# Cohomological Invariants of Simple Linear Algebraic Groups Arising via the Killing Form

by

Andrew E. Bishop

A thesis submitted in partial fulfillment of the requirements for the degree of

Master of Science

in

Mathematics

Department of Mathematics and Statistics

University of Alberta

# Abstract

Let $G$ be a linear algebraic group defined over a ground field $k$, and let $\mu$ be a $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-module. A **cohomological invariant** is a morphism $a : H^1(-,G) \to H^n(-,\mu)$ of two functors from the category of field extensions over $k$ to the category of sets where $H^1(-,G)$ is the functor of isomorphism classes of $G$-torsors and $H^n(-,\mu)$ is the functor of abelian Galois cohomology groups with coefficients in $\mu$.

The objective of this thesis is to investigate the existence of nontrivial cohomological invariants arising via the Killing form in several settings, with the primary target being split groups of type $E_8$. We note that for such groups not much is known. The only known invariant is due to M. Rost and it lives in dimension 3. To deal with the type $E_8$ we first study its subgroup of type $D_8$. In Chapter VI we give results regarding the existence of cohomological invariants for groups of type $D_n$, not necessary simply connected or adjoint. After that we pass to type $E_8$. Our main result establishes the existence of a nontrivial cohomological invariant in degree 6 for the subfunctor of $H^1(-,E_8)$ consisting of torsors spitting over a quadratic extension of the base field. It is worth mentioning that all torsors in the kernel of the Rost invariant have this property, so that our result will complement the recent result of N. Semenov who constructed a cohomological invariant for the kernel of the Rost invariant for $E_8$ in degree 5.

# Contents

1 Introduction . . . . . . . . . . 1

**I Quadratic Forms and Witt Rings 8**

1 Quadratic Forms . . . . . . . . . . 8

2 Witt Rings . . . . . . . . . . 17

3 Pfister Forms . . . . . . . . . . 19

**II Root Systems 23**

1 Root Systems . . . . . . . . . . 23

2 Dynkin Diagrams . . . . . . . . . . 26

**III Galois Cohomology 28**

1 Cohomology Groups . . . . . . . . . . 28

2 Abelian Galois Cohomology . . . . . . . . . . 36

3 Residue Maps . . . . . . . . . . 40

4 Non-Abelian Cohomology . . . . . . . . . . 43

5 Twisting Actions . . . . . . . . . . 48

6 Forms of Algebraic Objects . . . . . . . . . . 54

7 Cohomological Invariants . . . . . . . . . . 56

**IV Algebraic Groups 62**

1 Algebraic Groups . . . . . . . . . . 62

2 Jordan-Chevalley Decomposition . . . . . . . . . . 67

3 Tori and Split Groups . . . . . . . . . . 69

4 Reductive, Semisimple and Simple Algebraic Groups . . . . . . . . . . 74

**V Lie Algebras 81**

1 Lie Algebra of an Algebraic Group . . . . . . . . . . 81

2 Killing Forms and the Chevalley Basis . . . . . . . . . . 84

3 Killing Forms of Twisted Lie Algebras . . . . . . . . . . . . . . . . . . . . . . . 95

**VI Cohomological Invariants Arising via the Killing Form** **101**

1 Simply Connected Groups of Types $D_n$ . . . . . . . . . . . . . . . . . . . . . . 101

2 The Centres of Simply Connected Groups of Type $D_{2n}$ . . . . . . . . . . . . 102

3 Non-Simply Connected Groups of $D_4$ . . . . . . . . . . . . . . . . . . . . . . 106

4 Non-Simply Connected Groups of Type $D_8$ . . . . . . . . . . . . . . . . . . . . 111

5 Groups of Type $E_8$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 115

**A Diagonalization of a Subform of the Killing Form for Twisted Lie Algebras of Type $E_8$** **122**

# 1 Introduction

The primary goal of this thesis is to construct a new cohomological invariant for algebraic groups of type $E_8$. Cohomological invariants for algebraic groups are an algebraic analogue of characteristic classes in topology, so let us begin by discussing some relevant concepts in topology.

In almost all applications, a topological space $X$ under consideration is equipped with a continuous action of a group $G$ on that space, that is to say the action map

$$G \times X \to X$$

is continuous. In this setting we may consider the quotient of $X$ by the action of $G$ - the set $X/G$. This set comes equipped with a natural (smallest) topology such that the quotient map

$$\begin{aligned} X &\to B = X/G \\ x &\mapsto xG \end{aligned}$$

is continuous. That is to say, a subset of $B$ is open if and only if its pre-image is open. The fibres of this map are of course precisely the $G$-orbits in $X$.

If the action of $G$ on $X$ is free, that is if the only element of $G$ with fixed points under its action is $1 \in G$, then one can identify each fibre of the map with the group $G$, and so abusing terminology we can say that the group $G$ is the fibre of the continuous map $X \to B$. (In particular, one may choose a "base point" $x$ in each fibre of $G$ and views the points $(g, x)$ as in correspondence with $gx$.)

We may often wish to consider the case that $G$ is a topological group. We do not exclude the case where $G$ is a group with the discrete topology.

**Example 1.1.** *Let $Y$ be a simply connected covering of a topological space $X$. Consider the fundamental group $\pi_1(X)$. Then $Y$ may be given an action of $\pi_1(X)$ on $Y$ such that $X = Y/\pi_1(X)$.*

Another interesting type of examples is continuous maps $X \to B$ whose fibres are all isomorphic to some Lie group $G$. Such examples arise in the theory of topological $G$-bundles. It should be noted that this class of maps is very restrictive, and so the broader class of maps which have the **homotopy lifting property** is often studied instead.

**Definition 1.2.** *A (weak)* ***fibration*** *is a map of topological spaces $p : X \to B$ which satisfies the* ***homotopy lifting property*** *with respect to any CW-complex $Z$.*

*Recall that a map $p : X \to B$ is said to satisfy the homotopy lifting property with respect to some topological space $Z$ if for any homotopy*

$$f : Z \times [0,1] \to B$$

*and for any map*

$$\tilde{f}_0 : Z \to X$$

*lifting $f_0 := f \mid_{Z\times\{0\}}$, there exists a homotopy*

$$\tilde{f} : Z \times [0,1] \to X$$

*lifting $f$, with $\tilde{f} \mid_{Z\times\{0\}} = \tilde{f}_0$.*

The following diagram illustrates the situation:

$$\begin{tikzcd}
Z \arrow[r, "\tilde{f}_0"] \arrow[d, hook] & X \arrow[d, "p"] \\
Z \times [0,1] \arrow[r, "f"] \arrow[ur, "\tilde{f}"] & B
\end{tikzcd}$$

Fibrations can be seen as a precise way to describe the space $X$ as being "parameterized" by the space $B$.

The existence of a fibration $X \to X/G$ allows us to compute the homotopy groups of the space $X$ by consideration of the homotopy groups of the base $X/G$ and the fibre $G$. In this case the homotopy groups of $X$ and $G$ are related by the exact sequence

$$... \to \pi_{n+1}(X/G) \to \pi_n(G) \to \pi_n(X) \to \pi_n(X/G) \to \pi_{n-1}(G) \to ...$$

**Definition 1.3.** *A* ***fibre bundle*** *is a surjective fibration $p : X \to B$ which satisfies the following local triviality condition: fix a base point $b_0 \in B$ and let the "fibre" $F = p^{-1}(b_0)$. Then for all $b \in B$ there exists an open neighborhood $U_b$ with a local homeomorphism*

*$p^{-1}(U_b) \xrightarrow{\sim} U_b \times F$ whose projection onto $U_b$ agrees with $p$. The situation is illustrated below.*

$$\begin{tikzcd}
p^{-1}(U_b) \arrow[r, "\sim"] \arrow[d, "p"] & U_b \times F \arrow[dl, two heads] \\
U_b &
\end{tikzcd}$$

**Definition 1.4.** *A **principal $G$-bundle** $p$ over a topological space $B$ is a fibre bundle $p : P \to B$ together with a continuous (right) action of $G$ on $P$ which preserves fibres of $p$ and the action of which is freely transitive on the fibres. In such a bundle, each fibre of $p$ is homeomorphic to $G$ and $P/G$ is homeomorphic to $B$.*

The final example above is key to our purposes due to the following constructions.

**Definition 1.5.** *A **universal $G$-bundle** is a principal $G$-bundle $p : E_G \to B_G$ such that $E_G$ is contractible. Such a space $B_G$ is called a **classifying space** for $G$.*

The reasoning behind the name "classifying space" is revealed by the following result.

**Theorem 1.6.** *(Classification Theorem) There is a natural bijective correspondence between equivalence classes of principal $G$-bundles and homotopy classes of maps $X \to B_G$. [5]*

This correspondence can be roughly described as follows: upon fixing a continuous map $f : X \to B_G$ we can consider the pullback $E_G^*$ defined as

$$f^*(E_G) := \{(x, e) \mid f(x) = p(e)\} \subseteq X \times E_G.$$

Consider the restriction to $f^*(E_G)$ of the projection $X \times E_G \twoheadrightarrow X$. We identify the fibre at a specific point $x_0$ with a subset of $E_G$ in the obvious way. That fibre then has the form $p^{-1}(f(x_0))$ is by definition isomorphic to $G$, since it is a fibre of $p$. As such the map described from $E_G^*$ to $X$ is itself a principal $G$-bundle.

It can be further shown that homotopic maps produce isomorphic $G$-bundles via this procedure, and one can check that this correspondence is indeed a bijection.

The following definition has been the main objective of our topological discussion, as its algebraic analogue is central to our research. The idea was first introduced in 1935 by Stiefel and Whitney.

**Definition 1.7.** *Let $G$ be a topological group. A **characteristic class** $c$ for $G$-bundles associates to each $G$-bundle $\zeta$ over $X$ a cohomology class $c(\zeta) \in H^*(X)$ naturally with respect* *to $G$-bundle maps, i.e. for any map of $G$-bundles*

$$(\tilde{f}, f) : \zeta \to \zeta'$$

*one has $f^*c(\zeta') = c(\zeta)$.*

The study of characteristic classes was one motivating factor in the broader development of cohomology theory, as it was an early example of a contravariant construction. We end our discussion of topology with the following result about characteristic classes.

**Theorem 1.8.** *Characteristic classes for $G$-bundles are in bijective correspondence with $H^*(B_G)$.*

*Proof.* See [5]. □

We now move to the algebraic settting. The algebraic analogue of a characteristic class is called a **cohomological invariant.** The study of such objects was initiated by J.-P. Serre in the mid 1990s.

Recall that in algebra instead of topological $G$-bundles one studies $G$-torsors. Loosely speaking, if $G$ is an algebraic group over a base $X$ then a $G$-torsor is a variety $Y$ over $X$ together with a simply transitive action of $G$ which is locally (with respect to the étale topology) isomorphic to $G$ as a variety. The set of all isomorphism classes of $G$-torsors is denoted by $H^1(X, G)$.

The main focus of this thesis will be the case where the base $X = \operatorname{Spec} k$ consists of a unique point and $G$ is an affine algebraic group defined over $k$. Recall that in this particular case, $G$-torsors can be defined in terms of non-abelian Galois cohomology (see III.4.11).

Furthermore, it looks natural to replace topological cohomology groups $H^*(X)$ with an algebraic analogue $H^*(k, \mu)$ where $\mu$ is a $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-module. Thus we arrive to the main definition in our thesis:

**Definition 1.9.** *Let $G$ be an algebraic group defined over a field $k$. Consider two functors from the category $Fields_{/k}$ of field extensions of $k$ to the category Set of sets: namely the functor $H^1(-, G)$ of isomorphism classes of $G$-torsors and the functor $H^n(-, \mu)$ of abelian Galois cohomology groups with coefficients in $\mu$.*

*A **cohomological $\mu$-invariant** (alternatively a cohomological invariant with coefficients in $\mu$) in degree $n$ is a morphism*

$$a : H^1(-, G) \to H^n(-, \mu)$$

*of these functors.*

Thus, for any field extension $F/k$ we have a map

$$a_F : H^1(F, G) \to H^n(F, \mu)$$

compatible with field extensions $L/F$.

A natural question appears immediately - how to describe all cohomological invariants for a given group $G$. This is a widely open and challenging problem, not much is known in general.

If $G$ is simple it is known that there are no cohomological invariants in degree 1. In degree 2, all cohomological invariants essentially come from Tits algebras, i.e. they can be described with the use of the cohomology map

$$H^1(k, G) \to H^2(k, Z)$$

where $Z$ is the kernel of the simply connected covering $\hat{G} \to G$.

In degree 3, M. Rost (see [9]) described all cohomological invariants with coefficients in $\mu = \mathbb{Q}/\mathbb{Z}(d)$ (this is the Tate twist - see III.3.5) for simply connected groups and later on A. Merkurjev extended his result for all semisimple groups. [14]

Finally, we note that for orthogonal algebraic groups and groups of types $G_2$ and $F_4$ (see examples in section III.7) J.-P. Serre classified all possible invariants with coefficients in $\mu_2$. Besides these types, nothing is known in general.

A few years ago, V. Chernousov put forward a new idea of construction of cohomological invariants with the use of orthogonal representations. Namely, assume we are given an orthogonal representation $\lambda : G \to O(f)$. It induces a natural mapping

$$\lambda^* : H^1(F, G) \to H^1(F, O(f))$$

where $F/k$ is any field extension of the base field $k$.

Recall that the elements of $H^1(F, O(f))$ are in one-to-one correspondence with isomorphism classes of nondegenerate quadratic forms over $F$ having the same dimension as $f$ (see §III.6.6). Thus to every class $[\zeta] \in H^1(F, G)$ we may associate in a functorial way a nondegenerate quadratic form $f_\zeta$. Now if $n$ is a maximal positive integer such that for all field extensions $F/k$ and all classes of cocycles $[\zeta] \in H^1(F, G)$ the classes of $f_\zeta - f$ are contained in the $n$-th power of the fundamental ideal (see Definition I.2.2) $I^n(F)$, but not all in $I^{n+1}(F)$, then we have a well-defined non-trivial cohomological invariant

$$a_\lambda : H^1(-, G) \to I^n/I^{n+1} \simeq H^n(-, \mu_2)$$

in degree $n$ with coefficients in $\mu_2$. The last isomorphism above is due to the famous Voevodsky's Theorem.

Of course, the main difficulty here is to understand when the class of $f_\zeta - f$ is nonzero in the Witt ring and how to compute $n$.

In the present work, we examine the case of the adjoint representation for a group $G$ of type $E_8$. Our results show that this construction produces a new invariant in degree $n = 6$. Before stating it, we first recall a natural idea coming from topology. For a given $G$-bundle $Y$ over $X$, to check if it is trivial or not one can start from any characteristic class $c$. If $c(Y) \neq 0$ then $Y$ is not trivial. Otherwise one can consider the subfunctor $\operatorname{Ker}(c)$ of $c$ and try to construct a new characteristic class $c_1 : \operatorname{Ker}(c) \to H^*(X)$. If $c_1(Y) \neq 0$ we are done. If it is not, we can continue in a similar way. Of course, the main difficulty here is to construct $c_1, c_2$ and so on.

Here is an illuminating example in algebraic setting. Assume we are given a class $[f] \in W(F)$ of a nondegenerate $n$-dimensional quadratic form $f$ over a field $F$ of characteristic $\neq 2$ and we want to check if it is trivial or not. We may then consider "a characteristic class" $c_0 : W(F) \to H^0(F, \mathbb{Z}/2)$ given by dimension. If $c_0([f]) \neq 0$ we are done. Otherwise we consider the kernel $\operatorname{Ker}(c_0) = I \subset W(F)$ and pass to the map $c_1 : I \to H^1(F, \mathbb{Z}/2)$ given by discriminant. If $c_1([f]) \neq 1$ we are done. Otherwise we take $\operatorname{Ker}(c_1) = I^2 \subset I \subset W(F)$ and consider the Arason invariant $I^2 \to H^2(F, \mathbb{Z}/2)$ whose kernel is $I^3$ and so on. It is worth mentioning that we use the following fundamental result in the algebraic theory of quadratic forms: for an arbitrary positive integer $n$ there is a well-defined map $c_n : I^n \to H^n(F, \mathbb{Z}/2)$ whose kernel is $I^{n+1}$. This process terminates since if $l = [\log_2 n]$ then by Hauptsatz the dimension of any anisotropic quadratic form in $I^{l+1}F$ is

$$\geq 2^{l+1} > 2^{\log_2 n + 1} = 2n.$$

In the theory of algebraic groups over non-closed fields for any simple simply connected algebraic group $G$ the only known cohomological invariant is due to M. Rost. It lives in degree 3:

$$R : H^1(F, G) \to H^3(F, \mathbb{Q}/\mathbb{Z}(2)).$$

Its kernel $\operatorname{Ker}(R)$ is highly nontrivial in the general case and following the above philosophy one would like to construct a cohomological invariant $c : \operatorname{Ker}(R) \to H^n(F, \mathbb{Q}/\mathbb{Z}(2))$ in some degree $n$. However nothing is known in this direction. For our purposes we replace the coefficient module $\mathbb{Q}/\mathbb{Z}(2)$ by $\mu_2$ and we will consider a split group $G = E_8$ of type $E_8$. It is then known that any $E_8$-torsor in the $\mathrm{Ker}(R)$ is split by a quadratic extension of the ground field. Therefore it makes sense to consider the subfunctor $H^1_{quad}(-, E_8) \subset H^1(-, E_8)$ consisting of $E_8$-torsors splitting over a quadratic extension of the base field. In this notation our main result is the following.

**Theorem.** *There exists a nontrivial cohomological invariant $H^1_{quad}(-, E_8) \to H^6(-, \mu_2)$.*

Finally we note that cohomological invariants cannot exist in high degrees; the upper bound of such degrees is the essential dimension $\mathrm{ed}(E_8)$ of type $E_8$. Therefore, it is natural to turn to the problem of classification of all such cohomological invariants (recall that the Rost invariant lives in degree 3; furthermore N. Semenov constructed an invariant in degree 5. We expect one more invariant in degree 9 and no more).

In this thesis, we begin by reviewing several topics relevant to this construction. We will begin with a discussion of quadratic forms and the Witt ring, including the powers of the fundamental ideal, their elements, and their quotients. Next, we briefly discuss root systems of simple linear algebraic groups and their classification by Dynkin diagrams, which will play a central role in later computations. The third chapter is focused on Galois cohomology, and includes more in depth discussion of topics such as torsors and cohomological invariants, and the relationship between torsors and cohomology. We then move to general reviews of topics from the study of linear algebraic groups and of Lie algebras which are relevant to our setting, as well as the correspondence between the two. The discussion on Lie algebras is largely focused on a quadratic form called the Killing form.

The final chapter contains the original research of this thesis, therein we show some results about cohomological invariants arising via the Killing form in increasingly complicated settings. The primary target of this thesis was to investigate the existence of a non-trivial cohomological invariant arising via the Killing form for simple groups of type $E_8$. In §VI.5 we show that such a non-trivial invariant does exist.

Throughout the duration of this thesis we will assume that the base field has characteristic not equal to 2.

# CHAPTER I

# Quadratic Forms and Witt Rings

## 1 Quadratic Forms

In this chapter we collect some basic facts on quadratic forms and Witt rings which we will need later on. For their proofs we refer to [12] and [8].

**Definition 1.1.** *An $n$-**dimensional quadratic form** over $k$ is a homogeneous polynomial of degree 2 in $n$ variables. That is to say, a quadratic form is a polynomial of the form*

$$f(X) = \sum_{i,j=1}^{n} a_{ij} X_i X_j,$$

*where $X = (X_1, ..., X_n)$ is an indeterminate over $k^n$ and the coefficients $a_{ij}$ are elements of $k$.*

Notice that if we set $a'_{ij} := \frac{1}{2}(a_{ij} + a_{ji})$ for all $i, j = 1, ..., n$ then we have

$$f(X) = \sum_{i,j=1}^{n} a_{ij} X_i X_j = \sum_{i,j=1}^{n} a'_{ij} X_i X_j,$$

so that $a'_{ij} = a'_{ji}$ for all $i, j = 1, ..., 2$. In this way we may rewrite any quadratic form in such a way that the coefficients are rendered symmetric.

Written in this manner, our quadratic form $f(X)$ gives rise to a symmetric matrix $M_f := (a'_{ij})$. There is a natural notion of equivalence of quadratic forms, which amounts to congruency of these matrices.

Recall that two $n \times n$ matrices $A$ and $B$ over $k$ are **congruent** if there exists an $n \times n$

invertible matrix $S \in \mathrm{GL}(n, k)$ such that

$$A = SBS^T.$$

This is equivalent to saying $A$ and $B$ define the same map $k^n \to k^n$ up to a linear replacement of variables.

**Definition 1.2.** *Let $f, g$ be $n$-dimensional quadratic forms over $k$. We consider $f$ and $g$ to be* ***equivalent quadratic forms*** *if there is an invertible linear replacement of variables*

$$Y_i = \sum_{j=1}^{n} b_{ij} X_j$$

*such that $f(X_1, ..., X_n) = g(Y_1, ..., Y_n)$.*

**Lemma 1.3.** *Two quadratic forms $f$ and $g$ over $k$ are equivalent if and only if the associated matrices $M_f$ and $M_g$ are congruent.*

*Proof.* See [12, Chapter I, Section 1]. □

**Theorem 1.4.** *The above definition defines an equivalence relation on the set of all quadratic forms over $k$.*

*Proof.* This follows directly from Lemma 1.3 along with the well known fact that congruency is an equivalence relation on a matrix algebra. □

Another perspective is to view $f$ as a **quadratic map** $Q_f : k^n \to k$. This is done in the obvious way, i.e.

$$Q_f(X) = f(X)$$

or alternatively

$$Q_f(X) = X^t M_f X,$$

where $X \in k^n$ is a column vector.

Notice that not only does a quadratic form determine uniquely a quadratic map, but the converse is also true. This more geometric outlook can be translated to the study of symmetric bilinear forms.

**Definition 1.5.** *Let* V *be an $n$-dimensional $k$-vector space. A* ***symmetric bilinear form*** *on* V *is a map*
$B : \mathrm{V} \times \mathrm{V} \to k$ *such that for all $u, v, w \in \mathrm{V}$, $c \in k$,*

*1.* $B(u,v) = B(v,u)$

*2.* $B(u, v+w) = B(u,v) + B(u,w)$

*3.* $B(cu, v) = cB(u,v)$.

Given a quadratic map $Q : k^n \to k$ we may obtain a symmetric bilinear form $B : k^n \times k^n \to k$ by setting

$$B(X,Y) := \frac{1}{2}(Q(X+Y) - Q(X) - Q(Y)).$$

Similarly, if $B$ is a symmetric bilinear pairing $B : k^n \times k^n \to k$ we may define $Q : k^n \to k$ by setting

$$Q(X) := B(X,X).$$

This correspondence enables us to work over $k$-vector spaces other than $k^n$ as well. Suppose $\mathrm{V}$ is a finite dimensional $k$-vector space, and $B$ a symmetric bilinear pairing $B : \mathrm{V} \times \mathrm{V} \to k$. Let $Q$ be the quadratic map $Q : \mathrm{V} \to k$, $X \mapsto B(X,X)$. The pair $(\mathrm{V}, B)$ is called a **quadratic space.** Since $B$ and $Q$ uniquely determine one another it is equally as correct to express our quadratic space as $(\mathrm{V}, Q)$. A quadratic space $(\mathrm{V}, B)$ is said to be $n$-dimensional if $\mathrm{V}$ is $n$-dimensional as a $k$-vector space.

Upon fixing a basis $\{e_1, ..., e_n\}$ for $\mathrm{V}$, the quadratic space $(\mathrm{V}, B)$ determines uniquely a quadratic form $f_B$ given by

$$f_B(X) := B(X,X) = \sum_{i,j=1}^{n} B(e_i, e_j) X_i X_j.$$

**Theorem 1.6.** *Given a quadratic space $(\mathrm{V}, B)$ and two bases $\{e_1, ..., e_n\}$ and $\{e'_1, ..., e'_n\}$ for $\mathrm{V}$, the quadratic forms $\sum_{i,j=1}^{n} B(e_i, e_j) X_i X_j$ and $\sum_{i,j=1}^{n} B(e'_i, e'_j) X_i X_j$ are equivalent. Moreover a quadratic space $(\mathrm{V}, B)$ determines uniquely an equivalence class of quadratic forms.*

*Proof.* See [12, Chapter I, Section 1]. □

To render the above correspondence bijective, we require also a notion of equivalence of quadratic spaces.

**Definition 1.7.** *Two quadratic spaces $(\mathrm{V}, B_q)$ and $(\mathrm{W}, B_r)$ are called* ***isometric*** *if there is a vector space isomorphism $\phi : \mathrm{V} \to \mathrm{W}$ such that for all $X, Y \in \mathrm{V}$,*

$$B_q(X,Y) = B_r(\phi(X), \phi(Y)).$$

*We denote isometry by $(\mathrm{V}, B_q) \cong (\mathrm{W}, B_r)$.*

**Theorem 1.8.** *Isometry defines an equivalence relation on the set of all quadratic spaces over $k$.*

*Proof.* See [12, Chapter I, Section 1]. □

In fact, isometric quadratic spaces give rise to the same equivalence classes of quadratic forms.

**Theorem 1.9.** *There is a one-to-one correspondence between equivalence classes of quadratic forms and isometry classes of quadratic spaces, given by Theorem 1.6. We view this correspondence as an identification.*

*Proof.* See [12, Chapter I, Section 1]. □

Now that we have covered the basic definitions of quadratic forms and the equivalent notions of symmetric bilinear forms and quadratic spaces, we may begin to discuss some of the properties they may have.

**Theorem 1.10.** *Let* $(\mathrm{V}, B)$ *be a quadratic space. The following conditions are equivalent:*

1. *Let $f$ be a quadratic form belonging to the equivalence class associated to* $(\mathrm{V}, B)$*. The corresponding symmetric matrix $M_f$ is invertible,*

2. *The map $X \mapsto B(-, X)$ is a vector space isomorphism between* $\mathrm{V}$ *and its dual space* $\mathrm{V}^\star$*.*

3. $B(X, Y) = 0$ *for all* $Y \in \mathrm{V}$ *if and only if* $X = 0$*.*

*Proof.* See [12, Proposition I.1.2]. □

**Definition 1.11.** *A quadratic space* $(\mathrm{V}, B)$ *is called* ***regular*** *or* ***non-singular*** *if any (and therefore all) of the conditions of Theorem 1.10 hold.*

Observe that being a regular quadratic space is a class property under isometry, that is it holds for either all elements of an isometry class or none.

Let $\mathrm{V}$ be a $k$-vector space with $\mathrm{W}$ a subspace of $\mathrm{V}$, and $B : \mathrm{V} \times \mathrm{V} \to k$ a symmetric bilinear form. Then the restriction $B\mid_{\mathrm{W}\times\mathrm{W}}$ together with $\mathrm{W}$ forms a quadratic space as well.

We define the **orthogonal complement** of $\mathrm{W}$ in $\mathrm{V}$ (with respect to $B$) in the usual way:

$$\mathrm{W}^\perp := \{X \in \mathrm{V} \mid B(X, Y) = 0, \ \forall Y \in \mathrm{W}\}.$$

Note that $\mathrm{W}^\perp$ is also a vector subspace of V, and so $(\mathrm{W}^\perp, B\mid_{\mathrm{W}^\perp\times\mathrm{W}^\perp})$ is also a quadratic space. Similarly,

$$\mathrm{V}^\perp := \{X \in \mathrm{V} \mid B(X,Y) = 0,\ \forall Y \in \mathrm{V}\}.$$

By Definition 1.11, $(\mathrm{V}, B)$ is regular if and only if $\mathrm{V}^\perp = \{0\}$.

**Proposition 1.12.** *Let* $(\mathrm{V}, B)$ *be a quadratic space and* W *a subspace of* V*. Then*

$$\dim \mathrm{W} + \dim \mathrm{W}^\perp = \dim \mathrm{V}$$

*and*

$$(\mathrm{W}^\perp)^\perp = \mathrm{W}.$$

*Proof.* See [12, Proposition I.1.3]. □

One very important property of quadratic forms is that they can all be diagonalized, in the sense that every equivalence class of quadratic forms contains an element of the type

$$f(X) = \sum_{i=1}^{n} a_i X_i^2.$$

This allows us to express every quadratic form in a concise and easy to manipulate fashion, which we now work towards describing.

**Definition 1.13.** *Let* $d \in k^\times$*. We say that a quadratic form* $f$ ***represents*** $d$ *if there exists some* $X \in k^n$ *such that* $f(X) = d$*.*

Quadratic forms have the distinctive property that for all $a \in k$ and for any quadratic form $f$ over $k$, $f(aX) = a^2 f(X)$. Therefore if a quadratic form $f$ represents some element $d$ of $k^\times$, $f$ also represents $a^2 d$ for all $a \in k^\times$. To make use of this property we define the **group of square classes** of $k$.

**Definition 1.14.** *The square classes of* $k$ *are the multiplicative cosets of* $k^\times$ *modulo* $(k^\times)^2$*. The quotient group* $k^\times/(k^\times)^2$ *is called the group of square classes.*

We denote by $D(f)$ the set of all $d \in k^\times$ represented by $f$. In view of the above remarks, $D(f)$ is a union of square classes. Under the identification of square classes with elements of the quotient group, it is a subset of the group of square classes. In general, it is not a subgroup.

$D(f)$ is dependent only on the equivalence class of $f$, and so we may also discuss meaningfully the elements of $k^\times$ represented by a quadratic space, or an isometry class of quadratic spaces.

**Definition 1.15.** *If $D(f)$ is a subgroup of $k^\times/(k^\times)^2$, the quadratic form $f$ is called a* ***group form.***

There are important examples of group forms, including the Pfister forms with which we will later concern ourselves.

The next step in being able to manipulate quadratic forms and spaces is to develop some operations we can use to build up more complex quadratic spaces from simpler building blocks. These operations - orthogonal sums and tensor products - obey some familiar and desirable properties.

**Definition 1.16.** *Let* $(\mathrm{V}_1, B_1)$ *and* $(\mathrm{V}_2, B_2)$ *be quadratic spaces, and let* $\mathrm{V} := \mathrm{V}_1 \oplus \mathrm{V}_2$. *Define* $B : \mathrm{V} \times \mathrm{V} \to k$ *by*

$$B((x_1, x_2), (y_1, y_2)) = B_1(x_1, y_1) + B_2(x_2, y_2).$$

*Then* $(\mathrm{V}, B)$ *is a quadratic space called the* ***orthogonal sum*** *of* $(\mathrm{V}_1, B_1)$ *and* $(\mathrm{V}_2, B_2)$ *and denoted by*

$$(\mathrm{V}_1, B_1) \perp (\mathrm{V}_2, B_2).$$

If $f_1(X_1, ..., X_n)$ and $f_2(Y_1, ..., Y_m)$ are quadratic forms over $k$ associated to quadratic spaces $(\mathrm{V}_1, B_1)$ and $(\mathrm{V}_2, B_2)$ respectively, then the orthogonal sum $(\mathrm{V}_1, B_1) \perp (\mathrm{V}_2, B_2)$ has an associated quadratic form

$$f(X_1, ..., X_n, Y_1, ..., Y_m) = f_1(X_1, ..., X_n) + f_2(Y_1, ..., Y_m).$$

As one might hope, this operation respects our notions of equivalence for quadratic spaces. That is to say, the operation $\perp$ is well defined on isometry classes of quadratic spaces.

Moreover, orthogonal summation is both symmetric and associative when viewed as an operation on isometry classes of quadratic spaces. In other words, given three quadratic spaces, $(\mathrm{V}_1, B_1)$, $(\mathrm{V}_2, B_2)$, and $(\mathrm{V}_3, B_3)$ we have

1. $(\mathrm{V}_1, B_1) \perp (\mathrm{V}_2, B_2) \cong (\mathrm{V}_2, B_2) \perp (\mathrm{V}_1, B_1)$.
2. $((\mathrm{V}_1, B_1) \perp (\mathrm{V}_2, B_2)) \perp (\mathrm{V}_3, B_3) \cong (\mathrm{V}_1, B_1) \perp ((\mathrm{V}_2, B_2) \perp (\mathrm{V}_3, B_3))$.

By convention we write $\langle d \rangle$ for the isometry class of the one-dimensional quadratic space corresponding to the 1-fold quadratic form $f(X_1) = dX_1^2$, where $d \in k$. By the previous remarks concerning square classes, $\langle d \rangle \cong \langle d' \rangle$ for any $d'$ in the square class of $d$.

**Theorem 1.17.** *(Representation Criterion) Let* $(\mathrm{V}, B)$ *be a quadratic space and let* $f$ *be an associated quadratic form. Then for any element* $d \in k^\times$, $f$ *represents* $d$ *if and only if there* *exists a quadratic space* $(\mathrm{V}', B')$ *such that*

$$(\mathrm{V}, B) \cong \langle d \rangle \perp (\mathrm{V}', B').$$

*Proof.* See [12, Theorem I.2.3]. □

The following important corollary follows by induction.

**Corollary 1.18.** *Let* $(\mathrm{V}, B)$ *be an* $n$*-dimensional quadratic space over* $k$*, with an associated quadratic form* $f$*. Then there exist some* $d_i \in D(f) \cup \{0\}$ *such that*

$$(\mathrm{V}, B) \cong \langle d_1 \rangle \perp ... \perp \langle d_n \rangle.$$

For brevity, we denote $\langle d_1, ..., d_n \rangle := \langle d_1 \rangle \perp ... \perp \langle d_n \rangle$. This corollary can also be rewritten in the language of quadratic forms.

**Corollary 1.19.** *Every finite dimensional quadratic form can be diagonalized, that is to say if* $f$ *is an* $n$*-fold quadratic form over* $k$ *it is equivalent to some quadratic form of the type*

$$f'(x) = \sum_{i=1}^{n} d_i x_i^2$$

*with each* $d_i \in D(f) \cup \{0\}$*.*

*Proof.* See [12, Corollary I.2.4]. □

Using diagonalized forms renders many computations and properties more straightforward. For example, the **discriminant** of a quadratic form $f$ (written $d(f)$) is the square class of the determinant of the corresponding matrix $M_f$. The discriminant is a class property, i.e. if $f$ and $g$ are equivalent quadratic forms then $d(f) = d(g)$. Given a diagonalization $f \cong \langle f_1, ..., f_n \rangle$ it is then clear to see that

$$d(f) = [f_1 \dots f_n].$$

Now that we have some idea of how to decompose quadratic spaces into smaller parts, let us begin to classify these parts. One property that helps with this classification is the idea of isotropy.

**Definition 1.20.** *Let* $(\mathrm{V}, B)$ *be a quadratic space, and let* $X \in V$*. The vector* $X$ *is called* ***isotropic*** *if* $X$ *is nonzero and* $B(X, X) = 0$*.*

A quadratic space containing isotropic vectors is called an **isotropic** space. Moreover, a quadratic space in which every vector is isotropic, i.e. a quadratic space of the form

$$\langle 0\rangle \perp ... \perp \langle 0\rangle,$$

is called **totally isotropic**. A quadratic space which is not isotropic, that is which contains no isotropic vectors, is called an **anisotropic** quadratic space.

Suppose $(\mathrm{V}, B)$ is a regular $n$-dimensional quadratic space. We know that there are elements $d_1, ..., d_n$ of $k$ such that

$$(\mathrm{V}, B) \cong \langle d_1\rangle \perp ... \perp \langle d_n\rangle.$$

The space $(\mathrm{V}, B)$ has an associated quadratic form $f(X) = d_1X_1^2 + ... + d_nX_n^2$, with a corresponding matrix $M_f$ that is diagonal with entries $d_i$. Since $(\mathrm{V}, B)$ being regular implies $M_f$ is invertible, it is clear that each $d_i$ must be nonzero. In other words, $(\mathrm{V}, B)$ contains no vector $v$ such that $v$ is orthogonal to every vector in V (including itself.)

Already here we can see a starting point for decomposing spaces - it is clear that any quadratic space may be broken into a regular subspace and a totally isotropic subspace. As it turns out the types of regular spaces which can be isotropic are even more limited.

**Theorem 1.21.** *Every (regular) isotropic 2-dimensional form is isometric to* $\langle 1, -1\rangle$. *Such a form is called* ***hyperbolic plane*** *and denoted* $\mathbb{H}$.

*Proof.* See [12, Theorem I.3.2]. □

**Definition 1.22.** *An orthogonal sum of hyperbolic planes, that is to say a quadratic space of the form* $\mathbb{H} \perp ... \perp \mathbb{H}$ *is called a* ***hyperbolic space.*** *The corresponding quadratic form is called a* ***hyperbolic quadratic form*** *or a* ***split quadratic form.***

So the two dimensional space $\mathbb{H}$ and the one dimensional space $\langle 0\rangle$ are the two simplest examples of isotropic spaces. In fact, every more complex isotropic space contains copies of one or both of these spaces.

**Theorem 1.23.** (Witt's Decomposition Theorem*) Every quadratic space is an orthogonal sum of an anisotropic space, a hyperbolic space, and a totally isotropic space. Moreover, the summands are unique up to isometry.*

*Proof.* See [12, Theorem I.4.1] (the proof follows on p.14 after several other results). □

Expressed symbolically, for any quadratic space $(\mathrm{V}, q)$ there exists an anisotropic space $(\mathrm{V}_a, q_a)$, a hyperbolic space $(\mathrm{V}_h, q_h)$, and a totally isotropic space $(\mathrm{V}_t, q_t)$, which are unique up to isometry such that

$$(\mathrm{V}, q) \cong (\mathrm{V}_a, q_a) \perp (\mathrm{V}_h, q_h) \perp (\mathrm{V}_t, q_t).$$

The spaces $(\mathrm{V}_a, q_a)$, $(\mathrm{V}_h, q_h)$, and $(\mathrm{V}_t, q_t)$ are called respectively the **anisotropic, hyperbolic, and totally isotropic parts** of $(\mathrm{V}, q)$.

The hyperbolic part of a quadratic space V is necessarily of the form $m \cdot \mathbb{H}$ (meaning the orthogonal sum of $m$ copies of $\mathbb{H}$) for some integer $m$. This integer $m$ is called the **Witt index** of V.

One important tool used in the proof of this theorem, which is also essential to manipulating and determining isometry of quadratic spaces, is Witt's Cancellation Theorem.

**Theorem 1.24.** (Witt's Cancellation Theorem) *Let $f, g, h$ be quadratic forms such that $f \perp h \cong g \perp h$. Then $f \cong g$.*

*Proof.* See [12, Theorem I.4.2]. □

Another important operation on quadratic spaces is the so-called **tensor product** or **Kronecker product** which is defined as follows.

**Theorem 1.25.** *Consider two quadratic spaces $(\mathrm{V}_1, B_1)$ and $(\mathrm{V}_2, B_2)$, with $x_1, y_1 \in \mathrm{V}_1$ and $x_2, y_2 \in \mathrm{V}_2$. Let V be the tensor product of vector spaces $\mathrm{V} = \mathrm{V}_1 \otimes \mathrm{V}_2$. The tensor product of quadratic spaces $(\mathrm{V}, B) = (\mathrm{V}_1, B_1) \otimes (\mathrm{V}_2, B_2)$ defined by*

$$B(x_1 \otimes y_1, x_2 \otimes y_2) = B_1(x_1, y_1)B_2(x_2, y_2)$$

*is a quadratic space.*

*Proof.* See [12, Chapter I, Section 6]. □

Like orthogonal sums, tensor products are well-defined when viewed as operations on isometry classes of quadratic spaces, and they are symmetric and associative in the same sense. In addition they obey a distributive law over orthogonal sums.

**Theorem 1.26.** *Tensor products are associative, symmetric, and well-defined on isometry classes of quadratic forms. Tensor products also distribute over orthogonal sums, i.e. for all quadratic spaces $(V_i, B_i)$ with $i = 1, 2, 3$,*

$$(\mathrm{V}_1, B_1) \otimes ((\mathrm{V}_2, B_2) \perp (\mathrm{V}_3, B_3)) = ((\mathrm{V}_1, B_1) \otimes (\mathrm{V}_3, B_3)) \perp ((\mathrm{V}_1, B_1) \otimes (\mathrm{V}_2, B_2)).$$

*In particular for diagonal forms*

$$\langle a_1, ..., a_s\rangle \otimes \langle b_1, ..., b_r\rangle = \langle a_1b_1, ..., a_1b_r, a_2b_1, ..., a_sb_r\rangle,$$

*where $a_1, ..., a_s, b_1, ..., b_r \in k$.*

*Proof.* See [12, Chapter I Section 6]. □

The distributive property of tensor products over orthogonal sums has the following important consequence:

**Example 1.27.** *Let $f$ be an $n$-dimensional quadratic form. Then the tensor product $f \otimes \mathbb{H}$ is a hyperbolic space, in particular*

$$f \otimes \mathbb{H} \cong n \cdot \mathbb{H}.$$

*Proof.* Let $f \cong \langle f_1, ..., f_n\rangle$ be a diagonalization of $f$. Then one has

$$\begin{aligned} f \otimes \mathbb{H} &= \langle f_1, ..., f_n\rangle \otimes \langle 1, -1\rangle \\ &= \langle f_1, -f_1, ..., f_n, -f_n\rangle \\ &= \langle f_1, -f_1\rangle \perp ... \perp \langle f_n, -f_n\rangle \\ &= n \cdot \mathbb{H}. \end{aligned}$$

(Note that for all $a \in k$ the form $\langle a, -a\rangle$ is a regular two-dimensional form representing zero, and therefore a hyperbolic plane by Theorem 1.21.) □

# 2 Witt Rings

With the properties of orthogonal sums and tensor products given above we begin to see some semblance to a ring structure. Off hand, the isometry classes of quadratic spaces over $k$ do not form a ring due to the absence of additive inverses. An algebraic structure which does not necessarily have additive inverses, but which otherwise possesses a ring structure, is called a **semiring.**

**Theorem 2.1.** *Isometry classes of regular quadratic spaces over $k$ form a semiring with respect to the operations $\perp$ and $\otimes$.*

*Proof.* See [12, Chapter II Section 1]. □

Given such a structure, we construct a ring using a process known as the Grothendieck construction. Starting with a semiring $M$, we define an equivalence relation $\sim$ on $M \times M$ given by

$$(a, b) \sim (c, d) \iff a + d = b + c.$$

We then consider the equivalence classes of $M \times M$ modulo this relation. It is easy to check that these equivalence classes still form a semiring with the operations

$$(a, b) \oplus (c, d) := (a + c, b + d) \text{ and } (a, b) \otimes (c, d) := (ac + bd, ad + bc).$$

Furthermore, each element $(a, b)$ now has an additive inverse $(b, a)$ since

$$(a, b) + (b, a) = (a + b, b + a) \sim (0, 0).$$

So the equivalence classes of $M \times M/\sim$ form a ring, called the **Grothendieck ring** of $M$ and denoted $Groth(M)$.

Let $M(k)$ denote the semiring formed by all regular isometry classes of quadratic spaces over $k$, together with the operations $\perp$ and $\otimes$. Then the Grothendieck ring $Groth(M(k))$ of $M(k)$ is a ring called the **Witt-Grothendieck ring** which we will denote by $\widehat{W}(k)$.

Elements of the Witt-Grothendieck ring will be expressed as $q_1 - q_2$ (as opposed to $(q_1, q_2)$) where $q_1$ and $q_2$ are forms over $k$. By writing $q_1 \in \widehat{W}(k)$ we mean $q_1 - 0$. There is a well-defined notion of dimension in $\widehat{W}(k)$, namely

$$\dim(q_1 - q_2) = \dim(q_1) - \dim(q_2).$$

The Witt-Grothendieck ring possesses two very important ideals.

**Theorem 2.2.** *The natural map* $\dim : \widehat{W}(k) \twoheadrightarrow \mathbb{Z}$ *is a ring homomorphism. Its kernel is called the* ***fundamental ideal*** *of* $\widehat{W}(k)$*, denoted* $\hat{I}(k)$*.*

*Proof.* See [12, Chapter II Section 1]. □

The second important ideal is the ideal $\mathbb{Z} \cdot \mathbb{H}$ generated by all hyperbolic spaces and their additive inverses. By Example 1.27, this ideal in fact contains only hyperbolic spaces and inverses of hyperbolic spaces.

**Definition 2.3.** *The* ***Witt ring*** *is the quotient ring* $W(k) := \widehat{W}(k)/\mathbb{Z} \cdot \mathbb{H}$.

Since the operations in the Witt ring and Witt-Grothendieck ring arise directly from orthogonal sums and tensor products of quadratic spaces, we will also call these operations orthogonal sums and tensors products (or simply sums and products.) In these structures they will be denoted by $\oplus$ and $\otimes$, respectively.

The symbols $q_1 - q_2$ behave in a natural way in that

$$(q_1 - q_2) \oplus (q_3 - q_4) = (q_1 \oplus q_3) - (q_2 \oplus q_4),$$
$$(q_1 - q_2) \otimes (q_3 - q_4) = (q_1 \otimes q_3 \oplus q_2 \otimes q_4) - (q_1 \otimes q_4 \oplus q_2 \otimes q_3).$$

Additive inverses in the Witt ring appear in a more natural way compared to the Witt-Grothendieck ring. Let $q$ be an $n$-dimensional quadratic form and let $(-q)(X) := -q(X)$. Then in $W(k)$ one has

$$q \oplus (-q) = n \cdot \mathbb{H} = 0.$$

The image of the fundamental ideal $\hat{I}(k)$ of $\widehat{W}(k)$ under the quotient map $\widehat{W}(k) \twoheadrightarrow W(k)$ is called the fundamental ideal of $W(k)$, and is denoted by $I(k)$. The quadratic forms corresponding to elements of $I(k)$ are precisely those of even dimension.

Working in the Witt ring rather than the set of all isometry classes or in the Witt-Grothendieck ring is helpful because it gives us an algebraic structure which is simpler than that of the Witt-Grothendieck ring, while retaining all information regarding the anisotropic part of quadratic spaces. Since the isometry class of the hyperbolic and totally isotropic parts are dependent only on dimension, it is the anisotropic part which is by far the most interesting.

**Theorem 2.4.** *There is a one-to-one correspondence between anisotropic forms over $k$ and elements of $W(k)$. In particular, every element of the Witt ring has a unique representative which is anisotropic.*

*Proof.* See [12, Proposition II.1.4]. □

# 3 Pfister Forms

For $a \in k$ we denote by $\langle\langle a \rangle\rangle$ the two dimensional quadratic form $\langle 1, -a \rangle$. This is called a 1-fold Pfister form.

**Definition 3.1.** *A (n-fold) Pfister form is any quadratic form of the type $\langle\langle a_1, ..., a_n \rangle\rangle := \bigotimes_{i=1}^{n} \langle\langle a_i \rangle\rangle$, where the $a_i$ are in $k$.*

**Example 3.2.** *A hyperbolic plane $\mathbb{H} = \langle 1, -1 \rangle = \langle\langle 1 \rangle\rangle$ is a Pfister form.*

In fact, hyperbolic planes have a very special place among Pfister forms.

**Theorem 3.3.** *A Pfister form is isotropic if and only if it is a hyperbolic space.*

*Proof.* Clearly, if a Pfister form is hyperbolic then it is also isotropic. For a proof of the converse see [12, Theorem X.1.7]. □

This theorem can be reformulated as the following:

**Corollary 3.4.** *The Pfister form $\langle\langle x_1, ..., x_n, y\rangle\rangle$ is hyperbolic if and only if $\langle\langle x_1, ..., x_n\rangle\rangle$ represents $y$.*

A major cause for interest in Pfister forms is that they give us a path to studying the quotient rings $I^n/I^{n+1}$ for each natural number $n$. This is because the fundamental ideal $I$ of the Witt ring $W(k)$ is generated additively by quadratic forms of the type $\langle 1, a\rangle$, where $a$ varies over $k$ [12, Proposition II.1.2]. That is to say, $I$ is additively generated by the 1-fold Pfister forms over $k$. The following theorem is a result of this fact.

**Theorem 3.5.** *For all $n \in \mathbb{N}$, $I^n$ is additively generated by the $n$-fold Pfister forms over $k$.*

*Proof.* See [12, Proposition X.1.2]. □

The following result due to Arason and Pfister describes another important property of the powers of the fundamental ideal:

**Theorem 3.6.** (Hauptsatz) *Let $q$ be a quadratic form over $k$. If $q \in I^n$ and $\dim q < 2^n$ then $q$ is hyperbolic.*

*Proof.* See [2]. □

Recall that the elements of $k^\times$ represented by some particular form $f$ is a union of square classes of $k$, denoted by $D(f)$. We defined a group form to be a quadratic form for which the elements of the quotient group $k^\times/(k^\times)^2$ representing these square classes form a subgroup.

**Theorem 3.7.** *Let $\phi$ be a Pfister form over $k$. Then $\phi$ is a group form.*

*Proof.* See [12, Theorem X.1.8]. □

Any quadratic form $f$ over $k$ can also be considered as a quadratic form over any field extension $\ell$ of $k$. We denote $f$ viewed as a form over $\ell$ by

$$f_\ell := \ell \otimes_k f.$$

Suppose $\phi$ is an $n$-fold Pfister form (therefore a $2^n$-dimensional quadratic form). Let

$$X := (X_1, ..., X_{2^n}), \qquad Y := (Y_1, ..., Y_{2^n})$$

where the $X_i$ and $Y_j$ are indeterminates over $k$. Now let $\ell$ be the pure transcendental extension $k(X, Y)$ of $k$.

Certainly $\phi_\ell$ is still a Pfister form, and thus also a group form. This implies there exist some rational functions $Z_1, ..., Z_{2^n} \in k(X, Y)$ such that

$$\phi_\ell(X)\phi_\ell(Y) = \phi_\ell(Z_1, ..., Z_{2^n}),$$

or in other words $\phi_\ell$ represents $\phi_\ell(X)\phi_\ell(Y)$.

This observation motivates the definition of a **multiplicative form** over $k$.

**Definition 3.8.** *Let $q$ be an $n$-dimensional quadratic form over $k$, and let $X := (X_1, ..., X_n)$ and $Y := (Y_1, ..., Y_n)$ be $n$-tuples of indeterminates over $k$. The form $q$ is called a* ***multiplicative form*** *if $q_{k(X,Y)}$ represents $q(X)q(Y)$.*

As noted above, any Pfister form is multiplicative. In fact, among anisotropic forms the two notions are equivalent.

**Theorem 3.9.** *An anisotropic quadratic form $f$ over $k$ is multiplicative if and only if it is a Pfister form.*

*Proof.* See [12, Theorem X.2.8]. □

We conclude our preliminary discussion of quadratic forms with a lemma useful for computations in the Witt ring.

**Lemma 3.10.** *Let $a, b \in k$. Then in the Witt ring $W(k)$ we have*

$$\langle\langle a\rangle\rangle \oplus \langle\langle b\rangle\rangle = \langle\langle ab\rangle\rangle \oplus \langle\langle a, b\rangle\rangle.$$

*Proof.*

$$\begin{aligned}
\langle\langle ab\rangle\rangle \oplus \langle\langle a, b\rangle\rangle &= \langle 1, -ab, 1, -a, -b, ab\rangle \\
&= \langle 1, -a\rangle \oplus \langle 1, -b\rangle \oplus \langle -ab, ab\rangle \\
&= \langle\langle a\rangle\rangle \oplus \langle\langle b\rangle\rangle \oplus \mathbb{H} \\
&= \langle\langle a\rangle\rangle \oplus \langle\langle b\rangle\rangle
\end{aligned}$$

□

**Corollary 3.11.** *Let $x_1, ..., x_n, y, z \in k$. Then in the Witt ring $W(k)$ we have*

$$\langle\langle x_1, ..., x_n, y\rangle\rangle \oplus \langle\langle x_1, ..., x_n, z\rangle\rangle = \langle\langle x_1, ..., x_n, yz\rangle\rangle \oplus \langle\langle x_1, ..., x_n, y, z\rangle\rangle.$$

# CHAPTER II

# Root Systems

## 1 Root Systems

Let V be a finite dimensional vector space over $\mathbb{R}$, and let $\alpha \in$ V. A reflection with respect to $\alpha$ is an invertible linear transformation $s_\alpha$ such that

1. $s_\alpha(\alpha) = -\alpha$
2. The set $V^{s_\alpha} \subset$ V of vectors fixed by $s_\alpha$ is a hyperplane, that is to say a subspace of codimension 1.

**Lemma 1.1.** *Let $R$ be a finite set spanning* V *and let $\alpha \in R$. Then there exists at most one reflection $s_\alpha$ with respect to $\alpha$ such that $s_\alpha(R) = R$.*

*Proof.* See [16, Chapter V, Section 1]. □

**Definition 1.2.** *A finite set $\Sigma$ of vectors $\Sigma \subset$ V is called a (reduced)* ***root system*** *if it satisfies the following geometric properties:*

1. *$\Sigma$ spans* V.
2. *$\Sigma$ does not contain the zero vector.*
3. *For all $\alpha \in \Sigma$, there exists a reflection $s_\alpha$ with respect to $\alpha$ such that $s_\alpha(\Sigma) = \Sigma$. By Lemma 1.1 it is unique.*
4. *For all $\alpha, \beta \in \Sigma$, the vector $\beta - s_\alpha(\beta)$ is an integral multiple of $\alpha$.*
5. *For all $\alpha \in \Sigma$, the only scalar multiples of $\alpha$ contained in $\Sigma$ are $\pm\alpha$.*

If $\Sigma$ is a root system for a vector space V, then $\dim$ V is called the **rank** of $\Sigma$.

**Definition 1.3.** *The **Weyl group** of a root system $\Sigma$, denoted $W(\Sigma)$ is the subgroup of* $\mathrm{GL}(\mathrm{V})$ *generated by the set of reflections* $\{s_\alpha \mid \alpha \in \Sigma\}$.

Let V be a $k$-vector space with $B : \mathrm{V} \times \mathrm{V} \to k$ a bilinear form. Let $X \in \mathrm{GL}(\mathrm{V})$. One says that $X$ **preserves** $B$ if, for all $u, v \in \mathrm{V}$, one has $B(X(v), X(u)) = B(u, v)$.

For any such bilinear form $B$, the set of all linear transformations preserving $B$ is a subgroup of GL(V) called the **orthogonal group** of $B$ and denoted $O(B)$ or $O(B, \mathrm{V})$ if the space V is not clear from context.

Given a subgroup $G$ of GL(V) and a bilinear form $B$ on V, we say that $B$ is **invariant under** $G$ if $G \subseteq O(B, \mathrm{V})$.

**Proposition 1.4.** *Let $\Sigma$ be a root system for a vector space* V. *Then there exists a positive definite symmetric bilinear form* $(-,-) : \mathrm{V} \times \mathrm{V} \to \mathbb{R}$ *which is invariant under* $W(\Sigma)$.

*Proof.* See [16, Proposition V.1]. □

Let $\mathrm{V}^*$ denote the vector space dual of V. For $x \in \mathrm{V}^*$, $y \in \mathrm{V}$, we adopt the notation $\langle x, y\rangle := x(y)$. Then for each $\alpha \in \Sigma$ there is a unique element $\alpha^*$ of $\mathrm{V}^*$ such that $\langle \alpha^*, \alpha\rangle = 2$ and for all $v$ in the hyperplane $\mathrm{V}^{s_\alpha}$ of V fixed by $s_\alpha$, one has $\langle \alpha^*, v\rangle = 0$. This element $\alpha^*$ is called the **dual root** of $\alpha$.

**Proposition 1.5.** *Let $\Sigma$ be a root system for a vector space* V *and let*

$$\Sigma^* := \{\alpha^* \mid \alpha \in \Sigma\}.$$

*Then $\Sigma^*$ is a root system for $V^*$, called the **dual root system** of $\Sigma$.*

*Proof.* See [16, Proposition V.2]. □

It can be shown [16, Section 6] that for all $\alpha \in \Sigma$, $(\alpha^*)^* = \alpha$ and so $(\Sigma^*)^* = \Sigma$. For any root system $\Sigma$, we have

$$W(\Sigma) \simeq W(\Sigma^*).$$

**Proposition 1.6.** *For any choice of invariant (under $W(\Sigma)$) symmetric bilinear form*

$$(-,-) : \mathrm{V} \times \mathrm{V} \to \mathbb{R}$$

*and for all $\alpha, \beta \in R$, one has*

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

*Proof.* See [16, Section V.5]. □

Let $\Sigma$ be a root system for V and let $(-,-)$ be a fixed symmetric positive definite bilinear form on V, which is invariant under $W(\Sigma)$. The bilinear form $(-,-)$ defines a Euclidean structure on V whereby the length of a vector V is given by

$$|v| = \sqrt{(v,v)}.$$

Let $\theta_{\alpha,\beta}$ denote the angle between two roots $\alpha$ and $\beta$ with respect to this structure. A list of cases and possible values of $\theta_{\alpha,\beta}$ is given in [16, Chapter V Section 7]. In particular, the angle $\theta_{\alpha,\beta}$ is an integer multiple of either $\pi/6$ or $\pi/4$.

**Proposition 1.7.** *If $\alpha, \beta \in \Sigma$ are not colinear, and if $\langle \alpha^*, \beta \rangle > 0$, then $\alpha - \beta \in \Sigma$.*

*Proof.* See [16, Proposition V.3]. □

Let $R, R'$ be root systems for vector spaces $\mathrm{V}, \mathrm{V}'$. The root systems $R$ and $R'$ are **isomorphic** if there is a vector space isomorphism $\varphi : \mathrm{V} \to \mathrm{V}'$ such that $\varphi(R) = R'$ and for all $\alpha, \beta \in R$,

$$\langle \alpha^*, \beta \rangle = \langle \varphi(\alpha)^*, \varphi(\beta) \rangle.$$

**Definition 1.8.** *Let $\Sigma$ be a root system for a $k$-vector space* V*. A subset $S \subset \Sigma$ is called a **base** or **system of simple roots** for $\Sigma$ if*

1. *$S$ is a basis of $V$.*
2. *Every root $\alpha \in \Sigma$ can be written in the form*

$$\alpha = \sum_{s_i \in S} a_i s_i,$$

*where the $a_i$ are scalars in $\mathbb{R}$ each with the same sign.*

*An element of $S$ is called a **simple root.***

Every root system has a base (see [16, Theorem V.1]). Let $\Sigma$ be a root system and fix a base $S$. Then a root $\alpha$ in $\Sigma$ is called a **positive root** if the scalars $a_i$ in the above definition are positive. The set of positive roots in $\Sigma$ (with respect to $S$) is denoted $\Sigma^+$ or $\Sigma^+_S$ if $S$ is not clear from context. Roots which are not positive are called **negative roots** and the set of all negative roots in $\Sigma$ with respect to $S$ is denoted $\Sigma^-$ or $\Sigma^-_S$.

**Proposition 1.9.** *If $\Sigma$ is a root system with a base $S$ then*

$$S^* := \{\alpha^* \mid \alpha \in S\}$$

*is a base for the dual root system* $\Sigma^*$.

*Proof.* See [16, Proposition V.4]. □

Let $\Sigma$ be a root system for a vector space V and $S$ a base of $\Sigma$ with elements $\alpha_i$ indexed by natural numbers $i = 1, .., n$ where $n = \dim \mathrm{V}$.

The **Cartan matrix** for $\Sigma$ associated to $S$ is the matrix with $i, j$th entry equal to $\langle \alpha_i^*, \alpha_j \rangle$. The Cartan matrix determines the root system up to isomorphism (see [16, Proposition V.8]).

# 2 Dynkin Diagrams

Let $\Sigma$ be a root system with a base $S$. The **Coxeter graph** of $\Sigma$ with respect to $S$ is a multigraph with vertices for each element in $S$, such that the number of edges joining the vertices corresponding to $\alpha, \beta \in S$ is equal to $\langle \alpha^*, \beta \rangle \langle \beta^*, \alpha \rangle$.

**Proposition 2.1.** *The isomorphism class of the Coxeter graph is independent of the choice of* $S$.

*Proof.* This is a direct result of [12, Theorem V.2]. □

Let $\Sigma_1$ and $\Sigma_2$ be root systems of vector spaces $\mathrm{V}_1$ and $\mathrm{V}_2$, respectively. Then $\Sigma_1 \cup \Sigma_2$ is a root system for $\mathrm{V}_1 \oplus \mathrm{V}_2$. This new root system is called the **direct sum** of $R_1$ and $R_2$.

**Definition 2.2.** *A root system is called **reducible** if it is isomorphic to the direct sum of two other nonzero root systems. Otherwise, it is called **irreducible.***

**Proposition 2.3.** *A root system* $\Sigma$ *is irreducible if and only if its Coxeter graph is nonempty and connected.*

*Proof.* See [16, Proposition V.12]. □

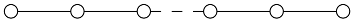
Unfortunately, Coxeter graphs do not determine uniquely the isomorphism class of their root system. This is remedied with the introduction of **Dynkin diagrams.**

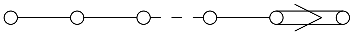
**Definition 2.4.** *The Dynkin diagram of a root system* $\Sigma$ *with base* $S$ *is a directed Coxeter graph of* $\Sigma$ *with respect to* $S$, *so that every edge between two non-orthogonal vertices is directed toward the shorter of the two.*

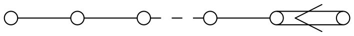
**Proposition 2.5.** *The Dynkin diagram of a root system determines that root system up to isomorphism.*

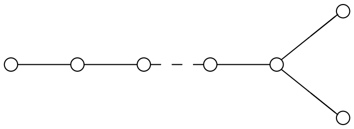
*Proof.* See [16, Proposition V.13]. □

By the above facts, a classification of root systems amounts to a classification of connected Dynkin diagrams. There are 4 infinite families of connected Dynkin diagrams with $n$ vertices.

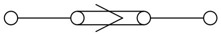
$A_n$ :


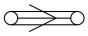
$B_n$ :


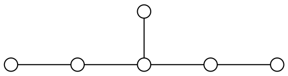
$C_n$ :


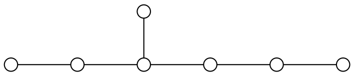
$D_n$ :


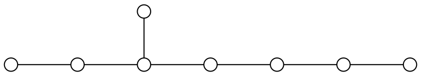
In addition there are 5 exceptional cases.

$F_4$ :


$G_2$ :


$E_6$ :


$E_7$ :


$E_8$ :


(See [16, Chapter V, Section 14].)

# CHAPTER III

# Galois Cohomology

## 1 Cohomology Groups

Let $G$ be an (abstract) group. By a $G$-module we mean a $\mathbb{Z}[G]$-module. Let $A$ be a $G$-module. We denote by $A^G$ the submodule of $A$ consisting of all elements $a \in A$ which are invariant under $G$. One has

$$\mathrm{Hom}_G(\mathbb{Z}, A) = \mathrm{Hom}(\mathbb{Z}, A)^G \cong A^G,$$

where we view $\mathbb{Z}$ as a trivial $G$-module and $\mathrm{Hom}_G(\mathbb{Z}, A)$ denotes the group of $G$-module homomorphisms $\mathbb{Z} \to A$ and $\mathrm{Hom}(\mathbb{Z}, A)$ the group of abstract group homomorphisms, with the action of $G$ on $\mathrm{Hom}(\mathbb{Z}, A)$ induced by that on $A$.

Since the $\mathrm{Hom}(\mathbb{Z}, -)$ is a covariant, left-exact functor, the above equation implies that $A^G$ is also a covariant left-exact functor from $G$-modules to abelian groups.

That is to say, for every short exact sequence of $G$-modules

$$0 \to A \to B \to C \to 0$$

there is an induced sequence of abelian groups

$$0 \to A^G \to B^G \to C^G$$

which is also exact.

**Definition 1.1.** *A $G$-module is called* ***co-induced*** *if it is isomorphic to some $G$-module of the form $\mathrm{Hom}(\mathbb{Z}[G], X)$ where $X$ is any abelian group (here the action of $G$ on $\mathbb{Z}[G]$ is by left multiplication).*

**Definition 1.2.** *A* ***cohomological extension*** *of the functor $A^G$ is a sequence of functors*

$$H^q(G, A) : G\text{-modules} \to \text{Abelian groups}$$

*for all non-negative integers $q$ which satisfy the following conditions:*

1. *For all $G$-modules $A$, one has $H^0(G, A) = A^G$.*
2. *For short exact sequences of $G$-modules*

   $$0 \to A \to B \to C \to 0$$

   *there exist boundary morphisms $\delta : H^q(G, C) \to H^{q+1}(G, A)$ such that the sequence*

   $$... \to H^q(G, A) \to H^q(G, B) \to H^q(G, C) \xrightarrow{\delta} H^{q+1}(G, A) \to ...$$

   *is exact.*
3. *If $A$ is a co-induced module, then for all $q \geq 1$ one has $H^q(G, A) = 0$.*

**Theorem 1.3.** *There exists one and only one cohomological extension of the functor $A^G$, up to canonical equivalence.*

*Proof.* See [6, Theorem IV.1]. □

**Definition 1.4.** *The groups $H^q(G, -)$ whose existence and uniqueness guaranteed by Theorem 1.3 are called the ($q$-th)* ***cohomology groups*** *of $A$.*

**Definition 1.5.** *A* ***free resolution*** *of a $G$-module $A$ is an exact sequence*

$$... \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} A \to 0$$

*such that $P_i$ is a free module for all non-negative integers $i$.*

The existence portion of the proof of Theorem 1.3 given in [6] involves choosing a free resolution

$$... \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} \mathbb{Z} =: P_{-1}$$

of the $G$-module $\mathbb{Z}$. The existence of such a resolution is guaranteed by a well-known result in ring theory.

The **standard complex** is a particular choice of this resolution, namely $P_i := \mathbb{Z}[G^{i+1}]$ for all non-negative integers $i$. Note that $P_i$ has a basis of the form

$$G \times ... \times G \quad (i+1 \text{ factors})$$

with elements $(g_0, ..., g_i)$. For ease of notation, throughout this section we will define actions and homomorphisms on this basis, with the understanding that they may be extended linearly to all of $P_i$.

The action of $G$ on $P_i$ is defined for all $s, g_0, ..., g_i \in G$ by

$$s.(g_0, ..., g_i) = (sg_0, ..., sg_i).$$

The homomorphisms $d_i : P_i \to P_{i-1}$ are given by

$$d_i : (g_0, ..., g_i) \mapsto \sum_{j=0}^{i} (-1)^j (g_0, ..., g_{j-1}, g_{j+1}, ..., g_i).$$

Note that for $i = 0$ this definition results in the constant map

$$d_0 : g \mapsto 1.$$

The proof of Theorem 1.3 also defines the complex $K$ to be

$$0 \to \mathrm{Hom}_G(P_0, A) \xrightarrow{\delta_0} \mathrm{Hom}_G(P_1, A) \xrightarrow{\delta_1} ...$$

and the $i$-th cohomology group $H^i(G, A)$ of $A$ is taken to be the $i$-th cohomology group of the complex $K$, i.e. the group

$$\ker(\delta_i)/\mathrm{im}(\delta_{i-1}).$$

**Definition 1.6.** *An $i$-cocycle is an element of* $\ker(\delta_i)$*, and $i$-coboundary is an element of* $\mathrm{im}(\delta_{i-1})$*. So an element of the $i$-th cohomology group is an equivalence class of $i$-cocycles, modulo $i$-coboundaries. We will very often use cocycles in their capacity as a representative of an element of a cohomology group.*

Now consider some $f \in \mathrm{Hom}_G(P_i, A)$. A priori, $f$ is a map $G^{i+1} \to A$ such that for all $s, g_0, ..., g_i \in G$

$$f(sg_0, ..., sg_i) = s.f(g_0, ..., g_i).$$

Let $\varphi : G^i \to A$ be a function defined by

$$\varphi(g_1, ..., g_i) = f(1, g_1, g_1g_2, ..., g_1...g_i).$$

One can check that $\varphi$ determines $f$ - we will view this as an identification, whereby we can view an $i$-cocycle as a map $G^i \to A$ rather than $G^{i+1} \to A$.

**Proposition 1.7.** *A map $\varphi : G \to A$ is a 1-cocycle if and only if for all $g, h \in G$ one has*

$$\varphi(gh) = \varphi(g) + g.\varphi(h).$$

*Such a map is called a* ***crossed homomorphism.***

*Proof.* See [6, Chapter IV, Section 2]. □

**Proposition 1.8.** *A 1-cocycle $\varphi$ is a 1-coboundary if and only if there exists some $a \in A$ such that for all $g \in G$*

$$\varphi(g) = g.a - a.$$

*Proof.* See [6, Chapter IV, Section 2]. □

**Proposition 1.9.** *A function $\varphi : G \times G \to A$ is a 2-cocycle if and only if it satisfies the following condition for all $g_1, g_2, g_3 \in G$ :*

$$g_1.\varphi(g_2, g_3) - \varphi(g_1g_2, g_3) + \varphi(g_1, g_2g_3) - \varphi(g_1, g_2) = 0.$$

*Proof.* See [6, Chapter IV, Section 2]. □

Let $G$ be a group with $G' < G$, and let $A'$ be a $G'$-module. We can define the $G$-module $A := \mathrm{Hom}_{G'}(\mathbb{Z}[G], A')$ (where $\mathbb{Z}[G]$ has a natural $G'$-module structure induced by the inclusion map $G' \hookrightarrow G$ and left-multiplication) with the action of $G$ on $A$ given by

$$(g.\varphi)(z) = \varphi(zg^{-1})$$

for all $g \in G$, $\varphi \in A$, $z \in \mathbb{Z}[G]$.

**Proposition 1.10.** *(Shapiro's Lemma) In the above setting,*

$$H^q(G, A) = H^q(G', A') \quad \text{for all } q \geq 0.$$

*Proof.* See [6, Proposition IV.2]. □

If $H$ and $G$ are groups and $f : H \to G$ a group homomorphism, then $f$ induces a homomorphism of the standard complexes discussed previously in this section. Resultantly, $f$ also induces homomorphisms

$$f^* : H^q(G, A) \to H^q(H, A)$$

defined for any $G$-module $A$ and for all non-negative integers $q$.

**Example 1.11.** *Let $G$ be a group with $H < G$, and let $\iota : H \hookrightarrow G$ be the inclusion map. Then the induced homomorphisms*

$$\iota^* : H^q(G, A) \to H^q(H, A)$$

*are called the **restriction homomorphisms,** and are denoted by* Res.

**Example 1.12.** *Let $G$ be a group, $H \triangleleft G$ a normal subgroup, and $A$ a $G$-module. Let $\pi : G \twoheadrightarrow G/H$ be the quotient map. Endow $A^H$ with the natural $G/H$ module structure arising from the $G$-module structure of $A$. Then $\pi$ induces homomorphisms*

$$\pi^* : H^q(G/H, A^H) \to H^q(G, A^H).$$

*Composing $\pi^*$ with the homomorphisms $H^q(G, A^H) \to H^q(G, A)$ induced by the inclusion $A^H \hookrightarrow A$ yields new homomorphisms*

$$\mathrm{Inf} : H^q(G/H, A^H) \to H^q(G, A)$$

*called the **inflation homomorphisms.***

**Proposition 1.13.** *(Group Extension) Let $G$ be a group, $H \triangleleft G$ a normal subgroup, and $A$ a $G$-module. Then the sequence*

$$0 \to H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G, A) \xrightarrow{\mathrm{Res}} H^1(H, A)$$

*is exact.*

*Proof.* See [6, Proposition IV.4]. □

**Proposition 1.14.** *Let $G$ be a group, $H \triangleleft G$ a normal subgroup, and $A$ a $G$-module. Let $q \geq 1$ and suppose that for all $i = 1, ..., q-1$ one has $H^i(H, A) = 0$. Then*

$$0 \to H^q(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^q(G, A) \xrightarrow{\mathrm{Res}} H^q(H, A)$$

*is an exact sequence.*

*Proof.* See [6, Proposition IV.5]. □

Let $A$ be a $G$-module and $H$ a subgroup of $G$ with finite index $n$. There are maps called the **corestriction maps**

$$\mathrm{Cor} : H^q(H, A) \to H^q(G, A)$$

defined for all nonnegative integers $q$. In reality these maps arise more naturally on the **homology groups,** which we will not discuss here. However, they may also be defined on cohomology groups using an explicit construction for $q = 0$ and then by applying the technique of **dimension shifting** to extend to $q \geq 1$.

Recall that there are natural identifications $H^0(H, A) = A^H$ and $H^0(G, A) = A^G$, and so we may define Cor for $q = 0$ as a map $A^H \to A^G$. Let $\{g_1, ..., g_n\}$ be a set of left coset representatives for $H$ in $G$, and define

$$\begin{aligned} \mathrm{Cor} : A^H &\to A^G \\ a &\mapsto \sum_{i=0}^{n} g_i.a. \end{aligned}$$

One must check that the map Cor does not depend on our choice of $g_i$, and that elements of the image are invariant under $G$. Indeed, if $g_i$ and $g_i'$ are representatives of the same coset of $H$, then there exists some $h \in H$ such that $g_i' = g_i h$ and so for all $a \in A^H$

$$g_i'.a = (g_i h).a = g_i.(h.a) = g_i.a,$$

meaning Cor is independent of our choices $g_i$. Furthermore, for all $g \in G$ the set $\{gg_1, ..., gg_n\}$ is still a set of coset representatives. Thus for all $a \in A^H$

$$g. \sum_{i=1}^{n} g_i.a = \sum_{i=1}^{n} (gg_i).a = \sum_{i=1}^{n} g_i.a,$$

i.e. $\mathrm{Cor}(a)$ is invariant under the action of $G$. We now extend Cor to $q \geq 1$ via dimension shifting.

Consider a $G$-module $A$, and let $A^*$ be the $G$-module $\mathrm{Hom}(G, A)$. Consider the map

$\varphi : A \to A^*$ given by

$$\begin{aligned} \varphi(a) : G &\to A \\ g &\mapsto ga \end{aligned}$$

and let $A'$ be the quotient module $A^*/\varphi(A)$. Then the sequence

$$0 \to A \to A^* \to A' \to 0$$

is exact. Moreover, since $A^*$ is co-induced, the resultant long exact sequence of cohomology groups includes boundary maps which are isomorphisms

$$H^q(G, A') \xrightarrow{\sim} H^{q+1}(G, A)$$

for all $q \geq 1$.

In particular, this isomorphism allows us to inductively define the corestriction map (and indeed many other maps) on the groups $H^q(G, A)$.

**Proposition 1.15.**

*If $H < G$ with finite index $n$, then the map*

$$\mathrm{Cor} \circ \mathrm{Res} : H^q(G, A) \to H^q(G, A)$$

*sends*

$$\varphi \mapsto n \times \varphi := \varphi + ... + \varphi, \qquad (n \text{ summands.})$$

*Proof.* See [6, Proposition IV.8]. □

**Theorem 1.16.** *Let $G$ be a group. There exists a unique family of homomorphisms called the **cup product***

$$\begin{aligned} \cup : H^p(G, A) \otimes H^q(G, B) &\to H^{p+q}(G, A \otimes B) \\ \alpha \otimes \beta &\mapsto \alpha \cup \beta \end{aligned}$$

*defined functorially for all $G$-modules $A, B$ (where $G$ acts componentwise on $A \otimes B$) and for all nonnegative integers $p, q$ which satisfy the following properties:*

1. *The diagram*

$$\begin{tikzcd}
A^G \otimes B^G \arrow[r] \arrow[d, "\otimes"] & H^0(G,A) \otimes H^0(G,B) \arrow[d, "\cup"] \\
(A \otimes B)^G \arrow[r] & H^0(G, A \otimes B)
\end{tikzcd}$$

   *is commutative.*

2. *Let $A, A', A'', B$ be $G$ modules. Given a short exact sequence*

$$0 \to A \to A' \to A'' \to 0,$$

   *if the induced sequence*

$$0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$$

   *is also exact, then for all nonnegative integers $p, q$ and for all $\alpha'' \in H^p(G, A'')$, $\beta \in H^q(G, B)$, one has*

$$(\delta(\alpha'')) \cup \beta = \delta(\alpha'' \cup \beta) \in H^{p+q+1}(G, A \otimes B)$$

   *where $\delta$ represents the boundary homomorphisms of Definition 1.2.*

3. *Let $A, B, B', B''$ be $G$ modules. Given a short exact sequence*

$$0 \to B \to B' \to B'' \to 0,$$

   *if the induced sequence*

$$0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$$

   *is also exact, then for all nonnegative integers $p, q$ and for all $\alpha \in H^p(G, A)$, $\beta'' \in H^q(G, B'')$, one has*

$$\alpha \cup \delta(\beta'') = (-1)^p \delta(\alpha \cup \beta'') \in H^{p+q+1}(G, A \otimes B).$$

*Proof.* See [6, Theorem IV.4]. □

Suppose we let $A = B = \mathbb{Z}/2\mathbb{Z}$ with trivial $G$-module structure. Then $A \otimes B \cong \mathbb{Z}/2\mathbb{Z}$

and so we have maps defined for all nonnegative integers $p, q$

$$\cup : H^q(G, \mathbb{Z}/2\mathbb{Z}) \otimes H^p(G, \mathbb{Z}/2\mathbb{Z}) \to H^{p+q}(G, \mathbb{Z}/2\mathbb{Z}).$$

These maps allow us to give a ring structure on the abelian group

$$H^*(G, \mathbb{Z}/2\mathbb{Z}) := \bigoplus_{p \geq 0} H^p(G, \mathbb{Z}/2\mathbb{Z}),$$

with the operations $\oplus$ and $\cup \circ \otimes$.

We conclude the section by listing some more convenient properties of the cup product.

**Proposition 1.17.** *The cup product has the following properties for all $G$-modules $A, B, C$ and for all $\alpha \in H^i(G, A)$, $\beta \in H^j(G, B)$, $\gamma \in H^\ell(G, C)$ where $i, j, \ell$ are nonnegative integers:*

1. $(\alpha \cup \beta) \cup \gamma = \alpha \cup (\beta \cup \gamma)$.
2. $\mathrm{Res}(\alpha \cup \beta) = \mathrm{Res}(\alpha) \cup \mathrm{Res}(\beta)$
3. $\mathrm{Cor}(\alpha \cup \mathrm{Res}(\beta)) = \mathrm{Cor}(\alpha) \cup \beta$.

*Proof.* See [6, Proposition IV.9]. □

# 2 Abelian Galois Cohomology

**Galois cohomology** is a special case of the cohomology groups of the previous section.

Let $\ell$ be a Galois extension of $k$. Recall that the **Galois group** of $\ell/k$ is defined as

$$\mathrm{Gal}(\ell/k) = \{\sigma : \ell \xrightarrow{\sim} \ell \mid \sigma(x) = x \quad \forall x \in k\}.$$

**Definition 2.1.** *Let $\{H_i\}$ be a family of groups indexed by a set $I$ which is equipped with a partial order $<$ such that for all $i < j$ there exists a homomorphism*

$$\varphi_{ji} : H_j \to H_i.$$

*The **inverse limit** (or **projective limit**) of the family $\{H_i\}$ is the set*

$$\varprojlim \{H_i\} := \{(..., h_i, h_j, ...) \in \prod_{i \in I} H_i \mid \varphi_{ji}(h_j) = h_i \quad \forall i < j\}.$$

**Proposition 2.2.** *The Galois group* $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ *is naturally isomorphic to the inverse limit*

$$\varprojlim \mathrm{Gal}(\ell/k)$$

*where* $\ell$ *varies over finite Galois extensions of* $k$*. Here the partial ordering is given by* $\ell > \ell'$ *if* $\ell'$ *is a subfield of* $\ell$ *and the homomorphisms*

$$\varphi : \mathrm{Gal}(\ell/k) \to \mathrm{Gal}(\ell'/k)$$

*are given by* $\sigma \mapsto \sigma|_{\ell'}$.

*Proof.* To give an element of the inverse limit is to give for each finite Galois extension $\ell/k$ an element of the Galois group $\mathrm{Gal}(\ell/k)$, that is an automorphism

$$\sigma_\ell : \ell \to \ell$$

which is the identity map on $k$, such that for any larger finite Galois extension $\ell \subset \ell' \subset k^{\mathrm{sep}}$ one has $\sigma'_\ell \mid_\ell = \sigma_\ell$.

We wish to see that given such a family of automorphisms there exists a unique $\varphi \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$ such that $\sigma_\ell = \varphi|_\ell$ for all finite Galois extensions $\ell/k$. To define such an automorphism, let $x$ be in $k^{\mathrm{sep}}$, then $x$ also lies in some finite Galois extension $\ell/k$. It is well-defined to set $\varphi(x) = \sigma_\ell(x)$, since if $x$ lies in another finite Galois extension $\ell'$ then there is a third finite Galois extension $\ell, \ell' \subset \ell'' \subset k^{\mathrm{sep}}$ and one has

$$\sigma_\ell(x) = \sigma_{\ell'}(x) = \sigma_{\ell''}(x).$$

This map is obviously injective.

To see that it is surjective, suppose we are given an element $\sigma$ of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$. It suffices to see that for every finite Galois extension $\ell/k$, the restriction $\sigma_\ell := \sigma|_\ell$ of $\sigma$ to $\ell$ is an automorphism of $\ell$, in particular that $\sigma(x) \in \ell$ for all $x \in \ell$.

Indeed, let $x \in \ell$. Then $x$ is the solution of an irreducible monic polynomial $f$ with coefficients in $k$, i.e. there exist elements $a_0, ..., a_{n-1} \in k$ such that

$$x^n + a_{n-1}x^{n-1} + ... + a_0 = 0.$$

Then one also has

$$\sigma(x^n + a_{n-1}x^{n-1} + ... + a_0) = \sigma(x)^n + a_{n-1}\sigma(x)^{n-1} + ... + a_0 = 0.$$

Moreover $f$ splits in $\ell$, so that there exist elements $b_0, ..., b_n \in \ell$ such that

$$\sigma(x)^n + a_{n-1}\sigma(x)^{n-1} + ... + a_0 = (\sigma(x) - b_0) \cdot ... \cdot (\sigma(x) - b_n) = 0.$$

Thus $\sigma(x) = b_i$ for some $i = 1, ..., n$, and so $\sigma(x) \in \ell$. □

Let $\Gamma$ be the group $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ equipped with the profinite topology, that is the topology for which normal subgroups $N \lhd \Gamma$ with finite index form a basis of open sets.

Let $A$ be a discrete $\Gamma$-module on which $\Gamma$ acts continuously. Notice that since $A$ has the discrete topology this means that the fibers of the action map

$$\Gamma \times A \to A$$

are open sets.

**Proposition 2.3.** *The action of* $\Gamma$ *on* $A$ *is continuous if and only if* $\mathrm{Stab}_\Gamma(a)$ *is open for all* $a \in A$.

*Proof.* As noted above, it is clear that the action is continuous if and only if the fibers of the action map are open sets. For all $b \in \mathrm{Orb}_\Gamma(a)$ choose a particular $\sigma_b \in \Gamma$ with $\sigma_b(b) = a$, then the fiber of $a$ is the set

$$\{(\varphi \circ \sigma_b, b) \mid b \in \mathrm{Orb}_\Gamma(a), \varphi \in \mathrm{Stab}_\Gamma(a)\}.$$

Recall that in a topological group, translation maps are homeomorphisms. Therefore the sets

$$\{\varphi \circ \sigma_b \mid b \in \mathrm{Orb}_\Gamma(a), \varphi \in \mathrm{Stab}_\Gamma(a)\}$$

are open if and only if $\mathrm{Stab}_\Gamma(a)$ is open, and since $A$ is given the discrete topology the fiber of $a$ is open if and only if each of those sets are. □

Choose a discrete $\Gamma$-module $A$ with a continuous action as described above. We will commonly work with the **mod 2 Galois cohomology,** that is the case where $A = \mu := \mathbb{Z}/2\mathbb{Z}$.

There are two equivalent ways in which to define the **Galois cohomology groups.** First, we may apply the construction of Section 1, with the additional mandate that all $\Gamma$-modules be given the discrete topology and all actions and maps are continuous.

The **Galois cohomology groups** are the resultant groups

$$H^q(k, A) := H^q(\Gamma, A).$$

An equivalent definition arises from the direct limit.

**Definition 2.4.** *Let $\{H_i\}$ be a family of groups indexed by a set $I$ equipped with a partial order $<$ such that for all $i < j \in I$ there exists a homomorphism*

$$\varphi_{ij} : H_i \to H_j.$$

*We define an equivalence relation $\sim$ on $\bigsqcup_{i \in I} H_i$ such that for all $i, j \in I$ and for all $h_i \in H_i, h_j \in H_j$, we have $h_i \sim h_j$ if there exists some $k \in I$ such that $\varphi_{ik}(h_i) = \varphi_{jk}(h_j)$. The* ***direct limit*** *(or* ***inductive limit****) of the family $\{H_i\}$ is the quotient set*

$$\varinjlim H_i = \bigsqcup_{i \in I} H_i / \sim .$$

Let $\{F_i\}$ be the family of finite Galois field extensions over $k$, and let $<$ be a partial ordering of $I$ given by $i < j$ if and only if $F_i \subseteq F_j$. Let the maps $\varphi_{ij}$ be the inclusion maps.

Let $A$ be a discrete $\Gamma$-module with a continuous action. For all $i \in I$, let $A^i$ be the submodule of $A$ invariant under each element of $\mathrm{Gal}(k^{\mathrm{sep}}/F_i) < \Gamma$. This module has a natural structure as a $\mathrm{Gal}(F_i/k)$-module arising from the $\Gamma$-module structure of $A$, and so we may consider the cohomology groups $H^q(\mathrm{Gal}(F_i/k), A^i)$.

Now, suppose $F_i$ and $F_j$ are finite Galois extensions of $k$ with $F_i \subseteq F_j$. We have restriction and inclusion maps

$$r : \mathrm{Gal}(F_j/k) \twoheadrightarrow \mathrm{Gal}(F_i/k)$$
$$i : A^i \hookrightarrow A^j$$

by which we may define a homomorphism

$$\varphi_{ij} : H^q(\mathrm{Gal}(F_i/k), A^i) \to H^q(\mathrm{Gal}(F_j/k), A^j)$$
$$\sigma : \mapsto i \circ \sigma \circ r$$

(see the construction of the inflation map in Example 1.12).

**Proposition 2.5.** *Let $q$ be a nonnegative integer, and let $\{H_i\}$ be the family*

$$H_i := H^q(\mathrm{Gal}(F_i/k), A^i)$$

*with the partial ordering $<$ and homomorphisms $\varphi_{ij}$ described above. Then*

$$\varinjlim H_i \cong H^q(k, A).$$

*Proof.* See [17, Section II.1.1]. □

We conclude this section with the following fundamental result due to Emmy Noether:

**Theorem 2.6.** *(Hilbert's Theorem 90) Let $\ell/k$ be a Galois extension. Then*

$$H^1(\ell/k, G_m(\ell)) = H^1(\ell/k, \ell^*) = 1.$$

# 3 Residue Maps

**Theorem 3.1.** *Let $G$ be a profinite group with let $N \triangleleft G$ a closed normal subgroup, and let $C$ be a discrete $G/N$ module. Suppose that the short exact sequence*

$$1 \to N \to G \to G/N \to 1$$

*is split and that for all $i > 1$ one has $H^i(N, C) = 0$. Let $\pi_i$ be the natural map $H^i(G/N, C) \to H^i(G, C)$ induced by the quotient $G \twoheadrightarrow G/N$,using the natural interpretation of $C$ as a $G$-module arising from its structure as a $G/N$-module. Then there exists a map*

$$r : H^i(G, C) \to H^{i-1}(G/N, \mathrm{Hom}(N, C))$$

*called the* ***residue map*** *such that the sequence*

$$0 \to H^i(G/N, C) \xrightarrow{\pi_i} H^i(G, C) \xrightarrow{r} H^{i-1}(G/N, \mathrm{Hom}(N, C)) \to 0$$

*is exact.*

*Proof.* See [9, Theorem II.6.1]. □

The residue map behaves well with respect to cup product. In particular, suppose $C_1, C_2$ are $G/N$-modules as in Theorem 3.1. Let $i$ and $j$ be positive integers and let $\alpha \in H^i(G, C_1)$ and $\beta \in H^j(G/N, C_2)$.

**Proposition 3.2.** *In the above situation, one has*

$$r(\alpha \cup \beta) = r(\alpha) \cup \beta \in H^{i+j-1}(G/N, \mathrm{Hom}(N, C_1 \otimes C_2)).$$

*Proof.* See [9, Proposition II.6.6]. □

Now, let $k$ be a field together with a discrete valuation $v : k \to \mathbb{Z}$, and let $\overline{k}$ be the residue field of $k$ (with respect to $v$.) We further assume for the sake of simplicity that $k$ is complete. As usual, let $k^{\text{sep}}$ be a separable closure of $k$.

Recall that a field extension $\ell$ of $k$ with discrete valuation $v$ is called **unramified** if the ramification index $e_{w/v}$ for a unique extension of discrete valuation $v$ to $\ell$ is equal to 1. In other words, the extension is unramified if a uniformizer $\pi \in k$ for $v$ is still a uniformizer for $w$. It is well known that there is a unique maximal unramified extension inside $k^{\text{sep}}$ of any such field.

Let $k^{\text{un}}$ be the maximal unramified extension of $k$. It follows from Hensel's Lemma that $\text{Gal}(k^{\text{un}}/k) \simeq \text{Gal}(\overline{k}^{\text{sep}}/\overline{k})$.

**Definition 3.3.** *The* ***inertia group*** *of $k$, which we denote by $I_k$, is the kernel of the natural map*

$$\text{Gal}_k \to \text{Gal}_{\overline{k}}.$$

*That is to say,* $\text{Gal}_k/I = \text{Gal}(k^{\text{un}}/k)$.

Let $C$ be a finite $\Gamma_{\overline{k}}$-module whose order is not divisible by the characteristic of the residue field. We may view $C$ as a $\Gamma_k$-module on which the inertia group acts trivially.

**Lemma 3.4.** *The sequence $1 \to I_k \to \Gamma_k \to \Gamma_{\overline{k}} \to 1$ satisfies the hypotheses of Theorem 3.1, that is to say*

1. *the sequence above is exact and split,*

2. *for all $i > 1$, one has $H^i(I, C) = 0$.*

*Proof.* See [9, Lemmas II.7.5 & II.7.6]. □

**Definition 3.5.** *Let $C$ be as above and let $n$ be a natural number not divisible by the characteristic of $\overline{k}$ and such that $nC = 0$. We define the* ***$d$-th Tate twist of*** *$C$ (denoted $C(d)$) for integers $d$ as follows:*

$$C(d) = \begin{cases} \mu_n^{\otimes d} \otimes C & \text{if } d \geq 0, \\ \text{Hom}(\mu_n^{\otimes -d}, C) & \text{if } d < 0. \end{cases}$$

Note that the above definition is independent of one's choice of $n$. We have the following key example.

**Example 3.6.** *In the definition above, let $C = \mu_2$ and $d = -1$. One has*

$$\mu_2(-1) = \mu_2.$$

The following proposition is essential to our application of residue maps to show the nontriviality of cohomological invariants.

**Proposition 3.7.** *Let $\pi \in k$ be a uniformizer, and let $\alpha \in H^i(k, C)$. Then there exist unique elements $\alpha_0 \in H^i(\overline{k}, C)$ and $\alpha_1 \in H^{i-1}(\overline{k}, C(-1))$ such that*

$$\alpha = \alpha_0 + (\pi)_n \cup \alpha_1.$$

*Furthermore one has $r(\alpha) = \alpha_1$. [9]*

We will later consider the case where $C = \mu_2$ and the field $k$ is a pure transcendental extension of some ground field $\ell$, i.e. $k = \ell(t_1, ..., t_m)$ and the valuation $v : k \to \mathbb{Z}$ is related to the variable $t_m$. One has $\overline{k} = \ell(t_1, ..., t_{m-1})$.

Notice that this extension is not complete. We define the residue in this case by first passing via the restriction to the cohomology groups for the completion, $H^i(k_v, \mu_2)$, and then taking the usual residue. In other words, the residue is defined by the following commutative diagram:

$$\begin{tikzcd}
H^i(k, \mu_2) \arrow[r, "\text{Res}"] \arrow[dr] & H^i(k_v, \mu_2) \arrow[d, "r"] \\
 & H^{i-1}(\overline{k}, \mu_2)
\end{tikzcd}$$

In this situation, the residue map can be explicitly computed as follows.

**Example 3.8.** *Let $\alpha \in H^i(k, \mu_2)$, we wish to compute the residue of $\alpha$. Due to a result of Voevodsky, $\alpha$ may be written in the form*

$$\alpha = \sum_{j=1}^{i} (a_{j1}) \cup ... \cup (a_{ji})$$

*and so it suffices to compute the residue of symbols $(a_{j1}) \cup ... \cup (a_{ji})$. Note that any element $a \in k$ can be written in the form*

$$a = \pi^i u$$

*for the uniformizer $\pi$ and some unit $u$ in $k$. Combine this with the following relations:*

- *for all $a, b \in k$, one has $(ab) = (a) + (b)$,*

- *since we are taking values in $\mu_2$, we have $(a) \cup (b) = (b) \cup (a)$,*
- *for $\pi$ a unit, $(\pi) \cup (-\pi) = 0$ and $(\pi) \cup (\pi) = (\pi) \cup (-1)$,*

*and it can be infered that computation of the residue reduces to the following two cases, where $\pi$ is a uniformizer and $u_j$ are units:*

1. $(u_1) \cup ... \cup (u_i)$,
2. $(\pi) \cup (u_2) \cup ... \cup (u_i)$.

*In the first case, it is known that the residue is zero. In the second case, it can be shown that the residue of the cup product is equal to the cup product of the residues of just the units, i.e.*

$$r : (\pi) \cup (u_2) \cup ... \cup (u_i) \mapsto (\overline{u_2}) \cup ... \cup (\overline{u_i}).$$

This last example will be our primary tool in checking that the cohomological invariant established later is nontrivial.

# 4 Non-Abelian Cohomology

Throughout this section $G$ is assumed to be a **profinite group**, that is $G$ is a topological group which is Hausdorff, compact, and totally disconnected. The most important case for our purposes is where $G = \mathrm{Gal}(k^{\mathrm{sep}}/k)$.

**Definition 4.1.** *A $G$-set is a discrete topological space $E$ together with a continuous action of $G$ on $E$.*

**Definition 4.2.** *A **morphism** of $G$-sets is a map $f : E \to E'$ such that for all $x \in E$ and for all $s \in G$,*

$$s.f(x) = f(s.x).$$

*A morphism of $G$-sets is an **isomorphism** if it is bijective.*

**Definition 4.3.** *Let $E$ be a $G$-set. We define*

$$H^0(G, E) := E^G,$$

*where $E^G$ is the subset of $E$ consisting of all elements invariant under $G$ (in keeping with the notation of the previous section.)*

**Definition 4.4.** *A $G$-group $A$ is a $G$-set endowed with a group structure such that for all $a, b \in A$, $s \in G$,*

$$s.(ab) = (s.a)(s.b).$$

Note: an abelian $G$-group is a $G$-module.

**Definition 4.5.** *Let $A$ be a $G$-group. A* ***1-cocycle*** *of $G$ in $A$ is a continuous map*

$$\begin{aligned} \varphi : G &\to A \\ s &\mapsto \varphi(s) \end{aligned}$$

*satisfying*

$$\varphi(st) = \varphi(s) \cdot (s.\varphi(t))$$

*for all $s, t \in G$.*

The set of all 1-cocycles of $G$ in $A$ is denoted by $Z^1(G, A)$. Two cocycles $\varphi, \sigma \in Z^1(G, A)$ are said to be **cohomologous** (denoted $\varphi \sim \sigma$) if for some $a \in A$ and for all $s \in G$ one has

$$\varphi(s) = a\sigma(s)a^{-s},$$

where $a^{-s} := s(a^{-1})$ as is the standard convention. It is easy to see that $\sim$ is an equivalence relation on $Z^1(G, A)$.

**Definition 4.6.** *The quotient set $Z^1(G, A)/\sim$ is called the* ***first cohomology set*** *of $G$ in $A$ and is denoted by $H^1(G, A)$.*

As one might hope for, the cohomology sets $H^0(G, A)$ and $H^1(G, A)$ are functorial in $A$, and if $A$ is an abelian group they coincide with the cohomology groups of Definition 1.2.

However, $H^0(G, A)$ and $H^1(G, A)$ are viewed instead in the category of pointed sets. The distinguished element in $H^0(G, A)$ is the identity element of $A$, while the distinguished element in $H^1(G, A)$ is the equivalence class of the constant map $s \mapsto 1$, called the **neutral element.**

Non-abelian Galois cohomology behaves well with respect to group extensions.

Suppose $H$ is a closed normal subgroup of $G$. There is a natural action of $G/H$ on $A^H$, so we may define the cohomology set $H^1(G/H, A^H)$.

We can also define an action of $G/H$ on the cohomology set $H^1(H, A)$. First, consider the action of $G$ on $Z^1(H, A)$ given by

$$s \cdot (a_h) := (s(a_{s^{-1}hs}))$$

for all $h \in H, s \in G$ and for all 1-cocycles $a = (a_h)$ in $Z^1(H, A)$. We wish to consider this as an action on the cohomology set $H^1(H, A)$. To this end, let us check that the action of $G$ respects cohomology classes.

Indeed, suppose $a, b \in Z^1(H, A)$ are cohomologous, i.e. there exists some $x \in A$ such that $a_h = x b_h x^{-h}$ for all $h \in H$. Let $s \in G$ and let $(\tilde{a}_h) = s \cdot (a_h)$ and $(\tilde{b}_h) = s \cdot (b_h)$ so that

$$\tilde{a}_h = s a_{s^{-1}hs}, \qquad \tilde{b}_h = s b_{s^{-1}hs}. \tag{III.1}$$

Then for all $h \in H$ one has

$$\begin{aligned} \tilde{a}_h &= s a_{s^{-1}hs} \\ &= s(x b_{s^{-1}hs} x^{-s^{-1}hs}) \\ &= s(x) s(b_{s^{-1}hs}) s(x^{-s^{-1}hs}) \\ &= (sx) \tilde{b}_h s(s^{-1}hs(x^{-1}) \\ &= (sx) \tilde{b}_h h(sx^{-1}) \\ &= (sx) \tilde{b}_h h(sx)^{-1} \end{aligned}$$

so $(\tilde{a}_h)$ and $(\tilde{b}_h)$ are also cohomologous.

Furthermore, the action of $H$ on $Z^1(H, A)$ is trivial when one passes to $H^1(H, A)$. Indeed, for all $a \in Z^1(H, A)$ and for all $h, k \in H$, the $k$-component of $h \cdot a$ is of the form

$$\begin{aligned} h(a_{h^{-1}(kh)}) &= h(a_{h^{-1}}(h^{-1}(a_{kh}))) \\ &= h(a_{h^{-1}})(a_{kh}) \\ &= h(a_h^{-1})(a_k)k(a_h) \end{aligned}$$

and in fact

$$h(a_h^{-1})^{-k} = k(h(a_{h^{-1}})^{-1}) = k(a_h).$$

Thus, $h(a) \sim a$.

As such, we may view the action on $Z^1(H, A)$ (and thus on $H^1(H, A)$ as well) as an action of the quotient group $G/H$.

**Proposition 4.7.** *The natural maps form an exact sequence*

$$1 \to H^1(G/H, A^H) \to H^1(G, A) \to H^1(H, A)^{G/H}.$$

*Proof.* We will prove only the injectiveness of the map $i : H^1(G/H, A^H) \to H^1(G, A)$.

Let $\alpha \in \ker(i)$, i.e. given a representative $a$ of the cohomology class $\alpha$ there exists some $x \in A$ such that for all $s \in G$ one has

$$i(a) : s \mapsto xx^{-s}.$$

We wish to show then that $a$ is cohomologous to the trivial cocycle in $Z^1(G/H, A^H)$, that is to say there exists some $y \in A^H$ such that for every coset $gH \in G/H$

$$a : gH \mapsto yy^{-gH}.$$

It suffices to show that $x$ is invariant under the action of $H$, and thus $y = x$. Indeed, for all $h \in H$ one has

$$\begin{aligned} a(h) &= a(1_G) \\ i(a)(h) &= i(a)(1_G) \\ xx^{-h} &= xx^{-1} \\ xh(x^{-1}) &= 1 \end{aligned}$$

showing $h(x^{-1}) = x^{-1}$ and therefore $x^{-1} \in A^H$. Since $A^H$ is a group, the result follows. □

We conclude this section by discussing the notion of torsors over a $G$-group and the deep relation between torsors and cohomology.

Let $A$ be a $G$-group and let $E$ be a $G$-set. We say that $A$ **acts on the left** on $E$ if there is a left group action of $A$ on $E$ such that for all $s \in G$, $a \in A$, $x \in E$, one has

$$s.(a.x) = (s.a).(s.x).$$

We say that $A$ **acts on the right** (compatibly with $G$) on $E$ if the obvious analagous definition holds.

**Definition 4.8.** *A (right) torsor $P$ over $A$ is a nonempty $G$-set on which $A$ acts on the right, such that for all $x, y \in P$ there exists a unique element $a \in A$ such that $y = x.a$. In other words, the action of $A$ on $P$ is simply transitive.*

There is an obvious analagous definition of a left torsor. Throughout this paper however, the term torsor will refer by default to a right torsor.

An isomorphism of torsors $P, P'$ over $A$ is a bijective map $f : P \to P'$ such that for all

$x \in P$ and for all $a \in A$ one has

$$f(x.a) = f(x).a.$$

**Example 4.9.** *Let $P = A$, with $A$ acting on itself by right translation. This action is of course simply transitive - for any elements $a_1, a_2 \in A$ the unique element $a \in A$ such that $a_1 a = a_2$ is $a_1^{-1}a_2$. The action is also clearly compatible with that of $G$, and so $A$ is indeed a torsor over itself. A torsor over $A$ which is isomorphic to $A$ itself is called a* ***trivial torsor****.*

**Lemma 4.10.** *Let $P$ be a torsor over $A$. The torsor $P$ is trivial if and only if there is an element of $P$ which is fixed under the action of $G$.*

*Proof.* Suppose $P$ is a trivial torsor. Then $P$ has an element corresponding to the identity element $1 \in A$, which is invariant under the action of $G$.

Conversely, suppose there is some element $p_0 \in P$ which is invariant under $G$. Then for all $p \in P$ there exists a unique element $a_p \in A$ such that $p_0.a_p = p$. Consider now the bijection

$$\varphi : P \to A$$
$$p \mapsto a_p.$$

It remains to see that $\varphi$ respects the action of $G$. Indeed, for arbitrary $p \in P$, $a \in A$, one has by definition that $\varphi(g.p)$ is the unique element of $A$ such that

$$p_0.\varphi(g.p) = g.p.$$

On the other hand,

$$p_0.(g.\varphi(p)) = (g.p_0).(g.\varphi(p)) = g.(p_0.\varphi(p)) = g.(p_0.a_p) = g.p.$$

By uniqueness, $g.\varphi(p) = \varphi(g.p)$. □

**Proposition 4.11.** *Let $A$ be a $G$-group. Then the set of isomorphism classes of torsors over $A$ is in bijective correspondence with $H^1(G, A)$.*

*Proof.* See [17, Proposition 33]. □

The proof of Proposition 4.11 given in [17] constructs a bijection from the set of all equivalence classes of torsors over $A$ to $H^1(G, A)$ as follows: if $P$ is a torsor over $A$, first choose a point $x \in P$. For all $s \in G$ there exists a unique element $a_s \in A$ such that $s.x = x.a_s$. The map $\varphi : s \mapsto a_s$ is then a 1-cocycle, and a different choice of $x$ will result in a cohomologous 1-cocycle (see remarks following Definition 4.2.)

# 5 Twisting Actions

Let $A$ be a $G$-group and let $P$ be a torsor over $A$. Let $Q$ be a $G$-set on which $A$ acts on the left. We define the relation $\sim$ on the direct product $P \times Q$ as follows: we say $(p, q) \sim (p', q')$ if and only if there exists some element $a \in A$ such that $(p.a, a^{-1}.q) = (p', q')$.

**Proposition 5.1.** *The relation $\sim$ is an eqivalence relation on $P \times Q$.*

*Proof.* To see that $\sim$ is reflexive, simply choose $a = 1$. To see that it is symmetric, note that if $(p.a, a^{-1}.q) = (p', q')$ then $(p, q) = (p'.a^{-1}, a.q')$. Now, suppose

$$(p, q) \sim (p', q') \sim (p'', q''),$$

say there exist $a, b \in A$ such that

$$\begin{aligned}(p.a, a^{-1}.q) &= (p', q')\\ (p'.b, b^{-1}.q') &= (p'', q'').\end{aligned}$$

Then one has

$$(p.(ab), (ab)^{-1}.q) = (p'', q'').$$

□

The quotient $(P \times Q)/\sim$ given the componentwise action of $G$ is called the **twisting of $Q$ by $P$** and is denoted by ${}^{P}Q$. The action of $G$ is well-defined on equivalence classes. As a shorthand we will denote the equivalence class of $(p, q)$ by $p \cdot q$.

Under view of the bijection in Proposition 4.11, we can also consider a twisting of $Q$ by a cocycle of $A$ in $G$.

**Definition 5.2.** *Let $\varphi : G \to A$ be a cocycle $s \mapsto a_s$. Then the **twisting** of $Q$ by $\varphi$ is the set $Q$ with a new action of $G$ on $Q$ given by*

$$s._{\varphi}q := \varphi(s).(s.q)$$

*for all $s \in G$, $q \in Q$, and is denoted by ${}^{\varphi}Q$. It is defined functorially for $Q$.*

Let us show that these two constructions are essentially the same. Namely, let $P$ be an $A$-torsor and fix a point $p_0 \in P$. For all $s \in G$ there exists a unique $a_s \in A$ such that $s.p_0 = p_0 a_s$. As noted in §4 the map

$$\varphi : s \mapsto a_s$$

is a 1-cocycle.

Indeed, let $s, t \in G$ and consider $\varphi(st) = a_{st}$. We wish to show that $a_{st} = a_s(s.a_t)$, which is by definition the unique element of $A$ such that $p_0.a_{st} = (st).p_0$. Indeed

$$\begin{aligned} p_0.(a_s(s.a_t)) &= (p_0.a_s).(s.a_t) \\ &= (s.p_0).(s.a_t) \\ &= s.(p_0.a_t) \\ &= s.(t.p_0) \\ &= (st).p_0. \end{aligned}$$

Now, observe that every equivalence class $[(p, q)]$ in ${}^PQ$ has a unique representative of the form $[(p_0, q')]$, since there exists a unique element $a \in A$ such that $p = p_0.a$, and so

$$(p, q) = (p_0.a, q) \sim (p_0, a.q).$$

Then consider the map

$$\begin{aligned} \lambda : {}^PQ &\to {}^\varphi Q \\ [(p_0, q)] &\mapsto q. \end{aligned}$$

By the preceeding remarks, $\lambda$ is bijective. Let us show that it is an isomorphism of $G$-sets, i.e. that for all $s \in G$ and for all $(p_0, q) \in {}^PQ$ one has

$$\lambda(s._P(p_0, q)) = s._\varphi q.$$

Indeed,

$$\begin{aligned} \lambda(s._P(p_0, q)) &= \lambda(s.p_0, s.q) \\ &= \lambda(p_0.a_s, s.q) \\ &= \lambda(p_0, a_s.(s.q)) \\ &= a_s.(s.q) \\ &= s._\varphi q. \end{aligned}$$

**Proposition 5.3.** *If $\varphi$ and $\sigma$ are cohomologous 1-cocycles, then ${}^\varphi Q$ and ${}^\sigma Q$ are isomorphic as $G$-sets.*

*Proof.* Let $\sigma, \varphi$ be 1-cocycles of $G$ in $A$ and suppose they are cohomologous, i.e.

$$\varphi : s \mapsto a_s, \quad \sigma : s \mapsto b_s$$

and there exists some $c \in A$ such that $a_s = c b_s c^{-s}$ for all $s \in G$. Let

$$\begin{aligned} \lambda : {}^{\varphi}Q &\to {}^{\sigma}Q \\ x &\mapsto c^{-1}.x. \end{aligned}$$

We wish to show that $\lambda$ is an isomorphism of torsors, that is to say that for all $s \in G$ and for all $q \in {}^{\varphi}Q$ one has

$$\lambda(s._{\varphi}q) = s._{\sigma}\lambda(q).$$

Indeed, a straightforward computation shows this is the case:

$$\begin{aligned} \lambda(s._{\varphi}q) &= \lambda(a_s.(s.q)) \\ &= c^{-1}.(c b_s (s.c^{-1}).(s.q)) \\ &= b_s(s.c^{-1}).(s.q) \\ &= b_s.(s.(c^{-1}.q)) \\ &= b_s.(s.\lambda(q)) \\ &= s._{\sigma}\lambda(q). \end{aligned}$$

□

A significant consequence of Proposition 5.3 is that it makes sense to consider (up to isomorphism) the twisting of $Q$ by an equivalence class of cocycles, i.e. by an element of $H^1(G, A)$.

Twistings by cocycles distribute across direct products, i.e. given a 1-cocycle $\varphi$ of $G$ in $A$ and two $G$-sets $Q$ and $R$ on which $A$ acts on the left, one has

$${}^{\varphi}(Q \times R) = {}^{\varphi}Q \times {}^{\varphi}R.$$

The elements of these two $G$-sets are by definition the same, and direct computation will immediately show that $G$ acts on each in the same way.

Twistings also preserve $G$-group structures, in the sense that if $Q$ is in fact a $G$-group, the same group structure makes ${}^{\varphi}Q$ into a $G$-group.

Indeed, if $Q$ is a $G$-group with $x, y \in Q$, $s \in G$, and $A$ is a $G$-group acting on the left on

$Q$ with $\varphi \in Z^1(G, A)$, then

$$\begin{aligned} s._\varphi(xy) &= \varphi(s).(s.(xy)) = \varphi(s).((s.x)(s.y)) \\ &= (\varphi(s).(s.x))(\varphi(s).(s.y)) = (s._\varphi x)(s._\varphi y). \end{aligned}$$

**Example 5.4.** *Let $A$ be a $G$-group and let $\varphi$ be a 1-cocycle of $G$ in $A$. Consider the left group action of $A$ on itself by inner automorphisms, i.e. the group action given by the map*

$$\begin{aligned} A \times A &\to A \\ (a, b) &\mapsto aba^{-1}. \end{aligned}$$

*Under this action $A$ acts on the left on itself, and so we may consider the twisting of $A$ by $\varphi$. This is a $G$-group denoted by ${}^\varphi A$. It has the same elements as $A$, and the action of $G$ is given by*

$$s._\varphi a = \varphi(s).(s.a) = \varphi(s)(s.a)\varphi(s)^{-1}.$$

**Proposition 5.5.** *Let $A$ be a $G$-group, $Q$ a $G$-set on which $A$ acts on the left. Then for any 1-cocycle $\varphi$ of $G$ in $A$, the $G$-group ${}^\varphi A$ described above acts on the left on ${}^\varphi Q$.*

*Proof.* This is a matter of verifying that the map

$$\begin{aligned} \cdot_\varphi : {}^\varphi A \times {}^\varphi Q &\to {}^\varphi Q \\ (a, x) &\mapsto a._\varphi x \end{aligned}$$

is a $G$-morphism. Indeed, for all $s \in G$, $a \in A$, $x \in Q$, one has

$$\begin{aligned} s._\varphi(a.x) &= \varphi(s).(s.(a.x)) = \varphi(s).((s.a).(s.x)) \\ &= (\varphi(s)(s.a)).(s.x) = (\varphi(s)(s.a)\varphi(s)^{-1}\varphi(s)).(s.x) \\ &= (\varphi(s)(s.a)\varphi(s)^{-1}).(\varphi(s).(s.x)) = (\varphi(s).(s.a)).(\varphi(s).(s.x)) \\ &= (s._\varphi a).(s._\varphi x). \end{aligned}$$

□

**Proposition 5.6.** *Let $A$ be a $G$-group and $\varphi$ a 1-cocycle of $G$ in $A$. Then there exists a natural bijection*

$$\tau_\varphi : H^1(G, {}^\varphi A) \to H^1(G, A)$$

*given by*

$$\tau_\varphi(\sigma) : s \mapsto \sigma(s)\varphi(s)$$

*for all* $\sigma \in H^1(G, {}^{\varphi}A)$.

*Proof.* Let $\varphi(s) = a_s$ be a cocycle of $G$ in $A$, and let $\sigma(s) = b_s$ be a cocycle of $G$ in ${}^{\varphi}A$. We wish to show first that the new family $(c_s) := (b_s)(a_s)$ satisfies the cocycle condition, that is that for all $s, t \in G$

$$c_{st} = c_s s.c_t.$$

Indeed, one may check that

$$\begin{aligned} c_{st} &= b_{st}a_{st} \\ &= b_s s._{\varphi} b_t a_s s.a_t \\ &= b_s a_s s.b_t a_s^{-1} a_s s.a_t \\ &= b_s a_s s.b_t s.a_t \\ &= c_s s.c_t. \end{aligned}$$

Now consider the inverse map

$$\begin{aligned} H^1(G, A) &\to H^1(G, {}^{\varphi}A) \\ (d_s) &\mapsto (d_s)(a_s)^{-1} =: (e_s). \end{aligned}$$

It remains to show that this map is well-defined, however the computations are exactly analagous. □

We should emphasize here that in the nonabelian context $H^1(G, {}^{\varphi}A)$ and $H^1(G, A)$ are not in general groups and so $\tau_{\varphi}$ is merely a bijection. However, if $A$ happens to be abelian, then $\tau_{\varphi}$ coincides with the translation by the equivalence class of $\varphi$.

Now we consider the case where $A, B$ are $G$-groups with $A < B$. The group action of $G$ is well-defined on left cosets of $A$, and so $B/A$ is a $G$-set (in general not a $G$-group, since $A$ may not be normal in $B$.) Then we may define as before

$$H^0(G, B/A) := (B/A)^G = \{[b] \mid b \in B, \quad s.b \in bA \quad \forall s \in G\},$$

where $[b]$ denotes the left coset of $b$ in $B/A$.

Let $[b] \in (B/A)^G$ and consider its preimage $bA \subseteq B$. The set $bA$ is also a $G$-set (with the action inherited from $B$) and $A$ acts on $bA$ on the right via right multiplication. Moreover, for all $a, a' \in A$ there exists a unique element of $A$, namely $a^{-1}a'$, such that

$$ba.(a^{-1}a') = ba'.$$

That is to say, $bA$ is a torsor over $A$. Recall that there is a natural bijective correspondence between the set of all torsors over $A$ and the set $H^1(G, A)$. This allows us to define a map $\delta : H^0(G, B/A) \to H^1(G, A)$ by letting $\delta([b])$ be the element in $H^1(G, A)$ which corresponds to the torsor $bA$.

**Definition 5.7.** *Let $A$ and $B$ be pointed sets with distinguished elements $1_A$ and $1_B$, respectively. Recall that a homomorphism of pointed sets $f : A \to B$ is a set theoretical map such that $f(1_A) = 1_B$.*

*The* ***kernel*** *of the map $f$ is the set*

$$\{a \in A \mid f(a) = 1_B\}$$

*and is denoted* $\ker(f)$

*A sequence of pointed sets*

$$\cdots \to A_{-1} \to A_0 \to A_1 \to \ldots$$

*is called* ***exact*** *if*

$$\mathrm{im}(A_{n-1} \to A_n) = \ker(A_n \to A_{n+1})$$

*for all integers $n$ for which these sets are defined.*

**Proposition 5.8.** *The sequence*

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

*is exact.*

*Proof.* See [17, Proposition 36]. □

**Proposition 5.9.** *Let $\varphi \in Z^1(G, B)$. Then one has*

$$[\varphi] \in \mathrm{im}(H^1(G, A) \to H^1(G, B))$$

*if and only if $({}^{\varphi}(B/A))^G$ is nonempty.*

*Proof.* See [17, Proposition 37]. □

# 6 Forms of Algebraic Objects

Let $\mathrm{V}$ and $\mathrm{V}'$ be algebraic varieties over $k$ endowed with some additional algebraic structure.

**Example 6.1.** *A $k$-algebra $\mathrm{V}$ is a vector space (thus also an algebraic variety) with the additional structure of a multiplication map*

$$\times : \mathrm{V} \times \mathrm{V} \to \mathrm{V}$$

*satisfying standard axioms.*

**Example 6.2.** *An algebraic group $G$ over $k$ is an algebraic variety together with a group multiplication $G \times G \to G$ and inverse map $G \to G$ which are regular functions and respect standard axioms for group multiplication.*

**Example 6.3.** *A quadratic space $(\mathrm{V}, f)$ is a vector space together with a quadratic form*

$$f : \mathrm{V} \to k$$

*satisfying the axioms of Chapter 1.*

We can consider any such algebraic objects $\mathrm{V}$ and $\mathrm{V}'$ over a field extension $\ell/k$ in the usual way, employing the standard notation $\mathrm{V}_\ell := \mathrm{V} \otimes \ell$.

**Definition 6.4.** *The objects $\mathrm{V}$ and $\mathrm{V}'$ are $k$-**forms** of one another if there exists an isomorphism (in whatever category $\mathrm{V}$ and $\mathrm{V}'$ fall in)*

$$\varphi : \mathrm{V}_{k^{\mathrm{sep}}} \to \mathrm{V}'_{k^{\mathrm{sep}}}.$$

Let $\Gamma := \mathrm{Gal}(k^{\mathrm{sep}}/k)$ as previously. Let $\mathrm{Iso}_{k^{\mathrm{sep}}}(\mathrm{V}, \mathrm{V}')$ be the set of all isomorphisms preserving the additional structure $\mathrm{V}_{k^{\mathrm{sep}}} \to \mathrm{V}'_{k^{\mathrm{sep}}}$ and let

$$\mathrm{Aut}_{k^{\mathrm{sep}}}(\mathrm{V}) = \mathrm{Iso}_{k^{\mathrm{sep}}}(\mathrm{V}, \mathrm{V}).$$

There is a natural action of $\Gamma$ on $\mathrm{Iso}_{k^{\mathrm{sep}}}(\mathrm{V}, \mathrm{V}')$ (and thus also on $\mathrm{Aut}_{k^{\mathrm{sep}}}(\mathrm{V})$) given for $f \in \mathrm{Iso}_{k^{\mathrm{sep}}}(\mathrm{V}, \mathrm{V}')$ by

$$\begin{aligned} {}^{\sigma}f : \mathrm{V}_{k^{\mathrm{sep}}} &\to \mathrm{V}'_{k^{\mathrm{sep}}} \\ v &\mapsto \sigma \circ f \circ \sigma^{-1}(v). \end{aligned}$$

One can check that if $f$ is given as a polynomial, this amounts to applying $\sigma$ to the coefficients of $f$.

**Proposition 6.5.** *The family* $(a_\sigma) = f^{-1} \circ {}^\sigma f$ *is a cocycle of* $\Gamma$ *with values in* $\mathrm{Aut}_{k^{\mathrm{sep}}}(\mathrm{V})$.

*Proof.* We wish to check that for all $\sigma, \varphi \in \Gamma$ one has $a_{(\varphi\sigma)} = a_\varphi \circ \varphi.a_\sigma$. Direct computation shows

$$\begin{aligned} a_\varphi \circ \varphi.a_\sigma &= (f^{-1} \circ {}^\varphi f) \circ \varphi.(f^{-1} \circ {}^\sigma f) \\ &= (f^{-1} \circ \varphi \circ f \circ \varphi^{-1}) \circ (\varphi \circ f^{-1} \circ \sigma \circ f \circ \sigma^{-1}\varphi^{-1}) \\ &= f^{-1} \circ \varphi\sigma \circ f \circ \sigma^{-1}\varphi^{-1} \\ &= f^{-1} \circ {}^{(\varphi\sigma)} f \\ &= a_{(\varphi\sigma)}. \end{aligned}$$

□

The result above gives a process by which, given a $k$-form of V, we may obtain a cocycle in $Z^1(\Gamma, \mathrm{Aut}(\mathrm{V}))$. Notice that if $f$ and $g$ are isomorphisms

$$f, g : \mathrm{V}_{k^{\mathrm{sep}}} \xrightarrow{\sim} \mathrm{V}'_{k^{\mathrm{sep}}}$$

then $h := g^{-1} \circ f$ is an automorphism of $\mathrm{V}_{k^{\mathrm{sep}}}$ and one has

$$h \circ f^{-1} \circ {}^\sigma f \circ h^{-\sigma} = g^{-1} \circ {}^\sigma g,$$

thus $f$ and $g$ give rise to cohomologous cocycles. In particular, an isomorphism class of $k$-forms of V determines uniquely an element of $H^1(\Gamma, \mathrm{Aut}_{k^{\mathrm{sep}}}(\mathrm{V}))$.

Furthermore, suppose V′ and V″ are two $k$-forms of V with

$$\begin{aligned} f &: \mathrm{V}_{k^{\mathrm{sep}}} \xrightarrow{\sim} \mathrm{V}'_{k^{\mathrm{sep}}} \\ g &: \mathrm{V}_{k^{\mathrm{sep}}} \xrightarrow{\sim} \mathrm{V}''_{k^{\mathrm{sep}}} \end{aligned}$$

If V′ and V″ of V give rise to cohomologous cocycles $(a_\sigma)$ and $(b_\sigma)$, this means there is an automorphism $h$ of V such that

$$h \circ f^{-1} \circ {}^\sigma f \circ h^{-\sigma} \cong_k g^{-1} \circ {}^\sigma g.$$

It is readily seen that $g \circ h \circ f^{-1}$ is then an isomorphism (over $k$) $\mathrm{V}' \to \mathrm{V}''$, and so there is an injective map from the set of isomorphism classes of $k$-forms into $H^1(\Gamma, \mathrm{Aut}_{k^{\mathrm{sep}}}(\mathrm{V}))$.

**Theorem 6.6.** *Let* $(\mathrm{V}, f)$ *be a quadratic space over* $k$*. Then there exists a natural bijection* $\lambda$ *from the set of isomorphism classes of* $k$*-forms of* $(\mathrm{V}, f)$ *to* $H^1(\Gamma, \mathrm{Aut}_{k^{\mathrm{sep}}}(\mathrm{V}, f))$.

*Proof.* We have already established the existence of a well-defined and injective map in the general setting. We shall now give a sketch of the construction of an inverse map in the case of quadratic spaces.

Note that $\mathrm{Aut}_{k^{\mathrm{sep}}}(\mathrm{V})$ is nothing more than orthogonal group $\mathcal{O}_{k^{\mathrm{sep}}}(f)$. Let

$$\varphi \in Z^1(\Gamma, \mathcal{O}_{k^{\mathrm{sep}}}(f))$$

and consider the twisting ${}^{\varphi}(\mathrm{V} \otimes_k k^{\mathrm{sep}})$.

Consider the $k$-vector subspace W of $\mathrm{V} \otimes k^{\mathrm{sep}}$ of elements invariant under the twisted action of $\Gamma$

$$\mathrm{W} := ({}^{\varphi}(\mathrm{V} \otimes k^{\mathrm{sep}}))^{\Gamma}.$$

It is known that $\dim \mathrm{W} = \dim \mathrm{V}$ and so

$$(\mathrm{W} \otimes k^{\mathrm{sep}}, f) \cong (\mathrm{V} \otimes k^{\mathrm{sep}}, f).$$

Moreover, it is known that the restriction $g := f \mid_{\mathrm{W}}$ of $f : \mathrm{V} \otimes k^{\mathrm{sep}} \to k^{\mathrm{sep}}$ takes values in $k$, and so by construction the quadratic space $(\mathrm{W}, g)$ is a $k$-form of $(\mathrm{V}, f)$. □

# 7 Cohomological Invariants

Let $k_0$ be a field and consider the category of all field extensions over $k_0$, denoted by Fields/$k_0$. We fix two (contravariant) functors $A$ and $H$ with

$$A : \mathrm{Fields}/k_0 \to \mathrm{Sets}$$
$$H : \mathrm{Fields}/k_0 \to \mathrm{AbelianGroups}.$$

**Definition 7.1.** *The set of all morphisms of functors* $\alpha : A \to H$ *form a group under pointwise addition. This group is denoted* $\mathrm{Inv}(A, H)$ *(or* $\mathrm{Inv}_{k_0}(A, H)$ *if the ground field is not clear from context) and its elements are called* $H$***-invariants.***

Recall that a morphism of functors $\alpha : A \to H$ is a family of maps

$$\{\alpha_k\} : A(k) \to H(k)$$

defined for all field extensions $k$ over $k_0$ such that for any morphism $i : k \to k'$ of field extensions over $k$ one has a commutative diagram

$$\begin{tikzcd}
A(k) \arrow[r, "\alpha_k"] \arrow[d, "A_i"] & H(k) \arrow[d, "H_i"] \\
A(k') \arrow[r, "\alpha_{k'}"] & H(k')
\end{tikzcd}$$

There are many possible choices for the functors $A$ and $H$. We list a few examples below.

**Example 7.2.** *$A : k \mapsto \mathrm{Et}_n(k)$ where $\mathrm{Et}_n(k)$ denotes the set of all étale $k$-algebras of rank $n$.*

**Example 7.3.** *$A : k \mapsto \mathrm{Quad}_n(k)$ where $\mathrm{Quad}_n(k)$ denotes the set of all isomorphism classes of $n$-dimensional regular quadratic forms over $k$.*

**Example 7.4.** *$A : k \mapsto \mathrm{Pf}_n(k)$ where $\mathrm{Pf}_n(k)$ denotes the set of all isomorphism classes of $n$-fold Pfister forms over $k$.*

**Example 7.5.** *$A : k \mapsto \mathrm{Torsors}_G(k)$ where $G$ is a smooth linear algebraic group over $k_0$ and $\mathrm{Torsors}_G(k)$ denotes the set of all $G$-torsors over $k$. In this case we will denote the group of invariants by $\mathrm{Inv}(G, H)$ in place of $\mathrm{Inv}(A, H)$.*

**Example 7.6.** *For all field extensions $k/k_0$, let $\Gamma_k := \mathrm{Gal}(k^{\mathrm{sep}}/k)$. Let $C$ be a discrete $\Gamma_{k_0}$ module (in particular we will often choose $C = \mu_2$). For all $k/k_0$ there exists a unique (up to conjugation) map $\Gamma_k \to \Gamma_{k_0}$ which we allows us to view $C$ as a module over $\Gamma_k$, hence we may define cohomology groups*

$$H^i(k, C) := H^i(\Gamma_k, C).$$

*We further define $H(k, C) := \bigoplus H^i(k, C)$. In this case we write $\mathrm{Inv}(A, C)$ or $\mathrm{Inv}^i(A, C)$ for $\mathrm{Inv}(A, H)$ (or in the case that $A = \mathrm{Torsors}_G$ we write $\mathrm{Inv}(G, C)$, resp. $\mathrm{Inv}^i(G, C)$).*

**Definition 7.7.** *The elements of $\mathrm{Inv}(A, C)$ in the case above are called* ***cohomological invariants.***

**Example 7.8.** *$H : k \mapsto W(k)$ where $W(k)$ is the Witt Ring (see Definition 2.3 in Chapter 1).*

Many choices of the functor $A$ are in fact equivalent to the functor $\mathrm{Torsors}_G$ for an appropriate group $G$.

**Example 7.9.** *The functor* $k \mapsto \mathrm{Quad}_n(k)$ *is isomorphic to* $\mathrm{Torsors}_{O_n}$.

**Example 7.10.** *The functor* $k \mapsto \mathrm{Et}_n(k)$ *is isomorphic to* $\mathrm{Torsors}_{S_n}$ *(where* $S_n$ *is the group of permutations on* $n$ *objects).*

For details of these constructions, the reader may refer to [9] examples 3.1 and 3.2.

**Definition 7.11.** *Let us fix a base point* $1 \in A$*, i.e. compatible points in* $A(k)$ *for each field extension* $k/k_0$*, so that* $A$ *becomes a functor*

$$A : \mathrm{Fields}/k_0 \to \mathrm{PointedSets}$$

*For example, one may choose*

$$A : k \mapsto \mathrm{Torsors}_G(k) = H^1(k, G)$$

*where* $G$ *is some (not necessarily abelian) algebraic group over* $k_0$*. An* $H$*-invariant* $a : A \to H$ *is called* ***normalized*** *if for all* $k/k_0$ *one has* $a(k) : 1_{A(k)} \mapsto 1_{H(k)}$.

**Definition 7.12.** *For all* $k/k_0$ *the inclusion* $k_0 \hookrightarrow k$ *induces a map* $\iota_k^* : H(k_0) \to H(k)$*. Then for all* $h \in H(k_0)$ *we may define an invariant* $a_h : A \to H$ *given by*

$$\begin{aligned} a_h(k) : A(k) &\to H(k) \\ x &\mapsto \iota_k^*(h). \end{aligned}$$

*An invariant of this form is called* ***constant.***

**Proposition 7.13.** *Let* $a$ *be an* $H$*-invariant. Then there exist unique* $H$*-invariants* $a_c$ *and* $a_n$ *such that* $a_c$ *is constant,* $a_n$ *is normalized, and* $a = a_c + a_n$.

Now let us work towards giving some examples of cohomological invariants. We consider the setting $\mathrm{Inv}(G, \mu_2)$ i.e. the set of cohomological invariants

$$a : H^1(-, G) \to H^*(-, \mu_2).$$

First we note that $\mathrm{Inv}(G, \mu_2)$ has a natural structure of an abelian group. Specifically, given two invariants

$$a, b : H^1(-, G) \to H^*(-, \mu_2)$$

we define the invariant

$$(a+b) : H^1(-,G) \to H^*(-,\mu_2)$$

as follows. For all field extensions $k/k_0$ and for all classes of cocycles $[\zeta] \in H^1(k,G)$, define

$$\begin{aligned}(a+b)_k : H^1(k,G) &\to H^*(k,\mu_2)\\ [\zeta] &\mapsto a_k([\zeta]) + b_k([\zeta]).\end{aligned}$$

Next, we give this abelian group a module structure - an idea put forth by J.-P. Serre. Let $R$ be the ring

$$R := H(k_0,\mu_2) = \bigoplus_{i=0,1,\ldots} H^i(k_0,\mu_2)$$

where multiplication is by the cup product (the existence of such a ring structure is also mentioned in §1). It should be noted that the choice of $\mu_2$ is necessary for this ring structure to make sense; for arbitrary modules the cup products do not have coefficients in the original module.

Note that if $k_0$ is separably closed, then $\mathrm{Gal}(k_0^{\mathrm{sep}}/k_0) = 1$ and so $H^0(k_0,\mu_2) = \mu_2$, while for all $i > 0$, the $i$-th cohomology group $H^i(k_0,\mu_2)$ is zero. As such, in this special case $R = \mathbb{Z}/2$.

We wish to consider $\mathrm{Inv}(G,\mu_2)$ as an $R$-module. Let $r \in R$, and let $a \in \mathrm{Inv}(G,\mu_2)$. For all $k/k_0$ we define the invariant $r \cdot a$ as follows. Consider the map

$$\oplus\mathrm{Res} : R \to \bigoplus_{i=0,1,\ldots} H^i(k,\mu_2)$$

given by restrictions. Let $r_k \in H^i(k,\mu_2)$ be the image of $r$ under said map. Then the invariant $(r \cdot a)$ is defined for all $k/k_0$ and for all classes $[\zeta] \in H^1(k,G)$ by

$$\begin{aligned}(r\cdot a)_k : H^1(k,G) &\to H^*(k,\mu_2)\\ [\zeta] &\mapsto ra_k([\zeta]).\end{aligned}$$

We are now ready to give some explicit examples of cohomological invariants.

**Example 7.14.** *Let $f$ be an $n$-dimensional split quadratic form over a ground field $k_0$. It was shown by J.-P. Serre (see [9]) that in this case* $\mathrm{Inv}(G,\mu_2)$ *is a free module with a basis consisting of the* ***Stiefel-Whitney classes*** *(for a discussion of Stiefel-Whitney classes, the reader may refer to* § *VI.17 in [9]). We give the basic idea of their construction here.*

*Let $k/k_0$ be a field extension. We can produce a map $H^1(k,G) \to H^i(k,\mu_2)$ for all integers*

$0 \leq i \leq n$ by use of the fact that $H^1(k, G)$ in this case is in one-to-one correspondence with the set of all isomorphism classes of regular quadratic forms of dimension n (see 6.6).

Consider an isomorphism class of quadratic forms with a diagonalized representative $g = \langle a_1, ..., a_n \rangle$. For all integers $0 \leq i \leq n$ one may define a map

$$g \mapsto \sum_{j_1 < ... < j_i} (a_{j_1}) \cup ... \cup (a_{j_i}).$$

It remains to check that these maps are well defined, one may again refer to [9] for a proof. These maps are denoted by $w_i$ and are called the Stiefel-Whitney classes.

It is interesting to consider some of the low dimensional cases. For instance when $i = 0$ the summation is empty and so $w_0$ is the constant map $[g] \mapsto 0$. This map is called the ***trivial invariant.***

Also of interest is the case $i = 1$; here we have

$$w_1 : [g] \mapsto \sum_{j=1}^{n} (a_j) = \left( \prod_{j=1}^{n} a_j \right).$$

In other words, $w_1$ is precisely the discriminant.

**Example 7.15.** Let $G_0$ be a split group of type $G_2$ over $k_0$. We wish to describe $\mathrm{Inv}(G_0, \mu_2)$. Since an element here is a morphism $H^1(-, G_0) \to H^*(-, \mu_2)$, the first question we must answer is this: how does $H^1(k, G_0)$ look for extensions $k/k_0$? To answer this question we introduce the notion of an ***octonion algebra*** over $k$, which is a generalization of a quaternion algebra.

Let $a, b, c$ be arbitrary elements of $k^\times$. We define an 8-dimensional vector space $\mathrm{V}_{(a,b,c)}$ (or simply $\mathrm{V}$ if it is not necessary to distinguish these elements) which has a basis $\{e_0 := 1, e_1, ..., e_7\}$ which satisfies the following rules for multiplication:

$$e_1^2 = a,\ e_2^2 = b,\ e_3^2 = c,$$

$$e_1 e_2 = -e_2 e_1 = e_4,\ e_2 e_3 = -e_3 e_2 = e_5,$$

$$e_3 e_4 = -e_4 e_3 = e_6,\ e_4 e_5 = -e_5 e_4 = e_7.$$

Octonion algebras are associated with a quadratic form called the ***norm*** which is given in the following way. First, one must define the ***conjugate*** map $: \mathrm{V} \to \mathrm{V}$ which sends $e_0 \mapsto e_0$

*and for $i > 0$ sends $e_i \mapsto -e_i$. The norm is then the quadratic form*

$$N : \mathrm{V} \times \mathrm{V} \to k$$
$$v \mapsto (v)(\overline{v}).$$

*Of course, one must check that the product above actually lives in $k = \mathrm{Span} e_0$, since a priori it is simply an element of the vector space* V*. However, this is well known to be the case. Moreover, it can be shown that the norm on $\mathrm{V}_{(a,b,c)}$ is in fact the 3-fold Pfister form $\langle\langle a, b, c\rangle\rangle$.*

*We now consider the special case of octonion algebra where $a = b = c = 1$, which we will call a split octonion algebra. This terminology is justified in that such an algebra produces a norm $\langle\langle 1, 1, 1\rangle\rangle$ which is a split quadratic form, and furthermore it can be shown that the group $\mathrm{Aut}(\mathrm{V}(1, 1, 1), \cdot)$ of multiplication preserving vector space endomorphisms $\mathrm{V} \to \mathrm{V}$ is a split group of type $G_2$. We take this group to be $G_0$.*

*Now by 6.6 we have that $G_0$ corresponds to the set of isomorphism classes of $\mathrm{V}(1, 1, 1)$ over $k^{\mathrm{sep}}$, which is the same as saying the isomorphism classes of $\mathrm{V}(a, b, c)$ over $k^{\mathrm{sep}}$ for arbitrary $a, b, c \in k^{\times}$. Due to the fact that two octonion algebras are isomorphic if and only if their norms are isomorphic as quadratic forms, this is then equivalent to the set of isomorphism classes of 3-fold Pfister forms over $k$.*

*Now let us return to the original question. We can define an invariant $w$ in dimension 3 by use of the equivalence above. Starting from $H^1(k, G_0)$ we pass to the set of isomorphism classes of 3-fold Pfister forms over $k$, and $w_k$ is then the map*

$$[\langle\langle a, b, c\rangle\rangle] \mapsto (a) \cup (b) \cup (c).$$

*J.-P. Serre showed in [9] that $\mathrm{Inv}(G_0, \mu_2)$ (we may also write $\mathrm{Inv}(G_2, \mu_2)$ to signify an arbitrary split group of type $G_2$) is a free module with the basis $\{1, w\}$.*

# CHAPTER IV

# Algebraic Groups

## 1 Algebraic Groups

During this section, we will deal with some of the basic properties of algebraic groups, and the important connection between algebraic groups and Lie algebras. We will assume some basic knowledge of algebraic geometry, specifically the definition and properties of affine algebraic varieties.

**Definition 1.1.** *An **algebraic** $k$**-group** is an algebraic variety $G$ over a field $k$ equipped with a group structure, such that the product and inverse maps are morphisms of algebraic varieties. That is to say, $G$ has a distinguished element $e$, a product map $\mu : G \times G \to G$ , and an inverse map $i : G \to G$ which satisfy the following properties for all $g, h, k \in G$.*

1. $\mu(g, e) = \mu(e, g) = g$
2. $\mu(g, i(g)) = \mu(i(g), g) = e$
3. $\mu(g, \mu(h, k)) = \mu(\mu(g, h), k)$
4. $\mu : G \times G \to G$ *and* $i : G \to G$ *are morphisms of algebraic varieties.*

*Throughout this paper we will only consider ground fields $k$ of characteristic not equal to 2.*

Note: in the above definition $G \times G$ is the direct product (as a variety) of $G$ with itself.

**Example 1.2.** *Let $\mathrm{G}_m \subseteq \mathbb{A}^1_k$ be an open subset of 1-dimensional affine space consisting of invertible elements. Clearly it is stable with respect to multiplication and inversion, hence $\mathrm{G}_m$ is an algebraic group defined over $k$. For any field extension $\ell/k$ one has $\mathrm{G}_m(\ell) = \ell^\times$.*

**Example 1.3.** *Let $F$ be a field with $a, b \in F^{\times}$. A* ***quaternion algebra*** $Q = (\frac{a,b}{F})$ *over $F$ is an $F$-algebra on two generators, say $i$ and $j$ which the defining relations*

1. $i^2 = a$

2. $j^2 = b$

3. $ij = -ji$

*Given such $Q$ one can associate a map $Q \to k$,*

$$x_0 1 + x_1 i + x_2 j + x_3 ij \mapsto x_0^2 - a x_1^2 - b x_2^2 + ab x_3^2$$

*called the* ***reduced norm*** *and denoted by* $\mathrm{Nrd}_Q$.

*Let $\mathrm{GL}_1(Q) \subset Q$ be the subset consisting of all elements $x \in Q$ whose reduced norm $\mathrm{Nrd}_Q(x) \in k$ is invertible. Note that $\mathrm{GL}_1(Q)$ is defined by polynomial inequalities and therefore open in $Q$.*

*Note that the reduced norm is in fact a 2-fold Pfister form, in particular* $\mathrm{Nrd} = \langle\langle a, b \rangle\rangle$. *One can easily check*

$$\mathrm{Nrd}_Q(xy) = \mathrm{Nrd}_Q(x)\mathrm{Nrd}_Q(y)$$

*for all $x, y \in Q$. Thus, $\mathrm{GL}_1(Q)$ is an algebraic group over $k$.*

**Example 1.4.** *Let $V$ be a finite dimensional $k$-vector space. Then $GL(\mathrm{V})$ is an affine variety over $k$, and the product and inverse maps arising from the regular group structure are morphisms. That is to say, $GL(\mathrm{V})$ is a linear algebraic group over $k$.*

The **right and left translation maps** $G \to G$ by an element $y \in G$ are defined, respectively as

$$R_y : x \mapsto xy$$

$$L_y : x \mapsto yx.$$

The fact that these maps are invertible morphisms of varieties directly implies one remarkable fact about algebraic groups: any local property holding at a given point holds at every point of $G$. (Since if $S$ is an open neighborhood of some point $x$, the image of $S$ under $L_{yx^{-1}}$ is an open neighborhood of $y$.)

The group $G$ is called a **linear algebraic group** or **affine algebraic group** if $G$ is affine as a variety. This is the type of algebraic group central to our research, and from this point forward an algebraic group should be taken to be linear, unless otherwise specified.

Recall that an algebraic variety (and thus also an algebraic group) is a topological space with the **Zariski topology.** Just as algebraic geometry is often concerned with closed (in the Zariski topology) subvarieties and group theory is often concerned with subgroups, **closed subgroups** are central to the theory of algebraic groups.

**Definition 1.5.** *Let $G$ be an algebraic group. A* ***closed subgroup*** *$H$ of $G$ is a subset which is both a subgroup and a closed subvariety. We denote this by $H \leq G$.*

A closed subgroup $H \leq G$ is called **normal** if it is a normal subgroup in the standard group theoretic sense, that is to say the left and right cosets of $H$ are equal. We denote a closed normal subgroup of $G$ by $H \trianglelefteq G$.

**Example 1.6.** *Recall the quaternion algebra $Q = (\frac{a,b}{F})$ from a previous example. Consider the set*

$$\mathrm{SL}(1, D) = \{x \in Q \mid \mathrm{Nrd}(x) = 1\}.$$

*This is a 3-dimensional closed subgroup of* $\mathrm{GL}(1, Q)$*, and in fact it is normal.*

Homomorphisms of algebraic groups are also defined in a predictable manner.

**Definition 1.7.** *A* ***homomorphism*** *of algebraic groups is a map $f : G \to H$ where $G$ and $H$ are algebraic groups, such that $f$ is a homomorphism with respect to the group structures of $H$ and $G$ as well as a morphism with respect to the variery structures of $H$ and $G$.*

An **isomorphism** $f : H \to G$ of algebraic groups is a homomorphism which is an isomorphism both of algebraic groups and of algebraic varieties, and two algebraic groups are called isomorphic if there exists an isomorphism between them. An **automorphism** of algebraic groups is an isomorphism $f : G \to G$.

It may occur that two algebraic groups $H$ and $G$ are not isomorphic as $k$-groups, but become isomorphic when viewed as algebraic groups over some field extension.

**Definition 1.8.** *Let $H$ and $G$ be $k$-groups. As discussed in the previous chapter, $H$ is called a $k$-**form** of $G$ if $H$ and $G$ are isomorphic over the separable closure of $k$, that is if*

$$H \otimes k^{\mathrm{sep}} \cong G \otimes k^{\mathrm{sep}}.$$

**Example 1.9.** *The quaternion algebra $Q = (\frac{a,b}{k})$ from previous examples is a $k$-form of the $2 \times 2$ matix algebra over $k$, $M_{2,k}$.*

*The reduced norm over $k^{\mathrm{sep}}$ corresponds to the determinant, hence* $\mathrm{GL}_1(Q)$ *is a $k$-form of* $\mathrm{GL}_{2,k}$.

*To see that this is the case, let $c, d \in k^{\text{sep}}$ such that $c^2 = a$ and $d^2 = b$, with $c$ and $d$ invertible. Let $Q^{\text{sep}} := Q \otimes_k k^{\text{sep}} = \left(\frac{a,b}{k^{\text{sep}}}\right)$. We wish to show that $Q^{\text{sep}}$ is isomorphic to the quaternion algebra $\left(\frac{1,1}{k^{\text{sep}}}\right)$.*

*In $Q^{\text{sep}}$ one has generators $i, j$ with the properties*

$$i^2 = c^2, \quad j^2 = d^2, \quad ij = -ji.$$

*Let $i' = ic^{-1}$ and $j' = jd^{-1}$. Then one has*

$$i'^2 = i^2(c^{-1})^2 = c^2(c^{-1})^2 = 1$$

$$j'^2 = j^2(d^{-1})^2 = d^2(d^{-1})^2 = 1$$

$$i'j' = ijc^{-1}d^{-1} = -jic^{-1}d^{-1} = -j'i',$$

*that is to say $i'$ and $j'$ satisfy the necessary conditions for generators of $\left(\frac{1,1}{k^{\text{sep}}}\right)$ and thus*

$$\left(\frac{1,1}{k^{\text{sep}}}\right) \cong k^{\text{sep}}[i', j'] \subseteq Q^{\text{sep}}.$$

*Moreover, since $i'$ and $j'$ obviously generate $Q^{\text{sep}}$ over $k^{\text{sep}}$ the above inclusion is in fact an equality and we have*

$$\left(\frac{1,1}{k^{\text{sep}}}\right) \cong Q^{\text{sep}}.$$

*Since $\left(\frac{1,1}{k^{\text{sep}}}\right) = \left(\frac{1,1}{k}\right) \otimes_k k^{\text{sep}}$, it remains only to be seen that $\left(\frac{1,1}{k}\right)$ is isomorphic to $M_{2,k}$ over $k$.*

*Indeed, let us consider the homomorphism $\varphi : \left(\frac{1,1}{k}\right) \to M_{2,k}$ defined on generators by*

$$i' \mapsto \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad j' \mapsto \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$$

*and extended linearly to $\left(\frac{1,1}{k}\right)$. We claim that $\varphi$ is an isomorphism.*

*By linearity one has*

$$\varphi(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \varphi(i'j') = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

*Clearly $\{\varphi(1), \varphi(i'), \varphi(j'), \varphi(i'j')\}$ is linearly independent, and so*

$$\dim(\operatorname{im}(\varphi)) = \dim(M_{2,k}) = \dim\left(\frac{1,1}{k}\right) = 4.$$

*Therefore, $\phi$ is bijective. It now suffices to see that*

$$\varphi(i')^2 = \varphi(j')^2 = 1,$$

*which is obvious, and that*

$$\varphi(j')\varphi(i') = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = -\varphi(i')\varphi(j').$$

*This demonstrates $\varphi$ is indeed an isomorphism, and so $Q$ is a $k$-form of $M_{2,k}$.*

**Example 1.10.** *The group $\mathrm{SL}(1, D)$ defined in Example 1.3 is a $k$-form of $\mathrm{SL}_{2,k}$.*

*To see this, let us consider $\mathrm{SL}(1, D)$ as a subset of $Q := \left(\frac{a,b}{k}\right)$ and pass to $Q^{\mathrm{sep}} := Q \otimes k^{\mathrm{sep}}$ and consider its image under the map $\varphi$ from Example 1.9. For all $x \in Q^{\mathrm{sep}}$ one has*

$$x := x_1 + x_2 i + x_3 j + x_4 ij \mapsto \begin{bmatrix} x_1 + x_2 & -x_3 - x_4 \\ -x_3 + x_4 & x_1 - x_2 \end{bmatrix}$$

*(where the $x_i$ are uniquely determined coefficients in $k^{\mathrm{sep}}$.) Computing the determinant yields*

$$\begin{aligned} \det(\varphi(x)) &= (x_1 + x_2)(x_1 - x_2) - (-x_3 - x_4)(-x_3 + x_4) \\ &= x_1^2 - x_2^2 - x_2^3 + x_4^2 \\ &= \mathrm{Nrd}(x), \end{aligned}$$

*therefore $\varphi(x) \in \mathrm{SL}_{2,k} \otimes k^{\mathrm{sep}}$ if and only if $x \in \mathrm{SL}(1, D) \otimes k^{\mathrm{sep}}$. Since $\varphi$ is an isomorphism it follows that $\mathrm{SL}(1, D)$ is a $k$-form of $\mathrm{SL}_{2,k}$.*

One important class of algebraic groups is the **simple algebraic groups.** These groups can be seen as in some sense the ‘building blocks’ for all algebraic groups, and they are fundamental in seeing the connections between algebraic groups, Lie algebras, and root systems.

Recall that a set in a topological space is called **connected** if it cannot be written as the proper union of two or more disjoint, relative open subsets.

**Definition 1.11.** *An algebraic group is called* ***simple*** *if it contains no reduced, normal, closed, connected, nontrivial subgroup.*

As it turns out, there is a deep correspondence between simple algebraic groups over an algebraically closed field $k$ and root systems. A major goal of this section and the next is to describe this correspondence.

A (linear) **representation** of a group $G$ is a morphism of algebraic groups $\phi : G \to GL(\mathrm{V})$, where V is a finite dimensional $k$-vector space.

Such a representation of $G$ amounts to a linear group action of $G$ on V; indeed given a representation $\varphi$ a group action is defined by $(g, v) \mapsto \varphi(g)(v)$, which is linear in the second argument. Conversely, given a linear group action $\psi : G \times \mathrm{V} \to \mathrm{V}$ the map

$$\varphi : G \to \mathrm{GL}(\mathrm{V}), \quad \varphi(g) : v \mapsto \psi(g, v)$$

is a representation of $G$.

**Theorem 1.12.** *(Chevalley) Every affine algebraic group has a represenation which is in fact an isomorphism between G and its image. In particular, for every linear algebraic group G there exists a finite dimensional vector space* V *such that G is isomorphic to a closed subgroup of* GL(V).

*Proof.* See [11, Theorem 8.6]. □

# 2 Jordan-Chevalley Decomposition

Let V be a finite dimensional vector space over a ground field $k$.

**Definition 2.1.** *An operator $n \in \mathrm{End(V)}$ is **nilpotent** if $n^s = 0$ for some $s \in \mathbb{N}$.*

**Definition 2.2.** *An operator $s \in \mathrm{End}(V)$ is **semisimple** if its minimal polynomial has no multiple roots. (Equivalently for $k$ algebraically closed, $s$ is diagonalizable.)*

**Definition 2.3.** *An operator $u \in \mathrm{End(V)}$ is **unipotent** if $1 - u$ is nilpotent.*

If $k$ is a perfect field then the following results hold:

**Lemma 2.4.** *For all $x \in \mathrm{End(V)}$ there exist unique $x_s, x_n \in \mathrm{End(V)}$ such that:*

1. *$x_s$ is semisimple, $x_n$ is nilpotent, $x = x_s + x_n$, and $x_s x_n = x_n x_s$,*
2. *there exist polynomials $p, q$ with coefficients in $k$ such that $p(x) = x_s$ and $q(x) = x_n$,*
3. *if $A, B$ are subspaces of V with $A \subseteq B \subseteq \mathrm{V}$ such that $x(B) \subseteq A$, then $x_s(B) \subseteq A$ and $x_n(B) \subseteq A$,*

4. *if $x, y \in \mathrm{End(V)}$ such that $xy = yx$, then $(x+y)_s = x_s + y_s$ and $(x+y)_n = x_n + y_n$.*

*Proof.* See [11, Theorem 15.3]. □

**Lemma 2.5.** *For all $x \in \mathrm{GL(V)}$, there exist $x_s, x_u \in \mathrm{GL(V)}$ such that:*

1. *$x_s$ is semisimple, $x_u$ is unipotent, and $x_s x_u = x_u x_s = x$.*
2. *there exist polynomials $p, q$ with coefficients in $k$ such that $p(x) = x_s$ and $q(x) = x_u$,*
3. *if $A, B$ are subspaces of $\mathrm{V}$ with $A \subseteq B \subseteq \mathrm{V}$ such that $x(B) \subseteq A$, then $x_s(B) \subseteq A$ and $x_u(B) \subseteq A$,*
4. *if $x, y \in \mathrm{GL(V)}$ such that $xy = yx$, then $(xy)_s = x_s y_s$ and $(xy)_u = x_u y_u$.*

*Proof.* See [11, Theorem 15.3]. □

**Definition 2.6.** *If the conditions for existence are met, $x_s$ is called the* ***semisimple part*** *of $x$. Similarly, $x_n$ is called the* ***nilpotent part*** *of $x$ and $x_u$ is called the* ***unipotent part.***

We wish to be able to apply these results to algebraic groups in a more general setting. This can be achieved via a representation

$$G \hookrightarrow \mathrm{GL(V)}.$$

There are two main difficulties involved here. Firstly, we wish to see that $x_s$ and $x_u$ are in $G$ when chosen in this manner. Secondly, we would hope that $x_s$ and $x_u$ are independent of our choice of representation.

We begin by considering the map

$$\begin{aligned} \rho : G &\hookrightarrow \mathrm{GL}(k[G]), & \rho &: x \mapsto \rho_x \\ \rho_x : k[G] &\to k[G], & \rho_x &: f(g) \mapsto f(gx). \end{aligned}$$

Of course, $k[G]$ is an infinite dimensional vector space if $\dim G > 0$, so to move forward we need a way to talk about semisimple and nilpotent elements in an infinite dimensional context.

**Fact 2.7.** *For all $x \in G(k)$, there exists a family of finite dimensional subspaces $\mathrm{W}_i \subset k[G]$ with $W_0 \subset W_1 \subset W_2 \subset ...$ such that $k[G] = \bigcup_i \mathrm{W}_i$ and $\rho_x(\mathrm{W}_i) = \mathrm{W}_i$ for all $i$.*

**Definition 2.8.** *$\rho_x$ is* ***semisimple*** *if $\rho_x |_{\mathrm{W}_i}$ is semisimple for all $i$.*

**Definition 2.9.** *$\rho_x$ is* ***nilpotent*** *if $\rho_x |_{\mathrm{W}_i}$ is nilpotent for all $i$.*

**Definition 2.10.** *$\rho_x$ is* ***unipotent*** *if $\rho_x - 1$ is nilpotent.*

As an embedding of $G$ into $\mathrm{GL}(k[G])$, the differential (see Proposition 1.6 in Chapter V) of $\rho$ also gives rise to an embedding

$$* : \mathrm{Lie}(G) \hookrightarrow \mathrm{End}(k[G])$$

called the **right convolution.**

**Theorem 2.11.** *(Jordan-Chevalley)*
*Let $G$ be an algebraic group over a perfect field $k$. Then:*

1. *For all $g \in G(k)$ there exist unique $g_s, g_u \in G(k)$ such that $g = g_s g_u = g_u g_s$, $\rho_{g_s}$ is semisimple, and $\rho_{g_u}$ is unipotent. The element $g_s$ is called the* ***semisimple part*** *of $g$ and $g_u$ the* ***unipotent part.***

2. *For all $x \in \mathrm{Lie}(G)$ there exist unique $x_s, x_n \in \mathrm{Lie}(G)$ such that $x = x_s + x_n$, $x_s x_n = x_n x_s$, $*x_s$ is semisimple, and $*x_n$ is nilpotent.*

3. *If $\varphi : G \to G'$ is a morphism of algebraic groups with $g \in G(k)$, then $\varphi(g_s) = \varphi(g)_s$ and $\varphi(g_u) = \varphi(g)_u$.*
   *Furthermore, for all $x \in \mathrm{Lie}(G)$ one has $d\varphi(x_s) = d\varphi(x)_s$ and $d\varphi(x_n) = d\varphi(x)_n$.*

*Proof.* See [11, Theorem 15.3] and remarks in section 34.2 relating to section 15.3. □

# 3 Tori and Split Groups

The next portion of our discussion on algebraic groups will focus on tori, and the notion of split groups and split tori. We begin by considering the case of GL(V), for some $k$-vector space V.

A subset $S$ of End(V) is called diagonalizable if there exists a basis of V in which every element of $S$ is diagonal, or equivalently given a fixed basis of V if there exists $A \in \mathrm{GL(V)}$ such that $AXA^{-1}$ is diagonal for all $X \in S$.

A subset $S$ of End(V) is called **triangularizable** if there exists a basis of V such that every element of $S$ is triangular.

**Proposition 3.1.** *Suppose $k = k^{\mathrm{sep}}$ and $M \in \mathrm{GL(V)}$ is a set of commuting matrices, i.e. $XY = YX$ for all $X, Y \in S$. Then $M$ is triangularizable. Moreover, there exists a basis of* V *such that every element of $M$ is triangular and every semisimple element of $M$ is diagonal.*

*Proof.* See §15.4 in [11]. □

Of course, the above proposition also implies that any set of commuting semisimple elements is diagonalizable.

By $D(\mathrm{V})$ we denote the set of all diagonal matrices in $\mathrm{GL}(\mathrm{V})$. An algebraic group is called **diagonalizable** if it is isomorphic to a closed subgroup of $D(\mathrm{V})$ for some vector space V.

**Proposition 3.2.** *An algebraic group over $G$ over $k^{\text{sep}}$ is diagonalizable if and only if it is abelian and consists of semisimple elements.*

*Proof.* See [11]. □

The abelian group $\mathrm{Hom}(G, G_m)$ is called the **character group** of $G$ and is denoted by $X(G)$. Diagonalizable groups have important properties related to $X(G)$. Observe that $X(G)$ has a natural interpretation as a subset of the set $k[G]$ of all regular functions on $G$. Moreover, $X(G)$ is linearly independent over $k^{\text{sep}}$ as a subset of $k^{\text{sep}}[G]$ (see [11] Section 16.1.)

**Definition 3.3.** *An algebraic group $G$ is called a* ***d-group*** *if $X(G)$ is a basis of $k^{\text{sep}}[G]$.*

Of course since $X(G)$ is a priori linearly independent, it suffices for $G$ to be a d-group that $X(G)$ should form a system of generators for $k^{\text{sep}}[G]$.

**Proposition 3.4.** *An algebraic group $G$ is a d-group if and only if $G$ is diagonalizable over $k^{\text{sep}}$.*

**Definition 3.5.** *A* ***torus*** *is a connected d-group. Equivalently, a torus is a group which is isomorphic to a closed connected subgroup of $D_n$ over $k^{\text{sep}}$.*

A torus $T \subseteq G$ is called a **maximal torus** if there exists no torus $S$ which is 'larger' in the sense that $T \subsetneq S \subseteq G$.

**Definition 3.6.** *Let $G$ be a group and $T \subseteq G$ a maximal torus. The* ***rank*** *of $G$ is $\dim T$.*

The usefullness of studying maximal tori is due in large part to the following theorem.

**Theorem 3.7.** *All maximal tori of a group $G$ are conjugate when viewed over the separable closure of the base field.*

*Proof.* See [11]. □

In particular, all maximal tori have the same dimension, and so the rank of $G$ is well-defined.

**Proposition 3.8.** *If $G$ is a d-group, then $X(G)$ is a finitely generated group. Moreover, if $G$ is a torus then $X(G)$ has no torsion, that is $X(G) \simeq \mathbb{Z}^n$ for some natural number $n$.*

*Proof.* See [11]. □

A torus $T$ over $k$ is called $k$-split if $X(T)$ spans $k[T]$. In particular, this means the characters are defined over $k$. As it turns out, a torus $T$ is $k$-split if and only if it is isomorphic over $k$ to $\mathrm{G}_m \times ... \times \mathrm{G}_m$ (see [11], Section 34.3.)

**Definition 3.9.** *A reductive group $G$ is called $k$**-split** if there exists a maximal torus $T \subset G$ which is $k$-split. (Reductive groups will be defined in the following section.)*

**Example 3.10.** *Consider the special linear group $\mathrm{SL}_{n,k} \subset \mathrm{GL}_{n,k}$ consisting of $n \times n$ matrices with entries in $k$ and determinant 1. $\mathrm{SL}_{n,k}$ is a reductive group.*

*Let $T$ be the subgroup of $\mathrm{SL}(n,k)$ consisting of all $n \times n$ diagonal matrices with entries in $k$ and determinant 1.*

*Consider the map $\varphi : T \to G_m \times ... \times G_m$ ($n-1$ factors) given by*

$$D := \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{bmatrix} \mapsto (d_1, ..., d_{n-1}).$$

*Since* $\det D = 1$ *and thus $d_n = \frac{1}{d_1 ... d_{n-1}}$, it is clear that $\varphi$ is bijective and also that $\varphi$ and its inverse are given by regular functions. It is also easy to see that $\varphi$ preserves multiplication, and so $\varphi$ is an isomorphism of algebraic groups.*

*This establishes that $T$ is a split torus. We claim that $T \subset \mathrm{SL}_{n,k}$ is a maximal torus, and so $\mathrm{SL}_{n,k}$ is a split algebraic group.*

*Indeed, suppose there exists some torus $T'$ which lies between $T$ and $\mathrm{SL}_{n,k}$, that is to say $T \subseteq T' \subseteq \mathrm{SL}_{n,k}$. We wish to see that $T$ and $T'$ coincide.*

*Since $T'$ is a torus it is diagonalizable, that is to say there exists some $a \in \mathrm{SL}_{n,k}(k^{\mathrm{sep}})$ such that $T'' := aT'a^{-1}$ is a closed subgroup of $D_n$. However $T$ is by definition the intersection of $D_n$ with $\mathrm{SL}_{n,k}$, and so one has*

$$T' \cong T'' \subseteq T.$$

*It then follows that*

$$\dim T' = \dim T'' \leq \dim T$$

*and so $T' = T$.*

*Since $T$ is a split torus and now shown to be a maximal, $\mathrm{SL}_{n,k}$ is by definition a split group.*

**Definition 3.11.** *Let $f$ be an $n$-dimensional quadratic form over $k$. The* ***orthogonal group*** $\mathrm{O}(f)$ *of $f$ is the group of all linear transformations $X \in \mathrm{GL}_{n,k}$ which preserve $f$. That is to say,*

$$\mathrm{O}(f) = \{X \in \mathrm{GL}_{n,k} \mid f(v) = f(Xv) \text{ for all } v \in k^n\}.$$

**Definition 3.12.** *The* ***special orthogonal group*** $\mathrm{SO}(f)$ *of $f$ is the subgroup of* $\mathrm{O}(f)$ *consisting of transformations with determinant equal to 1.*

**Proposition 3.13.** *Let $f$ be a quadratic form over an infinite field $k$. The special orthogonal group* $\mathrm{SO}(f)$ *of a quadratic form $f$ is a split group if and only if $f$ is a split (i.e. hyperbolic) quadratic form.*

*Proof.* Let $\dim f = 2n$. Suppose $f$ is a split quadratic form over $k$. Without loss of generality, say

$$f(u_1, v_1, ..., u_n, v_n) = u_1v_1 + ... + u_nv_n$$

where $i = 1, ..., n$. Let

$$T = \left\{ \begin{bmatrix} x_1 & & & & \\ & x_1^{-1} & & & \\ & & \ddots & & \\ & & & x_n & \\ & & & & x_n^{-1} \end{bmatrix} \;\middle|\; x_1, ..., x_n \in k \right\}.$$

It is clear that $T$ is a split torus, in particular $T \cong G_m \times ... \times G_m$ ($n$ factors.) We claim that $T \subset \mathrm{SO}(f)$ is also a maximal torus.

First, let us check that $T$ lies in $\mathrm{SO}(f)$. It is obvious that $T$ consist of matrices with determinant 1. Let $w := (u_1, v_1, ..., u_n, v_n)$. Then

$$\begin{aligned} f(T(w)) &= f(u_1x_1, v_1x_1^{-1}, ..., u_nx_n, v_nx_n^{-1}) \\ &= u_1v_1x_1x_1^{-1} + ... + u_nv_nx_nx_n^{-1} \\ &= u_1v_1 + ... + u_nv_n \\ &= f(w), \end{aligned}$$

so indeed $T$ lies in $\mathrm{SO}(f)$.

Now, suppose $T'$ is another torus in $\mathrm{SO}(f)$ such that

$$T \subset T' \subset \mathrm{SO}(f).$$

Since $T'$ is abelian and $T \subset T'$, one has that $T' \subset C_{\mathrm{GL}_{2n}}(T)$. We claim that $C_{\mathrm{GL}_{2n}}(T) = D_{2n}$. One inclusion is obvious, since $T \subset D_{2n}$ and $D_{2n}$ is abelian. On the other hand suppose $y \in C_{\mathrm{GL}_{2n}}(T)$, that is to say for all

$$x := \begin{bmatrix} x_1 & & & & \\ & x_1^{-1} & & & \\ & & \ddots & & \\ & & & x_n & \\ & & & & x_n^{-1} \end{bmatrix} \in T$$

one has $yxy^{-1} = x$. Equivalently, $x^{-1}yx = y$.

Let $y \in \mathrm{GL}_{2n}$ and suppose by way of contradiction that there exist some indices $i, j$ such that $y_{ij} \neq 0$, i.e. $y \notin D_{2n}$. Then there exists some $t \in T$ such that $t_{ii} \neq t_{ij}$. Computation will show that $(x^{-1}yx)_{ij} = x_{ii}^{-1}y_{ij}x_{jj} \neq y_{ij}$, thus we have $T' \subset C_{\mathrm{GL}_{2n}}(T) = D_{2n}$.

We now claim that $T = D_{2n} \cap \mathrm{SO}(f)$. Indeed, suppose

$$A := \begin{bmatrix} a_1 & & \\ & \ddots & \\ & & a_{2n} \end{bmatrix} \in D_{2n} \cap \mathrm{SO}(f)$$

with $a_1, ..., a_n \in k$ and consider $f$ as a quadratic form over a pure transcendental extension

$$k(z) := k(z_1, ..., z_{2n}).$$

One has

$$f(A(z_1, ..., z_{2n})) = f(z_1, ..., z_{2n}) = z_1z_2 + ... + z_{2n-1}z_{2n}.$$

On the other hand,

$$\begin{aligned} f(A(z_1, ..., z_{2n})) &= f(a_1z_1, ..., a_{2n}z_{2n}) \\ &= a_1a_2z_1z_2 + ... + a_{2n-1}a_{2n}z_{2n-1}z_{2n} \end{aligned}$$

and so for all $i = 1, ..., n$ we have $a_{2n}a_{2n-1} = 1$, that is to say $A \in T$.

This shows that $D_{n,k(z)} \cap \mathrm{SO}(f_{k(z)}) \subseteq T_{k(z)}$ and so $T$ is a maximal torus, thus $\mathrm{SO}(f)$ is split.

Conversely, suppose $\mathrm{SO}(f)$ is a split group with split maximal torus $T$. We proceed by induction on $n$.

Suppose $n = 1$, then $f$ is split (hyperbolic) if and only if $f$ is isotropic. Since $T \cong G_m$ we may choose $t \in T(k)$ to be of infinite order. Then there exists an eigenvalue $a$ of $t$ with infinite order. Let $v$ be a corresponding eigenvector, i.e. $t(v) = av$. Then since $t \in \mathrm{SO}(f)$

$$f(v) = f(t(v)) = f(av) = a^2 f(v).$$

Since $a$ is of infinite order $a^2 \neq 1$ and so $v$ must be an isotropic vector, thus $f$ is hyperbolic.

Now let $n$ be arbitrary. By induction, $f$ has a $2n-2$-dimensional subform $f'$ which is hyperbolic, say

$$f = g \oplus f'.$$

Then $g$ has dimension 2 and so by the argument above is hyperbolic.

□

# 4 Reductive, Semisimple and Simple Algebraic Groups

Recall that a topological space $T$ is called **irreducible** if $T$ cannot be written as the union of two closed subsets $\emptyset \neq U, V \subsetneq T$.

**Theorem 4.1.** *An algebraic variety $X$ has finitely many maximal, irreducible subspaces. They are called the* ***irreducible components*** *of $X$.*

*Proof.* See [11]. □

Of course, the above result also applies to algebraic groups.

**Corollary 4.2.** *Let $G$ be an algebraic group with identity element $e$. Then there is a unique irreducible component $G^\circ$ of $G$ which contains $e$. It is called the* ***identity component*** *of $G$.*

Recall that for any (abstract) group $G$ the **commutator** of two elements $x, y \in G$ is defined as $(x, y) := xyx^{-1}y^{-1}$. If $A, B < G$ are closed subgroups we define

$$(A, B) := \langle \{(x, y) \mid x \in A, y \in B\} \rangle < G.$$

In general this is a subgroup, but need not be closed, as demonstrated by the following example, taken from [11], Exercise 7.10.

**Example 4.3.** *Let $G = \mathrm{GL}_{2,\mathbb{C}}$ with $a = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $b = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ Let $A = \langle a \rangle, B = \langle b \rangle$.*

*Both $a$ and $b$ have order 2, thus $A$ and $B$ are closed. However, computation will show that*

$$\langle A, B\rangle = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{N} \right\},$$

*which is not a closed subgroup.*

However, certain conditions on the groups $A$ and $B$ guarantee that a commutator subgroup is closed.

**Proposition 4.4.** *Let $G$ be an algebraic group with closed subgroups $A, B < G$.*

1. *If $A$ is connected then $(A, B)$ is closed and connected.*

2. *If $A$ and $B$ are normal subgroups of $G$, then $(A, B)$ is a closed normal subgroup of $G$.*

*Proof.* See [11, Proposition 17.2]. □

Note that the above result immediately implies that for any algebraic group $G$, the **commutator subgroup** $(G, G)$ of $G$ is a closed normal subgroup.

**Definition 4.5.** *Let $G$ be an algebraic group. The **derived series** of $G$ is a sequence of closed normal subgroups defined in the following manner:*

$$\mathcal{D}^0 G = G,$$

$$\mathcal{D}^{i+1} G = (\mathcal{D}^i G, \mathcal{D}^i G).$$

**Definition 4.6.** *An algebraic group $G$ is **solvable** if there exists some natural number $n \in \mathbb{N}$ such that $\mathcal{D}^n G = \{e\}$. (Therefore also $\mathcal{D}^m G = \{e\}$ for all $m \geq n$.)*

**Definition 4.7.** *The **radical** of an algebraic group $G$ is the unique maximal, normal, solvable, connected subgroup of $G$, denoted $R(G)$.*

**Definition 4.8.** *The subgroup of $R(G)$ comprising its unipotent elements is called the **unipotent radical** of $G$ and is denoted $R_u(G)$.*

**Definition 4.9.** *A group $G$ is called **semisimple** if $G$ is connected and nontrivial, with $R(G) = \{e\}$.*

**Definition 4.10.** *A group $G$ is called **reductive** if $G$ is connected and nontrivial, with $R_u(G) = \{e\}$.*

**Definition 4.11.** *A semisimple group $G$ is called **simple** if $G$ contains no nontrivial proper, closed, connected, normal subgroup $e \neq H \lhd G$.*

Clearly, all simple groups are semisimple, and all semisimple groups are reductive. The converse statements are not true.

**Proposition 4.12.** *The special linear group $SL_{n,k}$ is simple.*

*Proof.* Without loss of generality we assume that $k$ is separably closed. Suppose by way of contradiction there exists some proper normal subgroup $N_k \lhd \mathrm{SL}_{n,k}$ satisfying the conditions of Definition 4.11. That is to say $N_k$ is nontrivial, connected, closed, and normal in $\mathrm{SL}_{n,k}$. Taking $k$ points of $N$, we still have a proper normal subgroup $N(k) \lhd G := \mathrm{SL}(n,k)$. Abusing notation, we will denote $N(k)$ by $N$.

Let us first ascertain that $N$ contains at least one nontrivial semisimple element. Suppose by way of contradiction that there are no nonidentity semisimple elements in $N$. Then by Theorem 2.11, $N$ consists of unipotent elements.

It is known that any group consisting of unipotent matrices is upper triangularizable, i.e. there exists some $a \in G$ such that

$$aNa^{-1} \subseteq U := \left\{ X := \begin{bmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \middle| X \in G \right\}.$$

Moreover, $N$ is by assumption normal, thus one has

$$N = aNa^{-1} \subseteq U.$$

On the other hand there exists a matrix $b \in G$, namely

$$b = \alpha \begin{bmatrix} 0 & 0 & 1 \\ 0 & \iddots & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

where $\alpha$ is a scalar such that $\alpha^n = (-1)^{n+1}$, such that for any upper triangular matrix $u$, the conjugation $bub^{-1}$ of $u$ by $b$ is lower triangular. (To see this, one may first note that $b^{-1} = b$ and then compute $(bub^{-1})_{ij} = b_{n-i,n-j}$.)

Since $N$ is nontrivial we may choose a nonidentity element $u \in N$. By the above remarks, $bub^{-1}$ is a nonidentity lower triangular matrix, in particular $bub^{-1} \notin N$. However $N$ is assumed to be normal in $G$, which gives a contradiction. Thus $N$ contains at least one semisimple element other than 1.

We claim next that $N$ necessarily contains a semisimple element $g \in N$ which is of infinite order.

Consider first the case where $N \cap D_n$ is infinite. Note that this is a closed subgroup of $G$. Then its connected component $(N \cap D_n)^\circ$ is nontrivial, since the connected component of a group has finite index. In particular, $(N \cap D_n)^\circ$ is a torus of dimension at least one, i.e.

$$(N \cap D_n)^\circ \cong G_m \times ... \times G_m.$$

As such it is clear that $(N \cap D_n)^\circ$ contains many elements of infinite order, and by extension so does $N \cap D_n$. Since every element of $D_n$ is semisimple, we may say that $N$ has semisimple elements of infinite order.

In fact, it turns out that this is the only case. Suppose by way of contradiction that $N \cap D_n$ is finite, say

$$N \cap D_n = \{d_1, ..., d_s\}, \quad s \in \mathbb{N}.$$

Let $N_i$ be the conjugacy class in $N$ of $d_i$ for all $i = 1, ..., s$,

$$N_i := \{x d_i x^{-1} \mid x \in N\}.$$

It is known that the conjugacy class of any semisimple element in a group is closed, so each $N_i$ is closed in $N$. Furthermore, each $N_i$ is a proper subset of $N$. To see this, one notes that if $d_i \neq 1$ then $1 \notin N_i$ so $N_i$ is a proper subset of $N$, while if $d_i = 1$ then $N_i = \{1\}$ which is a proper subset since $N$ is by assumption nontrivial.

Since $N$ is irreducible as a variety it cannot be written as a finite union of closed subvarieties, in particular

$$N' := \bigcup_{i=1}^{s} N_i \neq N.$$

Now observe that by construction $N'$ consists of all semisimple elements in $N$, since for a matrix to be semisimple means exactly for it to be contained in the conjugacy class of a diagonal matrix. To restate, one has

$$N' = N_{ss} := \{s \in N \mid s \text{ is semisimple}\}.$$

It is known that since $N_{ss}$ is nontrivial, it contains an open (in $N$) subset $U$ which is dense in $N$, i.e. $N = \overline{U} \subseteq N_{ss}$. On the other hand, one has $N_{ss} = N' \subsetneq N$, which provides our contradiction.

Now that we know $(N \cap D_n)^\circ$ is a torus of positive dimension, that is $(N \cap D_n)^\circ \cong G_m \times ... \times G_m$, let us choose an injection

$$\varphi : G_m \times 1 \times ... \times 1 \hookrightarrow N.$$

For ease of notation will write $G_m$ instead $G_m \times 1... \times 1$ using the obvious identification. It is known that any homomorphism $G_m \to D_n$ takes the form

$$x \mapsto \begin{bmatrix} x^{m_1} & & \\ & \ddots & \\ & & x^{m_n} \end{bmatrix}$$

for some integers $m_i$. Let us choose $t \in G_m$ of infinite order, and consider

$$g := \varphi(t) = \begin{bmatrix} t^{m_1} & & \\ & \ddots & \\ & & t^{m_n} \end{bmatrix}.$$

Since $\varphi$ is an injection, $g$ again has infinite order. In particular $g \neq 1$. Since $t$ has infinite order and $t^{m_1+...+m_n} = \det(g) = 1$, we may conclude that $g$ is not a scalar matrix. Without loss of generality, say $m_1 \neq m_2$.

Let

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

One may compute

$$t^q = \begin{bmatrix} t^{q\times m_1} & & \\ & \ddots & \\ & & t^{q\times m_n} \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 1 & -1 & & \\ 0 & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$

$$A'_q := t^q A t^{-q} A^{-1} = \begin{bmatrix} 1 & t^{q\times(m_1-m_2)} - 1 & & \\ 0 & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}.$$

Since $N$ is normal it contains $A'_q$ for all natural numbers $q$.

Notice that for all integers $q \neq r$ one has $A'_q \neq A'_r$, since given $A'_q = A'_r$ we would have (seeing as $t$ has infinite order)

$$t^{q\times(m_1-m_2)-1} = t^{r\times(m_1-m_2)-1} q \times (m_1 - m_2) - 1 \qquad = r \times (m_1 - m_2) - 1 q = r.$$

In particular, there are infinitely many distinct matrices $A'_q \in N$.

Since $N$ is closed, it thus also contains

$$\overline{\{A'^i \mid i \in \mathbb{N}\}} = \left\{ \begin{bmatrix} 1 & x & & \\ 0 & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix} \middle| \quad x \in k \right\} =: E_{1,2}(k).$$

To see that the closure of the set containing each $A'^i$ is indeed $E_{1,2}(k)$, note that $E_{1,2}(k)$ is isomorphic as a variety to the affine line over $k$. Consequentially, any infinite subset of $E_{1,2}(k)$ is dense.

By choosing instead

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

and using the analagous arguments one has $E_{2,1}(k) \subset N$.

For all integers $i \neq j$, $i, j = 1, ..., n$ and for all $\lambda \in k$, let $E_{i,j}(\lambda)$ denote the matrix with ones on the main diagonal, $\lambda$ at the $i, j$-th entry, and zeros elsewhere. Then one has

$$E_{1,i}(\lambda) = E_{1,2}(\lambda)E_{2,i}(1)E_{1,2}(\lambda)^{-1}E_{2,i}(1)^{-1}.$$

Since $E_{1,2}(\lambda) \in N$, $E_{2,i}(1) \in \mathrm{SL}(n, k)$, and $N \triangleleft \mathrm{SL}(n, k)$, we have $E_{1,i}(\lambda) \in N$ for all integers $i$ and for all $\lambda \in k$. Analagously we have $E_{i,1}(\lambda) \in N$ for all integers $i$ and for all $\lambda \in k$.

We now claim that matrices of such a form generate $\mathrm{SL}(n, k)$ multiplicatively. It is well known that $\mathrm{SL}(n, k)$ is generated by the set of all elementary matrices $E_{i,j}(\lambda)$, where $i, j = 1, ..., n$ and $\lambda \in k$ such that $i \neq j$. One may compute

$$E_{i,j}(\lambda) = E_{i,1}(\lambda)E_{1,j}(1)E_{i,1}(-\lambda)E_{1,j}(-1),$$

and so indeed these matrices generate $\mathrm{SL}(n, k)$. Therefore, $N = \mathrm{SL}(n, k)$, and the proof is complete. □

**Example 4.13.** *The special orthogonal group* $\mathrm{SO}(f)$ *of a quadratic form* $f$ *is a simple group.*

*Proof.* See [11]. □

# CHAPTER V

# Lie Algebras

## 1 Lie Algebra of an Algebraic Group

Given any algebraic group $G$ we may attach in a canonical way a **Lie algebra**, $\mathrm{Lie}(G)$. The study of these Lie algebras can reveal much about the corresponding groups. Our next objective moving forward is to describe this process.

Recall first the definition of a Lie algebra.

**Definition 1.1.** *A* ***Lie algbera*** *is a vector space $\mathcal{L}$ over some ground field $k$, together with a binary operation $[-,-] : \mathcal{L} \times \mathcal{L} \to \mathcal{L}$ called the* ***Lie bracket,*** *which satisfies the following conditions for all $X, Y, Z \in \mathcal{L}$.*

1. *The map $[-,-]$ is bilinear.*
2. $[X, Y] = -[Y, X]$.
3. $[X, [Y, Z]] + [Z, [X, Y]] + [Y, [Z, X]] = 0$.

A **subalgebra** $S$ of a Lie algebra $\mathcal{L}$ is a subspace of $\mathcal{L}$ which is closed under the Lie bracket, that is for all $X, Y \in S$, one has $[X, Y] \in S$.

We want $\mathrm{Lie}(G)$ to be the **tangent space** of $G$ at $e$. The ring $k[G]$ has a maximal ideal

$$\mathcal{M} := \{f \in k[G] \mid f(e) = 0\}.$$

The tangent space of $G$ at $e$ is given by $\mathrm{Tan}_e(G) := (\mathcal{M}/\mathcal{M}^2)^*$, where $(\mathcal{M}/\mathcal{M}^2)^*$ denotes the vector space dual of $\mathcal{M}/\mathcal{M}^2$, that is the space consisting of all linear maps $\phi : \mathcal{M}/\mathcal{M}^2 \to k$. Note that $k[G]$ is equal as a vector space to $\mathcal{M} \oplus k$.

Now that we know how our Lie algebra ought to look, we need to give $\mathrm{Tan}_e(G)$ the structure of a Lie algebra. To do so we introduce another vector space, $\mathrm{Der}_e(G)$ - the set of all **differentials** of $G$ at $e$.

**Definition 1.2.** *A differential is a linear map $\delta : k[G] \to k$ such that for all $f, g \in k[G]$, $\delta(fg) = \delta(f)g(e) + f(e)\delta(g)$.*

$\mathrm{Der}_e(G)$ is a subspace of $k[G]^*$, the vector space dual of the regular functions over $k$. Moreover, we claim that for all $\delta \in \mathrm{Der}_e(G)$, the following are true:

1. For any constant function $f \in k[G]$, $\delta(f) = 0$.

2. For all $g \in \mathcal{M}^2$, $\delta(g) = 0$.

The first part follows from the observation that

$$\delta(1) = \delta(1 \cdot 1) = \delta(1) \cdot 1 + \delta(1) \cdot 1 = \delta(1) + \delta(1).$$

The second is true because for all $g, h \in \mathcal{M}$,

$$\delta(gh) = \delta(g)h(e) + g(e)\delta(h) = \delta(g) \cdot 0 + 0 \cdot \delta(h) = 0.$$

Now, since $k[G] \cong \mathcal{M} \oplus k$, the differential $\delta$ is well-defined as a map $\mathcal{M} \to k$. Furthermore since $\delta$ vanishes on $\mathcal{M}^2$ it is also has a natural definition as a linear map $\mathcal{M}/\mathcal{M}^2 \to k$, or in other words as an element of $\mathrm{Tan}_e(G)$. The following proposition is a fundamental fact in the study of algebraic groups.

**Proposition 1.3.** *The above correspondence between $\mathrm{Der}_e(G)$ and $\mathrm{Tan}_e(G)$ is a vector space isomorphism.*

It remains to give this vector space a Lie algebra structure. We define the Lie bracket on $\mathrm{Der}_e(G)$ by setting

$$[\delta_1, \delta_2] = \delta_1\delta_2 - \delta_2\delta_1$$

for all $\delta_1, \delta_2 \in \mathrm{Der}_e(G)$. One checks first that $[\delta_1, \delta_2]$ is a differential under this definition. Indeed, for all $f, g \in k[G]$ one has

$$\begin{aligned} [\delta_1, \delta_2](fg) &= \delta_1\delta_2(fg) - \delta_2\delta_1(fg) \\ &= \delta_1(\delta_2(f)g(e) + f(e)\delta_2(g)) - \delta_2(\delta_1(f)g(e) + f(e)\delta_1(g)) \\ &= \delta_1\delta_2(f)g(e) + f(e)\delta_1\delta_2(g) - \delta_2\delta_1(f)g(e) - f(e)\delta_2\delta_1(g) \\ &= [\delta_1, \delta_2](f)g(e) + f(e)[\delta_1, \delta_2](g). \end{aligned}$$

Now, observe that for all $\delta_1, \delta_2 \in \mathrm{Der}_e(G)$ one has

$$[\delta_1, \delta_2] + [\delta_2, \delta_1] = \delta_1\delta_2 - \delta_2\delta_1 + \delta_2\delta_1 - \delta_1\delta_2 = 0,$$

and so that condition 2 of Definition 1.1 holds. For all $\delta_1, \delta_2, \delta_3 \in \mathrm{Der}_e(G)$ one checks condition 3 as follows:

$$\begin{aligned}
&[\delta_1, [\delta_2, \delta_3]] + [\delta_3, [\delta_1, \delta_2]] + [\delta_2, [\delta_3, \delta_1]] = [\delta_1, \delta_2\delta_3 - \delta_3\delta_2] + [\delta_3, \delta_1\delta_2 - \delta_2\delta_1] + [\delta_2, \delta_3\delta_1 - \delta_1\delta_3] \\
&= \delta_1(\delta_2\delta_3 - \delta_3\delta_2) - (\delta_2\delta_3 - \delta_3\delta_2)\delta_1 + \delta_3(\delta_1\delta_2 - \delta_2\delta_1) - (\delta_1\delta_2 - \delta_2\delta_1)\delta_3 + \delta_2(\delta_3\delta_1 - \delta_1\delta_3) - (\delta_3\delta_1 - \delta_1\delta_3)\delta_2 \\
&= \delta_1\delta_2\delta_3 - \delta_1\delta_3\delta_2 - \delta_2\delta_3\delta_1 + \delta_3\delta_2\delta_1 + \delta_3\delta_1\delta_2 - \delta_3\delta_2\delta_1 - \delta_1\delta_2\delta_3 + \delta_2\delta_1\delta_3 + \delta_2\delta_3\delta_1 - \delta_2\delta_1\delta_3 - \delta_3\delta_1\delta_2 + \delta_1\delta_3\delta_2 \\
&= 0.
\end{aligned}$$

Furthermore, it is straightforward to see that this map is bilinear (condition 1,) so this operation does indeed satisfy the properties of a Lie bracket. The vector space $\mathrm{Der}_e(G)$ together with this definition of a Lie bracket is called the **Lie algebra** of $G$, and is denoted by $\mathrm{Lie}(G)$.

There is a special representation of $G$ called the **adjoint representation,** which is defined using this Lie algebra. Let $G$ be an algebraic group with $\mathcal{L} := \mathrm{Lie}(G)$ it's Lie algebra. Let $W$ be a vector space over some ground field $k$ such that there is an embedding $G \hookrightarrow \mathrm{GL(W)}$ (recall that the existence of such a vector space W is guaranteed by Theorem 1.12.) We will view this as an identification. The Lie algebra $\mathcal{L}$ is then a subset of End(W), and so we have a well defined notion of multiplication between elements of $G$ and $\mathcal{L}$ in End(W).

**Definition 1.4.** *The adjoint representation of $G$ is the map $\mathrm{Ad} : G \to \mathrm{GL}(\mathcal{L})$ given by $\mathrm{Ad}(g) : X \mapsto gXg^{-1}$. The Lie algebra $\mathcal{L}$ is stable under conjugation by $G$, and so $\mathrm{Ad}(g)(X) \in \mathcal{L}$ for all $g \in G$, $X \in \mathcal{L}$ (see [11], Section 10.3 Definition 1.4.)*

The adjoint representation will prove useful in attaching to each simple algebraic group a root system.

**Proposition 1.5.** *Let $G$ be a semisimple group. The kernel of the adjoint representation $\mathrm{Ad} : G \to \mathrm{GL}(\mathcal{L})$ is the center $Z(G)$ of $G$. In other words, an element $g \in G$ is central if and only if it acts trivially on $\mathcal{L}$ by conjugation.*

*Proof.* See [4], Section 3.15. □

**Proposition 1.6.** *Given a morphism of algebraic groups*

$$\varphi : G \to G',$$

*the map* $\varphi$ *induces a morphism of the corresponding Lie algebras called* ***differential*** *of* $\varphi$ *and denoted*

$$d\varphi : \mathrm{Lie}(G) \to \mathrm{Lie}(G').$$

*Proof.* See [11, Section 5.4]. □

# 2 Killing Forms and the Chevalley Basis

Let $\mathcal{L}$ be a finite dimensional Lie algebra over $k$. There is an endomorphism of $\mathcal{L}$ associated to each element $x \in \mathcal{L}$ called the **adjoint endomorphism** of $x$, and denoted $\mathrm{ad}(x)$. The endomorphism is given by

$$\mathrm{ad}(x) : y \mapsto [x, y].$$

**Proposition 2.1.** *Let* $\mathcal{L}$ *be a finite dimensional Lie algebra over* $k$*. Then the map*

$$\mathcal{K} : \mathcal{L} \times \mathcal{L} \to k$$

$$\mathcal{K} : (x, y) \mapsto \mathrm{tr}(\mathrm{ad}(x)\mathrm{ad}(y))$$

*is a symmetric bilinear form called the* ***Killing form*** *of* $\mathcal{L}$*.*

Recall that a subalgebra $\mathcal{H}$ of $\mathcal{L}$ is a **Cartan subalgebra** if $\mathcal{H}$ is nilpotent and equal to its own normalizer, that is

$$\mathcal{H} = \{x \in \mathcal{L} \mid [x, \mathcal{H}] \subseteq \mathcal{H}\}.$$

**Definition 2.2.** *A semisimple (simple) Lie algebra* $\mathcal{L}$ *over* $k$ *is* ***split*** *if* $\mathcal{L}$ *contains a Cartan subalgebra* $\mathcal{H}$ *such that for all* $x \in \mathcal{H}$*, the adjoint representation* $\mathrm{ad}(x)$ *of* $x$ *is* $k$*-diagonalizable. Such a subalgebra is called a* ***split Cartan subalgebra*** *of* $\mathcal{L}$*.*

If $\mathcal{H}$ is split then there exists a basis of $\mathcal{L}$ consisting of eigenvectors $u_1, ..., u_m$ of $\mathrm{ad}(\mathcal{H}) \subseteq \mathrm{End}(\mathcal{L})$, where $m = \dim(\mathcal{L})$. Then for all $i = 1, ..., m$ there exists a linear function $\alpha_i$ in $\mathcal{H}^* = \mathrm{Hom}(\mathcal{H}, k)$ such that

$$\mathrm{ad}(h)(u_i) = \alpha_i(h)u_i$$

for all $h \in \mathcal{H}$.

**Definition 2.3.** *The functions $\alpha_i$ above are called* ***weights*** *of $\mathcal{H}$ and the one-dimensional subspaces $\langle u_i \rangle$ are called the* ***weight subspaces*** *of $\mathcal{H}$.*

It is known that the nonzero weights $\alpha_i$ form a root system $R := \{\alpha_1, ..., \alpha_\ell\}$ called the root system $R$ of $\mathcal{L}$ relative to $\mathcal{H}$.

Due to a famous result by Chevalley (see Theorem 2.4 below) the root system $R$ is independent of the choice of a split Cartan subalgebra $\mathcal{H}$. Therefore if we say $\mathcal{L}$ is of a certain type (e.g. $\mathcal{L}$ is of type $D_4$) we mean that $R$ is of that type, and this notion is well-defined.

**Theorem 2.4.** *(Chevalley) Over a separably closed field, all split Cartan subalgebras are conjugate.*

An important result due to Steinberg [20] shows that if $\mathcal{L}$ is a Lie algebra with $\mathcal{H}$ a split Cartan subalgebra, then $\mathcal{L}$ has a basis $\mathcal{B}$ of the form

$$\mathcal{B} = \{H_{\alpha_1}, ..., H_{\alpha_n}\} \cup \{X_\alpha \mid \alpha \in R\}$$

where $\{\alpha_1, ..., \alpha_n\}$ is a base of $R$, which satisfies the following relations for all $\alpha, \beta \in R$ and for all $i, j = 1, ..., n$:

1. $[H_{\alpha_i}, H_{\alpha_j}] = 0.$

2. $[H_{\alpha_i}, X_\alpha] = \langle \alpha^*, \alpha_i \rangle X_\alpha.$

3. If $\alpha = -\beta$ then $[X_\alpha, X_\beta] = H_\alpha$ where $H_\alpha$ is an integral combination of the roots $H_{\alpha_i}$, and furthermore if all roots have the same length then

$$H_\alpha := \sum_{i=1,...,n} a_i H_{\alpha_i}$$

with $a_1, ..., a_n$ being the unique integers such that

$$\sum_{i=1,...,n} a_i \alpha_i = \alpha.$$

4. If $\alpha + \beta \in R$ then

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

where $r$ is the unique positive integer such that

$$\alpha + r\beta \in R, \quad \alpha + (r+1)\beta \notin R.$$

5. If $\alpha \neq -\beta$ and $\alpha + \beta \notin R$ then
$$[X_\alpha, X_\beta] = 0.$$

**Definition 2.5.** *The basis of $\mathcal{L}$ described above is called a* ***Chevalley basis.***

Now, suppose $\mathcal{L}$ is a split simple Lie algebra of type $D_4$, $D_8$, or $E_8$ and $\mathcal{H}$ is a split Cartan subalgebra of $\mathcal{L}$ with basis $\mathcal{B}$ as given above. The Killing form $\mathcal{K}$ is a symmetric bilinear form, which by remarks in Chapter 1 we may also view as a quadratic form

$$\mathcal{K}(x) := \mathcal{K}(x, x).$$

We wish to compute the quadratic space $(\mathcal{L}, \mathcal{K})$.

**Proposition 2.6.** *Let $H := \mathrm{Span}_k\{H_{\alpha_1}, ..., H_{\alpha_n}\}$. Then*

$$(\mathcal{L}, \mathcal{K}) \cong (H, \mathcal{K}\mid_H) \oplus \bigoplus_{\alpha \in R^+} (4\check{h}xy)$$

*where $\check{h}$ is the* ***dual Coxeter number,*** *which is an integer dependent on the type of the root system $R$.*

If $R$ is of type $D_n$ then $\check{h} = 2n-2$. If $R$ is of type $E_8$ then $\check{h} = 30$. These are the examples with which we will be concerned.

Proposition 2.6 is a direct consequence of the four lemmas which follow.

**Lemma 2.7.** *For all $i = 1, ..., n$ and for all $\alpha \in R$, one has*

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

*Proof.* Observe that for all $X, Y \in \mathcal{L}$, to show that $\mathcal{K}(X, Y) = 0$ it suffices to show that the diagonal entries of the operator $\mathrm{ad}(X) \circ \mathrm{ad}(Y)$ are all zero. That is to say, for all $i = 1, ..., n$ and for all $\alpha \in R$:

1. One may write $\mathrm{ad}(X) \circ \mathrm{ad}(Y)(H_{\alpha_i})$ as a linear combination of elements of $\mathcal{B}$ excluding $H_{\alpha_i}$.

2. One may write $\mathrm{ad}(X) \circ \mathrm{ad}(Y)(X_\alpha)$ as a linear combination of elements of $\mathcal{B}$ excluding $X_\alpha$.

This fact will henceforth be used without mention.

Now let us make the relevant computations. Let $j = 1, ..., n$ and let $\beta \in R$.

$$\begin{aligned} \mathrm{ad}(X_\alpha) \circ \mathrm{ad}(H_{\alpha_i})(H_{\alpha_j}) &= [X_\alpha, [H_{\alpha_i}, H_{\alpha_j}]] \\ &= [X_\alpha, 0] \\ &= 0. \end{aligned}$$

If $\alpha = -\beta$ then

$$\begin{aligned} \mathrm{ad}(X_\alpha) \circ \mathrm{ad}(H_{\alpha_i})(X_\beta) &= [X_\alpha, [H_{\alpha_i}, X_\beta]] \\ &= [X_\alpha, \langle \beta^*, \alpha_i \rangle X_\beta] \\ &= \langle \beta^*, \alpha_i \rangle [X_\alpha, X_\beta] \\ &= \langle \beta^*, \alpha_i \rangle H_\alpha. \end{aligned}$$

If $\alpha + \beta \in R$ then

$$\begin{aligned} \mathrm{ad}(X_\alpha) \circ \mathrm{ad}(H_{\alpha_i})(X_\beta) &= [X_\alpha, [H_{\alpha_i}, X_\beta]] \\ &= [X_\alpha, \langle \beta^*, \alpha_i \rangle X_\beta] \\ &= \langle \beta^*, \alpha_i \rangle [X_\alpha, X_\beta] \\ &= \pm \langle \beta^*, \alpha_i \rangle (r+1) X_{\alpha+\beta}. \end{aligned}$$

where $r$ is as given in the properties of the Chevalley basis.

Finally, if $\alpha \neq -\beta$ and $\alpha + \beta \notin R$, then

$$\begin{aligned} \mathrm{ad}(X_\alpha) \circ \mathrm{ad}(H_{\alpha_i})(X_\beta) &= [X_\alpha, [H_{\alpha_i}, X_\beta]] \\ &= [X_\alpha, \langle \beta^*, \alpha_i \rangle X_\beta] \\ &= \langle \beta^*, \alpha_i \rangle [X_\alpha, X_\beta] \\ &= 0. \end{aligned}$$

□

**Lemma 2.8.** *For all $\alpha, \beta \in R$ such that $\alpha \neq \pm\beta$ one has*

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

*Proof.* Let $\gamma \in R$. If $\gamma \neq -\beta$ and $\beta + \gamma \notin R$ then

$$\begin{aligned} \mathrm{ad}(X_\alpha) \circ \mathrm{ad}(X_\beta)(X_\gamma) &= [X_\alpha, [X_\beta, X_\gamma]] \\ &= [X_\alpha, 0] \\ &= 0. \end{aligned}$$

If $\gamma = -\beta$ then

$$\begin{aligned} \mathrm{ad}(X_\alpha) \circ \mathrm{ad}(X_\beta)(X_\gamma) &= [X_\alpha, [X_\beta, X_\gamma]] \\ &= [X_\alpha, H_\beta] \\ &= \sum_{i=1,\ldots,n} b_i [X_\alpha, H_{\alpha_1}] \end{aligned}$$

where $b_1, ..., b_n$ are the unique integers such that

$$\sum_{i=1,\ldots,n} b_i \alpha_i = \beta.$$

Lastly, if $\beta + \gamma \in R$ then

$$\begin{aligned} \mathrm{ad}(X_\alpha) \circ \mathrm{ad}(X_\beta)(X_\gamma) &= [X_\alpha, [X_\beta, X_\gamma]] \\ &= [X_\alpha, \pm(r+1) X_{\beta+\gamma}] \\ &= \pm(r+1)[X_\alpha, X_{\beta+\gamma}]. \end{aligned}$$

where $r$ is as given in the properties of the Chevalley basis.

Now, if $\alpha + \beta + \gamma \in R$ one has

$$\pm(r+1)[X_\alpha, X_{\beta+\gamma}] = \pm(r+1)(s+1) X_{\alpha+\beta+\gamma}$$

where $s$ is the unique positive integer such that $\alpha + s(\beta+\gamma)$ is in $R$ but $\alpha + (s+1)(\beta+\gamma)$ is not. Since $\beta \neq -\gamma$ it holds that $\alpha \neq \alpha + \beta + \gamma$ and so the corresponding entry of the diagonal is zero.

If $-\alpha = \beta + \gamma$ then

$$\pm(r+1)[X_\alpha, X_{\beta+\gamma}] = \pm(r+1) H_\alpha$$

where $H_\alpha$ is defined analagously to $H_\beta$.

If $-\alpha \neq \beta + \gamma$ and $\alpha + \beta + \gamma \notin R$ then

$$\pm(r+1)[X_\alpha, X_{\beta+\gamma}] = 0.$$

Now, we let $i = 1, ..., n$ and compute

$$\begin{aligned} \mathrm{ad}(X_\alpha) \circ \mathrm{ad}(X_\beta)(H_{\alpha_i}) &= [X_\alpha, [X_\beta, H_{\alpha_i}]] \\ &= [X_\alpha, -\langle \beta^*, \alpha_i \rangle X_\beta] \\ &= -\langle \beta, \alpha_i \rangle^* [X_\alpha, X_\beta]. \end{aligned}$$

Recall that we are working under assumption $\alpha \neq -\beta$. If $\alpha + \beta \in R$ then

$$-\langle \beta^*, \alpha_i \rangle [X_\alpha, X_\beta] = \pm \langle \beta^*, \alpha_i \rangle (r+1) X_{\alpha+\beta}.$$

On the other hand, if $\alpha + \beta \notin R$ then

$$-\langle \beta^*, \alpha_i \rangle [X_\alpha, X_\beta] = 0.$$

□

**Lemma 2.9.** *For all $\alpha \in R$, one has*

$$\mathcal{K}(X_\alpha) := \mathcal{K}(X_\alpha, X_\alpha) = 0.$$

*Proof.* Let $\beta \in R$. Suppose first that $\beta \neq -\alpha$ and $\alpha + \beta \notin R$. Then

$$\begin{aligned} \mathrm{ad}(X_\alpha) \circ \mathrm{ad}(X_\alpha)(X_\beta) &= [X_\alpha, [X_\alpha, X_\beta]] \\ &= [X_\alpha, 0] \\ &= 0. \end{aligned}$$

Now, suppose $\alpha = -\beta$. Then

$$\begin{aligned}\mathrm{ad}(X_\alpha) \circ \mathrm{ad}(X_\alpha)(X_\beta) &= [X_\alpha, [X_\alpha, X_\beta]] \\ &= [X_\alpha, H_\alpha] \\ &= \sum_{i=1,\ldots,n} a_i [X_\alpha, H_{\alpha_i}] \\ &= -\sum_{i=1,\ldots,n} a_i \langle \alpha, \alpha_i \rangle X_\alpha.\end{aligned}$$

Finally, suppose $\alpha + \beta \in R$. Then

$$\begin{aligned}\mathrm{ad}(X_\alpha) \circ \mathrm{ad}(X_\alpha)(X_\beta) &= [X_\alpha, [X_\alpha, X_\beta]] \\ &= [X_\alpha, X_{\alpha+\beta}] \\ &= \pm(r+1)[X_\alpha, X_{\alpha+\beta}].\end{aligned}$$

If $-\alpha = \alpha + \beta$ (equivalently $2\alpha = -\beta$) then

$$\pm(r+1)[X_\alpha, X_{\alpha+\beta}] = \pm(r+1)H_\alpha.$$

If $2\alpha + \beta \in R$ then

$$\pm(r+1)[X_\alpha, X_{\alpha+\beta}] = \pm(r+1)(s+1)X_{2\alpha+\beta},$$

and of course $X_{2\alpha+\beta} \neq X_\beta$. If $2\alpha \neq -\beta$ and $2\alpha + \beta \notin R$ then

$$\pm(r+1)[X_\alpha, X_{\alpha+\beta}] = 0.$$

Now, let $i = 1, ..., n$. Then

$$\begin{aligned}\mathrm{ad}(X_\alpha) \circ \mathrm{ad}(X_\alpha)(H_{\alpha_i}) &= [X_\alpha, [X_\alpha, H_{\alpha_i}]] \\ &= -\langle \alpha^*, \alpha_i \rangle [X_\alpha, X_\alpha]\end{aligned}$$

If $2\alpha \in R$ then

$$-\langle \alpha^*, \alpha_i \rangle [X_\alpha, X_\alpha] = -\langle \alpha^*, \alpha_i \rangle (r+1) X_{2\alpha},$$

otherwise

$$-\langle \alpha^*, \alpha_i \rangle [X_\alpha, X_\alpha] = 0.$$

□

**Remark:** Note that some of the cases above cannot in fact occur if $\mathcal{L}$ is of type $D_4, D_8$, or $E_8$. However, the preceding lemmas hold for every type of root system, and as such have been proven without use of that assumption. The following lemma, on the other hand, holds only for root systems in which every root has equal length.

**Lemma 2.10.** *For all $\alpha \in R$,*

$$\mathcal{K}(X_\alpha, X_{-\alpha}) = 2\check{h}.$$

*Proof.* It was shown by Springer and Steinberg in [19] that for any long root $\alpha \in R$

$$\mathcal{K}(H_\alpha, H_\alpha) = 4\check{h},$$

and also that for any long root $\alpha$

$$\mathcal{K}(X_\alpha, X_{-\alpha}) = \frac{1}{2}\mathcal{K}(H_\alpha, H_\alpha).$$

□

With these lemmas established, Proposition 2.6 follows immediately. To render the computations more straightforward, we choose to consider the **normalized Killing form**

$$\mathcal{K}'(x) := \frac{1}{4\check{h}}\mathcal{K}(x).$$

From Proposition 2.6 it is immediately clear that

$$(\mathcal{L}, \mathcal{K}') \cong (H, \mathcal{K}' \mid_H) \oplus \bigoplus_{\alpha \in R^+} \mathbb{H}.$$

Of course, in the Witt ring this means that the unique anisotropic space representing the class of $(\mathcal{L}, \mathcal{K}')$ is $(H, \mathcal{K}' \mid_H)$.

Now, let us proceed to compute the form $(H, \mathcal{K}' \mid_H)$. It is known that for all $i, j = 1, ..., n$

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

where $\alpha_i' = \frac{2\alpha_i}{(\alpha_i, \alpha_j)}$ so that $(-', -')$ is the unique Weyl-invariant inner product such that for all long roots $\alpha$ (which includes every root in $D_4, D_8$, and $E_8$) one has $(\alpha', \alpha') = 2$.

Normalizing, one has $\mathcal{K}'(H_{\alpha_i}, H_{\alpha_j}) = \frac{1}{2}(\check{\alpha}_i, \check{\alpha}_j)$. So if $\alpha_i$ and $\alpha_j$ are non-adjacent with $i \neq j$, then $\mathcal{K}'(H_{\alpha_i}, H_{\alpha_j}) = 0$ and if $i = j$ then $\mathcal{K}'(H_{\alpha_i}, H_{\alpha_j}) = 1$.

Furthermore, for root systems $D_4, D_8$, and $E_8$ one has for adjacent roots

$$\begin{aligned}
\mathcal{K}'(H_{\alpha_i}, H_{\alpha_j}) &= \frac{1}{2}(\check{\alpha}_i, \check{\alpha}_j) \\
&= \frac{1}{2}\left(\frac{2\alpha_i}{(\alpha_i, \alpha_i)}, \frac{2\alpha_j}{(\alpha_j, \alpha_j)}\right) \\
&= \frac{1}{2}\left(\frac{2\alpha_i}{2}, \frac{2\alpha_j}{2}\right) \\
&= \frac{1}{2}(\alpha_i, \alpha_j) \\
&= -\frac{1}{2}
\end{aligned}$$

(see [16, Section V.7].)

**Proposition 2.11.** *Suppose $\mathcal{L}$ is split of type $D_4$. Then*

$$(H, \mathcal{K}' \mid_H) \cong \langle 1, 1, 1, 1 \rangle.$$

*In particular if $-1$ is a square, then $(\mathcal{L}, K')$ is a hyperbolic space.*

*Proof.* One has $R = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ with $\alpha_2$ adjacent to all other roots, and $\alpha_1, \alpha_3, \alpha_4$ all pairwise non-adjacent. Furthermore,

$$(\alpha_1, \alpha_2) = (\alpha_2, \alpha_3) = (\alpha_2, \alpha_4) = -1.$$

Let $x = H_{\alpha_1} x_1 + H_{\alpha_2} x_2 + H_{\alpha_3} x_3 + H_{\alpha_4} x_4$ and consider

$$\begin{aligned}
\mathcal{K}'(x) &= \mathcal{K}'(x, x) \\
&= x_1^2 + x_2^2 + x_3^2 + x_4^2 - x_1 x_2 - x_2 x_3 - x_2 x_4.
\end{aligned}$$

Now consider the invertible linear replacement of variables

$$\begin{aligned}
w_1 &= x_1 - \frac{x_2}{2} & w_2 &= \frac{x_2}{2} \\
w_3 &= x_3 - \frac{x_2}{2} & w_4 &= x_4 - \frac{x_2}{2}
\end{aligned}$$

so that

$$\mathcal{K}'(x) = w_1^2 + w_2^2 + w_3^2 + w_4^2.$$

□

The result can be generalized as follows:

**Proposition 2.12.** *Suppose $\mathcal{L}$ is split of type $D_n$ with $n \geq 4$. Then*

$$(H, \mathcal{K}' \mid_H) \cong \langle 1, 1 \rangle \oplus \langle \frac{1}{2}, ..., \frac{1}{2} \rangle.$$

*Proof.* As before, let $x = \sum_{i=1}^{n} = x_i H_{\alpha_i}$. Direct substitution leads to the normalized Killing form

$$\mathcal{K}'(x) = x_1^2 + \cdots + x_n^2 - x_1x_2 - \cdots - x_{n-2}x_{n-1} - x_{n-2}x_n.$$

Now let

$$w_{n-1} = x_{n-1} - \frac{1}{2}x_{n-2} \qquad\qquad w_n = x_n - \frac{1}{2}x_{n-2}$$

so that

$$\begin{aligned}\mathcal{K}'(x) &= x_1^2 + \ldots x_{n-3}^2 + \frac{1}{2}x_{n-2}^2 - x_1x_2 - \cdots - x_{n-3}x_{n-2} + w_{n-1}^2 + w_n^2 \\ &= \frac{1}{2}(2x_1^2 + \ldots 2x_{n-3}^2 + x_{n-2}^2 - 2x_1x_2 - \ldots 2x_{n-3}x_{n-2}) + w_{n-1}^2 + w_n^2 \\ &= \frac{1}{2}(x_1^2 + (x_1 - x_2)^2 + \cdots + (x_{n-3} - x_{n-2})^2) + w_{n-1}^2 + w_n^2.\end{aligned}$$

Now we make the replacement of variables

$$w_1 = x_1 \qquad\qquad w_i = w_{i-1} - w_i, \quad i = 2, \ldots, n-2$$

and one has

$$\mathcal{K}'(x) = \frac{1}{2}(w_1^2 + \cdots + w_{n-2}^2) + w_{n-1}^2 + w_n^2.$$

□

Notice that the above two propositions imply that the quadratic forms $\langle 1, 1, 1, 1 \rangle$ and $\langle 1, 1, \frac{1}{2}, \frac{1}{2} \rangle$ are equivalent. This motivates the following lemma:

**Lemma 2.13.** *For all $a \in k$, one has*

$$\langle a, a \rangle \cong \langle 2a, 2a \rangle.$$

*Proof.* Let $f(x) = 2ax_1^2 + 2ax_2^2$ and let

$$w_1 = x_1 + x_2 \qquad\qquad w_2 = x_1 - x_2.$$

Then

$$\begin{aligned} aw_1 + aw_2 &= a((x_1 + x_2)^2 + (x_1 - x_2)^2) \\ &= a(2x_1^2 + 2x_2^2) \\ &= f(x). \end{aligned}$$

□

One may also prove this lemma directly from the observation that

$$\langle 1, 1, 1, 1\rangle = \langle 1, 1, \frac{1}{2}, \frac{1}{2}\rangle$$

using Witt's Cancellation Theorem (see Theorem 1.24.)

**Corollary 2.14.** *Suppose $\mathcal{L}$ is split of type $D_n$ with $n \geq 4$. If $n$ is even then*

$$(H, \mathcal{K}' \mid_H) \cong \langle 1, \dots, 1\rangle.$$

*In particular, if $n$ is even and $-1$ is a square then $\mathcal{L}$ is hyperbolic.*
*If $n$ is odd, then*

$$(H, \mathcal{K}' \mid_H) \cong \langle \frac{1}{2}\rangle \oplus \langle 1, \dots, 1\rangle.$$

**Proposition 2.15.** *Suppose $\mathcal{L}$ is a split Lie algebra of type $E_8$. Then*

$$(H, \mathcal{K}' \mid_H) \cong \langle 1, 1, 1, 3, 3, 6, 10, 15\rangle.$$

*Proof.* Let $x = x_1 H_{\alpha_1} + \cdots + x_8 H_{\alpha_8}$. Direct substitution leads to the Killing form

$$\begin{aligned} \mathcal{K}'(x) =& x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2 \\ & x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_6 + x_5x_7 + x_5x_8. \end{aligned}$$

We then make the substitution of variables

$$\begin{aligned} w_1 &= x_1 - \frac{1}{2}x_2 & w_2 &= \frac{1}{2}x_2 - \frac{1}{3}x_3 \\ w_3 &= \frac{1}{3}x_3 - \frac{1}{4}x_4 & w_4 &= \frac{1}{4}x_4 - \frac{1}{5}x_5 \\ w_5 &= \frac{1}{30}x_5 & w_6 &= x_6 - \frac{1}{2}x_5 \\ w_7 &= \frac{1}{3}x_5 - \frac{1}{2}x_7 & w_8 &= x_8 - \frac{1}{2}x_7 \end{aligned}$$

and one may check that

$$\mathcal{K}'(x) = w_1 + 3w_2 + 6w_3 + 10w_4 + 15w_5 + w_6 + 3w_7 + w_8.$$

□

**Corollary 2.16.** *If $\mathcal{L}$ is a split Lie algebra of type $E_8$ over a field $k$, and $-1$ is a square in $k$, then $(H, \mathcal{K}' \mid_H)$ is a hyperbolic space.*

*Proof.* If $-1$ is a square, then $\{3, 3\}$ is hyperbolic, so

$$(H, \mathcal{K}' \mid_H) \cong \mathbb{H} \oplus \mathbb{H} \oplus \langle 1, 6, 10, 15 \rangle.$$

Note that the 3-dimensional form $\langle 6, 10, 15 \rangle$ represents 1, so by 1.17 there exist $a, b \in k$ such that $\langle 6, 10, 15 \rangle \cong \langle 1, a, b \rangle$. Moreover,

$$d(\langle 6, 10, 15 \rangle) = d(\langle 1, a, b \rangle) \in (k/k^2),$$

and since $d(\langle 6, 10, 15 \rangle)$ is square, one has $ab \in k^2$. In particular, $\langle a, b \rangle \cong \langle a, a \rangle$ and so

$$\langle 1, 6, 10, 15 \rangle \cong \mathbb{H} \oplus \mathbb{H}.$$

□

# 3 Killing Forms of Twisted Lie Algebras

Let $G$ be a split simply connected simple group. Then $G$ has a split maximal torus $T \cong G_m \times ... \times G_m$. Let $N$ be the normalizer of $T$ in $G$ (one has $T \subseteq N \subseteq G$.) Then $\mathcal{H} := \text{Lie}(T)$ is a split Cartan subalgebra of $\mathcal{L} := \text{Lie}(G)$. Let $\Sigma$ be a root system for $\mathcal{L}$ relative to $\mathcal{H}$.

Then the Weyl group $W$ of $\Sigma$ is isomorphic to the quotient $N/T$. It is shown in [7] that if the element $-1 \in \mathrm{Aut}(\Sigma)$ lies in $W$ (as is the case for groups of type $D_4$, $D_8$, and $E_8$,) then there exists a lifting $w_0$ of the element $-1 \in W$ to $N$, such that $w_0$ has order 2 and for all $t \in T$ one has $w_0 t w_0^{-1} = t^{-1}$ (see [11], Section 27.1.)

Recall that $\mathcal{L}$ has the form

$$\mathcal{L} = H \oplus \bigoplus_{\alpha \in \Sigma} \langle X_\alpha, X_{-\alpha} \rangle.$$

The action of $w_0$ on $\mathcal{L}$ by conjugation can be described on these parts - for $h \in H$ one has $w_0(h)w_0^{-1} = -h$.

**Proposition 3.1.** *For all $\alpha \in \Sigma$ one has $w_0(X_\alpha)w_0^{-1} = c_\alpha X_{-\alpha}$ for some $c_\alpha \in k$.*

*Proof.* Suppose $t$ is an element of $T(k^{\mathrm{sep}})$ and consider the conjugation of $w_0 X_\alpha w_0^{-1}$ by $t$. One finds

$$\begin{aligned} t(w_0 X_\alpha w_0^{-1})t^{-1} &= w_0 w_0^{-1} t w_0 X_\alpha w_0^{-1} t^{-1} w_0 w_0^{-1} \\ &= w_0 t^{-1} X_\alpha w_0 t^{-1} w_0^{-1} w_0^{-1} \\ &= w_0 t^{-1} X_\alpha t w_0^{-1} \\ &= w_0 \alpha(t^{-1}) X_\alpha w_0^{-1} \\ &= -\alpha(t) w_0 X_\alpha w_0^{-1}. \end{aligned}$$

In other words, for all $t \in T$, the element $w_0 X_\alpha w_0^{-1}$ is an eigenvector of $\mathrm{Ad}(t)$ with weight $-\alpha(t)$ and therefore lies in the one dimensional eigenspace $X_{-\alpha}$. □

Now consider a ground field $k$ and an element $d \in k$ which is not a square. Let $\ell/k$ be the quadratic extension $\ell := k(\sqrt{d})$, and let

$$\Gamma := \mathrm{Gal}(\ell/k) = \{1, \sigma\}$$

where $\sigma$ is the unique nontrivial element of $\Gamma$ which maps $\sqrt{d} \mapsto -\sqrt{d}$. Consider the cocycle $\zeta = (a_\tau) \in Z^1(k/\ell, G(\ell))$ given by

$$a_1 = 1, \qquad\qquad a_\sigma = w_0(t)$$

where $t$ is any element in $T(k)$.To see that $\zeta$ is in fact a cocycle, one checks that

$$a_{\tau_1\tau_2} = a_{\tau_1}\tau_1(a_{\tau_2})$$

for all $\tau_1, \tau_2 \in \Gamma$. If $\tau_1$ or $\tau_2$ are 1, this is trivial. In the remaining case we have

$$\begin{aligned} a_\sigma \sigma(a_\sigma) &= (w_0 t)\sigma(w_0 t) \\ &= (w_0 t)(w_0 t) \\ &= (w_0 t w_0^{-1})t \\ &= t^{-1}t \\ &= 1 = a_1 = a_{\sigma\sigma}. \end{aligned}$$

Consider the Lie algebra $\mathcal{L}$ together with the twisted action of $\Gamma$ by $\zeta$ on $\mathcal{L}$. As per Theorem 6.6, the subalgebra ${}^\zeta\mathcal{L}$ of elements invariant under the twisting action, together with the restriction of the Killing form to that subalgebra, is a $k$-form of $(\mathcal{L}, \mathcal{K})$.

Let us proceed to compute this invariant subspace, which we denote by $\mathcal{L}_\ell^{*\Gamma}$.

**Proposition 3.2.** *The subalgebra $\mathcal{H}$ is stable with respect to the twisted action, as are the two-dimensional subspaces $\langle X_\alpha, X_{-\alpha}\rangle$ for all $\alpha$.*

*Proof.* Each of these pieces is known to be stable under the standard action, and so it suffices to show that they are stable with respect to conjugation by $a_\sigma = w_0 t$.

Note that for all $\alpha \in \Sigma$ one has

$$\begin{aligned} w_0 t X_\alpha t^{-1} w_0^{-1} &= w_0 \alpha(t) X_\alpha w_0^{-1} \\ &= \alpha(t) c_\alpha X_{-\alpha}. \end{aligned}$$

As previously discussed, $\mathcal{H}$ is stable under conjugation by elements of $T$, and also stable under conjugation by $w_0$. Thus, it is stable under conjugation by $a_\sigma$. □

In view of the above proposition, we can see that

$$\mathcal{L}_\ell^{*\Gamma} = \mathcal{H}_\ell^{*\Gamma} \oplus \bigoplus_{\alpha\in\Sigma^+} (\langle X_\alpha, X_{-\alpha}\rangle^{*\Gamma}),$$

where for any subspace V of $\mathcal{L}$, we let $\mathrm{V}^{*\Gamma}$ denote the subspace of V invariant under the twisted action of $\Gamma$ by $\zeta$.

**Proposition 3.3.** *The following vectors are invariant under the twisted action, and form a basis of $\mathcal{L}_\ell^{*\Gamma}$.*

1. *For $i = 1, ..., n$, the vector $\sqrt{d}H_{\alpha_i}$.*

*2. For $\alpha \in \Sigma^+$, the vectors $X_\alpha + \sigma._\zeta(X_\alpha)$ and $\sqrt{d}(X_\alpha - \sigma._\zeta(X_\alpha))$.*

*Proof.* For $i = 1, ..., n$, one has

$$\begin{aligned}
\sigma._\zeta(\sqrt{d}H_{\alpha_i}) &= \sigma(w_0 t(\sqrt{d}H_{\alpha_i})t^{-1}w_0^{-1}) \\
&= -\sqrt{d}\sigma(w_0 t H_{\alpha_i} t^{-1} w_0^{-1}) \\
&= -\sqrt{d}\sigma(-H_{\alpha_i}) \\
&= -\sqrt{d}(-H_{\alpha_i}) \\
&= \sqrt{d}H_{\alpha_i}.
\end{aligned}$$

It is then clear that the vectors of this form constitute a basis for $\mathcal{H}$.

For $\alpha \in \Sigma^+$, one has

$$\begin{aligned}
\sigma._\zeta(X_\alpha + \sigma._\zeta(X_\alpha)) &= \sigma(w_0 t(X_\alpha + \sigma(w_0 t X_\alpha t^{-1} w_0^{-1})t^{-1})w_0^{-1}) \\
&= \sigma(w_0 t X_\alpha t^{-1} w_0^{-1}) + \sigma(w_0 t \sigma(w_0 t X_\alpha t^{-1} w_0^{-1}) t^{-1} w_0^{-1}) \\
&= \sigma._\zeta(X_\alpha) + X_\alpha
\end{aligned}$$

and

$$\begin{aligned}
\sigma._\zeta(\sqrt{d}(X_\alpha - \sigma._\zeta(X_\alpha))) &= -\sqrt{d}\sigma._\zeta(X_\alpha - \sigma._\zeta(X_\alpha)) \\
&= -\sqrt{d}(\sigma._\zeta(X_\alpha) - X_\alpha) \\
&= \sqrt{d}(X_\alpha - \sigma._\zeta(X_\alpha)).
\end{aligned}$$

Moreover, these two vectors are linearly independent. One has

$$\begin{aligned}
X_\alpha + \sigma._\zeta(X_\alpha) &= X_\alpha + \alpha(t)c_\alpha X_{-\alpha} \\
\sqrt{d}(X_\alpha - \sigma._\zeta(X_\alpha)) &= \sqrt{d}(X_\alpha - \alpha(t)c_\alpha X_{-\alpha}).
\end{aligned}$$

□

Using this basis, we may now compute the restriction of the reduced Killing form $\mathcal{K}'$ to the invariant subspace $\mathcal{L}_\ell^{*\Gamma}$. Let us first note that

$$(\mathcal{K}', \mathcal{L}_\ell^{*\Gamma}) = (\mathcal{K}', \langle\sqrt{d}H_{\alpha_1}, ...\sqrt{d}H_{\alpha_2}\rangle) \oplus \bigoplus_{\alpha\in\Sigma^+} (\mathcal{K}', \langle X_\alpha + \sigma._\zeta(X_\alpha), \sqrt{d}(X_\alpha - \sigma._\zeta(X_\alpha))\rangle)$$

since the summands are stable under the twisted action and therefore orthogonal to one another.

**Proposition 3.4.**

$$(\mathcal{K}', \langle \sqrt{d}H_{\alpha_1}, ...\sqrt{d}H_{\alpha_2}\rangle) \cong d(\mathcal{K}', \mathcal{H}).$$

*Proof.* This follows immediately from the observation that for all $i, j = 1, ..., n$ one has

$$\mathcal{K}'(\sqrt{d}H_{\alpha_i}, \sqrt{d}H_{\alpha_j}) = d\mathcal{K}'(H_{\alpha_i}, H_{\alpha_j}).$$

□

**Proposition 3.5.** *For all* $\alpha \in \Sigma^+$, *one has*

$$(\mathcal{K}', \langle X_\alpha + \sigma._\zeta(X_\alpha), \sqrt{d}(X_\alpha - \sigma._\zeta(X_\alpha))\rangle) \cong \alpha(t)c_\alpha\langle 1, -d\rangle = \alpha(t)c_\alpha\langle\langle d\rangle\rangle.$$

*Proof.* We compute the reduced Killing form on the basis elements:

$$\begin{aligned}
&\mathcal{K}'(X_\alpha + \sigma._\zeta X_\alpha, \sqrt{d}(X_\alpha - \sigma._\zeta X_\alpha)) \\
&= \sqrt{d}(\mathcal{K}'(X_\alpha, X_\alpha) - \mathcal{K}'(X_\alpha, \sigma._\zeta X_\alpha) + \mathcal{K}'(X_\alpha, \sigma._\zeta X_\alpha) - \mathcal{K}'(\sigma._\zeta X_\alpha, \sigma._\zeta X_\alpha)) \\
&= \sqrt{d}(\mathcal{K}'(X_\alpha, X_\alpha) - \mathcal{K}'(\sigma._\zeta X_\alpha, \sigma._\zeta X_\alpha)) \\
&= \sqrt{d}(0 - \mathcal{K}'(\sigma._\zeta X_\alpha, \sigma._\zeta X_\alpha)) \\
&= -\sqrt{d}\mathcal{K}'(w_0 t X_\alpha t^{-1} w_0^{-1}, w_0 t X_\alpha t^{-1} w_0^{-1}) \\
&= -\sqrt{d}\mathcal{K}'(\alpha(t)c_\alpha X_{-\alpha}, \alpha(t)c_\alpha X_{-\alpha}) \\
&= -\sqrt{d}\alpha(t)^2 c_\alpha^2 \mathcal{K}'(X_{-\alpha}, X_{-\alpha}) \\
&= -\sqrt{d}\alpha(t)^2 c_\alpha^2 (0) \\
&= 0.
\end{aligned}$$

$$\begin{aligned}
&\mathcal{K}'(X_\alpha + \sigma._\zeta X_\alpha, X_\alpha + \sigma._\zeta X_\alpha) \\
&= \mathcal{K}'(X_\alpha, X_\alpha) + 2\mathcal{K}'(X_\alpha, \sigma._\zeta X_\alpha) + \mathcal{K}'(\sigma._\zeta X_\alpha, \sigma._\zeta X_\alpha) \\
&= 2\mathcal{K}'(X_\alpha, \sigma._\zeta X_\alpha) \\
&= 2\mathcal{K}'(X_\alpha, \alpha(t)c_\alpha X_{-\alpha}) \\
&= 2\alpha(t)c_\alpha \mathcal{K}'(X_\alpha, X_{-\alpha}) \\
&= \alpha(t)c_\alpha.
\end{aligned}$$

$$\begin{aligned}&\mathcal{K}'(\sqrt{d}(X_\alpha - \sigma._\zeta X_\alpha), \sqrt{d}(X_\alpha - \sigma._\zeta X_\alpha))\\ &= d\mathcal{K}'((X_\alpha - \sigma._\zeta X_\alpha), (X_\alpha - \sigma._\zeta X_\alpha))\\ &= d\mathcal{K}'(X_\alpha, X_\alpha) - 2\mathcal{K}'(X_\alpha, \sigma._\zeta X_\alpha) + \mathcal{K}'(\sigma._\zeta X_\alpha, \sigma._\zeta X_\alpha)\\ &= -2d\mathcal{K}'(X_\alpha, \sigma._\zeta X_\alpha)\\ &= -d\alpha(t)c_\alpha.\end{aligned}$$

□

Now that we have a general formula, we will compute some specific cases. Let us assume henceforth that $-1$ is a square in $k$, so that $c_\alpha$ is also a square for all $\alpha \in \Sigma^+$ in each case (because all $c_\alpha$ are $\pm 1$).

We adopt the notation $\mathcal{K}'_{d,t}$ for the restriction of $\mathcal{K}$ to the invariant subspace of $\mathcal{L}$ under the twisted action of $\Gamma$ by $\zeta$, where $\zeta$ is the cocycle constructed above with parameters $\ell = k(\sqrt{d})$ and $t \in T(k)$. Then for Lie algebras of type $D_4, D_8$, and $E_8$, the restriction of $\mathcal{K}'_{d,t}$ to our Cartan subalgebra $\mathbb{H}$ becomes hyperbolic. From here forward we will work only in the Witt ring, and so for each of the aforementioned cases we have

$$\begin{aligned}\mathcal{K}'_{d,t} &= \bigoplus_{\alpha\in\Sigma^+} \alpha(t)c_\alpha\langle\langle d\rangle\rangle\\ &= \bigoplus_{\alpha\in\Sigma^+} \alpha(t)\langle\langle d\rangle\rangle\\ &= \langle\langle d\rangle\rangle \otimes \bigoplus_{\alpha\in\Sigma^+} \langle\alpha(t)\rangle.\end{aligned}$$

We will simplify our computations by working first with the form

$$\widetilde{\mathcal{K}}_t = \bigoplus_{\alpha\in\Sigma^+} \langle\alpha(t)\rangle.$$

# CHAPTER VI

# Cohomological Invariants Arising via the Killing Form

## 1 Simply Connected Groups of Types $D_n$

Let $G$ be a simple simply connected algebraic group of type $D_n$ over a ground field $k$ with Lie algebra $\mathrm{Lie}(G) = \mathcal{L}$. As before, let $\ell = k(\sqrt{d})$, let $1 \neq \sigma \in \mathrm{Gal}(\ell/k)$, and let $\varphi = (a_{\sigma,t})$ be a cocycle given by

$$a_{\sigma,t} = \check{\alpha}_1(t_1) \dots \check{\alpha}_n(t_n) w_0.$$

Consider the restriction of $\mathcal{K}$ to the $k$-vector subspace of $\mathcal{L} \otimes \ell$ invariant under the twisted action of $\mathrm{Gal}(\ell/k)$, denoted by $\mathcal{K}'_{d,t}$.

**Proposition 1.1.** *Suppose $-1$ is a square in $k$. If $n$ is even then the quadratic form $\mathcal{K}'_{d,t}$ is hyperbolic.*

*Proof.* We consider the following realization of the root system of type $D_n$ (see [16, Section V.16]). Let $\epsilon_1, ..., \epsilon_n$ be the standard basis of $\mathbb{R}^n$ and let

$$\Sigma := \{\pm\epsilon_i \pm \epsilon_j \mid 1 \leq i < j \leq n\}.$$

For a base $S$ we may take the simple roots

$$\alpha_i := \epsilon_i - \epsilon_{i+1}, \quad i < n, \quad \alpha_n := \epsilon_{n-1} + \epsilon_n.$$

It is easy to see that all roots of the form $-\epsilon_i \pm \epsilon_j$ where $i < j$ are negative. Since exactly half of all roots in $\Sigma$ have this form, it follows

$$\Sigma_S^+ = \{\epsilon_i \pm \epsilon_j \mid 1 \leq i < j \leq n\}.$$

We introduce the following notation for the positive roots in $\Sigma$ with respect to $S$ for all $1 \leq i < j \leq n$ :

$$\alpha_{i-j} := \epsilon_i - \epsilon_j, \quad \alpha_{i+j} := \epsilon_i + \epsilon_j.$$

To show that $\mathcal{K}'_{d,t}$ is hyperbolic, it suffices to show that all two dimensional quadratic forms

$$\langle \alpha_{i-j}(t), \alpha_{i+j}(t) \rangle$$

are hyperbolic, which since -1 is a square is equivalent to showing that $(\alpha_{i+j} - \alpha_{i+j})(t)$ is a square. Indeed, one has

$$\begin{aligned}(\alpha_{i+j} - \alpha_{i-j})(t) &= (\epsilon_i + \epsilon_j - \epsilon_i + \epsilon_j)(t) \\ &= (2\epsilon_j)(t) \\ &= \epsilon_j(t)^2.\end{aligned}$$

□

# 2 The Centres of Simply Connected Groups of Type $D_{2n}$

Let $f$ be a hyperbolic quadratic form of dimension $4n$ over a field $K$ of characteristic not 2, and let $G = \mathrm{Spin}(f)$, so that $G$ is a simply connected split algebraic group of type $D_{2n}$. It is known that

$$Z(G) \cong \mu_2 \times \mu_2,$$

although this decomposition is not unique.

Let $A$ be a subgroup of $Z(G)$, and consider the quotient group $G/A$ (we may consider the quotient of $G$ by any closed normal subgroup, see [11, Section 12]). The quotient map

$$\varphi : G \twoheadrightarrow G/A$$

induces the differential map

$$d\varphi : \mathrm{Lie}(G) \to \mathrm{Lie}(G/A)$$

(see 1.6).

Since the characteristic of $K$ is good (i.e. not equal to 2) one has $\mathrm{Lie}(\ker(\varphi)) = \ker(d\varphi)$. Since $\ker(\varphi) = A$ is finite the identity component $\ker(\varphi)^\circ$ of the kernel is 1, and thus

$$\mathrm{Lie}(\ker(\varphi)) = \mathrm{Tan}_e(\ker(\varphi)) = \mathrm{Lie}(\ker(\varphi)^\circ) = 0,$$

and so $d\varphi$ is injective.

Moreover, one has $\dim(\mathrm{Lie}(G)) = \dim(\mathrm{Lie}(G/A))$ since $\dim(G) = \dim(G/A)$, and so since $d\varphi$ has trivial kernel it is automatically surjective. As such, the map

$$d\varphi : \mathrm{Lie}(G) \to \mathrm{Lie}(G/A)$$

is an isomorphism, so $G/A$ is also of type $D_{2n}$.

If $A = 1$, then $G/A = G = \mathrm{Spin}(f)$. If $A = Z(G) = \mu_2 \times \mu_2$, the group $G/A$ is called **adjoint.**

It is known that there exists a decomposition $Z(G) = \mu_2 \times \mu_2$ such that

$$G/\langle -1, -1\rangle = \mathrm{SO}(f).$$

Under this decomposition, one has $G/\langle 1, -1\rangle \cong G/\langle -1, 1\rangle$. This group is called **half-spin**.

Let $A = \langle -1, 1\rangle$ (or equivalently $A = \langle 1, -1\rangle$) so that $G/A$ is the half-spin group. Consider the adjoint representation

$$\mathrm{Ad}_G : G \to \mathrm{Lie}(G) = \mathrm{Lie}(G/A).$$

Since $A \subset \ker(\mathrm{Ad}_G)$ the map $\mathrm{Ad}_G$ factors through $G/A$, in particular

$$\mathrm{Ad}_G = \mathrm{Ad}_{G/A} \circ \varphi,$$

where $\mathrm{Ad}_{G/A}$ is the adjoint representation $G/A \to \mathrm{Lie}(G/A) = \mathrm{Lie}(G)$ and as before $\varphi : G \twoheadrightarrow G/A$ is the quotient map.

Let $T \subset G$ be a split maximal torus, and let $T' = \varphi(T)$. Then $T'$ is a split maximal torus in $G/A$. Let $w_0 \in N := N_G(T)$ be as before, and let $w_0' = \varphi(w_0)$. Then $w_0' \in N_{G/A}(T')$ is of order 2 and for all $t' \in T'$ one has

$$w_0' t' (w_0')^{-1} = (t')^{-1}.$$

Let us consider the set of 1-cohomology classes over $K$ taking values in the subgroup $\langle T', w_0' \rangle \subset G/A$, that is the set

$$H^1(K, \langle T', w_0' \rangle).$$

Recall that the inclusion $\langle T', w_0' \rangle \hookrightarrow G/A$ induces a map

$$\varphi : H^1(K, \langle T', w_0' \rangle) \to H^1(K, G/A)$$

and so we may also view these as cohomology classes with coefficients in $G/A$.

**Remark:** The map $\varphi$ is not necessarily injective. However, suppose we have two cocycles $(a_{\sigma,t'})$ and $(a_{\sigma,s'})$ such that

$$\varphi([a_{\sigma,t'}]) = \varphi([a_{\sigma,s'}]).$$

Since the cocycles in $H^1(K, G/A)$ are cohomologous, the twisted Lie algebras are isomorphic, hence their Killing forms are isomorphic over the ground field. Thus, our construction of cohomological invariants below does not depend on the choice of representative of cohomology classes.

We now introduce the character and cocharacter groups for an arbitrary algebraic torus $T$. Recall that the character group of $T$ is the group

$$X(T) := \mathrm{Hom}(T, G_m).$$

**Definition 2.1.** *The* ***cocharacter group*** *of $T$ is the group*

$$X(T)_* := \mathrm{Hom}(G_m, T).$$

There exists a natural perfect pairing

$$\langle -, - \rangle : X(T)_* \times X(T) \to \mathbb{Z}$$

given as follows. For any $\lambda \in X(T)_*$ and $\mu \in X(T)$ the composition

$$\mu \circ \lambda : G_m \to G_m$$

is a morphism. It is well known that all such morphisms are of the form

$$\begin{aligned} \mu \circ \lambda : G_m &\to G_m \\ g &\mapsto g^n \end{aligned}$$

for some $n \in \mathbb{Z}$. Then we let $\langle \lambda, \mu \rangle := n$.

We now come back to a split maximal torus $T \subset G = \mathrm{Spin}(f)$. Since the above pairing is perfect for every $\alpha \in \Sigma \subset X(T)$ there exists a unique cocharacter, which we denote by $\check{\alpha} \in X(T)_*$ such that for all $\beta \in \Sigma$ and for all $t \in T$ one has

$$\mathrm{Ad}(\check{\alpha}(t))(X_\beta) = t^{\langle \beta, \alpha \rangle} X_\beta.$$

For simply connected groups, it is known that if

$$\alpha_1, ..., \alpha_{2n}$$

is a base of $\Sigma$ then every element $t \in T$ may be written uniquely as

$$t = \prod_{i=1}^{2n} \check{\alpha}_i(t_i)$$

for some elements $t_i \in G_m$ (see [20, Corollary to Lemma 3.28]).

In other words, the natural morphism

$$\begin{aligned} G_m \times \ldots \times G_m &\to T \\ (t_1, \ldots, t_{2n}) &\mapsto \prod_{i=1}^{2n} \check{\alpha}_i(t_i) \end{aligned}$$

is an isomorphism.

**Proposition 2.2.** *Let*

$$\begin{aligned} z_1 &= \check{\alpha}_1(-1)\check{\alpha}_3(-1)\ldots\check{\alpha}_{2n-3}(-1)\check{\alpha}_{2n-1}(-1) \\ z_2 &= \check{\alpha}_1(-1)\check{\alpha}_3(-1)\ldots\check{\alpha}_{2n-3}(-1)\check{\alpha}_{2n}(-1). \end{aligned}$$

*Then one has*

$$Z(G) = \langle z_1, z_2 \rangle.$$

*Proof.* It is clear that $z_1$ and $z_2$ are of order 2 and that $z_1 \neq z_2^{\pm 1}$. Since $Z(G) = \mu_2 \times$

$\mu_2$, it therefore suffices to show that $z_1, z_2 \in Z(G)$. Recall that the kernel of the adjoint representation

$$\mathrm{Ad} : G \to \mathrm{GL}(\mathrm{Lie}(G))$$

coincides with $Z(G)$. Since $T$ acts trivially on $\mathcal{H} = \mathrm{Lie}(T)$ by conjugation, it further suffices to show that, for all $\alpha \in \Sigma_S^+$, one has

$$z_1 X_\alpha z_1^{-1} = z_2 X_\alpha z_2^{-1} = X_\alpha,$$
$$z_1 X_{-\alpha} z_1^{-1} = z_2 X_{-\alpha} z_2^{-1} = X_{-\alpha}.$$

Using the relation

$$\check{\alpha}_i(t) X_\alpha \alpha_i(t^{-1}) = t^{\langle \alpha, \check{\alpha}_i \rangle} X_\alpha$$

one has

$$z_1 X_\alpha z_1^{-1} = (-1)^{\langle m, \alpha \rangle} X_\alpha$$

where

$$\langle m, \alpha \rangle = \sum_{i=1}^{2n} \langle \alpha_{2i-1}, \alpha \rangle$$

It suffices to show that the sum above is even. Furthermore it suffices to show this under the assumption that $\alpha$ is a simple root, i.e. $\alpha = \alpha_j$ for some $j = 1, ..., 2n$. Considering the Dynkin diagram of the root system of type $D_n$ (see Section 2) it is clear to see that we have three cases: either $j$ is odd in which case the term $\langle \alpha_j, \alpha_j \rangle = 2$ appears and all other terms are zero, $j$ is even and not equal to $2n$ in which case the terms $\langle \alpha_{j-1}, \alpha_j \rangle = -1$ and $\langle \alpha_{j+1}, \alpha_j \rangle = -1$ appear and all other terms are zero, or $j = 2n$ in which case all terms are zero.

The proof for $z_2$ is exactly the same except that the exceptional case is $j = 2n - 1$ rather than $j = 2n$. □

# 3 Non-Simply Connected Groups of $D_4$

Let us describe now the Killing form of some of these quotient groups. We begin with the case where $G$ is of type $D_4$ and $A = \langle z_2 \rangle$, so that $G' = G/A$ is of type $D_4$ half-spin.

We wish first to parametrize $k$-points of the maximal split torus $T' \subset G'$. Recall that every element $t \in T(k)$ has a unique decomposition $t = \check{\alpha}_1(t_1)\check{\alpha}_2(t_2)\check{\alpha}_3(t_3)\check{\alpha}_4(t_4)$. Consider the following two morphisms

$$\begin{aligned} \sigma : T \to T, &\quad t \mapsto \check{\alpha}_1(t_1t_4)\check{\alpha}_2(t_2)\check{\alpha}_3(t_3)\check{\alpha}_4(t_4) \\ \tau : T \to T, &\quad t \mapsto \check{\alpha}_1(t_1)\check{\alpha}_2(t_2)\check{\alpha}_3(t_3)\check{\alpha}_4(t_4^2). \end{aligned}$$

One easily checks that $\sigma$ is an automorphism of $T$ and $\ker(\tau\circ\sigma) = \langle z_2 \rangle$ and so the composition $\tau \circ \sigma$ can be identified with the quotient map $T \to T'$.

Under this identification, one checks that a preimage of $t' := \check{\alpha}_1(t'_1)\check{\alpha}_2(t'_2)\check{\alpha}_3(t'_3)\check{\alpha}_4(t'_4)$ is

$$t := \check{\alpha}_1(\frac{t'_1}{\sqrt{t'_4}})\check{\alpha}_2(t'_2)\check{\alpha}_3(t'_3)\check{\alpha}_4(\sqrt{t'_4}).$$

Recall that $\Sigma \subset X(T') \subset X(T)$. Therefore, for any root $\alpha \in \Sigma$ one has $\alpha(t) = \alpha(t')$ where $t \in T$ is a preimage of $t'$ under the quotient map $T \to T'$. Then we have

$$\begin{aligned} \alpha(t') &= \alpha(t) \\ &= \left(\frac{t'_1}{\sqrt{t'_4}}\right)^{\langle \alpha_1, \alpha\rangle} t_2'^{\langle \alpha_2,\alpha\rangle} t_3'^{\langle \alpha_3,\alpha\rangle} \sqrt{t'_4}^{\langle \alpha_4,\alpha\rangle} \\ &= t_1'^{\langle \alpha_1,\alpha\rangle} t_2'^{\langle \alpha_2,\alpha\rangle} t_3'^{\langle \alpha_3,\alpha\rangle} t_4'^{\frac{1}{2}\langle \alpha_4-\alpha_1,\alpha\rangle}. \end{aligned}$$

**Lemma 3.1.** *Let $t' := \check{\alpha}_1(t'_1)\check{\alpha}_2(t'_2)\check{\alpha}_3(t'_3)\check{\alpha}_4(t'_4) \in T'(k)$. For all $i < j$ one has modulo squares*

$$\alpha_{i-j}(t') = t'_4\alpha_{i+j}(t').$$

*Proof.* Since $\alpha_{i-j}$ and $\alpha_{i+j}$ are characters of $T'$, there exist unique integers $m_1, m_2, m_3, m_4$ such that

$$\alpha_{i-j}(t') = (t'_1)^{m_1}(t'_2)^{m_2}(t'_3)^{m_3}(t'_4)^{m_4}$$

and unique integers $n_1, n_2, n_3, n_4$ such that

$$\alpha_{i+j}(t') = t_1'^{n_1}t_2'^{n_2}t_3'^{n_3}t_4'^{n_4}.$$

By the same logic laid out in Proposition 1.1 the differences $m_1 - n_1, m_2 - n_2$, and $m_3 - n_3$

are even. On the other hand

$$\begin{aligned} m_4 - n_4 &= \frac{1}{2}\langle \alpha_4 - \alpha_1, \alpha_{i+j}\rangle - \frac{1}{2}\langle \alpha_4 - \alpha_1, \alpha_{i-j}\rangle \\ &= \frac{1}{2}\langle \alpha_4 - \alpha_1, 2\epsilon_j\rangle \\ &= \langle \alpha_4 - \alpha_1, \epsilon_j\rangle \\ &= \langle -\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4, \epsilon_j\rangle \\ &= 1. \end{aligned}$$

□

**Lemma 3.2.** *Let $\overline{\epsilon} = \epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4$. For all $i < j$, let $\alpha'_{i+j} = \overline{\epsilon} - \alpha_{i+j}$. Then for all $t' \in T'$ one has*

$$\alpha_{i+j}(t')\alpha'_{i+j}(t') = t'_4$$

*modulo squares.*

*Proof.* Let $k = 1, 2, 3, 4$. One has

$$\langle \alpha_k, \alpha_{i+j}\rangle + \langle \alpha_k, \alpha'_{i+j}\rangle = \langle \alpha_k, \overline{\epsilon}\rangle.$$

One checks that $\langle \alpha_k, \overline{\epsilon}\rangle$ is equal to 2 if $k = 4$ and 0 otherwise. Then

$$\begin{aligned} \alpha_{i+j}(t')\alpha'_{i+j}(t') &= \overline{\epsilon}(t) \\ &= t_1'^{\langle \alpha_1, \epsilon\rangle} t_2'^{\langle \alpha_2, \epsilon\rangle} t_3'^{\langle \alpha_3, \epsilon\rangle} t_4'^{\frac{1}{2}\langle \alpha_4 - \alpha_1, \epsilon\rangle} \\ &= t_1'^0 t_2'^0 t_3'^0 t_4'^1 \end{aligned}$$

□

Note that for all $i < j$ one has $\alpha'_{i+j}$ is equal to $\alpha_{i'+j'}$ for some $i' < j'$. Furthermore, $(\alpha'_{i+j})' = \alpha_{i+j}$ and $\alpha'_{i+j} \neq \alpha_{i+j}$. As such, the roots $\alpha_{i+j}$ are partitioned into pairs $(\alpha_{i+j}, \alpha'_{i+j})$.

**Proposition 3.3.** *Let $t' = \check{\alpha}_1(t'_1)\check{\alpha}_2(t'_2)\check{\alpha}_3(t'_3)\check{\alpha}_4(t'_4)$. The reduced Killing form $\mathcal{K}'_{d,t'}$ for half-spin groups of type $D_4$ is hyperbolic.*

*Proof.* By Lemma 3.1 one has

$$K'_{d,t'} = \langle\langle d, t'_4\rangle\rangle \otimes \bigoplus_{i<j} \langle \alpha_{i+j}(t')\rangle,$$

and by then Lemma 3.2 and the following remarks

$$\bigoplus_{i<j} \langle \alpha_{i+j}(t') \rangle = \langle\langle t'_4 \rangle\rangle \otimes f$$

for some 3-dimensional quadratic form $f$. Then

$$K'_{d,t'} = \langle\langle d, t'_4, t'_4 \rangle\rangle \otimes f$$

which is hyperbolic (because $-1$ is a square). □

Next we consider the adjoint group of type $D_4$, that is the quotient of a simply connected group of type $D_4$ by its center. We construct the quotient map again in a similar fashion, this time choosing

$$\begin{aligned} \sigma &: t \mapsto \check{\alpha}_1(t_1 t_3 t_4)\check{\alpha}_2(t_2)\check{\alpha}_3(t_3)\check{\alpha}_4(t_4) \\ \tau &: t \mapsto \check{\alpha}_1(t_1)\check{\alpha}_2(t_2)\check{\alpha}_3(t_3^2)\check{\alpha}_4(t_4^2). \end{aligned}$$

Thus, we may identify the quotient map $T \to T' = T/Z(G)$ with the map

$$\begin{aligned} G_m \times G_m \times G_m \times G_m &\to G_m \times G_m \times G_m \times G_m \\ (t_1, t_2, t_3, t_4) &\mapsto (t_1 t_3 t_4, t_2, t_3^2, t_4^2). \end{aligned}$$

Under this identification, if $t' = (t'_1, t'_2, t'_3, t'_4)$ and $t$ is a preimage of $t'$, say

$$t = (\frac{t'_1}{\sqrt{t'_3 t'_4}}, t'_2, \sqrt{t'_3}, \sqrt{t'_4})$$

then

$$\begin{aligned} \alpha(t') &= \alpha(t) \\ &= \left(\frac{t'_1}{\sqrt{t'_3 t'_4}}\right)^{\langle \alpha_1, \alpha \rangle} t_2'^{\langle \alpha_2, \alpha \rangle} \sqrt{t'_3}^{\langle \alpha_3, \alpha \rangle} \sqrt{t'_4}^{\langle \alpha_4, \alpha \rangle} \\ &= t_1'^{\langle \alpha_1, \alpha \rangle} t_2'^{\langle \alpha_2, \alpha \rangle} t_3'^{\frac{1}{2}\langle \alpha_3 - \alpha_1, \alpha \rangle} t_4'^{\frac{1}{2}\langle \alpha_4 - \alpha_1, \alpha \rangle}. \end{aligned}$$

**Lemma 3.4.** *For all $i < j$ and for all $t' \in T'$ the following* 1*-dimensional quadratic forms are isomorphic:*

$$\langle \alpha_{i+j}(t') \rangle = \langle t'_3 t'_4 \alpha_{i-j}(t') \rangle.$$

*Proof.* One computes

$$\begin{aligned}
\frac{1}{2}\langle \alpha_3 - \alpha_1, \alpha_{i+j}\rangle - \frac{1}{2}\langle \alpha_3 - \alpha_1, \alpha_{i-j}\rangle &= \frac{1}{2}\langle \alpha_3 - \alpha_1, 2\epsilon_j\rangle \\
&= \langle -\epsilon_1 + \epsilon_2 + \epsilon_3 - \epsilon_4, \epsilon_j\rangle \\
&= \pm 1, \\
\frac{1}{2}\langle \alpha_4 - \alpha_1, \alpha_{i+j}\rangle - \frac{1}{2}\langle \alpha_4 - \alpha_1, \alpha_{i-j}\rangle &= \frac{1}{2}\langle \alpha_4 - \alpha_1, 2\epsilon_j\rangle \\
&= \langle -\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4, \epsilon_j\rangle \\
&= 1.
\end{aligned}$$

□

**Lemma 3.5.** *For all $i < j$ and for all $t' \in T'$ one has*

$$\langle \alpha_{i+j}(t')\rangle = \langle t_4 \alpha'_{i+j}(t')\rangle.$$

*Proof.* We check

$$\begin{aligned}
\frac{1}{2}\langle \alpha_3 - \alpha_1, \alpha_{i+j}\rangle + \frac{1}{2}\langle \alpha_3 - \alpha_1, \alpha'_{i+j}\rangle &= \frac{1}{2}\langle \alpha_3 - \alpha_1, \overline{\epsilon}\rangle \\
&= \frac{1}{2}\langle -\epsilon_1 + \epsilon_2 + \epsilon_3 - \epsilon_4, \epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4\rangle \\
&= 0, \\
\frac{1}{2}\langle \alpha_4 - \alpha_1, \alpha_{i+j}\rangle + \frac{1}{2}\langle \alpha_4 - \alpha_1, \alpha'_{i+j}\rangle &= \frac{1}{2}\langle \alpha_4 - \alpha_1, \overline{\epsilon}\rangle \\
&= \frac{1}{2}\langle -\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4, \epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4\rangle \\
&= 1.
\end{aligned}$$

□

**Proposition 3.6.** *For adjoint groups of type $D_4$ we have*

$$\mathcal{K}'_{d,t'} = \langle\langle d, t'_1, t'_2, t'_3, t'_4\rangle\rangle + \langle\langle d, t'_3, t'_4\rangle\rangle.$$

*Proof.* The above two lemmas show

$$\begin{aligned}
\mathcal{K}'_{d,t'} &= \langle\langle d, t'_3 t'_4, t'_4\rangle\rangle \otimes \langle \alpha_{1-2}(t'), \alpha_{1-3}(t'), \alpha_{1-4}(t')\rangle \\
&= \langle\langle d, t'_3, t'_4\rangle\rangle \otimes \langle \alpha_{1-2}(t'), \alpha_{1-3}(t'), \alpha_{1-4}(t')\rangle.
\end{aligned}$$

One then computes the remaining roots to arrive at the result. We have

$$\langle \alpha_{1-2}(t'), \alpha_{1-3}(t'), \alpha_{1-4}(t') \rangle = \langle t'_2 t'_4, t'_1 t'_2 t'_3 t'_4, t'_1 t'_4 \rangle$$

and so

$$\begin{aligned}\mathcal{K}'_{d,t'} &= \langle\langle d, t'_3, t'_4 \rangle\rangle \otimes \langle t'_2 t'_4, t'_1 t'_2 t'_3 t'_4, t'_1 t'_4 \rangle \\ &= \langle\langle d, t'_3, t'_4 \rangle\rangle \otimes \langle t'_1, t'_2, t'_1 t'_2 \rangle \\ &= \langle\langle d, t'_3, t'_4 \rangle\rangle \otimes [\langle\langle t'_1, t'_2 \rangle\rangle + \langle 1 \rangle].\end{aligned}$$

$\square$

# 4 Non-Simply Connected Groups of Type $D_8$

Now let us pass to the half-spin group $G'$ of type $D_8$. Let $T' \subset G'$ be a maximal $k$-split torus. Let $T$ be its preimage under simply connected covering $G \to G'$. We can parametrize $k$-points of $T'$ in a similar fashion, letting

$$t := \check{\alpha}_1(t_1)\check{\alpha}_2(t_2)\check{\alpha}_3(t_3)\check{\alpha}_4(t_4)\check{\alpha}_5(t_5)\check{\alpha}_6(t_6)\check{\alpha}_7(t_7)\check{\alpha}_8(t_8) \in T$$

and choosing instead the maps $\sigma, \tau : T \to T$ given by

$$\begin{aligned}\sigma &: t \mapsto \check{\alpha}_1(t_1 t_8)\check{\alpha}_2(t_2)\check{\alpha}_3(t_3 t_8)\check{\alpha}_4(t_4)\check{\alpha}_5(t_5 t_8)\check{\alpha}_6(t_6)\check{\alpha}_7(t_7)\check{\alpha}_8(t_8) \\ \tau &: t \mapsto \check{\alpha}_1(t_1)\check{\alpha}_2(t_2)\check{\alpha}_3(t_3)\check{\alpha}_4(t_4)\check{\alpha}_5(t_5)\check{\alpha}_6(t_6)\check{\alpha}_7(t_7)\check{\alpha}_8(t_8^2).\end{aligned}$$

One finds that for a $k$-point $t' \in T'(k)$ its preimage $t$ in $T$ is of the form

$$t = \check{\alpha}_1\left(\frac{t'_1}{\sqrt{t'_8}}\right)\check{\alpha}_2(t'_2)\,\check{\alpha}_3\left(\frac{t'_3}{\sqrt{t'_8}}\right)\check{\alpha}_4(t'_4)\,\check{\alpha}_5\left(\frac{t'_5}{\sqrt{t'_8}}\right)\check{\alpha}_6(t_6)\,\check{\alpha}_7(t_7)\check{\alpha}_8\left(\sqrt{t'_8}\right) \tag{VI.1}$$

and for a root $\alpha$

$$\begin{aligned}\alpha(t') = &\left(\frac{t'_1}{\sqrt{t'_8}}\right)^{\langle\alpha_1,\alpha\rangle}(t'_2)^{\langle\alpha_2,\alpha\rangle}\left(\frac{t'_3}{\sqrt{t'_8}}\right)^{\langle\alpha_3,\alpha\rangle}(t'_4)^{\langle\alpha_4,\alpha\rangle}\left(\frac{t'_5}{\sqrt{t'_8}}\right)^{\langle\alpha_5,\alpha\rangle}(t'_6)^{\langle\alpha_6,\alpha\rangle}(t'_7)^{\langle\alpha_7,\alpha\rangle}\sqrt{t'_8}^{\langle\alpha_8,\alpha\rangle} \\ &= (t'_1)^{\langle\alpha_1,\alpha\rangle}(t'_2)^{\langle\alpha_2,\alpha\rangle}(t'_3)^{\langle\alpha_3,\alpha\rangle}(t'_4)^{\langle\alpha_4,\alpha\rangle}(t'_5)^{\langle\alpha_5,\alpha\rangle}(t'_6)^{\langle\alpha_6,\alpha\rangle}(t'_7)^{\langle\alpha_7,\alpha\rangle}(t'_8)^{\frac{1}{2}\langle\alpha_8-\alpha_1-\alpha_3-\alpha_5,\alpha\rangle}.\end{aligned}$$

To ease notation we will write below $t_i$ instead of parameters $t'_i$.

**Lemma 4.1.** *For all $i < j$, the following 1-dimensional quadratic forms are isomorphic:*

$$\langle \alpha_{i+j}(t) \rangle = \langle t_8 \alpha_{i-j}(t) \rangle.$$

*Proof.* By the methods of Proposition 1.1 the factors of $t_1$ through $t_7$ on the left and on the right are the same modulo squares. One checks

$$\begin{aligned}
&\frac{1}{2}\langle \alpha_8 - \alpha_1 - \alpha_3 - \alpha_5, \alpha_{i+j} \rangle - \frac{1}{2}\langle \alpha_8 - \alpha_1 - \alpha_3 - \alpha_5, \alpha_{i-j} \rangle \\
&= \frac{1}{2}\langle \alpha_8 - \alpha_1 - \alpha_3 - \alpha_5, 2\epsilon_j \rangle \\
&= \langle -\epsilon_1 + \epsilon_2 - \epsilon_3 + \epsilon_4 - \epsilon_5 + \epsilon_6 + \epsilon_7 + \epsilon_8, \epsilon_j \rangle \\
&= \pm 1.
\end{aligned}$$

□

**Corollary 4.2.** *For half-spin groups of type $D_8$ one has*

$$\mathcal{K}'_{d,t} = \langle\langle d, t_8 \rangle\rangle \otimes \bigoplus_{i<j} \langle \alpha_{i-j}(t) \rangle.$$

Let us break the part $\bigoplus_{i<j} \langle \alpha_{i-j}(t) \rangle$ into subforms. Note that the factor of $t_8$ on the left means that we can choose to ignore any factors of $t_8$ appearing in $\alpha_{i-j}(t)$ without changing the end result. As such we will consider $t_8 = 1$ in these computations. Similarly we may freely replace any root $\alpha_{i+j}$ with the corresponding root $\alpha_{i-j}$. Let

$$\mathcal{K}_l = \bigoplus_{i<j\leq 4} \langle \alpha_{i+j}(t) \rangle, \qquad \mathcal{K}_r = \bigoplus_{5\leq i<j} \langle \alpha_{i+j}(t) \rangle, \qquad \mathcal{K}_m = \bigoplus_{i\leq 4, 5\leq j} \langle \alpha_{i-j}(t) \rangle$$

so that

$$\bigoplus_{i<j} \langle \alpha_{i-j} \rangle = \mathcal{K}_l \oplus \mathcal{K}_r \oplus \mathcal{K}_m.$$

**Lemma 4.3.** *The quadratic form $\mathcal{K}_l$ defined above is of the form*

$$\mathcal{K}_l = \langle\langle t_2, t_1 t_3, t_4 \rangle\rangle - \langle\langle t_4 \rangle\rangle.$$

*Proof.* Let $\overline{\epsilon} := \epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4$ and $\alpha'_{i+j} = \overline{\epsilon} - \alpha_{i+j}$ as before. For all $i < j \leq 4$ one has

$$\langle \alpha'_{i+j}(t) \rangle = \langle t_4 \alpha_{i+j}(t) \rangle.$$

Indeed, one checks as in previous examples that the factors of $t_1, t_2$, and $t_3$ on the left and on the right are the same modulo squares. We may ignore factors of $t_8$ as stated, and no factors $t_5, t_6$ or $t_7$ appear. For $t_4$ one has

$$\begin{aligned} \langle \alpha_4, \alpha_{i+j} \rangle + \langle \alpha_4, \alpha'_{i+j} \rangle &= \langle \alpha_4, \overline{\epsilon} \rangle \\ &= \langle \epsilon_4 - \epsilon_5, \epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 \rangle \\ &= 1. \end{aligned}$$

Therefore

$$\mathcal{K}_l = \langle\langle t_4 \rangle\rangle \otimes \langle \alpha_{1+2}(t), \alpha_{1+3}(t), \alpha_{1+4}(t) \rangle.$$

We compute $\alpha(t)$ directly for each remaining root:

$$\alpha_{1+2}(t) = t_2, \qquad \alpha_{1+3}(t) = t_1 t_2 t_3, \qquad \alpha_{1+4}(t) = t_1 t_3 t_4.$$

Replacing, we have

$$\begin{aligned} \mathcal{K}_l &= \langle\langle t_4 \rangle\rangle \otimes \langle t_2, t_1 t_2 t_3, t_1 t_3 t_4 \rangle \\ &= \langle\langle t_4 \rangle\rangle \otimes \langle t_2, t_1 t_2 t_3, t_1 t_3 \rangle \\ &= \langle\langle t_4 \rangle\rangle \otimes (\langle\langle t_2, t_1 t_3 \rangle\rangle - \langle 1 \rangle) \\ &= \langle\langle t_2, t_1 t_3, t_4 \rangle\rangle - \langle\langle t_4 \rangle\rangle. \end{aligned}$$

□

**Lemma 4.4.** *The quadratic form $\mathcal{K}_r$ defined above is of the form*

$$\mathcal{K}_r = \langle\langle t_6, t_5 t_7, t_4 \rangle\rangle - \langle\langle t_4 \rangle\rangle.$$

*Proof.* After choosing $\overline{\epsilon} := \epsilon_5 + \epsilon_6 + \epsilon_7 + \epsilon_8$ and dropping all factors of $t_8$ which appear, the proof follows in exactly the same fashion as the previous lemma. □

**Lemma 4.5.** *The quadratic form $K_m$ defined above is of the form*

$$\mathcal{K}_m = \langle t_3 t_5 \rangle \otimes [\langle\langle t_2, t_6, t_1 t_3, t_5 t_7 \rangle\rangle \oplus \langle\langle t_2, t_4, t_1 t_3 \rangle\rangle \oplus \langle\langle t_4, t_6, t_5 t_7 \rangle\rangle].$$

*Proof.* We begin by noting that $\mathcal{K}_m$ consists of precisely roots of the form $\alpha_{i-j}$ where $i \leq 4$ and $j \geq 5$, which may be rewritten

$$\begin{aligned} \alpha_{i-j} &= \alpha_i + \cdots + \alpha_{j-1} \\ &= (\alpha_i + \cdots + \alpha_3) + (\alpha_4 + \cdots + \alpha_{j-1}) \\ &= \alpha_{i-4} + \alpha_{4-j} \end{aligned}$$

(note that $i$ may equal 4 in which case we consider $\alpha_{4-4} = 0$). We then have

$$\alpha_{i-j}(t) = \alpha_{i-4}(t)\alpha_{4-j}(t)$$

and this implies

$$\mathcal{K}_m = \langle \alpha_{1-4}(t), \alpha_{2-4}(t), \alpha_{3-4}(t), \alpha_{4-4}(t) \rangle \otimes \langle \alpha_{4-5}(t), \alpha_{4-6}(t), \alpha_{4-7}(t), \alpha_{4-8}(t) \rangle.$$

We compute (modulo squares)

$$\begin{array}{cccc} \alpha_{1-4}(t) = t_1t_3t_4 & \alpha_{2-4}(t) = t_1t_2t_3t_4 & \alpha_{3-4}(t) = t_2t_4 & \alpha_{4-4}(t) = 1 \\ \alpha_{4-5}(t) = t_3t_5 & \alpha_{4-6}(t) = t_3t_4t_5t_6 & \alpha_{4-7}(t) = t_3t_4t_6t_7 & \alpha_{4-8}(t) = t_3t_4t_7 \end{array}$$

and then we may rewrite

$$\begin{aligned} \mathcal{K}_m &= \langle \alpha_{1-4}(t), \alpha_{2-4}(t), \alpha_{3-4}(t), \alpha_{4-4}(t) \rangle \otimes \langle \alpha_{4-5}(t), \alpha_{4-6}(t), \alpha_{4-7}(t), \alpha_{4-8}(t) \rangle \\ &= \langle t_1t_3t_4, t_1t_2t_3t_4, t_2t_4, 1 \rangle \otimes \langle t_3t_5, t_3t_4t_5t_6, t_3t_4t_6t_7, t_3t_4t_7 \rangle. \end{aligned}$$

One checks

$$\begin{aligned} \langle t_1t_3t_4, t_1t_2t_3t_4, t_2t_4, 1 \rangle &= \langle\langle t_2, t_4, t_1t_3 \rangle\rangle \oplus \langle\langle t_2, t_1t_3 \rangle\rangle \oplus \langle\langle t_4 \rangle\rangle \\ \langle t_3t_5, t_3t_4t_5t_6, t_3t_4t_6t_7, t_3t_4t_7 \rangle &= \langle t_3t_5 \rangle \otimes [\langle\langle t_4, t_6, t_5t_7 \rangle\rangle \oplus \langle\langle t_6, t_5t_7 \rangle\rangle \oplus \langle\langle t_4 \rangle\rangle] \end{aligned}$$

and

$$\begin{aligned} &\langle t_3t_5 \rangle \otimes [\langle\langle t_2, t_4, t_1t_3 \rangle\rangle \oplus \langle\langle t_2, t_1t_3 \rangle\rangle \oplus \langle\langle t_4 \rangle\rangle] \otimes [\langle\langle t_4, t_6, t_5t_7 \rangle\rangle \oplus \langle\langle t_6, t_5t_7 \rangle\rangle \oplus \langle\langle t_4 \rangle\rangle] \\ &\qquad = \langle t_3t_5 \rangle \otimes [\langle\langle t_2, t_6, t_1t_3, t_5t_7 \rangle\rangle \oplus \langle\langle t_2, t_4, t_1t_3 \rangle\rangle \oplus \langle\langle t_4, t_6, t_5t_7 \rangle\rangle]. \end{aligned}$$

□

**Proposition 4.6.** *For the half-spin group of type $D_8$, one has*

$$\mathcal{K}'_{d,t} = \langle\langle d, t_8\rangle\rangle \otimes [\langle\langle t_2, t_6, t_1t_3, t_3t_5, t_5t_7\rangle\rangle \oplus \langle\langle t_2, t_6, t_1t_3, t_5t_7\rangle\rangle \oplus \langle\langle t_2, t_4, t_1t_3, t_3t_5\rangle\rangle \oplus \langle\langle t_4, t_6, t_3t_5, t_5t_7\rangle\rangle].$$

*Proof.* Now that we have computed each of the summands we have

$$\mathcal{K}_l \oplus \mathcal{K}_r \oplus \mathcal{K}_m = \langle\langle t_2, t_6, t_1t_3, t_3t_5, t_5t_7\rangle\rangle \oplus \langle\langle t_2, t_6, t_1t_3, t_5t_7\rangle\rangle \oplus \langle\langle t_2, t_4, t_1t_3, t_3t_5\rangle\rangle \oplus \langle\langle t_4, t_6, t_3t_5, t_5t_7\rangle\rangle.$$

We then replace the values in Corollary 4.2. □

# 5 Groups of Type $E_8$

In this section we consider a simply connected group $G$ of type $E_8$ over a ground field $k$, twisted by a cocycle $\varphi$ which is split over some quadratic extension $\ell/k = k(\sqrt{d})$.

We use the realization of a root system of type $E_8$ given by Bourbaki in [3] as follows: let $\epsilon_1, ..., \epsilon_8$ be the standard basis for $\mathbb{R}^8$ and let

$$\Sigma := \{\pm\epsilon_i \pm \epsilon_j \mid i < j\} \cup \{\frac{1}{2}\sum_{i=1}^{8}(-1)^{v_i}\epsilon_i\}$$

where $v$ is an element of $(\mathbb{Z}/2\mathbb{Z})^8$ and $v_i$ denotes the $i^{th}$ component of $v$, such that $\sum_{i=1}^{8} v_i = 0$.

Let $S$ be the system of simple roots consisting of

$$\alpha_1 := \frac{1}{2}\left(\epsilon_1 - \sum_{i=2}^{6}\epsilon_i + \epsilon_8\right), \qquad \alpha_2 := \epsilon_2 + \epsilon_1, \qquad \alpha_i := \epsilon_{i-1} - \epsilon_{i-2}, \quad i = 3, ..., 8.$$

Then $\Sigma_S^+$ is comprised of the roots of the following forms:

$$\epsilon_i \pm \epsilon_j, \quad i > j, \qquad\qquad \frac{1}{2}\left(\epsilon_8 + \sum_{i=1}^{7}(-1)^{u_i}\epsilon_i\right) \tag{VI.2}$$

where $u$ is an element of $(\mathbb{Z}/2\mathbb{Z})^7$ such that $\sum_{i=1}^{7} u_i = 0$.

The root $\tilde{\alpha} = \epsilon_7 + \epsilon_8$ is the **longest root**. One has

$$\tilde{\alpha} = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 5\alpha_5 + 4\alpha_6 + 3\alpha_7 + 2\alpha_8.$$

**Proposition 5.1.** *The subset of roots of the form*

$$\epsilon_i \pm \epsilon_j, \quad i > j$$

*in $\Sigma$ form a subsystem of type $D_8$ with base*

$$\begin{array}{cccc} \beta_1 := -\tilde{\alpha}, & \beta_2 := \alpha_8, & \beta_3 := \alpha_7, & \beta_4 := \alpha_6, \\ \beta_5 := \alpha_5, & \beta_6 := \alpha_4, & \beta_7 := \alpha_3, & \beta_8 := \alpha_2. \end{array}$$

*Proof.* This follows immediately from the extended Dynkin diagram of type $E_8$. □

Consider the normalized Killing form of $G$

$$\mathcal{K}'_{d,t} = \langle\langle d \rangle\rangle \otimes \bigoplus_{\alpha \in \Sigma_S^+} \langle \alpha(t) \rangle$$

where, as usual,

$$t := \check{\alpha}_1(t_1)\check{\alpha}_2(t_2)\check{\alpha}_3(t_3)\check{\alpha}_4(t_4)\check{\alpha}_5(t_5)\check{\alpha}_6(t_6)\check{\alpha}_7(t_7)\check{\alpha}_8(t_8) \in T.$$

Let $f$ be the subform of $\bigoplus_{\alpha \in \Sigma_S^+} \langle \alpha(t) \rangle$ corresponding to the roots in the subsystem of Proposition 5.1. Let $\Sigma'$ be the set of remaining positive roots

$$\Sigma' = \frac{1}{2}\left(\epsilon_8 + \sum_{i=1}^{7} (-1)^{u_i} \epsilon_i\right), \quad \sum_{i=1}^{7} u_i = 0$$

and let $g$ be the subform of $\bigoplus_{\alpha \in \Sigma_S^+}$ corresponding to roots in $\Sigma'$. Then

$$\mathcal{K}'_{d,t} = \langle\langle d \rangle\rangle \otimes (f \oplus g).$$

**Corollary 5.2.**

$$f = \langle\langle t_1\rangle\rangle \otimes [\langle\langle t_4, t_7, t_8, t_5t_7, t_2t_3t_5\rangle\rangle + \langle\langle t_4, t_7, t_8, t_2t_3t_5\rangle\rangle + \langle\langle t_6, t_7, t_8, t_5t_7\rangle\rangle + \langle\langle t_4, t_6, t_5t_7, t_2t_3t_5\rangle\rangle].$$

*Proof.* Our computation of the quadratic form $f$ will be based on the formula in Proposition 4.6. To apply this formula we have first to write the element

$$t := \check{\alpha}_1(t_1)\check{\alpha}_2(t_2)\check{\alpha}_3(t_3)\check{\alpha}_4(t_4)\check{\alpha}_5(t_5)\check{\alpha}_6(t_6)\check{\alpha}_7(t_7)\check{\alpha}_8(t_8) \in T, \tag{VI.3}$$

which arises in the cocycle $\phi$, in the form (modulo squares)

$$t = \check{\beta}_1\left(\frac{u_1}{\sqrt{u_8}}\right)\check{\beta}_2(u_2)\check{\beta}_3\left(\frac{u_3}{\sqrt{u_8}}\right)\check{\beta}_4(u_4)\check{\beta}_5\left(\frac{u_5}{\sqrt{u_8}}\right)\check{\beta}_6(u_6)\check{\beta}_7(u_7)\check{\beta}_8(\sqrt{u_8})$$

(see formula (VI.1)) where $u_1, \ldots, u_8$ are rational functions in $t_1, \ldots, t_8$ and then substitute $u_1, \ldots, u_8$ instead of $t_1, \ldots, t_8$ in the formula of Proposition 4.6.

Note that check operation $\check{\alpha}$ is linear with respect to $\alpha$ because all roots in $E_8$ have the same length. Then since

$$\begin{aligned}\alpha_1 &= \frac{1}{2}(\tilde{\alpha} - 3\alpha_2 - 4\alpha_3 - 6\alpha_4 - 5\alpha_5 - 4\alpha_6 - 3\alpha_7 - 2\alpha_8)\\ &= \frac{1}{2}(-\beta_1 - 3\beta_8 - 4\beta_7 - 6\beta_6 - 5\beta_5 - 4\beta_4 - 3\beta_3 - 2\beta_2).\end{aligned}$$

we conclude that modulo squares one has

$$\check{\alpha}_1(t_1) = \check{\beta}_1\left(\frac{1}{\sqrt{t_1}}\right)\check{\beta}_2\left(\frac{1}{t_1}\right)\check{\beta}_3\left(\frac{1}{t_1\sqrt{t_1}}\right)\check{\beta}_5\left(\frac{1}{\sqrt{t_1}}\right)\check{\beta}_6\left(\frac{1}{t_1}\right)\check{\beta}_8\left(\frac{1}{t_1\sqrt{t_1}}\right)$$

and therefore substituting this expression in (VI.3) one gets

$$t = \check{\beta}_1\left(\frac{1}{\sqrt{t_1}}\right)\check{\beta}_2\left(\frac{t_8}{t_1}\right)\check{\beta}_3\left(\frac{t_7}{t_1\sqrt{t_1}}\right)\check{\beta}_4(t_6)\check{\beta}_5\left(\frac{t_5}{\sqrt{t_1}}\right)\check{\beta}_6\left(\frac{t_4}{t_1}\right)\check{\beta}_7(t_3)\check{\beta}_8\left(\frac{t_2}{t_1\sqrt{t_1}}\right).$$

Thus, modulo squares we have

$$u_1 = t_2, \quad u_2 = t_1t_8, \quad u_3 = t_1t_2t_7, \quad u_4 = t_6, \quad u_5 = t_2t_5, \quad u_6 = t_1t_4, \quad u_7 = t_3, \quad u_8 = t_1.$$

Lastly,

$$\langle\langle u_2, u_6, u_1u_3, u_3u_5, u_5u_7\rangle\rangle = \langle\langle t_1t_8, t_1t_4, t_1t_7, t_1t_5t_7, t_2t_3t_5\rangle\rangle,$$

$$\langle\langle u_2, u_6, u_1u_3, u_5u_7\rangle\rangle = \langle\langle t_1t_8, t_1t_4, t_1t_7, t_2t_3t_5\rangle\rangle,$$

$$\langle\langle u_2, u_4, u_1u_3, u_3u_5\rangle\rangle = \langle\langle t_1t_8, t_6, t_1t_7, t_1t_5t_7\rangle\rangle,$$

$$\langle\langle u_4, u_6, u_3u_5, u_5u_7\rangle\rangle = \langle\langle t_6, t_1t_4, t_1t_5t_7, t_2t_3t_5\rangle\rangle.$$

Since $u_8 = t_1$ the result follows. □

Now let us compute the form $g$. A table showing the roots in $\Sigma'$ in various forms and giving a diagonalization of $g$ may be found in the Appendix.

A straightforward, albeit lengthy foiling process shows that the form $g$ may be rewritten as

$$\langle t_3, t_1t_3t_8, t_1t_3t_7, t_1t_3t_7t_8, t_3t_6, t_1t_3t_6t_8, t_1t_3t_6t_7, t_1t_3t_6t_7t_8\rangle \\ \otimes \langle 1, t_1t_4, t_1t_2t_3, t_1t_2t_3t_4, t_5, t_1t_4t_5, t_1t_2t_3t_5, t_1t_2t_3t_4t_5\rangle.$$

One then checks

$$\begin{aligned}\langle t_3, t_1t_3t_8, t_1t_3t_7, t_1t_3t_7t_8, t_3t_6, t_1t_3t_6t_8, t_1t_3t_6t_7, t_1t_3t_6t_7t_8\rangle \\ &= \langle t_3\rangle \otimes \langle\langle t_6\rangle\rangle \otimes \langle 1, t_1t_8, t_1t_7, t_1t_7t_8\rangle \\ &= \langle t_3\rangle \otimes \langle\langle t_6\rangle\rangle \otimes (\langle\langle t_1, t_7, t_8\rangle\rangle \oplus \langle\langle t_7, t_8\rangle\rangle \oplus \langle\langle t_1\rangle\rangle),\end{aligned}$$

and

$$\begin{aligned}\langle 1, t_1t_4, t_1t_2t_3, t_1t_2t_3t_4, t_5, t_1t_4t_5, t_1t_2t_3t_5, t_1t_2t_3t_4t_5\rangle \\ &= \langle\langle t_5\rangle\rangle \otimes \langle 1, t_1t_4, t_1t_2t_3, t_1t_2t_3t_4\rangle \\ &= \langle\langle t_5\rangle\rangle \otimes (\langle\langle t_1, t_2t_3, t_4\rangle\rangle \oplus \langle\langle t_2t_3, t_4\rangle\rangle \oplus \langle\langle t_1\rangle\rangle),\end{aligned}$$

and so altogether

$$g = \langle t_3\rangle \otimes \langle\langle t_5, t_6\rangle\rangle \otimes (\langle\langle t_1, t_7, t_8\rangle\rangle \oplus \langle\langle t_7, t_8\rangle\rangle \oplus \langle\langle t_1\rangle\rangle) \otimes (\langle\langle t_1, t_2t_3, t_4\rangle\rangle \oplus \langle\langle t_2t_3, t_4\rangle\rangle \\ \oplus \langle\langle t_1\rangle\rangle).$$

After foiling the last product and cancelation of hyperbolic spaces, this becomes

$$g = \langle t_3\rangle \otimes \langle\langle t_5, t_6\rangle\rangle \otimes (\langle\langle t_1, t_2t_3, t_4\rangle\rangle \oplus \langle\langle t_1, t_7, t_8\rangle\rangle \oplus \langle\langle t_2t_3, t_4, t_7, t_8\rangle\rangle). \tag{VI.4}$$

We see that $g$, like $f$, lies in the ideal $I^5$ and so $\mathcal{K}'_{d,t} = \langle\langle d\rangle\rangle \otimes (f \oplus g)$ lies in $I^6$.

**Proposition 5.3.** *The quadratic form $f \oplus g$ is represented in $I^5/I^6$ by a Pfister form $\langle\langle t_1, t_4, t_7, t_6t_8, t_2t_3t_5\rangle\rangle$.*

*Proof.* By Corollary 5.2 the image of $f$ in $I^5/I^6$ is represented by the sum of three Pfister forms

$$f_1 = \langle\langle t_1, t_4, t_7, t_8, t_2t_3t_5\rangle\rangle, \quad f_2 = \langle\langle t_1, t_6, t_7, t_8, t_5t_7\rangle\rangle = \langle\langle t_1, t_5, t_6, t_7, t_8\rangle\rangle \text{ and}$$

$$f_3 = \langle\langle t_1, t_4, t_6, t_5t_7, t_2t_3t_5\rangle\rangle.$$

Also, by (VI.4), the image of $g$ in $I^5/I^6$ is represented by the sum of $f_2$ and

$$g_2 = \langle\langle t_1, t_4, t_5, t_6, t_2t_3\rangle\rangle = \langle\langle t_1, t_4, t_5, t_6, t_2t_3t_5\rangle\rangle.$$

Lastly, $f_3 \oplus g_2$ modulo $I^6$ is represented by

$$\langle\langle t_1, t_4, t_6, t_7, t_2t_3t_5\rangle\rangle$$

and therefore $f \oplus g$ modulo $I^6$ is represented by

$$\langle\langle t_1, t_4, t_7, t_8, t_2t_3t_5\rangle\rangle + \langle\langle t_1, t_4, t_6, t_7, t_2t_3t_5\rangle\rangle = \langle\langle t_1, t_4, t_7, t_6t_8, t_2t_3t_5\rangle\rangle$$

as required. □

Thus we proved the following.

**Theorem 5.4.** *Let $H^1_{quad}(-, E_8)$ be a subfunctor of $H^1(-, E_8)$ consisting of $E_8$-torsors splitting over quadratic extensions. There exists a nontrivial cohomological invariant*

$$H^1_{quad}(-, E_8) \to H^6(-, \mathbb{Z}/2)$$

*given by*

$$(d, t) \to (d) \cup (t_1) \cup (t_4) \cup (t_7) \cup (t_6t_8) \cup (t_2t_3t_3).$$

# Bibliography

[1] Arason, J.K. and R. Elman, *Powers of the Fundamental Ideal in the Witt Ring,* Journal of Algebra vol. 239, Issue 1.
Academic Press, 2001.

[2] Arason, J.K. and A. Pfister, *Beweis des Krullschen Durchschnittsatzes für den Wittring,* Invent. Math. vol. 12.
Springer, 1971.

[3] Bourbaki, N., *Lie Groups and Lie Algebras Chapters 4-6.*
Springer, Heidelberg, 2002.

[4] Borel, A., *Linear Algebraic Groups.*
Springer, New York, 1991.

[5] Bruner, Robert R., Michael Catanzaro, and J. Peter May, *Characteristic Classes.*
University of Chicago.

[6] Cassels, J.W.S., and A. Frölich, *Algebraic Number Theory.*
Academic Press, London, 1967.

[7] Demazure, M., and A. Grothendieck, *Schemas en Groupes Reductifs,* SGA 3 vol. III, Lecture Notes in Mathematics, vol. 153.
Springer, Berlin, 1970.

[8] Elman, R., N. Karpenko, and A. Merkurjev *The Algebraic and Geometric Theory of Quadratic Forms.*
American Mathematical Society, Providence, 2008.

[9] Garibaldi, S., A. Merkujev, and J.P. Serre, *Cohomological Invariants in Galois Cohomology.*
American Mathematical Society, Providence, 2003.

[10] Gille, P., and T. Szamuely, *Central Simple Algebras and Galois Cohomology.* Cambridge University Press, Cambridge, 2006.

[11] Humphreys, James E., *Linear Algebraic Groups.* Springer, New York, 1981.

[12] Lam, T.Y., *Quadratic Forms over Fields.* American Mathematical Society, Providence, 2004.

[13] Lang, S., *Algebra.* Springer, New York, 2002.

[14] Merkurjev, A. *Degree three cohomological invariants of semisimple groups.* J. Eur. Math. Soc., 18 (2016), no. 2, 657-680.

[15] Malagon, A.L., *Killing Forms of Lie Algebras.* PhD Dissertation at Emory University, (2009).

[16] Serre, J.P., *Complex Semisimple Lie Algebras.* Springer, New York, 1987.

[17] Serre, J.P., *Galois Cohomology.* Springer, Berlin, 1997.

[18] Springer, T.A., *Linear Algebraic Groups.* Birkhäuser, Boston, 1981.

[19] Springer, T.A. and R. Steinberg, *Conjugacy Classes,* Lecture Notes in Mathematics **Vol. 131** 167-266. Springer, New York, 1970.

[20] Steinberg, R., *Lectures on Chevalley Groups.* 1967.

[21] Wikipedia contributors. ”Characteristic class.” Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 27 Aug. 2017. Web. 13 Nov. 2017.

[22] Wikipedia contributors. ”Coxeter Element.” Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 10 Nov. 2018. Web. 16 Feb. 2019.

# Appendix A

# Diagonalization of a Subform of the Killing Form for Twisted Lie Algebras of Type $E_8$

In this section, we present a table showing several presentations of each positive root in the set $\Sigma'$ described in the final section above, together with the coefficient of the Killing form corresponding to each. We will begin with some explanation of the information presented in said table, as well as how this information may be derived.

A priori, the positive roots in $\Sigma'$ are all vectors in $\mathbb{R}^8$ of the form

$$\frac{1}{2}\left(\epsilon_8 + \sum_{i=1}^{7}(-1)^{a_i}\epsilon_i\right)$$

where the $a_i$ are integers modulo 2 such that $\sum_{i=1}^{7} a_i = 0$. The clearest way to list exhaustively the positive roots in $\Sigma'$ is to identify them with the vector $a = (a_1, a_2, ..., a_7)$ in $(\mathbb{Z}/\mathbb{Z}_2)^7$. This is the information presented in the first column.

The second column gives the regular presentation of each root as a vector in the standard basis of $\mathbb{R}^8$. For example, the vector

$$a = (1, 1, 0, 0, 0, 0, 0)$$

in $(\mathbb{Z}/\mathbb{Z}_2)$ would be identified with the root

$$\frac{1}{2}(-\epsilon_1 - \epsilon_2 + \epsilon_3 + \epsilon_4 + \epsilon_5 + \epsilon_6 + \epsilon_7 + \epsilon_8) = \left(-\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right).$$

Next, we must convert this vector from the standard basis into the basis

$$\mathcal{B} = \{\alpha_1, \alpha_2, ..., \alpha_8\}$$

of simple roots defined in Section 5. This is done by simply multiplying each vector by the appropriate change of basis matrix $M$, for which we have used RStudio. The matrix itself is

$$M = \begin{bmatrix} \frac{1}{2} & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ -\frac{1}{2} & 1 & 1 & -1 & 0 & 0 & 0 & 0 \\ -\frac{1}{2} & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ -\frac{1}{2} & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ -\frac{1}{2} & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 5 \\ -1 & 1 & 1 & 1 & 1 & 1 & 1 & 7 \\ 0 & 0 & 2 & 2 & 2 & 2 & 2 & 10 \\ 0 & 0 & 0 & 2 & 2 & 2 & 2 & 8 \\ 0 & 0 & 0 & 0 & 2 & 2 & 2 & 6 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{bmatrix}.$$

Finally, each of these roots $\alpha$ correspond to a coefficient in the quadratic form $g$ discussed in Section 5. This coefficient, which is simply $\alpha(t)$ reduced modulo squares, is obtained from vector in the third column. The formula for this coefficient is given at the end of Chapter V, namely one has for a given root $\beta = b_1\alpha_1 + \cdots + b_8\alpha_8$

$$\beta(t) = \prod_{i=1}^{8} \alpha_i(t)^{b_i}.$$

In our case one has (modulo squares)

$$\begin{array}{rrrr} \alpha_1(t) = t_3 & \alpha_2(t) = t_4 & \alpha_3(t) = t_1t_4 & \alpha_4(t) = t_2t_3t_5 \\ \alpha_5(t) = t_4t_6 & \alpha_6(t) = t_5t_7 & \alpha_7(t) = t_6t_8 & \alpha_8(t) = t_7 \end{array}$$

and so $\beta(t)$ is given by the simple formula

$$\beta(t) = t_1^{b_3} t_2^{b_4} t_3^{b_1+b_4} t_4^{b_2+b_3+b_5} t_5^{b_4+b_6} t_6^{b_5+b_7} t_7^{b_6+b_8} t_8^{b_7}.$$

The final column of the table is then simply this monomial, reduced modulo squares.

| Tuple in $(\mathbb{Z}/2\mathbb{Z})^7$ | Vector in $\mathbb{R}^8$, Standard Basis | Vector in Basis $\mathcal{B}$ | Coefficient |
|---|---|---|---|
| $(0,1,1,1,1,1,1)$ | $(\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,0,0,0,0,0,0,0)$ | $t_3$ |
| $(1,0,0,0,0,0,1)$ | $(-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,2,3,4,3,2,1,0)$ | $t_1t_3t_8$ |
| $(0,1,1,1,1,0,0)$ | $(\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,1,2,2,2,2,1)$ | $t_1t_3t_7$ |
| $(1,0,0,0,0,1,0)$ | $(-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,3,4,3,2,1,1)$ | $t_1t_3t_7t_8$ |
| $(1,0,0,0,1,1,1)$ | $(-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,2,2,1,0,0,0)$ | $t_3t_6$ |
| $(0,1,1,1,0,0,1)$ | $(\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,1,2,2,2,1,0)$ | $t_1t_3t_6t_8$ |
| $(1,0,0,0,1,0,0)$ | $(-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,3,4,3,2,2,1)$ | $t_1t_3t_6t_7$ |
| $(0,1,1,1,0,1,0)$ | $(\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,1,2,2,2,1,1)$ | $t_1t_3t_6t_7t_8$ |
| $(0,1,1,0,0,0,0)$ | $(\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,2,4,4,3,2,1)$ | $t_3t_5$ |
| $(1,0,0,1,1,1,0)$ | $(-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,2,2,1,1,1,1)$ | $t_3t_5t_8$ |
| $(0,1,1,0,0,1,1)$ | $(\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,1,2,2,1,0,0)$ | $t_1t_3t_5t_7$ |
| $(1,0,0,1,1,0,1)$ | $(-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,2,2,1,1,1,0)$ | $t_3t_5t_7t_8$ |
| $(1,0,0,1,0,0,0)$ | $(-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,3,4,3,3,2,1)$ | $t_1t_3t_5t_6$ |
| $(0,1,1,0,1,1,0)$ | $(\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,1,2,2,1,1,1)$ | $t_1t_3t_5t_6t_8$ |
| $(1,0,0,1,0,1,1)$ | $(-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,2,2,1,1,0,0)$ | $t_3t_5t_6t_7$ |
| $(0,1,1,0,1,0,1)$ | $(\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,1,2,2,1,1,0)$ | $t_1t_3t_5t_6t_7t_8$ |
| $(1,0,1,1,1,1,1)$ | $(-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,0,1,0,0,0,0,0)$ | $t_1t_3t_4$ |
| $(0,1,0,0,0,0,1)$ | $(\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,2,2,4,3,2,1,0)$ | $t_3t_4t_8$ |
| $(1,0,1,1,1,0,0)$ | $(-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,2,2,2,2,2,1)$ | $t_3t_4t_7$ |
| $(0,1,0,0,0,1,0)$ | $(\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,2,4,3,2,1,1)$ | $t_3t_4t_7t_8$ |
| $(0,1,0,0,1,1,1)$ | $(\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,1,2,1,0,0,0)$ | $t_1t_3t_4t_6$ |
| $(1,0,1,1,0,0,1)$ | $(-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,2,2,2,2,1,0)$ | $t_3t_4t_6t_8$ |
| $(0,1,0,0,1,0,0)$ | $(\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,2,4,3,2,2,1)$ | $t_3t_4t_6t_7$ |
| $(1,0,1,1,0,1,0)$ | $(-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,2,2,2,2,1,1)$ | $t_3t_4t_6t_7t_8$ |
| $(1,0,1,0,0,0,0)$ | $(-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,3,4,4,3,2,1)$ | $t_1t_3t_4t_5$ |
| $(0,1,0,1,1,1,0)$ | $(\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,1,2,1,1,1,1)$ | $t_1t_3t_4t_5t_8$ |
| $(1,0,1,0,0,1,1)$ | $(-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,2,2,2,1,0,0)$ | $t_3t_4t_5t_7$ |
| $(0,1,0,1,1,0,1)$ | $(\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,1,2,1,1,1,0)$ | $t_1t_3t_4t_5t_7t_8$ |
| $(0,1,0,1,0,0,0)$ | $(\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,2,4,3,3,2,1)$ | $t_3t_4t_5t_6$ |

| Tuple in $(\mathbb{Z}/2\mathbb{Z})^7$ | Vector in $\mathbb{R}^8$, Standard Basis | Vector in Basis $\mathcal{B}$ | Coefficient |
|---|---|---|---|
| $(1,0,1,0,1,1,0)$ | $(-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,2,2,2,1,1,1)$ | $t_3t_4t_5t_6t_8$ |
| $(0,1,0,1,0,1,1)$ | $(\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,1,2,1,1,0,0)$ | $t_1t_3t_4t_5t_6t_7$ |
| $(1,0,1,0,1,0,1)$ | $(-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,2,2,2,1,1,0)$ | $t_3t_4t_5t_6t_7t_8$ |
| $(0,0,0,0,0,0,0)$ | $(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,3,3,5,4,3,2,1)$ | $t_1t_2$ |
| $(1,1,1,1,1,1,0)$ | $(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,0,1,1,1,1,1,1)$ | $t_1t_2t_8$ |
| $(0,0,0,0,0,1,1)$ | $(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,2,2,3,2,1,0,0)$ | $t_2t_7$ |
| $(1,1,1,1,1,0,1)$ | $(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,0,1,1,1,1,1,0)$ | $t_1t_2t_7t_8$ |
| $(1,1,1,1,0,0,0)$ | $(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,2,3,3,3,2,1)$ | $t_2t_6$ |
| $(0,0,0,0,1,1,0)$ | $(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,2,3,2,1,1,1)$ | $t_2t_6t_8$ |
| $(1,1,1,1,0,1,1)$ | $(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,0,1,1,1,1,0,0)$ | $t_1t_2t_6t_7$ |
| $(0,0,0,0,1,0,1)$ | $(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,2,2,3,2,1,1,0)$ | $t_2t_6t_7t_8$ |
| $(0,0,0,1,1,1,1)$ | $(\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,1,1,0,0,0,0)$ | $t_1t_2t_5$ |
| $(1,1,1,0,0,0,1)$ | $(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,2,3,3,2,1,0)$ | $t_2t_5t_8$ |
| $(0,0,0,1,1,0,0)$ | $(\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,2,3,2,2,2,1)$ | $t_2t_5t_7$ |
| $(1,1,1,0,0,1,0)$ | $(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,2,3,3,2,1,1)$ | $t_2t_5t_7t_8$ |
| $(1,1,1,0,1,1,1)$ | $(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,0,1,1,1,0,0,0)$ | $t_1t_2t_5t_6$ |
| $(0,0,0,1,0,0,1)$ | $(\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,2,2,3,2,2,1,0)$ | $t_2t_5t_6t_8$ |
| $(1,1,1,0,1,0,0)$ | $(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,2,3,3,2,2,1)$ | $t_2t_5t_6t_7$ |
| $(0,0,0,1,0,1,0)$ | $(\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,2,3,2,2,1,1)$ | $t_2t_5t_6t_7t_8$ |
| $(1,1,0,0,0,0,0)$ | $(-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,3,5,4,3,2,1)$ | $t_1t_2t_4$ |
| $(0,0,1,1,1,1,0)$ | $(\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,1,1,1,1,1,1)$ | $t_1t_2t_4t_8$ |
| $(1,1,0,0,0,1,1)$ | $(-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,2,3,2,1,0,0)$ | $t_2t_4t_7$ |
| $(0,0,1,1,1,0,1)$ | $(\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,1,1,1,1,1,0)$ | $t_1t_2t_4t_7t_8$ |
| $(0,0,1,1,0,0,0)$ | $(\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,2,3,3,3,2,1)$ | $t_2t_4t_6$ |
| $(1,1,0,0,1,1,0)$ | $(-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,2,3,2,1,1,1)$ | $t_2t_4t_6t_8$ |
| $(0,0,1,1,0,1,1)$ | $(\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,1,1,1,1,0,0)$ | $t_1t_2t_4t_6t_7$ |
| $(1,1,0,0,1,0,1)$ | $(-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,2,3,2,1,1,0)$ | $t_2t_4t_6t_7t_8$ |
| $(1,1,0,1,1,1,1)$ | $(-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,0,1,1,0,0,0,0)$ | $t_1t_2t_4t_5$ |
| $(0,0,1,0,0,0,1)$ | $(\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,2,2,3,3,2,1,0)$ | $t_2t_4t_5t_8$ |

| Tuple in $(\mathbb{Z}/2\mathbb{Z})^7$ | Vector in $\mathbb{R}^8$, Standard Basis | Vector in Basis $\mathcal{B}$ | Coefficient |
|---|---|---|---|
| $(1,1,0,1,1,0,0)$ | $(-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,2,3,2,2,2,1)$ | $t_2t_4t_5t_7$ |
| $(0,0,1,0,0,1,0)$ | $(\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,2,3,3,2,1,1)$ | $t_2t_4t_5t_7t_8$ |
| $(0,0,1,0,1,1,1)$ | $(\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,1,1,1,0,0,0)$ | $t_1t_2t_4t_5t_6$ |
| $(1,1,0,1,0,0,1)$ | $(-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2})$ | $(1,1,2,3,2,2,1,0)$ | $t_2t_4t_5t_6t_8$ |
| $(0,0,1,0,1,0,0)$ | $(\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,2,2,3,3,2,2,1)$ | $t_2t_4t_5t_6t_7$ |
| $(1,1,0,1,0,1,0)$ | $(-\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2},\frac{1}{2})$ | $(1,1,2,3,2,2,1,1)$ | $t_2t_4t_5t_6t_7t_8$ |