to U it is enough to check that it is fixed under the twisted action of σ^*. For this, we have:

$$\begin{aligned}
\sigma^* \cdot (X_\alpha + X_{-\alpha}) &= \lambda(c)\sigma((X_\alpha + X_{-\alpha})) = \lambda(c)(X_\alpha + X_{-\alpha}) \\
&= X_{-\alpha} + X_\alpha \text{ ; and} \\
\sigma^* \cdot ((\theta+1)X_\alpha + \theta X_{-\alpha}) &= \lambda(c)\sigma((\theta+1)X_\alpha + \theta X_{-\alpha}) \\
&= \lambda(c)(\theta X_\alpha + (\theta+1)X_{-\alpha}) \\
&= \theta X_{-\alpha} + (\theta+1)X_{-\alpha}\,.
\end{aligned}$$

So these two elements clearly live in U. They are also linearly independent because if you consider the matrix associated to these elements it is $\begin{bmatrix} 1 & \theta+1 \\ 1 & \theta \end{bmatrix}$. The determinant of this matrix is $\theta - \theta - 1 = -1 = 1$, hence these elements are linearly independent and thus form a basis for $U = V_L^{\Gamma^*}$. Let $e_1 = X_\alpha + X_{-\alpha}$ and $e_2 = (\theta+1)X_\alpha + \theta X_{-\alpha}$.

Now we can compute the twisting of $p = [0,0]$. Note that by definition $p(X_\alpha) = p(X_{-\alpha}) = 0$. Then we have:

$$\begin{aligned}
p(e_1) &= 0^2 + 1 \cdot 1 + 0^2 = 1\,; \\
p(e_2) &= 0^2 + (\theta+1)(\theta) + 0^2 = \theta^2 + \theta = x\,; \\
p(e_1 + e_2) &= p(\theta X_\alpha + (\theta+1)X_{-\alpha}) = (\theta)(\theta+1) = x \text{ ; and} \\
b_p((e_1, e_2)) &= p(e_1 + e_2) + p(e_1) + p(e_2) = 1 + x + x = 1\,.
\end{aligned}$$

Thus we can conclude that $p|_U = y_1^2 + y_1 y_2 + x y_2^2 = [1, x]$ is the twisted form of $[0,0]$ with respect to (x).

Now we focus on computing the twisting, by (x), of the portion of the Killing form related to C^{ad} (resp. W_{Cartan}). In fact, we will show that this portion of the Killing form is unaffected by twisting. At the beginning of this Section we fixed a decomposition $T^{ad} \simeq G_m \times G_m \times ... \times G_m$. Given an arbitrary element $s \in T^{ad}$ we can write $s = (s_1, ..., s_n)$. We know that for the automorphism c defined in Section 1.2, $c(s) = s^{-1} = (s_1^{-1}, ..., s_n^{-1})$. Our

goal is to show that c acts trivially on C^{ad} (resp.W_{Cartan}), which would prove our claim that the portion of the Killing form related to C^{ad} is unaffected by twisting.

We have

$$\begin{aligned} C^{ad} &= \mathrm{Lie}(T^{ad}) = \mathrm{Lie}(G_m \times G_m \times ... \times G_m) \\ &\simeq \mathrm{Lie}(G_m) \times \mathrm{Lie}(G_m) \times ... \times \mathrm{Lie}(G_m). \end{aligned}$$

So to show that c acts trivially on C^{ad} it is enough to show that c acts trivially on each component $\mathrm{Lie}(G_m)$. Let $a \in \mathrm{Lie}(G_m)$. Since $\mathrm{Lie}(G_m) \subset G_m(k[\epsilon])$ (as discussed in Chapter 4) we know that we can identify a with $1 + a\epsilon \in G_m(k[\epsilon])$. We know c takes $1 + a\epsilon$ to its inverse, which is $1 - a\epsilon$. Indeed, $(1 + a\epsilon)(1 - a\epsilon) = 1 + a\epsilon - a\epsilon - a^2\epsilon^2 = 1$ because $\epsilon^2 = 0$. However, since we are in characteristic 2 we have $1 - a\epsilon = 1 + a\epsilon$ and therefore c acts trivially on $\mathrm{Lie}(G_m)$, as desired.

Now we will proceed to compute the twisting of our newly twisted Killing form by $((t_1), ..., (t_r))$. Note that since $\mu_2 \times \cdots \times \mu_2 \subset T^{ad}$, this cocycle will act trivially on the Cartan subalgebra C^{ad} and so twisting does not change the portion of the Killing form related to the Cartan subalgebra at all. So we focus our attention on the portion of the Killing form not related to the Cartan subalgebra. From the above we have the form $[1, x]$ defined on a K-vector space U with basis e_1, e_2 described above.

In our situation, we have a short exact sequence

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{G}_m \longrightarrow \mathrm{G}_m \longrightarrow 1\,,$$

where the map between G_m and G_m is squaring. Now let $a \in \mathrm{G}_m(K)$ and let $\sqrt{a}$ be a lifting of a in $\mathrm{G}_m(\overline{K})$. Recall that in Section 2.3 we defined two embedding maps:

$$\pi_i \colon \overline{K} \to \overline{K} \otimes \overline{K}, y \longmapsto \begin{cases} y \otimes 1 & i = 1 \\ 1 \otimes y & i = 2 \end{cases}.$$

Then, $\pi_1^*(\sqrt{a}) = \sqrt{a} \otimes 1$ and

$$(\pi_2^*(\sqrt{a}))^{-1} = (1 \otimes \sqrt{a})^{-1} = 1 \otimes \frac{1}{\sqrt{a}}$$

are both elements of $\mathrm{G}_m(\overline{K} \otimes \overline{K})$. Their product is $(\sqrt{a} \otimes 1)(1 \otimes \frac{1}{\sqrt{a}}) = (\sqrt{a} \otimes \frac{1}{\sqrt{a}}) \in \mathrm{G}_m(\overline{K} \otimes \overline{K})$. However, note that $(\sqrt{a} \otimes \frac{1}{\sqrt{a}})^2 = (a \otimes \frac{1}{a}) = \frac{a}{a}(1 \otimes 1) = 1 \otimes 1$, so $(\sqrt{a} \otimes \frac{1}{\sqrt{a}}) \in \mu_2(\overline{K} \otimes \overline{K})$, as we expected from the general construction in Section 2.3.

Recall that we started our twisting process working over $V = \langle X_\alpha, X_{-\alpha} \rangle$. Now let $\alpha = \sum m_i \alpha_i \in X(T)$. Then if $t \in T(S)$, where S is any k-algebra, and $t = \prod \delta_i(s_i)$, then $\alpha(t) = s_1^{m_1} \cdots s_r^{m_r}$. Also recall that we defined

$$U = \langle e_1, e_2 \rangle = \langle X_\alpha + X_{-\alpha}, (\theta + 1)X_\alpha + \theta X_{-\alpha} \rangle.$$

Now let $a = t_1^{m_1} \cdots t_r^{m_r}$ and

$$L = K(\sqrt{t_1^{m_1} \cdots t_r^{m_r}}) = K(\sqrt{a}).$$

In order to compute the twisting of $[1, x]$ by

$$t \leftrightarrow ((t_1), ..., (t_n)) \in \prod K^\times/(K^\times)^2,$$

we must find 2 linearly independent elements of $U_L := U \otimes_K L$ which satisfy the condition

$$\pi_1^*(x) = t(\pi_2^*(x)).$$

Note that $t = \prod \delta_i(\sqrt{t_i} \otimes \frac{1}{\sqrt{t_i}})$ and then

$$\begin{aligned} t(\pi_2^*(x)) &= \prod (\sqrt{t_i} \otimes \tfrac{1}{\sqrt{t_i}})^{m_i} \pi_2^*(x) \\ &= \prod (\sqrt{t_i^{m_i}} \otimes \tfrac{1}{\sqrt{t_i^{m_i}}}) \pi_2^*(x) \\ &= (\sqrt{t_1^{m_1}} \cdots \sqrt{t_r^{m_r}} \otimes \tfrac{1}{\sqrt{t_1^{m_1}} \cdots \sqrt{t_r^{m_r}}}) \pi_2^*(x) \\ &= (\sqrt{a} \otimes \tfrac{1}{\sqrt{a}}) \pi_2^*(x). \end{aligned}$$

Any element of $U(L \otimes L)$ can be written as $w = ce_1 + de_2$ where $c, d \in L \otimes L$ and $\{e_1, e_2\}$ is the basis for U described above. Then the action is given by $a \cdot w = (\sqrt{a} \otimes \frac{1}{\sqrt{a}})(ce_1 + de_2)$. Now we must find two linearly independent elements w_1, w_2 of $U_L = U \otimes L$ such that $\pi_1(w_i) = a(\pi_2(w_i))$ for $i = 1, 2$. Consider first $w_1 = \sqrt{a}e_1$. Then,

$$\begin{aligned}
\pi_1(w_1) &= (\sqrt{a} \otimes 1)e_1\,; \\
\pi_2(w_2) &= (1 \otimes \sqrt{a})e_1 \text{ ; and} \\
a(\pi_2(w_2)) &= (\sqrt{a} \otimes \frac{1}{\sqrt{a}})\pi_2(w_1) = (\sqrt{a} \otimes \frac{1}{\sqrt{a}})(1 \otimes \sqrt{a})e_1 = (\sqrt{a} \otimes \frac{\sqrt{a}}{\sqrt{a}})e_1 \\
&= (\sqrt{a} \otimes 1)e_1 = \pi_1(w_1)\,.
\end{aligned}$$

Similarly, one can check that $w_2 = \sqrt{a}e_2$ satisfies the given condition. It remains to see that w_1, w_2 are linearly independent. The matrix associated to w_1, w_2 is $\begin{bmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{a} \end{bmatrix}$ which has determinant $a \neq 0$, hence these vectors are linearly independent and thus form a basis for $Y := \{w \in U_L \mid \pi_1(w) = a\pi_2(w)\}$.

We can now compute the twisting of $p = [1, x]$ by the cocyle $((t_1), ..., (t_r))$. Note that by definition $p(e_1) = 1$, $p(e_2) = x$. Then,

$$\begin{aligned}
p(w_1) &= p(\sqrt{a}e_1) = \sqrt{a}^2 p(e_1) = a\,; \\
p(w_2) &= p(\sqrt{a}e_2) = \sqrt{a}^2 p(e_2) = ax\,; \\
p(w_1 + w_2) &= p(\sqrt{a}(e_1 + e_2)) = \sqrt{a}^2 p(e_1 + e_2) = ax \text{ ; and} \\
b_p((w_1, w_2)) &= \sqrt{a}^2(p(e_1 + e_2) + p(e_1) + p(e_2)) = a(x + x + 1) = a\,.
\end{aligned}$$

Thus after twisting our form becomes $ay^2 + ayz + axz^2 = a(y^2 + yz + xz^2) = a[1, x] = t_1^{m_1} \cdots t_r^{m_r}[1, x]$.

5.2 Special Case - Type B_r

As we mentioned we will not use the orthogonal representation constructed in Chapter 4 to help us compute a lower bound for a group G of type B_r. Instead we use the following well known representation

$$\lambda \colon G \longrightarrow \mathrm{SO}(f) := \mathrm{O}^+(f) \subset \mathrm{GL}_{2r+1}\,,$$

where $f = [0,0] \oplus [0,0] \oplus .... \oplus [0,0] \oplus \langle 1 \rangle$ is a non-degenerate $2r+1$ dimensional quadratic form.

A maximal torus $T \subset G$ is a block matrix of size $2r+1 \times 2r+1$ which is of the form

$$\begin{bmatrix} \begin{bmatrix} t_1 & 0 \\ 0 & t_1^{-1} \end{bmatrix} & & & & \\ & \ddots & & & \\ & & \ddots & & \\ & & & \begin{bmatrix} t_r & 0 \\ 0 & t_r^{-1} \end{bmatrix} & \\ & & & & 1 \end{bmatrix} . \quad (\dagger)$$

Note that each 2×2 block preserves the form $[0,0]$ because

$$\begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = (tx, t^{-1}y)$$

and therefore we get $xy \longmapsto txt^{-1}y = tt^{-1}xy = xy$.

Now consider the element c of the Weyl Group of G which is a $2r+1 \times 2r+1$ block matrix consisting of 2×2 blocks of the form

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and whose bottom right entry is a 1. Note that c permutes t and t^{-1} for any $t \in T$ and has order 2, and therefore matches the definition of c defined in Section 1.2. Now we will twist the quadratic form f from above with respect to the cocycle $((t_1), ..., (t_r), (x))$ as we did in Section 5.1.

To do this we can repeat the exact same arguments as in the previous Section. The only thing which needs to be noted is that the basis for the character group $X(T)$ in our current case is different than before. It consists of the projections $\alpha_i \colon T \to \mathrm{G}_m$ which send $t \in T$ to t_i, where t is defined as matrix like in (†). Then, mimicking the reasoning from Section 5.1, we get that after twisting our quadratic form f becomes the orthogonal sum of $\langle 1 \rangle$ and binary quadratic forms of the shape $t_1^{m_1} \cdots t_r^{m_r}[1, x]$. Even more, we know that after twisting the quadratic form f is precisely

$$t_1[1, x] \oplus t_2[1, x] \oplus ... \oplus t_r[1, x] \oplus \langle 1 \rangle. \tag{5.1}$$

Chapter 6

Incompressibility of Canonical Monomial Forms

6.1 Introduction to Canonical Monomial Forms

Let k be an algebraically closed field of characteristic 2, $K := k(t_1, t_2, ..., t_n, x)$ a pure transcendental extension of k of transcendence degree $n+1$. Consider the quadratic form f over K defined as:

$$f := \oplus_{\mu \in F_2^n} m_f(\mu)\, t^\mu\, [1, x] \oplus \mathbb{H} \oplus \mathbb{H} \oplus ... \oplus \mathbb{H}\,, \tag{6.1}$$

where F_2 is the field with 2 elements, $\mu = (\mu_1, ..., \mu_n) \in F_2^n$, $t^\mu = t_1^{\mu_1} t_2^{\mu_2} \dots t_n^{\mu_n}$ and $m_f(\mu)$ the number of times a given summand appears. Note that $m_f(\mu)$ may be 0. We will refer to $m_f(\mu)$ as the multiplicity of the summand $t^\mu[1, x]$. We define a monomial quadratic form as any quadratic form of the shape (6.1).

The proof of the main Theorem in [Ar2] tells us that the Witt group of a field of characteristic 2 is a group of exponent 2, i.e. all elements have order 2. If a quadratic form gets sent to zero under the natural map $Quad(K) \to W_q(K)$, where $Quad(K)$ is the set of all quadratic forms over K, then by

the definition of the Grothendieck group it must be isometric to a sum of hyperbolic planes. Combining these two facts, $t^\mu[1,x] \oplus t^\mu[1,x]$ has a zero image in the Witt group of K and is therefore isomorphic to the direct sum of two copies of the hyperbolic plane, $\mathbb{H} \oplus \mathbb{H}$. So if $m_f(\mu) \geq 2$ we can apply the above replacement a finite number of times until $m_f(\mu) = 0$ or 1. Doing this, we get that f is isomorphic to

$$f := \oplus_{\mu \in F_2^n} m_f(\mu)\, t^\mu\, [1,x] \oplus \mathbb{H} \oplus .... \oplus \mathbb{H}\,,$$

where $m_f(\mu) = 0$ or 1. For all μ such that $m_f(\mu) = 1$, let V be the vector subspace of F_2^n generated by them. Choose a basis of V, say $\mu_1, \mu_2, ...\mu_s$. Then define $u_i = t^{\mu_i}$ for $i = 1, ..., s$. We know that any $\mu \in V$ can be written as $\mu = \sum_{i=1}^{s} \alpha_i u_i$ where $\alpha_i = 0$ or 1 so then $t^\mu = u_1^{\alpha_1} ... u_s^{\alpha_s}$. This allows us to conclude that the quadratic form f has descent to the field $k(u_1, ..., u_s, x) \subset k(t_1, ..., t_n, x)$ and viewing f over this field we may write:

$$f := u_1[1,x] \oplus u_2[1,x] \oplus ... \oplus u_s[1,x] \oplus_{\mu \in V} u^\mu[1,x] \oplus \mathbb{H} \oplus .... \oplus \mathbb{H}\,,$$

where u^μ is a monomial in the u_i of length at least 2. When a monomial quadratic form is written in such a way we say that it is a *canonical monomial form*. The main result in this Chapter is the following Theorem:

Theorem 6.1.1. *Let f be a canonical monomial form over $K := k(t_1, ..., t_n, x)$, i.e.*

$$f = t_1[1,x] \oplus ... \oplus t_n[1,x] \oplus_\mu t^\mu[1,x] \oplus \mathbb{H} \oplus ... \oplus \mathbb{H}.$$

Then f is an incompressible quadratic form.

We defer the proof of this Theorem to later on in the Chapter. The next two Sections will demonstrate why this is really a useful result.

6.2 Rank of Monomial Quadratic Forms

We saw in Section 6.1 that a monomial quadratic form was defined as a quadratic form of the shape

$$f := \oplus_{\mu \in F_2^n} m_f(\mu)\, t^\mu\, [1, x] \oplus \mathbb{H} \oplus \mathbb{H} \oplus ... \oplus \mathbb{H}\,,$$

where F_2 is the field with 2 elements, $\mu = (\mu_1, ..., \mu_n) \in F_2^n$ and $t^\mu = \prod t_i^{\mu_i}$. We saw previously that up to isomorphism we may assume that $m_f(\mu) = 0$ or 1. We then define the *rank* of a monomial quadratic form to be the rank of the F_2-subspace of F_2^n generated by all μ appearing above with $m_f(\mu) = 1$.

We would now like to determine the ranks of the twisted Killing forms we computed in Chapter 5. These of course are monomial quadratic forms. Note that after twisting, the portion of the Killing forms related to the Cartan subalgebra did not change and so are isometric to an orthogonal sum of hyperbolic planes and potentially a one-dimensional form $\langle 1 \rangle$. So these parts of the Killing forms will not play a part in the computation of rank.

Now for groups of type A_n, D_n, E_6, E_7, E_8 and G_2, all positive roots appeared when we computed the portion of their Killing forms not related to the Cartan subalgebra. That is, a binary quadratic form $[0, 0]$ defined on $L_\alpha = \langle X_\alpha, X_{-\alpha} \rangle$ appeared in the Killing form for all positive roots α; in particular, for all simple roots $\alpha_1, \ldots, \alpha_r$. As a result, the following binary quadratic forms appeared after twisting:

$$t_1[1, x],\ t_2[1, x], ..., t_n[1, x], \quad (*)$$

along with some others. These elements correspond to

$$(1, 0, ..., 0), (0, 1, 0, ..., 0), ..., (0, 0, ..., 1) \in F_2^n\,,$$

which clearly generate a subspace of rank n. Thus, the rank of the twisted Killing forms for these types is equal to the rank of the given simple algebraic group. Moreover, since all the summands of the form $(*)$ appear, these twisted Killing forms are not only monomial, but are in fact canonical monomial forms.

Next we deal with groups of type C_n. Here, for the portion of the Killing form not related to the Cartan subalgebra, only the long positive roots appeared. From the appendices of [Bo02] we get an explicit description of all long positive roots as:

$$\sum_{i \leq j < n} \alpha_j + \alpha_n \ \ (1 \leq i \leq n) \, .$$

For each long positive root we have a corresponding element $\mu \in F_2^n$. For example, $\alpha_j + \alpha_{j+1} + ... + \alpha_n$ corresponds to $(0, 0, ..., 0, 1, 1, ..., 1)$ where the first 1 occurs in the j-th position. So the long positive roots correspond to n elements in F_2^n. They are:

$$(1, 1, 1, ..., 1), (0, 1, 1, ..., 1), ..., (0, 0, ..., 0, 1) \ . \ (+)$$

We claim these are linearly independent. Indeed, if we compute the determinant of the matrix

$$\begin{bmatrix} 1 & 1 & 1 & ... & 1 \\ 0 & 1 & 1 & ... & 1 \\ : & : & : & : & : \\ 0 & 0 & ... & 0 & 1 \end{bmatrix}$$

it is clearly 1 because this is an upper triangular matrix. Thus, the elements listed in $(+)$ generate a subspace of dimension n and hence the twisted Killing form associated to groups of type C_n has rank n. Also, since this form has rank n, it can be turned into a canonical monomial form by the process described in Section 6.1.

We now turn to groups of type B_n. For the proof of Theorem 1.2.1 we really need to work with monomial quadratic forms which are of rank n. However

if we used the Killing form computed in Section 3.3 this would give us a monomial quadratic form of rank $n-1$. It is for this reason we use the so-called standard representation described in Section 5.2.

We recall equation (5.1) where we computed the twisted quadratic form to be

$$t_1[1,x] \oplus t_2[1,x] \oplus ... \oplus t_n[1,x] \oplus \langle 1 \rangle$$

which clearly has rank n, as desired.

For the same reason as for type B_n, we will not discuss the rank of the twisted, normalized Killing form for groups of type F_4. As mentioned previously, we will prove Theorem 1.2.1 for groups of type F_4 using an alternative method which is detailed in Section 7.2.

The key takeaway from this Section is that for simple algebraic groups of all types (except F_4) we have a quadratic form which can be turned into a canonical monomial form of rank equal to the rank of the group.

6.3 A Reduction of the Problem

When we computed Killing forms in Chapter 3 they were all of the form

$$\bigoplus_i [0,0] \oplus l\langle 0 \rangle \oplus m\langle 1 \rangle.$$

In Chapter 4 when we constructed the "non-degenerate Killing" representation we passed to the normalization of these Killing forms. Then by the discussion in Section 2.1 we know that these normalized Killing forms fall into one of two types:

$$\overline{q} \simeq \bigoplus_i [0,0] \oplus \langle 1 \rangle$$

or

$$\overline{q} \simeq \bigoplus_i [0,0].$$

As well, if $\langle 1 \rangle$ appears in the normalization $\overline{q}$, then by the explicit construction in Chapter 3 we know this term came from the Cartan subalgebra. In Chapter 5 we twisted these Killing forms and we saw that the portion of the Killing forms related to the Cartan subalgebra remained unchanged. So after twisting the term $\langle 1 \rangle$ remains unchanged. As well, the $[0,0]$ terms related to the Cartan subalgebra remained unchanged. On the other hand, the $[0,0]$ terms not related to the Cartan subalgebra became $t_1^{m_1} \cdots t_n^{m_n}[1,x] = t^m[1,x]$ after twisting.

So after twisting, our normalized Killing forms take on one of two forms:

$$\begin{aligned} &\bigoplus_{Cartan} [0,0] \oplus \bigoplus_{non-Cartan} t^m[1,x] \\ &\simeq \bigoplus_{Cartan} \mathbb{H} \oplus \bigoplus_{non-Cartan} t^m[1,x] \end{aligned}$$

or

$$\begin{aligned} &\langle 1 \rangle \oplus \bigoplus_{Cartan} [0,0] \oplus \bigoplus_{non-Cartan} t^m[1,x] \\ &\simeq \langle 1 \rangle \oplus \bigoplus_{Cartan} \mathbb{H} \oplus \bigoplus_{non-Cartan} t^m[1,x] \end{aligned}$$

where $\mathbb{H}$ as usual denotes the hyperbolic plane.

Now, the main goal of this Chapter is to prove the incompressibility of these normalized, twisted Killing forms. Assume that they have rank n. We would like first to show that if we can prove the incompressibility of

$$\bigoplus_{Cartan} \mathbb{H} \oplus \bigoplus_{non-Cartan} t^m[1,x],$$

then the incompressibility of

$$\langle 1 \rangle \oplus \bigoplus_{Cartan} \mathbb{H} \oplus \bigoplus_{non-Cartan} t^m[1,x]$$

will follow.

Indeed, suppose

$$q = \langle 1 \rangle \oplus \bigoplus_{Cartan} \mathbb{H} \oplus \bigoplus_{non-Cartan} t^m[1, x]$$

and assume it were compressible. This means there is a subfield $k \subset L \subset K$ with $\text{tr.deg}_k L \leq n$ and a quadratic form q' defined over L such that $q' \otimes_L K \simeq q$. Since q is odd-dimensional and non-degenerate so too must be q'. Then by Lemma 2.1.5 we can write

$$q' \simeq \langle a \rangle \oplus q'_0$$

where q'_0 is an even-dimensional form and $a \in L^\times$ is determined uniquely up to squares. Now since the $\langle 1 \rangle$ term in q is also determined uniquely up to squares and $q' \otimes_L K \simeq q$ it follows that $a \equiv 1 \pmod{K^2}$, i.e. a is a square in K. Now define the field $\widetilde{L} = L[\sqrt{a}]$. Because a is a square in K we get that $L \subset \widetilde{L} \subset K$. Also, since $\widetilde{L}/L$ is an algebraic extension, we have $\text{tr.deg}_k(L) = \text{tr.deg}_k(\widetilde{L})$. Thus, if q were compressible to q' defined over L, it must also be compressible to $\widetilde{q}' = q' \otimes_L \widetilde{L}$, which is defined over $\widetilde{L}$. However, in $\widetilde{L}$ a is equivalent to 1 mod squares, thus $\widetilde{q}' = \langle 1 \rangle \oplus \widetilde{q}'_0$ where $\widetilde{q}'_0$ is an even-dimensional form.

Now since $\widetilde{q}' \otimes_{\widetilde{L}} K \simeq q$ and both terms are made up of the sum of an even-dimensional form, plus the uniquely determined (up to isometry) 1-dimensional form $\langle 1 \rangle$, by [EKM, Proposition 7. 31], we can conclude that

$$\widetilde{q}'_0 \simeq \bigoplus_{Cartan} \mathbb{H} \oplus \bigoplus_{non-Cartan} t^m[1, x]$$

Thus if q is compressible so is

$$\bigoplus_{Cartan} \mathbb{H} \oplus \bigoplus_{non-Cartan} t^m[1, x]$$

and our claim follows.

Summarizing: to prove the incompressibility of our twisted, normalized

Killing forms, it is enough to prove Theorem 6.1.1. In the next Section we will highlight some results regarding the Witt group that will be needed to prove Theorem 6.1.1.

6.4 Preliminary Results

6.4.1 Decomposition inside the Witt Group in Characteristic 2

In this Section we will work with a field of Laurent series $K((s))$ where the coefficient field K is of characteristic 2. By Theorems 2.2.1 and 2.2.2, given a quadratic form f defined over $K((s))$, we may decompose its image in the Witt group as

$$f_W = f_{m,W} + f_{m-1,W} + ... + f_{0,W}$$

where $f_{i,W} \in W_q(K((s)))_i$. The following Lemma allows us to give a more precise description of these components.

Lemma 6.4.1. *Let $\{\alpha_i\}_{i=1}^N$ be a basis for K as a K^2-vector space. We can decompose $f_W = f_{m,W} + f_{m-1,W} + ... + f_{0,W}$ in such a way that it satisfies the following:*

If n is even,

$$f_{n,W} = \sum_{i<j} [\alpha_i, u_j^2 \alpha_j s^{-n}]_W + \sum_{i<j} [\alpha_i s^{-1}, v_j^2 \alpha_j s^{-n+1}]_W,$$

where $u_i, v_j \in K$. If n is odd,

$$f_{n,W} = \sum_{i,j=1}^{N} [\alpha_i, u_j^2 \alpha_j s^{-n}]_W,$$

where $u_j \in K$.

Proof. Suppose first that $n = 2m$ is even. Then

$$f_{2m,W} = \sum [p_i, q_i s^{-2m}]_W + \sum [p_i' s^{-1}, q_i' s^{-2m+1}]_W$$

where $p_i, q_i, p_i', q_i' \in K$. Since $\{\alpha_i\}_{i=1}^N$ is a basis for K/K^2 we get that $p_i = \sum_{i,j=1}^N e_{ij}^2 \alpha_j$ and similarly for the q_i, p_i', q_i'. Replacing the p_i, q_i, p_i', q_i' with these expressions and using the biadditivity of $[\ ,\ ]_W$ we get that:

$$\begin{aligned} f_{2m,W} \quad &= \quad \sum_{i,j=1}^N [u_i^2 \alpha_i, v_j^2 \alpha_j s^{-2m}]_W + \sum_{i,j=1}^N [u_i'^2 \alpha_i s^{-1}, v_j'^2 \alpha_j s^{-2m+1}]_W \\ &\overset{2.3a,2.3b}{=} \sum_{i,j=1}^N [\alpha_i, w_{ij}^2 \alpha_j s^{-2m}]_W + \sum_{i,j=1}^N [\alpha_i s^{-1}, w_{ij}'^2 \alpha_j s^{-2m+1}]_W. \end{aligned}$$

where $u_i, v_j, u_i', v_j' \in K$ and $w_{ij} = u_i v_j$, $w_{ij}' = u_i' v_j'$. If $i = j$ above we have that

$$[\alpha_i, w_{ii}^2 \alpha_i s^{-2m}]_W \overset{2.2a}{=} [\alpha_i, w_{ii} s^{-m}]_W$$

and

$$[\alpha_i s^{-1}, w_{ii}'^2 \alpha_i s^{-2m+1}]_W \overset{2.2b}{=} [\alpha_i s^{-1}, w_{ii}' s^{-m+1}]_W .$$

If $i > j$ we get that

$$[\alpha_i, w_{ij}^2 \alpha_j s^{-2m}]_W \overset{2.1a}{=} [\alpha_j, w_{ij}^2 \alpha_i s^{-2m}]_W$$

and

$$[\alpha_i s^{-1}, w_{ij}'^2 \alpha_j s^{-2m+1}]_W \overset{2.1b}{=} [\alpha_j s^{-1}, w_{ij}'^2 \alpha_i s^{-2m+1}]_W .$$

If $n = 2m-1$ is odd, following what we did in the even case, yields

$$\begin{aligned} f_{2m-1,W} &= \sum_{i,j=1}^{N} [u_i^2\alpha_i, v_j^2\alpha_j s^{-2m+1}]_W + \sum_{i,j=1}^{N} [u_i'^2\alpha_i s^{-1}, v_j'^2\alpha_j s^{-2m+2}]_W \\ &\overset{2.1c}{=} \sum_{i,j=1}^{N} [\alpha_i, w_{ij}^2\alpha_j s^{-2m+1}]_W + \sum_{i,j=1}^{N} [\alpha_j, w_{ij}'^2\alpha_i s^{-2m+1}]_W \\ &= \sum_{i,j=1}^{N} [\alpha_i, z_j^2\alpha_j s^{-2m+1}]_W \,. \end{aligned}$$

where $u_i, v_j, u_i', v_j' \in K$, $w_{ij} = u_i v_j$, $w_{ij}' = u_i' v_j'$ and $z_j \in K$. The last equality follows from the biadditivity of $[\ ,\ ]_W$. □

Theorem 6.4.2. *Given a quadratic form f, its image in the Witt group can be decomposed uniquely up to isometry as $f_W = f_{n,W} + f_{n-1,W} + ... + f_{0,W}$, where $f_{n,W}, ..., f_{0,W}$ are as in Lemma 6.4.1.*

Proof. We already know by the previous Theorem that a decomposition exists, so we only need to prove uniqueness. Suppose

$$f_W = f_{n,W} + f_{n-1,W} + ... + f_{0,W} = f'_{m,W} + f'_{m-1,W} + ... + f_{0,W}$$

are 2 different decompositions of f_W. We first claim that $n = m$. Suppose not. Then without loss of generality we may assume $n > m$. Let us compare the images of these decompositions in the quotient group $W_q(K((s)))_n / W_q(K((s)))_{n-1}$. $f'_{m,W} + f'_{m-1,W} + ... + f_{0,W}$ equals 0 whereas the other decompostion has image $f_{n,W}$. We consider separately the cases n is even and odd.

<u>n is even:</u> Here we may write

$$f_{n,W} \overset{6.4.1}{=} \sum_{i<j} [\alpha_i, u_j^2\alpha_j s^{-n}]_W + \sum_{i<j} [\alpha_i s^{-1}, v_j^2\alpha_j s^{-n+1}]_W$$

and

$$\Phi \colon W_q(K((s)))_n / W_q(K((s)))_{n-1} \overset{2.2.2}{\simeq} K \wedge_{K^2} K \oplus K \wedge_{K^2} K \,.$$

Then we have that

$$\Phi(f_{n,W}) = \left(\sum_{i<j} u_j^2(\alpha_i \wedge \alpha_j), \sum_{i<j} v_j^2(\alpha_i \wedge \alpha_j) \right) .$$

Since $\{\alpha_i \wedge \alpha_j\}_{i<j}$ is a basis for $K \wedge_{K^2} K$, $\Phi(f_{n,W}) = 0 \Leftrightarrow u_j^2 = v_j^2 = 0 \ \forall \ j$. This would imply that $f_{n,W} = 0$, a contradiction.

<u>n is odd:</u> Here we may write

$$f_{n,W} \overset{6.4.1}{=} \sum_{i,j=1}^{N} [\alpha_i, u_j^2 \alpha_j s^{-n}]_W$$

and

$$\phi \colon W_q(K((s)))_n / W_q(K((s)))_{n-1} \overset{2.2.2}{\simeq} K \otimes_{K^2} K \, .$$

Then we have that

$$\phi(f_{n,W}) = \sum_{i,j=1}^{N} u_j^2(\alpha_i \otimes \alpha_j) \, .$$

Since $\{\alpha_i \otimes \alpha_j\}_{i,j=1}^{N}$ is a basis for $K \otimes_{K^2} K$, $\phi(f_{n,W}) = 0 \Leftrightarrow u_j^2 = 0 \ \forall \ j$, a contradiction.

Thus $n = m$. If $n = 0$ there is nothing to prove so we may assume that $n \geq 1$. In particular we now know that in either decomposition f has the same image in $W_q(k((s)))_n / W_q(k((s)))_{n-1}$. If n is even, $\Phi(f_{n,W}) = \Phi(f'_{n,W})$

$$\begin{aligned} &\Rightarrow \ \sum u_j^2(\alpha_i \wedge \alpha_j) = \sum u_j'^2(\alpha_i \wedge \alpha_j) \text{ and } \sum v_j^2(\alpha_i \wedge \alpha_j) = \sum v_j'^2(\alpha_i \wedge \alpha_j) \\ &\Leftrightarrow \ u_j^2 = u_j'^2 \text{ and } v_j^2 = v_j'^2 \Leftrightarrow f_{n,W} = f'_{n,W} \, . \end{aligned}$$

Similarly we can see that $f_{n,W} = f'_{n,W}$ in the case that n is odd. Putting everything together we have that

$$\begin{aligned} (f_{0,W} + ... + f_{n-1,W}) + f_{n,W} &= (f'_{0,W} + ... + f'_{n-1,W}) + f'_{n,W} \\ \overset{2.1.7}{\Rightarrow} f_{0,W} + ... + f_{n-1,W} &= f'_{0,W} + ... + f'_{n-1,W} \, . \end{aligned}$$

By induction, the proof is completed. □

6.4.2 Anisotropicity of Canonical Monomial Forms

Theorem 6.4.3. *Let f be a canonical monomial form defined over $K := k(t_1, ..., t_n, x)$ without any summands isometric to the hyperbolic plane. Then f is anisotropic.*

Proof. Assume the contrary. Then there exist $g_1, ...g_s \in k[t_1, ..., t_n, x]$ such that $f(g_1, ..., g_s) = 0$. We may assume from the outset that $g_1, ..., g_s$ are coprime.

Consider first the case when $n = 1$ and $f = t_1[1, x] \overset{2.2.5}{=} [t_1^{-1}, xt_1]$. By Lemma 2.2.6 this form is isotropic if and only if $(t_1^{-1})(xt_1) = x$ is in the image of the map $\wp\colon K \to K$ which sends $y \to y + y^2$.

Suppose that there is $p/q \in k(t_1, x)$ such that $\wp(p/q) = p^2/q^2 + p/q = x$ or equivalently $p(p + q) = xq^2$. Assume without loss of generality that p/q is reduced, i.e. p, q are relatively prime. We have two cases to consider. First assume that q is non constant. Let h be any irreducible factor of q. Clearly it divides the right hand side so it must also divide the left. Since it can't divide p by assumption it must divide $p + q$. But then $h|p + q, h|q$ so we also get $h|p + q - q = p$, but this contradicts the fact that p, q are relatively prime.

Now assume q is constant, say $q = 1$. The right hand side becomes x and so it is of degree 1. The left hand side becomes $p^2 + p$. If x does not appear in the expression of p, then it cannot appear in $p^2 + p$, thus we cannot have equality. If x appears in p with degree ≥ 1, then x appears in $p^2 + p$ with degree at least 2, a contradiction.

We may now assume that $f = t_1[1, x] \oplus [1, x]$ or f is a canonical monomial form defined over $K := k(t_1, ..., t_n, x)$ where $n \geq 2$. The commonality amongst all these cases is that in f there are summands which both include

and omit t_1. If $f(g_1, ..., g_s) = 0$ we may separate those terms which include and omit the indeterminate t_1 to write:

$$\begin{aligned} 0 &= \left(\bigoplus_{\mu \in \Gamma_1} t^\mu[1, x] \oplus \bigoplus_{\mu \in \Gamma_2} t^\mu[1, x] \right) (g_1, ..., g_s) \\ &= \sum_{\mu \in \Gamma_1} t^\mu (g_i^2 + g_i g_{i+1} + x g_{i+1}^2) + \sum_{\mu \in \Gamma_2} t_1 t^{\tilde{\mu}} (g_j^2 + g_j g_{j+1} + x g_{j+1}^2) \,, \end{aligned}$$

where $t^{\tilde{\mu}} = (t_1^{-1}) t^\mu$, $\Gamma_1 = \{\mu \in F_2^n \text{ such that } \mu_1 = 0\}$, i.e. those t^μ omitting t_1 and $\Gamma_2 = \{\mu \in F_2^n \text{ such that } \mu_1 = 1\}$, i.e. those t^μ which include t_1.

$$\Rightarrow \sum_{\mu \in \Gamma_1} t^\mu (g_i^2 + g_i g_{i+1} + x g_{i+1}^2) = \sum_{\tilde{\mu} \in \Gamma_1} t_1 t^{\tilde{\mu}} (g_j^2 + g_j g_{j+1} + x g_{j+1}^2) \ . (\dagger)$$

Since the g_i are polynomials in $k[t_1, ..., t_n, x]$ the above equality will continue to hold if we evaluate at $t_1 = 0$. Doing so yields:

$$\sum_{\mu \in \Gamma_1} t^\mu (\widetilde{g_i}^2 + \widetilde{g_i} \widetilde{g}_{i+1} + x \widetilde{g_{i+1}^2}) = 0 \,,$$

where $\widetilde{g_i}$ is g_i evaluated at $t_1 = 0$ and the equality occurs in $k[0, t_2, ..., t_n, x] \simeq k[t_2, ..., t_n, x]$. We have two possible cases to consider: Case 1: There is a non-zero $\widetilde{g_i}$ or Case 2: $\widetilde{g_i} = 0 \ \forall \ i$. If we are in the first case, this tells us that the quadratic form $\bigoplus_{\mu \in \Gamma_1} t^\mu[1, x]$ is isotropic. However, since t_1 does not appear in any of the t^μ, this quadratic form is defined over $k(t_2, ..., t_n, x)$ and by induction must be anisotropic. This gives us a contradiction. The second case could only occur if each g_i were divisible by t_1. Replacing the g_i appearing on the left hand side of $(\dagger)$ with $t_1 g_i'$ yields:

$$\begin{aligned} & \sum_{\mu \in \Gamma_1} t^\mu ((t_1 g_i')^2 + t_1 g_i' t_1 g_{i+1}' + x (t_1 g_{i+1}')^2) = \sum_{\tilde{\mu} \in \Gamma_1} t_1 t^{\tilde{\mu}} (g_j^2 + g_j g_{j+1} + x g_{j+1}^2) \\ \Rightarrow & \sum_{\mu \in \Gamma_1} t_1^2 \left(t^\mu (g_i'^2 + g_i' g_{i+1}' + x g_{i+1}'^2) \right) = \sum_{\tilde{\mu} \in \Gamma_1} t_1 t^{\tilde{\mu}} (g_j^2 + g_j g_{j+1} + x g_{j+1}^2) \,. \end{aligned}$$

Dividing both side of this equation by t_1 and evaluating at $t_1 = 0$ tells us

that:

$$0 = \sum_{\mu \in \Gamma_2} t^{\tilde{\mu}} (\widetilde{g}_j^2 + \widetilde{g}_j \widetilde{g}_{j+1} + x \widetilde{g}_{j+1}^2) \, .$$

Then again we have the two cases we mentioned above. Following the same argument as before, if at least one $\widetilde{g_j} \neq 0$ our induction hypothesis leads to a contradiction. So assume $\widetilde{g_j} = 0 \; \forall \; j$. This can only occur if each g_j is divisible by t_1. But this now means that t_1 divides all of $g_1, ..., g_s$, contradicting our initial assumption that they were coprime. $\square$

6.5 Proof of Theorem 6.1.1

Before proceeding to the proof Theorem 6.1.1 we will first recall some useful ideas related to differential bases and coefficient fields. We will then cover a series of results which will culminate in the proof of this Theorem.

6.5.1 Differential Bases and Coefficient Fields

Let K/k be a finitely generated field extension, where k is an algebraically closed field of characteristic 2. As usual, $\Omega_{K/k}$ denotes the K-vector space of Kähler differentials. We define a *differential basis* for K/k to be a set of elements $\{ \alpha_i \}_{i \in I}$ such that $\{ d\alpha_i \} \subset \Omega_{K/k}$ is a vector space basis.

We say that a set of elements $\{ x_\lambda \}_{\lambda \in \Lambda} \subset K$ is a 2-*basis* for K over k if the set W of monomials in the x_λ having degree < 2 in each x_λ separately, forms a vector space basis for K over the subfield $k \cdot K^2 = K^2 \subset K$.

We now collect a series of results from [Ei, Ch16 and A1.3] and present them as a Lemma for later use:

Lemma 6.5.1. *We have the following results related to differential bases and* 2*-bases:*

1. *Any separating transcendence basis for K over k is a* 2*-basis.*

2. *If B is a 2-basis for K over k, then B is a separating transcendence basis for K/k.*

3. *A differential basis B for K/k is a separating transcendence basis for K/k.*

4. *Any separating transcendence basis for K over k is a differential basis.*

5. *A differential basis B for K/k is a 2-basis and conversely.*

Now, let R be a complete discrete valuation ring (DVR) containing our algebraically closed, characteristic 2 field k, with maximal ideal I. Denote its quotient field by K and its residue field by $\overline{K}$. It follows from the Cohen Structure Theorem [Ei, Thm 7.7] that $R \simeq \overline{K}[[x]]$ and $K \simeq \overline{K}((x))$. It is important to note that such a decomposition is not unique. In particular, the decomposition depends on the choice of a coefficient field in K, i.e. a field contained in R that maps isomorphically onto $\overline{K}$ under the canonical map $R \to \overline{K}$. Such coefficient fields do exist because the field extension $\overline{K}/k$ is separable. The following Theorem describes all coefficient fields.

Theorem 6.5.2. *Let R be as above. If B is a differential basis for $\overline{K}$ over k, then there is one-to-one correspondence between coefficients fields $\widetilde{E} \subset R$ containing k and sets $\widetilde{B} \subset R$ of representatives for B.*

Proof. See [Ei, Theorem 7.8]. □

6.5.2 The Module of Differentials for Discrete Valuation Rings

Let R be a DVR (not necessarily complete) with quotient field K and residue field $\overline{K}$. Assume that R contains k. Let π be a uniformizer and define $I = (\pi)$. Then we have a canonical k-map $\phi\colon R \to \overline{K}$, $x \to \bar{x}$ whose kernel is I. Abusing notation we denote $\phi(k)$ by k. We will assume that $\overline{K}/k$ has transcendence degree n and hence the field extension K/k has transcendence degree $n+1$ by [Bo72, Ch.6, §8].

Proposition 6.5.3. (Conormal sequence) *The following sequence*

$$I/I^2 \xrightarrow{d} \overline{K} \otimes_R \Omega_{R/k} \xrightarrow{D_\phi} \Omega_{\overline{K}/k} \longrightarrow 0,$$

where the right-hand side map is given by $D_\phi(a \otimes db) = a \cdot d\bar{b}$ *and the left-hand side map takes the class* $f + I^2$ *to* $1 \otimes df$*, is an exact sequence of* $\overline{K}$ *modules.*

Proof. See [Ei, Prop. 16.3]. □

Corollary 6.5.4. *Let* $d\bar{a}_1, \ldots, d\bar{a}_n$ *be a* $\overline{K}$*-basis of* $\Omega_{\overline{K}/k}$*. Then the set*

$$\{\, 1 \otimes d\pi, 1 \otimes da_1, \ldots, 1 \otimes da_n \,\} \tag{6.2}$$

is a $\overline{K} - basis\ of\ \overline{K} \otimes \Omega_{R/k}$*.*

Proof. It follows immediately from Proposition 6.5.3 that the set (6.2) is a system of generators of the $\overline{K}$-vector space $\overline{K} \otimes \Omega_{R/k}$, hence it suffices to establish that it consists of linearly independent vectors.

Let $\bar{b}_1, \ldots, \bar{b}_{n+1} \in \overline{K}$ be such that

$$\bar{b}_1(1 \otimes da_1) + \ldots + \bar{b}_n(1 \otimes da_n) + \bar{b}_{n+1}(1 \otimes d\pi) = 0.$$

Applying D_ϕ we conclude that $\bar{b}_1 = \ldots = \bar{b}_n = 0$. Then $\bar{b}_{n+1} \otimes d\pi = 0$. Assume that $\bar{b}_{n+1} \neq 0$. Note that by [Ei, Cor. 16.13] the map d is injective. Therefore

$$\begin{aligned} 0 &\neq 1 \otimes d(b_{n+1}\pi) \\ &= 1 \otimes b_{n+1} \cdot d\pi + 1 \otimes \pi \cdot db_{n+1} \\ &= \bar{b}_{n+1} \otimes d\pi + \bar{\pi} \otimes db_{n+1} \\ &= 0 + 0 = 0, \end{aligned}$$

a contradiction completing the proof. □

Proposition 6.5.5. *Assume that* R *is the localization of a finitely generated* k*-algebra. Then* $\Omega_{R/k}$ *is a free* R*-module of rank* $n + 1$*.*

Proof. Since $\Omega_{R/k}/I\Omega_{R/k} \simeq \Omega_{R/k} \otimes_R \overline{K}$ is generated by the set (6.2) consisting of $n+1$ elements, it follows from Nakayama's Lemma [Ei, Cor 4.8] that $\Omega_{R/k}$ is also generated by $n+1$ elements, namely $d\pi, da_1, \ldots, da_n$. Then there exists an exact sequence of R-modules

$$0 \longrightarrow M \longrightarrow R^{n+1} \longrightarrow \Omega_{R/k} \longrightarrow 0.$$

Since K/R is flat, tensoring by K we get an exact sequence

$$0 \longrightarrow M \otimes_R K \longrightarrow K^{n+1} \longrightarrow \Omega_{R/k} \otimes_R K \longrightarrow 0.$$

Since the formation of differentials commutes with localization [Ei, Prop. 16.9], it follows $\Omega_{K/k} \simeq \Omega_{R/k} \otimes_k K$. Since K/k is separable, $\Omega_{K/k}$ is a K-vector space of dimension $n+1$. It follows that $\Omega_{R/k} \otimes_R K$ is a K-vector space of dimension $n+1$ and hence $M \otimes_R K = 0$. But M has no torsion and therefore $M = 0$. □

The following Corollary follows immediately from the proof of the Proposition.

Corollary 6.5.6. *Let $a_1, \ldots, a_n \in R$ be such that $\{\bar{a}_1, \ldots, \bar{a}_n\}$ is a differential basis of $\Omega_{\overline{K}/k}$. Then, $\{\pi, a_1, \ldots, a_n\}$ is a differential basis for $\Omega_{R/k}$.*

We should also note that our argument shows $\{d\pi, da_1, \ldots, da_n\}$ is a K-basis of the K-vector space $\Omega_{K/k}$.

Before proceeding, we need the following definition. We say that a differential basis $\{a_1, a_2, \ldots, a_{n+1}\}$ for K/k *comes from* $\overline{K}$ if a_{n+1} is a uniformizer of K and $a_1, \ldots, a_n \in R$ are such that $\{\bar{a}_1, \ldots, \bar{a}_n\}$ is a differential basis for $\overline{K}/k$.

6.5.3 A Key Result

Let $K = k(x, t_1, \ldots, t_n)$ be a pure transcendental extension of k of degree $n+1$. Also, let ν be the valuation on $K = k(x, t_1, ..., t_n)$ associated to t_1. It is characterized by:

$$\nu(t_1) = 1 \text{ and } \nu(h) = 0 \quad \forall\ h \in k(x, t_2, ..., t_n)^{\times}\,.$$

For notational convenience we write $t_1 = \pi$, so we may use the two interchangeably. Let $R \subset K$ be the corresponding discrete valuation ring. Note that $K^2 \subset K$ is a finite field extension of degree 2^{n+1}. If $a_{i_1}, \ldots, a_{i_l} \in K$, we will denote the subfield generated by K^2 and $a_{i_1}, \ldots, a_{i_l}$ by $K^2(a_{i_1}, \ldots, a_{i_l}) \subset K$

Lemma 6.5.7. *Let $\{a_1, \ldots, a_n, \pi\}$ be a differential basis for K/k coming from $\overline{K}$. Let $w \in R$. If*

$$w = \sum c^2_{\epsilon_1,\ldots,\epsilon_n} a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} + \pi(\sum d^2_{\nu_1,\ldots,\nu_n} a_1^{\nu_1} \cdots a_n^{\nu_n})$$

with $\epsilon_1, \ldots, \epsilon_n, \nu_1, \ldots, \nu_n \in \{0, 1\}$ and $c_{\epsilon_1,\ldots,\epsilon_n}$, $d_{\nu_1,\ldots,\nu_n} \in K$, then all of $c_{\epsilon_1,\ldots,\epsilon_n}$ and $d_{\nu_1,\ldots,\nu_n}$ are contained in R.

Proof. If one of $c_{\epsilon_1,\ldots,\epsilon_n}$ or $d_{\nu_1,\ldots,\nu_n}$ is in $K \setminus R$, then multiplying the above equality by an appropriate power of π we get

$$\pi^{2s} w = \sum (c'_{\epsilon_1,\ldots,\epsilon_n})^2 a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} + \pi(\sum (d'_{\nu_1,\ldots,\nu_n})^2 a_1^{\nu_1} \cdots a_n^{\nu_n}) \tag{6.3}$$

with $s > 0$, $c'_{\epsilon_1,\ldots,\epsilon_n}$, $d'_{\nu_1,\ldots,\nu_n} \in R$ and at least one of the c' or d' which appear is a unit. Passing to equivalence classes modulo π we have

$$\sum (\bar{c'}_{\epsilon_1,\ldots,\epsilon_n})^2 \bar{a}_1^{\epsilon_1} \cdots \bar{a}_n^{\epsilon_n} = 0.$$

However, by Lemma 6.5.1 $\{\bar{a}_1, \ldots, \bar{a}_n\}$ is a 2-basis for $\overline{K}$, hence all coefficients $c'_{\epsilon_1,\ldots,\epsilon_n}$ are divisible by π. Then cancelling π in (6.3) and arguing similarly we conclude that all $d'_{\nu_1,\ldots,\nu_n}$ are divisible by π – a contradiction. □

Theorem 6.5.8. *Let $F \subset K$ be a subfield with* $\mathrm{tr.deg}_k(F) < n+1$. *There exists a differential basis $B = \{a_1, \ldots, a_{n+1}\}$ for $\Omega_{K/k}$ coming from $\overline{K}$ such that $F \subset K^2(a_{i_1}, , \ldots, a_{i_l})$ where $l < n+1$.*

Proof. Without loss of generality we may assume that $\mathrm{tr.deg}_k(F) = n$. Since k is perfect there exists a differential basis $\{a'_1, \ldots, a'_n\}$ for $\Omega_{F/k}$ consisting of n elements with $a'_i \in R$ for all $i = 1, \ldots, n$. Note that

$$F = F^2(a'_1, \ldots, a'_n) \subset K^2(a'_1, \ldots, a'_n)$$

(the equality is due to Lemma 6.5.1). Let $\widetilde{F} = k(a'_1, \ldots, a'_n)$. Then $F \subset F^2 \cdot \widetilde{F}$, hence it suffices to prove the assertion for $\widetilde{F}$. Thus, replacing F with $\widetilde{F}$ if necessary, we may assume that $F = k(a'_1, \ldots, a'_n)$.

We next remark that without loss of generality we can also modify any a'_i by multiplying it by any square in $K^\times$. It easily follows from this remark that we can additionally assume that all a'_i, $i = 1, \ldots, n-1$ are units and that the last element a'_n is either a unit or a uniformizer for ν. Lastly, we can take an algebraic closure of F in K and after that we arrive to the field which we still denote by F with the properties:

1. $\mathrm{tr.deg}_k(F) = n$;
2. F is algebraically closed in K;
3. F contains a differential basis $\{a'_1, \ldots, a'_n\}$ such that a'_i, $i = 1, \ldots, n-1$, are units and that the last element a'_n is either a unit or a uniformizer.

We consider the case when a'_n is a uniformizer only. The case when a'_n is a unit can be treated along the same lines. In this case we set $a_{n+1} = a'_n$. Up to numbering we may also assume that $d\bar{a}'_1, \ldots, d\bar{a}'_i$ viewed as elements of the $\overline{K}$-vector space $\Omega_{\overline{K}/k}$ are linearly independent and that other $d\bar{a}'_j$ with $j > i$ are linear combinations of $d\bar{a}'_1, \ldots, d\bar{a}'_i$. We set $a_1 = a'_1, \ldots, a_i = a'_i$.

If $i = n-1$, then letting a_n to be any element in R with the property that

$\{\bar{a}_1, \ldots, \bar{a}_{n-1}, \bar{a}_n\}$ is a differential basis for $\Omega_{\overline{K}/k}$ we get, by Corollary 6.5.6, that

$$B = \{a_1, \ldots, a_n, a_{n+1}\}$$

is a differential basis for $\Omega_{R/k}$ (and hence for $\Omega_{K/k}$) coming from $\overline{K}$ and we are done.

Let $i < n-1$. Choose $\bar{b}_{i+1}, \ldots, \bar{b}_n \in \overline{K}$ such that

$$\{\bar{a}_1, \ldots, \bar{a}_i, \bar{b}_{i+1}, \ldots, \bar{b}_n\} \tag{6.4}$$

is a differential basis for $\overline{K}/k$. By Corollary 6.5.6, the set

$$\{a_1, \ldots, a_i, b_{i+1}, \ldots, b_n, \pi\}$$

is a differential basis of $\Omega_{K/k}$ coming from $\overline{K}$.

Write a'_{i+1} in the form

$$a'_{i+1} = \sum c^2_{\epsilon_1,\ldots,\epsilon_n} a_1^{\epsilon_1} \cdots a_i^{\epsilon_i} b_{i+1}^{\epsilon_{i+1}} \cdots b_n^{\epsilon_n} + \pi(\sum d^2_{\nu_1,\ldots,\nu_n} a_1^{\nu_1} \cdots a_i^{\nu_i} b_{i+1}^{\nu_{i+1}} \cdots b_n^{\nu_n})$$

Since a'_{i+1} is a unit, Lemma 6.5.7 tells us that $c_{\epsilon_1,\ldots,\epsilon_n}$, $d_{\nu_1,\ldots,\nu_n}$ are contained in R. Then passing to equivalence classes modulo π we have

$$\bar{a}'_{i+1} = \sum \bar{c}^2_{\epsilon_1,\ldots,\epsilon_n} \bar{a}_1^{\epsilon_1} \cdots \bar{a}_i^{\epsilon_i} \bar{b}_{i+1}^{\epsilon_{i+1}} \cdots \bar{b}_n^{\epsilon_n}.$$

If one of $\epsilon_{i+1}, \ldots, \epsilon_n$, say ϵ_s, was not 0 and the corresponding coefficient $\bar{c}_{\epsilon_1,\ldots,\epsilon_n} \neq 0$ we would get that

$$\{\bar{a}'_{i+1}, \bar{a}_1, \ldots, \bar{a}_i, \bar{b}_{i+1}, \ldots, \bar{b}_{s-1}, \bar{b}_{s+1}, \ldots, \bar{b}_n\}$$

is a 2-basis for $\overline{K}/k$ and in particular $d\bar{a}_1, \ldots, d\bar{a}_i, d\bar{a}'_{i+1}$ would be linearly independent in $\Omega_{\overline{K}/k}$ – a contradiction. Thus

$$\bar{a}'_{i+1} = \sum \bar{c}^2_{\epsilon_1,\ldots,\epsilon_n} \bar{a}_1^{\epsilon_1} \cdots \bar{a}_i^{\epsilon_i}. \tag{6.5}$$

Since $\bar{a}'_{i+1}, \ldots, \bar{a}'_1$ are linearly independent in $\Omega_{\overline{F}/k}$ one of the coefficients $\bar{c}_{\epsilon_1,\ldots,\epsilon_n}$ is not contained in $\overline{F}$. Up to numbering we may assume that $\bar{c} = \bar{c}_{1,0,\ldots,0} \notin \overline{F}$. Up to replacing a'_{i+1} by an element

$$a'_{i+1} - (\sum c^2_{\epsilon_1,\ldots,\epsilon_n} a_1^{\epsilon_1} \cdots a_i^{\epsilon_i})'$$

(and thus passing to a new field F satisfying the above properties (1), (2), (3)) where $'$ means that the term $c^2_{1,0\ldots,0}a_1$ is missing, we arrive to the situation when

$$\bar{a}'_{i+1} = \bar{c}^2 \bar{a}_1$$

with $\bar{c} \notin \overline{F}$. The following claim says that this is impossible.

Claim: c is algebraic over F and hence $c \in F$.

Indeed, assume that $F(c)$ is a pure transcendental extension of F. To get a contradiction it suffices to show that the restriction $w = \nu|_{k(c)}$ is trivial on $k(c)$. But if $w \neq 1$ then $\overline{k(c)} = k$ (because k is algebraically closed) implying $\bar{c} \in k \subset \overline{F}$ – a contradiction completing the proof. □

6.5.4 Residue Operators

We now switch notation, letting K denote an arbitrary field of characteristic 2 and define $L = K((s))$ to be the field of formal Laurent series over K. Recall that Lemma 2.2.1 gives an infinite filtration

$$W_q(K((s)))_0 \subset W_q(K((s)))_1 \subset \cdots W_q(K((s)))_n \subset \cdots \subset W_q(K((s)))$$

of the quadratic Witt group of $K((s))$. In this Section we will focus on the zero term $W_q(K((s)))_0$ only. It is generated by quadratic forms $[\alpha, \beta]_W$ and $[\alpha s^{-1}, \beta s]_W \simeq s[\alpha, \beta]_W$ with $\alpha, \beta \in K$. By Lemma 2.2.2 we have

$$W_q(K((s)))_0 \simeq W_q(K) \oplus W_q(K).$$

Under this isomorphism $[\alpha,\beta]_W$ is sent to $[\alpha,\beta]_W$ in the first summand and $s[\alpha,\beta]_W$ is sent to $[\alpha,\beta]_W$ in the second summand. This gives rise to two natural maps

$$\partial_1 \colon W_q(K((s)))_0 \to W_q(K) \text{ and } \partial_2 \colon W_q(K((s)))_0 \to W_q(K),$$

which we call the *first residue* and the *second residue* respectively.

The aim of this Subsection is to show that the first residue doesn't depend on the presentation $L = K((s))$, i.e. it doesn't depend on the choice of a coefficient field $\widetilde{K} \subset L$ and a choice of a uniformizer of L. We will also show that the second residue is defined up to similarity only.

First, let $\pi \in L$ be an arbitrary uniformizer. Then, $\pi = su^{-1}$ for some unit u where $u = u_0 + u_1 s + u_2 s^2 + \cdots$ with $u_i \in K$. Note that we can write $u = u_0 + u'$ where u' is divisible by s. Clearly the choice of π doesn't affect generators of $W_q(K((s)))_0$ of the form $[\alpha,\beta]_W$ (because $\alpha,\beta \in K$). As for generators of the form $s[\alpha,\beta]_W$, we have the following equivalence of quadratic forms:

$$\begin{aligned} s[\alpha,\beta]_W &= \pi u[\alpha,\beta]_W = \pi[\alpha u^{-1}, \beta u]_W \\ &= \pi[\alpha(u_0+u')^{-1}, \beta(u_0+u')]_W \overset{Lm.\,2.2.3}{=} \pi[\alpha u_0^{-1}, \beta u_0]_W \\ &= \pi u_0[\alpha,\beta]_W. \end{aligned}$$

Thus the second residues for the uniformizers s and π differ by a scalar $u_0 \in K$.

Now let $\widetilde{K} \subset L$ be an arbitrary coefficient field so that $L \simeq \widetilde{K}((s)))$. Recall that by definition $\widetilde{K} \subset K[[s]]$ and that it maps isomorphically onto K under the canonical map $K[[s]] \to K$. Let $\widetilde{\alpha}, \widetilde{\beta} \in \widetilde{K}$ be such that $\widetilde{\alpha} \to \alpha$ and $\widetilde{\beta} \to \beta$. Then we have $\widetilde{\alpha} = \alpha + \alpha_1 s + \alpha_2 s^2 + \cdots$ and $\widetilde{\beta} = \beta + \beta_1 s + \beta_2 s^2 + \cdots$.

Here $\alpha_i, \beta_i \in K$. Therefore

$$[\widetilde{\alpha}, \widetilde{\beta}]_W = [\alpha + \alpha_1 s + \cdots\ ,\ \beta + \beta_1 s + \cdots]_W \overset{Lm.\,2.2.3}{\simeq} [\alpha, \beta]_W.$$

Similarly, we have $s[\widetilde{\alpha}, \widetilde{\beta}]_W \simeq s[\alpha, \beta]_W$. It follows that the first and second residues don't depend on the choice of a coefficient field.

6.5.5 Proof of Incompressibility

We are now ready to carry out the proof of Theorem 6.1.1. All notation in this Subsection is the same as defined in Section 6.1. We will proceed by induction on the transcendence degree n of $K = k(t_1, ..., t_n, x)$ over $k(x)$. The base of induction, $n = 0$, follows easily.

Lemma 6.5.9. *Let $K = k(x)$ and let $f = [1, x] \oplus \mathbb{H} \oplus \cdots \oplus \mathbb{H}$. Then f is incompressible.*

Proof. Assume the contrary. Any subfield of K of transcendence degree 0 over k coincides with k, because k is algebraically closed. Hence, if f were compressible then it would be defined over k and in particular it would be hyperbolic. This would imply it has a zero image in the Witt Group $W_q(K)$. However, by Theorem 6.4.3 $[1, x]$ is anisotropic and therefore f has non-zero image in $W_q(K)$, giving us a contradiction and completing the proof. □

Now let $n > 0$ and suppose that Theorem 6.1.1 is proved for all canonical monomial quadratic forms of rank $< n$. We can define a valuation ν on K associated to t_1 as in Subsection 6.5.3. As a matter of notation let $\pi := t_1$, so we may use them interchangeably. As usual $\widehat{K}$ will denote the completion of K with respect to this valuation and $\overline{K}$ will denote the residue field. We also set $K_1 = k(t_2, \ldots, t_n, x)$.

Suppose that f were compressible. Then there would exist a field F (which we can assume has transcendence degree n over k) and a quadratic form g over F satisfying: $k \subset F \subset K$ and $g_K \simeq f$.

Lemma 6.5.10. *The image f_W of f in the Witt group $W_q(\widehat{K})$ lives in $W_q(\widehat{K})_0$. Its image under the isomorphism $\varphi\colon W_q(\widehat{K})_0 \xrightarrow{\sim} W_q(\overline{K}) \oplus W_q(\overline{K})$ is*

$$(\sum[(t_{i_1})^{-1}\dots(t_{i_l})^{-1}, xt_{i_1}\dots t_{i_l}]_W, \sum[t_{i_1}\dots t_{i_m}, x/t_{i_1}\dots t_{i_m}]_W)\,,$$

where $2 \le i_1 < i_2 < ... < i_l, i_m \le n$. In particular the first residue of f is a canonical monomial form of rank $n-1$ and the second residue of f, up to similarity, is a nontrivial monomial form of rank $\le n-1$.

Proof. A general summand of f_W can be split into two cases:

Case 1 - Includes t_1: In this case we get a summand of the form $t_1 t_{i_1}...t_{i_k}[1,x]_W$ where $2 \le i_1 < i_2 < ... < i_k \le n$. By Lemma 2.2.5 it is isomorphic to

$$[(t_{i_1}...t_{i_k})t_1^{-1}, (x(t_{i_1})^{-1}...(t_{i_k})^{-1})t_1]_W \in W_q(\widehat{K})_0.$$

Its image under φ would be $(0, [t_{i_1}\dots t_{i_k}, x/t_{i_1}\dots t_{i_k}]_W)$.

Case 2 - Omits t_1: In this case we get a summand of the form $t_{i_1}...t_{i_k}[1,x]_W$ where $2 \le i_1 < i_2 < ... < i_k \le n$. By Lemma 2.2.5 this equals

$$[(t_{i_1})^{-1}\dots(t_{i_k})^{-1}, xt_{i_1}\dots t_{i_k}]_W \in W_q(\widehat{K})_0.$$

Its image under φ would be $([(t_{i_1})^{-1}\dots(t_{i_k})^{-1}, xt_{i_1}\dots t_{i_k}]_W, 0)$. □

According to Theorem 6.5.8 there exists a differential basis

$$B = \{a_1, \dots, a_{n+1}\}$$

for $\Omega_{K/k}$ coming from $\overline{K}$ and index i such that

$$F \subset K^2(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_{n+1}).$$

Up to numbering we will assume that $i = n+1$. Our differential basis contains a uniformizer with respect to ν, say π', and it gives rise to a

coefficient field $\widetilde{K_1} \subset F \subset \widehat{K}$ and presentation $\widehat{K} \simeq K_1((\pi'))$. To simplify notation we will denote π' by π.

Since $f_W \in W_q(\widehat{K})_0$, so is $(g_{\widehat{K}})_W$. Since the first and second residues (up to similarity) don't depend on a choice of a coefficient field and uniformizer, the first residue of $(g_{\widehat{K}})_W$ is equal to the first residue of f_W, which is a canonical monomial form of rank $n-1$ by the previous Lemma. Similarly, up to similarity, the second residue of $(g_{\widehat{K}})_W$ coincides with that of f_W and therefore is nontrivial.

We now pass to computing the residues of $(g_{\widehat{K}})_W$. Since g is nondegenerate it can be written as a direct sum of 2-dimensional forms $[b_i, c_i]$ with $b_i, c_i \in F$. In turn, b_i, c_i can be written as sums of terms of the form $\alpha^2 a_{i_1} a_{i_2} \cdots a_{i_s}$ with $\alpha \in K \subset \widehat{K}$ and $i_s \leq n$. Using the fact that $[a\alpha^2, b] \simeq [a, b\alpha^2]$ (by Lemma 2.2.8) and the biadditivity of the symbol $[-,-]_W$, we conclude that the image of $g_{\widehat{K}}$ in the Witt group can be written as a direct sum of symbols

$$[a_{i_1} a_{i_2} \cdots a_{i_s}, \frac{\alpha^2}{\pi^{2l}} a_{j_1} a_{j_2} \cdots a_{j_p}]_W$$

where $\alpha \in K_1$ and $l \geq 0$.

There are two cases for π: either $\pi = a_{n+1}$ or $\pi = a_i$ with $i \leq n$. We consider the case when $\pi = a_{n+1}$ only. In particular, in this case $a_1, \ldots, a_n$ is a 2-basis of K_1 (because B came from $\overline{K} = K_1$). The second case can be treated along the same lines.

We will now consider g as a form over $\widehat{K}$ so that for brevity we will write simply g instead of $g_{\widehat{K}}$. By Theorem 6.4.2 we can write g_W uniquely (up to isometry) in the form

$$g_W = g_m + g_{m-1} + \ldots + g_0$$

where g_i is a sum of symbols of the form

$$[a_{i_1} a_{i_2} \cdots a_{i_s}, \frac{\alpha^2}{\pi^{2i}} a_{j_1} a_{j_2} \cdots a_{j_p}]_W$$

with $\alpha \in K_1$. In the above decomposition, we write g_i instead of $g_{i,W}$ to ease notation. Note that g_0 has trivial second residue (because π is not involved in a_{i_l}, a_{j_l}). So to finish the proof of incompressibility of f it remains to show that $g_n + \cdots + g_1 = 0$ in the Witt group $W_q(\widehat{K})$ because this would contradict the fact that the second residue of f_W is nontrivial.

Let us start from the highest component g_m. We will assume that m is even to begin with and write $m = 2n$. By Lemma 2.2.2

$$W_q(K((\pi)))_{2n}/W_q(K((\pi)))_{2n-1} \simeq K \wedge_{K^2} K \oplus K \wedge_{K^2} K.$$

The class of a generator $[\alpha, \beta\pi^{-2n}]_W$ corresponds to $\alpha \wedge \beta$ in the first summand, but the class of a generator $[\alpha\pi^{-1}, \beta\pi^{-2n+1}]_W$ corresponds to $\alpha \wedge \beta$ in the second summand.

To simplify writing we introduce multi-indices a_{I_j} where $I_j = (a_{i_1} \ldots, a_{i_s})$ and a_{I_j} is the product of the corresponding a_{i_p}. Thus $a_{I_1}, \ldots, a_{I_{2^n}}$ is a K_1^2-basis of K_1. Choose any order $I_1 < \ldots < I_{2^n}$. Our form g_m is a sum of forms of type

$$[a_{I_j}, \frac{\alpha^2}{\pi^{2n}} a_{I_s}]_W$$

with $\alpha \in K_1$. Recall that if $I_j = I_s$ then, by Equation (2.2a), we can rewrite this as $[a_{I_j}, \frac{\alpha}{\pi^n}]_W$. It follows that g_m can be written as $g_m = g'_m + g''_m$ where

$$g'_m = \oplus_j \left[a_{I_j}, \sum_{s \neq j} \frac{a_{I_s}}{\pi^{2n}} \alpha_s^2 \right]_W$$

with $\alpha_s \in K_1$ and g''_m lives in $W_q(K_1((\pi)))_n$. Then using the fact that g_W lives in $W_q(K_1((\pi)))_0$ and arguing as in Theorem 6.4.2 we easily conclude that $g'_m = 0$. Note that in such a way we have eliminated the highest component g_m of g living in $W_q(K_1((s)))_{2n}$, but we possibly acquire the component g''_m in odd degree $W_q(K_1((\pi)))_n$ if n is odd. We can repeat the above process with the next highest non-zero component of g_W. If it has even degree the same argument as above reduces it to a component of

smaller degree. Proceeding in this way we eventually arrive at the situation where the only components left are those with odd degree. If a component has odd degree, say $2l+1$ then it can be written in the form

$$\sum_j \left(\sum_s \left[a_{I_j}, \frac{a_{I_s}}{\pi^{2l+1}} \alpha_s^2 \right]_W \right)$$

with $\alpha_s \in K_1$. However, application of the same argument as in Theorem 6.4.2 shows that this component is automatically 0. This completes the proof of the fact that $g_m + \cdots + g_1 = 0$ and hence the proof of incompressibility of f.

Chapter 7

Proof of the Main Theorem

In this Chapter we will finally prove our main result, Theorem 1.2.1.

7.1 Proof of Theorem 1.2.1

We now proceed to prove Theorem 1.2.1 except for groups of Type F_4 which we defer to the next Section.

To each of our simple, rank r, algebraic groups, G, of adjoint type we associated a non-degenerate quadratic form which we will call q. In Chapter 4 we constructed an irreducible orthogonal representation which we called the "non-degenerate Killing" representation:

$$\lambda_0 \colon G \longrightarrow \mathcal{O}(V, q)\,.$$

This induces a map

$$\lambda \colon H^1(K, G) \longrightarrow H^1(K, \mathcal{O}(V, q))\,,$$

where $K = k(t_1, ..., t_r, x)$. We know from cohomology theory that $H^1(K, \mathcal{O}(V, q))$ is in one-to-one correspondence with the set of isometry classes of the non-

degenerate quadratic form q. Let $\zeta \in H^1(K, G)$ be a cocycle corresponding to $((t_1), ..., (t_r), (x))$ as in Chapter 5. Then $\lambda(\zeta) = \eta$ is a cocycle, but also corresponds to a quadratic form, say ${}_\eta q$, which is the twisting of q by η.

In the previous Section, we saw that for each type of simple algebraic group described in Section 1.2 this twisted quadratic form ${}_\eta q$ is a non-degenerate, rank r, canonical monomial form. Then, by Theorem 6.1.1 we know that this form is incompressible, i.e. it cannot descend to a field of transcendence degree lower than $r + 1 = tr.deg_k K$.

We claim then that η is an incompressible cocycle. If not, then there exists $k \subset E \subset K$ and η_E defined over E, such that $\eta_E \otimes_E K \simeq \eta$. Then since twisting commutes with base extension, we get that

$$({}_\eta q)_E \otimes_E K \simeq {}_{\eta_E \otimes_E K} q = {}_\eta q$$

$\Rightarrow \eta_q$ is compressible, which is a contradiction.

Also, we claim that since η is incompressible, then ζ is incompressible. Indeed, suppose towards a contradiction that ζ is compressible. Then there exists a field $k \subset E \subset K$ and $\zeta_E \in H^1(E, G)$ such that $\zeta_E \otimes_E K \simeq \zeta$. Then, $\lambda(\zeta_E) \otimes K \simeq \lambda(\zeta_E \otimes K) = \lambda(\zeta) = \eta$. This would imply that η compresses to $\eta_E = \lambda(\zeta_E)$, a contradiction.

Thus we have found an incompressible cocycle $\zeta \in H^1(K, G)$ where $K = k(t_1, ..., t_r, x)$ has transcedence degree $r + 1$. Thus, we have proven $ed(G) \geq r + 1$. Finally, arguing in exactly the same way as in the proof of $ed(G) \geq r + 1$, we can show that $ed(G; 2) \geq r + 1$. Thus, we have proven Theorem 1.2.1. □

7.2 Lower Bound for $ed(F_4)$

To deal with the special case of F_4 we will need the notion of cohomological invariants; see [GMS]. We will give the definition of a cohomological invari-

ant for the special case of a split group of type F_4 and a general definition can be found in [GMS]. For k an algebraically closed field we define two functors:

$$\alpha\colon Fields_k \longrightarrow F_4\text{-Torsors},\ F \longmapsto H^1(F, F_4)\ ;\ \text{and}$$
$$\beta\colon Fields_k \longrightarrow Abelian\,Groups,\ F \longmapsto H^5(F, \mathbb{Z}/2)\,.$$

Recall that a natural transformation $\gamma\colon \alpha \to \beta$ is a family of maps γ_F such that for all $F \subset E$ the following diagram commutes:

$$\begin{array}{ccc} \alpha(F) = H^1(F, F_4) & \xrightarrow{\gamma_F} & H^5(F, \mathbb{Z}/2) = \beta(F) \\ \downarrow res & \circlearrowleft & \downarrow res \\ \alpha(E) = H^1(E, F_4) & \xrightarrow{\gamma_E} & H^5(E, \mathbb{Z}/2) = \beta(E) \end{array}$$

(where the vertical arrows are restriction mappings). If there exists a natural transformation $\gamma : \alpha \to \beta$ then we say that γ is a cohomological invariant for F_4 in dimension 5.

Theorem 7.2.1. *If there exists a non-trivial cohomological invariant of F_4 in dimension 5, then $ed(G) \geq 5$.*

Proof. Since the invariant is non-trivial, there is a field E/k and a cocycle $\zeta_E \in H^1(E, F_4)$ such that $\gamma_E(\zeta_E) \neq 1$. Suppose ζ_E descends to $k \subset F \subset E$ where F is of minimal possible transcendence degree. Then by the commutative diagram from above we have that $\gamma_E(res(\zeta_F)) = res(\gamma_F(\zeta_F)) \Leftrightarrow \gamma_E(\zeta_E) = res(\gamma_F(\zeta_F))$ and since $\gamma_E(\zeta_E) \neq 1 \Rightarrow \gamma_F(\zeta_F) \neq 1$. We claim then that $\mathrm{tr.deg}_k(F) \geq 5$. Assume otherwise, i.e. $\mathrm{tr.deg}_k(F) \leq 4$. Then by the discussion below it follows that $H^i(F, \mathbb{Z}/2) = 1\ \forall\ i \geq 5$, which would be a contradiction. □

Note that the above Theorem is true for any abelian group G and for arbitrary positiver integer i instead of 5. We now introduce the notion of cohomological dimension as defined in [Se02, Section 3.1]. Let F be a field, F_s its separable closure and $\Gamma = \mathrm{Gal}(F_s/F)$. Let p be a prime number. We

say that the *p-cohomological dimension* of Γ, denoted $cd_p(\Gamma)$, is n if for all discrete, p-primary torsion Γ-modules A, $H^i(\Gamma, A) = 0 \ \forall \ i \geq n+1$. Recall that a Γ-module is just a finite abelian group upon which Γ acts.

Then we can define the *cohomological dimension* of Γ as:

$$cd(\Gamma) = \sup_{p \text{ prime}} \{cd_p(\Gamma)\}.$$

Also, by definition $H^i(F, G) = H^i(\Gamma, G)$, so $cd(F) = cd(\Gamma)$.

With these definitions in hand we have the following result from [Se02]:

Theorem 7.2.2. *Let k' be an extenstion of k of transcendence degree N. If p is a prime, we have that $cd_p(G_{k'}) \leq N + cd_p(G_k)$.*

In the situation of Theorem 7.2.1 we have k is algebraically closed, $k' = F$. We assumed that $\text{tr.deg}_k(F) \leq 4 \overset{7.2.2}{\Rightarrow} cd_p(F) \leq 4 + cd_p(k) = 4$ since k is algebraically closed. This implies that $H^i(\Gamma_F, A) = 1$ for all $i \geq n+1$ where A is any p-primary torsion group and $\Gamma_F = Gal(F_{sep}/F)$.

Now in the previous paragraph let $p = 2$ and $i = 5$. Since $\mathbb{Z}/2$ is a 2-torsion group we get that $H^5(F, \mathbb{Z}/2) = 1$, which is precisely what was needed to complete the proof of Theorem 7.2.1.

Putting everything together we get that if F_4 has a cohomological invariant in dimension 5, then $ed(F_4) \geq 5$. This is well known to be true when the characteristic of the base field is not 2, see [GMS, Chapter 6, Section 22]. However H.P. Petersson proved the existence of such a cohomological invariant when the base field has characteristic 2 in [Pe]. Thus, by Theorem 7.2.1 we have $ed(F_4) \geq 5 = 4 + 1 = \text{rank}(F_4) + 1$.

Now let K/k be a field extension with $tr.deg_k(K) = 5$. Let $\zeta_K \in H^1(K, G)$ be an incompressible cocycle which we know exists by the previous paragraph. Let L/K be a finite field extension of odd degree and let ζ_L denote the image of ζ_K in $H^1(L, G)$. Now assume that ζ_L is compressible, i.e. there is a field $k \subset E \subset L$ with $tr.deg_k E < 5$ such that ζ_L compresses to a cocycle $\zeta_E \in H^1(E, G)$.

Let γ denote the cohomological invariant for F_4 in dimension 5 which we have proven the existence of previously. Consider $\gamma(\zeta_K) \in H^5(K, \mathbb{Z}/2)$. Consider the following composition of the restriction and corestriction mapping:

$$H^5(K, \mathbb{Z}/2) \xrightarrow{res} H^5(L, \mathbb{Z}/2) \xrightarrow{cor} H^5(K, \mathbb{Z}/2)$$

The image of $\gamma(\zeta_K)$ under this composition is $[L : K]\gamma(\zeta_K) = \gamma(\zeta_K)$ because $H^5(K, \mathbb{Z}/2)$ is a group of exponent 2. However, since γ is a natural transformation we know that the image of $\gamma(\zeta_K)$ under the restriction mapping above is the same as the image of $\gamma(\zeta_E)$ under the restriction mapping:

$$H^5(E, \mathbb{Z}/2) \xrightarrow{res} H^5(L, \mathbb{Z}/2)$$

Now since $tr.deg_k E < 5$ we have shown above that this implies $H^5(E, \mathbb{Z}/2) = 1$ and therefore $res(\gamma(\zeta_E)) = 1 = res(\gamma(\zeta_K))$. This contradicts the fact that $cor \circ res(\gamma(\zeta_K)) = \gamma(\zeta_K)$. Thus we have proven ζ_L must be incompressible, i.e $ed(F_4; 2) \geq 5$. $\square$

7.3 Applications of the Main Result

We will conclude by providing proofs for the two Theorems mentioned at the end of Section 1.2, each of which rely on Theorem 1.2.1.

Proof of Theorem 1.2.2. We first consider the even-dimensional case, i.e. $\mathcal{O}_{2n}$. This a split group of rank n, therefore by 1.2.1 we have the lower bound $n + 1 \leq ed(\mathcal{O}_{2n})$. To define the orthogonal group we really need a field of definition and a non-degenerate quadratic form of the appropriate dimension. Suppose $\mathcal{O}_{2n}$ is defined over an algebraically closed field of characteristic 2. By Lemma 2.1.5, an arbitrary even dimensional quadratic form over a field k is of the form $f = \oplus_{i=1}^n [b_i', c_i'] \overset{2.2.5}{\simeq} \oplus_{i=1}^n b_i[1, c_i]$ where $b_i \in k^\times, c_i \in k$.

Each quadratic form $[1, c_i]$ corresponds to a quadratic separable extension

L_i/k which is obtained by adjoining a root of the separable polynomial $t^2 + t + c_i$. Such an extension corresponds to $H^1(k, \mathbb{Z}/2)$. Thus, isometry classes of the set of two dimensional forms $\{[1, c_1], ..., [1, c_n]\}$ correspond to $H^1(k, A)$ where $A = \mathbb{Z}/2 \times ... \times \mathbb{Z}/2 = (\mathbb{Z}/2)^n$. By examining long exact sequences of Galois cohomology, one can show that every element in $H^1(k, A)$ can be compressed to $k(x)$, a purely transcendental extension of degree 1. Thus our quadratic form can compresses to the field $k(x)(b_1, ..., b_n)$ which has transcendence degree $n + 1$. This shows that $ed(\mathcal{O}_{2n}) \leq n + 1$. Thus we have

$$n + 1 \leq ed(\mathcal{O}_{2n}) \leq n + 1,$$

i.e $ed(\mathcal{O}_{2n}) = n + 1$.

Now we will consider the odd-dimensional case, i.e. we will show $ed(\mathcal{O}_{2n+1}) = n + 2$. First we will show that $n + 2$ is a lower bound by mimicking the main argument of Section 6.3. Let k be our algebraically closed, characteristic 2 base field. Consider the field $K = k(t_1, ..., t_{n+1}, x)$ and the $(2n + 1)$-dimensional, non-degenerate quadratic form $f = \langle t_1 \rangle \oplus t_2[1, x] \oplus ... \oplus t_{n+1}[1, x]$. We will show that this form is incompressible, thus giving us the lower bound we desire. Suppose f is compressible, i.e. there is a non-degenerate, $2n + 1$-dimensional form g defined over a field $k \subset E \subset K$. By Lemma 2.1.5 we may write $g = \langle c \rangle \oplus e_1[1, e_2] \oplus ... \oplus e_n[1, e_{n+1}]$. Since $g \otimes_E K \simeq f$, we know that $c \equiv t_1 \ (mod\ K^2)$.

Now consider the field extension $\widetilde{E} = E(\sqrt{ct_1^{-1}})$. Since this extension is algebraic, $\text{tr. deg}_k(E) = \text{tr. deg}_k(\widetilde{E})$. So if f could compress to g defined over E, it could also compress to $\widetilde{g} = g \otimes_E \widetilde{E}$, which is defined over $\widetilde{E}$. However, in $\widetilde{E}$ we have $\langle c \rangle = \langle t_1 \rangle$ because $c = \sqrt{ct_1^{-1}}^2 t_1$. Then, arguing in the same way as in Section 6.3, if f is compressible, then so is $t_2[1, x] \oplus ... \oplus t_{n+1}[1, x]$. However, this is a canonical monomial form, so by Theorem 6.1.1 we know this form is incompressible. Thus we obtain a contradiction. So we have a form f defined over a field $K = k(t_1, ..., t_{n+1}, x)$, a field of transcendence degree $n + 2$, which is incompressible. Thus $n + 2 \leq ed(\mathcal{O}_{2n+1})$.

It remains to show that $n + 2$ is an upper bound for $ed(\mathcal{O}_{2n+1})$. This

is straightforward since an arbitrary non-degenerate $(2n+1)$-dimensional form over k can be written as $\langle a\rangle \oplus [b_1, c_1] \oplus ... \oplus [b_n, c_n]$. Then arguing as in the even-dimensional case $\mathcal{O}_{2n}$ we know that this form can be defined over the field $K = k(a, b_1, b_2, ..., b_n, x)$ for some transcendental element x. Thus $ed(\mathcal{O}_{2n+1}) \leq n + 2$. □

Proof of Theorem 1.2.3. Our goal is to show $ed(G_2) = 3$. Since $\text{rank}(G_2) = 2$, Theorem 1.2.1 tells us that $2+1 = 3 \leq ed(G_2)$. Recall that when we talk about the essential dimension of G_2, what we are really talking about is the essential dimension of the cohomology functor $H^1(-, G_2)$. By [KMRT, Propostion 33.24], for an arbitrary field extension K/k, $H^1(K, G_2)$ is in 1:1 correspondence with isomorphism classes of Octonion Algebras over K. Then, by [Pe] these isomorphism classes of Octonion Algebras are in one-to-one correspondence with the so called 3-Pfister forms. These are special quadratic forms which depend on 3 parameters, say $a, b, c \in K$, and are defined as

$$\begin{aligned}\langle\langle a, b, c\rangle\rangle &= [1, a] \otimes (\langle b\rangle \otimes \langle c\rangle) \\ &= [1, a] \oplus b[1, a] \oplus c[1, a] \oplus bc[1, a]\end{aligned}$$

What's important to note is that these 3-Pfister forms are examples of canonical monomial forms depending on 3 independent parameters. By Theorem 6.1.1 we know such forms are incompressible and so by the 1:1 correspondences described previously, it follows that $ed(G_2) \leq 3$. Since $3 \leq ed(G_2) \leq 3$, we get $ed(G_2) = 3$, as desired. □

Bibliography

[Ar1] J. Arason, *Generators and Relations for $W_q(K((S)))$ in characteristic 2*, Preprint. RH-19-2006 Science Institute University of Iceland Dunhaga 3, IS 107 Reykjavik

[Ar2] J. Arason, *Generators and Relations for $W_q(K)$ in characteristic 2*, Preprint. RH-18-2006 Science Institute University of Iceland Dunhaga 3, IS 107 Reykjavik

[BF03] G. Berhuy, G. Favi, *Essential Dimension: A Functorial Point of View (After A. Merkurjev)*, Documenta Mathematica **8** 279-330 (2003).

[Bo72] N. Bourbaki, *Commutative Algebra (Translated from French)*, Hermann (1972).

[Bo02] N. Bourbaki, *Lie Groups and Lie Algebras (Chapters 4-6)*, Springer (2002).

[BRV] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential Dimension of Moduli of Curves and other Algebraic Stacks*, Journal of the European Math. Society **13 no. 4** 1079-1112 (2011).

[BuRe] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106 no. 2** 159-179 (1997).

[ChSe] V. Chernousov, J.-P. Serre, *Lower Bounds for Essential Dimensions via Orthogonal Representations*, Journal of Algebra **305 no.2** 1055-1070 (2006).

[DeGr] M. Demazure, A. Grothendieck, *Structure des Schémas en Groupes Réductifs*, SGA 3 III LN 153, Springer-Verlag (1970).

[Du] A. Duncan, *Essential dimensions of A7 and S7*, Math. Res. Lett. **17 no. 2** 263-266 (2010).

[Ei] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer Science+Business Media LLC, New York (2004).

[EKM] R. Elman, N. Karpenko, A. Merkurjev, *The Algebraic and Geometric Theory of Quadratic Forms*, American Mathematical Society, USA (2008).

[GMS] S. Garibaldi, A. Merkurjev, J.-P. Serre, *Cohomological Invariants in Galois Cohomology*, American Mathematical Society, USA (2003).

[Hu] J.E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Graduate Texts in Mathematics **Vol. 9**, Springer (1972).

[Hu2] J.E. Humphreys, *Linear Algebraic Groups*, Graduate Texts in Mathematics **Vol. 21**, Springer (1998).

[KM] N. Karpenko, A. Merkurjev, *Essential Dimension of Finite p-groups*, Inventiones Mathematicae **172** 491-508 (2008).

[KMRT] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, *The Book of Involutions*, American Mathematical Society, USA (1998).

[La] S. Lang, *Algebra. Revised Third Edition*, Springer-Verlag, New York (2002).

[Ma] A.L. Malagon, *Killing Forms of Lie Algebras*, PhD Dissertation at Emory University, (2009).

[Me] A. Merkurjev, *Essential Dimension: A Survey*, to appear in Transformation groups.

[Pe] H.P. Petersson, *Structure Theorems for Jordan Algebras of Degree Three Over Fields of Arb+itrary Characteristic*, Comm. Alg. **32** 1019-1049 (2004).

[Re] Z. Reichstein, *Presentation on Essential Dimension at Spring School on Torsors, Motives and Cohomological Invariants, May 2013, Fields Institute, Toronto*

[Re2] Z. Reichstein, *Essential dimension*, Proceedings of the International Congress of Mathematicians, Hyderabad, India, (2010)

[Se79] J.-P. Serre, *Local fields (Translated from the French by Marvin Jay Greenberg)*, Springer-Verlag, New York (1979).

[Se02] J.-P. Serre, *Galois Cohomology (Translated from the French by Patric Ion)*, Springer-Verlag, New York (2002).

[SpSt] T.A. Springer, R. Steinberg, *Conjugacy Classes*, Lecture Notes in Mathematics **Vol. 131** 167-266, Springer-Verlag, New York (1970).

[Wa] W. Waterhouse, *Introduction to Affine Group Schemes*, Springer-Verlag, New York (1979).