On the Second Stiefel-Whitney Class of Scaled Trace Forms of Central Simple Algebras.

Rosali Brusamarello

Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://repository.lsu.edu/gradschool_disstheses

Recommended Citation


This Dissertation is brought to you for free and open access by the Graduate School at LSU Scholarly Repository. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Scholarly Repository. For more information, please contact gradetd@lsu.edu.
INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6” x 9” black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI
A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700  800/521-0600

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
ON THE SECOND STIEFEL-WHITELEY CLASS OF
SCALED TRACE FORMS OF CENTRAL
SIMPLE ALGEBRAS

A Dissertation
Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy
in
The Department of Mathematics

by
Rosali Brusamarello
Lic.Math.. Universidade Federal do Mato Grosso do Sul-Brazil. 1988
M.S.. Universidade de Sao Paulo-Brazil. 1991
May 1998
Acknowledgments

This dissertation would not be possible without several contributions. The most important of them, without any doubt, was given by my advisor, Professor Jorge Morales. I am grateful for his advice, guidance and dedication. This work was motivated by a question brought to our attention by Professor David Lewis of University College Dublin. I would like to thank him for sharing his ideas with us and for his comments.

I thank all the people in the Department of Mathematics for providing me with a pleasant working environment. A special thanks to Gretchen Whipple for her friendship and for proof-reading this dissertation.

I am grateful for the financial support provided by CAPES - Brazil and Universidade Estadual de Maringá - Brazil.

I wish to extend a very special thank you to my family in Brazil, whose encouragement and support were strong enough to overcome the distance.

Finally, a heartfelt thank you to Eliezer, who gave me a lot of emotional support.
Table of Contents

Acknowledgments ...................................................................................................... ii

Abstract ....................................................................................................................... iv

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

1 Quadratic Forms and Central Simple Algebras .................................. 4
   1.1 Quadratic Forms .................................................................................. 4
   1.2 Central Simple Algebras ...................................................................... 15

2 Cohomology ............................................................................................................. 21
   2.1 Cohomology of Groups ......................................................................... 21
   2.2 Non-abelian Cohomology ....................................................................... 28
   2.3 Galois Cohomology ................................................................................ 31
   2.4 Galois Descent ..................................................................................... 35
   2.5 Springer’s spinor interpretation of the Hasse invariant ....................... 38

3 Representation of Linear Algebraic Groups ......................................... 41
   3.1 Basic Concepts and Examples ................................................................... 41
   3.2 Lie Algebra of an Algebraic Group ......................................................... 44
   3.3 Diagonalizable Groups and Algebraic Tori ........................................... 46
   3.4 Jordan-Chevalley Decomposition ............................................................ 47
   3.5 Reductive Groups .................................................................................. 47
   3.6 Representations ..................................................................................... 48
   3.7 Orthogonal Representations .................................................................... 52
   3.8 Rationality Properties ........................................................................... 57

4 The Second Stiefel-Whitney Class of Trace Forms ...................... 60
   4.1 Definition of the Stiefel-Whitney Classes ........................................... 60
   4.2 Serre’s Formula ..................................................................................... 62
   4.3 Trace Form of a Central Simple Algebra ............................................. 68

5 Scaled Trace Forms of Central Simple Algebras ................................. 71
   5.1 The case where $A$ is a split algebra ..................................................... 74
   5.2 The general case ................................................................................... 81

References .................................................................................................................... 87

Vita .................................................................................................................................. 89

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Abstract

In this work we compute the second Stiefel-Whitney class $w_2$ of the scaled trace form $Q_{A,a}(x) = \text{tr}_{A/k}(ax^2)$, where $A$ is a central simple algebra over a perfect field $k$ of characteristic different from two. $a \in A$ is a fixed element, and $\text{tr}_{A/k}$ is the reduced trace.

The first three chapters provide background material about quadratic forms, central simple algebras, group cohomology, and representations of linear algebraic groups.

The fourth chapter presents two known results about the second Stiefel-Whitney class of trace forms: Serre's formula for the case of étale algebras and Saltman's formula for the case of central simple algebras.

Our computation of $w_2(Q_{A,a})$ is done in Chapter 5. We start with the case where $A = M_n(k)$. We express $w_2(Q_{M_n(k),a})$ as a sum involving corestrictions of quaternion algebras over certain factors of $E \otimes_k E$, where $E$ is a commutative étale algebra over $k$ that depends on the semisimple part of $a$. When $A$ is an arbitrary central simple algebra we can find an isomorphism $\varphi : A \otimes_k k_s \to M_n(k_s)$ ($k_s$ is the separable closure of $k$) such that $\varphi(a) := b \in M_n(k)$. Using Galois cohomology and representation theory of reductive groups we show that

$$w_2(Q_{A,a}) = w_2(Q_{M_n(k),b}) + \frac{n(n-1)}{2}[A],$$

where $[A]$ is the class of $A$ in the Brauer group of $k$.
Introduction

Trace forms and their variants arise naturally in the study of finite-dimensional algebras such as commutative étale algebras, central simple algebras and Lie algebras. It is natural to ask for the associated Stiefel-Whitney classes.

In 1984 J.-P. Serre [24] expressed the second Stiefel-Whitney invariant of the trace form of a commutative étale algebra in terms of other cohomological invariants. His formula had important applications to embedding problems and to the inverse Galois problem [29]. Serre’s formula was generalized to all higher Stiefel-Whitney invariants by B. Kahn [8].

In the case of central simple algebras, D. Saltman (1987, unpublished as far as we know) and later Serre [25] described, using different methods, the second Stiefel-Whitney class of the form $\text{tr}(x^2)$, where $\text{tr}$ is the reduced trace. (See also Tignol [28] and Lewis-Morales [13].) More recently, A. Quéguiner [18, 19] computed this invariant for the form $\text{tr}(\sigma(x), x)$ of a central simple algebra equipped with an involution $\sigma$.

In this work we shall be interested in scaled trace forms of central simple algebras, that is, quadratic forms of the type $Q_{A,a}(x) = \text{tr}_{A/k}(ax^2)$, where $\text{tr}_{A/k}$ is the reduced trace of a central simple algebra $A$ over a perfect field $k$ of characteristic different from two and $a$ is a fixed element of $A$. The form $Q_{A,a}$ has been studied by David Lewis in [11], where he established its general properties and gave formulas for its signature and discriminant. The next question was naturally the computation of the Hasse invariant (second Stiefel-Whitney invariant), which was left as an open problem in [11]. Our results provide a full computation of the second Stiefel-Whitney invariant $w_2$ of $Q_{A,a}$. 
The results and basic concepts about quadratic forms and central simple algebras used throughout our work are presented in Chapter 1.

In Chapter 2 we review some aspects of cohomology of groups such as: non-abelian cohomology, Galois cohomology, and Galois descent. Springer’s spinor representation of the Hasse invariant [26. 4.7] is presented in the last section of Chapter 2, where we give a slightly different proof and a minor correction to his formula.

Chapter 3 deals with linear algebraic groups with emphasis on representation theory. The main result in this chapter is an explicit description, in terms of weights, of the obstruction to lift a rational orthogonal representation $G \to \text{SO}$ of a reductive algebraic group $G$ to a spinor representation $G \to \text{Spin}$ (Theorem 3.37).

We start Chapter 4 with Delzant’s definition of the Stiefel-Whitney classes of a quadratic form. Then we focus our attention on the second Stiefel-Whitney class of trace forms by presenting Serre’s formula in the case of étale algebras and Saltman’s formula in the case of central simple algebras.

The formula for the computation of the second Stiefel-Whitney class of scaled trace forms of central simple algebras is given in Chapter 5. We start by showing that we can reduce the problem to the case where the scaling factor $a \in \mathcal{A}$ is a semisimple element. Then we carry out the computations for the case when $\mathcal{A}$ is a split algebra. In (5.12) we express $w_2(Q_{M_a(k),a})$ as a sum involving corestrictions of quaternion algebras over certain factors of $E \otimes_k E$, where $E$ is a commutative étale algebra over $k$ which depends on the semisimple element $a$. Finally, we consider $\mathcal{A}$ an arbitrary central simple algebra. Using Galois cohomology and representation theory of reductive groups, we show that

$$w_2(Q_{A,a}) = w_2(Q_{M_a(k),b}) + \frac{n(n-1)}{2}[\mathcal{A}].$$
where \([A]\) is the class of \(A\) in the Brauer group of \(k\) and \(b \in M_n(k)\) is an element whose similarity class is canonically determined by \(a\) according to Lemma 1.49. The general form \(\text{la} (5.18)\) is obtained by combining this result with the expression for \(w_2(Q_{M_n(k),b})\).
Chapter 1
Quadratic Forms and Central Simple Algebras

In this chapter we introduce some basic concepts of quadratic forms and central simple algebras that will be useful throughout our work. Most of the results are presented without proof since they are standard and easily found in any basic book of quadratic forms. Two good references are [10] and [21].

1.1 Quadratic Forms
Orthogonal Decomposition

Let $k$ be a field of characteristic different from 2. The multiplicative group of nonzero elements of $k$ will be denoted by $\hat{k}$.

**Definition 1.1.** Consider $V$ a finite dimensional vector space over $k$. A **quadratic form** is a map $q : V \to k$ such that:

(i) $q(ax) = a^2 q(x)$ for all $a \in k, x \in V$;

(ii) $b_q(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y))$ is a bilinear form.

The pair $(V, q)$ is called a **quadratic space**. For simplicity sometimes we write just $q$ for $(V, q)$ and $b$ for $b_q$. A quadratic space $(V, q)$ is called **nondegenerate** (or regular) if $b_q(x, y) = 0$ for all $y \in V$ implies $x = 0$.

From now on, unless otherwise stated, our quadratic spaces are nondegenerate.

**Definition 1.2.** A vector $x \in V$ is said to be **isotropic** if $b(x, x) = 0$, and **anisotropic** otherwise. Two vectors $x, y \in V$ are said to be **orthogonal** if $b(x, y) = 0$.

Two subsets $U, W$ of $V$ are **orthogonal** if $b(x, y) = 0$ for all $x \in U$ and $y \in W$.

If $(V_1, q_1)$ and $(V_2, q_2)$ are quadratic spaces, then their **orthogonal sum** $(V, q)$ is defined by: $V = V_1 \oplus V_2$ and $q(x_1 \oplus x_2) = q_1(x_1) + q_2(x_2)$ for $x_1 \in V_1$ and $x_2 \in V_2$. 

4

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
We write \( q = q_1 \perp q_2 \). One can easily check that if \( x_1 \in V_1 \) and \( x_2 \in V_2 \) then they are orthogonal with respect to \( q \).

**Theorem 1.3.** [21. Chap 1. Theorem 3.5] *Every quadratic space \((V, q)\) is the orthogonal sum of one-dimensional subspaces. In other words, \( V \) has a basis of orthogonal vectors.*

**Notation** We denote the one-dimensional quadratic space \((kx, q)\) where \( q(x) = a \in k \) by \(< a >\). If \( a_1, \ldots, a_n \in k \), then \(< a_1 \perp \ldots \perp a_n >\) is denoted by \(< a_1, \ldots, a_n >\). From the previous theorem every quadratic space \((V, q)\) can be written in the form \( q = < a_1, \ldots, a_n >\) for some \( a_i \in k \). We refer to it as a *diagonalization* of \( q \). A quadratic form can have more than one diagonalization.

**Equivalences**

Two quadratic spaces \((V, q)\) and \((V', q')\) are *isometric* if there exists a linear isomorphism \( \varphi : V \to V' \) such that

\[
q'(\varphi(x), \varphi(y)) = b_q(x, y) \quad \text{for all } x, y \in V
\]

(equivalently, \( q'(\varphi(x)) = q(x) \)). We denote \((V, q) \simeq (V', q')\) or just \( q \simeq q' \). The relation \( \simeq \) is an equivalence relation on the set of quadratic spaces over \( k \). The isomorphism \( \varphi \) involved is called an *isometry* between the quadratic spaces.

Now we shall define another equivalence relation between two quadratic forms, \( q \) and \( q' \), of the same dimension. We say that \( q \) and \( q' \) are *simply-equivalent* if we can find diagonalizations \( q = < a_1, \ldots, a_n >\) and \( q' = < b_1, \ldots, b_n >\) and indices \( i, j \) such that \(< a_i, a_j > \simeq < b_i, b_j >\) and \( a_k = b_k \) for all \( k \neq i, j \). We say that \( q \) and \( q' \) are *chain-equivalent* if there is a sequence of quadratic forms of same dimension \( q_0, q_1, \ldots, q_m \) such that \( q = q_0 \), \( q_m = q' \), and \( q_i \) is simply-equivalent to \( q_{i+1} \) for \( i = 0, \ldots, m - 1 \). This is an equivalence relation, denoted by \( \simeq \), on the set of quadratic forms of a fixed dimension.
Clearly if $q_1 \approx q_2$ then $q_1 \simeq q_2$. The converse is also true and is a powerful tool in the study of quadratic forms.

**Theorem 1.4.** (Witt's Chain-Equivalence) [10, Chap 1, Theorem 5.2] If two quadratic forms are isometric then they are chain-equivalent.

**Orthogonal Groups**

Consider the set of all isometries $\varphi : (V, q) \rightarrow (V, q)$. This set forms a group with respect to composition, called the **orthogonal group** of $(V, q)$, denoted by $O(V, q)$. Later the notations $O(V)$ and $O(q)$ will also be used to represent $O(V, q)$.

A simple argument from linear algebra shows that if $\sigma \in O(V, q)$, then $\det \sigma = \pm 1$. The set

$$SO(V, q) = \{ \sigma \in O(V, q) : \det \sigma = 1 \}$$

is a subgroup of $O(V, q)$ and is called the **special orthogonal group** of $(V, q)$.

The following example of an isometry will be useful to describe all elements of $O(V, q)$.

**Example 1.5.** Let $x \in V$ be an anisotropic vector and define $\tau_x : V \rightarrow V$ by

$$\tau_x(y) = y - 2 \frac{b(x, y)}{b(x, x)} x.$$ 

This linear map, which can be shown to be an isometry, is called a **reflection** relative to the hyperplane $W = \{ y \in V : b(x, y) = 0 \}$.

The name reflection is suggested by the first of the following properties of $\tau_x$:

1. $\tau_x(x) = -x$ and $\tau_x|_W = \text{id}_W$.
2. $\det \tau_x = -1$.

The next theorem describes the group $O(V, q)$ in terms of reflections.
Theorem 1.6. (Cartan-Dieudonné)[10. Appendix Chap 1] Let \((V,q)\) be a quadratic space and \(\dim V = n\). Then each isometry \(\sigma \in O(V,q)\) is a product of at most \(n\) reflections.

Field Extensions

Let \(L\) be an extension of \(k\). If \((V,q)\) is a quadratic space over \(k\), we define \((V_L,q_L)\), a quadratic space over \(L\), as follows:

\[
V_L = V \otimes_k L \quad \text{and} \quad b_{q_L}(x \otimes \alpha, y \otimes \beta) = \alpha \beta b_q(x,y)
\]

for all \(x, y \in V\) and \(\alpha, \beta \in L\).

Consider a Galois extension \(L\) of \(k\) with Galois group \(G = \text{Gal}(L/k)\). The action of \(G\) on \(V_L\) is given by

\[
\sigma(\sum_{i=1}^n x_i \otimes \lambda_i) = \sum_{i=1}^n x_i \otimes (\sigma \lambda_i) \quad \text{for} \quad \sigma \in G.
\]

We also have an action of \(G\) on any bilinear forms \(b\) over \(V_L\) given by \(\sigma b(x,y) = \sigma(b(\sigma^{-1} x, \sigma^{-1} y))\) for \(x, y \in V_L\). From the definition of \(b_{q_L}\) we have that \(\sigma b_{q_L} = b_{q_L}\) for all \(\sigma \in G\). On the other hand, if we consider a quadratic form \(q'\) on \(V_L\) such that \(\sigma b_{q'} = b_{q'}\) for all \(\sigma \in G\), then \(q' = q_L\) for a unique quadratic form \(q\) on \(V\).

Lemma 1.7. Given \(q\) and \(q'\) two quadratic forms over \(k\) of the same dimension. There is a Galois extension \(L\) of \(k\) such that \(q_L\) and \(q'_L\) are isometric. In particular, any two quadratic forms over \(k\) of the same dimension become isometric over the separable closure of \(k\).

Proof. Consider \(q = \langle a_1, \ldots, a_n \rangle\) and \(q' = \langle b_1, \ldots, b_n \rangle\) with \(a_i, b_i \in k\). Let \(c_i\) be the square root of \(a_i^{-1} b_i\) and consider the field \(L\) generated by the \(c_i\)'s. The isometry \(\varphi : V_L \to V_L\) between \(q_L\) and \(q'_L\) is given by the matrix \(\text{diag}(c_1, \ldots, c_n)\).

\(\square\)
The following theorem is an immediate consequence of a theorem by Springer (see [21. Chap 2. Theorem 5.3]).

**Theorem 1.8.** Let $L$ be an extension of $k$ of odd degree. If $q$ and $q'$ are of the same dimension and $q_L \simeq q'_L$. then $q \simeq q'$ over $k$.

**The Witt-Groethendieck Group**

Let $Q$ be the set of all isometry classes of quadratic spaces over $k$. The element in $Q$ representing a quadratic space $(V, q)$ will be denoted again by $q$ and the addition in $Q$, induced by the orthogonal sum, will be denoted by $\perp$. In fact, $Q$ is a monoid with respect to $\perp$.

The fact that cancellation law holds in $Q$ is one of the basic theorems of quadratic forms.

**Theorem 1.9.** (Witt Cancellation) [10. Chap 1. Theorem 4.2] If $q, q_1, q_2$ are arbitrary quadratic forms such that $q \perp q_1 \simeq q \perp q_2$. then $q_1 \simeq q_2$.

Now define the following equivalence relation on $Q \times Q$:

$$(q_1, q_2) \sim (q'_1, q'_2) \iff q_1 \perp q'_2 = q_2 \perp q'_1 \in Q.$$

**Definition 1.10.** The set of equivalence classes with respect to $\sim$ is called the **Witt-Groethendieck group of $k$**, denoted by $\hat{W}(k)$.

The operation in $\hat{W}(k)$ is induced by

$$(q_1, q_2) + (q'_1, q'_2) = (q_1 \perp q'_1, q_2 \perp q'_2).$$

The zero element is $(0, 0) = (q, q)$ for any $q \in Q$. Hence the inverse of $(q, q')$ is $(q', q)$.

The map $i: Q \rightarrow \hat{W}(k)$ defined by $i(q) = (q, 0)$ is injective, so we can identify $Q$ with $i(Q)$. Note that $(q, q') = i(q) - i(q') = q - q'$. so each element of $\hat{W}(k)$ can be written as a formal difference of elements in $Q$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Our goal now is to describe $\hat{W}(k)$ by generators and relations. Consider the group ring $\mathbb{Z}[\hat{k}/\hat{k}^2]$ and the group homomorphism

$$\pi : \mathbb{Z}[\hat{k}/\hat{k}^2] \rightarrow \hat{W}(k)$$

defined by $\pi[a] = <a>$ for all $[a] \in \hat{k}/\hat{k}^2$. It is clear that $<a> = <ab^2>$ for any $b \in \hat{k}$. It follows from this and from Theorem 1.3 that $\pi$ is surjective.

**Theorem 1.11.** [21. Chap 2. Theorem 9.1] Let $\pi$ be as above. Hence $\ker(\pi)$ is generated by the elements $[a] + [b] - [c] - [d] \in \mathbb{Z}[\hat{k}/\hat{k}^2]$ satisfying $<a, b> \simeq <c, d>$.

**Proof.** If $\alpha \in \ker \pi$ then $\alpha = [\alpha_1] + \cdots + [\alpha_n] - [\beta_1] - \cdots - [\beta_n]$ with $<\alpha_1, \ldots, \alpha_n> \simeq <\beta_1, \ldots, \beta_n>$. By Witt's chain-equivalence Theorem 1.4.

$<\alpha_1, \ldots, \alpha_n> \simeq <\beta_1, \ldots, \beta_n>$. This means that we have quadratic forms $<\alpha_1, \ldots, \alpha_n> = q_0, q_1, \ldots, q_{m-1}, q_m = <\beta_1, \ldots, \beta_n>$ such that $q_i$ is simply-equivalent to $q_{i+1}$. Consider the diagonalizations that make $q_i$ simply-equivalent to $q_{i+1}$ and write them as elements of $\mathbb{Z}[\hat{k}/\hat{k}^2]$. Then there are $a, b, c, d \in \hat{k}/\hat{k}^2$ such that $q_i - q_{i+1} = [a] + [b] - [c] - [d]$ and $<a, b> \simeq <c, d>$.

Hence we have

$$\alpha = q_0 - q_m = (q_0 - q_1) + (q_1 - q_2) + \cdots + (q_{m-1} - q_m)$$

$$= ([a_1] + [b_1] - [c_1] - [d_1]) + ([a_2] + [b_2] - [c_2] - [d_2]) + \cdots + ([a_m] + [b_m] - [c_m] - [d_m])$$

with $<a_i, b_i> \simeq <c_i, d_i>$. $\square$ Now we are able to give a description of $\hat{W}(k)$ by generators and relations.

**Corollary 1.12.** The group $\hat{W}(k)$ is generated by the elements $<a>$, $a \in \hat{k}$, subject to the relations:
(1) \(< a > = < ab^2 > for all a, b \in \hat{k}.

(2) \(< a > + < b > = < a + b > + < (a + b)ab > for a + b \neq 0.

Invariants

One of the basic questions in quadratic forms is the classification problem. The desire is to associate invariants with a quadratic space so that it is completely determined by them.

The first and most obvious invariant of a quadratic space \((V, q)\) is the dimension of the vector space \(V\). We call it the \textit{dimension of } \(q\).

The subgroup \(I(k) = \{ q_1 - q_2 \in \hat{W}(k) : \dim q_1 = \dim q_2 \}\) of \(\hat{W}(k)\) is called the \textit{fundamental idea l}. This subgroup plays an important role in the theory of quadratic forms.

If \((V, q)\) is a quadratic space, then by 1.3 there are \(a_1, \ldots a_n \in \hat{k}\) such that \(q = < a_1, \ldots a_n >\). Define \(\det(q) = a_1 \cdots a_n \in \hat{k}/k^2\) as the \textit{determinant of } \(q\), which is independent of the diagonalization.

These two invariants are sufficient to classify the quadratic spaces over finite fields (see [21, Chap 2. §3]).

The next important invariant is the Hasse invariant. However we need the notion of quaternion algebras in order to define it.

\textbf{Definition 1.13.} Let \(a, b \in \hat{k}\). We define the \textit{quaternion algebra} \((a, b)\) to be the \(k\)-algebra on two generators \(i, j\) with the relations:

\[ i^2 = a, \ j^2 = b, \text{ and } ij = -ji. \]

A basis of \((a, b)\) is \(\{1, i, j, ij\}\), so \((a, b)\) is a four-dimensional \(k\)-algebra.

\textbf{Example 1.14.} If \(k = \mathbb{R}\), \(a = b = -1\) then \((-1, -1)\) is the well-known ring of \textit{Hamilton quaternions}. 

10
Proposition 1.15. [10. Chap 3. Proposition 1.1] Consider $a.b,c,d \in k$. Then

1. $(a.b) \cong (ac^2, bd^2)$.

2. The center of $(a.b)$ is $k$.

3. $(a.b)$ has no proper two-sided ideals.

4. $(-1, 1) \cong M_2(k)$ (2 × 2 matrices over $k$).

Remark 1.16. From properties (2) and (3), we have that the quaternion algebra $(a.b)$ is a central simple algebra, which will be defined and discussed later in this chapter.

The quaternion algebras help us to classify the binary (of dimension 2) quadratic forms as follows:

Theorem 1.17. [10. Chap 3. Corollary 2.9] The quadratic forms $< a.b >$ and $< c.d >$ are isometric if and only if $(a.b) \cong (c.d)$ and $ab = cd$ in $k/k^2$.

Next we define de Hasse invariant, which is an element of the Brauer group of $k$ (see Definition 1.40).

Definition 1.18. If $q = < a_1, \ldots, a_n >$, we define the Hasse invariant of $q$, denoted $h(q)$, by the formula

$$h(q) = \prod_{i<j}(a_i, a_j).$$

where the product is the tensor product in the Brauer group of $k$. For $n = 1$, $h(q) = 1$ by definition.

The definition of $h(q)$ does not depend on the chosen diagonalization of $q$. This can be shown using the Witt chain-equivalence Theorem 1.4 and Proposition 1.15.

The next lemma facilitates in the computations of Hasse invariants and can be easily verified.
Lemma 1.19. Let $q, q'$ be two quadratic forms. Then

$$h(q \perp q') = h(q) \cdot h(q') \cdot (\det q \cdot \det q').$$

Remark 1.20. The determinant and the Hasse invariant are the first and the second cases in a sequence of invariants of quadratic forms called the Stiefel-Whitney classes. We will define them in Chapter 4.

Clifford Algebras

Let $V$ be a vector space over $k$. We define $T^n(V) = V \otimes \cdots \otimes V$ ($n$ times) for $n > 0$, $T^0(V) = k$ and $T^n(V) = 0$ for $n < 0$.

Then $T(V) = \bigoplus_{n \in \mathbb{Z}} T^n(V)$ is a $\mathbb{Z}$-graded vector space. If $x_1 \otimes \cdots \otimes x_n \in T^n(V)$ and $y_1 \otimes \cdots \otimes y_m \in T^m(V)$, then we define

$$(x_1 \otimes \cdots \otimes x_n)(y_1 \otimes \cdots \otimes y_m) = x_1 \otimes \cdots \otimes x_n \otimes y_1 \otimes \cdots \otimes y_m \in T^{n+m}(V).$$

This defines a product in $T(V)$; so $T(V)$ is a $\mathbb{Z}$-graded $k$-algebra. It is called the tensor algebra of $V$.

Definition 1.21. Let $(V, q)$ be a quadratic space over $k$ and $T(V)$ its tensor algebra. Denote by $I(q)$ the two-sided ideal of $T(V)$ generated by the set \{ $x \otimes x - q(x) : x \in V$ \}. The quotient algebra

$$C(V, q) = \frac{T(V)}{I(q)}$$

is called the Clifford algebra of $(V, q)$. For simplicity we also denote $C(V, q)$ by $C(q)$. We represent by $\bar{u}$ an element $u \in T(V)$ viewed as an element of $C(q)$.

There is a canonical map $V \to C(V, q)$ given by $x \mapsto \bar{x}$. It is clear that $C(V, q)$ is generated by $\bar{V}$.

Properties:

(i) If $x$ and $y$ are orthogonal in $(V, q)$, then $\bar{x} \bar{y} = -\bar{y} \bar{x}$ in $C(V, q)$.

(ii) If $x \in V$ is an anisotropic vector, then $\bar{x}$ is invertible in $C(V, q)$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
(iii) If $x_1, \ldots, x_n$ is an orthogonal basis of $(V, q)$, then $x_1, \ldots, x_n$ generates $C(V, q)$ as a $k$-algebra. Since $x_i^2 = q(x_i)$ and $x_i x_j = -x_j x_i$ for $i \neq j$, the products

$$x_1^{e_1} \cdots x_n^{e_n} \text{ with } e_i \in \{0, 1\}.$$ 

generate $C(V, q)$ as a $k$-vector space.

(iv) The property (iii) implies that the canonical map $V \to C(q)$ is injective. Hence we can identify $V$ with $\tilde{V}$ and omit the bar notation.

(v) There is a canonical involution $'$ on $C(q)$ defined by $(x_1 \cdots x_k)' = x_k \cdots x_1$ for $x_i \in V$. Clearly this involution is trivial on $V$.

**Example 1.22.** Consider the binary form $q = \langle a_1 b \rangle$ with $a_1 b \notin \dot{k} / k^2$. Then $C(q)$ is the quaternion algebra $(a_1 b)$ as defined in 1.13.

The isometry $x \mapsto -x$ of $V$ induces an automorphism of $C(q)$ of order two, that we shall denote by $\gamma$. Hence we can use $\gamma$ to define a grading on $C(q)$ as follows:

$$C_0(q) = \{ s \in C(q) : \gamma(s) = s \} \quad \text{(even part)}$$

$$C_1(q) = \{ s \in C(q) : \gamma(s) = -s \} \quad \text{(odd part)}$$

We have that $C(q) = C_0(q) \oplus C_1(q)$.

**Remark 1.23.** Note that if $s \in C_0(q)$ (resp., $C_1(q)$), then $s$ is a $k$-linear combination of products $x_1 \cdots x_r$ with $r$ even (resp., odd).

**Lemma 1.24.** Let $t \in O(q)$ be an isometry of $q$. Then there exists an invertible element $s_t \in C(q)$ such that for $x \in V$, $t(x) = d(t)s_txs_t^{-1}$. where $d(t)$ is the determinant of $t$. 

13
Proof. First, consider $t$ a reflection $\tau_x$ with $x$ an anisotropic (so invertible) element of $V$. hence $d(t) = -1$. For $y \in V$.

$$t(y) = \tau_x(y) = y - \frac{b_q(y \cdot x)}{q(x)} x$$

$$= y - (yx + yx)x^{-2}x$$

$$= -xyx^{-1}.$$ 

Now from the Cartan-Dieudonné Theorem 1.6, given $t \in O(q)$ there are anisotropic vectors $x_1, \ldots, x_r$ in $V$ such that $t = \tau_{x_1} \cdots \tau_{x_r}$. Hence $d(t) = (-1)^r$ and

$$t(y) = \tau_{x_1} \cdots \tau_{x_r}(y) = \tau_{x_1} \cdots \tau_{x_{r-1}}(-x_r y x_r^{-1})$$

$$= (-1)^r(x_1 \cdots x_r)y(x_r^{-1} \cdots x_1^{-1})$$

$$= (-1)^r s_t y s_t^{-1}.$$ 

where $s_t = x_1 \cdots x_r$. $\square$

In fact we proved more than the theorem required. We have shown that the element $s_t$ can be chosen to be even (resp., odd) if $d(t) = 1$ (resp., $-1$). As a result, we can say that $t(x) = \gamma(s_t)y s_t^{-1}$.

The set $P(q) = \{s \in C(q) : s \text{ is invertible and } \gamma(s)Vs^{-1} = V\}$ is a subgroup of the group of invertible elements of $C(q)$. For each $s \in P(q)$ define $\alpha_s : V \rightarrow V$ by $\alpha_s(x) = \gamma(s)x s^{-1}$. From this we get a homomorphism $\alpha : P(q) \rightarrow \text{Aut}(V)$. In fact one can show that the maps $\alpha_s$ are isometries and we actually have

$$\alpha : P(q) \rightarrow O(q).$$

From the above lemma, $\alpha$ is surjective. Moreover.

Proposition 1.25. [21. Chap 9. Theorem 3.3] Let $\alpha$ be as above. then there is an exact sequence

$$1 \rightarrow \hat{k} \rightarrow P(q) \xrightarrow{\alpha} O(q) \rightarrow 1.$$ 

14
Denote by $\text{Pin}(q)$ the subgroup of $P(q)$ consisting of elements $s$ such that $ss' = 1$. The restriction of the map $\alpha$ to $\text{Pin}(q)$ will be denote by $\pi$. The sequence

$$1 \to \{\pm 1\} \to \text{Pin}(q) \xrightarrow{\pi} \text{O}(q)$$

is exact, but the map $\pi$ may not be surjective.

**Definition 1.26.** The *spinor norm* is the homomorphism $\beta : \text{O}(q) \to \hat{k}/\hat{k}^2$ defined on the generators $\tau_x$ by $\beta(\tau_x) = q(x) \in \hat{k}/\hat{k}^2$.

One can check that the sequence

$$1 \to \{\pm 1\} \to \text{Pin}(q) \xrightarrow{\pi} \text{O}(q) \xrightarrow{\beta} \hat{k}/\hat{k}^2$$

is exact. In particular if $\hat{k}/\hat{k}^2 = 1$, then we have the following short exact sequence

$$1 \to \{\pm 1\} \to \text{Pin}(q) \xrightarrow{\pi} \text{O}(q) \to 1. \quad (1.1)$$

**Definition 1.27.** The inverse image $\pi^{-1}(\text{SO}(q))$ is called the *spin group* of $(V, q)$ and denoted by $\text{Spin}(q)$. In fact, $\text{Spin}(q) = \text{Pin}(q) \cap \text{C}_0(q)$.

**Theorem 1.28.** If $\hat{k}/\hat{k}^2 = 1$, then the following sequence is exact

$$1 \to \{\pm 1\} \to \text{Spin}(q) \xrightarrow{\pi} \text{SO}(q) \to 1.$$

### 1.2 Central Simple Algebras

In this section we only consider finite dimensional algebras over a field $k$ (of any characteristic).

**Definition 1.29.** An algebra $A$ is called *simple* if it has no two-sided ideals other than 0 and $A$.

**Theorem 1.30.** (Wedderburn) Let $A$ be a simple algebra over $k$ and $M$ a minimal right ideal of $A$. Then $D = \text{End}_A(M)$ is a division algebra and $A \cong M_n(D)$ for some $n \in \mathbb{N}$.
Proof. Since $M$ is a minimal right ideal of $A$, it is easy to see that every nonzero endomorphism of $M$ is an isomorphism (so invertible). Hence $\text{End}_A(M)$ is a division algebra.

Recall that for any ring $R$ we have $R \cong \text{End}_R(R)$ when $R$ is considered as a right module over itself. This isomorphism is given by

$$R \to \text{End}_R(R), \quad x \mapsto (y \mapsto xy).$$

Hence we have $A \cong \text{End}_A(A)$.

Now since $A$ is simple, $AM = A$. Hence there are $a_i \in A, x_i \in M$ such that

$$1 = a_1x_1 + \cdots + a_nx_n.$$

We choose one of these equations which has $n$ minimal. Since $a = a_1(x_1a) + \cdots + a_n(x_na)$ for all $a \in A$, we have that

$$A = a_1M + \cdots + a_nM.$$

One can check that this is a direct sum. Since $M$ is minimal the map $x \mapsto a_ix$ is an isomorphism $M \cong a_iM$. Thus we have

$$A \cong M^n = M \oplus \cdots \oplus M.$$

Putting all these facts together we get

$$A \cong \text{End}_A(A) \cong \text{End}_A(M^n) \cong M_n(\text{End}_A(M)) = M_n(D).$$

where $D = \text{End}_A(M)$. □

**Proposition 1.31.** [21. Chap 8. Proposition 1.9] If $D$ and $\Delta$ are division algebras such that $M_n(D) \cong M_m(\Delta)$, then $D \cong \Delta$ and $m = n$. 

16
Remark 1.32. Note that \( \dim_k A = \dim_D M_n(D) = n^2 \). Hence the dimension of a simple \( k \)-algebra is always a square. The square root \( n \) of this dimension is called degree of \( A \).

Definition 1.33. A \( k \)-algebra is called central if its center is \( k \). An algebra that is both central and simple is called central simple algebra.

Example 1.34. Let \( a, b \in k \). then the quaternion algebra \( (a, b) \) defined in 1.13 is a central simple algebra (see Proposition 1.15).

Lemma 1.35. [21. Chap. 8. Lemma 2.3] If \( A \) is a \( k \)-algebra, then
\[
M_n(k) \otimes_k A \cong M_n(A).
\]
In particular, \( M_n(k) \otimes M_m(k) \cong M_{mn}(k) \).

Theorem 1.36. [21. Chap. 8. Theorem 3.2] Let \( A, B \) be \( k \)-algebras.

(i) If \( A \) and \( B \) are central, then \( A \otimes B \) is central.

(ii) If \( A \) is a central simple algebra and \( B \) is simple, then \( A \otimes B \) is simple.

(iii) If \( A \) and \( B \) are central simple algebras, then \( A \otimes B \) is also a central simple algebra.

Definition 1.37. For a \( k \)-algebra \( A \), define a new algebra \( A^{op} \) by \( A^{op} = A \) as additive abelian groups and the product \( \circ \) in \( A^{op} \) is given by \( a \circ b = ba \). Clearly \( A^{op} \) is a \( k \)-algebra. It is called the opposite algebra of \( A \).

Lemma 1.38. If \( A \) is a central simple algebra over \( k \), then \( A^{op} \) is also a central simple algebra over \( k \).

Proof. Every left (right) ideal of \( A \) is a right (left) ideal of \( A^{op} \). Thus \( A^{op} \) is simple. Clearly the center of \( A^{op} \) coincides with the center of \( A \). \( \square \)

Theorem 1.39. Let \( A \) be a central simple algebra over \( k \). Then \( A \otimes A^{op} \cong M_n(k) \) where \( n = \dim A \).
Proof. For $a \in A$ and $b \in A^{op}$ define the map

$$A \times A^{op} \to \text{End}_k(A) \quad \text{by} \quad (a, b) \mapsto (x \to axb).$$

This map is bilinear and multiplicative. Hence by the universal property of the tensor product there is an algebra homomorphism

$$\varphi : A \otimes A^{op} \to \text{End}_k(A).$$

Since $A \otimes A^{op}$ is simple, $\varphi$ is injective. In fact, $\varphi$ is bijective because the dimensions coincide. Therefore

$$A \otimes A^{op} \cong \text{End}_k(A) \cong M_n(k). \quad \Box$$

**Definition 1.40.** We say that two central simple algebras $A, B$ are similar ($A \sim B$) if $A \cong M_n(D)$ and $B \cong M_m(D)$ for some division algebra $D$ and some $m, n \in \mathbb{N}$. This defines an equivalence relation on the set of central simple algebras over $k$. The set of equivalence classes is called the **Brauer group**, denoted $\text{Br}(k)$.

We need to check that indeed $\text{Br}(k)$ is a group. First if $A \sim A'$ and $B \sim B'$, then from Lemma 1.35 we have $A \otimes B \sim A' \otimes B'$. Hence tensor product is compatible with the equivalence relation and induces a product in $\text{Br}(k)$. From the commutativity and the associativity of tensor product we get the same properties for the product in $\text{Br}(k)$. The neutral element is the class of the matrix algebras $\{M_n(k) : n \in \mathbb{N}\}$ and $A^{op}$ is the inverse element of $A$ (see 1.39).

**Remark 1.41.** The tensor product of quaternion algebras has the property:

$$(a, b) \otimes (a, c) \cong (a, bc) \otimes M_2(k) \quad \text{(see [10, Corollary 2.11])}.$$

Hence $(a, b) \otimes (a, c) = (a, bc)$ in $\text{Br}(k)$. Similarly, $(a, b) \otimes (c, b) = (ac, b)$ in $\text{Br}(k)$.

The Brauer group has also a cohomological interpretation (see Corollary 2.10). The automorphisms of central simple algebras can be totally described as follows:
Theorem 1.42. (Skolem-Noether) [21, Chap 8. Theorem 4.2] Let $A$ be a central simple algebra over $k$ and $B$ a simple $k$-algebra. If $\sigma, \tau : B \rightarrow A$ are two algebra homomorphisms, then there exists an inner automorphism $\varphi$ of $A$ such that $\tau = \varphi \sigma$.

Corollary 1.43. Every automorphism of a central simple algebra is an inner automorphism.

Next consider $L$ a field extension of $k$. If $A$ is a $k$-algebra, then $A_L = A \otimes_k L$ is a $L$-algebra. Clearly $\dim_k(A) = \dim_L(A_L)$.

Definition 1.44. A field extension $L$ of $k$ is called a splitting field of $A$ if $A_L \cong M_n(L)$ for some $n$. We also say that $A$ splits over $L$.

Theorem 1.45. [7, Corollary 4.8] Let $A$ be a central simple algebra over $k$ and $D$ be the division algebra such that $A \cong M_n(D)$. Then any maximal subfield of $D$ is a splitting field of $A$.

Theorem 1.46. [21, Chap 8. Theorem 5.5] Every central simple algebra has a separable splitting field.

Consider $A$ a central simple algebra over $k$ of dimension $n^2$. If $L$ is a splitting field of $A$, then there exists an isomorphism $i : A \otimes_k L \rightarrow M_n(L)$. To each element $a \in A$ we can associate a matrix $i(a \otimes 1)$ in $M_n(L)$. Let $c(X, a) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_0$ be the characteristic polynomial of $i(a \otimes 1)$ in $L[X]$. It can be shown that $c(X, a)$ does not depend on the choice of $L$ and has coefficients in $k$.

Definition 1.47. Let $A$ be a central simple algebra over $k$. $a \in A$. The polynomial $c(X, a)$ is called the characteristic polynomial of $a$. The coefficient $(-1)^n \alpha_0$ is called the reduced norm of $a$ and $-\alpha_{n-1}$ is called the reduced trace of $a$. We will denote them by $n(a)$ and $\text{tr}(a)$ respectively.
From matrix algebra theory, we have the following properties:

\[(1) n(ab) = n(a)n(b)\]
\[n(aa) = \alpha^n n(a).\]
\[(2) \text{tr}(a + b) = \text{tr}(a) + \text{tr}(b)\]
\[\text{tr}(aa) = a \text{tr}(a).\]
\[\text{tr}(ab) = \text{tr}(ba).\]

for \(a, b \in A\) and \(\alpha \in k\).

The reduced trace will be used later to define the scaled trace forms over central simple algebras. Each scaled trace form will be associated to a pointed algebra, which we shall discuss now.

**Definition 1.48.** A **pointed algebra** over \(k\) is a pair \((A, a)\), where \(A\) is a central simple algebra over \(k\) and \(a\) is a fixed element of \(A\). Two pointed algebras \((A, a)\) and \((B, b)\) are said to be **isomorphic** if there exists a \(k\)-algebra isomorphism \(\varphi : A \rightarrow B\) with \(\varphi(a) = b\).

Let \(k_s\) be the separable closure of \(k\). A **twist** of \((A, a)\) is a pointed algebra \((B, b)\) over \(k\) such that \((A \otimes k_s, a) \cong (B \otimes k_s, b)\) as pointed algebras over \(k_s\).

**Lemma 1.49.** Let \(A\) be a central simple algebra over \(k\) and let \(a \in A\). Then there exists \(b \in M_n(k)\), unique up to conjugacy, such that \((A, a)\) is a twist of \((M_n(k), b)\).

**Proof.** Since \(A\) is a central simple algebra, there exists an isomorphism \(\varphi : A \otimes k_s \rightarrow M_n(k_s)\), where \(n\) is the degree of \(A\) over \(k\) (Theorem 1.46). By the Skolem-Noether Theorem, \(\gamma(\varphi)\varphi^{-1}\) is an inner automorphism for all \(\gamma \in \Gamma = \text{Gal}(k_s/k)\).

In particular \(\varphi(a)\) and \(\gamma(\varphi(a))\) are similar in \(M_n(k_s)\) for all \(\gamma \in \Gamma\). It follows that the elementary divisors associated with \(\varphi(a)\) have coefficients in \(k\). Thus \(\varphi(a)\) is similar to a matrix in \(M_n(k)\). Uniqueness follows from the fact that a similarity class is uniquely determined by its elementary divisors. \(\square\)
Chapter 2
Cohomology

2.1 Cohomology of Groups

Let $G$ be a group, written multiplicatively, and let $A$ be an abelian group, written additively. We say that $G$ acts on the left on $A$ if we have a map $(g, x) \mapsto gx$ of $G \times A$ into $A$ such that

$$g(x + y) = gx + gy$$

$$(g_1g_2)x = g_1(g_2x)$$

$$1x = x$$

for $g, g_1, g_2 \in G$ and $x, y \in A$.

Given the group ring $\mathbb{Z}[G]$, $A$ becomes a $\mathbb{Z}[G]$-module if we define

$$(\sum \alpha_g g)x = \sum \alpha_g gx.$$ 

Conversely, if $A$ is a $\mathbb{Z}[G]$-module, then $A$ becomes a $G$-module by restricting the action to $G$. The elements of $A$ that are fixed by $G$ form a subgroup of $A$, denoted by $A^G$.

Let $A$ be a $G$-module and $C^n(G, A)$ be the set of functions on $n$ variables in $G$ into $A$. The elements of $C^n(G, A)$ are called $n$-cochains. A 0-cochain is an element of $A$. With the usual definitions of addition and zero, $C^n(G, A)$ is an abelian group.

Now we define a map $d$ from $C^n(G, A)$ into $C^{n+1}(G, A)$. The differential $d\alpha$ of an $n$-cochain $\alpha$ is the $(n + 1)$-cochain

$$(d\alpha)(g_1, \ldots, g_{n+1}) = g_1\alpha(g_2, \ldots, g_{n+1})$$

$$+ \sum_{j=1}^{n} (-1)^j \alpha(g_1, \ldots, g_j g_{j+1} \ldots, g_{n+1})$$

$$+ (-1)^{n+1} \alpha(g_1, \ldots, g_n).$$

The $n$-cochains such that $d\alpha = 0$ are called $n$-cocycles. If $\alpha$ is a $(n - 1)$-cochain, then the $n$-cochain $d\alpha$ is called an $n$-coboundary. We write $Z^n(G, A)$ and $B^n(G, A)$.
for the groups of all $n$-cocycles and $n$-coboundaries respectively. It can be verified that $d(d\phi) = 0$. so $B^n(G, A) \subset Z^n(G, A)$.

**Definition 2.1.** The factor group

$$H^n(G, A) = \frac{Z^n(G, A)}{B^n(G, A)}$$

(2.1)

is called the $n^{th}$ cohomology group of $G$ with coefficients in $A$.

The elements of $H^0(G, A)$ are the elements of $A$ such that $g \cdot a = a$ for all $g \in G$. thus $H^0(G, A) = A^G$.

A 1-cocycle in $H^1(G, A)$ is a map $\phi$ from $G$ into $A$ satisfying the identity

$$\phi(gg') = g \cdot \phi(g') + \phi(g).$$

It is also called a crossed homomorphism.

A 2-cocycle in $H^2(G, A)$ is a map $\phi$ from $G \times G$ into $A$ such that

$$g \cdot \phi(g', g^\prime) - \phi(gg', g^\prime) + \phi(g, g'g^\prime) - \phi(g, g') = 0.$$
is also exact. Hence the functor $\text{Hom}_G(\mathbb{Z}, -)$ is left exact.

The following definition requires the notion of derived functors, which can be found in any introductory book of homological algebra.

**Definition 2.2.** The right derived functors of the functor $\text{Hom}_G(\mathbb{Z}, A)$ are the *cohomology groups of $G$ with coefficients in $A$*, denoted by $H^n(G, A), n \geq 0$.

Briefly these cohomologies are computed as follows:

Consider a sequence $P_i$ of projective $G$-modules such that the sequence

$$
\cdots \rightarrow P_i \rightarrow P_{i-1} \rightarrow \cdots \rightarrow P_0 \rightarrow \mathbb{Z} \rightarrow 0
$$

is exact (such a sequence is called a *projective resolution* of $\mathbb{Z}$). Now consider the cochain complex $\text{Hom}_G(P, A)$. By taking cohomology of this complex we have

$$
H^n(G, A) = H^n(\text{Hom}_G(P, A)).
$$

We refer to [7, section 6.9] for a good connection between the two definitions.

The functors $H^n(G, -)$ are *universal δ-functors* (see [30, section 2.1]). Hence they have the following properties:

1. For every $n \geq 0$ and every exact sequence of $G$-module

   $$
   0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0,
   $$

   there is a homomorphism (called *connecting homomorphism*)

   $$
   \partial : H^n(G, C) \rightarrow H^{n+1}(G, A)
   $$

   such that the sequence of cohomology groups

   $$
   \cdots \rightarrow H^n(G, B) \rightarrow H^n(G, C) \xrightarrow{\partial} H^{n+1}(G, A) \rightarrow H^{n+1}(G, B) \rightarrow \cdots
   $$

   is exact. This sequence is called the *long exact cohomology sequence*.

23

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
(2) For each commutative diagram of $G$-modules with exact rows

\[
\begin{array}{cccccc}
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0
\end{array}
\]

we have a commutative diagram

\[
\begin{array}{cccccccc}
\cdots & \longrightarrow & H^n(G, B) & \longrightarrow & H^n(G, C) & \overset{\partial}{\longrightarrow} & H^{n+1}(G, A) & \longrightarrow & H^n(G, B) & \longrightarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\cdots & \longrightarrow & H^n(G, B') & \longrightarrow & H^n(G, C') & \overset{\partial'}{\longrightarrow} & H^{n+1}(G, A') & \longrightarrow & H^n(G, B') & \longrightarrow & \cdots
\end{array}
\]

(3) (the universal property) If $T^n$ is another $\delta$-functor and $f^0 : T^0 \rightarrow H^0(G, -)$ is a natural transformation of functors in dimension zero, then there is a unique morphism \( \{ f^n : T^n \rightarrow H^n(G, -), n \geq 0 \} \) of $\delta$-functors extending $f^0$.

**Restriction and Corestriction**

Now we will define some maps in cohomology. The universal property will be of great help in this matter.

Let $H$ be a subgroup of $G$. We can consider a $G$-module $A$ as an $H$-module and define a new $\delta$-functor $H^n(H, A)$. The natural inclusion

\[
H^0(G, A) = A^G \hookrightarrow A^H = H^0(H, A)
\]

is a map in dimension zero between the $\delta$-functors $H^n(G, -)$ and $H^n(H, -)$. By the universal property, this map extends uniquely to a morphism of $\delta$-functors. This means that for each $n \geq 0$ we obtain a map

\[
\text{Res} : H^n(G, A) \rightarrow H^n(H, A)
\]

which is called *restriction*. This is the same map obtained by restricting the cocycles in $C^n(G, A)$ to $H$. 

24

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Now assume that $H$ has finite index in $G$. If $a \in A^H$ and $g \in G$, then the element $ga$ depends only on the left coset of $g \mod H$. Hence the sum

$$N_{G/H}(a) = \sum_{g \in G/H} ga$$

is finite. We call it the norm of $a$. It is easy to check that $N_{G/H}(a) \in A^G$ for all $a \in A^H$. Thus we get a homomorphism in dimension zero, functorial in $A$.

$$N_{G/H} : H^0(H, A) \to H^0(G, A).$$

As before we use the universal property to extend to higher dimensions and we obtain

$$\text{Cor} : H^n(H, A) \to H^n(G, A)$$

for all $n \geq 0$. This map is called corestriction.

**Remark 2.3.** Using the universal property, one can easily show that

$$\text{Cor} \circ \text{Res} = \text{Card}(G/H).$$

**Cup Product**

Let $R$ be a commutative ring. Consider an action of $G$ on $R$ by ring automorphisms. We shall define the cup product, which is a family of homomorphisms

$$H^p(G, R) \otimes H^q(G, R) \to H^{p+q}(G, R)$$

for every pair $(p, q)$.

We start by defining the cross product.

Let $G$ and $G'$ be two groups. Let

$$P : \cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0 \quad \text{and} \quad Q : \cdots \to Q_1 \to Q_0 \to \mathbb{Z} \to 0$$

be projective resolutions of $\mathbb{Z}$ over $\mathbb{Z}G$ and $\mathbb{Z}G'$ respectively. For every integer $n$, define an abelian group $T^n(P, Q, R)$ as follows:

$$T^n(P, Q, R) = \sum_{i=0}^{n} \text{Hom}_C(P_i, R) \otimes \text{Hom}_{C'}(Q_{n-i}, R).$$
Now for every \( n \) define a homomorphism

\[
d : T^n(P, Q, R) \to T^{n+1}(P, Q, R)
\]

by \( d(a \otimes b) = (da) \otimes b + (-1)^n a \otimes (db) \) for every \( a \in \text{Hom}_G(P, R) \) and \( b \in \text{Hom}_{G'}(Q_{n-1}, R) \). One can easily check that \( d^2 = 0 \). Thus we obtain a chain complex

\[
\cdots \to T^{n-1}(P, Q, R) \xrightarrow{d} T^n(P, Q, R) \xrightarrow{d} T^{n+1}(P, Q, R) \to \cdots
\]

which we denote \( \text{Hom}_G(P, R) \otimes \text{Hom}_{G'}(Q, R) \).

For every pair \((p, q)\), we define a homomorphism

\[
\rho : H^p(G, R) \otimes H^q(G, R) \to H^{p+q}[\text{Hom}_G(P, R) \otimes \text{Hom}_{G'}(Q, R)]
\]

as follows:

Let \( a \in H^p(G, R) \) and \( b \in H^q(G, R) \). If \( \alpha \) and \( \beta \) are cocycles representing \( a \) and \( b \) respectively, then \( \alpha \otimes \beta \) is an element of \( \text{Hom}_G(P, R) \otimes \text{Hom}_{G'}(Q, R) \) and \( d(\alpha \otimes \beta) = d\alpha \otimes \beta + (-1)^p \alpha \otimes d\beta = 0 \). Hence \( \alpha \otimes \beta \) is in \( Z^{p+q}[\text{Hom}_G(P, R) \otimes \text{Hom}_{G'}(Q, R)] \) and represents an element

\[
c \in H^{p+q}[\text{Hom}_G(P, R) \otimes \text{Hom}_{G'}(Q, R)].
\]

One can easily verify that \( c \) does not depend on the choices of \( \alpha \) and \( \beta \) and that the assignment \( a \otimes b \to c \) determines the homomorphism \( \rho \).

There is a natural homomorphism

\[
\mu : \text{Hom}_G(P, R) \otimes \text{Hom}_{G'}(Q, R) \to \text{Hom}_{G \times G'}(P \otimes Q, R)
\]

given by

\[
\mu(f \otimes f')(x \otimes y) = f(x)f'(y) \quad \text{for} \quad x \in P, y \in Q,
\]
The cross product $\times : H^p(G, R) \otimes H^q(G', R) \to H^{p+q}(G \times G', R)$ is the map that makes the following diagram commutative:

$$
\begin{array}{ccc}
H^p(G, R) \otimes H^q(G', R) & \xrightarrow{\times} & H^{p+q}[\text{Hom}_G(P, R) \otimes \text{Hom}_{G'}(Q, R)] \\
\downarrow & & \downarrow \\
H^{p+q}(G \times G', R) & = & H^{p+q}[\text{Hom}_{G \times G'}(P \otimes Q, R)].
\end{array}
$$

If we consider $G = G'$, then we have a map

$$
\times : H^p(G, R) \otimes H^q(G, R) \to H^{p+q}(G \times G, R).
$$

If $\tau$ is the involution $\tau(g, h) = (h, g)$ on $G \times G$, then $\tau$ induces a map $\tau^* : H^*(G \times G, R) \to H^*(G \times G, R)$ and $\tau^*(b \times a) = (-1)^{pq}(a \times b)$ for $a \in H^p(G, R)$ and $b \in H^q(G, R)$ (see [30, Lemma 6.7.12]). It follows that the cross product is graded-commutative. That is, $a \times b = (-1)^{pq}b \times a$ for $a \in H^p(G, R)$ and $b \in H^q(G, R)$.

The diagonal map $d : G \to G \times G$ is injective and induces a restriction map in cohomology

$$
d^* : H^n(G \times G, R) \to H^n(G, R).
$$

**Definition 2.4.** The cup product is defined by the composition

$$
d^* \circ \times : H^p(G, R) \otimes H^q(G, R) \to H^{p+q}(G, R).
$$

Given $a \in H^p(G, R)$ and $b \in H^q(G, R)$ the cup product $a \cdot b$ is the element $d^*(a \times b) \in H^{p+q}(G, R)$.

We list here just two of the many properties of the cup product. Both are inherited from the cross product.

1. The cup product is associative.
2. For every $a \in H^p(G, R)$ and every $b \in H^q(G, R)$, we have

$$
a \cdot b = (-1)^{pq}(b \cdot a) \quad \text{in} \quad H^{p+q}(G, R).
$$

(2.2)
Next let us consider the direct sum
\[ H^*(G, R) = \bigoplus_{n=0}^{\infty} H^n(G, R). \]

Then for every \( n \geq 0 \), \( H^n(G, R) \) is a subgroup of the abelian group \( H^*(G, R) \). The elements of \( H^n(G, R) \) are called the \( n \)-dimensional homogeneous elements of the group \( H^*(G, R) \). It follows from the definition that every \( a \in H^*(G, R) \) can be written as a sum \( a = \sum_{i=1}^{m} a_i \), with the \( a_i \)'s being homogeneous elements of different dimensions. Given \( a = \sum_{i=1}^{m} a_i \) and \( b = \sum_{j=1}^{n} b_j \), two elements of \( H^*(G, R) \), we define a product
\[ a \cdot b = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i \cdot b_j, \]
where the operation in the right hand side is the cup product. This product is associative. Moreover, we have

**Proposition 2.5.** [30. Proposition 6.7.11] The abelian group \( H^*(G, R) \) is a graded-commutative ring with unity.

### 2.2 Non-abelian Cohomology

Let \( G \) be a group and \( A \) a group (not necessarily abelian) on which \( G \) acts on the left. We shall define \( H^0(G, A) \) and \( H^1(G, A) \) in such way that they are pointed sets. They shall also coincide with the pointed set structure of the cohomology groups in the abelian situation.

We start by again defining \( H^0(G, A) = \mathcal{A}^G \). A map \( \phi : G \to A \) satisfying
\[ \phi(gh) = \phi(g)\phi(h) \]
for all \( g, h \in G \)
is called a \( 1 \)-cocycle. If there is \( a \in A \) such that \( \phi(g) = a^{-1}g(a) \) for all \( g \in G \), then \( \phi \) is a coboundary. We say that two cocycles \( \phi \) and \( \psi \) are cohomologous if there exists \( a \in A \) such that \( \psi(g) = a^{-1}\phi(g)a \). This defines an equivalence relation in the set of \( 1 \)-cocycles. The quotient set will be called the cohomology set of \( G \) with
values in A. denoted by $H^1(G, A)$. In this set we have a distinguished element, namely the class of the trivial cocycle $o(g) = 1$ for all $g \in G$. Hence $H^1(G, A)$ is a pointed set.

Let $f : A \to B$ be a $G$-homomorphism between the groups $A$ and $B$. If we restrict $f$ to $A^G$, then the image would be contained in $B^G$. Hence $f$ induces a map

$$f_0 : H^0(G, A) \to H^0(G, B).$$

Now given a cocycle $o : G \to A$, the composition $f \circ o : G \to B$ is a cocycle of $B$. This composition is compatible with the equivalence relation. Thus $f$ induces a map

$$f_1 : H^1(G, A) \to H^1(G, B).$$

Note that $f_0$ is a group homomorphism, but $f_1$ is just a morphism of pointed sets (takes distinguished element to distinguished element). The kernel of a morphism of pointed sets is the preimage of the distinguished element. Thus we can talk about exact sequences of pointed sets.

Our goal now is to define connecting homomorphisms in order to obtain part of the long exact cohomology sequence.

Let

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

be an exact sequence of non-abelian $G$-modules, with $i(A)$ being normal in $B$. We first define the connecting homomorphism

$$\partial_0 : H^0(G, C) \to H^1(G, A).$$

For $c \in C^G$ choose $b \in B$ such that $p(b) = c$. Since $p$ is a $G$-homomorphism and $g c = c$ for all $g \in G$, we have that $p(gb) = p(b)$ for all $g \in G$. Then $b^{-1}g(b) \in \ker p = i(A)$. Define $o : G \to A$ by $o(g) = i^{-1}(b^{-1}g(b))$. It is a straightforward computation
to show that \( \sigma \) is a cocycle of \( A \) and its cohomology class is independent of the choice of \( b \). Define the cohomology class of \( \sigma \) as \( \partial_0(c) \).

Assume that \( A \) is contained in the center of \( B \), in particular \( A \) is abelian. Consider the cohomology group \( H^2(G, A) \) as a pointed set. We shall define

\[
\partial_1 : H^1(G, C) \to H^2(G, A).
\]

For this consider \( \sigma : G \to C \) a cocycle of \( C \) and for each \( g \in G \) choose \( \nu(g) \in B \) such that \( p(\nu(g)) = \sigma(g) \). Since \( \sigma(gh) = \sigma(g)\sigma(h) \), we have that \( p(\nu(gh)) = p(\nu(g)\nu(h)) \). By exactness of (2.3)

\[
\nu(gh) \equiv \nu(g)\nu(h) \mod A \quad \text{for all } g, h \in G.
\]

Hence \( \varphi(g, h) = \nu(g)\nu(h)\nu(gh)^{-1} \) is an element of \( A \) for all \( g, h \in G \). By straightforward computation one shows that:

1. The map \( \varphi \) is a 2-cocycle of \( A \).
2. The class of \( \varphi \) in \( H^2(G, A) \) depends neither on the choice of \( \sigma \) within its class nor on the choice of \( \nu \).

We denote by \( \partial_1(\sigma) \) the class of \( \varphi \) in \( H^2(G, A) \).

**Proposition 2.6.** Consider the exact sequence (2.3) of non-abelian \( G \)-modules with \( A \) central in \( B \). Then the sequence of pointed sets below is exact

\[
0 \to H^0(G, A) \xrightarrow{i_0} H^0(G, B) \xrightarrow{p_0} H^0(G, C) \xrightarrow{\partial_0} H^1(G, A) \xrightarrow{i_1} H^1(G, B) \xrightarrow{p_1} H^1(G, C) \xrightarrow{\partial_1} H^2(G, A).
\]

**Proof.** Exactness at \( H^0(G, A) \) and \( H^0(G, B) \) follows essentially from the exactness of the short exact sequence (2.3) at \( A \) and \( B \).

If \( c \in C^G \) and \( \partial_0(c) \) is a coboundary, then we can choose \( b \in p^{-1}(c) \) such that \( \partial_0(c)(g) = i^{-1}(b^{-1}g(b)) = 1 \) for all \( g \in G \). Hence \( gb = b \) for all \( g \in G \). thus
\[ c = p(b) = p_0(b). \] Conversely, if there exists \( b \in B^G \) such that \( p_0(b) = c \), then 
\[ \partial_0(c)(g) = i^{-1}(b^{-1}g(b)) = 0 \] for all \( g \in G \). Thus we have exactness at \( H^0(G, C) \).

If \( \phi \in H^1(G, A) \) is in the kernel of \( i_1 \), then \( i \circ \phi(g) = b^{-1}g(b) \) for some \( b \in B \). Hence \( \phi(g) = i^{-1}(b^{-1}g(b)) \) for all \( g \in G \) and \( \phi = \partial_0(c) \) where \( c = p(b) \). Conversely, if \( \phi \in \text{Im}(\partial_0) \), then there exists \( b \in B \) such that \( \phi(g) = i^{-1}(b^{-1}g(b)) \). Thus \( i_1(\phi)(g) = i \circ \phi(g) = b^{-1}g(b) \), that is, \( i_1(\phi) = 1 \). This shows the exactness at \( H^1(G, A) \).

Since \( p \circ i = 1 \) we have \( (p_1 \circ i_1)(\phi) = p \circ i \circ \phi \) for all \( \phi \in H^1(G, A) \). Conversely, if \( \phi \in \ker p_1 \), then \( p \circ \phi(g) = c^{-1}g(c) \) for some \( c \in C \). Since \( p \) is surjective, there is \( b \in B \) such that \( p(b) = c \), thus \( \phi(g) = b^{-1}g(b) \) is a coboundary. Hence \( \phi \) must be the image by \( i_1 \) of a coboundary in \( H^1(G, A) \). We have exactness at \( H^1(G, B) \).

For \( \phi \in H^1(G, B) \) we have
\[
(\partial_1 \circ p_1)(\phi)(g, h) = p_1(\phi)(g)gp_1(\phi)(h)[p_1(\phi)(gh)]^{-1}
\]
\[
= p(\phi(g)gp_1(\phi)(h)p_1(\phi)(gh)^{-1})
\]
\[
= 1.
\]
Hence \( \text{Im} \ p_1 \subset \ker \partial_1 \). On the other hand, if \( \phi \in H^1(G, C) \) is in the kernel of \( \partial_1 \), then there exists a map \( \psi : G \to B \) such that \( p \circ \psi = \phi \) and \( \partial_1(\phi)(g, h) = \psi(g)g\psi(h)\psi(gh)^{-1} \) is a coboundary. Thus we can choose \( \psi' : G \to B \) cohomologous to \( \psi \) such that
\[
\partial_1(\phi)(g, h) = \psi'(g)g\psi'(h)\psi'(gh)^{-1} = 1 \quad \text{for all } g, h \in G.
\]
Hence \( \psi'(gh) = \psi'(g)g\psi'(h) \), that is, \( \psi' \) is a cocycle of \( B \) and \( \phi = p \circ \psi = p \circ \psi' = p_1(\psi') \). This shows the exactness at \( H^1(G, C) \) and concludes the proof. \( \square \)

### 2.3 Galois Cohomology

The largest Galois extension of any field \( k \) is the separable closure \( k_s \), the union \( \cup L_i \) of the partially ordered set \( \{L_i : i \in I\} \) of all finite Galois field extensions of \( k \).
Theorem 2.7. [30. Theorem 6.11.1] The Galois group \( \text{Gal}(k_s/k) \) is isomorphic to the inverse limit \( \varprojlim \text{Gal}(L_i/k) \) of finite groups.

Let \( L \) be a finite Galois extension of \( k \). Denote by \( G_L \) and \( \Gamma \) the Galois groups \( \text{Gal}(L/k) \) and \( \text{Gal}(k_s/k) \) respectively. If \( A \) is a \( \Gamma \)-module we define

\[
H^n(\Gamma, A) = \varprojlim H^n(G_L, A(L))
\]

the \( n^{th} \) cohomology of \( \Gamma \) with coefficients in \( A \). Usually we denote \( H^n(\Gamma, A) \) by \( H^n(k, A) \). If \( A \) is not abelian only \( H^0(k, A) \) and \( H^1(k, A) \) are defined.

Our goal is to describe \( H^2(k, k_s) = \varprojlim H^2(G_L, L) \).

Definition 2.8. The relative Brauer group \( \text{Br}(L/k) \) is the set of all central simple \( k \)-algebras \( A \) that split over \( L \), that is, \( A \otimes_k L \cong M_n(L) \). \( n = [L : k] \).

Hence the Brauer group of \( k \) defined in 1.40 is:

\[
\text{Br}(k) = \bigcup_{i \in I} \text{Br}(L_i/k).
\]

Theorem 2.9. Let \( L \) be a finite Galois extension of \( k \). then

\[
\text{Br}(L/k) \cong H^2(G_L, L).
\]

Sketch of the Proof. Define a vector space \( A \) over \( L \) with basis \( \{a_\sigma : \sigma \in G_L\} \). Hence the elements of \( A \) can be written uniquely in the form \( \sum_{\sigma \in G_L} c_\sigma a_\sigma \) with \( c_\sigma \in L \). Now given a 2-cocycle \( \nu \in H^2(G_L, L) \) we can introduce a multiplication in \( A \) with relations

\[
a_\sigma a_\tau = \nu(\sigma, \tau) a_{\sigma\tau} \quad \text{and} \quad a_\sigma c = \sigma(c) a_\sigma \quad \text{for all} \ c \in L.
\]

The 2-cocycle condition gives the associativity of this product. Denote by \( A(\nu) \) the algebra obtained. The following facts are not trivial. We refer to [7. Section 8.4] for the proofs.
(1) The algebra $A(\psi)$ is a central simple algebra over $k$.

(2) $A(\psi) \otimes_k A(\varphi) \cong A(\psi + \varphi) \otimes_k M_n(k)$.

(3) The trivial 2-cocycle yields the matrix algebra $M_n(k)$, where $n = [L : k]$.

(4) $A(\psi) \cong A(\varphi)$ if and only if $\psi$ and $\varphi$ differ by a coboundary.

(5) Every central simple algebra is isomorphic to an algebra $A(\psi)$ for some cocycle $\psi \in H^2(G_L, \hat{L})$.

Hence we can conclude that the correspondence $\psi \mapsto A(\psi)$ defines a group isomorphism

$$H^2(G_L, \hat{L}) \cong \text{Br}(L/k)$$

as desired. □

As an immediate consequence of the above theorem we have the cohomological interpretation of the Brauer group.

**Corollary 2.10.** The Brauer group $\text{Br}(k)$ of $k$ is isomorphic to $H^2(k, \hat{k}_s)$. □

**Notation** We denote by $\text{Br}_n(k)$ the subgroup of $\text{Br}(k)$ consisting of elements $x$ such that $n \cdot x = 0$.

Let $L$ be a finite Galois extension of $k$. Denote by $\text{GL}_n(L)$ the group of invertible $n \times n$ matrices with entries in $L$. The Galois group $G_L$ acts on $\text{GL}_n(L)$, therefore $H^1(G_L, \text{GL}_n(L))$ can be defined.

**Proposition 2.11.** (Hilbert's 90) The cohomology set $H^1(G_L, \text{GL}_n(L))$ is trivial. In particular, $H^1(G_L, \hat{L})$ is trivial.

**Proof.** Consider a cocycle $\phi : G_L \to \text{GL}_n(L)$: by definition we have $\phi(gh) = \phi(g) \cdot g\phi(h)$ for all $g, h \in G_L$. Define $b(x) = \sum_{g \in G_L} \phi(g) \cdot g(x)$ for $x \in L^n$. We will show that the set $\{b(x) : x \in L^n\}$ generates $L^n$. For this, assume that a linear form
$u$ vanishes on all the $b(x)$. Then for any $y \in L$

$$0 = u(b(y)) = \sum_{g \in G_L} o(g)u(g(y)g(x)) = \sum_{g \in G_L} g(y)u(o(g)g(x)).$$

It follows that $u(o(g)g(x)) = 0$ for each $g \in G_L$, by the linear independence of characters, whence $u = 0$.

Now let $x_1, \ldots, x_n$ be vectors in $L^n$ such that $b(x_1), \ldots, b(x_n)$ are linearly independent. Let $c$ be the matrix sending the canonical basis to $x_1, \ldots, x_n$, then we obtain the invertible matrix $b = \sum_{g \in G_L} o(g)g(c)$. By making $h \in G_L$ act on this equation we get

$$h(b) = \sum_{g \in G_L} ho(g) \cdot (hg(c))$$

$$= \sum_{g \in G_L} o(h)^{-1} \cdot o(hg) \cdot (hg)(c)$$

$$= o(h)^{-1} \cdot b.$$ 

Hence $o(h) = b \cdot h(b)^{-1}$ for all $h \in G_L$, that is, $o$ is a coboundary. □

Let $\mu_n$ be the group of the $n^{th}$ roots of unity in $k$ and assume that $\gcd(n, \text{Char}(k)) = 1$. Consider the following exact sequence

$$1 \rightarrow \mu_n \rightarrow k^n \rightarrow k_s \rightarrow 1.$$ 

where the map $n$ is given by $a \mapsto a^n$. By taking cohomology we get the following exact sequence of groups

$$1 \rightarrow \hat{k} \rightarrow k \rightarrow H^1(k, \mu_n) \rightarrow H^1(k, \hat{k}_s)$$

$$\rightarrow H^1(k, \hat{k}_s)^n \rightarrow H^2(k, \mu_n) \rightarrow H^2(k, \hat{k}_s)^n \rightarrow H^2(k, \hat{k}_s).$$

Using Hilbert's 90 Theorem 2.11 and the exactness of the above sequence we have the following two corollaries.

**Corollary 2.12.** For $\mu_n$ and $k$, as before, we have

$$H^1(k, \mu_n) = \hat{k}/k^n.$$ 

34
Corollary 2.13. The group $H^2(k, \mu_n)$ is isomorphic to $Br_n(k)$, which is the kernel of the map

$$H^2(k, \hat{k}_s) \xrightarrow{\cong} H^2(k, \hat{k}_s).$$

Remark 2.14. (1) From Corollary 2.12 an element $a \in \hat{k}/\hat{k}^2$ can be viewed as an element of $H^1(k, \mathbb{Z}/2)$. More explicitly, if $\lambda$ is the square root of $a$ in $k_s$, we define $(a)(\sigma) \in \mathbb{Z}/2$ by the following $\sigma(\lambda) = (-1)^{(a)(\sigma)}\lambda$ for all $\sigma \in \Gamma$. The cocycle $(a) : \Gamma \to \mathbb{Z}/2$ corresponds to the element $a \in \hat{k}/\hat{k}^2$.

(2) The quaternion algebra $(a, b)$ is an element of order two in $Br(k) = H^2(k, \hat{k}_s)$. Thus $(a, b) \in H^2(k, \mu_2).$ In fact, we can view $(a, b)$ as being the cup product between the 1-cocycles $(a, b) \in H^1(k, \mu_2) = H^1(k, \mathbb{Z}/2).$ More explicitly, the cup product $(a) \cdot (b) \in H^2(k, \mu_2)$ is defined by $(a) \cdot (b)(\sigma, \tau) = (-1)^{(a)(\sigma)(b)(\tau)}$ for all $\sigma, \tau \in \Gamma$. One can check that the algebra associated with the 2-cocycle $(a) \cdot (b)$ is exactly $(a, b)$.

2.4 Galois Descent

To describe other cohomology groups which are important in our work, we need the notion of "Galois descent".

Definition 2.15. Let $V$ be a vector space over $k$ and $V^*$ be the dual of $V$. Denote $T^n(V) = V \otimes \cdots \otimes V$ ($n$ times). A tensor of type $(p, q)$ in $V$ is an element $x \in T^p_q(V) = T^p(V) \otimes T^q(V^*)$. The pairs $(V, x)$ and $(V', x')$ are called $k$-isomorphic if there is a $k$-linear isomorphism $f : V \to V'$ such that $f(x) = x'$.

Example 2.16. 1) A bilinear form defined on $V$ is an element in $V^* \otimes V^*$. hence it is a tensor of type $(0, 2)$ in $V$. Here $k$-isomorphic means isometric over $k$.

2) Let $A$ be a $k$-algebra. The product in $A$ is an element of $A^* \otimes A^* \otimes A$. Now if we fix an element $a \in A$, then we get an element in $A^* \otimes A^* \otimes A \otimes A$. Hence the product in $A$ together with the fixed point is a tensor of type $(2, 2)$. Denote
this tensor just by $a$. The pairs $(A, a)$ and $(B, b)$ are $k$-isomorphic if there is a $k$-algebra isomorphism $f : A \to B$ such that $f(a) = b$ (compare with 1.48).

For any Galois extension $L$ of $k$ with $G = \text{Gal}(L/k)$ we can consider $V_L = V \otimes_k L$ and $x_L = x \otimes 1 \in T_L^p(V_L) = T^p_q(V) \otimes_k L$. We say that $(V, x)$ and $(V', x')$ are $L$-isomorphic if they become isomorphic over $L$, that is, if there is a $L$-isomorphism $f : V_L \to V'_L$ such that $f(x_L) = x'_L$. For the extension of a bilinear space see section 1.1.

Fix a Galois extension $L$ of $k$. Denote by $E(V, x)$ the set of $k$-isomorphic classes of pairs $(V', x')$ that are $L$-isomorphic to $(V, x)$. Let $\text{Aut}(V_L, x_L)$ be the group of $L$-automorphisms of $(V_L, x_L)$. We want to compare $E(V, x)$ with $H^1(G, \text{Aut}(V_L, x_L))$. For this we need to define the action of $G$ on $\text{Aut}(V_L, x_L)$. First, $G$ acts on $V_L$ by $g(v \otimes \lambda) = v \otimes g\lambda$. Given $f : V_L \to V'_L$, define

$$g(f)(v) = g \cdot f(g^{-1}v) \text{ for all } g \in G.$$ 

This defines the action of $G$ on $\text{Aut}(V_L, x_L)$.

Let $(V', x') \in E(V, x)$, then there is a $L$-isomorphism $f : V_L \to V'_L$. Define $\phi : G \to \text{Aut}(V_L, x_L)$ as follows:

$$\phi(g) = f^{-1} \circ g(f) \text{ for all } g \in G.$$ 

One can easily check that $\phi$ is a cocycle and its class in $H^1(G, \text{Aut}(V_L, x_L))$ does not depend on the chosen $L$-isomorphism $f$. Hence we have a map

$$\varphi : E(V, x) \to H^1(G, \text{Aut}(V_L, x_L)).$$

**Proposition 2.17.** The map $\varphi$ above is a bijection.

*Proof.* Injectivity. Assume that $\varphi(V_1, x_1) = \varphi(V_2, x_2)$, then there are $L$-isomorphisms $f_1 : V_L \to (V_1)_L$ and $f_2 : V_L \to (V_2)_L$ such that $f_1^{-1}g(f_1) = f_2^{-1}g(f_2)$ for all $g \in G$. 

36

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Hence $g(f_2f_1^{-1}) = f_2f_1^{-1}$ for all $g \in G$. Thus the map $f_2f_1^{-1}$ is a $k$-isomorphism between $(V_1, x_1)$ and $(V_2, x_2)$.

**Surjectivity.** Consider $\varphi \in H^1(G, \text{Aut}(V_L, x_L))$. Since $\text{Aut}(V_L, x_L) \subseteq \text{GL}(V_L)$, by 2.11, $\varphi$ is a coboundary. Hence there is a $L$-isomorphism $f : V_L \rightarrow V_L$ such that

$$\varphi(g) = f^{-1} \circ g(f) \quad \text{for all} \quad g \in G.$$  

Extend $f$ to $T^p_q(V_L)$. Define $x' = f(x)$. We claim that $x'$ lies in $T^p_q(V)$, that is, $x'$ is fixed by $G$; indeed.

$$g(x') = g(f)(g(x)) = g(f)(x) = f \circ \varphi(g)(x) = f(x) = x'.$$

Hence $(V, x') \in E(V, x)$ and clearly $\varphi(V, x') = \varphi$. □

**Corollary 2.18.** Take $L = k_s$ and consider the pointed algebra $(M_n(k), b)$. Hence $H^1(k, \text{Aut}(M_n(k_s), b))$ is in one-to-one correspondence with the isomorphism classes of twists of $(M_n(k), b)$.

**Corollary 2.19.** Let $q$ be a quadratic form over $k$ and let $q_{k_s}$ be its extension to $k_s$. Then the set $H^1(k, \text{O}(q_{k_s}))$ is in one-to-one correspondence with the set of isometric classes of quadratic forms $q'$ over $k$ of the same dimension as $q$.

**Proof.** Note that $\text{Aut}(V_{k_s}, (b_q)_{k_s}) = \text{O}(q_{k_s})$. Since over the separable closure all the forms of the same dimension as $q$ become isometric, we have that all such forms are in $E(V, b_q)$. □

**Corollary 2.20.** Let $(V, q)$ be an $n$-dimensional quadratic space over $k$. The set of isometric classes of $n$-dimensional quadratic forms $q'$ over $k$ of the same determinant as $q$ is in one-to-one correspondence with the set $H^1(k, \text{SO}(q_{k_s}))$.

**Proof.** If $q$ and $q'$ have the same discriminant and become isometric over $k_s$, then the $k_s$-isomorphism $f : V_{k_s} \rightarrow V_{k_s}'$ has determinant in $k$. Hence the determinant of $\varphi(g) = f^{-1} \circ g(f)$ is 1. This implies that $\text{Aut}(V_{k_s}, q_{k_s}) = \text{SO}(q_{k_s})$. □
2.5 Springer's spinor interpretation of the Hasse invariant

Let us consider again the exact sequence

\[ 1 \to k \to P(q) \xrightarrow{\alpha} O(q) \to 1 \]

obtained in Proposition 1.25, but now we consider this sequence over \( k_s \). So \( \Gamma \) acts on this sequence. Since \( \hat{k}_s \) is central in \( P(q_{k_s}) \), the sequence of cohomology sets

\[ H^1(k, P(q_{k_s})) \xrightarrow{\alpha} H^1(k, O(q_{k_s})) \xrightarrow{\partial} H^2(k, \hat{k}_s) \]

is exact (see Proposition 2.6). We will omit the indices \( k_s \).

In [26] Springer gives a formula for the connecting homomorphism \( \partial \) in terms of Hasse invariants and determinants. We shall present a slightly different proof and include a minor correction of his formula.

First we recall how \( \partial \) is defined. Consider \( \phi : \Gamma \to O(q) \) and for each \( \sigma \in \Gamma \) consider an element \( s(\sigma) \) in \( P(q) \) such that \( \alpha(s(\sigma)) = \phi(\sigma) \). Then define \( \partial(\phi) \) as \( \psi : \Gamma \times \Gamma \to \hat{k}_s \) given by

\[ \psi(\sigma, \sigma') = s(\sigma')s(\sigma)^{-1}s(\sigma')^{-1} \text{ for all } \sigma, \sigma' \in \Gamma. \]  

(2.4)

**Remark 2.21.** The cocycle \( \phi \in H^1(k, O(q)) \) corresponds to a quadratic form \( q_1 \) of the same dimension as \( q \) (according to 2.19). Hence we can say that \( \partial \) takes \( q_1 \) into \( \psi \), which is an element of \( Br(k) \).

**Theorem 2.22.** Let \( q \) and \( q_1 \) be quadratic forms over \( k \) of the same dimension. Then

\[ \partial(q_1) = h(q)h(q_1)(\det(q) - \det(q_1)). \]  

(2.5)

where \( h \) denotes the Hasse invariant defined in 1.18.

38
Proof. Let \( q = \langle a_1, \ldots, a_n \rangle \) and \( q_1 = \langle b_1, \ldots, b_n \rangle \) with respect to the orthogonal bases \( \{e_1, \ldots, e_n\} \) and \( \{f_1, \ldots, f_n\} \) respectively. From Lemma 1.7, \( q \) and \( q_1 \) become isometric over \( k_s \). This isometry \( t \) is given by \( t(e_i) = c_i f_i \) where \( c_i \) is the square root of \( a_i^{-1} b_i \) in \( k_s \). Hence the cocycle \( \phi : \Gamma \rightarrow O(q) \) that corresponds to \( q_1 \) is given by

\[
\phi(\sigma)(e_i) = t^{-1}(\sigma c_i f_i) = (-1)^{\varepsilon_i(\sigma)} e_i.
\]

where \( \varepsilon_i(\sigma) \) is defined by \( \sigma(c_i) = (-1)^{\varepsilon_i(\sigma)} c_i \). We can write \( \phi(\sigma) \) as a product of reflections. More explicitly, denote by \( \tau_i \) the reflection defined by \( e_i \), that is, \( \tau_i(x) = x - \frac{b(x, e_i)}{q(e_i)} e_i \). Since \( \tau_i(e_i) = -e_i \) and \( \tau_i(e_j) = e_j \) for \( i \neq j \), we have \( \phi(\sigma) = \tau_1^{\varepsilon_1(\sigma)} \tau_2^{\varepsilon_2(\sigma)} \cdots \tau_n^{\varepsilon_n(\sigma)} \). It follows easily from the proof of Lemma 1.24 that \( s(\sigma) = e_1^{\varepsilon_1(\sigma)} \cdots e_n^{\varepsilon_n(\sigma)} \) is in the preimage of \( \phi(\sigma) \) by \( \alpha \). Hence \( \partial(q_1) \) (or \( \partial(\phi) \)) in \( H^2(k, k_s) \) is given by the class of \( \nu(\sigma, \sigma') = s(\sigma' \sigma) s^{-1}(\sigma' \sigma) \) for all \( \sigma, \sigma' \in \Gamma \). Now by direct computation and using the facts \( e_i^2 = a_i \) and \( e_i e_j = -e_j e_i \), one gets:

\[
\partial(q_1) = \nu(\sigma, \sigma') = (-1)^{\sum_{i < j} \varepsilon_i(\sigma) \varepsilon_j(\sigma')} \prod_{\varepsilon_i(\sigma) = \varepsilon_j(\sigma') = 1} a_i.
\]

Notice that

\[
(-1)^{\sum_{i < j} \varepsilon_i(\sigma) \varepsilon_j(\sigma')} = \prod_{i < j} (-1)^{\varepsilon_i(\sigma) \varepsilon_j(\sigma')} = \prod_{i < j} (a_i b_i a_j b_j).
\]

which is a product of quaternion algebras. The last equality follows from Remark 2.14.

We need to define a new cohomology class in \( H^2(k, k_s) \). Consider \( \alpha, \beta \in \hat{k} \) and let \( \lambda \) be the square root of \( \alpha \) in \( k_s \). Define

\[
\{\alpha, \beta\}(\sigma, \sigma') = \begin{cases} 
\beta & \text{if } \sigma(\lambda) = -\lambda \text{ and } \sigma'(\lambda) = -\lambda \\
1 & \text{otherwise.}
\end{cases}
\]
Hence

\[ \partial(q_1) = \prod_{i<j}(a_i b_j a_j b_i) \prod_{i=1}^{n}(a_i b_i a_i). \]  

(2.6)

We claim that \( \{a_i b_i a_i\} = (a_i b_i a_i) \). Assuming the claim we get

\[ \partial(q_1) = \prod_{i<j}(a_i b_i a_j b_j) \prod_{i=1}^{n}(a_i b_i a_i). \]

Now using 1.41 we have the following:

\[
\partial(q_1) = \prod_{i<j}(a_i a_j) \prod_{i<j}(b_i b_j) \prod_{i<j}(a_i b_j a_i b_j) \prod_{i=1}^{n}(a_i b_i a_i) = \prod_{i=1}^{n}(a_i a_i a_i)
\]

\[
= h(q)h(q_1) \prod_{i<j}(a_i b_j) \prod_{i=1}^{n}(a_i, -1)
\]

\[
= h(q)h(q_1)(\det(q) -\det(q_1))(-\det(q_1))
\]

We still need to prove our claim. For this we are going to use the obvious fact that if \( q_1 \cong q_2 \) then \( \partial(q_1) = \partial(q_2) \). We shall show that \( \{\alpha J\} = (\alpha J) \) for all \( \alpha J \in J \). Take \( q = (1 \alpha > \) and \( q_1 = (1 \alpha\alpha) > \). Since \( (1 \alpha J) = \{1, 1\} = 1 \), we get from (2.6) \( \partial(q_1) = (1 \alpha J) \{1, 1\} \{\alpha J, \alpha\} = (\alpha J, \alpha\}. \) Now take \( q_2 = (1 \alpha\alpha) > \).

Then we have \( \partial(q_2) = (1 \alpha J) \{1, 1\} \{\alpha J, \alpha\} = (\alpha J, \alpha\}. \) Since \( \{1, 1\} = 1 \), it follows that \( \{\alpha J, \alpha\} = (1 \alpha J) \{\alpha, \alpha\}. \) Now take \( \alpha = \alpha J \). Then \( \{\alpha^2, \alpha\} = (\alpha, \alpha) \{\alpha, \alpha\}. \) But \( \{\alpha^2, \alpha\} = 1 \) and we have \( \{\alpha, \alpha\} = (\alpha, \alpha)^{-1} = (\alpha, \alpha). \) Hence \( \{\alpha J, \alpha\} = (1 \alpha J) \{\alpha, \alpha\} = (\alpha J, \alpha\}. \) Now simply take \( \alpha = \alpha \) and \( J = 1 \). Then we have that \( \{\alpha J\} = (\alpha J) \) as desired. □

**Remark 2.23.** In our notation, the formula obtained by Springer should read:

\[ \partial(q_1) = h(q)h(q_1)(-\det(q) \cdot \det(q_1)) \]

(the minus sign is missing in his formula). Note that even with this correction Springer’s formula is different from (2.5). The reason is that Springer’s definition of the Hasse invariant is different from the one we are taken.
Chapter 3
Representation of Linear Algebraic Groups

3.1 Basic Concepts and Examples

Let $K$ be an algebraically closed field of arbitrary characteristic.

**Definition 3.1.** An *algebraic group* is an algebraic variety $G$ over $K$ together with:

(i) a distinguished element $e \in G$;

(ii) a morphism $\mu : G \times G \to G$, denoted by $\mu(x, y) = xy$;

(iii) a morphism $i : G \to G$, denoted by $i(x) = x^{-1}$.

with respect to which $G$ is a group.

An algebraic group whose underlying variety is affine is called an *affine algebraic group*.

**Example 3.2.**

1. The *additive group* $G_a$ is the affine line $\mathbb{A}^1$ with addition as the group operation.

2. The *general linear group* $GL_n$ is the group of all $n \times n$ invertible matrices with entries in the field $K$. Viewed as an affine variety, $GL_n$ has its algebra of polynomial functions generated by the $n^2$ coordinate functions $T_{ij}$ along with $1/\det(T_{ij})$.

3. The *multiplicative group* $GL_1$ is just a particular case of the previous example and can be identified with $K^*$.

4. The *special linear group* $SL_n$ consists of the matrices in $GL_n$ of determinant 1.
5. The symplectic group $\text{Sp}_{2n}$ consists of all $x \in \text{GL}_{2n}$ satisfying $'xJx = J$ where $'x$ = transpose of $x$ and

$$J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$ 

6. Let $Q$ be a quadratic form of rank $n$ over $\mathbb{K}$ (char $\mathbb{K} \neq 2$). If $B$ is a symmetric matrix representing $Q$, then

$$\text{SO}(Q) = \{x \in \text{SL}_n : 'xBx = B\}$$

is called the special orthogonal group of $Q$. When $Q$ is the unitary form ($Q = \langle 1, \ldots, 1 \rangle$), we denote $\text{SO}(Q)$ by $\text{SO}_n$.

7. Any closed subgroup of $\text{GL}_n$ is again an affine algebraic group. For example, the subgroup of upper triangular matrices

$$\mathcal{T}_n = \{x \in \text{GL}_n : x_{ij} = 0 \text{ for } j < i\}.$$ 

Remark 3.3. The groups $\text{SL}_n$, $\text{Sp}_{2n}$, and $\text{SO}(Q)$ are examples of the so-called classical groups.

Affine algebraic groups that are subgroups of some $\text{GL}_n$ are easier to handle, since we can use the special properties of matrices. The next theorem shows that all affine algebraic groups have this property.

Theorem 3.4. [5. §8.6] Every affine algebraic group is isomorphic to a closed subgroup of some $\text{GL}_n$.

Definition 3.5. We call linear algebraic groups the algebraic groups that are subgroups of some $\text{GL}_n$. Since we will consider only linear algebraic groups the word "linear" will be omitted.
**Definition 3.6.** The connected (irreducible) component of $e$ in an algebraic group $G$ is called the *identity component* and is denoted by $G^0$.

If $G = G^0$, then we say that $G$ is *connected*.

**Proposition 3.7.** [5. §7.3] Let $G$ be an algebraic group.

(a) $G^0$ is a normal subgroup of finite index in $G$, whose cosets are the connected, as well as irreducible, components of $G$.

(b) Every closed subgroup of finite index in $G$ contains $G^0$.

**Definition 3.8.** A morphism of varieties $\varphi : G \to G'$ is a *morphism of algebraic groups* if it is also a group homomorphism.

**Proposition 3.9.** [5. §7.4] Let $\varphi : G \to G'$ be a morphism of algebraic groups.

Then,

(a) $\ker \varphi$ is a closed subgroup of $G$.

(b) $\operatorname{Im} \varphi$ is a closed subgroup of $G'$.

(c) $\varphi(G^0) = \varphi(G)^0$.

(d) $\dim G = \dim \ker \varphi + \dim \operatorname{Im} \varphi$.

Let $V$ be a $n$-dimensional vector space over $K$. The group $\operatorname{GL}(V)$ of all invertible endomorphisms of $V$ can be identified with $\operatorname{GL}_n$ by choosing a basis of $V$.

A morphism $\varphi : G \to \operatorname{GL}(V)$ of algebraic groups is called a *rational representation*.

**Definition 3.10.** Let $V^*$ be the dual vector space of $V$. The *dual* or *contragredient* representation $\varphi' : G \to \operatorname{GL}(V^*)$ is defined by

$$\varphi'(g)(\lambda) = \lambda \circ \varphi(g)^{-1} \quad \text{for } g \in G \text{ and } \lambda \in V^*.$$ 

If $\varphi$ is isomorphic to $\varphi'$, we say that $\varphi$ is *self-dual*.
3.2 Lie Algebra of an Algebraic Group

Definition 3.11. A vector space \( L \) over \( K \), with an operation \( L \times L \to L \) denoted \( (x, y) \mapsto [x, y] \) and called the bracket operation, is called a Lie algebra over \( K \) if the following conditions are satisfied:

1. The bracket operation is \( K \)-bilinear.
2. \([x, x] = 0\) for all \( x \in L \).
3. \([x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0\) \( (x, y, z \in L) \).

Any subspace of an associative \( K \)-algebra which is closed under the bracket operation

\[[x, y] = xy - yx\]

is a Lie algebra over \( K \). An example to keep in mind is the associative algebra \( M_n(K) \).

Let \( G \) be an algebraic group over \( K \). A derivation of \( K[G] \) is a \( K \)-linear map \( \delta : K[G] \to K[G] \) which satisfies

\[\delta(xy) = x\delta(y) + \delta(x)y.\]

We denote by \( \text{Der} K[G] \) the set of all derivations of \( K[G] \). One can easily check that if \( \delta, \delta' \in \text{Der} K[G] \), then \([\delta, \delta'] = \delta\delta' - \delta'\delta\) is again a derivation of \( K[G] \). Hence \( \text{Der} K[G] \) is a Lie algebra. The action of \( G \) on \( K[G] \) given by \((\lambda_x f)(y) = f(x^{-1}y)\) for all \( x, y \in G \) is called left translation.

Definition 3.12. Let \( \mathcal{L}(G) = \{\delta \in \text{Der} K[G] : \delta\lambda_x = \lambda_x\delta \text{ for all } x \in G\} \). This is a subspace of \( \text{Der} K[G] \). Since the bracket of two derivations in \( \mathcal{L}(G) \) is again a derivation in \( \mathcal{L}(G) \), \( \mathcal{L}(G) \) is also a Lie algebra. We call \( \mathcal{L}(G) \) the Lie algebra of \( G \).

Fix an element \( x \in G \) and consider the rational functions \( f \) which are defined at \( x \), that is, those which have an expression \( f = g/h \) \((g, h \in K[G]) \) with \( h(x) \neq 0\).
These functions form a subring of the function field \( K(G) \) including \( K'[G] \). This subring is called the *local ring of \( x \) on \( G \) and denoted \( \mathfrak{O}_x \). The unique maximal ideal \( \mathfrak{m}_x \) of \( \mathfrak{O}_x \) consists of all rational functions \( g/h \in \mathfrak{O}_x \) such that \( g(x) = 0 \) and \( h(x) \neq 0 \). We define the *tangent space* \( \mathcal{T}_x(G) \) of \( G \) at \( x \) as being the dual vector space \( (\mathfrak{m}_x/\mathfrak{m}_x^2)^* \) over \( K = \mathcal{O}_{\mathfrak{m}_x} \) (see [5. §5] for more details).

We shall show that \( \mathcal{L}(G) \) can be identified with \( \mathcal{T}_e(G) \), where \( e \) is the identity of \( G \). For this we define \( \theta : \mathcal{L}(G) \rightarrow \mathcal{T}_e(G) \) by \( \theta(\delta)(f) = (\delta f)(e) \) for \( \delta \in \mathcal{L}(G) \) and \( f \in K'[G] \).

**Theorem 3.13.** [5. Theorem 9.1] Let \( G \) be an algebraic group. Let \( \mathcal{L}(G) \) and \( \mathcal{T}_e(G) \) be as above. Then \( \theta : \mathcal{L}(G) \rightarrow \mathcal{T}_e(G) \) is a vector space isomorphism (functorial in \( G \)).

The tangent space \( \mathcal{T}_e(G) \) is made into a Lie algebra by transporting the bracket operation of \( \mathcal{L}(G) \) via \( \theta \). Henceforth we identify \( \mathcal{L}(G) \) with \( \mathcal{T}_e(G) \).

The next corollary is an immediate consequence of the properties of \( \mathcal{T}_e(G) \) [5. §5].

**Corollary 3.14.** We have \( \mathcal{L}(G) = \mathcal{L}(G^0) \) and \( \dim \mathcal{L}(G) = \dim G \).

**Example 3.15.** 1) If \( G = \text{GL}_n(K) \), then \( \mathcal{L}(G) = \mathcal{M}_n(K) \) (\( \text{GL}_n \) is Zariski open in \( \mathcal{M}_n \)).

2) The Lie algebras of the classical groups \( \text{SL}_n, \text{Sp}_{2n}, \) and \( \text{SO}(Q) \) are subalgebras of the corresponding matrix algebras. More precisely:

\[
\mathcal{L}(\text{SL}_n) = \mathfrak{sl}_n = \{X \in \mathcal{M}_n : \text{Tr}X = 0\}
\]

\[
\mathcal{L}(\text{Sp}_{2n}) = \mathfrak{sp}_{2n} = \{X \in \mathcal{M}_{2n} : \, ^tXJ = -JX\}
\]

\[
\mathcal{L}(\text{SO}(Q)) = \mathfrak{so}(Q) = \{X \in \mathcal{M}_n : \, ^tXB = -BX\}
\]

where \( J \) and \( B \) are as in Example 3.2.
If $G \subset \text{GL}_n(K)$ then for any $g \in G$ we have $g\mathcal{L}(G)g^{-1} = \mathcal{L}(G)$. Hence we can define a morphism of algebraic groups

$$\text{Ad} : G \to \text{GL}(\mathcal{L}(G)) \text{ by } g \mapsto \varphi_g.$$ 

where $\varphi_g(x) = gxg^{-1}$ for all $x \in \mathcal{L}(G)$. This morphism is called the adjoint representation of $G$.

### 3.3 Diagonalizable Groups and Algebraic Tori

An algebraic group $G$ is diagonalizable if it is isomorphic to a closed subgroup of the group $D_n$ of diagonal matrices for some $n$. If $G$ is isomorphic to some $D_n$, then $G$ is called an algebraic torus. It can be shown that any connected diagonalizable group is an algebraic torus. A maximal torus of $G$ is a torus of maximal dimension in $G$.

A character of an algebraic group $G$ is a morphism of algebraic groups $\chi : G \to \text{GL}_1$ where $\text{GL}_1$ is the multiplicative group. With the operation $(\chi_1 \chi_2)(x) = \chi_1(x)\chi_2(x)$, the characters of $G$ form an abelian group. We denote this by $X(G)$. For example: If $\chi : \text{GL}_1 \to \text{GL}_1$ is a morphism, then $\chi(t) = t^m$ for some $m \in \mathbb{Z}$. Hence $X(\text{GL}_1) \cong \mathbb{Z}$.

If $g : G \to G'$ is a morphism of algebraic groups, then we shall denote by $g^*$ the dual homomorphism $g^* : X(G') \to X(G)$ defined by $g^*(\chi) = \chi \circ g$.

**Lemma 3.16.** If $G$ is a connected algebraic group, then $X(G)$ is torsion-free. In particular, if $T$ is a $n$-dimensional torus, then $X(T) \cong \mathbb{Z}^n$.

**Proof.** If $\chi \in X(G)$, then $\chi(G) \subset \text{GL}_1$ is connected. But the only connected subgroups of $\text{GL}_1$ are $\{0\}$ and $\text{GL}_1$. Thus for $n > 0$ $n\chi \neq 0$, unless $\chi = 0$. Since $T \cong D_n \cong \text{GL}_1 \times \cdots \times \text{GL}_1$ ($n$ times), we have $X(T) = X(\text{GL}_1)^n = \mathbb{Z}^n$. □
3.4 Jordan-Chevalley Decomposition

Let $V$ be a finite dimensional vector space over $K$. An element $a \in V$ is nilpotent if $a^n = 0$ for some $n$ (all the eigenvalues of $a$ are 0). If $a - 1$ is nilpotent (all the eigenvalues of $a$ are 1), then $a$ is called unipotent.

If the minimal polynomial of $a$ has distinct roots ($a$ is diagonalizable over $K$), then $a$ is called semisimple.

Lemma 3.17. [1. Proposition 4.2] Let $a \in \text{End}(V)$.

(a) There exist unique $a_s$ and $a_n$ in $\text{End}(V)$ such that $a = a_s + a_n$. $a_s$ is semisimple. $a_n$ is nilpotent. and $a_s a_n = a_n a_s$.

(b) There exist monic polynomials $p(T), q(T)$ in one variable. such that $a_s = p(a)$ and $a_n = q(a)$. In particular. $a_s$ and $a_n$ commute with any endomorphism of $V$ that commutes with $a$.

(c) If $A \subset B \subset V$ are subspaces such that $aB \subset A$. then $a_s B \subset A$ and $a_n B \subset A$.

The decomposition of $a \in \text{End}(V)$ given by the above lemma is called the (additive) Jordan-Chevalley decomposition of $a$.

3.5 Reductive Groups

Definition 3.18. The maximal connected solvable normal subgroup of $G$ is called the radical of $G$, denoted by $R(G)$. If $G$ is connected and $R(G) = \{e\}$, we say that $G$ is semisimple. Equivalently, $G$ is semisimple if it has no closed connected commutative normal subgroups except $\{e\}$. An important example is $\text{SL}_n(K)$.

The subgroup of $R(G)$ consisting of all its unipotent elements is the unipotent radical of $G$, denoted by $R_u(G)$. A connected group $G$ is said to be reductive if $R_u(G) = \{e\}$. We have $\text{GL}_n(K)$, any torus, and any semisimple group as examples of reductive groups.
Theorem 3.19. [17. Theorem 2.4] Let $G$ be a reductive group. Then

1. $R(G) = Z(G)^0$ is a torus.
2. The commutator subgroup $H = (G, G)$ is a semisimple group.
3. $G = H \cdot Z(G)^0$ is an almost direct product ($H \cap Z(G)^0$ is finite).

3.6 Representations

In this section $G$ denotes a reductive algebraic group and $T$ a maximal torus of $G$.

Definition 3.20. Let $\rho : G \rightarrow \text{GL}(V)$ be a rational representation of $G$. For $\alpha \in X(T)$ let

$$V_{\alpha} = \{ v \in V : \rho(t)v = \alpha(t)v \ \text{for all} \ t \in T \}.$$ 

If the subspace $V_{\alpha}$ is not $\{0\}$, we say $\alpha \in X(T)$ is a weight of $\rho$ relative to $T$. The integer $m_{\alpha} = \dim(V_{\alpha})$ is called the multiplicity of $\alpha$.

Since $\rho(T)$ is diagonalizable in $\text{GL}(V)$, we can write

$$V = \bigoplus_{\alpha \in X(T)} V_{\alpha}$$

(see [27. 2.5.2]). This is called the weight decomposition of $\rho$ relative to $T$.

In particular, when $\rho : G \rightarrow \text{GL}(\mathcal{L}(G))$ is the adjoint representation (defined at the end of section 3.2), the nonzero weights of $\rho$ relative to $T$ are called the roots of $G$ relative to $T$. We denote this set by $\Phi(G, T)$.

We will see that if $G$ is semisimple, then $\Phi(G, T)$ is an abstract root system in $X(T) \otimes \mathbb{R}$, as defined in [5. pg 229]. We will now review this definition.

Definition 3.21. Let $V$ be a finite dimensional vector space over $\mathbb{R}$. An abstract root system in $V$ is a subset $\Psi$ of $V$ satisfying:

1. $\Psi$ is finite, spans $V$, and does not contain $0$.
2. If $\alpha \in \Psi$, then the only multiples of $\alpha$ in $\Psi$ are $\pm \alpha$.  

48
(3) If \( \alpha \in \Psi \), there is a reflection \( \tau_\alpha \) relative to \( \alpha \) which leaves \( \Psi \) stable.

(4) If \( \alpha, \beta \in \Psi \), then \( \tau_\alpha(\beta) = \beta \) is an integral multiple of \( \alpha \).

Since \( \Psi \) is a finite spanning set of \( V \), there is at most one reflection relative to \( \alpha \) leaving \( \Psi \) stable. Hence (4) is unambiguous. The rank of \( \Psi \) is the dimension of \( V \).

The group \( W(\Psi) \subset \text{GL}(V) \) generated by the \( \tau_\alpha \) is finite and is called Weyl group of \( \Psi \).

**Theorem 3.22.** [5. Theorem 27.1] Let \( G \) be semisimple and \( T \) a fixed maximal torus. Define \( V = X(T) \otimes \mathbb{Q} \). then \( \Phi(G, T) \) is an abstract root system in \( V \).

**Remark 3.23.** Since the roots of \( G \) and \( (G, G) \) (or \( G/Z(G)^0 \)) are in natural 1-1 correspondence, there is no difficulty about treating an arbitrary reductive group (we can use 3.19 (3)).

**Notation** There is an inner product on \( V \) denoted by \( (\alpha, \beta) \). Relative to this the reflection \( \tau_\alpha \) is given by:

\[
\tau_\alpha(\beta) = \beta - 2\frac{(\beta, \alpha)}{(\alpha, \alpha)} \alpha.
\]

We denote \( 2\frac{(\beta, \alpha)}{(\alpha, \alpha)} \) by \( \langle \beta, \alpha \rangle \).

A subset \( \Delta \) of \( \Psi \) is called a base if \( \Delta = \{\alpha_1, \ldots, \alpha_l\} \) is a basis of \( V \) and each \( \alpha \in \Psi \) can be written as a linear combination \( \alpha = \sum c_i \alpha_i \), with the \( c_i \) integers all of the same sign. It can be shown that such bases do exist and are unique up to a unique element in \( W(\Psi) \) ([6. Theorem 10.1 and Theorem 10.3]).

One associates to a base \( \Delta \) of \( \Psi \) the so-called Dynkin diagram. This is a finite graph having \( \Delta \) as its set of vertices, each vertex supplied with suitable “weight”, and in which \( \alpha \) and \( \beta \) in \( \Delta \) are joined by \( \langle \alpha, \beta \rangle \) edges. It can be shown that the Dynkin diagram does not depend on the chosen base and it determines \( \Psi \) up to isomorphism.
The root system $Ψ$ is called *irreducible* if it cannot be partitioned into a union of two mutually orthogonal proper subsets. There are only nine possibilities of Dynkin diagrams of irreducible root systems: the four classical series $A_l, B_l, C_l,$ and $D_l$ and five exceptional systems $E_6, E_7, E_8, F_4,$ and $G_2$. See [6, §11 and §12] for a description of these Dynkin diagrams. Every root system is the disjoint union of irreducible root systems in suitable subspaces of $V$. Thus these diagrams give a complete classification of root systems.

The root systems of the classical groups $\text{SL}_{l+1}, \text{Sp}_{2l}, \text{SO}_{2l+1},$ and $\text{SO}_{2l}$ are of the type $A_l, C_l, B_l,$ and $D_l$ respectively. We refer to [1, §23] for these computations.

A vector $\lambda \in V$ is called an *abstract weight* provided all $<\lambda, \alpha>$ ($\alpha \in Ψ$) are integers. These vectors form a lattice $Λ$. The *root lattice*. $Λ_r$ spanned by $Ψ$ is a subgroup of $Λ$ of finite index. If $Δ = \{\alpha_1, \ldots, \alpha_l\}$ is a base of $Ψ$. $Λ$ has a corresponding basis of *fundamental weights* $\{\lambda_1, \ldots, \lambda_l\}$ for which $<\lambda_i, \alpha_j> = δ_{ij}$.

**Proposition 3.24.** [5, §31.1] *All weights of rational representations are abstract weights.*

From (3.4) we know that it is always possible to find an isomorphism of $G$ onto a closed subgroup of some $\text{GL}(V)$. The weights of this representation generate the group $X(T)$. Hence we have that

$$Λ_r \subset X(T) \subset Λ,$$

with finite indexes.

The quotient $Λ/X(T)$ is called the *fundamental group of $G$*, denoted $π(G)$. When $X(T) = Λ$ we say that $G$ is *simply connected*. At the other extreme if $X(T) = Λ_r$, then we say that $G$ is of *adjoint type.*
The structure of the quotient group $\Lambda/\Lambda_r$ is known for the irreducible root systems. We list some of them:

- $A_l : \mathbb{Z}/(l + 1)$
- $B_l, C_l : \mathbb{Z}/2$
- $D_l$ (l even): $\mathbb{Z}/2 \times \mathbb{Z}/2$
- $D_l$ (l odd) : $\mathbb{Z}/4$.

**Remark 3.25.** Root systems, bases, and fundamental weights are also well-known for the irreducible cases. They are completely described in tables, see [16. pg. 292].

The root systems which will be of interest to us are $D_l$ and $B_l$. In the following example we construct $D_l$ and $B_l$ based on [6. §12.1].

**Example 3.26.** Let $e_1, \ldots, e_l$ denote the canonical basis of $\mathbb{R}^l$. Denote by $I$ the lattice generated by this basis. Define $\Phi = \{ \alpha \in I : (\alpha, \alpha) = 2 \}$. It is easy to check that $\Phi$ is a root system in $V = \mathbb{R}^l$. Clearly we have

$$\Phi = \{ \pm(e_i \pm e_j), i \neq j \}.$$

A base of $\Phi$ is given by $\{ \alpha_1, \ldots, \alpha_l \}$ where

$$\alpha_i = e_i - e_{i+1}, \quad (i < l),$$

$$\alpha_l = e_{l-1} + e_l.$$

The Dynking diagram corresponding to this root system is $D_l$.

The fundamental weights $\{\lambda_1, \ldots, \lambda_l\}$ must satisfy $<\lambda_i, \alpha_j> = \delta_{ij}$. By direct computation one gets:

$$\lambda_i = e_1 + \cdots + e_i, \quad (i < l - 1)$$

$$\lambda_{l-1} = \frac{1}{2}(e_1 + \cdots + e_{l-1} - e_l)$$

$$\lambda_l = \frac{1}{2}(e_1 + \cdots + e_{l-1} + e_l).$$

51
Similarly we can construct $B_l$. A base for $B_l$ is

$$\{\varepsilon_1 - \varepsilon_2, \varepsilon_2 - \varepsilon_3, \ldots, \varepsilon_{l-1} - \varepsilon_l, \varepsilon_l\}.$$ 

The fundamental weights with respect to this base are

$$\lambda_i = \varepsilon_1 + \cdots + \varepsilon_i \quad (i < l)$$

$$\lambda_l = \frac{1}{2}(\varepsilon_1 + \cdots + \varepsilon_l).$$

**Remark 3.27.** A maximal torus $M$ in $\text{SO}(2l, K)$ (or $\text{SO}(2l+1, K)$) has dimension $l$. Thus the lattice $X(M) \otimes_{\mathbb{Z}} \mathbb{R}$ can be identified with $\mathbb{R}^l$. The canonical basis $\varepsilon_1, \ldots, \varepsilon_l$ of $\mathbb{R}^l$ corresponds to a basis $\chi_1, \ldots, \chi_l$ of $X(M)$.

Hence when we consider the root system $D_l$ or $B_l$ as $\Phi(\text{SO}, M)$ we should replace $\varepsilon_i$ by $\chi_i$ in the previous example.

**Definition 3.28.** An isogeny is a surjective morphism $f : G \rightarrow H$ of algebraic groups having finite kernel. One can check that $G$ is simply connected if, for any connected group $H$, any isogeny $f : H \rightarrow G$ is an isomorphism. Similarly, $G$ is of adjoint type if any isogeny $f : G \rightarrow H$ is an isomorphism (see [17, Theorem 2.6]).

**Proposition 3.29.** [2, Exposé 23] Let $G$ be a semisimple algebraic group. Then there exists a unique isogeny $\pi : \tilde{G} \rightarrow G$ with $\tilde{G}$ a simply connected algebraic group. ($\pi : \tilde{G} \rightarrow G$ is called universal covering of $G$).

**Example 3.30.** Let $G = \text{SO}(V)$, the canonical projection $\pi : \text{Spin}(V) \rightarrow \text{SO}(V)$ is an isogeny. See Theorem 1.28. It is also well-known that $\text{Spin}(V)$ is simply connected.

### 3.7 Orthogonal Representations

Let $\rho : G \rightarrow \text{GL}(V)$ be a rational representation. If $\rho$ leaves invariant some non-singular symmetric bilinear form in $V$, that is, if there exists $b : V \times V \rightarrow K$ such
that \( b(\rho(g)u, \rho(g)v) = b(u, v) \) for all \( g \in G \). \( u, v \in V \). then \( \rho(g) \) is an isometry. Hence we have \( \rho : G \to O(V, q_b) \). We call this an orthogonal representation. If \( T \) is a torus of \( G \). then \( \rho(T) \subset SO(V, q) \) because \( T \) is connected.

Note that an orthogonal representation is self-dual in the sense of 3.10.

Our goal in this section is to decide under which conditions an orthogonal representation \( \rho : G \to SO(V, q) \) can be lifted to \( Spin(V, q) \): that is. when we can find \( \tilde{\rho} : G \to Spin(V, q) \) such that \( \pi \circ \tilde{\rho} = \rho \).

The next proposition allows us to restrict the situation to a maximal torus of \( G \).

**Proposition 3.31.** Let \( H \) be a connected reductive group over \( K \). Let \( T \subset H \) be a maximal torus and let \( \eta : H \to SO(V) \) be an orthogonal representation. Then \( \eta \) lifts to \( Spin(V) \) if and only if \( \eta|_T : T \to SO(V) \) lifts to \( Spin(V) \).

**Proof.** The "only if" part being trivial, we shall only proof the "if" part of the statement.

Let us assume first that \( H \) is a semisimple algebraic group. Let \( p : \tilde{H} \to H \) be its universal covering (according to 3.29). Let \( \tilde{T} \subset \tilde{H} \) be the preimage of \( T \) by \( p \) and let \( \tilde{\eta} : \tilde{H} \to Spin(V) \) be the lifting of \( \eta \) to \( \tilde{H} \).

The subgroup \( \ker p \) is central: hence it is contained in \( \tilde{T} \). By hypothesis. \( \tilde{\eta} \) vanishes on \( \tilde{T} \cap \ker p = \ker p \). Thus \( \tilde{\eta} \) factors through \( H \).

Now suppose that \( H \) is reductive. Then the derived group \( H' \) of \( H \) is semisimple and \( H = Z(H) \cdot H' \) with \( Z(H) \cap H' \) finite (3.19).

Write \( T = S \cdot Z(H) \) where \( S \) is a maximal torus in \( H' \). Let \( \eta_1 : T \to Spin(V) \) be the lifting of \( \eta|_T \) given by our hypothesis and let \( \eta_2 : H' \to Spin(V) \) be the lifting of \( \eta|_{H'} \) given by the semisimple case considered above. Notice that \( \eta_1 \) and \( \eta_2 \) coincide on \( Z(H) \cap H' \): hence the map \( \tilde{\eta}(zh') = \eta_1(z)\eta_2(h') \) (\( z \in Z(H), h' \in H' \)) is well-defined and is a homomorphism on \( H = Z(H) \cdot H' \). \( \square \)
We will now explore more of the properties of the weights of orthogonal representations.

**Lemma 3.32.** Let $G$ be a reductive group and let $\rho : G \rightarrow SO(V)$ be an orthogonal representation. If $T$ is a torus of $G$ and $\alpha \in X(T)$ is a weight of $\rho$, then $-\alpha \in X(T)$ is also a weight of $\rho$ and $m_{\alpha} = m_{-\alpha}$.

**Proof.** Let $V = \bigoplus_{\alpha \in X(T)} V_{\alpha}$ be the weight decomposition of $\rho$ relative to $T$. We identify $(V_{\alpha})^*$ with the set of linear forms on $V$ that vanish on $V_J$ for all weights $J \neq \alpha$. Consider the isomorphism $\varphi : V \rightarrow V^*$ given by $\varphi(v)(u) = b(u, v)$ for all $u, v \in V$. We claim that $\varphi(V_{\alpha}) = (V_{-\alpha})^*$. Indeed, let $v \in V_{\alpha}$ and $u \in V_J$, so for any $t \in T$

$$\varphi(v)(u) = b(u, v) = b(\rho(t)u, \rho(t)v) = b(J(t)u, \alpha(t)v) = b(t \alpha(t)u, \alpha(t)v).$$

Hence $\varphi(v)(u) \neq 0$ if and only if $J(t)\alpha(t) = 1$ for all $t \in T$. Therefore $\varphi(V_{\alpha})$ vanishes on $V_J$ for all $J$ such that $J + \alpha \neq 0$ in $X(T)$. Equivalently, $\varphi(V_{\alpha}) = (V_{-\alpha})^*$. Next we will show that $(V_{\alpha})^* = (V^*)_{-\alpha}$. If $v \in V_{-\alpha}$, then $\varphi(v) \in (V_{\alpha})^*$. We need to show that $\rho'(t)\varphi(v) = -\alpha(t)\varphi(v)$, where $\rho'$ is the dual representation defined in 3.10. Indeed

$$\rho'(t)\varphi(v)(u) = \varphi(v)(\rho(t)^{-1}u) = b(\rho(t)^{-1}u, v) = b(u, \rho(t)v) = b(u, -\alpha(t)v) = -\alpha(t)b(u, v) = -\alpha(t)\varphi(v)(u).$$

Hence $(V_{\alpha})^* \subset (V^*)_{-\alpha}$. From this inclusion and since $(V^*)^* = V$, we also have

$$(V^*)_{-\alpha} = [(V^*)_{-\alpha}]^* \subset [(V^{**})_{\alpha}]^* = (V_{\alpha})^*.$$

Now the lemma follows by self-duality. □

**Proposition 3.33.** Let $T$ be an algebraic torus and let $\rho : T \rightarrow SO(V, q)$ be an orthogonal representation. For each weight $\alpha \neq 0$ of $\rho$, we choose one element of...
the set \( \{\alpha, -\alpha\} \). Let \( \alpha_1, \ldots, \alpha_r \) be the weights chosen in this way. Then the weight spaces \( V_{\pm\alpha_i} \) are totally isotropic (with respect to \( q \)) and there is an orthogonal decomposition

\[
V \cong V_0 \perp_{i=1}^r (V_{\alpha_i} \oplus V_{-\alpha_i}).
\]

(3.2)

where \( V_0 \) is the space of fixed points and \( (V_{\alpha_i} \oplus V_{-\alpha_i}) \) is hyperbolic for \( i = 1, \ldots, r \).

Proof. Let \( v \in V_\alpha \) and \( u \in V_j \). From (3.1) we have that if \( b_q(v, u) \neq 0 \) then \( J(t)\alpha(t) = 1 \), that is, \( J = -\alpha \) in \( X(T) \). This shows that \( V_\alpha \) is orthogonal to \( V_j \) for all \( J \neq -\alpha \); hence the subspaces \( V_{\alpha_i} \oplus V_{-\alpha_i} \) are pairwise orthogonal. The same computation also shows that each \( V_{\alpha_i} \) is totally isotropic since \( \alpha_i \neq -\alpha_i \). \( \Box \)

Let \( \mathcal{M} \) be a maximal torus of \( \text{SO}(V, q) \) containing \( \rho(T) \). Let \( s = \text{rank}(M) = [\dim V/2] \) and let \( \chi_1, \ldots, \chi_s \in X(M) \) be such that \( \pm \chi_1, \ldots, \pm \chi_s \) are all the weights for the action of \( M \) on \( V \). It is easy to see directly that \( \chi_1, \ldots, \chi_s \) is a basis for \( X(M) \).

Lemma 3.34. Let \( \alpha_1, \ldots, \alpha_r \) and \( \chi_1, \ldots, \chi_s \) be as above. Let \( m_i \) be the multiplicity of \( \alpha_i \). Let \( d = \chi_1 + \cdots + \chi_s \). Then \( \rho^*(d) = m_1\alpha_1 + \cdots + m_r\alpha_r \).

Proof. First we shall show that \( \rho^*(\chi_i) \in X(T) \) is a weight of \( \rho \) relative to \( T \). We have that there exists \( v \neq 0 \) in \( V(T) \) such that

\[
m \cdot v = \chi_i(m) \cdot v \quad \text{for all} \ m \in M.
\]

Since \( \rho(T) \subset \mathcal{M} \) we get that

\[
\rho(t) \cdot v = \chi_i(\rho(t)) \cdot v \quad \text{for all} \ t \in T.
\]

Hence \( \chi_i \circ \rho = \rho^*(\chi_i) \) is a weight of \( \rho \) relative to \( T \). Equivalently, \( \rho^*(\chi_i) \in \{\alpha_j, -\alpha_j, 0\} \) for some \( j \in \{1, \ldots, r\} \). Replacing \( \chi_i \) by \( -\chi_i \), if necessary, we can assume \( \rho^*(\chi_i) \in \{\alpha_j, 0\} \).
Now since $M$ preserves the factors in the decomposition (3.2), each of the subspaces $V_{\alpha_j}$ has a decomposition

$$V_{\alpha_j} = \bigoplus_{\rho^* (\chi_i) = \alpha_j} V_{\chi_i}.$$  

The weight spaces $V_{\chi_i}$ have dimension one and $V_{\alpha_j}$ has dimension $m_j$. Thus there are exactly $m_j$ weights $\chi_i$ with $\rho^* (\chi_i) = \alpha_j$. □

**Remark 3.35.** Note that the class of $\rho^*(d)$ in the quotient group $X(T)/2X(T)$ is independent of the choices we have made to define $d$. We shall see below that this class is exactly the obstruction for $\rho$ to admit a lifting $\tilde{\rho} : T \to Spin(V,q)$.

Let $\pi : Spin(V) \to SO(V)$ be the canonical projection and let $\tilde{M} \subseteq Spin(V)$ be the maximal torus with $\pi(\tilde{M}) = M$. Identifying $X(M)$ with its image $\pi^*(X(M))$, we can regard $X(\tilde{M})$ as a lattice in $X(M) \otimes \mathbb{Q}$ containing $X(M)$.

**Lemma 3.36.** The group $X(\tilde{M})/X(M)$ is generated by the class of $\frac{1}{2} d = \frac{1}{2} \sum \chi_i$.

**Proof.** Since $Spin(V)$ is simply connected, $X(\tilde{M})$ coincides with the lattice of fundamental weights of the root system $\Phi(Spin(V),\tilde{M})$. But the root system $\Phi(Spin(V),\tilde{M})$ is equal to the root system $\Phi(SO(V),M)$ because there is an isogeny between $SO(V)$ and $Spin(V)$. Hence $\Phi(Spin(V),\tilde{M})$ is $D_s$ if dim $V = 2s$ and $B_s$ if dim $V = 2s + 1$. The lemma follows immediately from the explicit description of the fundamental weights for $D_s$ and $B_s$ given in Example 3.26. □

We are now ready to prove the main theorem of this section:

**Theorem 3.37.** Let $G/K$ be a connected reductive group. Let $\rho : G \to SO(V,q)$ be a representation rational over $K$. Let $\pm \alpha_1, \pm \alpha_2, \ldots, \pm \alpha_r$ be the set of nonzero weights of $\rho$ relatively to some maximal torus $T \subseteq G$ and let $m_1, m_2, \ldots, m_r$ be the corresponding multiplicities.
Then there exists a $K$-homomorphism $\hat{\rho} : G \to \text{Spin}(V)$ such that $\pi \circ \hat{\rho} = \rho$ if and only if $\sum_i m_i \alpha_i \in 2X(T)$.

**Proof.** Let $M$ be the maximal torus of $\text{SO}(V)$ such that $\rho(T) \subset M$. Let $\rho^* : X(M) \to X(T)$ be the map induced by $\rho$. By Proposition 3.31 and Lemma 3.34, it is enough to show that the restriction of $\rho$ to $T$ can be lifted to $\hat{\rho} : T \to \tilde{M}$ if and only if $\rho^*(d) \in 2X(T)$.

By duality, the map $\rho : T \to M \subset \text{SO}(V)$ can be lifted to $\text{Spin}(V)$ if and only if $\rho^* : X(M) \to X(T)$ can be extended to $X(M)$. Since $X(M) = X(M) + \frac{1}{2}d\mathbb{Z}$, the homomorphism $\rho^*$ can be extended to $X(M)$ if and only if $\rho^*(d) \in 2X(T)$. □

### 3.8 Rationality Properties

Let $k$ be an arbitrary subfield of $K$ and $X$ an affine variety over $K$. If the ideal $\mathcal{J}(X)$ of all polynomials vanishing on $X$ is generated by $k$-polynomials, we say that $X$ is defined over $k$. If $X$ is a closed subset of $\mathbb{A}^n$ defined over $k$, we let $X(k) = X \cap k^n$ be its set of $k$-rational points.

When $X$ and $Y$ are defined over $k$, we say that a morphism $\varphi : X \to Y$ is defined over $k$ (or is a $k$-morphism) if all the coordinate functions can be represented by polynomials with coefficients in $k$.

Now we review some definitions and results of this chapter that have rationality properties, which will be important later.

1. **We say that an algebraic group $G$ is defined over $k$ (or is $k$-group) if the variety $G$, $\mu : G \times G \to G$, and $i : G \to G$ are defined over $k$. If $G$ is a $k$-group, the set $G(k)$ of its $k$-rational points is a subgroup of $G$.**

2. **If $G$ is a linear $k$-group, then there exists a $k$-isomorphism of $G$ onto a $k$-subgroup of $\text{GL}_n(K)$.**

3. **If $G$ is a $k$-group, then $G^0$ is also.**
Let \( \varphi : G \to G' \) be a \( k \)-morphism of \( k \)-groups. Then the image of \( \varphi \) is a \( k \)-subgroup of \( G' \). (The kernel need not be defined over \( k \).)

If \( G \) is a \( k \)-group, its Lie algebra has a natural \( k \)-structure with \( \mathcal{L}(G) \cong \mathcal{K} \otimes_k \mathcal{L}(G)(k) \). In this case \( \text{Ad} : G \to \text{GL}(\mathcal{L}(G)) \) is a \( k \)-morphism.

**Remark 3.38.** In the next two results we have to assume \( k \) is perfect in order to obtain the desired rationality properties. Recall that \( k \) is perfect if the algebraic closure \( \bar{k} \) coincides with the separable closure \( k_s \). Hence showing that an element or a morphism is defined over \( k \) is the same as showing that they are invariant under the action of the Galois group \( \text{Gal}(\bar{k}/k) \).

Consider \( V \) with a \( k \)-structure: \( \text{End}(V) \) also has a \( k \)-structure. If \( a \in \text{End}(V) \) is \( k \)-rational and \( k \) is perfect, then \( a_s \) and \( a_n \) are also \( k \)-rational.

**Proof.** Denote \( E = \text{End}(V) \). We are assuming that \( a \in E(k) \). The elements \( a_s \) and \( a_n \) obtained in 3.17 are in \( E(\bar{k}) \) (see the proof of [1. Proposition 4.2]). If \( s \in \text{Gal}(\bar{k}/k) \), then \( s \) acts on \( E(\bar{k}) \) and we have that \( a = s(a) = s(a_s) + s(a_n) \). Since \( s \) acts as an algebra automorphism, we see that \( s(a_n) \) is nilpotent and commutes with \( s(a_s) \). Moreover, since \( a_s \) is semisimple, \( \bar{k}[a_s] \) is a semisimple algebra. Hence \( s(\bar{k}[a_s]) = \bar{k}[s(a_s)] \) is also semisimple, so \( s(a_s) \) remains semisimple.

By the uniqueness of the Jordan decomposition we have that \( s(a_s) = a_s \) and \( s(a_n) = a_n \). Since \( k \) is perfect it follows that \( a_s \) and \( a_n \) are defined over \( k \). □

If \( \rho : G \to \text{SO}(V) \) is defined over a perfect field \( k \) and a lifting \( \tilde{\rho} : G \to \text{Spin}(V) \) of \( \rho \) exists, then \( \tilde{\rho} \) is also defined over \( k \).

**Proof.** First we show that \( \tilde{\rho} \) is unique. Suppose that \( \rho_1, \rho_2 : G \to \text{Spin}(V) \) are such that \( \pi \rho_1 = \pi \rho_2 = \rho \). Then \( \rho_1(x) = u(x) \rho_2(x) \) for all \( x \in G \) with \( u(x) \in \ker \pi = \mathbb{Z}/2 \).

Thus we get a map \( u : G \to \mathbb{Z}/2 \), which must be trivial because \( G \) is connected. Therefore \( \rho_1(x) = \rho_2(x) \) for all \( x \in G \).
We have that $\tilde{\rho}$ is a $\bar{k}$-homomorphism. The action of $s \in \text{Gal}(\bar{k}/k)$ on $\tilde{\rho}$ is given by $(s\tilde{\rho})(x) = s\tilde{\rho}(s^{-1}x)$. Hence

$$\pi(s\tilde{\rho})(x) = \pi s\tilde{\rho}(s^{-1}x) = s\pi\tilde{\rho}(s^{-1}x) = s\rho(s^{-1}x) = \rho(x).$$

since $\rho$ is defined over $k$ and $\pi$ commutes with the action of $s$. From the uniqueness of $\tilde{\rho}$ we conclude that $s\tilde{\rho} = \tilde{\rho}$ for all $s \in \text{Gal}(\bar{k}/k)$. Since $k$ is perfect, this shows that $\tilde{\rho}$ is defined over $k$. $\square$. 

59
Chapter 4
The Second Stiefel-Whitney Class of Trace Forms

In 1984 J.P. Serre [24] expressed the second Stiefel-Whitney class of the trace form of a commutative étale algebra in terms of other cohomological invariants. In the case of central simple algebras, D. Saltman (1987, unpublished) described the second Stiefel-Whitney class of the form $\text{tr}(x^2)$. Our goal in this chapter is to present these two results in some detail. Our proof of Saltman's result is not based on his work, but on a paper by D. Lewis and J. Morales [13].

4.1 Definition of the Stiefel-Whitney Classes

The second Stiefel-Whitney class, as the name suggests, is one of a family of classes of quadratic forms, which we shall define in this section. These classes were defined by Delzant in [4] and we are following his idea.

Let $k$ be a field of characteristic different from two. Denote by $k_s$ the separable closure of $k$ and by $\Gamma$ the Galois group of $k_s$ over $k$. As in Chapter 2, we denote by $H^n(k, \mathbb{Z}/2)$ the $n$th cohomology group of $\Gamma$ with coefficients in $\mathbb{Z}/2$.

According to Proposition 2.5, $H^*(k, \mathbb{Z}/2) = \bigoplus_{n=1}^{\infty} H^n(k, \mathbb{Z}/2)$ is a graded-commutative ring. In fact, this is a commutative ring because we are in characteristic two. Denote by $\hat{H}$ the completion of $H = H^*(k, \mathbb{Z}/2)$, so

$$\hat{H} = \prod_{n=0}^{\infty} H^n(k, \mathbb{Z}/2).$$

An element $\beta \in \hat{H}$ can be written as a "formal series": $\beta = \sum_{i=0}^{\infty} \beta_i$. The operation in $\hat{H}$ is given by multiplication of formal series:

$$\sum_{i=0}^{\infty} \alpha_i \cdot \sum_{j=0}^{\infty} \beta_j = \sum_{k=0}^{\infty} (\alpha \beta)_k, \quad \text{where} \quad (\alpha \beta)_k = \sum_{p+q=k} \alpha_p \beta_q.$$
Lemma 4.1. The set $1 + \hat{H}^+ = \{1 + \sum_{i \geq 1} \beta_i : \beta_i \in H^i(k, \mathbb{Z}/2)\}$ is a multiplicative subgroup of $\hat{H}$.

Proof. Let $\alpha = 1 + \sum_{i \geq 1} \alpha_i$ and $\beta = 1 + \sum_{j \geq 1} \beta_j$ be elements of $1 + \hat{H}^+$. Hence

$$\alpha \cdot \beta = 1 + \sum_{i \geq 1} \alpha_i + \sum_{j \geq 1} \beta_j + (\sum_{i \geq 1} \alpha_i) \cdot (\sum_{j \geq 1} \beta_j)$$

$$= 1 + \sum_{k \geq 1} \gamma_k,$$

for $\gamma_k \in H^k(k, \mathbb{Z}/2)$. Hence $1 + \hat{H}^+$ is closed for multiplication. Now write $\alpha = 1 - z$ where $z = \sum_{i \geq 1} \alpha_i$ (recall that we are in characteristic two). Thus

$$\alpha^{-1} = \frac{1}{1 - z} = \sum_{n \geq 0} z^n = 1 + \sum_{n \geq 1} z^n \in 1 + \hat{H}^+.$$ 

Note that $(z^n)_p = 0$ for $n > p$, hence each coefficient of $z^n$ is finite. Therefore $1 + \hat{H}^+$ is a subgroup of $\hat{H}$. □

Let $\hat{k}$ be the multiplicative group of $k$ and $D = \hat{k}/\hat{k}^2$. We can identify $D$ with $H^1(k, \mathbb{Z}/2)$ (see Corollary 2.12). We denote by $(a)$ the class of $[a] \in D$ in $H^1(k, \mathbb{Z}/2)$.

Define the map $\bar{w} : D \to 1 + \hat{H}^+$ by $[a] \mapsto 1 + (a)$. This set-theoretical map can be extended to a group homomorphism as follows:

$$\bar{w} : \mathbb{Z}[D] \to 1 + \hat{H}^+. \quad [a_1] + \cdots + [a_n] \mapsto \prod_{i=1}^n (1 + (a_i)).$$

Combining $\bar{w}$ with the map $\pi : \mathbb{Z}[D] \to \hat{W}(k)$ defined in section 1.1, we have

$$\begin{array}{c}
\mathbb{Z}[D] \xrightarrow{w} 1 + \hat{H}^+ \\
\downarrow \pi \\
\hat{W}(k).
\end{array}$$

Proposition 4.2. The map $\bar{w}$ induces a group homomorphism

$$w : \hat{W}(k) \to 1 + \hat{H}^+. \quad q = <a_1, \ldots, a_n> \mapsto \prod_{i=1}^n (1 + (a_i)).$$

This homomorphism does not depend on the diagonalization of $q$. 

61
Proof. We have to check that ker \( \pi \subset \ker \tilde{w} \). From theorems 1.11 and 1.17, we have that ker \( \pi \) is generated by the elements \([a] + [b] - [c] - [d] \in \mathbb{Z}[D]\) such that \((a, b) \cong (c, d)\) and \(ab = cd\). Recall that the quaternion algebra \((a, b)\) corresponds to the cup product \((a) \cdot (b)\) in \(H^2(k, \mathbb{Z}/2)\). The group \(H^1(k, \mathbb{Z}/2)\) is written additively, so \(ab\) corresponds to \((a) + (b)\). It is enough to check that the generators of ker \( \pi \) are in ker \( \tilde{w} \). Let \( x = [a] + [b] - [c] - [d] \) be a generator of ker \( \pi \). Hence
\[
\tilde{w}(x) = \sum \left( a_{j_1} \cdots a_{j_n} \right)
\]
It follows that \( \tilde{w}(x) = 0 \), as desired. \( \square \)

Definition 4.3. Let \( q \in \widetilde{W}(k) \) be a quadratic form of dimension \( n \). Then \( w(q) = 1 + \sum_{i=1}^{n} w_i(q) \). The coefficient \( w_i(q) \in H^i(k, \mathbb{Z}/2) \) is called the \( i \)-th Stiefel-Whitney class of \( q \).

More explicitly if \( q = < a_1, \ldots, a_n > \), then
\[
w_i(q) = \sum_{1 \leq j_1 < \cdots < j_i \leq n} (a_{j_1}) \cdots (a_{j_i}).
\]
In particular, \( w_1(q) = (a_1) + \cdots + (a_n) \) is the discriminant of \( q \). The second class \( w_2(q) = \sum_{i < j} (a_i) \cdot (a_j) \) coincides with the Hasse invariant of \( q \) (compare with Definition 1.18).

4.2 Serre’s Formula

In this section we shall present the formula given by Serre in [24] to compute the Hasse invariant of the form \( \text{Tr}_{E/k}(x^2) \), where \( E \) is an étale algebra over \( k \).

Before we explain Serre’s work, we need to mention the relation between \( H^2 \) and extensions of groups.
Definition 4.4. Let $G$ and $A$ be abelian groups. An extension of $G$ by $A$ is a short exact sequence

$$0 \to A \to X \stackrel{\pi}{\to} G \to 0.$$ 

Two extensions $0 \to A \to X_i \to G \to 0$ $(i = 1, 2)$ are equivalent if there is an isomorphism $\varphi : X_1 \to X_2$ such that the diagram

$$\begin{array}{c}
0 \longrightarrow A \longrightarrow X_1 \longrightarrow G \longrightarrow 0 \\
\| \quad \quad \downarrow \varphi \quad \quad \| \\
0 \longrightarrow A \longrightarrow X_2 \longrightarrow G \longrightarrow 0
\end{array}$$

commutes.

Given an extension $0 \to A \to X \stackrel{\pi}{\to} G \to 0$, choose a set map $s : G \to X$ such that $s(1)$ is the identity in $X$ and $s \circ \pi(g) = g$ for all $g \in G$. This map is called a section. Since $\pi$ is a homomorphism, $s(gh)$ and $s(g)s(h)$ are elements of $X$ mapping to $gh \in G$. Hence their difference lies in $A$. We can define

$$d(g, h) = s(g)s(h)s(gh)^{-1},$$

which is a 2-cocycle of $A$. Moreover.

Theorem 4.5. [30. Theorem 6.6.3] The equivalence classes of extensions of $G$ by $A$ are in one-to-one correspondence with the elements of the cohomology group $H^2(G, A)$.

The following example is necessary to Serre’s argument.

Example 4.6. Let $G = \Sigma_n$ be the symmetric group of order $n$ and $A = \mathbb{Z}/2$. According to [22],

$$H^2(\Sigma_n, \mathbb{Z}/2) = \begin{cases} 
0 & \text{if } n = 1 \\
\mathbb{Z}/2 & \text{if } n = 2, 3 \\
\mathbb{Z}/2 \oplus \mathbb{Z}/2 & \text{if } n \geq 4.
\end{cases}$$
We will be interested in the element \( s_n \in H^2(\Sigma_n, \mathbb{Z}/2) \) corresponding to the extension

\[
0 \rightarrow \mathbb{Z}/2 \rightarrow \Sigma_n \xrightarrow{\pi} \Sigma_n \rightarrow 0
\]

denoted by (II') in [22. pg 355]. The extension \( s_n \) is completely characterized by the following properties:

1. If \( x \in \Sigma_n \) and \( p(x) \) is a transposition, then \( x \) has order two.
2. If \( x \in \Sigma_n \) and \( p(x) \) is a product of two disjoint transpositions, then \( x \) has order four.

Recall that \( O_n(k) \) is the orthogonal group of the \( n \)-dimensional unitary quadratic space \((k^n, n < 1)\). Hence we can identify \( \Sigma_n \) with a subgroup of \( O_n(k) \). The following sequence of algebraic groups is exact (see (1.1) after Definition 1.26)

\[
0 \rightarrow \mathbb{Z}/2 \rightarrow \text{Pin}_n \xrightarrow{\pi} O_n \rightarrow 0.
\]

Let \( X \) be the preimage of \( \Sigma_n \) by \( \pi \). Then the following diagram of algebraic groups is commutative

\[
\begin{array}{ccc}
0 & \rightarrow & \mathbb{Z}/2 \\
\| & & \downarrow \pi \\
0 & \rightarrow & \text{Pin}_n \\
\end{array}
\]

\[
\begin{array}{ccc}
0 & \rightarrow & \mathbb{Z}/2 \\
\| & & \downarrow \pi \\
0 & \rightarrow & O_n \\
\end{array}
\]

**Lemma 4.7.** Let \( n \geq 4 \). Then the extension \( 0 \rightarrow \mathbb{Z}/2 \rightarrow X \xrightarrow{\pi} \Sigma_n \rightarrow 0 \) is the extension \( s_n \).

**Proof.** Consider the quadratic space \((V, q)\), where \( V = k^n \) and \( q = n < 1 \). Take a basis \( \{e_1, \ldots, e_n\} \) in \( k^n \) such that \( q(e_i) = 1 \) and \( b_q(e_i, e_j) = 0 \) for \( i \neq j \). Let \( C(V) \) be the Clifford algebra of \((V, q)\). Let \( i, j \) be indices such that \( i \neq j \). Then \( q(e_i - e_j) = (e_i - e_j)^2 = 2 \). Now take \( x = \frac{1}{\sqrt{2}} (e_i - e_j) \) in \( C(V) \). Since \( x \in C_1(V) \), \( \pi(x)(v) = -vxv^{-1} \) for all \( v \in V \). one
can easily check that:

(1) \(-xe_i x^{-1} = e_j, \quad -xe_j x^{-1} = e_i, \quad \text{and} \quad -xe_k x^{-1} = e_k \) for \( k \neq i, j \).

(2) \( xx' = 1 \).

These two properties show that \( x \) is an element of \( \text{Pin}_n(k_s) \). The first property also shows that the image of \( x \) on \( O_n \) can be identified with the permutation \( (ij) \).

Clearly the other element of \( X \) that is mapped into \( (ij) \) is \(-x = \frac{1}{\sqrt{2}}(e_j - e_i) \). Note that both have order two.

Now if we consider a product of two disjoint transpositions, say \((ij)(kl)\), then \( x = \pm \frac{1}{\sqrt{2}}(e_i - e_j)(e_k - e_l) \in X \) are the elements in the preimage of \((ij)(kl)\). We have that \((e_i - e_j)\) and \((e_k - e_l)\) are orthogonal, so they anticommute in \( C(V) \). Hence

\[ x^2 = -\frac{1}{4}(e_i - e_j)^2(e_k - e_l)^2 = -\frac{1}{4}2.2 = -1. \]

Thus \( x \) has order.

We proved that the elements \( x \in X \) such that \( \pi(x) \) is a transposition have order two and the elements \( x \in X \) such that \( \pi(x) \) is a product of two disjoint transpositions have order four. These are precisely the properties that characterize \( s_n \).

An immediate consequence of the lemma is that the following diagram of algebraic groups

\[
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & \tilde{\Sigma}_n & \longrightarrow & \Sigma_n & \longrightarrow & 0 \\
\| & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & \text{Pin}_n & \longrightarrow & O_n & \longrightarrow & 0
\end{array}
\]

is commutative.

Let \( E \) be an \( \acute{e} \)tale algebra of rank \( n \geq 1 \) over \( k \). Then over \( k_s \), we have that \( E \cong k_s \times \cdots \times k_s \) (\( n \) times). From Galois descent, the cohomology set \( H^1(k, \text{Aut}(k_s^n)) \) classifies the \( \acute{e} \)tale algebras over \( k \) of rank \( n \).
Clearly we have $\text{Aut}(k^n_s) \cong \Sigma_n$. Let $e : \Gamma \rightarrow \Sigma_n$ be the cocycle corresponding to $E$ in $H^1(k, \Sigma_n)$. Hence $e$ induces a map in cohomology
\[ e^* : H^2(\Sigma_n, \mathbb{Z}/2) \rightarrow H^2(k, \mathbb{Z}/2). \]

The quadratic form $Q_E : E \rightarrow k$ is defined by $Q_E(x) = \text{Tr}_{E/k}(x^2)$. Hence $Q_E$ is a nondegenerate quadratic form of rank $n$ over $k$. From 2.19, $Q_E \in H^1(k, \mathcal{O}_n)$.

**Lemma 4.8.** Let $i^* : H^1(k, \Sigma_n) \rightarrow H^1(k, \mathcal{O}_n)$ be the map induced by the inclusion $i : \Sigma_n \rightarrow \mathcal{O}_n$. Then $i^*(e) = Q_E$.

**Proof.** The cocycle $e$ is obtained by choosing an isomorphism $f : E \otimes k_s \rightarrow k^n_s$ and defining $e(\sigma) = f^{-1} \circ \sigma(f)$ for all $\sigma \in \Gamma$. Since $f$ is an algebra isomorphism, $f$ preserves the trace forms. Hence $i \circ e : \Gamma \rightarrow \mathcal{O}_n$ is a cocycle that represents $Q_E$ in $H^1(k, \mathcal{O}_n)$. □

Serre's formula for the Hasse invariant of $Q_E$ is given in the following theorem.

**Theorem 4.9.** Keep the notation as above. Then
\[ w_2(Q_E) = e^*(s_n) + (2, d_E). \]

Before proving the theorem, we need to make explicit the action of $\Gamma$ on $\tilde{\Sigma}_n$. The cohomology classes $(2, (d_E)) \in H^1(k, \mathbb{Z}/2)$ play an important role in this action. Recall that $\chi : \Gamma \rightarrow \mathbb{Z}/2$, defined by $\sigma(\sqrt{2}) = (-1)^{\chi(\sigma)}\sqrt{2}$ for all $\sigma \in \Gamma$, represents $(2)$. If $\varepsilon : \Sigma_n \rightarrow \mathbb{Z}/2$ is the signature map, then the composition $\Gamma \xrightarrow{\varepsilon} \Sigma_n \xrightarrow{\varepsilon} \mathbb{Z}/2$ represents $(d_E)$.

Now if $x \in \tilde{\Sigma}_n$ and $p(x)$ is a transposition, then from the description of $x$ in the proof of Lemma 4.7 we get that $\sigma(x) = (-1)^{\chi(\sigma)}\cdot x$ for all $\sigma \in \Gamma$. For an arbitrary element $x \in \tilde{\Sigma}_n$, $\varepsilon(p(x)) = 0$ (resp. 1) if $p(x)$ is a product of an even (resp. odd) number of transpositions. Hence $\sigma(x) = ((-1)^{\chi(\sigma)})^{\varepsilon(p(x))}\cdot x$. 66
Proof of Theorem 4.9 We refer to [24. §2.2] for the argument for the cases \( n = 1, 2, 3 \).

Assume \( n \geq 4 \). By taking cohomology in the diagram (4.1), we get the commutative diagram

\[
\begin{array}{ccc}
H^1(k, \Sigma_n) & \longrightarrow & H^2(k, \mathbb{Z}/2) \\
\downarrow i^* & & \downarrow \\
H^1(k, \mathbb{O}_n) & \longrightarrow & H^2(k, \mathbb{Z}/2).
\end{array}
\]

From Lemma 4.8, \( i^*(e) = Q_E \). From the Springer's spinor interpretation of the Hasse invariant (Theorem 2.22), \( \partial(Q_E) = w_2(Q_E) \). We have to show that \( \partial(Q_E) = e^*(s_n) + (2, d_E) \).

The 2-cocycle \( s_n \) can be described by \( s_n(\sigma, \tau) = s(\tau)s(\gamma)s(\text{sgn} \gamma)^{-1} \), where \( s : \Sigma_n \rightarrow \tilde{\Sigma}_n \) is a section in the extension

\[
0 \rightarrow \mathbb{Z}/2 \rightarrow \tilde{\Sigma}_n \xrightarrow{p} \Sigma_n \rightarrow 0.
\]

Hence

\[
e^*(s_n)(\sigma, \tau) = e_n(e(\sigma), e(\tau)) = s(e(\sigma))s(e(\tau))s(e(\text{sgn} \gamma))^{-1}.
\]

On the other hand, we can use \( s : \Sigma_n \rightarrow \tilde{\Sigma}_n \) to make our choice of a preimage of \( e(\sigma) \) in \( \tilde{\Sigma}_n \) for each \( \sigma \in \Gamma \). Denote \( x_\sigma = se(\sigma) \in \tilde{\Sigma}_n \) for each \( \sigma \in \Gamma \). Hence

\[
\partial(Q_E)(\sigma, \tau) = x_\sigma x_\tau x_\sigma^{-1}
\]

\[
= x_\sigma((-1)^{\chi(\text{sgn} \gamma)}x_\sigma^{(p(x_\tau))})x_\tau x_\sigma^{-1}
\]

\[
= x_\sigma(-1)^{\chi(\text{sgn} \gamma)x(\text{sgn} \gamma)}x_\tau x_\sigma^{-1}
\]

\[
= (2, d_E)x_\sigma x_\tau x_\sigma^{-1}.
\]

The last equality follows from Remark 2.14(2). But \( x_\sigma x_\tau x_\sigma^{-1} = e^*(s_n)(\sigma, \tau) \). Therefore \( \partial(Q_E) = e^*(s_n) + (2, d_E) \) (written additively). \( \square \)

Remark 4.10. (1) The Stiefel-Whitney classes \( w_n(Q_E) \) with \( n > 2 \) can also be computed using the formula given by B. Kahn in [8].

(2) Serre [24] also computed \( w_2 \) of the form \( Q_{E, a}(x) = \text{tr}_{E/k}(ax^2) \) for \( a \in E \).
4.3 Trace Form of a Central Simple Algebra

Let $A$ be a central simple algebra of degree $n$ over $k$. We define $T_A : A \to k$ by $T_A(x) = \text{tr}_{A/k}(x^2)$. where $\text{tr}$ is the reduced trace defined in 1.47.

Our goal in this section is to determine the Hasse invariant of $T_A$. As mentioned before, the argument presented here is based on a paper by D. Lewis and J. Morales [13].

If $A = M_n(k)$, then we denote the trace form $T_{M_n(k)}$ by $T$.

**Proposition 4.11.** If $n$ is odd and $A$ is a central simple algebra of degree $n$ over $k$, then $T_A \sim T$.

**Proof.** Let $D$ be the division algebra such that $A \cong M_n(D)$. Then any maximal subfield $L$ of $D$ is a splitting field of $A$ (see Theorem 1.45). Since the degree of $L$ over $k$ is odd and $T_A \sim T$ over $L$, we get $T_A \sim T$ over $k$ from Theorem 1.8. □

Throughout this section, we assume that $n$ is even.

**Theorem 4.12.** Let $A$ be a central simple algebra of degree $n$ over $k$. Then

$$w_2(T_A) = \frac{n}{2}[A] + \frac{n(n-2)}{8}(-1,-1).$$

where $[A]$ denotes the class of $A$ in $\text{Br}(k)$.

**Proof.** We know that the elements of the group $\text{Aut}(M_n) \cong \text{PGL}_n$ are, in fact, isometries of $T$. Since $\text{Aut}(M_n)$ is a connected algebraic group, we actually have $\text{Aut}(M_n) \subset \text{SO}(T)$. Now since $\text{Spin}(T)$ is a universal cover of $\text{SO}(T)$ and $\text{SL}_n$ is simply connected, we can find a lifting $\bar{i} : \text{SL}_n \to \text{Spin}(T)$ such that the diagram

$$\begin{array}{ccc}
1 & \longrightarrow & \mu_n \\
\downarrow 1 & & \downarrow 1 \\
1 & \longrightarrow & \text{SL}_n & \longrightarrow & \text{Aut}(M_n) & \longrightarrow & 1 \\
\downarrow i & & \downarrow i & & \downarrow i \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \text{Spin}(T) & \longrightarrow & \text{SO}(T) & \longrightarrow & 1
\end{array}$$

(4.2)

commutes.

**Claim** The map $\bar{i} : \mu_n \to \mu_2$ is nontrivial.

\[\text{Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.}\]
Assume the claim. Then \( \bar{\iota}(\xi) = \xi^{n/2} \). Now by taking cohomology in the above diagram we get the diagram

\[
\begin{array}{ccc}
H^1(k, \text{Aut}(M_n)) & \xrightarrow{\partial} & H^2(k, \mu_n) \\
\downarrow \iota^* & & \downarrow \iota^* \\
H^1(k, \text{SO}(T)) & \xrightarrow{\partial} & H^2(k, \mu_2),
\end{array}
\]

which commutes.

We have that \( \iota^*(A) = T_A \) (see Lemma 4.8). From Theorem 2.22. \( \partial(T_A) = w_2(T_A) + w_2(T) \). The connecting homomorphism \( \partial \) takes \( A \) into its class \([A]\) in \( H^2(k, \mu_n) \subset \text{Br}(k) \). Hence \( \iota^*(\partial(A)) = \frac{n}{2}[A] \). By the commutativity of the diagram, we get

\[
w_2(T_A) = \frac{n}{2}[A] + w_2(T).
\]

Now by taking the canonical basis \( \{e_{ij}\} \) of \( M_n(k) \), one can easily compute that \( w_2(T) = \frac{n(n-2)}{8}(-1, -1) \).

**Proof of Claim** It is enough to show that \( \bar{\iota} : \mu_n \to \mu_2 \) is nontrivial over some extension of \( k \). We can assume that \( k/k^2 \neq 1 \) by replacing \( k \) by \( k(t) \) if necessary.

From the diagram (4.2), we get the following commutative diagram in cohomology

\[
\begin{array}{ccc}
\text{Aut}(M_n(k)) & \xrightarrow{\partial} & H^1(k, \mu_n) \\
\downarrow \iota^* & & \downarrow \iota^* \\
\text{SO}(T) & \xrightarrow{\partial} & H^1(k, \mu_2).
\end{array}
\]

It is enough to show that \( \iota^* \) is nontrivial. The map \( \text{SO}(T) \to H^1(k, \mu_2) = \hat{k}/\hat{k}^2 \) is the spinor norm \( \mathcal{S} \) defined in 1.26. Hence it is enough to find an element \( a \in \text{GL}_n(k) \) such that \( \mathcal{S}(\text{Inn}(a)) \) is not a square in \( \hat{k} \).

Let \( a = \text{diag}(d, 1, \ldots, 1) \), where \( d \) is not a square in \( \hat{k} \). Consider the canonical basis \( \{e_{ij}\} \) of \( M_n(k) \) and set

\[
v_i = e_{i1} - de_{1i},
\]

\[
w_i = e_{i1} - e_{1i}.
\]
Hence, by direct computation, one can check that

\[ \text{Inn}(a) = \tau_{v_2} \tau_{w_2} \tau_{v_3} \tau_{w_3} \cdots \tau_{v_n} \tau_{w_n}, \]

where \( \tau_v \) is the reflection associated to \( v \), as defined in 1.5. Hence

\[ \beta(\text{Inn}(a)) \equiv \prod_{i=2}^{n} \text{tr}(v_i^2) \text{tr}(w_i^2) \pmod{\hat{k}^2} \]

\[ \equiv (-2d)^{n-1} (-2)^{n-1} \pmod{\hat{k}^2} \]

\[ \equiv d \pmod{\hat{k}^2}. \]

Since \( d \not\in \hat{k}^2 \), this finishes the proof. \( \square \)
Chapter 5
Scaled Trace Forms of Central Simple Algebras

In this chapter we provide a formula to compute the second Stiefel-Whitney class of scaled trace forms of central simple algebras. We will see that the formula for the general situation depends strongly on the formula for the split algebra. We start by computing the latter.

Let $k$ be a perfect field of characteristic different from 2. Let $A$ be a central simple algebra of degree $n$ over $k$. Let $a$ be a nonzero element in $A$ and define $Q_{A,a} : A \rightarrow k$ by $Q_{A,a}(x) = \text{tr}_{A/k}(ax^2)$ for all $x \in A$, where tr denotes the reduced trace. This quadratic form is called the scaled trace form.

The proof of the following lemma is based on Lewis' work on scaled trace forms [11].

**Lemma 5.1.** The quadratic form $Q_{A,a}$ is nonsingular if and only if $a$ and $-a$ have no common eigenvalue.

**Proof.** First we shall show that $Q_{A,a}$ is nonsingular if and only if $xa + ax = 0$ implies $x = 0$. The bilinear form $b_{A,a} : A \times A \rightarrow k$ associated to $Q_{A,a}$ is defined by $b_{A,a}(x, y) = \frac{1}{2} \text{tr}_{A/k}(axy + yxa)$. Assume that $b_{A,a}(x, y) = 0$ for all $y \in A$. Then

$$0 = b_{A,a}(x, y) = \frac{1}{2} \text{tr}_{A/k}(axy + ayx) = \frac{1}{2} \text{tr}_{A/k}(yax + yxa)$$

$$= \frac{1}{2} \text{tr}_{A/k}(y(ax + xa)). \quad \text{(5.1)}$$

Hence $\text{tr}_{A/k}(y(ax + xa)) = 0$ for all $y \in A$. Since the usual trace form is nonsingular we must have $ax + xa = 0$. By hypothesis it follows that $x = 0$. thus $Q_{A,a}$ is nonsingular.
Conversely, assume that $ax + xa = 0$. Then from (5.1), $b_{A,a}(x,y) = 0$ for all $y \in A$. Since $Q_{A,a}$ is nonsingular, we have $x = 0$.

Now we need to show that $ax + xa = 0$ implies $x = 0$ if and only if $a$ and $-a$ have no common eigenvalue. Let $V = M_n(\bar{k})$, where $\bar{k}$ is the algebraic closure of $k$. Consider $M = "left multiplication by $a"$ and $N = "right multiplication by $-a$." endomorphisms of $V$. Clearly we have that $M.N = N.M$, thus $M$ and $N$ are simultaneously trigonalizable (see [5, 15.4]). Moreover, the diagonal entries of $M$ and $N$ are the eigenvalues of $a$ and $-a$, respectively. Hence $\det(M - N) = 0$ if and only if $a$ and $-a$ have a common eigenvalue. Thus $ax + xa = 0$ implies $x = 0$ if and only if the system $(M - N)X = 0$ has a nontrivial solution, that is, if and only if $\det(M - N) \neq 0$. □

Next we reduce the problem to the case where the scaling factor $a \in A$ is a semisimple element.

**Proposition 5.2.** Let $a_s$ be the semisimple part of $a$ in its Jordan decomposition. Then $Q_{A,a} \simeq Q_{A,a_s}$.

*Proof.* Let $a = a_s + a_n$ be the Jordan decomposition of $a$, where $a_s$ is semisimple and $a_n$ is nilpotent (see 3.17). We shall show that $Q_{A,a}$ and $Q_{A,a_s}$ are Witt-equivalent, which will be sufficient since the two forms have the same rank.

Recall that if $U \subset A$ is a totally isotropic subspace, then $A$ is Witt-equivalent to the space $U^\perp/U$ endowed with the form induced by $Q_{A,a}$ (see [9, Proposition 3.7.9]). Hence it will be enough to show that there is a subspace $U \subset A$ totally isotropic with respect to $Q_{A,a}$ such that $\text{tr}_{A/k}(a_n x^2) = 0$ for all $x \in U^\perp$.

Let $U \subset A$ be a subspace satisfying the following conditions:

(i) $\text{tr}_{A/k}(x^2) = 0$ for all $x \in U$

(ii) $aU \subset U$ and $Ua \subset U$
(iii) \( U \) is maximal among the subspaces of \( A \) satisfying (i) and (ii).

Let \( U^\perp \) be the orthogonal complement of \( U \) with respect to the form \( \text{tr}_{A/k}(x^2) \) (which is, by virtue of (ii), also the orthogonal of \( U \) with respect to \( \text{tr}_{A/k}(ax^2) \)). We shall show that the form \( \text{tr}_{A/k}(a_nx^2) \) is identically zero on \( U^\perp \) by showing the inclusion \( a_n U^\perp \subseteq U \).

Consider the ring \( R = k[a] \otimes_k k[a] \) equipped with the involution \( \overline{x} \otimes y = y \otimes x \). We define an \( R \)-module structure on \( A \) by \( (x \otimes y) \cdot \alpha = x \alpha y \) for \( x, y \in k[a] \) and \( \alpha \in A \). Notice that, by virtue of (ii), the subspace \( U \) is actually an \( R \)-submodule of \( A \).

Define \( \langle \alpha, \beta \rangle = \text{tr}_{A/k}(\alpha \beta) \) for \( \alpha, \beta \in A \). We verify that for \( z \in R \) we have \( \langle z \alpha, \beta \rangle = \langle \alpha, z \beta \rangle \) (it is enough to see this for \( z \) of the form \( z = x \otimes y \), in which case the equality is obvious). It follows immediately from this property that \( U^\perp \) is an \( R \)-submodule as well.

The next step is to show that (iii) implies that \( U^\perp / U \) is a semisimple \( R \)-module. Let \( \mathfrak{r} \) be the radical of \( R \) and let \( m \geq 1 \) be the smallest integer such that \( \mathfrak{r}^m U^\perp \subseteq U \) (\( \mathfrak{r} \) is a nilpotent ideal). Suppose that \( m \geq 2 \) and let \( l \) be the smallest integer with \( l \geq m/2 \). Then

\[
\langle \mathfrak{r} U^\perp, \mathfrak{r} U^\perp \rangle = \langle U^\perp, \mathfrak{r}^2 U^\perp \rangle = \langle U^\perp, \mathfrak{r}^2 U^\perp \rangle = \{0\},
\]

since \( \mathfrak{r} = \mathfrak{r}^2 \) and \( \mathfrak{r}^2 U^\perp \subseteq U \). Hence \( \mathfrak{r} U^\perp \) is a totally isotropic \( R \)-submodule, and therefore \( U + \mathfrak{r} U^\perp \) is also. By (iii) we must have \( U + \mathfrak{r} U^\perp = U \), that is, \( \mathfrak{r} U^\perp \subseteq U \).

This contradicts the minimality of \( m \); therefore \( m = 1 \).

Since \( a_n \otimes 1 \) is in the radical \( \mathfrak{r} \), we have \( a_n U^\perp \subseteq U \). Therefore \( \text{tr}_{A/k}(a_n xy) = \text{tr}_{A/k}((a_n x)y) = 0 \) for all \( x, y \in U^\perp \), as claimed. \( \Box \)
5.1 The case where $A$ is a split algebra

Throughout this section we shall assume that $A = M_n(k)$. Let $b \in M_n(k)$ be a fixed element so that $Q_{M_n(k),b}$ is nondegenerate. In view of Proposition 5.2 we can assume, without loss of generality, that $b \in A$ is semisimple. For simplicity, we shall write $Q_b$ for $Q_{M_n(k),b}$.

For the remainder of this section, we fix a commutative étale algebra $E \subset M_n(k)$ of dimension $n$ over $k$ containing $b$. We identify the matrix algebra $M_n(k)$ with the algebra of $k$-endomorphisms $\text{End}_k(E)$.

Let $L = E \otimes_k E$ and let $\varphi : L \to \text{End}_k(E)$ be the $k$-linear homomorphism given on pure tensors by

$$\varphi(x \otimes y)(z) = \text{Tr}_{E/k}(yz)x.$$  \hfill (5.2)

It is easy to see that $\varphi$ is an isomorphism of $k$-vector spaces. (Since it is essentially the canonical isomorphism $E \otimes_k E^* \cong \text{End}_k(E)$ as $k$-vector spaces, where $E$ and its dual $E^*$ have been identified via the trace form of $E$.)

**Lemma 5.3.** Let $x, y \in E$. then $\text{Tr}(\varphi(x \otimes y)) = \text{Tr}_{E/k}(yx)$.

**Proof.** Choose a basis for $E$ and write down the matrix of $\varphi(x \otimes y)$ with respect to this basis. $\square$

**Proposition 5.4.** Let $\varphi$ be the map of (5.2). Then for all $u, v \in L$ we have

$$\text{Tr}_{L/k}((b \otimes 1)uv) = \text{Tr}(b\varphi(u)\varphi(v)).$$  \hfill (5.3)

where $\overline{\cdot}$ is the involution on $L$ given by $\overline{x \otimes y} = y \otimes x$. In particular, the map $\varphi$ is an isometry between the quadratic spaces $(L, \text{Tr}_{L/k}((b \otimes 1)uv))$ and $(\text{End}_k(E), \text{Tr}(bz^2))$. 

74
Proof. It is enough to prove (5.3) for \(u\) and \(v\) of the form \(u = x \otimes y\) and \(v = x' \otimes y'\).

By direct computation we have

\[
\{ \varphi(u) \varphi(v) b \}(w) = \varphi(u) (\text{Tr}_{E/k}(y'bw)x') \\
= \text{Tr}_{E/k}(y'bw) \varphi(u)(x') \\
= \text{Tr}_{E/k}(y'bw) \text{Tr}_{E/k}(yx')x \\
= \text{Tr}_{E/k}(yx') \cdot \varphi(x \otimes y'b)w.
\]

It follows from the above computation and Lemma 5.3. that

\[
\text{Tr}(\varphi(u) \varphi(v)) = \text{Tr}_{E/k}(bxy') \text{Tr}_{E/k}(yx') \\
= \text{Tr}_{L/k}(bxy') \otimes yx' \\
= \text{Tr}_{L/k}((b \otimes 1)(x \otimes y)(x' \otimes y')) \\
= \text{Tr}_{L/k}((b \otimes 1)u\tilde{v}).
\]

Similarly we have that \(\text{Tr}_{L/k}((1 \otimes b)u\tilde{v}) = \text{Tr}(b_\varphi(u) \varphi(v))\). Let \(J = (b \otimes 1 + 1 \otimes b)/2\).

Hence \(\text{Tr}_{L/k}(Ju\tilde{v}) = \text{Tr}(b_\varphi(u) \varphi(v))\). Since \(\text{Tr}_{L/k}(Ju\tilde{v})\) is the symmetric bilinear form associated to \(\text{Tr}_{L/k}((b \otimes 1)u\tilde{u})\), the last statement of the proposition follows.

\(\square\)

The Proposition 5.4 allows us to reduce our problem to the case when the underlying algebra is a commutative étale algebra. This situation is generally better understood. In particular, the Proposition 5.4 will allow us to compute invariants for \(\text{Tr}(bx^2)\).

The following result has been proved by David Lewis in [12. Section 4]. This can also be proved using 5.4.

**Corollary 5.5.** If the form \(Q_b = \text{Tr}(bx^2)\) is nondegenerate, then its discriminant is equal to \((-1)^{n(n-1)/2} \det b\).

75
Proof. From 5.4. the discriminant of $Q_b$ is equal to the discriminant of $\text{Tr}_{L/k}(b \otimes 1)u \bar{u}$). Since the bilinear form associated to $\text{Tr}_{L/k}(b \otimes 1)u \bar{u}$ is $\text{Tr}_{L/k}(Ju \bar{v})$, we have

$$\text{disc}(Q_b) = \det(\text{Tr}_{L/k}(Ju \bar{v}))$$

$$= \mathcal{N}_{L/k}(J) \cdot \det(\text{Tr}_{L/k}(u \bar{v})).$$

By direct computation, we get that $\det(\text{Tr}_{L/k}(u \bar{v})) = (-1)^{n(n-1)/2}$. It remains to show that $\mathcal{N}_{L/k}(J) = \det b$. Let $e_1, \ldots, e_n$ be the set of indecomposable idempotents for the algebra $E_s = E \otimes k_s$. Hence $b = \sum_{i=1}^n b_i e_i$ for some $b_1, \ldots, b_n \in k_s$. Since $1 = \sum_{j=1}^n e_j$, we have

$$b \otimes 1 = \sum_{i=1}^n b_i e_i \otimes \sum_{j=1}^n e_j = \sum_{i,j=1}^n b_i e_i \otimes e_j$$

and

$$1 \otimes b = \sum_{i,j=1}^n b_j e_i \otimes e_j.$$

Hence $J = \sum_{i,j=1}^n \frac{b_i + b_j}{2} e_i \otimes e_j$, and

$$\mathcal{N}_{L/k}(J) = \prod_{i,j=1}^n \frac{b_i + b_j}{2}$$

$$= \left( \prod_{i=1}^n b_i \right) \left( \prod_{i<j} \frac{b_i + b_j}{2} \right) \left( \prod_{j<i} \frac{b_i + b_j}{2} \right)$$

$$\equiv \det b \pmod{k^2}. $$

Note that $\prod_{i<j} \frac{b_i + b_j}{2}$ is invariant under the action of $\Gamma = \text{Gal}(k_s/k)$, thus it is in $k$. □

Let $e_1, \ldots, e_n$ be the system of indecomposable idempotents for the algebra $E_s = E \otimes k_s$. Then $\mathcal{S} := \{e_i \otimes e_j : i, j = 1, \ldots, n\}$ is a system of indecomposable idempotents for $E_s \otimes E_s$.

The factors in the decomposition of $L = E \otimes E$ as a product of fields are in one-to-one correspondence with the orbits of the Galois group $\Gamma$ acting on $\mathcal{S}$. The set $\mathcal{S}$ splits as a disjoint union of $\Gamma$-stable subsets

$$\mathcal{S} = \{e_i \otimes e_i : i = 1, \ldots, n\} \cup \{e_i \otimes e_j : i \neq j; i, j = 1, \ldots, n\}.$$
This corresponds to a splitting of $L$ as a product of algebras

$$L = E \times M.$$  \hfill (5.4)

Note that the involution $\overline{xy} = y \otimes x$ on $E \otimes E$ is the identity on the factor $E$ in (5.4) and permutes all the idempotents corresponding to $M$. An immediate consequence of the last observation is the following Lemma:

**Lemma 5.6.** The algebra $M$ of (5.4) splits, as an algebra with involution, in the form

$$M = \prod_{i=1}^{r} L_i.$$ \hfill (5.5)

where $L_i$ is either a field preserved by the involution and on which the involution is not the identity, or a product $L_i = F_i \times F_i$ where $F_i$ is a field and the involution on $L$ interchanges the two factors of $L_i$. \hfill \square

Given $b \in E$, we denote by $T_b$ the form $\text{Tr}_{E/k}(br^2)$ on $E$ and by $S_b$ the form $\text{Tr}_{M/k}(b \otimes 1z\bar{z})$ on $M$. Using Proposition 5.4 and the above decomposition (5.4), we can write $Q_b$ as an orthogonal sum

$$Q_b \simeq T_b \perp S_b.$$ \hfill (5.6)

We know that $\text{disc}(T_b) = \det(b) \cdot d_{E/k}$. Thus by Corollary 5.5 we have $\text{disc}(S_b) = (-1)^{n(n-1)/2}d_{E/k}$; in particular, $\text{disc}(S_b)$ is independent of $b$.

We shall next calculate the invariant $w_2$ of the form $Q_b$. It is easier first to calculate $w_2$ of the form $Q_1 \perp Q_b$ and then use the addition formulas. Recall that if $q_1$ and $q_2$ are quadratic forms over $k$, then

$$w_2(q_1 \perp q_2) = w_2(q_1) + w_2(q_2) + (\text{disc}(q_1),\text{disc}(q_2)) \quad (\text{see } 1.19).$$ \hfill (5.7)

From (5.6), we obtain

$$Q_1 \perp Q_b \simeq (T_1 \perp T_b) \perp (S_1 \perp S_b).$$ \hfill (5.8)
By taking $w_2$ on both sides, we get

$$w_2(Q_1 \perp Q_b) = w_2(T_1 \perp T_b) + w_2(S_1 \perp S_b). \quad (5.9)$$

(Note that $\text{disc}(S_b \perp S_1)$ is a square.)

Let $F_i \subset L_i$ be the field fixed by the involution. Let $J_i \in F_i$ be the component of $J = (1 \otimes b + b \otimes 1)/2$ in $L_i$. Let $S_i^b(z) = \text{Tr}_{L_i/k}(J_i z\bar{z})$. With this notation, we have

$$S_1 \perp S_b = \bigoplus_{i=1}^{r} (S_i^1 \perp S_i^b). \quad (5.10)$$

The following result gives an expression for $w_2$ for each of the terms on the right-hand side of (5.10). The argument in the proof is essentially the same given in [15. Proposition 2.1].

**Proposition 5.7.** Let $J_i \in F_i$ be the component of $J$ in $L_i$. Write $L_i = F_i[t]/(t^2 - d_i)$ with $d_i \in F_i$. Then

$$w_2(S_i^1 \perp S_i^b) = \text{Cor}_{F_i/k}(d_i, -J_i) + [F_i : k](-1, -1). \quad (5.11)$$

where $\text{Cor}_{F_i/k} : \text{Br}(F_i) \to \text{Br}(k)$ is the corestriction map (see Section 2.1).

**Proof.** Define $X_i^b := \text{Tr}_{L_i/F_i}(z\bar{z}) \perp \text{Tr}_{L_i/F_i}(J_i z\bar{z})$. This is a four dimensional quadratic form over $F_i$. Note that

$$X_i^b =< 1, J_i > \otimes \text{Tr}_{L_i/F_i}(z\bar{z})$$

$$= < 1, J_i > \otimes < 1, -d_i >$$

$$= < 1, J_i, -d_i, -J_i d_i >.$$

Hence $X_i^b \in I^2(F_i)$.

Riehm [20. §6] proved that the following diagram is commutative

$$
\begin{array}{ccc}
I^2(F_i) & \xrightarrow{\Phi_{F_i}} & \text{Br}_2(F_i) \\
\downarrow^{\text{Tr}_{F_i/k}} & & \downarrow^{\text{Cor}_{F_i/k}} \\
I^2(k) & \xrightarrow{\Phi_k} & \text{Br}_2(k).
\end{array}
$$
where the maps $\Phi_k$ and $\Phi_{F_i}$ are given by the Witt invariant (in Scharlau's book [21] terminology). Hence we have

$$
\Phi_k(S_1 \perp S_b) = \Phi_k(\text{Tr}_{F_i/k} X_i) = \text{Cor}_{F_i/k}(X_i) = \text{Cor}_{F_i/k}(d_i - \beta_i).
$$

The result follows using the well-known formulas relating the Witt invariant with the Hasse invariant (see [21. pg 81]). □

**Remark 5.8.** An alternative proof of (5.11) can be given using the general formula of B. Kahn [8. Théorème 2] for the corestriction of total Stiefel-Whitney invariants.

As an immediate application, we have

**Corollary 5.9.** Keeping the above notation,

$$
w_2(S_1 \perp S_b) = \frac{n(n-1)}{2} (-1, -1) + \sum_{i=1}^r \text{Cor}_{F_i/k}(d_i - \beta_i).
$$

**Proof.** This follows immediately from Proposition 5.7 and equation (5.7). Recall that $\text{disc}(S_1 \perp S_b)$ is a square, thus $w_2$ behaves additively on (5.10). □

We can now state the corresponding result for $Q_b$:

**Theorem 5.10.** With the notation above, we have

$$
w_2(Q_b) = w_2(Q_1) + w_2(\frac{1}{2} \text{Tr}_{E'/k}(x^2)) + \frac{n(n-1)}{2} (-1, -1) \det b)
$$

$$
+ \sum_{i=1}^r \text{Cor}_{F_i/k}(d_i - \beta_i).
$$

(5.12)

where $E' = E[t]/(t^2 - b)$.

**Proof.** From (5.9) and Corollary 5.9 we obtain

$$
w_2(Q_1 \perp Q_b) = w_2(T_1 \perp T_b) + \sum_{i=1}^r \text{Cor}_{F_i/k}(d_i - \beta_i) + \frac{n(n-1)}{2} (-1, -1)
$$

79
Hence using that $\text{disc}(Q_b) = \text{det}(b)(-1)^{n(n-1)/2}$, we have

$$w_2(Q_b) = w_2(Q_1) + w_2(Q_1 \perp Q_b) + (\text{disc}(Q_1) \cdot \text{disc}(Q_b))$$

$$= w_2(Q_1) + w_2(T_1 \perp T_b) + \frac{n(n-1)}{2}(-1 - \text{det } b)$$

$$+ \sum_{i=1}^{r} \text{Cor}_{F/k}(d_i - \beta_i)$$

$$= w_2(Q_1) + w_2(T_1 \perp T_b) + \frac{n(n-1)}{2}(-1 - \text{det } b)$$

$$+ \sum_{i=1}^{r} \text{Cor}_{F/k}(d_i - \beta_i).$$

Note that

$$T_1 \perp T_b = \text{Tr}_{E/k}x^2 + \text{Tr}_{E/k}by^2$$

$$= \text{Tr}_{E/k}(x^2 + by^2).$$

Let $z = x + ty$ with $x, y \in E$ and $t^2 = b$, so $z^2 = x^2 + by^2 + 2xyt$. Hence

$$\text{Tr}_{E'/E}(z^2) = 2(x^2 + by^2),$$

that is, $x^2 + by^2 = \frac{1}{2} \text{Tr}_{E'/E}(z^2)$. It follows that

$$\text{Tr}_{E/k}(x^2 + by^2) = \frac{1}{2} \text{Tr}_{E/k}\text{Tr}_{E'/E}(z^2) = \frac{1}{2} \text{Tr}_{E'/k}(z^2).$$

Thus $w_2(T_1 \perp T_b) = w_2(\frac{1}{2} \text{Tr}_{E'/k}(x^2))$. Therefore we have the desired formula. □

**Remark 5.11.** The term $w_2(Q_1)$ of (5.12) is easy to compute directly:

$$w_2(Q_1) = \frac{m(m-1)}{2}(-1, -1), \text{ where } m = \frac{n(n-1)}{2}. $$

The term $w_2(\frac{1}{2} \text{Tr}_{E'/k}(x^2))$ of (5.12) can be described using Serre’s formula 4.9, but we have to account for the factor $\frac{1}{2}$.

For an arbitrary quadratic form $Q = \langle a_1, \ldots, a_n >$ and $\lambda \in \hat{k}$, we have that

$$w_2(\lambda Q) = \sum_{i<j} \left[ (\lambda) + (a_i) \right] \cdot \left[ (\lambda) + (a_j) \right]$$

$$= \sum_{i<j} (\lambda) \cdot (\lambda) + (\lambda) \sum_{i<j} (a_i) + (\lambda) \sum_{i<j} (a_j) + \sum_{i<j} (a_i) \cdot (a_j)$$

$$= \frac{n(n-1)}{2}(-1, \lambda) + (n-1)(\lambda, \text{disc}(Q)) + w_2(Q).$$

Now take $\lambda = \frac{1}{2} \equiv 2 \pmod{k^2}$ and $Q = \text{Tr}_{E'/k}(x^2)$. Hence $\text{disc } Q = d_{E'}$ and from Serre’s formula $w_2(Q) = e^*_{E'}(s_{2n}) + (2.d_{E'})$. Here $e^*_{E'} : \Gamma \to \Sigma_{2n}$ is the homomorphism defining $E'$. Hence using that $(-1, 2) = 0$ (because $<1, -2, -2>$ is isotropic), we get

$$w_2(\frac{1}{2}\text{Tr}_{E'/k}(x^2)) = \frac{n(n-1)}{2}(-1, 2) + (n-1)(2.d_{E'}) + e^*_{E'}(s_{2n}) + (2.d_{E'})$$

$$= n(2.d_{E'}) + e^*_{E'}(s_{2n}).$$

For $n$ even, $w_2(\frac{1}{2}\text{Tr}_{E'/k}(x^2)) = e^*_{E'}(s_{2n})$.

### 5.2 The general case

Let $(\mathcal{X}, a)$ be a general pointed algebra. By Proposition 5.2, we can assume that $a \in \mathcal{X}$ is semisimple. By Lemma 1.49, we can assume, without loss of generality, that $(\mathcal{X}, a)$ is a twist of a pointed algebra of the form $(M_n(k), b)$.

In this section we shall compare the quadratic forms $Q_{\mathcal{X}, a}$ and $Q_{M_n(k), b}$. For simplicity, we shall write $Q_b$ for $Q_{M_n(k), b}$ as we did in the previous section.

The same argument used in the proof of Proposition 4.11 shows that if $n$ is odd, then $Q_{\mathcal{X}, a} \cong Q_b$. Hence the situation for $n$ odd is particularly simple.

For the case when $n$ is even, we shall establish relations between the lower Stiefel-Whitney invariants of $Q_{\mathcal{X}, a}$ and $Q_b$ using Galois cohomology.

Let $G$ be the automorphism group of the pointed algebra $(M_n, b)$, regarded as an algebraic group over $k$. We shall first investigate the structure of $G$.

By the Skolem-Noether Theorem, the elements of $G$ are the inner automorphisms of $M_n$. Since they must fix $b$, we have

$$G \cong Z_{\text{GL}_n}(b)/\text{GL}_1.$$

where $Z_{\text{GL}_n}(b)$ is the centralizer of $b$ in $\text{GL}_n$ and $\text{GL}_1$ is the subgroup of scalar matrices.
Since $b$ is semisimple, the vector space $V = k^n$ is equal to the direct sum of its eigenspaces $V_1, V_2, \ldots, V_r$. Hence over the separable closure $k_s$, the group $Z_{\text{GL}_n}(b)$ admits the decomposition

$$Z_{\text{GL}_n}(b) = \prod_{i=1}^{r} \text{GL}(V_i). \quad (5.13)$$

This shows that $G$ is a connected reductive algebraic group.

Clearly the group $G$ acts on $M_n$ by automorphisms of $Q_b$. Equivalently, $G \subset O(Q_b)$. Since $G$ is connected, we must actually have $G \subset \text{SO}(Q_b)$. This simple observation has a nontrivial consequence:

**Proposition 5.12.** $w_1(Q_{A,a}) = w_1(Q_b)$.

**Proof.** Let $\text{det.} : H^1(k. O(Q_b)) \to H^1(k. \mathbb{Z}/2)$ be the map induced by the determinant map $O(Q_b) \to \mathbb{Z}/2$. It is easy to see directly from the cocycles that if $c_q$ is the class in $H^1(k. O(Q_b))$ corresponding to a quadratic form $q$, then $w_1(q) = w_1(Q_b) + \text{det.}(c_q)$. In particular, if $c_q$ is represented by a cocycle with values in $\text{SO}(Q_b)$, as is the case for $q = Q_{A,a}$, then $w_1(q) = w_1(Q_b)$. \qed

**Remark 5.13.** David Lewis proved the equivalent of Proposition 5.12 using generic splitting fields ([11, Proposition 3.1]).

Let $G^1 = Z_{\text{GL}_n}(b) \cap \text{SL}_n$. Observe that the restriction to $G^1$ of the canonical projection $Z_{\text{GL}_n}(b) \to G$ is an isogeny. Its kernel is $\mu_n$, the group of $n^{\text{th}}$ roots of unity. Hence we have the following exact sequence

$$1 \to \mu_n \to G^1 \to G \to 1.$$

Let $S \subset Z_{\text{GL}_n}(b)$ be a maximal torus defined over $k$. Then $T = S/\text{GL}_1$ and $T^1 = S/\text{SL}_n$ are maximal tori in $G$ and $G^1$ respectively.

By (5.13), the rank of $S$ is $n$. Hence $S$ is conjugated in $\text{GL}_n$ to the group of diagonal matrices $D_n$, say $S = gD_ng^{-1}$. Let $\pi_1, \ldots, \pi_n$ be the canonical projections.
Define $\chi_i : S \rightarrow GL_1$ by $\chi_i(t) = \pi_i(g^{-1}tg)$ for $1 \leq i \leq n$ (notice that the $\chi_i$'s are the weights for $S$ acting on $k^*_n$ via the inclusion $S \hookrightarrow GL_n$).

**Lemma 5.14.** Let $\rho : Z_{GL_n}(b) \rightarrow GL(M_n)$ be the restriction of the adjoint representation $\text{Ad} : GL_n \rightarrow GL(M_n)$. Then the weights of $\rho$ relative to $S$ are $\chi_i - \chi_j$ for $i, j = 1, \ldots, n$.

**Proof.** First we need to check that for all $t \in S$

$$\rho(t)(a_{kl}) = (\chi_i - \chi_j)(t)(a_{kl}) \text{ for some } 0 \neq (a_{kl}) \in M_n.$$  

Since $t \in S$, then $g^{-1}tg = \lambda \in D_n$. So $\chi_i(t) = \pi_i(\lambda)$ and $\rho(t) = \text{Ad}(\lambda)$. Let $\lambda = \text{diag}(\lambda_1, \ldots, \lambda_n)$. then for $(a_{kl}) \in M_n$

$$\text{Ad}(\lambda)(a_{kl}) = \lambda(a_{kl})\lambda^{-1} = (\lambda_k\lambda_l^{-1}a_{kl}).$$

On the other hand, $(\pi_i - \pi_j)(\lambda) = \lambda_i\lambda_j^{-1}$. so $(\pi_i - \pi_j)(\lambda)(a_{kl}) = (\lambda_i\lambda_j^{-1})(a_{kl})$. Hence

$$(\lambda_k\lambda_l^{-1}a_{kl}) = (\lambda_i\lambda_j^{-1})(a_{kl}).$$

If $i = j$, any matrix $(a_{kl}) \in D_n$ satisfies the equality. For $i = 1, \ldots, n$, all $\chi_i - \chi_i$ correspond to the trivial weight and each has multiplicity $n$. If $i \neq j$ the matrices $(a_{kl})$ with $a_{kl} = 0$ for all $k \neq i$ and $l \neq j$ satisfy the equality. Each of the nontrivial weights $\chi_i - \chi_j$ $(i, j \neq i, j)$ has multiplicity 1.

Now by counting the multiplicities, we can conclude that the weights $\chi_i - \chi_j$ ($i, j = 1, \ldots, n$) are all the weights of $\rho$ relative to $S$. □

**Remark 5.15.** When we restrict $\rho$ to $G^1$ the weights of $\rho$ relative to $T^1$ are again $\chi_i - \chi_j$, but we must consider the restrictions $\chi_i : T^1 \rightarrow GL_1$. Note that the characters $\chi_i : S \rightarrow GL_1$ don't factor through $T = S/GL_1$, but the characters $\chi_i - \chi_j$ do factor through $T$. Moreover, they are the weights of the representation $\rho : G \rightarrow SO(Q_b)$ relative to $T$.  

83
Proposition 5.16. Let $\pi : \text{Spin}(Q_b) \to \text{SO}(Q_b)$ be the canonical projection and $\rho : G^1 \to \text{SO}(Q_b)$ the adjoint representation. Then there exists a homomorphism $\tilde{\rho} : G^1 \to \text{Spin}(Q_b)$ such that $\pi \circ \tilde{\rho} = \rho$.

Proof. We shall verify the condition of Theorem 3.37. According to Lemma 5.14, the nonzero weights of $\rho$ are $\chi_i - \chi_j$ ($i \neq j$). Since the multiplicity of each of these weights is 1, by Theorem 3.37, the obstruction for the existence of $\tilde{\rho}$ is given by the class of $\rho^*(d) = \sum_{i<j}(\chi_i - \chi_j)$ in $X(T^1)/2X(T^1)$. This class is shown below to be trivial:

$$\rho^*(d) \equiv \sum_{i<j}(\chi_i + \chi_j) \pmod{2X(T^1)} \equiv (n-1)(\chi_1 + \cdots + \chi_n) \pmod{2X(T^1)}.$$

Since $(n-1)$ is odd, we need to show that $\chi_1 + \cdots + \chi_n = 0$ in $X(T^1)$. Consider the exact sequence $1 \to T^1 \to S \xrightarrow{\det} \text{GL}_1 \to 1$. This induces an exact sequence of character groups

$$0 \to X(\text{GL}_1) \xrightarrow{\det^*} X(S) \to X(T^1) \to 0.$$

Since $X(\text{GL}_1)$ is generated by $\text{id}$ (the identity) and $\det^*(\text{id}) = \chi_1 + \cdots + \chi_n$ we have that $\text{Im}(\det^*) = (\chi_1 + \cdots + \chi_n)$: the subgroup of $X(S)$ generated by $\chi_1 + \cdots + \chi_n$. Therefore $X(T^1) \cong X(S)/(\chi_1 + \cdots + \chi_n)$. □

Let $\rho : G \to \text{SO}(M_n, Q_b)$ be the representation given by $\rho(g)(x) = gxg^{-1}$. The following diagram of algebraic groups over $k$ is commutative and the rows are exact sequences.

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_n & \longrightarrow & G^1 & \longrightarrow & G & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \text{Spin}(Q_b) & \longrightarrow & \text{SO}(Q_b) & \longrightarrow & 1.
\end{array}
$$

Lemma 5.17. For $n$ even, the induced map $\tilde{\rho} : \mu_n \to \mu_2$ in the above diagram is nontrivial.
Proof. By the same computation as in (5.14), we have $\rho^*(d) \equiv (n - 1)(\chi_1 + \cdots + \chi_n)$ (mod $2X(T)$). Since $\chi_1 + \cdots + \chi_n \neq 0$ in $X(T)$ and $(n - 1)$ is odd, $\rho^*(d) \notin 2X(T)$.

Thus, by Theorem 3.37, the homomorphism $\rho : G \rightarrow SO(Q_b)$ cannot be lifted to $\text{Spin}(Q_b)$. Hence $\tilde{\rho} : \mu_n \rightarrow \mu_2$ is nontrivial, for otherwise $\tilde{\rho} : G^1 \rightarrow \text{Spin}(Q_b)$ would factor through $G$. □

We are now ready to prove the main result of this section:

**Theorem 5.18.** Let $Q_b$ and $Q_{A,a}$ be as above. Then

$$w_2(Q_{A,a}) = w_2(Q_b) + \frac{n(n - 1)}{2} [A],$$

where $[A]$ is the class of $A$ in the Brauer group $\text{Br}(k) = H^2(k, GL_1)$.

Proof. We assume first that $n$ is even. The set $H^1(k, G)$ classifies all the pointed algebras that are twists of $(M_n(k), b)$. Let $[A, a]$ denote the cohomology class in $H^1(k, G)$ associated with $(A, a)$. Let $[Q_{A,a}] \in H^1(k, SO(Q_b))$ be the class associated with the form $Q_{A,a}$. Taking cohomology in (5.15), we obtain a commutative diagram:

$$
\begin{array}{ccc}
H^1(k, G) & \xrightarrow{\partial} & H^2(k, \mu_n) \\
\rho^* \downarrow & & \rho^* \\
H^1(k, SO(Q_b)) & \xrightarrow{\partial'} & H^2(k, \mu_2).
\end{array}
$$

(5.16)

where $\partial$ and $\partial'$ are the coboundary maps.

It is easy to see that $\rho_*[A, a] = [Q_{A,a}]$ and that $\partial[A, a] = [A]$, the class of $A$ in $H^2(k, \mu_n) = \text{Br}_n(k)$.

By Springer's Theorem 2.22 (in additive notation), we have

$$w_2(Q_{A,a}) = w_2(Q_b) + \partial' \rho_*[A, a]$$

$$= w_2(Q_b) + \tilde{\rho}_*[A].$$

(5.17)

In the second equality we use the commutativity of diagram (5.16).
On the other hand, by Lemma 5.17, we have

$$\tilde{\rho}_2[\mathcal{A}] = \frac{n}{2}[\mathcal{A}]$$

Combining this equality with (5.17), we get

$$w_2(Q_{A,a}) = w_2(Q_b) + \frac{n}{2}[\mathcal{A}]$$

In the case when \( n \) is odd, we clearly have \( w_2(Q_{A,a}) = w_2(Q_b) \) because \( Q_{A,a} \cong Q_b \). Since the order of \([\mathcal{A}]\) is a divisor of \( n \), we can write a single formula for both \( n \) even and \( n \) odd:

$$w_2(Q_{A,a}) = w_2(Q_b) + \frac{n(n-1)}{2}[\mathcal{A}] \quad \Box$$

Finally, putting together Theorem 5.18 and Theorem 5.10 we obtain the most general formula:

**Theorem 5.19.** With the notation of Proposition 5.7 and Theorem 5.10, we have

$$w_2(Q_{A,a}) = w_2(Q_1) + \frac{n(n-1)}{2}[\mathcal{A}] + w_2\left(\frac{1}{2}\text{Tr}_{E'/k}(x^2)\right) + \frac{n(n-1)}{2}(-1 \cdot \det b) + \sum_{i=1}^{r} \text{Cor}_{F_i/k}(d_i, -\beta_i).$$

(5.18)

where \( E' = E[t]/(t^2 - b) \). \( \Box \)

See Remark 5.11 for the computation of the terms \( w_2(Q_1) \) and \( w_2\left(\frac{1}{2}\text{Tr}_{E'/k}(x^2)\right) \) in (5.18).
References


Vita

Rosalí Brusamarello was born on August 31, 1965, in Antônio Prado, state of Rio Grande do Sul, Brazil. She finished her undergraduate studies in “Licenciatura Plena em Matemática” at the Universidade Federal do Mato Grosso do Sul in December 1988. She earned a master of science degree in mathematics from Universidade de São Paulo in August 1991. From 1991 to 1994 she worked as an instructor at Universidade Estadual de Maringá, state of Paraná, Brazil. In August 1994 she came to the United States, on leave from her university, to pursue graduate studies in mathematics at Louisiana State University. She is currently a candidate for the doctoral degree in mathematics, which will be awarded in May 1998.
DOCTORAL EXAMINATION AND DISSERTATION REPORT

Candidate: Rosali Brusamarello

Major Field: Mathematics

Title of Dissertation: On the Second Stiefel-Whitney Class of Scaled Trace Forms of Central Simple Algebras

Approved:

Major Professor and Chairman

Dean of the Graduate School

EXAMINING COMMITTEE:

J. Hurewicz

Steven H. Weintraub

Lawrence Smith

Frank W. Zhou

Date of Examination: 3/12/98

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.