Hensel's lemma for the norm principle for type D_n groups

by

Amin Soofiani

B.Sc., University of Tehran, 2017

M.Sc., University of British Columbia, 2019

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in

The Faculty of Graduate and Postdoctoral Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

March 2025

The following individuals certify that they have read, and recommend to the Faculty of Graduate and Postdoctoral Studies for acceptance, the thesis entitled:

Hensel's lemma for the norm principle for type D_n groups

submitted by **Amin Soofiani** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy** in **Mathematics**.

Examining Committee:

Sujatha Ramdorai, Professor, Mathematics, UBC
Supervisor

Vladimir Chernousov, Professor, Mathematics, University of Alberta
Co-supervisor

Zinovy Reichstein, Professor, Mathematics, UBC
Supervisory Committee Member

Ben Williams, Associate Professor, Mathematics, UBC
Supervisory Committee Member

Malabika Pramanik, Professor, Mathematics, UBC
University Examiner

Michael Friedlander, Professor, Mathematics, UBC
University Examiner

Ján Mináč, Professor, Mathematics, Western University
External Examiner

Abstract

Classical norm principles examine the behavior of quadratic forms and central simple algebras under the extensions of the base field. Merkurjev reformulated them as a property of algebraic groups, and Gille reformulated them as a property of torsors under algebraic groups using Galois cohomology. After recalling the classical norm principles, we will show that Merkurjev's formulation of the norm principle for reductive linear algebraic groups is equivalent to Gille's formulation for torsors under semisimple groups. We will then prove that it is sufficient to show the norm principle for simply connected groups. Among classical groups, the only case for which the norm principle is open, are groups of type D_n. Absolutely simple, simply connected, classical groups of type D_n are spinor groups of central simple algebras with orthogonal involution. We will reduce the norm principle for the spinor groups to the case that the field extension has degree 2. We then focus on the spinor groups of skew-hermitian forms defined over quaternion algebras and will reduce the question in this case to the case that the skew-hermitian form is anisotropic. Let K be a complete discretely valued field with residue field k with $char(k) \neq 2$. Suppose that the norm principle holds for spinor groups $Spin(h)$ for every nonsingular skew-hermitian form h defined over every quaternion algebra with canonical involution defined over finite separable extensions of k. Then we will show that it holds for spinor groups $Spin(H)$ for every nonsingular skew-hermitian form H defined over every quaternion algebra with canonical involution defined over K.

Lay Summary

Groups are fundamental objects in mathematics, capturing the symmetries of other mathematical structures. The development of modern geometry and number theory would not have been possible without the concept of groups. Group theory also has applications beyond mathematics, including in fields such as physics, chemistry, materials science, and information security.

Linear algebraic groups, a branch of group theory, has emerged as an active area of research. These groups are closely related to other algebraic structures, such as quadratic and hermitian forms, central simple algebras, and Galois cohomology. A key conjecture in the theory of linear algebraic groups is the Norm Principle, which has connections to deep questions in the field, such as local-global principles and rationality problems.

This thesis establishes new results about the Norm Principle for linear algebraic groups of type D_n.

Preface

This dissertation is based on an original research project by the author, Amin Soofiani. The main results have been submitted for publication, and the manuscript is available on arXiv under the title **Hensel's lemma for the norm principle for spinor groups** (arXiv: 2412.15737). Additionally, the computational results from Chapter 7 are included in the manuscript **An explicit formula for Larmour's decomposition of hermitian forms**, which has been accepted for publication in the Journal of the Ramanujan Mathematical Society. This manuscript is also available on arXiv (arXiv: 2412.11110).

Table of Contents

List of Figures

Acknowledgements

First and foremost, I would like to thank my advisors, Vladimir Chernousov and Sujatha Ramdorai. I am deeply indebted to them for their invaluable support throughout my PhD. Their clarity of thought and passion for mathematics have always been a great source of inspiration to me.

I would also like to express my gratitude to the members of my PhD committee, Zinovy Reichstein, Ben Williams, and Ján Mináč, for their insightful and constructive feedback.

Last but not least, I would like to thank my parents and my sister for their endless love, support, and encouragement. They have always been there for me, and this journey would not have been possible without them.

Chapter 1

Introduction

To any finite separable field extension L/K, one can associate a particular map called the "norm" map from L to K. For a given algebraic group G over K, we can consider the base change of this group from K to L. The "norm principle for G" is a question regarding the behavior of the base change of G from K to L with respect to the norm map of the field extension L/K. It is an open question whether it holds for all algebraic groups. In this dissertation we study this question for groups of type D_n (this is the only open case among the classical groups).

1.1 Three classical theorems

Let K be a field, $char K \neq 2$, and L/K be a finite separable field extension. We recall three classical theorems from central simple algebras and quadratic form theory which examines the behavior of the base change of these objects with respect to the norm map of the field extensions.

Theorem 1.1.1. (The norm principle for a reduced norm map of central simple algebras) Let D be a central simple algebra over K. Consider the algebraic group $GL_1(D)$ and the reduced norm map

$$Nrd : GL_1(D) \longrightarrow \mathbb{G}_m.$$

If an element $x \in L^*$ is the reduced norm of an element in $GL_1(D)(L)$, then $N_{L/K}(x)$ is a reduced norm of an element of $GL_1(D)(K)$.

In other words, for the following diagram

$$\begin{array}{ccc} GL_1(D)(L) & \xrightarrow{Nrd_L} & \mathbb{G}_m(L) \\ & & \downarrow N_{L/K} \\ GL_1(D)(K) & \xrightarrow{Nrd_K} & \mathbb{G}_m(K) \end{array}$$

we have

$$\mathrm{Im}(N_{L/K} \circ Nrd_L) \subseteq \mathrm{Im}(Nrd_K).$$

Theorem 1.1.2. (Scharlau's norm principle) Let q be a regular quadratic form over K, $GO(q)$ the group of similitudes of q, $\mu : GO(q) \longrightarrow \mathbb{G}_m$ the multiplier map, and $G(q)$ the group of similarity factors of q. If an element $x \in L^*$ belongs to $G(q)(L)$, then $N_{L/K}(x) \in G(q)(K)$.

In other words, for the following diagram

$$\begin{array}{ccc} GO(q)(L) & \xrightarrow{\mu_L} & \mathbb{G}_m(L) \\ & & \downarrow{\scriptstyle N_{L/K}} \\ GO(q)(K) & \xrightarrow{\mu_K} & \mathbb{G}_m(K) \end{array}$$

we have

$$\mathrm{Im}(N_{L/K} \circ \mu_L) \subseteq \mathrm{Im}(\mu_K).$$

Theorem 1.1.3. (Knebusch's norm principle) Let q be a regular quadratic form over K, and $Spin(q)$ the spinor group of q. Consider the central subgroup $\mu_2 \subseteq Spin(q)$, which is the kernel of the map $Spin(q) \to O^+(q)$. For any field F containing K, let $h_F : H^1(F, \mu_2) \longrightarrow H^1(F, Spin(q))$ be the induced Galois cohomology map over F. Then

$$x \in \text{Ker } h_F \Rightarrow cor_{F/K}(x) \in \text{Ker } h_K.$$

In other words, for the following diagram (induced by a finite field extension L/K)

$$\begin{array}{ccc} H^1(L, \mu_2) & \xrightarrow{h_L} & H^1(L, Spin(q)) \\ \downarrow{\scriptstyle cor_{L/K}} & & \\ H^1(K, \mu_2) & \xrightarrow{h_K} & H^1(K, Spin(q)) \end{array}$$

we have

$$cor_{L/K}(\ker\ h_L) \subseteq \ker\ h_K.$$

Scharlau and Knebusch norm principles will be discussed in more details in Sections 3.1 and 3.2.

1.2 What is the Norm Principle?

Merkurjev formulated a general definition of the norm principle for the maps from reductive groups to tori, which we recall below. We call it the H^0−variant of the norm principle.

Definition 1.2.1. **(H^0–variant of the norm principle, due to Merkurjev)** Let G be a reductive linear algebraic group, and T an algebraic torus, both defined over K. Suppose $f : G \longrightarrow T$ is an algebraic group homomorphism defined over K. Let L/K be a finite separable field extension and consider the following diagram:

$$\begin{array}{ccc} G(L) & \xrightarrow{f_L} & T(L) \\ & & \downarrow N_{L/K} \\ G(K) & \xrightarrow{f_K} & T(K). \end{array}$$

We say that the norm principle holds for $f : G \longrightarrow T$ over L/K if
$\mathrm{Im}(N_{L/K} \circ f_L) \subseteq \mathrm{Im}(f_K)$.

Also, we say that the norm principle holds for $f : G \longrightarrow T$, if for every finite separable field extension L/K we have $\mathrm{Im}(N_{L/K} \circ f_L) \subseteq \mathrm{Im}(f_K)$.

The norm principle for the reduced norm map of central simple algebras (resp. Scharlau's norm principle) is an example of the H^0– variant of the norm principle, when $G = GL_1(D)$ (resp. $G = GO(q)$), $f = Nrd$ (resp. $f = \mu$, the multiplier map) and $T = \mathbb{G}_m$ (resp. $T = \mathbb{G}_m$).

In [1], it is shown that the H^0-variant of the norm principle for the map $f : G \to T$ described above, can be reduced to the H^0-variant of the norm principle for the canonical map $G \twoheadrightarrow G^{ab}$, where G^{ab} is the quotient of G by its commutator subgroup, i.e., $G^{ab} = G/[G,G]$ (which is a torus). We say that the norm principle holds for G over L/K if the H^0-variant of the norm principle holds for the map $G \longrightarrow G^{ab}$, and we say that the H^0– variant of the norm principle holds for G if it holds over any finite separable field extension L/K. The H^0–variant of the norm principle is not known in general for reductive groups. It is known when the semisimple part of the reductive group does not contain connected components D_n; $n \geq 4, E_6$ or E_7 (see Theorem 1.3.1). Also, it holds for some groups of type D_n: the group of proper similitudes of a central simple algebra with orthogonal involution $GO^+(A,\sigma)$, and the special Clifford group $\Gamma^+(A,\sigma)$ (see Sections 5.2 and 5.3).

Now we recall a cohomological version of the norm principle for semisimple groups. We call it the H^1–variant of the norm principle. This definition is due to Gille.

Definition 1.2.2. (H^1**–variant of the norm principle, due to Gille**) Let S be a semisimple linear algebraic group over K and $Z \subseteq S$ be a central subgroup. Let L/K be a finite separable field extension and consider the following diagram

$$\begin{array}{ccc} H^1(L,Z) & \xrightarrow{\alpha_L} & H^1(L,S) \\ \downarrow cor_{L/K} & & \\ H^1(K,Z) & \xrightarrow{\alpha_K} & H^1(K,S). \end{array}$$

We say that the norm principle holds for the pair (Z,S) over L/K if for every $u \in \ker(\alpha_L)$, we have $cor_{L/K}(u) \in \ker \alpha_K$.

Also, we say that the norm principle holds for the pair (Z,S), if for every finite separable field extension L/K, and for every $u \in \ker(\alpha_L)$, we have $cor_{L/K}(u) \in \ker \alpha_K$.

Knebusch's norm principle is an example of the H^1- variant of the norm principle, when $S = Spin(q)$ and $Z = \mu_2$.

The first results of the dissertation: We will prove in Section 4.4 that the H^1- variant of the norm principle for the pair (Z,S) can be reduced to the case where Z is the center of S. It will also be shown that it can further be reduced to the case that S is a simply connected group. Furthermore, in Section 4.3, we will prove that the H^0-variant for reductive groups is equivalent to the H^1-variant for semisimple groups.

The norm principle for groups over finite fields, local fields, and number fields: We know that $H^1(K,G)$ is trivial for any reductive group G over a **finite field** K. Therefore, the H^1-variant of the norm principle holds over finite fields. Also, $H^1(K,G)$ is trivial for any semisimple simply connected group G over a **local field** K. Therefore, the H^1-variant of the norm principle holds over local fields. Furthermore, by a theorem of Gille, the H^1-variant of the norm principle holds for semisimple groups of classical type over **number fields** (see Remark 5.1.5).

1.3 Hensel's lemma for the norm principle for type D_n groups

The following theorem shows that the H^0-variant of the norm principle holds for some types of groups, regardless of the field on which they are defined.

Theorem 1.3.1. (Barquero, Merkurjev) Let G be a K-reductive group, and the Dynkin diagram of the semisimple part of G (which is the derived subgroup $[G,G]$) does not contain connected components $D_n;\ n \geq 4, E_6$ or E_7. Then the H^0- variant of the norm principle holds for G.

The H^0-variant of the norm principle is open in general for type D_n groups. In this dissertation, we focus on the norm principle for groups of type D_n.

Let G be an absolutely simple, simply connected, classical K- linear algebraic group of type D_n. Then G is the spinor group $Spin(A,\sigma)$ for a central simple K-algebra A of degree $2n$ with orthogonal involution. We denote the center of $Spin(A,\sigma)$ by Z.

The simplest case of the norm principle for type D_n is when $A = M_{2n}(K)$, and σ is the orthogonal involution on A, adjoint to a $2n-$dimensional quadratic form q over K. We have the following exact sequence of algebraic groups associated to q:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_2 & \longrightarrow & Z & \longrightarrow & \mu_2 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mu_2 & \longrightarrow & Spin(q) & \longrightarrow & O^+(q) & \longrightarrow & 1 \end{array}$$

where Z is the center of $Spin(q)$, one of the groups μ_2 is the center of $O^+(q)$ (the special orthogonal group of q), and the other μ_2 is the kernel of the map $Spin(q) \to O^+(q)$.

Scharlau's norm principle for q is in fact equivalent to the H^1−variant of the norm principle for the pair $(\mu_2, O^+(q))$. Also Knebusch's norm principle for q states that the H^1−variant of the norm principle holds for the pair $(\mu_2, Spin(q))$. But it is not known whether or not the H^1−variant of the norm principle holds for the pair $(Z, Spin(q))$. In Section 6.1, we will show that if the H^1−variant of the norm principle holds for the spinor group over any separable quadratic field extension, then it holds over any finite separable field extension (Theorem 6.1.3).

As mentioned before, the H^1−variant of the norm principle holds for all classical groups over number fields, so in particular it holds for spinor groups of quadratic forms. One of the next natural cases one can investigate is the norm principle for the spinor groups of quadratic forms defined over function fields of curves over number fields. One of the helpful and strong tools to study algebraic properties over such fields is the local-global principle, which we describe below.

Local-Global principle for algebraic groups: Let F be a number field, C a smooth projective curve over F, $K = F(C)$ the function field of C, and V the set of closed points of C. To each $c \in V$ one can associate a natural discrete valuation ν_c on K. Let K_c be the completion of K with respect to the discrete valuation ν_c, and k_c be the residue field of K_c, which is a number field. Assume that G is a linear algebraic group defined over K. There is a global-to-local map

$$\rho_{G,V} : H^1(K, G) \longrightarrow \prod_{c \in V} H^1(K_c, G).$$

The kernel of $\rho_{G,V}$ is called the Tate-Shafarevich set, denoted by $Ш_V(G)$. We say that the local-global principle holds for G, when $Ш_V(G)$ is trivial.

Theorem 1.3.2. Let F, C, K, V, ρ be as above, and Z be the center of G. Assume that the following conditions hold:

(1) The H^1−variant of the norm principle holds for (Z, G) over K_c, for each $c \in V$.

(2) The local-global principle holds for G.

Then the H^1−variant of the norm principle holds for (Z, G) over K.

Proof. Let $\alpha : H^1(-, Z) \to H^1(-, G)$ be the Galois cohomology map induced by the embedding $Z \to G$. Consider the following commutative diagram:

$$\begin{array}{ccccccc}
H^1(L,Z) & & \xrightarrow{\alpha_L} & & H^1(L,G) & & \\
\downarrow{\scriptstyle cor_{L/K}} & \searrow^{\gamma_L} & & & & \searrow^{\theta_L} & \\
& & \prod_{c\in V} H^1(K_c\otimes_K L,Z) & & \xrightarrow{\beta_L} & & \prod_{c\in V} H^1(K_c\otimes_K L,G) \\
& & \downarrow{\scriptstyle cor_{L/K}} & & & & \\
H^1(K,Z) & & \xrightarrow{\alpha_K} & & H^1(K,G) & & \\
& \searrow^{\gamma_K} & & & & \searrow^{\theta_K} & \\
& & \prod_{c\in V} H^1(K_c,Z) & & \xrightarrow{\beta_K} & & \prod_{c\in V} H^1(K_c,G).
\end{array}$$

Let $u \in \operatorname{Ker}\alpha_L$, and $(w_c)_{c\in V} \in \prod_{c\in V} H^1(K_c \otimes_K L, Z)$ be the image of u under γ_L. Hence $\beta_L(w_c)_{c\in V} = 1$. By assumption (1), the H^1−variant of the norm principle holds for the pair (Z,G) over each extension $K_c \otimes_K L/K_c$, therefore $cor_{L/K}(w_c)_{c\in V} \in \operatorname{Ker}\beta_K$. Since $\theta_K \circ \alpha_K \circ cor_{L/K}(u) = \beta_K(cor_{L/K}(w_c)_{c\in V})$ and $\operatorname{Ker}\theta_K$ is trivial by assumption (2), we have $cor_{L/K}(u) \in \operatorname{Ker}\alpha_K$. □

Theorem 1.3.2 gives us a strategy to prove the norm principle over K, which is a function field of a curve defined over a number field. The local-global principle for G, which is the second assumption in Theorem 1.3.2, is open in general and it is an important question in the theory of linear algebraic groups. In the case which we are interested in, where G is the spinor group, the local global principle is known for example in the case where the number field F is totally imaginary, and G is the spinor group of a quadratic form. However, the local-global principle is widely open even in the case of spinor groups of quadratic forms. On the other hand, when q is an even dimensional quadratic form over K, then assumption (1) of Theorem 1.3.2 holds, which is a consequence of the following theorem (recall that $C(G)$ denotes the center of G):

Theorem 1.3.3. (Bhaskar, Chernousov, and Merkurjev) Let K be a complete discretely valued field with residue field k with $char(k) \neq 2$. Assume that the H^1−variant of the norm principle holds for $(C(Spin(q)), Spin(q))$ for every nondegenerate quadratic form q of even dimension defined over any finite extension of k. Then the H^1−variant of the norm principle holds for $(C(Spin(q)), Spin(q))$ for every nondegenerate quadratic form q of even dimension over K.

Since the norm principle is known for all algebraic groups of classical type over number fields, and the residue field of each K_c in Theorem 1.3.2 is a number field, then the H^1−variant of the norm principle holds for $(C(Spin(q)), Spin(q))$ over the completions K_c described in Theorem 1.3.2. We call Theorem 1.3.3 **Hensel's lemma for the norm principle** for the spinor group of quadratic forms.

The main result of this dissertation is a generalization of Theorem 1.3.3 to the case of skew-hermitian forms over quaternion algebras.

Theorem 1.3.4. (The main result of the dissertation) Let K be a complete discretely valued field with residue field k, such that *char* $k \neq 2$. Assume that the H^1- variant of the norm principle holds for $(C(Spin(h_1)), Spin(h_1))$ for every regular skew-hermitian form h_1 over any quaternion algebra D_1 defined over any finite extension of k. Then the H^1- variant of the norm principle holds for $(C(Spin(h)), Spin(h))$ for every regular skew-hermitian form h over any quaternion algebra D over K.

The main theorem is also formulated in Section 4.5 (Theorem 4.5.3) and Chapter 8 (Theorem 8.0.1) after defining all necessary notions.

When D (in Theorem 1.3.4) splits, i.e., $D \cong M_2(K)$, then h corresponds to a quadratic form over K, and the above question has an affirmative answer in this case by Theorem 1.3.3.

Let K and k be as in Theorem 1.3.4 and assume that the H^1- variant of the norm principle holds for $(C(Spin(h_1)), Spin(h_1))$ for every regular skew-hermitian form h_1 over any quaternion algebra D_1 defined over any finite extension of k. Then for every odd number n, the H^1- variant of the norm principle holds for every group of type D_n over K. This is a consequence of Theorem 1.3.4: the simply connected cover of any semisimple group of type D_n (when n is odd) is a spinor group of a skew-hermitian form over a quaternion algebra.

1.4 The plan

Chapter 1: The current chapter is devoted to a brief introduction to the norm principle, the statement of the main result, and the plan.

Chapter 2: This chapter contains the preliminaries: involutions on central simple algebras, quadratic and hermitian forms, linear algebraic groups, and nonabelian Galois cohomology.

Chapter 3: We quickly introduce the two classical norm principles of Scharlau and Knebusch from the algebraic theory of quadratic forms. They can be reformulated as a property for the image of maps from certain reductive algebraic groups to tori.

Chapter 4: This chapter begins with the definition of the H^0- variant of the norm principle for reductive groups due to Merkurjev. Then we discuss how the norm principles of Scharlau and Knebusch can be viewed as the H^0- variant of the norm principle for maps from certain reductive groups to tori.

Section 4.2 is devoted to the formulation of the H^1- variant of the norm principle for semisimple groups due to Gille. Theorem 4.3.1 shows that the two variants are equivalent. We will then prove that the H^1- variant of the norm principle for a semisimple group G can be obtained from the norm principle for its simply connected covering $\tilde{G}$ in Section 4.4. The H^1- variant of the norm principle is known for all absolutely simple simply connected linear algebraic groups G of types A_n, B_n, and C_n (see [1]). Hence we focus on absolutely simple simply connected linear algebraic groups of type D_n (which are the spinor groups), on which the norm principle is open in general. In Section 4.5 we discuss the main question of this dissertation, namely Theorem 1.3.4: Hensel's lemma for the H^1- variant of the norm principle for $Spin(h)$ where h is a skew-hermitian form defined over a quaternion algebra D over a complete discretely valued field K. The special case of this result where D is the split quaternion algebra is known (the main result in [4]).

Chapter 5: In order to prove the main result, i.e., Theorem 1.3.4, we need to generalize Scharlau and Knebusch's norm principles from quadratic forms to the nonsplit case, i.e., for certain types of D_n groups associated with nonsplit central simple algebras with orthogonal involutions. This generalization is studied in Chapter 5. The generalization of Knebusch norm principle is due to Gille, and it is a direct consequence of Theorem 5.1.2.

Chapter 6: We reduce the H^1- variant of the norm principle for $Spin(A, \sigma)$ over L/K to the case that the field extension L/K has degree 2. Although this reduction is valid for spinor group of any central simple algebra with orthogonal involution $Spin(A, \sigma)$, we will use this reduction in the special case that A is the matrix algebra with the orthogonal involution σ adjoint to a skew-hermitian form over a quaternion algebra. Lemma 6.2.7 reduces the norm principle to the case that the skew-hermitian form h in the main question (discussed in Section 4.5) is anisotropic. This reduction is done for the skew-hermitian forms over quaternion algebras, not over any arbitrary central simple algebra.

Chapter 7: A theorem due to Larmour, which is a generalization of Springer's decomposition theorem for quadratic forms to (skew-) hermitian forms, will be introduced (see Theorem 7.3.6). This theorem will be central in the rest of the dissertation.

Chapter 8: In Chapter 8, we prove some lemmas which will be used in the proof of the main theorem in Chapter 9.

Chapter 9: In the last chapter of the dissertation we prove the main theorem, by splitting up the problem into several cases, and then providing a proof for each case. All the reductions in the previous chapters will be utilized in Chapter 9. At the end of this chapter, we discuss some applications and related open questions.

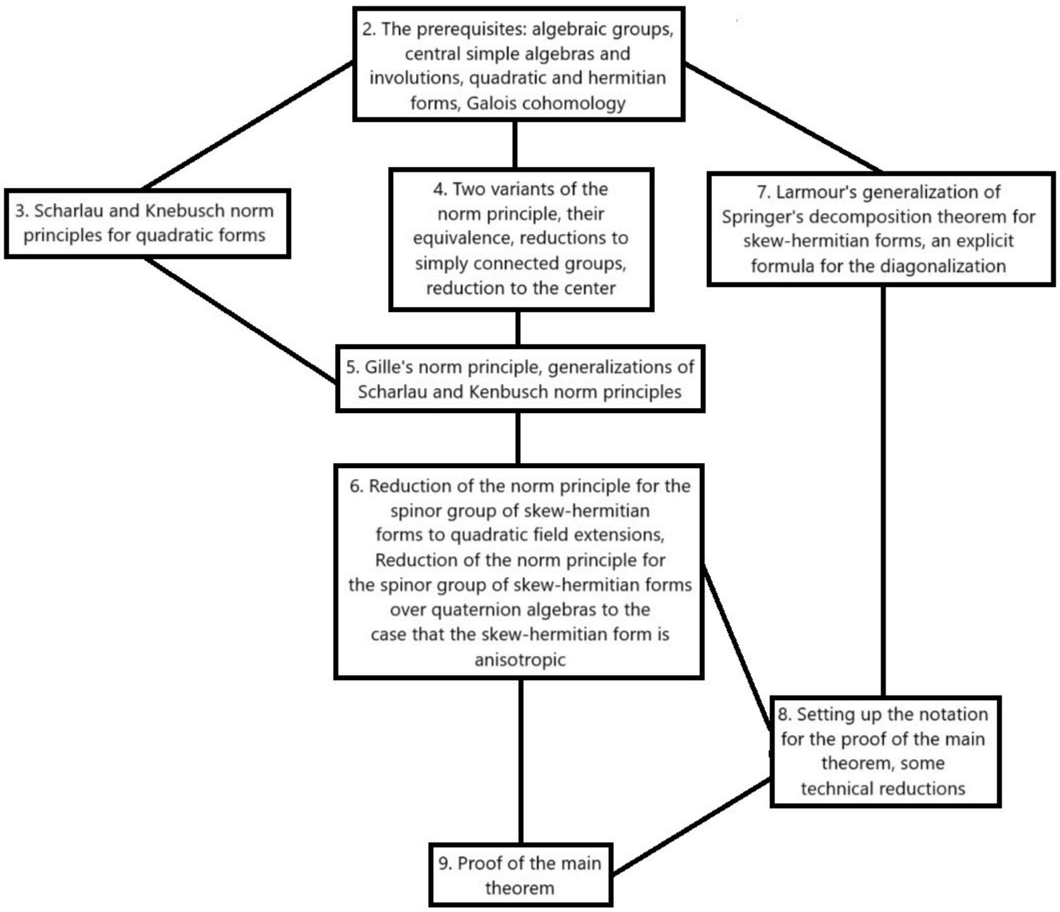


Figure 1.1: Connections between chapters

Chapter 2

The prerequisites

In this chapter we provide the background for the thesis: central simple algebras and involutions, quadratic and hermitian forms, linear algebraic groups, and Galois cohomology.

2.1 Linear algebraic groups

In this section we recall some of the basic definitions and properties of linear algebraic groups.

Linear algebraic group: Let K be a field and G be an affine variety defined over K endowed with the structure of a group. We say that G is a linear algebraic group over K if the product map $G \times G \to G$ and the inversion map $G \to G$ are morphisms of varieties.

Morphisms: Algebraic group homomorphisms are the maps which preserve both the group and variety structures of the objects. Kernels and images of algebraic group homomorphisms are again algebraic groups (see [10, Section 7.4, Proposition B]). Isomorphisms are defined accordingly. A surjective morphism with finite kernel is called an isogeny.

For any field extension L/K, we denote the group of $L-$points of G by $G(L)$.

Theorem 2.1.1. Every linear algebraic group G defined over K is a subgroup of $GL_n(K)$ for some $n \in \mathbb{N}$.

Proof. See [10, Section 8.6]. □

Examples of algebraic groups:

$GL_n = \{g \in \mathbb{A}^{n^2} \mid det(g) \neq 0\}$,

$SL_n = \{g \in GL_n \mid det(g) = 1\}$,

$O_n = \{g \in GL_n \mid g^t g = id\}$.

Theorem 2.1.2. Let G be an algebraic group defined over K. Then only one irreducible component of G (as a variety) passes through the identity element $e \in G$. We call that component the connected component of G, and denote it by G^0. Then G^0 is a normal algebraic subgroup of finite index in G.

Proof. See [10, Section 7.3]. □

Theorem 2.1.3. Let G be a linear algebraic group over K and H be a closed subgroup of G. Then the centralizer of H in G, i.e., $C_G(H)$, is a closed subgroup of G.

Proof. See [10, Section 8.2]. □

Theorem 2.1.4. The commutator subgroup $[G,G]$ of any linear algebraic group G is closed in G, and it is connected if G is.

Proof. See [10, Proposition 17.2]. □

For the definitions of direct, semidirect, and almost direct products of linear algebraic groups, we refer to [5], and [10, Section 8.4].

Algebraic torus: We say that a linear algebraic group G over K is an algebraic torus (or simply torus) if G is isomorphic to the direct product of a finite number of copies of $\mathbb{G}_m$ over $\bar{K}$. If G is already the direct product of a finite number of copies of $\mathbb{G}_m$ over K, then we say that G is a $K-$ split torus. For any linear algebraic group G over K, there exists a subtorus T in G defined over K which is maximal.

Solvable groups: We say that a linear algebraic group G is solvable if its derived series terminate in trivial group $\{1\}$, the series being defined by $D^0(G) = G$, $D^1(G) = [G,G]$, $D^{n+1}(G) = [D^n(G), D^n(G)]$, $n \geq 0$.

Jordan Decomposition: Let G be a linear algebraic group over K. We may embed G as a closed subgroup of some $GL_n(K)$ by Theorem 2.1.1. Let $x \in G$. There exist unique elements $x_s, x_u \in GL_n(K)$ such that x_s is semisimple, x_u is unipotent, and $x = x_s x_u$. For an arbitrary subgroup $G \leq GL_n(K)$, there is no reason x_s and x_u have to be in G, but they belong to G if G is closed (see [10, Sections 15.1, 15.2, and 15.3]). We call x_s and x_u the semisimple and unipotent parts of G, respectively. The semisimple and unipotent parts of each element are preserved under algebraic group morphisms (see [10, Theorem 15.3 c]). We say that x is semisimple if $x = x_s$ and unipotent if $x = x_u$. An algebraic group G is called unipotent, if all its elements are unipotent.

Semisimple linear algebraic group: Every linear algebraic group G has a unique largest normal solvable subgroup, which is automatically closed (see [10, Section 19.5]). We call this subgroup the radical of G, denoted by $R(G)$. If G is connected and $R(G)$ is trivial, then G is called semisimple. For example $SL_n(K)$ is semisimple.

Reductive linear algebraic group: Let G be a linear algebraic group. The subgroup of $R(G)$ consisting of all its unipotent elements is normal in G. We call it the unipotent radical of G, denoted $R_u(G)$. This subgroup is the largest connected normal unipotent subgroup of G. If G is connected and $R_u(G)$ is trivial, then G is called reductive. For example $GL_n(K)$, tori, and semisimple groups are reductive.

Theorem 2.1.5. Let G be a semisimple linear algebraic group, and $\{G_i \mid i \in I\}$ be the minimal closed connected normal subgroup of positive dimension. Then:

(a) Each G_i is semisimple.

(b) I is finite, for example $I = \{1, 2, \ldots, n\}$, and the product morphism $G_1 \times \cdots \times G_n \to G$ is an isogeny.

(c) $[G, G] = G$.

Proof. See [10, Theorem 27.5]. □

Each G_i in Theorem 2.1.5 is called a simple component of G. Such linear algebraic groups G_i are called simple. In other words, a semisimple linear algebraic group is called simple if it does not have any nontrivial closed connected normal subgroup. If G is simple over the separable closure of the base field, then we call it absolutely simple.

In this dissertation, we denote the center of any group G by $C(G)$.

Theorem 2.1.6. Let G be a reductive linear algebraic group. Then $R(G) = C(G)^0$ is a torus which has a finite intersection with $[G, G]$. Furthermore we have the almost direct product structure $G = [G, G] \cdot C(G)$.

Proof. See [10, Lemma 19.5 and Theorem 27.5(e)]. □

Split groups: If a semisimple linear algebraic group G defined over K contains a maximal torus which is K−split, then we say that G is K−split. Over the separable closure of the base field, any semisimple linear algebraic group becomes split.

Simply connected and adjoint semisimple groups: Let G be a linear algebraic group defined over a field K. There exists a Lie algebra over K associated to G, denoted by $Lie(G)$, and an adjoint representation $ad : G \to Lie(G)$ (see [10, Chapter 3]). Now assume that G is semisimple and split over K, with maximal split torus T. One can then define a root system, a weight lattice Λ, and a root lattice Λ_r. The group Λ/Λ_r is finite (see [13, Sections 24 and 25]). The character group of T, defined as the group of morphisms $T \to G_m$ (denoted by $X(T)$) can be inserted between Λ and Λ_r. Group G is called adjoint if $X(T) = \Lambda_r$ and it is called simply connected if $X(T) = \Lambda$. A semisimple group G is called adjoint (resp. simply connected) if it is adjoint (resp. simply connected) after base change to K^{sep}.

Theorem 2.1.7. For any semisimple linear algebraic group G there exist (up to isomorphism) a unique simply connected group $\widetilde{G}$ and a unique adjoint group $\bar{G}$ with central isogenies $\widetilde{G} \to G \to \bar{G}$.

Proof. See [13, Theorem 26.7]. □

Absolutely simple, simply connected (or adjoint), linear algebraic groups G have a classification into types A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, and G_2. In this dissertation we mainly work with groups of type D_n. Type D_n groups will further be explained in Section 2.4.

Weil restriction: For any finite separable field extension L/K and any algebraic group G defined over L, one can associate the algebraic group $R_{L/K}(G)$ defined over K, which is called the Weil restriction (or corestriction) of G from L to K. See [13, Section 20] for more details and the basic properties of the Weil restriction.

Norm one torus: Let L/K be a finite separable field extension. Then ${R_{L/K}}^{(1)}(\mathbb{G}_m) = \{x \in R_{L/K}(\mathbb{G}_m) \mid N_{L/K}(x) = 1\}$ is a torus over K, which is called the norm one torus.

Quasi-trivial torus: A torus T defined over K is called quasi-trivial if it is the product of a Weil restriction of split tori.

2.2 Central simple algebras and involutions

Let K be a field. A central simple algebra over K is a finite dimensional K−algebra $A \neq \{0\}$ with center K which has no two sided ideals except $\{0\}$ and A. A central simple algebra A is called a central division algebra if every nonzero element in A is invertible. If F/K is a field extension, then we write A_F for the $F-$ algebra obtained from A by extending scalars to F, which is a central F−algebra:

$$A_F := A \underset{K}{\otimes} F.$$

Theorem 2.2.1. (Wedderburn): For an algebra A over K, the following statements are equivalent:

(1) A is central simple.

(2) There is a field extension F/K such that $A_F \cong M_n(F)$ for some n.

(3) If Ω is an algebraically closed field containing K, then $A_\Omega \cong M_n(\Omega)$ for some n.

(4) There exists a central division algebra D over K such that $A \cong M_r(D)$ for some r.

If any (and hence all) of the conditions above holds for A, then the central division algebra D mentioned in (4) is unique up to isomorphism of K- algebras.

Proof. See [20, Chapter 8]. □

Splitting field: A field F for which condition (2) of Theorem 2.2.1 holds is called a splitting field of A. A central simple algebra A defined over K is called split if K is a splitting field for A.

Dimension and index: Let F/K be a field extension and A be a central simple algebra over K. Then the dimension of A over K is equal to the dimension of A_F over F (as vector spaces). Therefore, Wedderburn's theorem implies that the dimension of A is a square, in fact n^2, where n is the positive integer in conditions (2) and (3) of Theorem 2.2.1. The integer n is called the degree of A. The integer r in condition (4) is called the index of A, which is unique (thanks to the uniqueness of D up to isomorphism).

Reduced norm map: For any central simple algebra A over K, the reduced norm map of A is defined as follows: take an element $a \in A$, and consider a splitting field F of A. Then the reduced norm of a is defined as the determinant of the matrix in $M_n(F)$ which corresponds to a under the isomorphism $A_F \cong M_n(F)$. This value, which we denote by $Nrd(a)$, always lies in K and furthermore it does not depend on the choice of the splitting field F and the choice of the isomorphism $A_F \cong M_n(F)$ (see [20, Chapter 8]). Hence Nrd is a well defined map from A to K. Obviously, the restriction of Nrd to invertible elements of A is a group homomorphism $A^* \to \mathbb{G}_m$.

Involution: An involution on a central simple algebra A defined over a field K is a map $\sigma : A \to A$ such that:

(1) $\sigma(x+y) = \sigma(x) + \sigma(y)$ for $x, y \in A$,

(2) $\sigma(xy) = \sigma(y)\sigma(x)$ for $x, y \in A$,

(3) $\sigma(\sigma(x)) = x$ for $x \in A$.

The center K is preserved under σ. The restriction of σ to K is a field automorphism which is either an identity, or has degree 2. If this restriction is an identity, then we say that σ is an involution of the first kind. Otherwise, i.e., if the restriction is an automorphism of degree 2, then we say that σ is an involution of the second kind. An element $x \in A$ is called symmetric (with respect to the involution σ) is $\sigma(x) = x$, and it is called skew-symmetric if $\sigma(x) = -x$.

Example (Matrix Algebras): Let K be a field, n a natural number, and A the matrix algebra $A = M_n(K)$. Then A is a (split) central simple algebra of degree n and dimension n^2. Let $t : M_n(K) \to M_n(K)$ be the transpose map which sends any matrix $M \in M_n(K)$ to its transpose M^t. Then t is an involution of the first kind on A.

Example (Quaternion Algebras): A quaternion algebra over a field K (where $char\ K \neq 2$) is a central simple algebra of degree 2 over K. Every quaternion algebra Q has a $K-$basis $(1, i, j, k)$ such that

$$i^2 = a \in K^*, \quad j^2 = b \in K^*, \quad ij = -ji = k$$

(see [20, Chapter 8]).

The quaternion algebra Q is then denoted by $(\frac{a,b}{K})$. It is split if $Q \cong M_2(K)$, otherwise it is a central division algebra. In the second case we say that Q is a quaternion division algebra.

The unique $K-$ linear map $\tau : Q \to Q$ which sends 1, i, j, and k to 1, $-i$, $-j$, and $-k$ respectively, is an involution of the first kind on Q. This map does not depend on the choice of i, j, and k, and it is called the canonical involution on Q. Indeed, the map τ is the unique K- linear map $Q \to Q$ which is an identity on the center K and it maps any $x \in < i, j, k >$ to $-x$. The map

$$Q \to K$$

$$x \mapsto x\tau(x)$$

is a quadratic form of dimension 4 over K, which is called the norm form associated to Q.

Symmetric and skew-symmetric bilinear forms: Let V be a finite dimensional vector space over a field K with $char\ K \neq 2$, and $b : V \times V \to K$ be a bilinear form. We say that b is symmetric if $b(v, w) = b(w, v)$ for all $v, w \in V$, and skew-symmetric if $b(v, w) = -b(w, v)$ for all $v, w \in V$.

Regular bilinear forms and their adjoint involutions: The bilinear form $b : V \times V \to K$ is called regular, or nonsingular, if for any nonzero $v \in V$ we have $\{w \in V \mid b(v, w) = 0\} = \{0\}$.

Let $b : V \times V \to K$ be a regular bilinear form and $f \in End_K(V)$. There is a canonical $K-$ endomorphism of V, denoted by $\sigma_b(f)$, such that for all $v, w \in V$ we have ([13, Page 1])

$$b(v, f(w)) = b(\sigma_b(f)(v), w).$$

The map $\sigma_b : End_K(V) \to End_K(V)$ is an anti-automorphism of the central simple $K-$ algebra $End_K(V)$. This map is $K-$ linear, and it is called the adjoint anti-automorphism associated to the bilinear form b.

Theorem 2.2.2. Let K, V be as above. Then there is a one-to-one correspondence between equivalence classes of regular bilinear forms b on V modulo scalars in K^* and anti-automorphisms of $End_K(V)$ which are $K-$linear. Under this correspondence, $K-$ linear involutions on $End_K(V)$ correspond to regular bilinear forms which are either symmetric or skew-symmetric.

Proof. See [13, Page 1]. □

Theorem 2.2.3. Let (A, σ) be a central simple algebra of degree n over K with involution of the first kind, and let L be a splitting field of A. Then there is a regular bilinear form b on $V = L^n$ which is either symmetric or skew-symmetric such that σ_L is the involution on $End_L(V) \cong A_L$ adjoint to b.

Proof. See [13, Page 14, Proposition 2.1]. □

Orthogonal and symplectic involutions: An involution σ of the first kind on a central simple $K-$algebra A is called orthogonal if it corresponds to a symmetric bilinear form over any splitting field of A (see Theorem 2.2.3). Otherwise, i.e., if it corresponds to a skew-symmetric form, it is called symplectic.

The transpose involution on matrix algebras is an orthogonal type involution. The canonical involution on quaternion algebras is an example of a symplectic involution.

2.3 Quadratic forms

This section is devoted to quadratic forms. All the fields in this section are assumed to be of characteristic different from 2.

Quadratic form: Let K be a field and V a finite dimensional vector space over K. We say that the map $q : V \to K$ is a quadratic form defined over K if the following two conditions hold:

(1) For every $\lambda \in K$ and every $v \in V$ we have $q(\lambda v) = \lambda^2 q(v)$.

(2) The map

$$b_q : V \times V \longrightarrow K$$
$$(v, w) \mapsto \frac{q(v+w) - q(v) - q(w)}{2}$$

is $K-$ bilinear (note that by our assumption *char* $K \neq 2$). The bilinear form b_q is clearly symmetric.

Note that for any field extension L/K, q induces a quadratic form over the vector space $V_L := V \otimes_K L$, which is denoted by q_L.

If *dim* $V = n$, then we say that the dimension of q is n (*dim* $q = n$). Note that we often omit V when we define q. There exists a basis $(v_1, \dots, v_n)$ for V and scalars $a_1, \dots, a_n \in K$ such that for every i we have $q(v_i) = a_i$, and for every $i \neq j$, $b_q(v_i, v_j) = 0$. Then we write $q =< a_1, \dots, a_n >$ and we call it a digonalization of q ([14, Chapter 1]).

Regular quadratic forms: If *dim* $q = n$ and all the elements $a_1, \dots, a_n$ in a diagonalization of a quadratic form $q =< a_1, \dots, a_n >$ are nonzero, then we say that q is regular (in this case all the elements in any other diagonalization will be nonzero also). Unless the contrary is expressly stated, we assume that all quadratic forms in this sequel are regular. In this case the bilinear form b_q described above will be a regular bilinear form (the definition of regular bilinear forms can be found in section 2.2).

Isotropicity: If there exists a vector $v \in V$ such that $q(v) = a \in K$, then we say that q represents a. We denote by $D(q)$ the set of values in K^* represented by q, and by $[D(q)]$ the group generated by those values in K^*.

We say that q is $K-$ isotropic if q represents 0 non-trivially, and $K-$ anisotropic otherwise. If $q(v) = 0$ for a nonzero vector $v \in V$, then v is called a $K-$isotropic vector. Otherwise we say that v is $K-$anisotropic.

Sum and product: Let $q_1 =< a_1, \dots, a_m >$ and $q_2 =< b_1, \dots, b_n >$ be two quadratic forms over K. We define $q_1 \perp q_2$, the orthogonal sum of q_1 and q_2, as follows:

$$q_1 \perp q_2 :=< a_1, \dots, a_m, b_1, \dots, b_n >,$$

and $q_1 \otimes q_2$, the tensor product of q_1 and q_2 as:

$$q_1 \otimes q_2 :=< a_i b_j >_{1 \le i \le m,\ 1 \le j \le n} .$$

The product of a scalar $\lambda \in K$ and a quadratic form $q =< a_1, \dots, a_n >$ over K is defined as $\lambda q :=< \lambda a_1, \dots, \lambda a_n >$.

Note that the orthogonal sum, the tensor product, and the scalar product defined above are all independent of the choice of the diagonalization of the quadratic forms.

Determinant and discriminant: Let $q =< a_1, \dots, a_n >$ be a regular quadratic form over K. The element $det(q) = a_1 \dots a_n K^{*2} \in K^*/K^{*2}$ is called the determinant of q, and $disc(q) = (-1)^{\frac{n(n-1)}{2}} det(q) \in K^*/K^{*2}$ is called the discriminant of q. The determinant and discriminant of q are independent of the choice of the diagonalization of q. The $K-$ étale algebra $K(\sqrt{disc\ (q)}) = K[t]/(t^2 - disc(q))$ (with some ambiguity we take $disc\ (q)$ in this definition to be any representative in the square class of the discriminant) is called the discriminant extension of q, which is either a quadratic field extension of K (if $disc(q) \neq K^{*2}$), or the split $K-$ étale algebra $K \times K$ (if $disc(q) = K^{*2}$).

Isometries and orthogonal group: An isometry between two quadratic forms (V_1, q_1) and (V_2, q_2) defined over K, is a $K-$ isomorphism $f : V_1 \to V_2$ such that for every $v \in V_1$ we have $q_2(f(v)) = q_1(v)$. We denote the $K-$ isometry of q_1 and q_2 by $q_1 \cong q_2$. The set of all isometries between a quadratic form q and itself is an algebraic group, the product being the composition of linear maps. This group is called the orthogonal group of q, denoted by $O(q)$.

Hyperbolic forms: We say that a quadratic form q over K is hyperbolic, if there exists a quadratic form q' defined over K, and a $K-$ isometry $q \cong q' \perp < 1, -1 >$. A quadratic form q is called split (or totally hyperbolic) over K if there is a $K-$ isometry between q and an orthogonal sum of some number of quadratic forms $< 1, -1 >$.

Every (regular) quadratic form q over K has a decomposition $q = q' \perp q''$, where q' is $K-$ anisotropic and q'' is $K-$ split. This decomposition is unique up to $K-$ isometry.

The Witt ring: The set of isometry classes of all anisotropic quadratic forms over a field K with the following operations is a ring: for two classes $[q]$ and $[q']$, we define the sum $[q] + [q']$ to be the isometry class of the anisotropic part of the quadratic form $q \perp q'$. Also, we define the product $[q] \times [q']$ to be the isometry class of the anisotropic part of the quadratic form $q \otimes q'$. This ring is called the Witt ring of K, denoted by $W(K)$ (see [14, Chapter 2]).

Clifford algebra: Let q be an n dimensional quadratic form over K, and $V = K^n$. Recall the tensor algebra of V:

$$T(V) = K \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \cdots$$

The Clifford algebra of (V, q), denoted $C(V, q)$, is defined as the quotient of $T(V)$ by the ideal $I(q) = < v \otimes v - q(v) \mid v \in V >$. By abusing notation, we denote the image of an element $w \in T(V)$ in $C(V, q)$ by w again.

Since all the generators of $I(q)$ lie in the sum of homogeneous components of $T(V)$ of even degree, the $\mathbb{Z}$- grading of $T(V)$ induces a $\mathbb{Z}/2\mathbb{Z}$- grading of $C(V, q) = C_0(V, q) \oplus C_1(V, q)$. The subalgebra $C_0(V, q)$ is called the even Clifford algebra of (V, q). Note that $C_1(V, q)$ is not a subalgebra of $C(V, q)$ because it is not closed under multiplication, but it is a vector subspace of $C(V, q)$. If $dim\ q = n$, then $dim\ C(V, q) = 2^n$ and $dim\ C_0(V, q) = dim\ C_1(V, q) = 2^{n-1}$. The vector space V embeds into $C_1(V, q)$.

Now we state a fact about the Clifford algebra of even dimensional quadratic forms.

Theorem 2.3.1. Let q be an even dimensional quadratic form over K. Then:

(1) $C(V, q)$ is a central simple algebra over K.

(2) If $disc(q) \neq K^{*2}$ then the center of the even Clifford algebra $C_0(V, q)$ is the discriminant extension of q, i.e., $K(\sqrt{disc\ (q)})$. Furthermore, $C_0(V, q)$ is a central simple algebra over $K(\sqrt{disc\ (q)})$.

(3) If $disc(q) = K^{*2}$ then the center of the even Clifford algebra $C_0(V, q)$ is $K \times K$. If $C(V, q) = M_t(D)$ where D is a central $K-$ division algebra, then t is a power of 2 and $C_0(V, q) \cong M_{\frac{t}{2}}(D) \times M_{\frac{t}{2}}(D)$.

Proof. See [14, Chapter 5, Theorem 2.5]. □

The canonical involution on Clifford algebra: There is a canonical involution t on $T(V)$ defined on elementary tensors by $(v_1 \otimes \cdots \otimes v_n)^t = (v_n \otimes \cdots \otimes v_1)$. Since t stabilizes $I(q)$, it induces an involution on $C(V, q)$ and an involution on $C_0(V, q)$, which we denote by t by abusing notation. Let $\gamma : C(V, q) \to C(V, q)$ be the map that sends $u = u_0 + u_1$ ($u_0 \in C_0(V, q)$, $u_1 \in C_1(V, q)$) to $\gamma(u) = u_0 - u_1$.

Lemma 2.3.2. Let (V, q) be a quadratic form over a field K, and $f : V \to V$ be an isometry of q. Then there exists an invertible element $s_f \in C(V, q)$ such that $f(x) = \gamma(s_f) x {s_f}^{-1}$ for all $x \in V$.

Proof. See [2, Chapter 4, Lemma 10.10]. □

Clifford group: The Clifford group of q is an algebraic group defined as

$$\Gamma(q) = \{s \in C(V, q)^* | \gamma(s) V s^{-1} = V\}.$$

The map α_K: For any $s \in \Gamma(q)(K)$, there is an $K-$ linear map

$$\alpha_s : V \longrightarrow V$$

$$x \mapsto \gamma(s)xs^{-1}$$

And we get a group homomorphism

$$\alpha_K : \Gamma(q)(K) \longrightarrow GL(V)$$

$$s \mapsto \alpha_s.$$

The image of α_K lies in $O(q)(K)$ (see [2, Chapter 4, Lemma 4.10.15]). By abusing notation, we call α_K the map $\Gamma(q)(K) \to O(q)(K)$.

Theorem 2.3.3. For any field extension L/K we have an exact sequence

$$1 \longrightarrow L^* \longrightarrow \Gamma(q)(L) \xrightarrow{\alpha_L} O(q)(L) \longrightarrow 1.$$

Proof. See [2, Chapter 4, Theorem 4.10.16]. □

Hyperplane reflections: Let (V, q) be a quadratic form over K. To every anisotropic vector $v \in V$ one can associate the following map

$$\tau_v : V \longrightarrow V$$

$$x \mapsto x - \frac{2b_q(x,v)}{q(v)}v$$

which is called the hyperplane reflection associated to v. The map τ_v belongs to $O(q)$.

Let L/K be a field extension. For an $L-$ anisotropic vector $v \in V_L$, the pre-image of the hyperplane reflection $\tau_v \in O(q)(L)$ under the map $\alpha_L : \Gamma(q)(L) \to O(q)(L)$ is the set $\{\lambda v | \lambda \in L^*\}$ (see [2, Chapter 4, Theorem 4.10.16]).

Theorem 2.3.4. (Cartan-Dieudonne) Every isometry in $O(q)$ is product of some hyperplane reflections.

Proof. See [14, Chapter 1, Theorem 7.1]. □

The spinor norm map: Let (V, q) be a quadratic form over K, and $f \in O(q)(K)$ be the product of hyperplane reflections $\tau_{v_1} \dots \tau_{v_m}$ for some ansiotropic vectors $v_1, \dots, v_m \in V$. So the pre-image of f under the map $\alpha_K : \Gamma(q)(K) \to O(q)(K)$ is the set $\{\lambda v_1 \dots v_m | \lambda \in K^*\}$.

If $s \in C(V, q)$, we set $N_K(s) = s^t s$. The map $N_K : C(V, q)(K) \to C(V, q)(K)$ is called the norm of $C(V, q)(K)$. If $x \in V$, we have $N_K(x) = q(x)$.

Lemma 2.3.5. If $s \in \Gamma(q)(K)$, then $N_K(s) \in K^*$ and $N_K(\gamma(s)) = N_K(s)$.

Proof. See [2, Chapter 4, Lemma 4.10.14]. □

Therefore we get a group homomorphism $N_K : \Gamma(q)(K) \to K^*$, which sends s to $s^t s$.

For any element $\lambda \in K^*$, we have $N_K(\lambda) = \lambda^2$. Therefore Theorem 2.3.3 implies that the norm induces a group homomorphism $Sn_K : O(q)(K) \to K^*/K^{*2}$ satisfying $Sn_K(\tau_v) = q(v)K^{*2} \in K^*/K^{*2}$ for all $v \in V$ such that $q(v) \neq 0$. The map Sn_K is called the spinor norm map.

$Pin(q)$: for a quadratic form q over K,we denote by $Pin(q)$ the algebraic group defined by

$$Pin(q)(K) = \{x \in \Gamma(q)(K) \mid N_K(x) = 1\}.$$

Let K^{sep} be the separable closure of K. We have an exact sequence of groups

$$1 \longrightarrow \mu_2(K^{sep}) \longrightarrow Pin(q)(K^{sep}) \overset{\alpha_{K^{sep}}}{\longrightarrow} O(q)(K^{sep}) \longrightarrow 1,$$

(see [2, Chapter 4, Corollary 4.10.19]).

The special orthogonal group: Determinant of any isometry $f \in O(q)(K)$ belongs to $\mu_2(K)$. Let $det : O(q)(K) \longrightarrow \mu_2(K)$ be the determinant map. The kernel of this map is denoted by $O^+(q)(K)$ (the special orthogonal group of q). Its elements are called proper isometries.

The special Clifford group and the spinor group: The inverse image of $O^+(q)(K)$ in $\Gamma(V,q)(K)$ by the map α_K is called the special Clifford group of q, and is denoted by $\Gamma^+(q)(K)$. The spinor group of q is the group $Spin(q)(K) = Pin(q)(K) \cap \Gamma^+(q)(K)$.

We have an exact sequence of algebraic groups

$$1 \longrightarrow \mu_2(K^{sep}) \longrightarrow Spin(q)(K^{sep}) \overset{\alpha_{K^{sep}}}{\longrightarrow} O^+(q)(K^{sep}) \longrightarrow 1.$$

(see [2, Chapter 4, Lemma 5.10.21].)

Similitudes and multipliers: Let (V,q) be a regular quadratic form over K. A similitude of (V,q) over K is a $K-$linear map $g : V \longrightarrow V$ for which there exists a constant $\alpha \in K^*$, such that $q(g(v)) = \alpha q(v)$ for all $v \in V$. The element α is called the multiplier of g, and is denoted $\mu(g)$. The similitudes of q form a linear algebraic group $GO(q)$, which is called the group of similitudes of q. We denote by μ the multiplier map $\mu : GO(q) \longrightarrow \mathbb{G}_m$, which maps any similitude to its multiplier. The map μ is an algebraic group homomorphism whose kernel is $O(q)$.

Proper similitudes: Let $dim(q)$ be even and $g \in GO(q)$. By [13, Page 154], we have $det(g) = \pm\mu(g)^{\frac{n}{2}}$. The group of proper similitudes is defined as the following subgroup of $GO(q)$:

$$GO^+(q) := \{g \in GO(q) \mid det(g) = \mu(g)^{\frac{n}{2}}\}.$$

When g is a similitude of q (resp. proper similitude), then clearly every scalar multiple of g is also a similitude (resp. proper similitude). Hence $\mathbb{G}_m$ can be viewed as a subgroup of $GO(q)$ (resp. $GO^+(q)$). One defines $PGO(q) = GO(q)/\mathbb{G}_m$, and $PGO^+(q)(K) = GO^+(q)/\mathbb{G}_m$.

2.4 Algebraic groups associated to central simple algebras with involutions, and hermitian forms

Let (A, σ) be a central simple K−algebra with orthogonal involution. In this section we will recall the definitions of algebraic groups associated to (A, σ). When $A = M_n(K)$ and σ is the involution adjoint to a quadratic form q of dimension n over K, then the groups associated to q will coincide with the groups associated to (A, σ) which will be introduced in this section.

Similitudes, multipliers, and the orthogonal group: A similitude of (A, σ) is an element $g \in A$ such that $\sigma(g)g \in K^*$. The element $\sigma(g)g$ is called the multiplier of g. The similitudes of (A, σ) form an algebraic group which is denoted by $GO(A, \sigma)$. The map $\mu : GO(A, \sigma) \to \mathbb{G}_m$ which sends any similitude g to its multiplier $\sigma(g)g$ is called the multiplier map. The kernel of μ is called the orthogonal group of (A, σ), denoted by $O(A, \sigma)$, whose elements are called isometries of (A, σ).

Any scalar multiple of a similitude is also a similitude, so $\mathbb{G}_m$ can be viewed as a subgroup of $GO(A, \sigma)$. The quotient $GO(A, \sigma)/\mathbb{G}_m$ is denoted by $PGO(A, \sigma)$.

Proper similitudes and isometries: Let $n = deg\ A$ be even and $g \in GO(A, \sigma)$. Then $Nrd(g) = \pm\mu(g)^{\frac{n}{2}}$ (see [13, Page 163]). The similitude g is called proper if $Nrd(g) = \mu(g)^{\frac{n}{2}}$. We write $GO^+(A, \sigma)$ for the subgroup of $GO(A, \sigma)$ consisting of all proper similitudes.

$O^+(A, \sigma)$**,** $PGO^+(A, \sigma)$**,** $Spin(A, \sigma)$: the group $PGO^+(A, \sigma)$ is defined to be the quotient $GO^+(A, \sigma)/\mathbb{G}_m$. Also the special orthogonal group of (A, σ) is defined to be the subgroup of $O(A, \sigma)$ consisting of all proper isometries, denoted by $O^+(A, \sigma)$. There is an algebraic group $Spin(A, \sigma)$ defined over K, which fits in the following exact sequence:

$$1 \to \mu_2(K^{sep}) \to Spin(A, \sigma)(K^{sep}) \to O^+(A, \sigma)(K^{sep}) \to 1.$$

For the explicit construction of $Spin(A, \sigma)$, see [13, Page 186, Definition 13.30]. The group $Spin(A, \sigma)$ is the simply connected cover of $O^+(A, \sigma)$.

Groups associated to the involutions adjoint to quadratic forms on the matrix algebra: Let $A = M_n(K)$ and σ be the involution defined over A adjoint to an n− dimensional quadratic form q over K. Then we have the following isomorphisms of algebraic groups:

$GO(A, \sigma) = GO(q)$

$GO^+(A, \sigma) = GO^+(q)$

$O(A, \sigma) = O(q)$

$O^+(A, \sigma) = O^+(q)$

$PGO(A, \sigma) = PGO(q)$

$PGO^{+}(A,\sigma) = PGO^{+}(q)$

$Spin(A,\sigma) = Spin(q)$.

Groups of type D_n: If K is a field with $char\ K \neq 2$, then any absolutely simple, simply connected, linear algebraic group G of type D_n over K is of the form $Spin(A,\sigma)$ for a central simple algebra of degree $2n \geq 4$ with orthogonal involution. Any absolutely simple, adjoint, linear algebraic group G of type D_n over K is of the form $PGO^{+}(A,\sigma)$ for a central simple algebra of degree $2n \geq 4$ with orthogonal involution. There are central isogenies $Spin(A,\sigma) \to O^{+}(A,\sigma) \to PGO^{+}(A,\sigma)$. So studying semisimple linear algebraic groups of type D_n is closely related to central simple algebras with orthogonal involution.

Hermitian and skew-hermitian forms: Let (A,σ) be a central simple algebra with involution of any kind on a field K. Let M be a finitely generated left A module (which is automatically free). A hermitian form on M (with respect to the involution σ on A) is a bi-additive map

$$h : M \times M \to A$$

such that

(1) $h(\alpha x, \beta y) = \alpha h(x,y)\sigma(\beta)$ for all $x, y \in M$ and $\alpha, \beta \in A$,

(2) $h(y,x) = \sigma(h(x,y))$ for all $x, y \in M$.

If (2) is replaced by $h(y,x) = -\sigma(h(x,y))$, then we say that h is a skew-hermitian form.

The following concepts for hermitian and skew-hermitian forms are similarly defined as for quadratic forms: extending the scalars, regularity, diagonalization, isotropicity, hyperbolicity, orthogonal sums, isometry, similitude, and multiplier (see [20] and [12]). Note that the elements in the diagonalization of a hermitian (resp. skew-hermitian) form are symmetric (resp. skew-symmetric) elements of (A,σ). The Witt group of a central simple algebra with involution (A,σ) is also defined similarly: $W^{1}(A,\sigma)$ and $W^{-1}(A,\sigma)$, the Witt group of hermitian forms and skew-hermitian forms, respectively. Note that there is no natural product on the Witt group of (skew-) hermitian forms (similar to the tensor product of quadratic forms), but the addition is defined (the orthogonal sum).

Determinant and discriminant: Let $h = \langle a_1, \ldots, a_n \rangle$ be a regular hermitian or skew-hermitian form over (A,σ) defined over K. The element $det(h) = Nrd(a_1 \ldots a_n)K^{*2} \in K^{*}/K^{*2}$ is called the determinant of h, and $disc(h) = (-1)^{\frac{n(n-1)}{2}} det(h) \in K^{*}/K^{*2}$ is called the discriminant of h. The determinant and discriminant of h are independent of the choice of the diagonalization of h. The $K-$ étale algebra $K(\sqrt{disc\ (h)}) = K[t]/(t^2 - disc(h))$ (with some ambiguity we take $disc\ (h)$ in this definition to be any representative in the square class of the discriminant) is called the discriminant extension of h, which is either a quadratic field extension of K (if $disc(h) \neq K^{*2}$), or the split $K-$ étale algebra $K \times K$ (if $disc(h) = K^{*2}$).

Adjoint involution: The following theorem is an analogue of Theorem 2.2.2 for (skew-) hermitian forms.

Theorem 2.4.1. Let (A,σ) be a central simple $K-$ algebra with involution of any kind, M a left $A-$ module, and h a regular hermitian or a skew-hermitian form on M. Then there exists a unique involution σ_h on $End_A(M)$ such that $\sigma_h(\alpha) = \sigma(\alpha)$ for all $\alpha \in K$ and

$$h(v, f(w)) = h(\sigma_h(f)(v), w)$$

for all $v, w \in M$ and all $f \in End_A(M)$. The involution σ_h is called the adjoint involution with respect to h.

Proof. See [13, Page 42, Proposition 4.1]. □

Theorem 2.4.2. Let K, A, σ, and M be as before. Further, assume that σ is of the first kind. Then the map $h \mapsto \sigma_h$ is a one-to-one correspondence between regular hermitian and skew-hermitian forms on M (with respect to σ) up to a factor in K^* and involutions of the first kind on $End_A(M)$. The involutions σ_h on $End_A(M)$ and σ on A have the same type if h is hermitian, and have opposite types if h is skew-hermitian.

Proof. See [13, Page 43, Theorem 4.2]. □

Groups associated to (skew-) hermitian forms: Let K, A, σ, M, and h be as in Theorem 2.4.2. Furthermore, assume that h is skew-hermitian, and σ is of symplectic type. Then we set

$GO(h) := GO(End_A(M), \sigma_h)$

$GO^+(h) := GO^+(End_A(M), \sigma_h)$

$O(h) := O(End_A(M), \sigma_h)$

$O^+(h) := O^+(End_A(M), \sigma_h)$

$PGO(h) := PGO(End_A(M), \sigma_h)$

$PGO^+(h) := PGO^+(End_A(M), \sigma_h)$

$Spin(h) := Spin(End_A(M), \sigma_h)$

Morita equivalence: Let K be a field with $char\ K \neq 2$, $m, n \in \mathbb{N}$, and σ be an orthogonal involution on $A = M_n(K)$. Consider the split n-dimensional quadratic form on K^n, i.e., $< 1, \ldots, 1 >$, and denote its associated bilinear form by $g : K^n \times K^n \to K$. Let V be a right $A-$module of dimension m and $h : V \times V \to A$ be an $m-$dimensional skew-hermitian form over (A, σ). Let B_h be the following function:

$B_h : (V \otimes_A K^n) \times (V \otimes_A K^n) \to K$

$$(x \otimes a, y \otimes b) \mapsto g(a, h(x,y)b) \ for\ x, y \in V,\ a, b \in K^n.$$

One checks that B_h is a symmetric bilinear form on $V \otimes_A K^n$. By the identification $V \otimes_A K^n \cong K^{mn}$, we get an mn–dimensional quadratic form q_h over K, associated to h. The association $h \mapsto q_h$ is a one-to-one correspondence between m–dimensional skew-hermitian forms over (A, σ) and mn–dimensional quadratic forms over K. This is a special case of Morita equivalence (see [12, Chapter 1, Theorem 9.3.5]). This equivalence respects direct sums, isotropicity, and hyperbolicity.

2.5 Galois cohomology

Galois cohomology is one of the essential tools to study linear algebraic groups, quadratic and (skew-) hermitian forms. In this section we will recall some basic notions of Galois cohomology which will be used throughout the dissertation.

Γ**–set:** Let E be a discrete topological space and Γ be a profinite group. Let Γ act on E continuously:

$$\Gamma \times E \to E$$
$$(\tau, x) \mapsto x^\tau.$$

Such topological space is called a Γ–set. A morphism between two Γ–sets is a continuous map that preserves the group action of Γ.

Γ**–group:** A Γ–group A is a Γ–set with a group structure compatible with the action of Γ, i.e., for every $x, y \in A$ and every $\tau \in \Gamma$ we have $(xy)^\tau = x^\tau y^\tau$. Morphisms are defined accordingly. If A is abelian, then the notion of Γ–group coincides with the notion of Γ–module in abelian group cohomology.

$H^0(\Gamma, A)$**:** For a Γ–group A, we define the zeroth cohomology group of Γ in A as $H^0(\Gamma, A) = A^\Gamma$, the group consisting of all elements of A invariant under the action of Γ. The cohomology group $H^0(\Gamma, A)$ is functorial in A.

$H^1(\Gamma, A)$**:** Let A be a Γ–group. A cocycle of Γ in A is a map

$$a : \Gamma \to A$$
$$\tau \mapsto a_\tau$$

subject to the following conditions:

(1) a is continuous, and

(2) for every $\tau, \tau' \in \Gamma$ we have $a_{\tau\tau'} = a_\tau {a_{\tau'}}^\tau$.

Let us denote the set of all cocycles by $Z^1(\Gamma, A)$. One can then define the following equivalence relation between two cocycles a and a': we say that a and a' are cohomologous if there exists $b \in A$ such that for every $\tau \in \Gamma$ we have ${a'}_\tau = b^{-1} a_\tau b^\tau$. The quotient of $Z^1(\Gamma, A)$ by this relation is denoted by $H^1(\Gamma, A)$, and it is called the first cohomology set of Γ in A. The equivalence class of the trivial cocyle, i.e., the map that sends every element of Γ to the identity element of A, is called the distinguished element of $H^1(\Gamma, A)$. We use the term **pointed set** to refer to such sets. The cohomology set $H^1(\Gamma, A)$ is functorial in A. If A is an abelian group, then $H^1(\Gamma, A)$ carries a natural structure of an abelian group. The zeroth cohomology groups $H^0(\Gamma, A)$ and the first cohomology groups $H^1(\Gamma, A)$ (in case A is abelian) are also considered as pointed sets, the identity being the distinguished element.

Galois cohomology of algebraic groups: Let G be an algebraic group defined over a field K. Then the natural action of $Gal(K^{sep}/K)$ on the group $G(K^{sep})$ makes $G(K^{sep})$ a $Gal(K^{sep}/K)$–group. In this case we denote the zeroth and the first cohomologies by $H^0(K,G)$ and $H^1(K,G)$, respectively. The zeroth cohomology group $H^0(K,G)$ is simply just the $K-$ points of G, i.e., $G(K)$.

Principal homogeneous spaces: Let X be a variety and G be a linear algebraic group, both defined over K. Assume that there is an action of $G(K^{sep})$ on $X(K^{sep})$ satisfying the following conditions:

(1) the two actions of $Gal(K^{sep}/K)$ and $G(K^{sep})$ on $X(K^{sep})$ are compatible with each other, i.e., for every $\tau \in Gal(K^{sep}/K)$, $g \in G(K^{sep})$, and $x \in X(K^{sep})$, we have

$$(x^g)^\tau = (x^\tau)^{(g^\tau)}.$$

(2) the action of $G(K^{sep})$ on $X(K^{sep})$ is simply transitive.

Then we say that X is a principal homogeneous space (or torsor) over G.

Theorem 2.5.1. The elements in the first cohomology set $H^1(K,G)$ are in one to one correspondence with isomorphism classes of principal homogeneous spaces (torsors) over G.

Proof. See [21, Chapter 5, Proposition 33]. □

Under the bijection described above, the isomorphism class of a $G-$ torsor X corresponds to the distinguished element of $H^1(K,G)$, if and only if X has a K–point. In particular, the isomorphism class of G itself (as a torsor over G) corresponds to the distinguished element of $H^1(K,G)$.

Theorem 2.5.2. (Hilbert 90) Let K be a field and T be a split torus defined over K. Then $H^1(K,T)$ is trivial.

Proof. See [13, Theorem 29.2]. □

Theorem 2.5.3. Let $n \in \mathbb{N}$ and K be a field such that *char* K is either 0 or coprime to n. Then $H^1(K, \mu_n) = K^*/K^{*n}$.

Proof. See [13, Section 30]. □

Theorem 2.5.4. Let K be a field with *char* $K \neq 2$, and q be a regular quadratic form of dimension n over K. Then the elements in the set $H^1(K, O^+(q))$ are in a one-to-one correspondence with the isomorphism classes of regular quadratic forms q' of dimension n over K with $det(q) = det(q')$.

Proof. See [2, Corollary 4.11.3]. □

Cohomology exact sequences: The kernel of a map $M \to N$ of pointed sets is defined to be the pre-image of the distinguished element of N. Hence one can define the cohomology exact sequences.

Let A be a linear algebraic group defined over a field K, B a closed subgroup of A and $C := A(K^{sep})/B(K^{sep})$ be the $Gal(K^{sep}/K)$–set of left cosets of $B(K^{sep})$ in $A(K^{sep})$. The following exact sequence of pointed sets

$$1 \to B(K^{sep}) \to A(K^{sep}) \to C \to 1$$

gives rise to the following exact sequence of cohomology maps:

$$1 \to H^0(K, B) \to H^0(K, A) \to H^0(K, C) \to H^1(K, B) \to H^1(K, A).$$

See [13, Section 28.B] for the definition of the connecting map $H^0(K, C) \to H^1(K, B)$ and the proof of exactness (the other maps in the sequence above are defined by functoriality). If we assume that B is normal in A, then C will also be an algebraic group over K, hence $H^1(K, C)$ is well defined. In this case we have the exact sequence:

$$1 \to H^0(K, B) \to H^0(K, A) \to H^0(K, C) \to H^1(K, B) \to H^1(K, A) \to H^1(K, C).$$

See [13, Proposition 28.3] for the proof of exactness. This will be in particular of our interest when B is central in A.

Chapter 3

Two classical norm principles from the algebraic theory of quadratic forms

Let K be a field, $charK \neq 2$, and L/K be a finite separable field extension.

Let q be a regular quadratic form over K. One can extend q and construct a quadratic form over L, which will be denoted by q_L. Similarly, this can be done for (skew-) hermitian forms. A natural question to study is the behavior of the groups attached to quadratic, hermitian, and skew-hermitian forms with respect to the norm map of the field extensions.

We will state two related classical theorems.

3.1 Scharlau's norm principle

The first theorem concerns $G(q)$, the group of similarity factors of q. See [14, Chapter 7, Section 4, Page 204] for a definition of similarity factor.

Theorem 3.1.1. (**Scharlau's Norm Principle**) Let q be a regular quadratic form over K. Then, for any $x \in K^*$,

$$x \in G(q)(L) \Rightarrow N_{L/K}(x) \in G(q)(K).$$

Proof. See [14, Chapter 7, Section 4, Page 205]. □

Scharlau's norm principle has another formulation in terms of maps between algebraic groups. First we need a definition.

Definition 3.1.2. Let (V, q) be a regular quadratic space over K. A similitude of (V, q) over K is a K–linear map $g : V \longrightarrow V$ for which there exists a constant $\alpha \in K^*$, such that $q(g(v)) = \alpha q(v)$ for all $v \in V$. The element α is called the multiplier of g, and is denoted $\mu(g)$. The similitudes of q form an algebraic group over K, which will be denoted by $GO(q)$ ($or\ Sim(q)$). We denote by $\mu : GO(q) \longrightarrow \mathbb{G}_m$ the multiplier map, which maps any similitude to its multiplier. This map is a morphism of algebraic groups.

Let $\mu_* : GO(q)(*) \longrightarrow \mathbb{G}_m(*)$ be the multiplier map defined above over the field $*$. Consider the following diagram:

$$\begin{array}{ccc} GO(q)(L) & \xrightarrow{\mu_L} & \mathbb{G}_m(L) \\ & & \Big\downarrow N_{L/K} \\ GO(q)(K) & \xrightarrow{\mu_K} & \mathbb{G}_m(K). \end{array}$$

Then Scharlau's norm principle is equivalent to the following statement:

$$\mathrm{Im}(N_{L/K} \circ \mu_L) \subseteq \mathrm{Im}(\mu_K).$$

3.2 Knebusch's norm principle

For any field extension F of K, let $D(q)(F)$ be the set of values of F^* represented by q, and $[D(q)(F)]$ be the group generated by those values in F^*. It will be of interest to understand the behavior of this group under finite extensions with respect to the norm map.

Theorem 3.2.1. (**Knebusch's Norm Principle**) Let q be a regular quadratic form over K. Then, for any $x \in [D(q)(L)]$, we have $N_{L/K}(x) \in [D(q)(K)]$.

Proof. See [14, Chapter 7, Section 5, Page 206]. □

If degree of the extension $[L:K]$ is n, then for each $x \in [D(q)(L)]$, the element $N_{L/K}(x) \in K^*$ is expressible as a product n elements in $D(q)(K)$ (see the proof of Knebusch's norm principle in [14, Chapter 7, Section 5, Page 206]).

Knesbusch's norm principle for even dimensional quadratic forms has an equivalent formulation in terms of maps between algebraic groups: let (V, q) be a regular quadratic space of even dimension over K. Consider the special Clifford group $\Gamma^+(q)$, which is a subgroup of $C_0(V, q)^*$, the units of the even part of the Clifford algebra (see [13, Page 177]). Each element of $\Gamma^+(q)(K)$ can be mapped to an element of K^* via Sn_K, the spinor norm map (see [4, Page 37]). This map is defined as follows: any element in $\Gamma^+(q)(K)$ is equivalence class of an element $\lambda v_1 \ldots v_r$ in $C_0(V, q)^*$, where $\lambda \in K^*$ and vectors $v_1, \ldots, v_r$ are $K-$anisotropic. Then $Sn_K([\lambda v_1 \ldots v_r]) = \lambda^2 q(v_1) \ldots q(v_r)$. Clearly, the image of the map Sn_K consist of products of even number of values in K^* represented by q, up to squares.

Theorem 3.2.1 can be reformulated in the following way: let $Sn_* : \Gamma^+(q)(*) \longrightarrow \mathbb{G}_m(*)$ be the spinor norm map defined above over the field $*$ (which is an extension of K). Consider the following diagram:

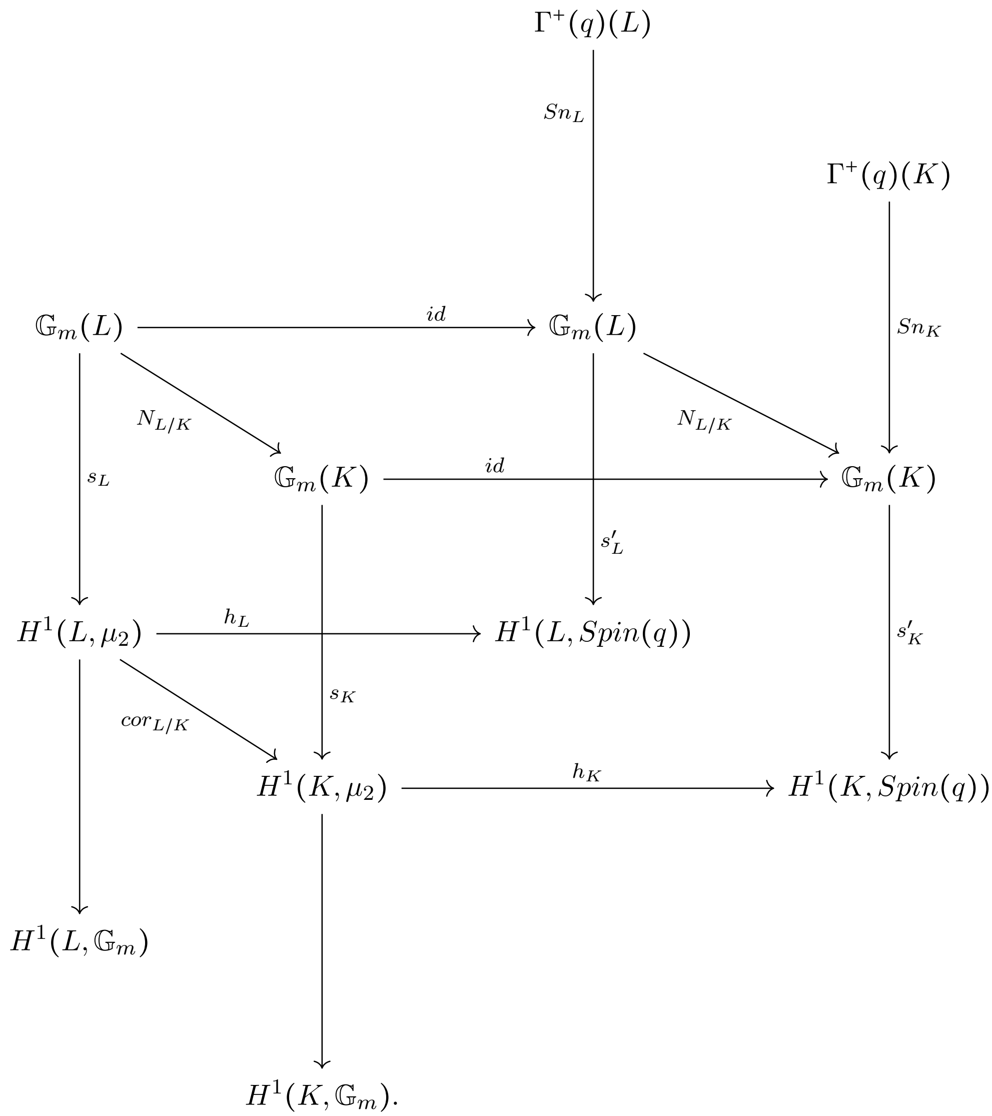
$$\begin{array}{ccc} \Gamma^+(q)(L) & \xrightarrow{Sn_L} & \mathbb{G}_m(L) \\ & & \big\downarrow{\scriptstyle N_{L/K}} \\ \Gamma^+(q)(K) & \xrightarrow{Sn_K} & \mathbb{G}_m(K). \end{array}$$

Then, Theorem 3.2.1 is equivalent to $\mathrm{Im}(N_{L/K} \circ Sn_L) \subseteq \mathrm{Im}(Sn_K)$.

Now we show that Theorem 3.2.1 is equivalent to Theorem 1.1.3 in Section 1.1. Consider the following commutative diagram:

$$\begin{array}{ccccccccc} & & 1 & & 1 & & & & \\ & & \downarrow & & \downarrow & & & & \\ 1 & \longrightarrow & \mu_2 & \longrightarrow & Spin(q) & \longrightarrow & O^+(q) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \big\downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Gamma^+(q) & \xrightarrow{\alpha} & O^+(q) & \longrightarrow & 1 \\ & & \big\downarrow{\scriptstyle \times 2} & & \big\downarrow{\scriptstyle Sn} & & & & \\ & & \mathbb{G}_m & \xrightarrow{id} & \mathbb{G}_m & & & & \\ & & \downarrow & & \downarrow & & & & \\ & & 1 & & 1. & & & & \end{array}$$

Recall that the map α in the above diagram is the restriction of the map $\alpha : \Gamma(q) \to O(q)$ (described in Theorem 2.3.3) to $\Gamma^+(q)$. Abusing notation, we denote the restriction by α as well. The above diagram gives rise to the following commutative diagram where s and s' are the connecting maps of the first and second columns, respectively, and the map h is induced by the map $\mu_2 \hookrightarrow Spin(q)$:



Recall that by Hilbert theorem 90, $H^1(K, \mathbb{G}_m) = 1$ and $H^1(L, \mathbb{G}_m) = 1$.

Lemma 3.2.2. Let $n = deg[L : K]$ be even. Then the following statements are equivalent:

1. $\operatorname{Im}(N_{L/K} \circ Sn_L) \subseteq \operatorname{Im}(Sn_K)$ (This is equivalent to the statement of Theorem 3.2.1).

2. $cor_{L/K}(\ker\ h_L) \subseteq \ker\ h_K$ (This is the statement of Theorem 1.1.3).

Proof. $1 \implies 2$:

Let $u \in Ker(h_L)$ and $v = cor_{L/K}(u)$. Since $H^1(L, \mathbb{G}_m) = 1$, $u \in \operatorname{Im}(s_L)$. Let l be an element in $\mathbb{G}_m(L)$ such that $s_L(l) = u$. Let $w = N_{L/K}(l)$. By the commutativity of the above diagram, $l \in \operatorname{Ker}(s'_L) = \operatorname{Im}(Sn_L)$. By assumption, we have $w \in \operatorname{Im}(Sn_K) = \operatorname{Ker}(s'_K)$, therefore $h_K(v) = s'_K(w) = 0$ and $v \in \operatorname{Ker}(h_K)$.

$2 \implies 1$:

Let $s \in \Gamma^+(q)(L)$, $l = Sn_L(s)$, $w = N_{L/K}(l)$. We would like to show $w \in \operatorname{Im}(Sn_K)$. Let $u = s_L(l)$, $v = cor_{L/K}(u)$. So we have $s'_L(l) = 0$ hence $u \in \operatorname{Ker}(h_L)$. By assumption, $h_K(v) = 0$, therefore $w \in \operatorname{Ker}(s'_K) = \operatorname{Im}(Sn_K)$. □

Chapter 4

Norm principle for algebraic groups

In the previous chapter, we recalled the behavior of the image of some algebraic group homomorphisms with respect to the norm map of field extensions. In this chapter, we recall the definition of the norm principle for any algebraic group homomorphism from a reductive group to an algebraic torus in general, in Section 4.1 (due to Merkurjev). Then in Section 4.2 we recall the cohomological formulation of the norm principle (due to Gille), and will show that the two formulations are equivalent (Section 4.3). We will then have a reduction of the norm principle to simply connected groups in Section 4.4, and will finally focus on type D_n groups in Sections 4.5 and 4.6.

4.1 H^0- variant of the norm principle (due to Merkurjev)

Let L/K be a finite separable field extension. Suppose G is a reductive group, and T is an algebraic torus, both defined over K. Suppose $f : G \longrightarrow T$ is an algebraic group homomorphism defined over K. Consider the following diagram:

$$\begin{array}{ccc} G(L) & \xrightarrow{f_L} & T(L) \\ & & \Big\downarrow{\scriptstyle N_{L/K}} \\ G(K) & \xrightarrow{f_K} & T(K). \end{array}$$

We say that the **H^0- variant of the norm principle holds for $f : G \longrightarrow T$ over L/K** if $\mathrm{Im}(N_{L/K} \circ f_L) \subseteq \mathrm{Im}(f_K)$. Also, we say that the **H^0- variant of the norm principle holds for** $f : G \longrightarrow T$, if for every finite separable field extension L/K we have $\mathrm{Im}(N_{L/K} \circ f_L) \subseteq \mathrm{Im}(f_K)$.

One can easily check that the Scharlau and Knebusch norm principles are two examples of the H^0- variants of the norm principle defined above. In Scharlau's (resp. Knebusch's) norm principle, $G = GO(q)$ (resp. $G = \Gamma^+(q)$), and $T = \mathbb{G}_m$.

Lemma 4.1.1. Let G be a reductive group. Assume that the H^0- variant of the norm principle holds for the canonical map $G \twoheadrightarrow G^{ab}$, where G^{ab} is the quotient of G by its commutator subgroup, i.e., $G^{ab} = G/[G, G]$ (which is a torus). Then the H^0- variant of the norm principle holds for any map $G \longrightarrow T$ where T is any algebraic torus.

Proof. See [1, Lemma 2.1]. □

Remark 4.1.2. The group G^{ab} is intrinsic to G. Therefore, according to Lemma 4.1.1, one might state the H^0- variant of the norm principle for G rather than $f : G \longrightarrow T$, since $G \longrightarrow G^{ab}$ depends only on G. By the **H^0-variant of the norm principle for** G, we mean the **H^0-variant of the norm principle for the canonical map** $G \to G^{ab}$.

4.2 H^1- variant of the norm principle (due to Gille)

The norm principle has another equivalent formulation in terms of Galois cohomology sets: for any field K and any algebraic group G over K, we denote the first cohomology set of $Gal(K^{sep}/K)$ in G by $H^1(K,G)$. This set is a group if G is commutative, otherwise it is a pointed set, i.e., a set with a distinguished element.

For any field extension L/K and an algebraic group G defined over K, there is a natural map called **restriction** (see [21, Chapter 2, Section 4, Page 12]):

$$res : H^1(K,G) \longrightarrow H^1(L,G).$$

Furthermore, if L/K is a finite separable field extension and G is commutative, then we have another map called **corestriction**:

$$cor : H^1(L,G) \longrightarrow H^1(K,G).$$

The kernel of any of the above cohomology maps is defined to be the preimage of the distinguished element.

Let S be a semisimple group over K, L/K a finite separable field extension, and $Z \subseteq S$ a central subgroup. Consider the following diagram

$$\begin{array}{ccc} H^1(L,Z) & \xrightarrow{\alpha_L} & H^1(L,S) \\ \big\downarrow{\scriptstyle cor_{L/K}} & & \\ H^1(K,Z) & \xrightarrow{\alpha_K} & H^1(K,S) \end{array}$$

whose rows are induced by the inclusion $Z \hookrightarrow S$. We say that the **H^1- variant of the norm principle holds for the pair** (Z,S) **over** L/K if for every $u \in \mathrm{Ker}(\alpha_L)$, we have $cor_{L/K}(u) \in Ker(\alpha_K)$.

Also, we say that the **H^1- variant of the norm principle holds for the pair** (Z,S), if for every finite separable field extension L/K, and for every $u \in \mathrm{Ker}(\alpha_L)$, we have $cor_{L/K}(u) \in \mathrm{Ker}(\alpha_K)$.

It is known that over certain fields K, some semisimple groups G do not have any non-trivial torsors (i.e., $H^1(-,G)$ is trivial). Therefore over such fields the H^1- variant of the norm principle holds for the pair (Z,G) for any central subgroup Z automatically. For example, $H^1(K,G)$ is trivial for any reductive group G over a finite field K. Therefore, the H^1–variant of the norm principle holds for (Z,G) where G is a semisimple group with a central subgroup Z defined over a finite field K. Also, $H^1(K,G)$ is trivial for any semisimple simply connected group G over a local field K. Therefore, the H^1- variant of the norm principle holds for (Z,G) where G is a simply connected group with a central subgroup Z defined over a local field K.

4.3 Equivalence of the two variants

In this section, we show that the two versions of the norm principle, the H^0- version for reductive groups and the H^1- version for semisimple groups, are equivalent. Therefore we will work with the H^1- version for the rest of the dissertation, which allows us to use tools from the Galois cohomology of semisimple linear algebraic groups to study the norm principle for type D_n groups.

Theorem 4.3.1. The following statements are equivalent (over L/K):

1. H^0- Variant of the norm principle holds for all reductive groups G.

2. H^1- Variant of the norm principle holds for all pairs (J,H), where H is a semisimple group and J a central subgroup in H.

Note that one can remove "over L/K" from the statement of the theorem; i.e., if (1) is true for all finite separable field extensions L of K, then the same is true for (2) and vice versa.

Proof. $(1 \Rightarrow 2)$:

Let H be a semisimple group over K and $J \subseteq H$ be a central subgroup. We have the following diagram and we need to show if $u \in \operatorname{Ker}(\alpha_L)$, then $cor_{L/K}(u) \in \operatorname{Ker}(\alpha_K)$.

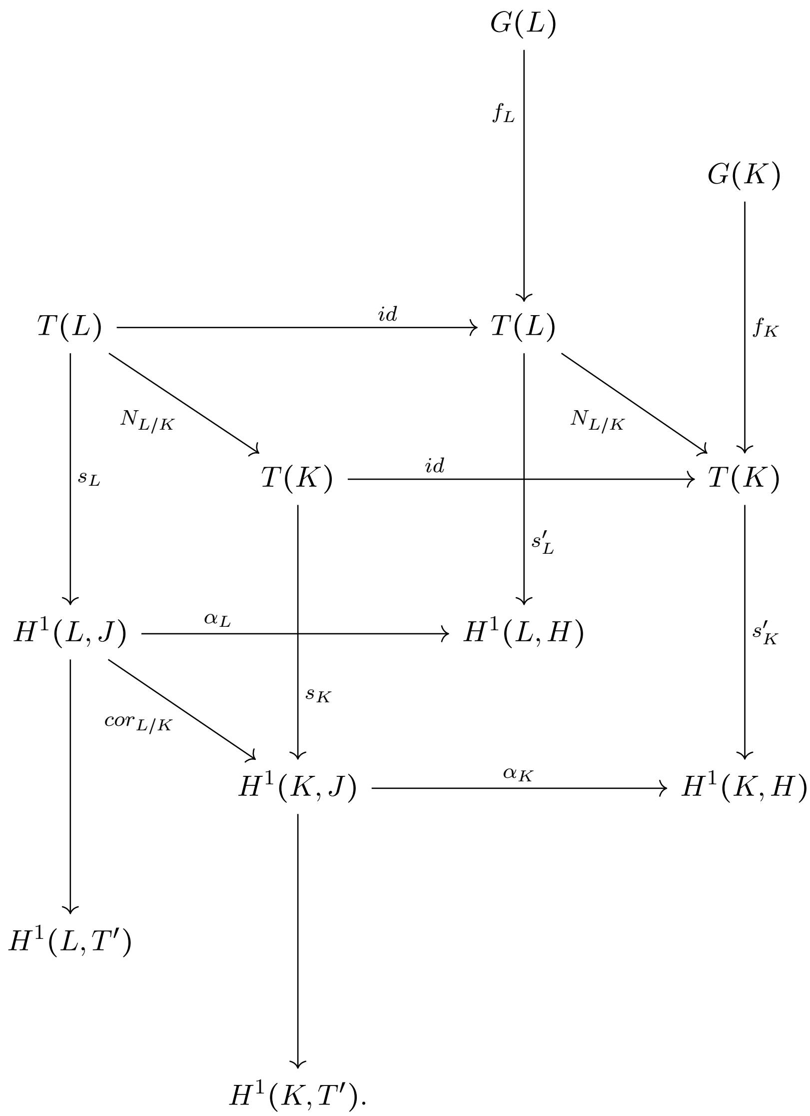
$$\begin{array}{ccc} H^1(L,J) & \xrightarrow{\alpha_L} & H^1(L,H) \\ \Big\downarrow{\scriptstyle cor_{L/K}} & & \\ H^1(K,J) & \xrightarrow{\alpha_K} & H^1(K,H). \end{array}$$

Recall that there is an anti-equivalence between the groups of multiplicative type (see [24, Chapter 7, Section 2]) and the abelian groups on which $\Gamma = Gal(K^{sep}/K)$ acts continuously (see [24, Chapter 7, Section 3]). Under this anti-equivalence, we can find an embedding $J \hookrightarrow T'$ where T' is a quasi-trivial torus over K. This can be done in the following way: Let A be the character group of J, and $a_1, a_2, \dots, a_n$ be generators of A as a Γ - module. For $1 \leq i \leq n$, let Δ_i be the subgroup of finite index in Γ which acts trivially on a_i. Then we have a surjection $\bigoplus_{i=1}^{n} \mathbb{Z}[\Gamma/\Delta_i] \longrightarrow A$, which corresponds to an embedding $J \hookrightarrow T'$ that we were looking for.

Consider the pushout of the morphisms $J \longrightarrow H$ and $J \longrightarrow T'$:

$$
\begin{array}{ccccccccc}
 & & 1 & & 1 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & J & \longrightarrow & H & \longrightarrow & G' & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle id} & & \\
1 & \longrightarrow & T' & \longrightarrow & G & \longrightarrow & G' & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle f} & & & & \\
 & & T & \xrightarrow{id} & T & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1. & & & &
\end{array}
$$

Since T' is a quasi-trivial torus, $H^1(L,T') = H^1(K,T') = 1$. This gives rise to the following commutative diagram where s and s' are the connecting maps of the first and second columns of the above diagram, respectively, and α is induced by the map $J \hookrightarrow H$.



Let $v = cor_{L/K}(u)$. Since $H^1(L,T') = 1$, $u \in \text{Im}(s_L)$. Let l be an element in $T(L)$ such that $s_L(l) = u$. Let $w = N_{L/K}(l)$. By the commutativity of the above diagram, $l \in \text{Ker}(s'_L) = \text{Im}(f_L)$. Since the H^0- variant of the norm principle holds for $f : G \longrightarrow T$, we have $w \in \text{Im}(f_K) = \text{Ker}(s'_K)$, therefore $\alpha_K(v) = s'_K(w) = 0$ and $v \in \text{Ker}(\alpha_K)$.

$(2 \Rightarrow 1)$:

Let $H = [G,G]$, $T = G^{ab}$, $T' = R(G)$ (the radical of G), $J = H \cap T'$, $G' = \frac{G}{R(G)}$. Then H is a semisimple group and $J \subseteq H$ is a central subgroup; with this set-up, the two diagrams above will again be commutative with exact rows and columns.

Let $s \in G(L)$, $l = f_L(s)$, $w = N_{L/K}(l)$. We would like to show $w \in \text{Im}(f_K)$. Let $u = s_L(l)$, $v = cor_{L/K}(u)$. So we have $s'_L(l) = 0$ hence $u \in \text{Ker}(\alpha_L)$. By assumption, the H^1- variant of the norm principle holds for the pair (J, H) over L/K, which implies that $\alpha_K(v) = 0$, therefore $w \in \operatorname{Ker}(s'_K) = \operatorname{Im}(f_K)$. □

4.4 Reduction to simply connected groups

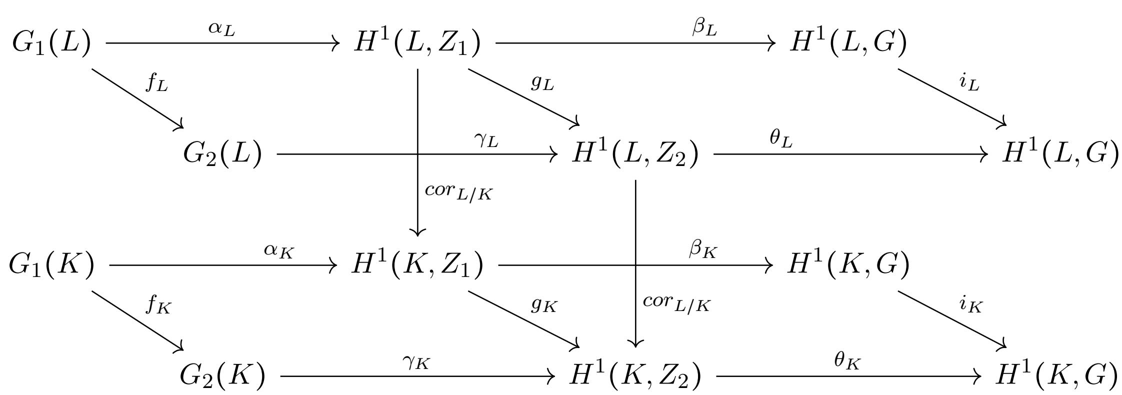
The next lemma states that in order to prove the H^1- variant of the norm principle for a pair (Z_1, G) it is enough to show the H^1- variant of the norm principle for (Z_2, G), where Z_2 is a central subgroup of G containing Z_1.

Lemma 4.4.1. Let L/K be a finite separable field extension and G be a semisimple algebraic group defined over K. Let $Z_1 \subseteq Z_2 \subseteq G$ be central subgroups. Then the H^1- variant of the norm principle for the pair (Z_2, G) over L/K implies the H^1- variant of the norm principle for the pair (Z_1, G) over L/K.

Proof. Let $G_1 := G/Z_1$ and $G_2 := G/Z_2$. We have the following diagram where i is the identity map:

$$\begin{array}{ccccc} G_1(-) & \longrightarrow & H^1(-, Z_1) & \longrightarrow & H^1(-, G) \\ {\scriptstyle f}\downarrow & & {\scriptstyle g}\downarrow & & {\scriptstyle i}\downarrow \\ G_2(-) & \longrightarrow & H^1(-, Z_2) & \longrightarrow & H^1(-, G). \end{array}$$

It gives rise to the following commutative diagram whose rows are exact:



Let $u \in \mathrm{Ker}(\beta_L) = Im(\alpha_L)$. Choose $v \in {\alpha_L}^{-1}(u)$, and put $w = \gamma_L(f_L(v))$. By assumption, $cor_{L/K}(w) \in \mathrm{Im}(\gamma_K) = \mathrm{Ker}(\theta_K)$. Hence $cor_{L/K}(u) \in \mathrm{Ker}(\beta_K)$ and the H^1- variant of the norm principle holds for the pair (Z_1, G) over L/K. □

Remark 4.4.2. From now on, by the **norm principle for** G (where G is a semisimple group), we shall mean the H^1**- variant of the norm principle for the pair** $(C(G), G)$ where $C(G)$ is the center of G, unless otherwise stated. By Lemma 4.4.1, it is enough to show the H^1- variant of the norm principle only for the full center of any semisimple group.

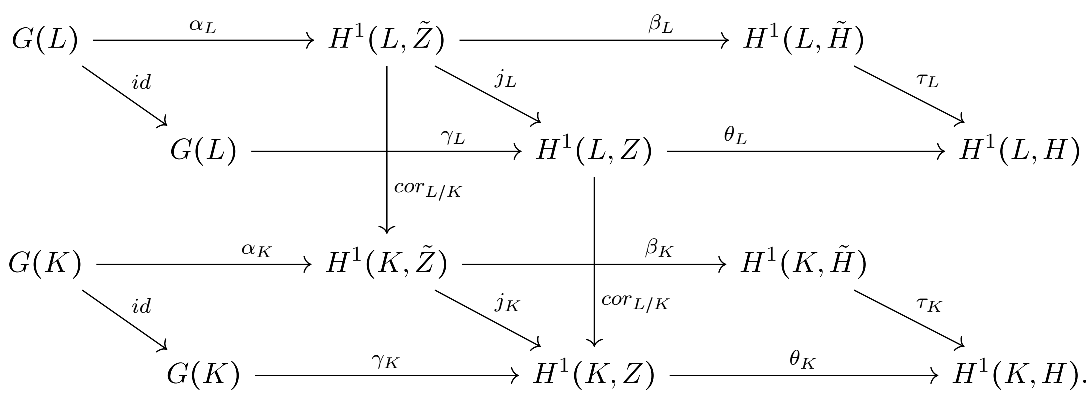
Now we show that the norm principle for a simply connected covering of a semisimple group implies the norm principle for the group itself.

Lemma 4.4.3. Let H be a semisimple algebraic group defined over K, L/K be a finite separable field extension, and $\phi : \tilde{H} \longrightarrow H$ be the simply connected covering of H. Then the norm principle for $\tilde{H}$ implies the norm principle for H (over L/K).

Proof. Let Z and $\tilde{Z}$ be the centers of H and $\tilde{H}$, respectively, and $G = H/Z = \tilde{H}/\tilde{Z}$. The following sequence (which is exact in rows)

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \tilde{Z} & \longrightarrow & \tilde{H} & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & Z & \longrightarrow & H & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

gives rise to the following commutative diagram whose rows are exact:



Let $v \in \text{Ker}(\theta_L)$. Choose $g \in {\gamma_L}^{-1}(v)$ and put $u = \alpha_L(g)$. By assumption, $cor_{L/K}(u) \in \text{Ker}(\beta_K) = Im(\alpha_K)$, therefore there exists $w \in G(K)$ such that $\alpha_K(w) = cor_{L/K}(u)$. Hence $cor_{L/K}(v) = \gamma_K(w) \in \text{Im}(\gamma_K) = \text{Ker}(\theta_K)$ and the norm principle holds for (Z, H).

□

Remark 4.4.4. By Lemmas 4.4.1 and 4.4.3, in order to prove the H^1- variant of the norm principle for a pair (Z, G), it is enough to prove it for $(C(\tilde{G}), \tilde{G})$, where $\tilde{G}$ is the simply connected covering of G, and $C(\tilde{G})$ is its center.

4.5 Norm principle for type D_n groups

The H^0- variant of the norm principle has been studied for various reductive groups.

Theorem 4.5.1. (Barquero and Merkurjev) Let G be a K-reductive group, and T a commutative K-group. Assume further that the Dynkin diagram of G does not contain connected components of type D_n; $n \geq 4, E_6$ or E_7. Then the H^0- variant of the norm principle holds for any K-group homomorphism $G \longrightarrow T$.

Proof. See [1, Theorem 1.1]. □

The norm principle is open for groups of type D_n in general. Theorem 4.3.1 and Remark 4.4.4 show that in order to prove the H^0- variant of the norm principle for reductive groups with connected components of type D_n, it is enough to show the H^1- variant of the norm principle for simply connected groups of type D_n.

Any absolutely simple, simply connected, classical K- linear algebraic group of type D_n is the spinor group $Spin(A, \sigma)$ for a central simple K-algebra A of degree $2n$ with orthogonal involution σ (see [13, Chapter 6]). Further results for groups of type D_n were obtained by Bhaskar, Chernousov and Merkurjev (see [4]).

In [4], the H^0- variant of the norm principle for the reductive group $\Omega(q)$, the extended Clifford group of a quadratic form q, over complete discretely valued fields and their residue fields has been studied. Under the equivalence of H^0 and H^1 variants of the norm principle proved in Section 4.3, the main result in [4] translates to the following:

Theorem 4.5.2. (**Bhaskar, Chernousov, and Merkurjev**)
Let K be a complete discretely valued field with residue field k and $char(k) \neq 2$. Assume that the H^1- variant of the norm principle holds for $Spin(q_1)$ for every regular quadratic form q_1 of even dimension defined over any finite extension of k. Then the H^1- variant of the norm principle holds for $Spin(q)$ for every regular quadratic form q of even dimension over K.

In other words, this result relates the norm principle for the spinor groups over the closed point in the spectrum of a complete discrete valuation ring to the norm principle over its generic point.

The main goal in this thesis is to generalize the above theorem to the case of skew-hermitian forms over quaternion algebras.

Let K be a field, *char* $K \neq 2$, and D a quaternion algebra over K. Suppose that σ is the canonical (symplectic) involution on D, and V is a left vector space over D of dimension n. Let h be a regular skew-hermitian form on V (with respect to the involution σ on D). It corresponds to an involution (the adjoint involution) σ_h on $End_D(V)$ (see [13, Page 1]), which is a central simple algebra of dimension $4n^2$ over K. The involution σ_h is orthogonal. Let $G = Spin(End_D(V), \sigma_h)$. We will simply denote G by $Spin(h)$.

The main result of this dissertation is the following:

Theorem 4.5.3. (The main theorem): Let K be a complete discretely valued field with residue field k, such that *char* $k \neq 2$. Assume that the norm principle holds for $G_1 = Spin(h_1)$ for every regular skew-hermitian form h_1 over any quaternion algebra D_1 defined over any finite extension of k. Then the norm principle holds for $G = Spin(h)$ for every regular skew-hermitian form h over any quaternion algebra D over K.

Let us consider the special case of split quaternion algebras. If a quaternion algebra D over K splits, i.e., $D = M_2(K)$, then by Morita equivalence (see Section 2.4, and [12, Chapter 1, Section 9]), any skew-hermitian form h corresponds to a quadratic form of even dimension over K, and by Theorem 4.5.2 we know that the H^1- variant of the norm principle for the spinor group of even dimensional quadratic forms over finite extensions of k implies the norm principle for the same objects over K. Therefore, Theorem 4.5.3 generalizes Theorem 4.5.2.

4.6 The plan for type D_n groups

Theorem 6.1.3 in Chapter 6 will show that the norm principle for the spinor group of a central simple algebra with orthogonal involution (A, σ) can be reduced to separable quadratic field extensions. To prove Theorem 6.1.3, we need generalizations of Scharlau and Knebusch norm principles to arbitrary (skew-) hermitian forms, which will be studied in Chapter 5. Theorem 6.1.3 will be applied in particular to our main question to reduce it to separable quadratic field extensions, by considering $(A, \sigma) = (End_D(V), \sigma_h)$ where (V, h) is a regular skew-hermitian space over a quaternion algebra D with respect to the canonical involution on D, and σ_h is the involution adjoint to h.

Since our main question concerns quaternion algebras over complete discretely valued fields, we need to consider the extension of a valuation from a valued field K to a quaternion division algebra D over K. By our reduction in Section 6.2, we will only need to work in the case where the skew-hermitian form h in the question is anisotropic. A key fact that will be needed is Larmour's theorem (Theorem 7.3.6), which is a generalization of Springer's decomposition theorem for quadratic forms (over complete discretely valued fields) to the case of (skew-) hermitian forms. This theorem is stated in Chapter 7. Also, we will describe how the diagonalization of an unramified or totally ramified skew-hermitian form looks like (Remark 7.3.5), which will be used in the proof of the main theorem.

In Chapter 8, we reduce the norm principle for $Spin(h)$, under specific assumptions, to the case that h is either unramified, or totally ramified (Remarks 8.3.2 and 8.3.3). Furthermore a strong theorem due to Merkurjev (Theorem 9.1.1) about the R- equivalence classes of the adjoint groups of type D_n will be stated, which will be used in Chapter 9 in some of the cases. Finally, we prove the main theorem in Chapter 8. All the reductions in Chapters 6 and 8 will be of essential use in the proof of the main result.

Chapter 5

More norm principles

In Chapter 8, we will study the norm principle for spinor groups of skew-hermitian forms over quaternion algebras defined over complete discretely valued fields. Note that when n is odd, then an absolutely simple simply connected group of type D_n is the spinor group of a skew-hermitian form over a quaternion algebra.

In Chapter 6, we will show that the norm principle holds for the spinor groups over finite separable field extensions if it holds over separable quadratic field extensions. This reduction uses generalizations of Scharlau and Knebusch norm principles, which we will discuss in this chapter (Theorems 5.2.1 and 5.3.2). Another norm principle due to Philippe Gille will be introduced in Section 5.1, which will be used in Section 5.2 to generalize the Knebusch norm principle.

5.1 R-equivalence and Gille's norm principle

In order to state Gille's norm principle, we need the notion of R-equivalence.

Definition 5.1.1. Let G be a linear algebraic group defined over K. Then $x, y \in G$ are said to be R-equivalent if there exists a K-rational map $\mathbb{A}^1 \dashrightarrow G$ defined at 0 and 1, which sends 0 to x and 1 to y. This defines an equivalence relation on $G(K)$. The set of all points in $G(K)$ which are $R-$equivalent to identity is denoted by $RG(K)$. For a connected linear algebraic group G over K, this set is in fact a normal subgroup of $G(K)$ (see [23, Section 6.2, Lemma 6.3] and [8, Section 2.1]).

An algebraic group G defined over K is said to be **R-trivial** if for all field extensions F/K, the group $G(F)$ has only one R- equivalence class, i.e., $RG(F) = G(F)$.

Let $\beta : \tilde{G} \longrightarrow G$ be a central $K-$isogeny of reductive algebraic groups defined over a field K with kernel Z. We have the exact sequence of the Galois cohomology pointed sets

$$1 \longrightarrow Z(K) \longrightarrow \tilde{G}(K) \xrightarrow{\beta_K} G(K) \xrightarrow{\phi_K} H^1(K, Z) \xrightarrow{e_K} H^1(K, \tilde{G}).$$

Let L/K be a finite separable field extension. In [8], Gille proved the following result.

Theorem 5.1.2. (**Gille**, [8]) $cor_{L/K}(\phi_L(RG(L)) \subseteq \phi_K(RG(K))$.

Remark 5.1.3. Suppose the element $u \in G(L)$ is R–equivalent to 1, and $u' = \phi_L(u)$. Note that $u' \in \mathrm{Ker}(e_L)$. By Theorem 5.1.2, $cor_{L/K}(u') \in \mathrm{Ker}(e_K)$ and $cor_{L/K}(u') = \phi_K(w)$ for an element $w \in G(K)$ which is R–equivalent to 1 in $G(K)$. Therefore, Theorem 5.1.2 shows that the property of simultaneously being in the kernel of e and being the image of an element R–equivalent to 1 is always preserved under the corestriction map L/K. So Theorem 5.1.2 can be viewed as some kind of norm principle, although it is not equivalent to any of the two variants introduced before.

Remark 5.1.4. Suppose $\tilde{G}$ is semisimple, and G is $K-$ rational (as a variety). Then by Theorem 5.1.2 we will have the H^1- variant of the norm principle for the pair $(Z, \tilde{G})$ (recall that Z is a central subgroup of $\tilde{G}$, which is kernel of the map $\tilde{G} \to G$) over L/K, since any two elements in G will be $R-$ equivalent.

Remark 5.1.5. It is known that for any semisimple adjoint linear algebraic group of classical type G over a number field K, the group $G(K)/R$ is trivial (see [8]). Therefore by Theorem 5.1.2, the norm principle holds for all classical semisimple algebraic groups over number fields.

5.2 Generalization of Knebusch's norm principle

This section concerns the norm principle for spinor norms, whose definition is as follows: by a **spinor norm** of a central simple algebra A with orthogonal involution σ over a field $*$, we mean the elements in the kernel of the following map:

$$H^1(*, \mu_2) \longrightarrow H^1(*, Spin(A, \sigma))$$

which is induced by the exact sequence

$$1 \longrightarrow \mu_2 \longrightarrow Spin(A, \sigma) \longrightarrow O^+(A, \sigma) \longrightarrow 1.$$

Note that Theorem 3.2.1 concerns the behavior of spinor norms of quadratic forms under finite separable field extensions, with respect to the norm map (when (A, σ) is the matrix algebra with orthogonal involution associated to q). Now we recall a generalization of Theorem 3.2.1, which is due to Gille (see [8]).

Theorem 5.2.1. Let μ_2 be the kernel of the morphism $Spin(A, \sigma) \to O^+(A, \sigma)$. Then the H^1- variant of the norm principle holds for the pair $(\mu_2, Spin(A, \sigma))$ over L/K.

Proof. The exact sequence

$$1 \longrightarrow \mu_2 \longrightarrow Spin(A, \sigma) \longrightarrow O^+(A, \sigma) \longrightarrow 1$$

gives rise to the following exact sequence

$$O^+(A, \sigma)(L) \xrightarrow{\delta_L} H^1(L, \mu_2) \xrightarrow{h_L} H^1(L, Spin(A, \sigma)).$$

Since the variety $O^+(A,\sigma)$ is rational (see [6, Proposition 2.4]), then we have the desired result by Remark 5.1.4. □

Note that if $(A,\sigma) = (M_n(K), \sigma_f)$ corresponds to a quadratic form f of dimension n over K, then Theorem 5.2.1 is equivalent to Knebusch's norm principle for quadratic forms, since the elements in $\mathrm{Ker}(h) : H^1(-,\mu_2) \xrightarrow{h} H^1(-, Spin(A,\sigma))$ are exactly the spinor norms.

5.3 Generalization of Scharlau's norm principle

In this section, we will generalize Scharlau's norm principle.

Consider a skew field with symplectic involution (D,σ) over a field K, and a skew-hermitian form h over (D,σ). We have the following commutative exact diagram:

$$
\begin{array}{ccccccccc}
 & & 1 & & 1 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & O^+(h) & \longrightarrow & PGO^+(h) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle id} & & \\
1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & GO^+(h) & \longrightarrow & PGO^+(h) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \times 2} & & \downarrow{\scriptstyle \mu} & & & & \\
 & & \mathbb{G}_m & \xrightarrow{id} & \mathbb{G}_m & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & & &
\end{array}
$$

Recall that the center of $O^+(h)$ is μ_2, and μ is the multiplier map (see Section 2.4). The proof of Theorem 4.3.1 shows that the H^0−variant of the norm principle for the multiplier map μ is equivalent to the H^1−variant of the norm principle for the pair $(\mu_2, O^+(h))$. Let β_K be the induced Galois cohomology map $\beta_K : H^1(K,\mu_2) \longrightarrow H^1(K, O^+(h))$. Recall that the elements of $H^1(K,\mu_2)$ are in one-to-one correspondence with isometry classes of skew-hermitian forms with the same dimension and the same discriminant as h, and the distinguished element of $H^1(K, O^+(h))$ is the K−isometry class of h (see [13, Section 29.D]). Let η be an element in $H^1(K,\mu_2) = K^*/K^{*2}$ and choose a representative for η, say $aK^{*2} \in K^*/K^{*2}$ for some $a \in K^*$. The map β_K sends the square class $\eta = [a]$ to the K−isometry class of the skew-hermitian form ah. Assume that $\eta \in \mathrm{Ker}\,\beta_K$. Then ah is isometric to the skew-hermitian form h over K, hence the element a will be a similarity factor for h over K. Conversely, if a is a similarity factor for h over K, i.e., if $ah \cong h$ over K, then the element η will be in the kernel of the map β_K. A same argument as above works if we replace the skew-hermitian form h with a quadratic form q: the elements in the kernel of the Galois cohomology map induced by the embedding $\mu_2 \to O^+(q)$ are in one-to-one correspondence with the square classes of the similarity factors of q. Hence, the H^1- variant of the norm principle for the pair $(\mu_2, O^+(q))$ is equivalent to Scharlau's norm principle for the quadratic form q (Theorem 3.1.1).

The next theorem is related to the hyperbolicity of skew-hermitian forms over skew fields and over the function fields of their Severi-Brauer varieties. Theorem 5.3.1 will be used to generalize Scharlau's norm principle (see Theorem 5.3.2). For definition of hyperbolic forms, see [20, Chapter 1, Section 4, Page 12]. Also for the Severi-Brauer varieties see [9, Chapter 5, Section 1, Page 115].

Theorem 5.3.1. Let (D, σ) be a skew field with symplectic involution and h a skew-hermitian form over (D, σ). Let E be the function field of $SB(D)$ (the Severi-Brauer variety over D). If h is hyperbolic over D_E, then it is hyperbolic over D.

Proof. See [11, Theorem 1.1]. □

Theorem 5.3.2. (Generalization of Scharlau's norm principle) Let (D, σ) be a skew field with symplectic involution σ over K, and h be a skew-hermitian form over (D, σ) with dimension d. Then the norm principle holds for $O^+(h)$ over any finite separable field extension L/K.

Proof. Let E be the function field of $SB(D)$, the Severi-Brauer variety of D. Consider the following commutative diagram, whose arrows are inclusions and $LE := L \underset{K}{\otimes} E$:

$$\begin{array}{ccc} L & \longrightarrow & LE \\ \uparrow & & \uparrow \\ K & \longrightarrow & E \end{array}$$

Let $V := D^d$, $D_L := D \underset{K}{\otimes} L$, $D_E := D \underset{K}{\otimes} E$, $D_{LE} := D \underset{K}{\otimes} LE$, $V_L := V_{D_L}$, $V_E := V_{D_E}$, and $V_{LE} := V_{D_{LE}}$. Also let h_{D_L}, h_{D_E}, and $h_{D_{LE}}$ be the corresponding skew-hermitian forms over V_L, V_E, and V_{LE}, respectively.

Let β_L be the induced Galois cohomology map $\beta_L : H^1(L, \mu_2) \longrightarrow H^1(L, O^+(h))$. Let η be an element in $H^1(L, \mu_2) = L^*/L^{*2}$ and choose a representative for η, say $aL^{*2} \in L^*/L^{*2}$ for some $a \in L^*$. Assume that $\eta \in \operatorname{Ker} \beta_L$, so $ah_L \cong h_L$. Hence $h_{D_L} \perp -ah_{D_L}$ is hyperbolic, and so is $h_{D_{LE}} \perp -ah_{D_{LE}}$. Since $SB(D)$ is a Severi-Brauer variety, D_E splits, i.e., $D_E \cong M_n(E)$ for some $n \in \mathbb{N}$. We also have $D_{LE} \cong M_n(LE)$. By Morita equivalence ([12], Chapter 1, Section 9), skew-hermitian forms over D_E (respectively D_{LE}) correspond to quadratic forms over E (respectively LE). So we get a quadratic form f_E (respectively f_{LE}). Under this correspondence, direct sums and hyperbolicity is preserved. Therefore, $h_{D_{LE}} \perp -ah_{D_{LE}}$ corresponds to a hyperbolic quadratic form $f_{LE} \perp -af_{LE}$, which means a is a multiplier of f_{LE}. By Scharlau's norm principle, $f_E \perp -N_{LE/E}(a)f_{LE}$ is hyperbolic, and by Theorem 5.3.1, $h \perp -N_{L/K}(a)h$ is hyperbolic. So $N_{L/K}(a)$ is a multiplier of h, and $cor_{L/K}(\eta) \in \operatorname{Ker}(\beta_K)$. □

Chapter 6

Two reductions

6.1 Reduction of the norm principle to quadratic field extensions

Assume that A is a central simple K-algebra with an orthogonal involution σ. In this section, we will reduce the norm principle for the spinor group of (A,σ), from arbitrary finite separable field extensions to quadratic field extensions.

The spinor group $Spin(A,\sigma)$ is a semisimple group of type D_n, whose center will be denoted by Z. Let $F := K(\sqrt{disc\ \sigma})$. Then $Z = \mathbf{R}_{F/K}(\mu_2)$ if n is even, and $Z = \text{Ker}\ (\mathbf{R}_{F/K}(\mu_4) \overset{Norm}{\longrightarrow} \mu_4)$ if n is odd (see [19, Page 332]).

Theorem 6.1.1. Let L/K be a finite separable field extension of an odd degree n, and $a \in K$. Then $aK^{*2} \in H^1(K,\mu_2)$ is a spinor norm iff $aL^{*2} \in H^1(L,\mu_2)$ is a spinor norm.

Proof. **From K to L**: trivial.

From L to K:

Since n is odd we have

$$cor_{L/K}(aL^{*2}) = cor_{L/K} \circ res_{L/K}(aK^{*2}) = a^n K^{*2} = aK^{*2},$$

and by Theorem 5.2.1,

$$cor_{L/K}(aL^{*2}) \in \text{Ker}(h_K : H^1(K,\mu_2) \longrightarrow H^1(K, Spin(A,\sigma))),$$

i.e., aK^{*2} is a spinor norm. □

Theorem 6.1.2. Let E/K be an infinite algebraic extension such that any finite subextension L/K is of odd degree. Then for any $a \in K$, $aK^{*2} \in H^1(K,\mu_2)$ is a spinor norm iff $aE^{*2} \in H^1(E,\mu_2)$ is a spinor norm.

Proof. **From K to E**: trivial.

From E to K: Consider the following exact sequence

$$O^+(A,\sigma)(E) \overset{\delta_E}{\longrightarrow} H^1(E,\mu_2) \overset{h_E}{\longrightarrow} H^1(E, Spin(A,\sigma)).$$

Suppsoe $aE^{*2} \in H^1(E, \mu_2)$ is a spinor norm, i.e., $aE^{*2} \in \operatorname{Ker} h_E$. Then there is an element $M \in O^+(A, \sigma)(E)$ such that $\delta_E(M) = aE^{*2}$.

Let L be a subfield of E which is a finite extension of K, such that $M \in O^+(A, \sigma)(L)$. Then the element aL^{*2} becomes a spinor norm over L, and since L/K is of odd degree, we conclude the result by Theorem 6.1.1. □

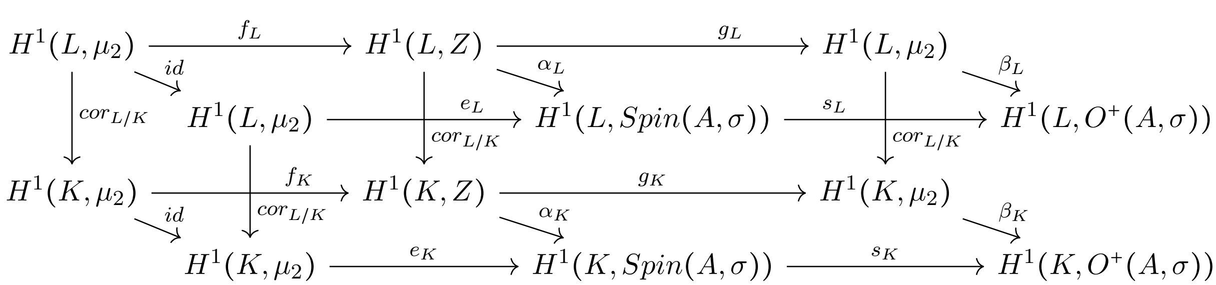
Now we prove the main result of this section:

Theorem 6.1.3. Let (A, σ) be a central simple algebra with orthogonal involution defined over a field K. Assume that the norm principle holds for $Spin(A, \sigma)$ over any separable quadratic field extension E/F, where F contains K. Then the norm principle holds for $Spin(A, \sigma)$ over any finite separable field extension L/K.

Proof. Consider the following commutative diagram whose vertical arrows are inclusions:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_2 & \longrightarrow & Z & \longrightarrow & \mu_2 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mu_2 & \longrightarrow & Spin(A,\sigma) & \longrightarrow & O^+(A,\sigma) & \longrightarrow & 1 \end{array}$$

It gives rise to:



It is commutative and exact in all rows. Let $u \in \operatorname{Ker}(\alpha_L)$. We will show that $cor_{L/K}(u) \in \operatorname{Ker}(\alpha_K)$.

Put $v = g_L(u)$, $w = cor_{L/K}(u)$. By commutativity of the above diagram, $v \in \operatorname{Ker}(\beta_L)$, so by Theorem 5.3.2, $cor_{L/K}(v) \in \operatorname{Ker}(\beta_K)$. We also have

$$s_K(\alpha_K(w)) = \beta_K(g_K(w)) = \beta_K(cor_{L/K}(v)) = 1,$$

hence $\alpha_K \in \mathrm{Ker}(s_K) = \mathrm{Im}(e_K)$. Let $bK^{*2} \in H^1(K, \mu_2)$ be a pre-image of $\alpha_K(w)$ under the map e_K. We have

$$bK^{*2} \in \mathrm{Ker}(e_K) \iff w \in \mathrm{Ker}(\alpha_K)$$

Therefore, the *obstruction to the norm principle* for $Spin(A, \sigma)$ over L/K lives in $H^1(K, \mu_2)$. If one shows that this obstruction is a spinor norm, then the norm principle holds.

Let $\theta \in L$ be a generator for the extension L/K, i.e., $L = K(\theta)$. Assume that f is the minimal polynomial of θ over K. Take any infinite algebraic extension E/K. We have

$$L \underset{K}{\otimes} E = \frac{K[x]}{(f(x))} \underset{K}{\otimes} E = \frac{E[x]}{(f(x))}$$

Let $f = f_1 f_2 \dots f_m$ be the factorization of f in $E[x]$ into irreducible polynomials (note that f_i's are distinct because of separability of L/K), and for every $1 \le i \le m$, let L_i be $\frac{E[x]}{(f_i)}$. Then

$$L \underset{K}{\otimes} E = \frac{E[x]}{(f_1)} \times \frac{E[x]}{(f_2)} \times \dots \times \frac{E[x]}{(f_m)} = L_1 \times L_2 \times \cdots \times L_m$$

So $L \underset{K}{\otimes} E = L_1 \times L_2 \times \cdots \times L_m$ is an étale algebra where each L_i is a finite separable extension of E of degree equal to $deg f_i$.

Let Γ be the Galois group of K^{sep}/K and $\Delta \subseteq \Gamma$ be a 2-Sylow subgroup. This corresponds to a tower $K \subseteq E \subseteq K^{sep}$ of fields where E is the elementwise fixed field of Δ, so that $Gal(K^{sep}/E) = \Delta$. The degree of every finite subextension L_i/E is going to be a power of 2, and the degree of every subextension of finite degree of E/K is odd. By Theorem 6.1.2, in order to show that $b\frac{K^*}{K^{*2}}$ is a spinor norm over K, it suffices to show it is a spinor norm over E.

Consider the restriction map, which sends u to $(u_1, \dots, u_m)$:

$$res_{L\underset{K}{\otimes}E/L} : H^1(L, Z) \longrightarrow H^1(L\underset{K}{\otimes}E, Z) = H^1(L_1 \times L_2 \times \cdots \times L_m, Z) = H^1(L_1, Z) \times \cdots \times H^1(L_m, Z)$$

$$u \mapsto (u_1, \cdots, u_m)$$

We have the following diagram (all arrows are inclusion maps)

$$\begin{array}{ccc} E & \longrightarrow & L \underset{K}{\otimes} E \\ \uparrow & & \uparrow \\ K & \longrightarrow & L \end{array}$$

which gives rise to the following (the group Z is abelian, so the corestriction maps exist):

$$\begin{array}{ccc} H^1(E,Z) & \xleftarrow{cor_{L\underset{K}{\otimes}E/E}} & H^1(L \underset{K}{\otimes} E, Z) = H^1(L_1,Z) \times \cdots \times H^1(L_m,Z) \\ {\scriptstyle res_{E/K}}\uparrow & & \uparrow{\scriptstyle res_{L\underset{K}{\otimes}E/L}} \\ H^1(K,Z) & \xleftarrow{cor_{L/K}} & H^1(L,Z) \end{array}$$

By chasing u in the diagram above, we get

$$res_{E/K}(cor_{L/K}(u)) = \prod_{i=1}^{m} cor_{L_i/E}(u_i). \tag{6.1}$$

Since Δ is a 2-Sylow subgroup, for every $1 \leq i \leq m$ there exists a tower $E = L_{i,0} \subseteq L_{i,1} \subseteq L_{i,2} \subseteq \cdots \subseteq L_{i,deg(f_i)} = L_i$ where each $L_{i,j}$ is a quadratic extension of $L_{i,j-1}$. We have

$$cor_{L_i/E}(u_i) = cor_{L_{i,1}/L_{i,0}} \circ cor_{L_{i,2}/L_{i,1}} \circ \cdots \circ cor_{L_{i,degf_i}/L_{i,degf_i-1}}(u_i).$$

By assumption, the norm principle holds for any separable quardratic field extension F_1/F_2. Hence each $cor_{L_i/E}(u_i)$ becomes a spinor norm, and so does their product (6.1). □

6.2 Reduction to anisotropic skew-hermitian forms

In this section, we will reduce the norm principle for spinor groups of skew-hermitian forms to the case that the skew-hermitian form is anisotropic.

First, we need to prove two lemmas in Galois cohomology.

Lemma 6.2.1. Let K be a field and G an algebraic group defined over K with center Z, and $\bar{G} = G/Z$. Then the coboundary map

$$\gamma_K : \bar{G}(K) \longrightarrow H^1(K,Z)$$

is a homomorphism of abstract groups.

Proof. Let h_1 be an element in $\bar{G}(K)$. Take a preimage g_1 of h_1 in $G(K^{sep})$. Then $\gamma_K(h_1)$ is the class of the following cocyle

$$a_1 : Gal(\bar{K}/K) \longrightarrow Z$$

$$s \mapsto {g_1}^{-1}{g_1}^s.$$

We can take another arbitrary element h_2 in $\bar{G}(K)$, a preimage $g_2 \in G(K)$, and a cocycle a_2 in a similar manner. Now $\gamma_K(h_1h_2)$ will be the class of the cocycle $s \mapsto (g_1g_2)^{-1}(g_1g_2)^s$. The element ${g_1}^{-1}{g_1}^s$ is in Z, so it commutes with ${g_2}^{-1}$. Then we have:

$$(g_1g_2)^{-1}(g_1g_2)^s = {g_2}^{-1}{g_1}^{-1}{g_1}^s{g_2}^s = ({g_1}^{-1}{g_1}^s)({g_2}^{-1}{g_2}^s)$$

which shows that the map γ_K is a homomorphism of abstract groups. □

Lemma 6.2.2. Let K be a field and G an algebraic group defined over K with a central subgroup Z. Let η_K be the induced map $\eta_K : H^1(K,Z) \longrightarrow H^1(K,G)$. Assume that a and b are two cocycles with coefficients in Z such that $\eta_K([a]) = \eta_K([b])$. Then $\eta_K([ab^{-1}]) = 1$.

Proof. Let i be the inclusion map $i : Z \longrightarrow G$. For any cocycle c with with coefficients in Z, the induced map η_K sends $[c]$ to $[i \circ c]$. Since $\eta_K([a]) = \eta_K([b])$, there exist an element $g \in G$ such that for every $s \in Gal(\bar{K}/K)$ we have $(i \circ a)(s) = g^{-1}((i \circ b)(s))g^s$. The subgroup Z is central in G, hence for any element $s \in Gal(\bar{K}/K)$ the elements $((i \circ a)(s))$ and $((i \circ b)(s))$ commute with every element of G. Therefore

$$(i \circ ab^{-1})(s) = g^{-1}g^s,$$

which means $i \circ ab^{-1}$ is cohomologous to 1. □

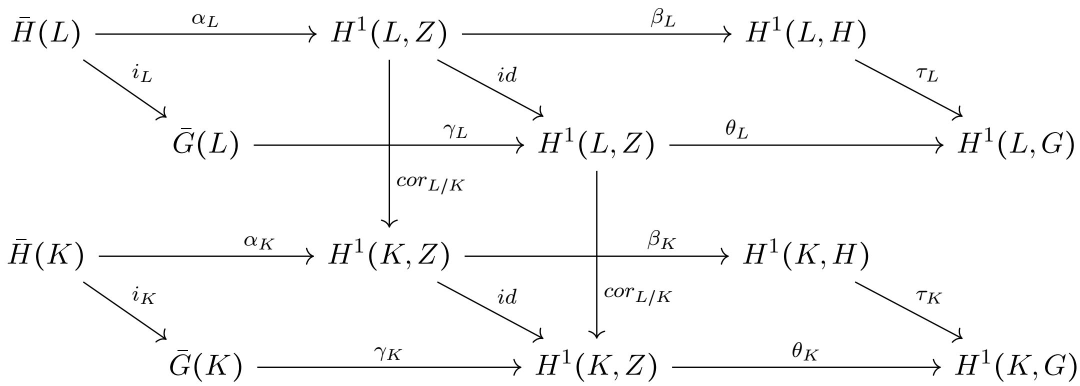
Now we prove a lemma which reduces the norm principle for a semisimple group G to one of its subgroups.

Lemma 6.2.3. Let K be a field, G be a semisimple group defined over K with center Z, and $\bar{G} = G/Z$. Let H be a semisimple subgroup of G containing Z, and $\bar{H} = H/Z$. Assume that for every finite separable field extension L/K, and every element g in $\bar{G}(L)$, there exist elements $g_1 \in R\bar{G}(L)$ and $g_2 \in \bar{H}(L)$ such that $g = g_1g_2$. If the H^1- variant of the norm principle holds for (Z,H), then it does so for (Z,G).

Proof. Consider the following diagram (which is exact in rows)

$$\begin{array}{ccccccccc}
1 & \longrightarrow & Z & \longrightarrow & H & \longrightarrow & \bar{H} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} & & \\
1 & \longrightarrow & Z & \longrightarrow & G & \longrightarrow & \bar{G} & \longrightarrow & 1
\end{array}$$

It gives rise to the following commutative diagram whose rows are exact:



The identity and inclusion are denoted by id and i, respectively.

Let $u \in \text{Ker}(\theta_L)$, $v := cor_{L/K}(u)$, and $g \in \bar{G}(L)$ such that $\gamma_L(g) = u$. By assumption, there exists $g_1 \in R\bar{G}(L)$ and $h \in \bar{H}(L)$ such that $g = g_1 h$. Put $u' := \gamma_L(i_L(h))$. By Lemma 6.2.1 the map γ_L is a group homomorphism, so:

$$u(u')^{-1} = \gamma_L(g)\gamma_L(i_L(h))^{-1} = \gamma_L(gh^{-1}) = \gamma_L(g_1).$$

Hence, $u(u')^{-1} \in \text{Ker}(\theta_L)$. The element $u(u')^{-1}$ is image of an element in $R\bar{G}(L)$ under γ_L, therefore by Theorem 5.1.2 we have $cor_{L/K}(u(u')^{-1}) \in \text{Ker}(\theta_K)$. Since $u' = \gamma_L(i_L(h)) = \alpha_L(h) \in \text{Im}(\alpha_L) = \text{Ker}(\beta_L)$, by assumption $cor_{L/K}(u') \in \text{Ker}(\beta_K) \subseteq \text{Ker}(\theta_K)$. Hence $cor_{L/K}((u')^{-1}) \in \text{Ker}(\theta_K)$ and by Lemma 6.2.2 we have $v \in \text{Ker}(\theta_K)$. □

Assume that G is an isotropic group. Let T be a maximal split torus in G, and P be a minimal parabolic subgroup in G containing $C_G(T)$, the centralizer of T in G. Then any element in P can be written as a product of an element in the unipotent radical of P (which is R-trivial), and an element in $C_G(T)$ (the Levi subgroup). By Levi decomposition of G, any element in G can be written as a product of an R-trivial element and an element in $C_G(T)$. Therefore, if the H^1- variant of the norm principle holds for $(Z, C_G(T))$, where Z is a central subgroup in G, then it holds for (Z, G), by applying Lemma 6.2.3 to $H = C_G(T)$.

We will now reduce the norm principle of the spinor groups, to that of the anisotropic spinor groups.

For spinor group of quadratic forms, the reduction to anisotropic case can be done by directly showing the norm principle for the spinor groups of isotropic quadratic forms. For an isotropic quadratic form q over K, we know that the spinor norm map of q is surjective, hence every scalar is a spinor norm. In the proof of Theorem 6.1.3, we showed that the obstructions to norm principle for $Spin(q)$ over K are elements in $H^1(K, \mu_2)$, and the norm principle holds for $Spin(q)$ if the obstructions are spinor norms. Therefore, the norm principle holds for $Spin(q)$ if q is $K-$ isotropic. What we will show for skew-hermitian forms is slightly different: we will prove that if the norm principle holds for the spinor groups of all anisotropic skew-hermitian forms, then it does so for the spinor groups of all skew-hermitian forms.

Lemma 6.2.4. Let (D, σ) be a central division algebra with symplectic involution over K, $charK \neq 2$, L/K a finite separable field extension, and h an isotropic regular skew-hermitian form on (D, σ) of dimension n. Assume that for every regular skew-hermitian form h' on (D, σ) of dimension at most $n-1$, the norm principle holds for $Spin(h')$ over L/K. Then the norm principle holds for $Spin(h)$ over L/K.

Proof. Let $Z = C(Spin(h))$, the center of $Spin(h)$. The skew-hermitian form h admits a decomposition $h = h_1 \perp h_2$ over K, where h_1 is the two dimensional skew-hermitian form $h_1(x_1, x_2) = x_1 {x_2}^\sigma$ (The skew-hermitian form h_2 is not necessarily anisotropic). The special orthogonal group of h_1 contains (but is not equal to) all two by two diagonal matrices with determinant 1 (because they preserve the skew-hermitian form). Hence, there is a one-dimensional torus T inside $O^+(h_1)$. The image of T in $PGO^+(h)$ will be denoted by $\bar{T}$. We have a sequence

$$Z \longrightarrow Spin(h) \longrightarrow O^+(h) \longrightarrow PGO^+(h) \tag{6.2}$$

and a short exact sequence

$$1 \longrightarrow Z \longrightarrow Spin(h) \longrightarrow PGO^+(h) \longrightarrow 1. \tag{6.3}$$

The centralizer of T in $O^+(h)$ is a subgroup of $O^+(h_1) \times O^+(h_2)$. So there are groups H and $\bar{H}$ such that they fit into the following diagram whose vertical arrows are inclusions:

$$\begin{array}{ccccccc}
 & & & & C_{O^+(h)}(T) & \longrightarrow & C_{PGO^+(h)}(\bar{T}) \\
 & & & & \downarrow & & \downarrow \\
 & & H & \longrightarrow & O^+(h_1) \times O^+(h_2) & \longrightarrow & \bar{H} \\
 & & \downarrow & & \downarrow & & \downarrow \\
Z & \longrightarrow & Spin(h) & \longrightarrow & O^+(h) & \longrightarrow & PGO^+(h)
\end{array}$$

The group H is in fact an almost direct product of $Spin(h_1)$ and $Spin(h_2)$. Consider the map $H \longrightarrow O^+(h_1) \times O^+(h_2)$ and the central elements $(-1,1)$ and $(1,-1)$ in $O^+(h_1) \times O^+(h_2)$. Let z_1 and z_2 be the pre-images of $(-1,1)$ and $(1,-1)$ in H, respectively. Each of them is a central element of order 2 in H, hence H must contain the center Z. So we have the following diagram:

$$\begin{array}{ccccccc} Z & \longrightarrow & H & \longrightarrow & O^+(h_1)\times O^+(h_2) & \longrightarrow & \bar{H} \\ \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \downarrow \\ Z & \longrightarrow & Spin(h) & \longrightarrow & O^+(h) & \longrightarrow & PGO^+(h) \end{array}$$

All vertical arrows in the diagram above are inclusions. Consider the simply connected covering $Spin(h_1) \times Spin(h_2) \longrightarrow H$. Let $\tilde{H} := Spin(h_1) \times Spin(h_2)$. By assumption, the norm principle holds for the groups $Spin(h_1)$ and $Spin(h_2)$. Let $\tilde{Z}$ be the center of $\tilde{H}$. Consider the following diagram:

$$\begin{array}{ccl} H^1(L,\tilde{Z}) & \xrightarrow{\alpha_L} & H^1(L,\tilde{H}) = H^1(L, Spin(h_1)) \times H^1(L, Spin(h_2)) \\ {\scriptstyle cor_{L/K}}\downarrow & & \\ H^1(K,\tilde{Z}) & \xrightarrow{\alpha_K} & H^1(K,\tilde{H}) = H^1(K, Spin(h_1)) \times H^1(K, Spin(h_2)) \end{array}$$

Let $u \in \mathrm{Ker}(\alpha_L)$. Then by assumption, the projection of $\alpha_K(cor_{L/K}(u))$ on each of the groups $H^1(K, Spin(h_1))$ and $H^1(K, Spin(h_2))$ will be trivial, so $cor_{L/K}(u) \in \mathrm{Ker}(\alpha_K)$. Therefore, the norm principle holds for the pair $(\tilde{Z}, \tilde{H})$. By Lemma 4.4.3, the norm principle holds for the pair (Z, H). We had shown a reduction of the norm principle for semisimple groups to the centralizer of their maximal tori. Therefore, since the group $\bar{H}$ contains the group $C_{PGO^+(h)}(\bar{T})$, the norm principle holds for $Spin(h)$ over L/K.

□

The norm principle is known for type A_n groups (see [1]). By the exceptional isomorphisms $D_2 \cong A_1 \times A_1$ and $D_3 \cong A_3$ (see [13, Chapter 4, Section 15.D]), we know the norm principle holds for type D_n groups when $n < 4$. Assume that the norm principle holds for $Spin(h)$ for all anisotropic skew-hermitian forms over (D, σ). Then using Lemma 6.2.4, we can conclude by induction that the norm principle holds for all type D_n groups. This conclusion is summarized in the next statement:

Lemma 6.2.5. Let (D, σ) be a central division algebra with symplectic involution over K, $char K \neq 2$, and L/K be a finite separable field extension. If the norm principle holds for $Spin(h)$ for all anisotropic skew-hermitian forms h over (D, σ), then so does for $Spin(h)$ for all skew-hermitian forms h over (D, σ).

According to Theorem 6.1.3, in the proof of the main theorem (in Chapter 9) we will have the hypothesis that the degree of the field extension in the question is 2. So in this section, from now on, we assume that L/K is a separable quadratic extension and let θ be a generator of this extension such that $\theta^2 \in K$ (such element exists because *char* $K \neq 2$). Consider a quaternion algebra D defined over K (which we denote by D_K as well). We will further reduce the norm principle for $Spin(h)$ over L/K to the case that h is $L-$anisotropic as well. In order to prove this reduction, we need the following fact.

Theorem 6.2.6. Let (D, σ) be a nonsplit quaternion algebra with canonical involution over K, and L/K a quadratic separable field extension. Let h be a skew hermitian form over (D, σ). Assume that D splits over L, and h is $L-$ isotropic. Then there is a diagonalization $h =< d_1, \ldots, d_n >$ over K such that $K(d_1) \cong L$.
With the above assumptions, we have

$$O^+(< d_1 >)(L) = {R_{L/K}}^{(1)}(\mathbf{G}_m).$$

Proof. See [18, Theorem A.1]. □

Lemma 6.2.7. With all the previous notations (as in Lemma 6.2.5) and a further assumption that D is a quaternion algebra, assume that the norm principle holds for $Spin(h)$ for any skew-hermitian form h which is anisotropic over L. Then the norm principle holds for $Spin(h)$ where h is any skew-hermitian form which is anisotropic over K (but not over L necessarily).

Proof. Assume that h is a $K-$anisotropic skew hermitian form which is $L-$isotropic. Let $Z = C(Spin(h))$.

Case 1: Assume that D does not split over L. Let $V = V_K$ be the left vector space over D_K on which h is defined. Take an isotropic vector $v \in V_L$. Write $v = v_1 + \theta v_2$ where $v_1, v_2 \in V$. Let $W :=< v_1, v_2 >$ be the subspace in V generated by v_1, v_2 and h_1 be the restriction of h to W. The subspace W has to be two dimensional, because otherwise there is a scalar $\lambda \in D$ such that $v_1 = \lambda v_2$ and we get $v = v_1 + \theta v_2 = (\lambda + \theta) v_2$, hence $h(v_2) = 0$, and h becomes isotropic over K as well.

The skew-hermitian form $h_{1,L}$ is hyperbolic, because it is two-dimensional and $v \in W$. By taking an orthogonal complement of W in V, we can write $h_K = h_{1,K} \perp h_{2,K}$. We can assume that $h_{1,L}(x_1, x_2) = x_1 {x_2}^{\sigma}$. The special orthogonal group of h_1 contains (but it is not equal to) all two by two diagonal matrices with determinant 1. So the one dimensional torus $T = \{diag(t, t^{-1}) \mid t \in K^*\}$ is contained in $SO(h_1)$. Now the argument in the proof of Lemma 6.2.4 can be repeated here: the norm principle for $Spin(h_2)$ implies the norm principle for $Spin(h)$. Let m be the isotropy index of h over L. By repeating this process m times, we will finally reduce to the case that the skew-hermitian form h is anisotropic over L, in which case the norm principle holds by assumption.

Case 2: Now assume that D splits over L, i.e., $D_L \cong M_2(L)$. By Theorem 6.2.6, there is a diagonalization $h =< d_1, \ldots, d_n >$ over K such that $K(d_1) \cong L$ and $O^+(< d_1 >)(L) = {R_{L/K}}^{(1)}(\mathbf{G}_m)$. Let $h_1 =< d_1 >$, $h_2 =< d_2, \ldots, d_n >$, and $T = O^+(h_1)$. The image of T in

$PGO^{+}(h)$ will be denoted by $\overline{T}$, and the connected component of its pre-image in $Spin(h)$ will be denoted by $\widetilde{T}$. The centralizer of T in $O^{+}(h)$ is the direct product $O^{+}(h_1)\cdot O^{+}(h_2)$. So there are groups H and $\overline{H}$ such that they fit into the following diagram whose vertical arrows are inclusions:

$$\begin{array}{ccccccc} & & & & C_{O^{+}(h)}(T) & \longrightarrow & C_{PGO^{+}(h)}(\overline{T}) \\ & & & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle id} \\ & & H & \longrightarrow & O^{+}(h_1)\cdot O^{+}(h_2) & \longrightarrow & \overline{H} \\ & & \downarrow & & \downarrow & & \downarrow \\ Z & \longrightarrow & Spin(h) & \longrightarrow & O^{+}(h) & \longrightarrow & PGO^{+}(h) \end{array}$$

The group H is in fact an almost direct product of $\widetilde{T}$ and $Spin(h_2)$.

By the same argument as in the proof of Lemma 6.2.4, Z is a subgroup of H and all we need to prove is the H^1-variant of the norm principle for the pair (Z,H).

Consider the product map $p:\widetilde{T}\times Spin(h_2)\longrightarrow H$ and let Z_1 be the pre-image of Z under this map. So we have the following diagram whose rows are exact:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Z_1 & \longrightarrow & \widetilde{T}\times Spin(h_2) & \longrightarrow & \widetilde{T}\times Spin(h_2)/\,Z_1 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle i} & & \\ 1 & \longrightarrow & Z & \longrightarrow & H & \longrightarrow & \overline{H} & \longrightarrow & 1 \end{array}$$

The map i is an isomorphism, because of the surjectivity of p. By a simple diagram chasing (same as the proof of Lemma 4.4.3), we can reduce the norm principle of the pair (Z,H) to the pair $(Z_1,\widetilde{T}\times Spin(h_2))$. The argument in the proof of Lemma 4.4.3 carries over here, by replacing the map $\phi:\widetilde{H}\longrightarrow H$ in Lemma 4.4.3 by $p:\widetilde{T}\times Spin(h_2)\longrightarrow H$.

Let $\pi:\widetilde{T}\times Spin(h_2)\longrightarrow\widetilde{T}$ be the projection map to the first component, and $j:Z_1\longrightarrow\widetilde{T}\times Spin(h_2)$ be the inclusion map. Put $Z_2:=\mathrm{Im}(\pi\circ j)$ and $Z_3:=C(Spin(h_2))$. The group Z can then be embedded into $Z_2\times Z_3$, and using Lemma 4.4.1, it will be enough to show the H^1- variant of the norm principle for the pair $(Z_2\times Z_3,\widetilde{T}\times Spin(h_2))$ over L/K. We have $H^1(-,\widetilde{T})=1$ (Hilbert 90), and the following identifications:

$$H^1(L,Z_2\times Z_3)\cong H^1(L,Z_2)\times H^1(L,Z_3),$$

$$H^1(-,\widetilde{T}\times Spin(h_2))\cong H^1(-,\widetilde{T})\times H^1(-,Spin(h_2))\cong H^1(-,Spin(h_2)).$$

For any element (u,v) in the kernel of the map

$$H^1(L,Z_2\times Z_3)\longrightarrow H^1(L,Spin(h_2)),$$

we need to prove $cor_{L/K}(v) \in \mathrm{Ker}(H^1(K, Z_3) \longrightarrow H^1(K, Spin(h_2)))$ (again, because $H^1(-, \widetilde{T})$ is trivial). Therefore the norm principle for $Spin(h_2)$ implies the norm principle for $Spin(h)$. Replacing h by h_2 and repeating this inductive argument several times, the question will finally be reduced to a case that the skew-hermitian form h_2 is anisotropic over L as well, in which case the norm principle holds by assumption. □

Remark 6.2.8. According to our main results in this chapter, we may assume that the extension L/K on which we want to show the norm principle for $Spin(h)$ is quadratic, and h is L- anisotropic.

Chapter 7

Larmour's generalization of Springer's decomposition theorem for skew-hermitian forms

In this section our goal is to state a generalization of quadratic forms Springer's decomposition theorem over complete discretely valued fields for skew-hermitian forms over quaternion division algebras which are defined over complete discretely valued fields. This generalization is proved by Larmour (see [15]; he proved it in more generality though, not only for skew-hermitian forms over quaternion algebras).

7.1 Springer's decomposition theorem for quadratic forms over complete discretely valued fields

Definition 7.1.1. A local ring R with maximal ideal m is called Henselian if Hensel's lemma holds, i.e., if $f(x)$ is any monic polynomial in $R[x]$, then any factorization of its image in $(R/m)[x]$ into a product of coprime monic polynomials can be lifted to a factorization in $R[x]$.

Definition 7.1.2. A discrete valuation ν on a field E is said to be Henselian if it extends uniquely to every finite field extension of E.

Proposition 7.1.3. A valuation ν on E is Henselian if and only if its valuation ring $\mathcal{O}_E$ is Henselian.

Proof. See [7, Theorem 4.1.3]. □

Remark 7.1.4. If a discrete valuation on a local ring A is complete, then A is Henselian.

Now we move towards stating Springer's decomposition theorem for quadratic forms over complete discretely valued fields: let K be a complete discretely valued field with uniformizer π and residue field k with *char* $k \neq 2$. Let $\mathcal{O}$ be the ring of integers of K and m be its maximal ideal.

If a quadratic form over K has a diagonalization with unit elements in $\mathcal{O}$, then we call it a unit quadratic form (or unramified quadratic form). To any unit quadratic form

$q =< u_1, u_2, \ldots, u_n >$ over K, one can associate the quadratic form $< \bar{u_1}, \bar{u_2}, \ldots, \bar{u_n} >$ over k, which we denote by $\bar{q}$.

Any quadratic form q over K can be diagonalized by elements in $\mathcal{O}$ and each diagonal entry can assumed to be of the form u or $u\pi$, where u is a unit (because any element of K is in one of those forms up to squares). Therefore q can be written as $q_0 \perp \pi q_1$, where q_0 and q_1 are unit quadratic forms. The quadratic forms q_0 and q_1 are determined uniquely up to isometry if q is K- anisotropic (see [14, Chapter 6, Section 1]). The quadratic forms $\bar{q_0}$ and $\bar{q_1}$ are called the first and second residue forms of q, respectively.

Theorem 7.1.5. (Springer's theorem) Let K be a complete discretely valued field with uniformizer π and residue field k with $char\ k \neq 2$. Then we have a group isomorphism

$$\begin{aligned} \partial = (\partial_0, \partial_1) : W(K) &\longrightarrow W(k) \oplus W(k) \\ [q] &\mapsto ([\bar{q_0}], [\bar{q_1}]) \end{aligned}$$

where the quadratic forms q_0 and q_1 are the first and second residue forms of q, respectively (defined above).

Remark 7.1.6. In Springer's theorem, ∂_1 depends on the choice of π, but ∂_0 does not.

7.2 Extension of the valuations to division algebras

Let K be a Henselian valued field, and D be a division algebra of degree n over K with involution τ of the first kind.

Let us denote the valuation on K by ν_K:

$$\nu_K : K \backslash \{0\} \longrightarrow \mathbb{Z}.$$

By [23], the valuation on K extends uniquely to the following valuation on D:

$$\nu_D : D \backslash \{0\} \longrightarrow \mathbb{Q}$$

$$x \mapsto \frac{1}{n}\ \nu_K(Nrd(x)).$$

Let $\mathcal{O}_D := \{d \in D | \nu_D(d) \geq 0\}$ be the ring of integers of D, $m_D := \{d \in D | \nu_D(d) > 0\}$ its maximal ideal, $\bar{D} := \mathcal{O}_D/m_D$ the residue division ring, and Γ_D the image of ν_D. We will denote by $\bar{*}$ the image of $* \in \mathcal{O}_D$ in $\bar{D}$.

The inclusion $\mathcal{O} \hookrightarrow \mathcal{O}_D$ induces an embedding $k = \mathcal{O}/m \hookrightarrow \bar{D} = \mathcal{O}_D/m_D$, and elements in the image of k under this embedding commute with all elements of $\bar{D}$, because K is the center of D. Therefore, $\bar{D}$ is a $k-$algebra.

Lemma 7.2.1. The map

$$\bar{\tau} : \bar{D} \longrightarrow \bar{D}$$
$$x + m_D \mapsto \tau(x) + m_D$$

is an involution induced on $\bar{D}$.

Proof. The map $Nrd : D \longrightarrow K$ is invariant under the involution τ (see [13, Page 14, Corollary 2.2]). So

$$\begin{aligned} \forall x \in \mathcal{O}_D,\ \nu_D(\tau(x)) &= \frac{1}{n}\nu_K(Nrd(\tau(x))) \\ &= \frac{1}{n}\nu_K(Nrd(x)) \\ &= \nu_D(x). \end{aligned}$$

Therefore τ maps $\mathcal{O}_D$ to $\mathcal{O}_D$ and m_D to m_D, and the map $\bar{\tau}$ is well-defined. Now we prove that $\bar{\tau}$ is in fact an involution on $\bar{D}$:

$$\begin{aligned} \forall x, y \in \mathcal{O}_D,\ \bar{\tau}(x + y + m_D) &= \tau(x + y) + m_D \\ &= (\tau(x) + m_D) + (\tau(y) + m_D) \\ &= \bar{\tau}(x + m_D) + \bar{\tau}(y + m_D) \end{aligned}$$

$$\begin{aligned} \forall x, y \in \mathcal{O}_D,\ \bar{\tau}(xy + m_D) &= \tau(xy) + m_D \\ &= \tau(y)\tau(x) + m_D \\ &= (\tau(y) + m_D)(\tau(x) + m_D) \\ &= (\bar{\tau}(y + m_D))(\bar{\tau}(x + m_D)) \end{aligned}$$

$$\begin{aligned} \forall x \in \mathcal{O}_D,\ \bar{\tau}(\bar{\tau}(x + m_D)) &= \bar{\tau}(\tau(x) + m_D) \\ &= \tau(\tau(x)) + m_D \\ &= x + m_D \end{aligned}$$

□

Any skew-hermitian form over (D, τ) has a diagonalization by skew-symmetric elements. If a skew-hermitian form over (D, τ) has a diagonalization with unit elements, then we call it a unit skew-hermitian form or unramified skew-hermitian form, in a similar manner to unit quadratic forms. To any unit skew-hermitian form $h = < u_1, u_2, \ldots, u_n >$ over (D, τ), one can associate the skew-hermitian form $< \bar{u_1}, \bar{u_2}, \ldots, \bar{u_n} >$ over $(\bar{D}, \bar{\tau})$, which we denote by $\bar{h}$. This argument works for hermitian forms as well.

Our case of interest in studying norm principle for type D_n groups is the spinor groups of skew-hermitian forms over quaternion algebras. From now on, we will assume that K is a complete discretely valued field with residue field k with *char* $K \neq 2$ and *char* $k \neq 2$, and D is a quaternion division algebra over K with symplectic involution τ. We will use the similar notations ν_K, $\mathcal{O}$, m, and π as before.

We know that the valuation ν_K can be extended uniquely to any intermediate field $K \subseteq F \subseteq D$. It also extends uniquely to the following valuation over D:

$$\nu_D : D \backslash \{0\} \longrightarrow \mathbb{Q}$$

$$x \mapsto \frac{1}{2}\, \nu_K(Nrd(x)).$$

The notations $\mathcal{O}_D$, m_D, $\bar{D}$, and Γ_D will be used as before.

Let x, y be two elements in D such that $x^2 = a$, $y^2 = b$, $D = (\frac{a,b}{K})$. Also put $z := xy = -yx$. The set $\{1, x, y, z\}$ is a $K-$basis of D. The involution τ induces an involution $\bar{\tau}$ on $\bar{D}$ (see Lemma 7.2.1).

We have two cases of ramification for D: it is either unramified (i.e., a and b are units), or ramified (i.e., a is a unit and b is a non-unit). The case where D is generated by two non-units a and b can be reduced to the ramified case, since $(\frac{a,b}{K}) \cong (\frac{a,-ab}{K})$ and if a and b are non-units, then ab will be unit up to squares; the norm forms associated to $(\frac{a,b}{K})$ and $\cong (\frac{a,-ab}{K})$ are both isometric to the form $< 1, -a, -b, ab >$, and the isometry of the norm forms implies the isomorphism of the quaternion algebras.

7.3 Larmour's theorem

Let h be a skew-hermitian form over (D, τ). We want to show h over (D, τ) can be decomposed as

$$h = h_0 \perp h_1,$$

where h_0 is a unit skew-hermitian form, and any element s in a diagonalization of h_1 satisfies $\nu_D(s) = \min\{\nu_D(t) \mid t \in D\} \cap \mathbb{Q}^+$. This value depends on the ramification of the quaternion algebra. We will see that if h is $K-$anisotropic, then this decomposition is unique up to isometry classes of h_0 and h_1.

Now we discuss the two cases of ramification of D below:

Case 1: D is unramified: $D = (\frac{a,b}{K})$ where both a and b are units.

The assumption implies that π is still a uniformizer for ν_D (unless otherwise stated, when we refer to the uniformizer of ν_D, we mean π). We have $\Gamma_D = \mathbb{Z}$ and $\nu_D(x) = \nu_D(y) = \nu_D(z) = 0$. Then h can obviously be written as $h = h_0 \perp h_1$, where h_0 is a unit skew-hermitian form and in the diagonalization of h_1 each element has value 1, because multiplying any element in the diagonalization of h by π^2 does not change the isometry class of h.

By [22, Page 21], $\bar{D}$ is isomorphic to $(\frac{\bar{a},\bar{b}}{k})$, which is a division quaternion algebra (the norm form of D is anisotropic and by Hensel's lemma, the norm form of $\bar{D}$ is anisotropic too). Then the involution $\bar{\tau}$ is the following:

$$\bar{\tau} : (\frac{\bar{a},\bar{b}}{k}) \to (\frac{\bar{a},\bar{b}}{k})$$
$$p + q\bar{x} + r\bar{y} + s\bar{z} \mapsto p - q\bar{x} - r\bar{y} - s\bar{z},$$

for $p, q, r, s \in k$.

Case 2: D is ramified: $D = (\frac{a,\pi}{K})$ where a is a unit. In fact if $D = (\frac{a,b}{K})$ with $\nu_K(a) = 0$ and $\nu_K(b) = 1$, then we can choose b to be the uniformizer of K, and hence without loss of generality assume that $b = \pi$.

In this case $y = \sqrt{\pi}$ is a uniformizer for ν_D (similar to case 1, unless otherwise stated, when we refer to the uniformizer of ν_D, we mean $y = \sqrt{\pi}$). We have $\Gamma_D = \{\frac{l}{2} | l \in \mathbb{Z}\}$, $\nu_D(x) = 0$, $\nu_D(y) = \nu_D(z) = \frac{1}{2}$.

In case 2, by [22, Page 22]), $\bar{D}$ is isomorphic to $k(\bar{x})$, which is a quadratic field extension of k. Note that in general, $k(\bar{x})$ is a quadratic étale extension of k, but in our case we know that $\bar{x}$ is not a square in k since otherwise by Hensel's lemma x will be a square in K which contradicts the fact that D is a division quaternion algebra. Therefore, $k(\bar{x})$ is a quadratic field extension of k.

The involution $\bar{\tau}$ will just be the nontrivial $k-$automorphism of $k(\bar{x})$, which is an involution of the second kind:

$$\bar{\tau} : k(\bar{x}) \to k(\bar{x})$$
$$p + q\bar{x} \mapsto p - q\bar{x},$$

for $p, q \in k$.

We want to show that h can be written as $h = h_0 \perp h_1$, where h_0 is a unit skew-hermitian form and in the digonalization of h_1 each element has value $\frac{1}{2}$ (up to squares). To verify this claim, it is just enough to show that replacing any skew-symmetric element α in the diagonalization of h by $-\pi^{-2}y\alpha y$ does not change the isometry class of h. This is proved in the next lemma.

Lemma 7.3.1. Let $\alpha \in D$ be a skew-symmetric element. Then $< \alpha > \cong < -\pi^{-2} y\alpha y >$.

Proof.

$$\begin{aligned} < \alpha > &\cong < \tau(\pi^{-1}y)\alpha(\pi^{-1}y) > \\ &\cong < (-\pi^{-1}y)\alpha(\pi^{-1}y) > \\ &\cong < -\pi^{-2}y\alpha y > . \end{aligned}$$

□

Note that

$$\nu_D(-\pi^{-2}y\alpha y) = -2 + 2\nu_D(y) + \nu_D(\alpha) = \nu_D(\alpha) - 1,$$

so replacing α by $-\pi^{-2}y\alpha y$ reduces the value of α by 1. Therefore we have the desired decomposition $h = h_0 \perp h_1$, where h_0 is a unit skew-hermitian form and in the digonalization of h_1 each element has value $\frac{1}{2}$.

In both cases, we get a similar decomposition as Springer's decomposition for quadratic forms:

$$h = h_0 \perp h_1. \tag{7.1}$$

Whenever we write $h = h_0 \perp h_1$, this is what we mean, and we will call this the **Larmour decomposition of** h. So the elements in the diagonalization of h_0 are units, and in h_1 they are non-units. This notation will be used in both unramified and ramified cases.

We seek a more concrete understanding of how the diagonal entries in h_0 and h_1 look like, for which we need the following facts:

Lemma 7.3.2. Let σ be an involution of any kind on D, and u, v be σ-symmetric or $\sigma-$skew symmetric units such that $\overline{u} = \overline{\tau}(\theta)\overline{v}\theta$ for some $\theta \in \overline{D}$. Then there is $t \in D$ with $\overline{t} = \theta$ and $u = \tau(t)vt$.

Proof. See [15, Lemma 2.2]. □

Lemma 7.3.3. With all assumptions on D as before (case 2), if $\theta_1, \theta_2 \in K$, then $\nu_D(\theta_1 + \theta_2 x) \in \mathbb{Z}$.

Proof. The proof in the case that one of the elements θ_1 and θ_2 is zero is trivial. So we can assume that they are both nonzero.

Assume the contrary: there exists $m \in \mathbb{Z}$ such that $\nu_D(\theta_1 + \theta_2 x) = \frac{2m+1}{2}$. So $\nu_K(Nrd(\theta_1 + \theta_2 x)) = 2m + 1$, hence there exists $l \in \mathcal{O}_K{}^*$ such that ${\theta_1}^2 - {\theta_2}^2 a = \pi^{2m+1} l$. Therefore, the binary quadratic form $< \overline{1}, -\bar{a} >$ is $k-$isotropic. By Springer's decomposition theorem (Theorem 7.1.5), the binary quadratic form $< 1, -a >$ is $K-$isotropic. But then the norm form $< 1, -a, -\pi, a\pi >$ will be K−isotropic, which implies that the quaternion algebra $(\frac{a,\pi}{K})$ is split, contradicting the assumption that it is a division algebra.

Alternative proof: The extension $K(x)/K$ is unramified, so the value group of $K(x)$ is same as the value group of K, which is $\mathbb{Z}$. □

Lemma 7.3.4. Let $h = h_0 \perp h_1$ be a skew-hermitian form over (D, τ) as before (over a ramified D, case 2).

(1) The skew-hermitian form h_0 is isometric over D to a unit skew-hermitian form whose diagonal entries are of the form αx where $\alpha \in \mathcal{O}_K{}^*$.

(2) The skew-hermitian form h_1 is isometric over D to a skew-hermitian form whose diagonal entries are of the form $\beta y + \gamma z$ where $\beta, \gamma \in \mathcal{O}_K$, such that at least one of β and γ is unit and $\nu_D(\beta y + \gamma z) = \frac{1}{2}$.

Proof. It is enough to show these two parts for one-dimensional skew-hermitian forms. Let u be a diagonal entry of $h := h_0 \perp h_1$. Therefore u is a skew-symmetric element $u = \alpha x + \beta y + \gamma z$, for some $\alpha, \beta, \gamma \in K$. Now we give a proof for each part.

(1) u is an element in the diagonalization of h_0:

We have $\nu_D(u) = 0$. If $\beta = \gamma = 0$, then we have the desired result. So we can assume that at least one of the elements β and γ is nonzero. Then

$$\nu_D(\beta y + \gamma z) = \nu_D(\beta + \gamma x) + \nu_D(y) = \nu_D(\beta + \gamma x) + \frac{1}{2}$$

is a non-integer by Lemma 7.3.3. Since $\nu_D(\alpha x)$ is an integer, we get $0 = \nu_D(u) = min\{\nu_D(\alpha x), \nu_D(\beta y + \gamma z)\}$ which forces $\nu(\alpha x) = 0$, and hence $\alpha \in \mathcal{O}_K{}^*$. This implies that $\beta y + \gamma z \in \mathcal{O}_D$, because its value cannot be negative (otherwise $\nu_D(u)$ would not be an integer). In fact we have $\beta y + \gamma z \in m_D$, because $\nu_D(\beta y + \gamma z)$ cannot be zero. This observation shows that $\overline{u} = \overline{\alpha x}$. Now by applying Lemma 7.3.2 to $\sigma = \tau$, $u = \alpha x + \beta y + \gamma z$, $v = \alpha x$ and $\theta = \overline{1}$, we get an element $t \in D$ such that $u = \tau(t)\alpha x t$, which implies that $< u > \cong < \alpha x >$.

(2) u is an element in the diagonalization of h_1:

So $\nu_D(u) = \frac{1}{2}$. If $\alpha = 0$ then we already have $u = \beta y + \gamma z$ (we will show later that β and γ satisfy the desired conditions). So we may assume that $\alpha \neq 0$. Also note that the elements β and γ cannot be zero simultaneously.

Since $\nu_D(\alpha x) \in \mathbb{Z}$ and $\frac{1}{2} = \nu_D(\alpha x + \beta y + \gamma z)$, we have

$$\nu_D(\alpha x) > \frac{1}{2} \qquad \textit{and} \qquad \nu_D(\beta y + \gamma z) = \frac{1}{2},$$

which forces $\alpha \in m$ and $\nu_D(\alpha x) \geq 1$. The element $(\beta y + \gamma z)y^{-1} = \beta + \gamma x$ will then be a unit. Consider the orthogonal involution $\tau_y : s \mapsto y^{-1}\tau(s)y$ on D. The element uy^{-1} is a τ_y-symmetric element because

$$\begin{aligned}\tau_y(uy^{-1}) = y^{-1}\tau(uy^{-1})y = (-\tau(y))^{-1}\tau(uy^{-1})(-\tau(y)) = \tau(y^{-1})\tau(uy^{-1})\tau(y)\\ = \tau(uy^{-2})\tau(y) = \frac{1}{\pi}uy = uy^{-1}.\end{aligned}$$

Furthermore, $uy^{-1} = -\alpha z + \beta + \gamma x$ is a unit. The fact that $\alpha \in m$ implies that $\overline{-\alpha z + \beta + \gamma x} = \overline{\beta + \gamma x}$, so by applying Lemma 7.3.2 to $\sigma = \tau_y$, $u = -\alpha z + \beta + \gamma x$, $v = \beta + \gamma x$ and $\theta = \overline{1}$, we get an element $t \in D$ such that $-\alpha z + \beta + \gamma x = \tau_y(t)(\beta + \gamma x)t$. Hence

$$\begin{aligned}u &= (-\alpha z + \beta + \gamma x)y\\ &= y^{-1}\tau(t)y(\beta + \gamma x)ty\\ &= y^{-1}\tau(t)y(\beta + \gamma x)yy^{-1}ty\\ &= y^{-1}\tau(t)y(\beta y + \gamma z)y^{-1}ty\\ &= \tau(y^{-1}ty)(\beta y + \gamma z)(y^{-1}ty),\end{aligned}$$

which gives the isometry $< \alpha x + \beta y + \gamma z > \cong < \beta y + \gamma z >$.

We still need to show that $\beta, \gamma \in \mathcal{O}_K$. Note that if one of the elements β or γ is 0, then we are done. So assume that they are both nonzero. Consider the following cases:

(i) $\nu_K(\beta) \neq \nu_K(\gamma)$:

We have $\frac{1}{2} = \nu_D(\beta y + \gamma z) = min\{\nu_K(\beta), \nu_K(\gamma)\} + \frac{1}{2}$. Hence both $\nu_K(\beta)$ and $\nu_K(\gamma)$ are nonnegative and at least one of them is 0, as desired.

(ii) $\nu_K(\beta) = \nu_K(\gamma) \geq 0$:

In this case

$$\frac{1}{2} = \nu_D(\beta y + \gamma z) \geq min\{\nu_D(\beta y), \nu_D(\gamma z)\},$$

therefore β and γ cannot be nonunits simultaneously.

(iii) $\nu_K(\beta) = \nu_K(\gamma) = -q < 0$ for $q \in \mathbb{N}$:

We have $\nu_D(\beta y + \gamma z) = \frac{1}{2}$, therefore $\nu_D(\beta + \gamma x) = 0$ which means the element $\beta^2 - \gamma^2 a$ will be a unit in K. The vector $(\overline{\pi^q \beta}, \overline{\pi^q \gamma})$ (which has nonzero coordinates) is a k-isotropic vector for the quadratic form $< \overline{1}, -\bar{a} >$. By Springer's decomposition theorem for quadratic forms over complete discretely valued fields, $< 1, -a >$ will be a $K-$isotropic quadratic form, which implies that the quadratic form $< 1, -a, -\pi, a\pi >$ is $K-$isotropic. This is a contradiction since $D = (\frac{a,\pi}{K})$ is a division algebra. Therefore, this case cannot occur at all. □

Remark 7.3.5. Let h be a skew-hermitian form over (D, τ), where D is ramified, and $h = h_0 \perp h_1$ be Larmour decomposition of h. The proof of Lemma 7.3.4 shows that if $u = \alpha x + \beta y + \gamma z$ is an element in the diagonalization of h_0, then replacing u with αx will not change the isometry class of h_0 (and therefore h). Similarly, if $u = \alpha x + \beta y + \gamma z$ is an element in the diagonalization of h_1, then replacing u with $\beta y + \gamma z$ will not change the isometry class of h_1 (and therefore h).

The next theorem states that Larmour decomposition (7.1) is unique up to isometry for anisotropic skew-hermitian forms.

Theorem 7.3.6. (Larmour's theorem) The skew-hermitian form $h = h_0 \perp h_1$ is $K-$anisotropic, if and only if h_0 and h_1 are $K-$ anisotropic. Furthermore, if h is $K-$anisotropic, then the decomposition $h = h_0 \perp h_1$ is unique up to isometry classes of h_0 and h_1.

Proof. See [15, Theorem 3.3 and Theorem 3.6]. Note that this fact is true regardless of the ramification of D. □

Chapter 8

Notations and lemmata

In this chapter we set up the notations and prove some reductions and lemmas which will be used in the proof of the main theorem, stated below:

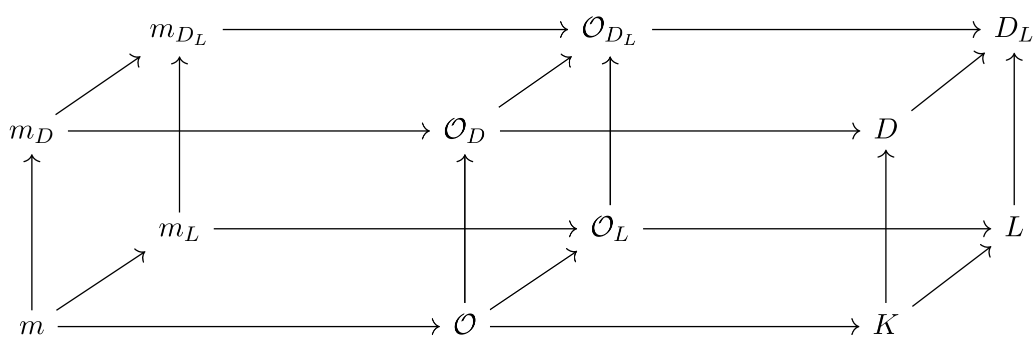
Theorem 8.0.1. Let K be a complete discretely valued field with residue field k and $char\ k \neq 2$. Assume that the norm principle holds for $Spin(h_1)$ for every regular skew-hermitian form h_1 over any quaternion algebra D_1 defined over any finite extension of k (with respect to the canonical involution). Then the norm principle holds for $Spin(h)$ for every regular skew-hermitian form h over any quaternion algebra D with respect to the canonical involution over K.

8.1 Notations

Now, we set up the notations which will be used in the proof of Theorem 8.0.1:

- K: a complete discretely valued field with $char\ K \neq 2$.
- ν: the valuation on K.
- π: a uniformizer for K.
- $\mathcal{O}$: the ring of integers of K.
- m: the maximal ideal of $\mathcal{O}$.
- k: the residue field of K, with $char\ k \neq 2$.
- Whenever we say that an object is ramified, we mean it is totally ramified (for field extensions, quaternion algebras, elements in the fields and algebras, and skew-hermitian forms).
- L/K: a quadratic field extension. The reduction of the main theorem to quadratic field extensions was proved in Section 6.1.
- $\sqrt{t}$: a generator of L over K; since $char\ K \neq 2$, we may assume that $L = K(\sqrt{t})$, where $t \in K^* \backslash K^{*2}$. If L/K is an unramified extension, then t is a unit of K. If L/K is ramified, then $t = c\pi$ for a unit $c \in \mathcal{O}^*$.
- $\overline{*}$ for $* \in \mathcal{O}$: the image of $*$ in k.
- l: residue field of L. If L/K is unramified, then $l = k(\sqrt{\bar{t}})$. If L/K is ramified then $l = k$.

- π': a uniformizer of L. If L/K is unramified, then $\pi' = \pi$. If L/K is ramified then $\pi' = \sqrt{c\pi}$ for a unit $c \in \mathcal{O}^*$ (recall that we assumed that $t = \sqrt{c\pi}$ is the generator of L/K).
- D: division quaternion algebra over K. So $D = (\frac{a,b}{K})$ where a and b are units in K, or $D = (\frac{a,\pi}{K})$ where a is a unit in K. We call D unramified in the first case, and ramified in the second one. Note that a ramified quaternion division algebra is of the form $D = (\frac{a,a'\pi}{K})$ where a, a' are units in K. Without loss of generality, by replacing $a'\pi$ with π if necessary, we may assume that $a' = 1$.
- ν_L, ν_D, ν_{D_L} respectively denote the extensions of ν to L, D, and D_L. The extension to D_L exists only if D_L is an L-division algebra.
- $1, x, y, z$: the basis for D over K such that if D is unramified then $x^2 = a$, $y^2 = b$, $z = xy = -yx$, and if D is ramified, then $x^2 = a$, $y^2 = \pi$, $z = xy = -yx$.
- $\mathcal{O}_L$, $\mathcal{O}_D$, $\mathcal{O}_{D_L}$ respectively denote the ring of integers of L, D, and D_L. Note that $\mathcal{O}_{D_L}$ is only defined if D_L is an L-division algebra.
- m_L, m_D, m_{D_L} respectively denote the maximal ideals of L, D, and D_L. Note that m_{D_L} is only defined if D_L is an L-division algebra.
- $\overline{D} := D/m_D$: the residue k-algebra.
- $\overline{\tau}$: the induced canonical involution on $\overline{D}$ (see Lemma 7.2.1).
- $\overline{D}_l := D_L/m_{D_L}$: the residue l-algebra. Note that $\overline{D}_l$ is only defined if D_L is an L-division algebra. If D_L is unramified over L, then $\overline{D}_l = (\frac{\overline{a},\overline{b}}{l})$ will be a division quaternion l-algebra. If D_L is ramified over L, then $\overline{D}_l = l(\sqrt{\overline{a}})$ is a quadratic field extension of l (see Section 7.3).
- $\overline{*}$ for $* \in \mathcal{O}_L$, $\mathcal{O}_D$, or $\mathcal{O}_{D_L}$: the image of $*$ in l, $\overline{D}$, or $\overline{D}_l$, respectively. Note that the image in $\overline{D}_l$ is only defined if D_L is an L-division algebra.
- The following diagram contains all the fields, maximal ideals, rings of integers, and the algebras. All the maps are inclusions:

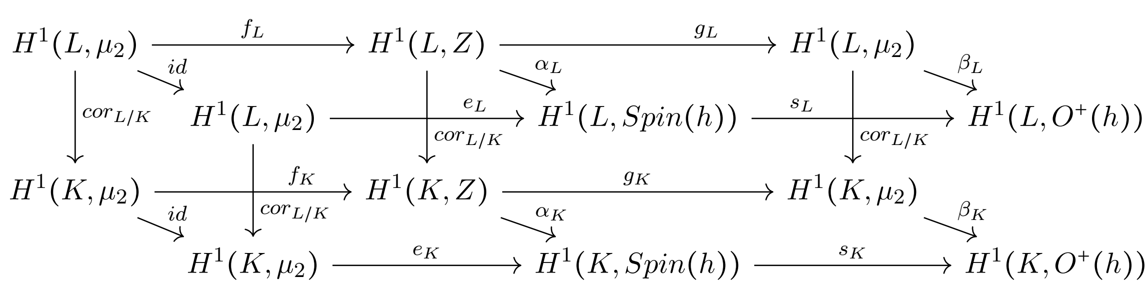


- h: a skew-hermitian form over (D, τ), where τ is the canonical involution on D. We assume that h is anisotropic over L (hence anisotropic over K too). The reduction of the main question to anisotropic skew-hermitian forms was proved in Section 6.2.
- $n = dim\ h$.
- $\overline{h}$: the residue form of an unramified form h defined over the residue algebra with canonical involution $(\overline{D}_l, \overline{\tau})$ (see Chapter 7).
- σ_h: the involution adjoint to h on the matrix algebra $M_n(D)$.
- $O^+(h) := O^+(M_n(D), \sigma_h)$, the special orthogonal group of h.
- $Spin(h) := Spin(M_n(D), \sigma_h)$, the Spinor group of h.
- $PGO^+(h) := PGO^+(M_n(D), \sigma_h)$, the projective general orthogonal group of h.
- $C(G)$: center of any group G.
- $Z = C(Spin(h))$.
- The following diagram relates the groups of type D_n which will be used in our argument. The rows are exact.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_2 & \longrightarrow & Z & \longrightarrow & \mu_2 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mu_2 & \longrightarrow & Spin(h) & \longrightarrow & O^+(h) & \longrightarrow & 1 \end{array}$$

- The above diagram gives rise to the following commutative diagram:

Diagram 8.1.1.



- f, g, e, s, α, β are the Galois cohomology maps in Diagram 8.1.1.
- u: an element in $\mathrm{Ker}(\alpha_L)$ (see Diagram 8.1.1).

- $\lambda \in L^*$ is a representative for $g_L(u)$ (see Diagram 8.1.1). Without loss of generality, we will assume that $\nu_L(\lambda) \in \{0, \nu_L(\pi')\}$. Note that if $\nu_L(\lambda) \neq 0$, then one of the following holds: $\nu_L(\lambda) = 1$ if L/K is unramified, or $\nu_L(\lambda) = \frac{1}{2}$ if L/K is ramified.
- $h = h_0 \perp h_1$: Larmour decomposition of h over K (see Section 7.3). Note that one of h_0 or h_1 could be trivial, i.e., with dimension 0; in that case we will have $h = h_0$ (unramified) or $h = h_1$ (ramified). The base change of the skew-hermitian forms h_0 and h_1 from K to L are denoted by $h_{0,L}$ and $h_{1,L}$, respectively.
- F: the discriminant extension of h over K, i.e.,

$$F := K[t]/(t^2 - (-1)^n Nrd_{D/K}\ (det\ (h))).$$

  This is a quadratic étale extension of K. So F is either a quadratic separable field extension of K, or it is isomorphic to $K \times K$.
- ψ: the nontrivial $K-$ automorphism of F.
- $M := L \underset{K}{\otimes} F$ the discriminant extension of h over L. Therefore, M is an étale quadratic extension of L: it is either a quadratic field extension of L, or isomorphic to $L \times L$.
- ψ_L: the nontrivial $L-$ automorphism of M.
- The following diagram shows the discriminant extensions of h over K and L (all arrows are inclusions):

$$\begin{array}{ccc} L & \longrightarrow & M := L \underset{K}{\otimes} F \\ \uparrow & & \uparrow \\ K & \longrightarrow & F \end{array}$$

- ν_F: the extension of the valuation ν from K to F, in case F is a field.
- ν_M: the extension of the valuation ν_L from L to M, in case M is a field.

  Note: If h is an unramified skew-hermitian form over K and M is a field, then the extension M/L is unramified. Therefore, π' is a uniformizer for M.

Lemma 8.1.2. Recall that $\sqrt{t}$ is a generator of the field extension L/K. Assume that D_L splits. Then $D_K \cong (\frac{t,w}{K})$ for some $w \in K$.

Proof. See [14, Page 67, Theorem 4.1]. □

Recall that to prove Theorem 8.0.1, we need to show that $cor_{L/K}(u) \in Ker(\alpha_K)$ **(see Diagram 8.1.1)**.

We will set up the necessary steps towards the proof of Theorem 8.0.1. We will use explicit formulas for some of the Galois cohomology maps in Diagram 8.1.1.

Explicit formulas for the maps f and g in Diagram 8.1.1:

Recall that when n is even, we have $Z = R_{F/K}(\mu_2)$, and $H^1(K,Z) = F^*/F^{*2}$ (see [19, Page 332]). Also in Diagram 8.1.1, the map $f_K : K^*/K^{*2} \longrightarrow F^*/F^{*2}$ is the natural map and g_K is given by the following (see [13, Section 13]):

$$g_K : F^*/F^{*2} \longrightarrow K^*/K^{*2}$$

$$[p] \mapsto [N_{F/K}(p)]$$

for every $p \in F^*$.

When n is odd, then $Z = \mathrm{Ker}(Norm : R_{F/K}(\mu_4) \longrightarrow \mu_4)$ (see [19, Page 332]), and $H^1(K,Z) = U(K)/U_0(K)$, where $U \subseteq \mathbb{G}_m \times R_{F/K}\mathbb{G}_m$ is the subgroup defined by

$$U(K) := \{(q,p) \in K^* \times F^* \mid q^4 = Norm_{F/K}(p)\}$$

and $U_0 \subseteq U$ is the subgroup defined by

$$U_0(K) := \{(N_{F/K}(p), p^4) \mid p \in F^*\}.$$

Then the maps f and g in Diagram 8.1.1 will be the following (by [13, Section 13]):

$$f_K : K^*/K^{*2} \longrightarrow U(K)/U_0(K)$$

$$[q] \mapsto [q, q^2]$$

and

$$g_K : U(K)/U_0(K) \longrightarrow K^*/K^{*2}$$

$$[q,p] \mapsto [N_{F/K}(p_0)],$$

where $p_0 \in F^*$ is such that $p_0\psi(p_0)^{-1} = q^{-2}p$.

8.2 The discriminant extension

We will need the following facts about the discriminant extension of h in the proof of the main theorem. Recall that F denotes the discriminant extension of h over K.

Lemma 8.2.1. Assume that D is ramified over K, so $D = (\frac{a,\pi}{K})$ where a is a unit and π is a uniformizer of K, and h is unramified with dimension n over K. Then

$$F \cong K \times K \quad \Longleftrightarrow \quad n \quad \textit{is even.}$$

Note that the above fact is equivalent to the following:

$$F \textit{ is a field} \Longleftrightarrow \quad n \quad \textit{is odd.}$$

In the second case, $F = K(\sqrt{a})$.

Proof. By Remark 7.3.5 we can assume that the skew-hermitian form h has a diagonalization $< u_1 x, u_2 x, \ldots, u_n x >$ where $u_i \in {\mathcal{O}_K}^*$.

$$F \cong K \times K \quad \Longleftrightarrow \quad (-1)^{\frac{2n(2n-1)}{2}} Nrd(u_1 u_2 \ldots u_n x^n) \in {K^*}^2 \quad \Longleftrightarrow a^n \in {K^*}^2.$$

If n is odd, then

$$a^n \in {K^*}^2 \quad \Longleftrightarrow \quad a \in {K^*}^2 \quad \Rightarrow \quad D \textit{ is split,}$$

therefore when $F \cong K \times K$, n must be even since we know that D is a division algebra. Conversely, if n is even, then $a^n \in {K^*}^2$ and hence $F \cong K \times K$.

This implies that

$$F \textit{ is a field} \Longleftrightarrow \quad n \quad \textit{is odd.}$$

So when F is a field (and n is automatically odd), we have $F = K(\sqrt{disc\ h}) = K(\sqrt{a})$. □

Remark 8.2.2. Assume that D is unramified over K. Then any element in the diagonalization of the ramified part of h, i.e., h_1, has the form πd, where d is a unit skew element in D_K. Since $Nrd(\pi d) = -\pi^2 d^2$ is a unit in K up to squares, the discriminant of h has to be a unit of K. Therefore, F (the discriminant extension of h over K) is either an unramified quadratic field extension of K, or it is isomorphic to $K \times K$.

8.3 Reduction to unramified and ramified skew-hermitian forms under a specific assumption

Assume that the skew-hermitian form $h_K \cong h_{0,K} \perp h_{1,K}$ satisfies the following, for an element $\lambda \in L^*$:

$$\lambda h_{0,L} \cong h_{0,L} \qquad \lambda h_{1,L} \cong h_{1,L}. \tag{8.1}$$

We allow one of h_0 or h_1 to be trivial.

In this section, we will prove a reduction of the norm principle under the assumption that the isometries [8.1] hold. The following argument is taken from [4].

Let $R = O^+(h_0) \times O^+(h_1)$ be a subgroup of $O^+(h)$, and $\widetilde{R}$ be the preimage of R under the map $Spin(h) \longrightarrow O^+(h)$.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_2 & \longrightarrow & Z & \longrightarrow & \mu_2 & \longrightarrow & 1 \\
 & & \big\downarrow{\scriptstyle id} & & \big\downarrow & & \big\downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \widetilde{R} & \longrightarrow & R & \longrightarrow & 1 \\
 & & \big\downarrow{\scriptstyle id} & & \big\downarrow & & \big\downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & Spin(h) & \longrightarrow & O^+(h) & \longrightarrow & 1
\end{array}$$

The above diagram gives rise to the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & H^1(L,\mu_2) & \xrightarrow{f_L} & H^1(L,Z) & \xrightarrow{g_L} & H^1(L,\mu_2) & \longrightarrow & 1 \\
 & & \big\downarrow{\scriptstyle id} & & \big\downarrow{\scriptstyle \alpha_{1,L}} & & \big\downarrow{\scriptstyle \beta_{1,L}} & & \\
1 & \longrightarrow & H^1(L,\mu_2) & \xrightarrow{e'_L} & H^1(L,\widetilde{R}) & \xrightarrow{s'_L} & H^1(L,R) & \longrightarrow & 1 \\
 & & \big\downarrow{\scriptstyle id} & & \big\downarrow{\scriptstyle \alpha_{2,L}} & & \big\downarrow{\scriptstyle \beta_{2,L}} & & \\
1 & \longrightarrow & H^1(L,\mu_2) & \xrightarrow{e_L} & H^1(L,Spin(h)) & \xrightarrow{s_L} & H^1(L,O^+(h)) & \longrightarrow & 1
\end{array}$$

So we have $\alpha_L = \alpha_{2,L} \circ \alpha_{1,L}$, and $\beta_L = \beta_{2,L} \circ \beta_{1,L}$ (see also Diagram 8.1.1).

Lemma 8.3.1. Assume that:

- the H^1- variant of the norm principle holds for the pair $(Z, \widetilde{R})$, and

- isometries [8.1] hold.

Then $cor_{L/K}(u) \in \mathrm{Ker}(\alpha_K)$.

Proof. The proof involves chasing elements in the diagram above. Let $v = \alpha_{1,L}(u)$. We have $\lambda h_{0,L} \cong h_{0,L}$ and $\lambda h_{1,L} \cong h_{1,L}$, therefore, $\beta_{1,L}([\lambda]) = 1$. This shows that $v \in \mathrm{Im}(e'_L)$, so there exists $a \in L$ such that $e'_L([a]) = v$.

The element $b = f_L([a])^{-1} u \in H^1(L,Z)$ is in the kernel of the map $\alpha_{1,L}$ (by Lemma 6.2.2), and therefore it is in the kernel of the map α_L. But u is also in the kernel of α_L, hence $f_L([a])^{-1} \in \mathrm{Ker}(\alpha_L)$, i.e., a is a spinor norm for h. By Knebusch's norm principle we have $cor_{L/K}(f_L([a])^{-1}) \in \mathrm{Ker}(\alpha_K)$.

By our assumption, the norm principle holds for the pair $(Z, \widetilde{R})$, therefore $cor_{L/K}(b) \in \mathrm{Ker}(\alpha_{1,K}) \subseteq \mathrm{Ker}(\alpha_K)$. Again, by Lemma 6.2.2, $cor_{L/K}(u) \in \mathrm{Ker}(\alpha_K)$. □

Remark 8.3.2. Lemma 8.3.1 shows that to prove Theorem 8.0.1, it will be enough to show the norm principle for the spinor groups of h_0 and h_1 under the following additional hypotheses:

- isometries [8.1] hold,
- the skew-hermitian form h has a nontrivial decomposition $h = h_0 \perp h_1$ (i.e., $dim\ h_0 \neq 0$, $dim\ h_1 \neq 0$).

Therefore, we have reduced the norm principle to the following two cases:

- unramified skew-hermitian forms (i.e., $h_K \cong h_{0,K}$), and
- ramified (i.e., totally ramified) skew-hermitian forms (i.e., $h_K \cong h_{1,K}$).

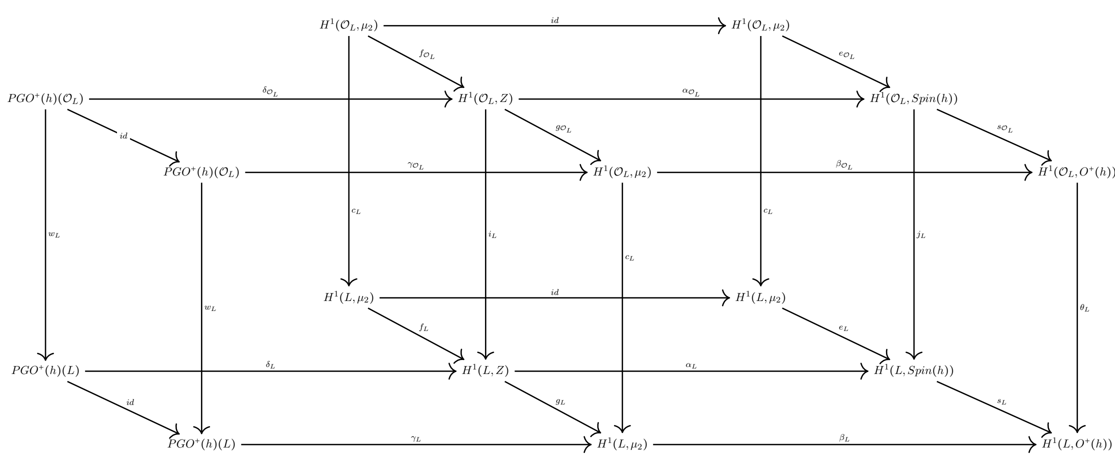
Remark 8.3.3. Note that if D is unramified over K, then since

$$Spin(h_{1,K}) = Spin(\frac{1}{\pi}h_{1,K}),$$

by Remark 8.3.2 we can assume that h is unramified (the skew-hermitian form $\frac{1}{\pi}h_{1,K}$ is unramified).

8.4 A reduction when h and D are unramified over L

Throughout this section we assume that h and D are unramified over L and will prove a reduction of the main theorem under this assumption. In this case, we may assume that the group $Spin(h)$ and its center Z are actually defined over $\mathcal{O}_L$ and by base change we obtain $Spin(h)$ and Z over L. Consider the following commutative exact diagram, induced by the base change $\mathcal{O}_L \longrightarrow L$:



In the above diagram, the maps c_L, i_L, and w_L are injective group homomorphisms, and the maps j_L and θ_L have trivial kernels by [17].

We need the following two lemmas in case h and D are unramified over L:

Lemma 8.4.1. If h and D are unramified over L, we can write the element u as a product $u = i_L(u_1)f_L(u_2)$, for some $u_1 \in H^1(\mathcal{O}_L, Z)$, $u_2 \in H^1(L, \mu_2)$, such that

$g_L(i_L(u_1)) = [\lambda]$,

$i_L(u_1) \in \mathrm{Ker}(\alpha_L)$,

$e_L(u_2) = 1$, and

$\alpha_{\mathcal{O}_L}(u_1) = 1$.

Proof. Consider the element $\lambda {\mathcal{O}_L}^{*2} \in H^1(\mathcal{O}_L, \mu_2)$. Then

$$\begin{aligned} \theta_L(\beta_{\mathcal{O}_L}(\lambda {\mathcal{O}_L}^{*2})) &= \beta_L(c_L(\lambda {\mathcal{O}_L}^{*2})) \\ &= \beta_L(\lambda L^{*2}) \\ &= \beta_L(g_L(u)) \\ &= s_L(\alpha_L(u)) \\ &= 1. \end{aligned}$$

By [17], $\mathrm{Ker}(\theta_L)$ is trivial. So we have $\beta_{\mathcal{O}_L}(\lambda {\mathcal{O}_L}^{*2}) = 1$, hence $\lambda {\mathcal{O}_L}^{*2} \in \mathrm{Im}(\gamma_{\mathcal{O}_L})$, and there exists an $\mathcal{O}_L$ point s in $PGO^{+}(h'')(\mathcal{O}_L)$ such that $\gamma_{\mathcal{O}_L}(s) = \lambda {\mathcal{O}_L}^{*2}$. Let $u_1 := \delta_{\mathcal{O}_L}(s) \in H^1(\mathcal{O}_L, Z)$. Then

$$\begin{aligned} g_L(i_L(u_1)) &= c_L(g_{\mathcal{O}_L}(u_1)) \\ &= c_L(g_{\mathcal{O}_L}(\delta_{\mathcal{O}_L}(s))) \\ &= c_L(\gamma_{\mathcal{O}_L}(s)) \\ &= c_L(\lambda {\mathcal{O}_L}^{*2}) \\ &= \lambda L^{*2}. \end{aligned}$$

Since $g_L(u) = [\lambda]$, so $u i_L(u_1)^{-1} \in \mathrm{Ker}(g_L) = \mathrm{Im}(f_L)$, hence there exists $u_2 \in H^1(L, \mu_2)$ such that $f_L(u_2) = u i_L(u_1)^{-1}$, therefore $u = i_L(u_1) f_L(u_2)$.

We have $u_1 \in \mathrm{Im}(\delta_{\mathcal{O}_L}) = \mathrm{Ker}(\alpha_{\mathcal{O}_L})$, so $\alpha_{\mathcal{O}_L}(u_1) = 1$. Hence

$$\alpha_L(i_L(u_1)) = j_L(\alpha_{\mathcal{O}_L}(u_1)) = j_L(1) = 1,$$

so $i_L(u_1) \in \mathrm{Ker}(\alpha_L)$.

Since $u \in \mathrm{Ker}(\alpha_L)$, by lemma 6.2.2, $f_L(u_2) = ui_L(u_1)^{-1} \in \mathrm{Ker}(\alpha_L)$. Hence $e_L(u_2) = \alpha_L(f_L(u_2)) = 1$.

Finally, since $j_L(\alpha_{\mathcal{O}_L}(u_1)) = \alpha_L(i_L(u_1)) = 1$ and the kernel of the map j_L is trivial by [17], we have $\alpha_{\mathcal{O}_L}(u_1) = 1$.

□

Lemma 8.4.2. Let h and D be unramified over L. Recall the elements u_1 and u_2 from Lemma 8.4.1. Then

$$cor_{L/K}(i_L(u_1)) \in \mathrm{Ker}(\alpha_K) \Rightarrow cor_{L/K}(u) \in \mathrm{Ker}(\alpha_K).$$

Proof. Since $e_L(u_2) = 1$, by Knebusch's norm principle we have $cor_{L/K}(u_2) \in \mathrm{Ker}(h_K)$, so $cor_{L/K}(f_L(u_2)) \in \mathrm{Ker}(\alpha_K)$. Then

$$cor_{L/K}(u) = cor_{L/K}(i_L(u_1)f_L(u_2)) = cor_{L/K}(i_L(u_1))cor_{L/K}(f_L(u_2)),$$

and by Lemma 6.2.2 we have $cor_{L/K}(u) \in \mathrm{Ker}(\alpha_K)$. □

8.5 A technical lemma

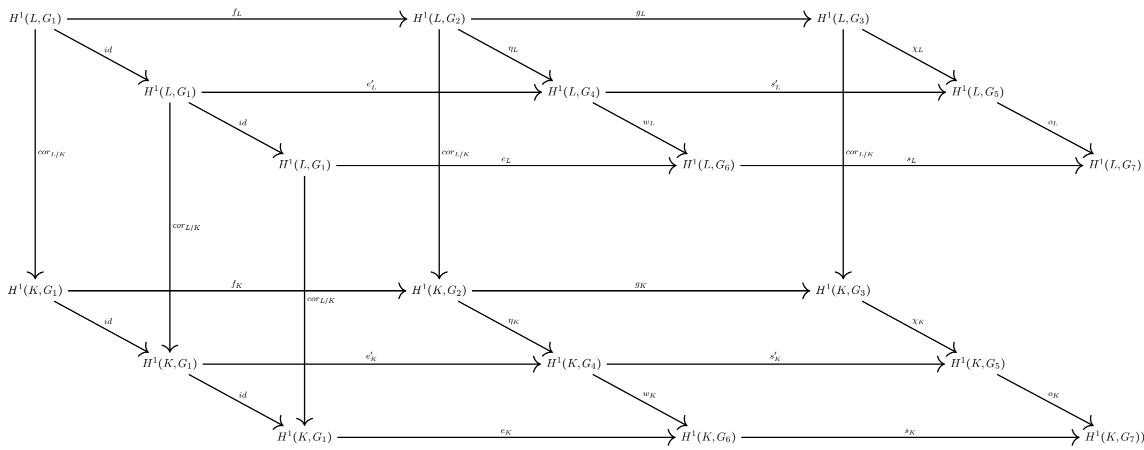
We will apply the following lemma in the proof of the main theorem in Section 9.4.

Lemma 8.5.1. Consider the linear algebraic groups G_1, G_2, G_3, G_4, G_5, G_6 and G_7 all defined over the field K, which fit into the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & G_1 & \longrightarrow & G_2 & \longrightarrow & G_3 & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G_1 & \longrightarrow & G_4 & \longrightarrow & G_5 & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G_1 & \longrightarrow & G_6 & \longrightarrow & G_7 & \longrightarrow & 1
\end{array}$$

Assume that all the vertical arrows are inclusions, G_2 is central in G_6 (and hence in G_4), and G_3 is central in G_7 (and hence in G_5).

Let L/K be a finite separable field extension. The above diagram gives rise to the following commutative diagram with exact horizontal rows:



Let $\alpha := w \circ \eta$, and $u \in \mathrm{Ker}(\alpha_L)$.

Assume that:

- (a) $u \in \mathrm{Ker}(\chi_L \circ g_L)$.
- (b) $cor_{L/K}(\mathrm{Ker}(\chi_L)) \subset \mathrm{Ker}(\chi_K)$.
- (c) $cor_{L/K}(\mathrm{Ker}(e_L)) \subset \mathrm{Ker}(e_K)$.
- (d) $cor_{L/K}(\mathrm{Ker}(\eta_L)) \subset \mathrm{Ker}(\eta_K)$.

Then $cor_{L/K}(u) \in \mathrm{Ker}(\alpha_K)$.

Proof. Put $v := \eta_L(u)$ and $\lambda := g_L(u)$. By assumption (a), $u \in \mathrm{Ker}(\chi_L \circ g_L) = \mathrm{Ker}({s_L}' \circ \eta_L)$, so $s'_L(v) = 1$. Let u_2 be a pre-image of v under ${e_L}'$. By (b) we have $\chi_K(cor_{L/K}(\lambda)) = 1$. Let $u_1 := u f_L(u_2)^{-1}$. We have

$$e_L(u_2) = w_L(e'_L(u_2)) = w_L(v) = \alpha_L(u) = 1.$$

So $u_2 \in \mathrm{Ker}(e_L)$ and assumption (c) implies that $cor_{L/K}(u_2) \in \mathrm{Ker}(e_K)$ and therefore $cor_{L/K}(f_L(u_2)) \in \mathrm{Ker}(\alpha_K)$.

Lemma 6.2.2 shows that $u_1 \in \mathrm{Ker}(\eta_L)$, because $\eta_L(u) = \eta_L(f_L(u_2)) = v$. By assumption (d) we have $\eta_K(cor_{L/K}(u_1)) = 1$, and $\alpha_K(cor_{L/K}(u_1)) = w_K \circ \eta_K(cor_{L/K}(u_1)) = 1$.

Therefore $cor_{L/K}(u_1)$ and $cor_{L/K}(f_L(u_2))$ are both in $\mathrm{Ker}(\alpha_K)$, and by Lemma 6.2.2, we have $cor_{L/K}(u) = cor_{L/K}(u_1 f_L(u_2)) \in \mathrm{Ker}(\alpha_K)$. □

Chapter 9

Proof of the main theorem

In this chapter, we will provide a proof of the main theorem, i.e., Theorem 8.0.1, in the following 4 cases separately. All the notations introduced in Chapter 8 will be used in the proof.

- **Case 1**: L/K is an unramified extension, and D_K is unramified over K.
- **Case 2**: L/K is a ramified extension, and D_K is unramified over K.
- **Case 3**: L/K is a ramified extension, and D_K is ramified over K.
- **Case 4**: L/K is an unramified extension, and D_K is ramified over K.

In each case we have several subcases, depending on the discriminant extension F, the element λ, the ramification of the skew-hermitian form h, the splitting of D over L, and the parity of n. We have listed all the subcases below. There are 14 different cases.

- D_K unramified
  - ***1***: *L/K unramified*
    - ***1.1***: λ *uniformizer*
    - ***1.2***: λ *unit*
  - ***2***: *L/K ramified*
    - ***2.1***: F *field*
    - ***2.2***: F *not field*

- D_K ramified
  - ***3***: *L/K ramified*
    - ***3.1***: λ *uniformizer*
    - ***3.2***: λ *unit*
      - ***3.2.1***: λ *uniformizer*
      - ***3.2.2***: λ *unit*
        - ***3.2.1***: h_K *unramified*
          - ***3.2.1.1***: n *even*
          - ***3.2.1.2***: n *odd*
        - ***3.2.2***: h_K *ramified*
  - ***4***: *L/K unramified*
    - ***4.1***: h_K *unramified*
      - ***4.1.1***: n *even*
      - ***4.1.2***: n *odd*
    - ***4.2***: h_K *ramified*
      - ***4.2.1***: D_L *nonsplit*
      - ***4.2.2***: D_L *split*
        - ***4.2.2.1***: λ *uniformizer*
        - ***4.2.2.2***: λ *unit*

One particularly illuminating case is subcase 1.2: D_K is unramified, the field extension L/K is unramified, and the element λ is a unit in L. Based on some reductions in Chapter 8 (Remarks 8.3.2 and 8.3.3) we can assume that in this case the form h is unramified over K (see Lemma 9.1.4). Hence, all the objects are unramified and we can apply Hensel's lemma directly (see the proof of subcase 1.2).

9.1 Proof of the main theorem: part 1

In this section we will prove the main theorem in case 1: L/K is unramified and D_K is unramified.

The elements a, b, and t are units; $x^2 = a$, $y^2 = b$, and $z = xy = -yx$ for $x, y, z \in D_K$. If D splits over L, then by Lemma 8.1.2, we assume that $t = a$.

Let us consider the following subcases:

- **Subcase 1.1**: λ is a uniformizer of L.
- **Subcase 1.2**: λ is a unit of L.

Subcase 1.1: λ is a uniformizer of L.

We prove a fact about the R-triviality of the adjoint group $PGO^+(h)$ under a specific assumption. The following theorem due to Merkurjev will be used:

Theorem 9.1.1.

$$PGO^+(h)(K)/R \cong G(h)/K^{*2}Hyp(h)$$

where:

$G(h) = \{s \in K^* \mid sh \cong h\}$ is the group of multipliers of h, and

$Hyp(h)$ is the subgroup of $G(h)$ generated by $\{N_{E/K}(E^*) \mid h \textit{ is hyperbolic over } E\}$ where E runs over finite extensions of K.

Proof. See [16, Theorem 1]. □

Lemma 9.1.2. Let E be a complete discretely valued field and *char* $E \neq 2$. Assume that Q is an unramified quaternion division algebra over E and $\mathfrak{h}$ is an anisotropic skew-hermitian form over Q with respect to the canonical involution on Q. Let μ be a uniformizer of E such that we have the E–isometry $\mu\mathfrak{h} \cong \mathfrak{h}$. Then $PGO^+(\mathfrak{h})(E)$ is R–trivial.

Proof. If $\mathfrak{h}$ is unramified or ramified, then we will have $\mu\mathfrak{h}_0 \cong \mathfrak{h}_0$ or $\mu\mathfrak{h}_1 \cong \mathfrak{h}_1$ which is impossible by Theorem 7.3.6. Hence, we assume that $\mathfrak{h}$ is neither unramified, nor ramified over E. Let $\mathfrak{h} = \mathfrak{h}_0 \perp \mathfrak{h}_1$ be the Larmour decomposition of $\mathfrak{h}$ over E (so *dim* $\mathfrak{h}_0$ and *dim* $\mathfrak{h}_1$ are nonzero).

Since μ is a multiplier of $\mathfrak{h}$ over E, we have the following isometries (over E):

$$\mathfrak{h}_{0,E} \perp \mathfrak{h}_{1,E} \cong \mathfrak{h}_E \cong \mu\mathfrak{h}_E \cong \mu\mathfrak{h}_{0,E} \perp \mu\mathfrak{h}_{1,E}.$$

The element μ is a uniformizer in E, hence by Theorem 7.3.6, we have the $E-$ isometry $\mathfrak{h}_{1,E} \cong \mu\mathfrak{h}_{0,E}$. Furthermore, $h_E \cong \mathfrak{h}_{0,E} \perp \mu\mathfrak{h}_{0,E}$.

Let $\theta \in G(\mathfrak{h})(E)$ (i.e., θ be a multiplier for $\mathfrak{h}$ over E). Up to squares in E^*, either θ is a unit in E^*, or $\theta = \theta'\mu$ for a unit θ' in E^*. Since $PGO^+(\mathfrak{h})(E)/R \cong G(\mathfrak{h})/{E^*}^2 Hyp(\mathfrak{h})$ (Theorem 9.1.1), we need to show $\theta \in {E^*}^2 Hyp(h)$.

The totally ramified extension $E(\sqrt{-\mu})$ splits $\mathfrak{h}$ and $\mu = N_{E(\sqrt{-\mu})/E}(\sqrt{-\mu})$. Thus $\mu \in Hyp(\mathfrak{h})$.

Case 1: Let θ be a unit in E^*. The $E-$isometry $\theta\mathfrak{h}_E \cong \mathfrak{h}_E$ implies that

$$\theta\mathfrak{h}_{0,E} \perp \theta\mu\mathfrak{h}_{0,E} \cong \mathfrak{h}_{0,E} \perp \mu\mathfrak{h}_{0,E},$$

hence by Theorem 7.3.6, we have $\mathfrak{h}_{0,E} \cong \theta\mathfrak{h}_{0,E}$.

Consider the field $E_1 = E(\sqrt{-\mu\theta})$, which is a complete discretely valued field with the same residue field as E. Over E_1, we have the isometries

$$\mathfrak{h}_{E_1} \cong \theta\mathfrak{h}_{E_1} \cong \theta\mathfrak{h}_{0,E_1} \perp \theta\mu\mathfrak{h}_{0,E_1} \cong \mathfrak{h}_{0,E_1} \perp \theta\mu\mathfrak{h}_{0,E_1} \cong \mathfrak{h}_{0,E_1} \perp -\mathfrak{h}_{0,E_1}.$$

So $\mathfrak{h}$ is hyperbolic over E_1, and $\theta\mu = N_{E_1/E}(\sqrt{-\theta\mu}) \in Hyp(\mathfrak{h})$. Since $\mu \in Hyp(\mathfrak{h})$, we have $\theta \in Hyp(\mathfrak{h})$, which shows that $PGO^+(\mathfrak{h})(E)$ is $R-$trivial by Theorem 9.1.1.

Case 2: Let $\theta = \theta'\mu$ for a unit θ' in E^*. Then $\theta' = \theta\mu^{-1} \in G(\mathfrak{h})$, and repeating the same argument as in Case 1 for θ' shows that $PGO^+(\mathfrak{h})(E)$ is $R-$trivial. □

The following lemma is going to be used in the current section, and also later in the proof of Case 3.

Lemma 9.1.3. Assume that λ is a uniformizer in L, and furthermore one of the following assumptions holds:

- L/K is unramified and D_K is unramified, or
- L/K is ramified and D_K is ramified.

Then $PGO^+(h)(L)$ is $R-$trivial.

Proof. Assume that D_L is an L-division algebra. Then D_L is unramified over L. By Lemma 9.1.2, $PGO^+(h)(L)$ is $R-$trivial.

Now assume that D_L is split. The skew-hermitian form h over D_L corresponds to a quadratic form q over L with $\lambda \in G(q)(L)$ (the group of similarity factors of q over L) by Morita equivalence, once we fix an isomorphism $M_2(L) \cong D_L$ (Morita equivalence preserves multipliers). Since λ is not a square in L, the Springer decomposition of quadratic forms implies that $q \cong q' \otimes < 1, \lambda >$ for an unramified quadratic form q' defined over L. Then by [4, Lemma 4.2], $PGO^+(q)(L)$ is $R-$ trivial, which also means that $PGO^+(h)(L)$ is $R-$trivial. □

Proof of the main theorem in subcase 1.1:

Proof. By Lemma 9.1.3 $PGO^+(h)(L)$ is $R-$trivial. Then Theorem 5.1.2 implies that $cor_{L/K}(u) \in \mathrm{Ker}(\alpha_K)$.

□

Subcase 1.2: λ is a unit of L.

Lemma 9.1.4. In subcase 1.2, we have the following isometries over L:

$$h_{0,L} \cong \lambda h_{0,L}, \quad \textit{and} \quad h_{1,L} \cong \lambda h_{1,L}.$$

Proof. If one of the skew-hermitian forms h_0 or h_1 is trivial, then we already have the desired result since $h_L \cong \lambda h_L$. So assume that both of them are nontrivial.

First assume that D_L is an $L-$division algebra. Then we have $\lambda h_{0,L} \perp \lambda h_{1,L} = \lambda h_L \cong h_L = h_{0,L} \perp h_{1,L}$. Every element in the diagonalization of h_0 (resp. h_1) has value 0 (resp. 1) over L. By Theorem 7.3.6 we have $h_{0,L} \cong \lambda h_{0,L}$ and $h_{1,L} \cong \lambda h_{1,L}$.

Now, assume that D splits over L. Fix an isomorphism $M_2(L) \cong D_L$. By Morita equivalence, the forms $h_{0,L}$ and $h_{1,L}$ correspond to quadratic forms $q_{0,L}$ and $q_{1,L}$ over L, respectively. Changing the isomorphism $M_2(L) \cong D_L$ affects Morita equivalence by a scalar. We choose the isomorphism such that the ramification of the forms is preserved under Morita equivalence, i.e., q_0 is unramified and q_1 is ramified. The isometry $h_L \cong \lambda h_L$ implies that $q_L \cong \lambda q_L$, so we have $\lambda q_{0,L} \perp \lambda q_{1,L} \cong q_{0,L} \perp q_{1,L}$. Note that the elements in the diagonalization of q_0 (resp. q_1) have value 0 (resp. 1) over L. Hence by Springer's decomposition theorem for quadratic forms over complete discretely valued fields, we have $q_{0,L} \cong \lambda q_{0,L}$ and $q_{1,L} \cong \lambda q_{1,L}$. Finally, by Morita equivalence $h_{0,L} \cong \lambda h_{0,L}$ and $h_{1,L} \cong \lambda h_{1,L}$. □

By Remarks 8.3.2, 8.3.3 and Lemma 9.1.4, we may assume that $h = h_0$, i.e., h is unramified. Let $\bar{h}$ be the residue skew-hermitian form defined over $(\overline{D_K}, \overline{\tau})$.

Proof of the main theorem in subcase 1.2:

Proof. Recall that k denotes the residue field of K and $l = k(\sqrt{\bar{t}})$ is the residue field of L. Note that even though we do not have a canonical valuation on D_L if it splits, but we still have a skew-hermitian form $\bar{h}$ defined over l, obtained by the base change of $\bar{h}$ from k to l.

Recall the element u_1 from Lemma 8.4.1. By specializing to the residue field we get

$$\overline{u_1} \in \mathrm{Ker}(\alpha_l : H^1(l, \bar{Z}) \longrightarrow H^1(l, Spin(\bar{h}))).$$

Since the norm principle holds for $Spin(\bar{h})$ over l/k, we get

$$N_{l/k}(\overline{u_1}) \in \mathrm{Ker}(\alpha_k : H^1(k, \bar{Z}) \longrightarrow H^1(k, Spin(\bar{h}))).$$

Then Hensel's lemma implies that $cor_{L/K}(i_L(u_1)) \in \mathrm{Ker}(\alpha_K)$. By Lemma 8.4.2, $cor_{L/K}(u) \in \mathrm{Ker}(\alpha_K)$.

□

9.2 Proof of the main theorem: part 2

In this section we will prove the main theorem in case 2: when L/K is ramified and D_K is unramified.

Lemma 9.2.1. If D_K is unramified over K, and D_L splits, then L/K must be unramified.

Proof. By Lemma 8.1.2, L can be embedded over K in D_K. Since D_K is unramified over K, any maximal subfield, in particular L, has to be unramified over K too. □

By Lemma 9.2.1, D_L is an unramified L–division algebra in case 2.

The skew-hermitian form h can be neither unramified nor ramified over K, i.e., both h_0 and h_1 could be nontrivial. However, h_L is unramified over L.

Recall that by Remark 8.2.2, F is either an unramified quadratic field extension of K, or it is isomorphic to $K \times K$. Now we give the proof of the main theorem in these two different cases separately, first when F is a field, and then in the case $F = K \times K$. Recall the element u_1 from Lemma 8.4.1.

Subcase 2.1: F is a field.

In this case, M is a ramified quadratic field extension of F.

Proof of the main theorem in subcase 2.1:

Proof. Assume that n is even. Then $H^1(K, Z) = F^*/F^{*2}$ and $H^1(L, Z) = M^*/M^{*2}$. The element u_1 has a representative v in ${\mathcal{O}_M}^*$. Since the extension M/F is ramified, $N_{M/F}(v)$ is a square in F^*, so $cor_{L/K}(i_L(u_1)) = 1 \in H^1(K, Z)$. Hence $cor_{L/K}(u) \in \mathrm{Ker}\ \alpha_K$ by Lemma 8.4.2.

Now assume that n is odd. The element u_1 has a representative $(q, p) \in {\mathcal{O}_L}^* \times {\mathcal{O}_M}^*$. Then $cor_{L/K}(u_1) = [(N_{L/K}(q), N_{M/F}(p))]$. Since both extensions M/F and L/K are ramified, both elements $N_{L/K}(q)$ and $N_{M/F}(p)$ are squares in K^* and F^*, respectively. Hence we have $cor_{L/K}(i_L(u_1)) = 1 \in H^1(K,Z)$ and $cor_{L/K}(u) \in \text{Ker } \alpha_K$ by Lemma 8.4.2.

□

Subcase 2.2: $F \cong K \times K$.

In this case, $M \cong L \times L$.

Proof of the main theorem in subcase 2.2:

Proof. Assume that n is even. Then $H^1(K,Z) = (K^* \times K^*)/(K^{*2} \times K^{*2})$ and $H^1(L,Z) = (L^* \times L^*)/(L^{*2} \times L^{*2})$. The element u_1 has a representative (v,w) in $\mathcal{O}_L{}^* \times \mathcal{O}_L{}^*$. Since the extension L/K is ramified, $cor_{L/K}(i_L(u_1)) = [(N_{L/K}(v), N_{L/K}(w))] = [(1,1)] = 1 \in H^1(K,Z)$. Hence $cor_{L/K}(u) \in \text{Ker } \alpha_K$ by Lemma 8.4.2.

Now assume that n is odd. Then the element u_1 has a representative $(q,(p,p')) \in \mathcal{O}_L{}^* \times (\mathcal{O}_L{}^* \times \mathcal{O}_L{}^*)$. Then $cor_{L/K}(u_1) = [(N_{L/K}(q),(N_{L/K}(p),N_{L/K}(p')))]$. Since L/K is a ramified extension, all elements $N_{L/K}(q)$, $N_{L/K}(p)$ and $N_{L/K}(p')$ are squares in K^*. Hence we have $cor_{L/K}(i_L(u_1)) = 1 \in H^1(K,Z)$ and $cor_{L/K}(u) \in \text{Ker } \alpha_K$ by Lemma 8.4.2.

□

9.3 Proof of the main theorem: part 3

The goal in this section is to prove the main theorem in case 3, when L/K is ramified and D_K is ramified. Note that D_L is then unramified over L.

Recall that $D = (\frac{a,\pi}{K})$ and $L = K(\sqrt{c\pi})$. The element a is unit over K; $x^2 = a,\ y^2 = \pi$, and $z = xy = -yx$ for $x,y,z \in D_K$.

Let us consider he following subcases:

- **Subcase 3.1**: λ is a uniformizer of L.
- **Subcase 3.2**: λ is a unit of L.

Proof of the main theorem in subcase 3.1:

Proof. If λ is a uniformizer of L, then by Lemma 9.1.3 $PGO^+(h)(L)$ is R−trivial, and Theorem 5.1.2 implies that $cor_{L/K}(u) \in \text{Ker}(\alpha_K)$.

□

In the rest of this section, we prove the main theorem in subcase 3.2: we assume that λ is a unit of L.

Lemma 9.3.1. In subcase 3.2, we have the following isometries over L:

$$h_{0,L} \cong \lambda h_{0,L}, \quad \textit{and} \quad h_{1,L} \cong \lambda h_{1,L}.$$

Proof. If one of the skew-hermitian forms h_0 or h_1 is trivial, then we already have the desired result since $h_L \cong \lambda h_L$. So assume that both of them are nontrivial.

First assume that D_L is an $L-$ division algebra. Then we have $\lambda h_{0,L} \perp \lambda h_{1,L} = \lambda h_L \cong h_L = h_{0,L} \perp h_{1,L}$. Every element in the diagonalization of h_0 (resp. h_1) has value 0 (resp. $\frac{1}{2}$) over L. By Theorem 7.3.6 we have $h_{0,L} \cong \lambda h_{0,L}$ and $h_{1,L} \cong \lambda h_{1,L}$.

Now, assume that D splits over L. Fix an isomorphism $M_2(L) \cong D_L$. By Morita equivalence, the forms $h_{0,L}$ and $h_{1,L}$ correspond to quadratic forms $q_{0,L}$ and $q_{1,L}$ over L, respectively. Changing the isomorphism $M_2(L) \cong D_L$ affects Morita equivalence by a scalar. We choose the isomorphism such that the ramification of the forms are preserved under Morita equivalence, i.e., q_0 is unramified and q_1 is ramified. The isometry $h_L \cong \lambda h_L$ implies that $q_L \cong \lambda q_L$, so we have $\lambda q_{0,L} \perp \lambda q_{1,L} \cong q_{0,L} \perp q_{1,L}$. Note that the elements in the diagonalization of q_0 (resp. q_1) have value 0 (resp. $\frac{1}{2}$) over L. Hence by Springer's decomposition theorem for quadratic forms over complete discretely valued fields we have $q_{0,L} \cong \lambda q_{0,L}$ and $q_{1,L} \cong \lambda q_{1,L}$. Finally, by Morita equivalence $h_{0,L} \cong \lambda h_{0,L}$ and $h_{1,L} \cong \lambda h_{1,L}$. □

By Remark 8.3.2 and Lemma 9.3.1, we may assume that either $h = h_0$ or $h = h_1$, i.e., h is either unramified or ramified.

Subcase 3.2.1: h_K is unramified

The group $Spin(h)$ and its center Z are actually defined over $\mathcal{O}_K$ and by base change we also get the original groups over K. Note that D_L is either an unramified $L-$division algebra, or it is a split algebra.

Proof of the main theorem in subcase 3.2.1:

Recall that the discriminant extension of K is F (and the discriminant extension of L is M), and also the element u_1 from Lemma 8.4.1.

Subcase 3.2.1.1: when n is even

Proof. In this case $F = K \times K$, hence $M = L \times L$ and $H^1(L, Z) = H^1(L, \mu_2) \times H^1(L, \mu_2) = (L^*/L^{*2}) \times (L^*/L^{*2})$. Since the quadratic extension L/K is totally ramified, any element in L^*/L^{*2} has a representative in K^*/K^{*2}, so $cor_{L/K}(i_L(u_1))$ is trivial in $H^1(K, Z) = (K^*/K^{*2}) \times (K^*/K^{*2})$, and in particular it implies that $cor_{L/K}(u) \in \text{Ker } \alpha_K$ by Lemma 8.4.2. □

Subcase 3.2.1.2: when n is odd

Proof. In this case, $M = L(x)$ and $H^1(L, Z) = U(L)/U_0(L)$ (see Section 8.1). Since the quadratic extension L/K (resp. $L(x)/K(x)$) is totally ramified, any element in $L^*/(L^*)^2$ (resp. $L(x)^*/L(x)^{*2}$) has a representative in $K^*/(K^*)^2$ (resp. $K(x)^*/K(x)^{*2}$). So we can represent u_1 as $u_1 = [(q,p)]$ where $q \in \mathcal{O}_K{}^*$ and $p \in \mathcal{O}_{K(x)^*}$, and then $cor_{L/K}(i_L(u_1)) = [(q^2, p^2)] = [(1,1)] = 1$, hence $cor_{L/K}(i_L(u_1)) \in \mathrm{Ker}(\alpha_K)$ and we are done by Lemma 8.4.2. □

Subcase 3.2.2: h_K is ramified

We will construct an unramified hermitian form h' in this subcase, and then will reduce the main question from h to h'. By Remark 7.3.5 we can assume that

$$h = <(\beta_1 + \gamma_1 x)y, \dots, (\beta_n + \gamma_n x)y>,$$

where $\beta, \dots, \beta_n, \gamma_1, \dots, \gamma_n \in \mathcal{O}_K$ and the elements $\beta_i + \gamma_i x$ are all units.

Consider the following orthogonal involution on D:

$$\tau_y : D \longrightarrow D$$

$$s \mapsto y^{-1}\tau(s)y.$$

Elements in the subfield $K(x)$ are invariant under τ_y. The following is a unit hermitian form over (D, τ_y) (since the elements of the maximal subfield $K(x)$ are invariant under τ_y):

$$h' = <\beta_1 + \gamma_1 x, \dots, \beta_n + \gamma_n x> .$$

Let $H = diag(\beta_1 + \gamma_1 x, \dots, \beta_n + \gamma_n x) \in M_n(D)$ be the diagonal matrix representing h'. Then the matrix Hy represents h.

Corollary 9.3.2. The norm principle for $Spin(h')$ is equivalent to the norm principle for $Spin(h)$.

Proof. Let σ_h and $\sigma_{h'}$ be the involutions on $M_n(D)$, adjoint to h and h', respectively. For all $M \in M_n(D)$ we have

$$\begin{aligned}\sigma_{h'}(M) &= H\tau_y(M^t)H^{-1}\\ &= Hy\tau(M^t)y^{-1}H^{-1}\\ &= Hy\tau(M^t)(Hy)^{-1}\\ &= \sigma_h(M).\end{aligned}$$

Hence the adjoint involutions σ_h and $\sigma_{h'}$ on $M_n(D)$ are identical. Therefore the algebraic groups $O^+(h)$ and $O^+(h')$ (respectively, $Spin(h)$ and $Spin(h')$) are identical,

□

Proof of the main theorem in subcase 3.2.2:

Proof. In subcase 3.2.2, in order to prove the main result for $Spin(h)$, it is enough to show it for $Spin(h')$ by Corollary 9.3.2. Since h' is an unramified form, then the same argument as in subcase 3.2.1 works for this subcase, and we are done. □

9.4 Proof of the main theorem: part 4

In this section, we prove the main theorem in case 4: $D_K \cong (\frac{a,\pi}{K})$ is ramified over K and $L = K(\sqrt{t})$ is an unramified extension of K. Recall that the elements a and t are units. We have $x^2 = a,\ y^2 = \pi$, and $z = xy = -yx$ for $x, y, z \in D_K$.

Lemma 9.4.1. Assume that $deg(h_0) \neq 0$. Then D_L is an L-division algebra and ramified over L.

Proof. If D_L splits over L, then the unitary group $U(h_0)$ contains the norm one torus ${R_{K(x)/K}}^{(1)}(\mathbb{G}_m)$ which becomes a split torus over L, contradicting the fact that h is anisotropic over L. Therefore D_L is an $L-$ division algebra. Since L/K is unramified, D_L is ramified as an algebra over L. □

Lemma 9.4.2. In case 4, we have the following isometries over L:

$$h_{0,L} \cong \lambda h_{0,L}, \quad \textit{and} \quad h_{1,L} \cong \lambda h_{1,L}.$$

Proof. If one of the skew-hermitian forms h_0 or h_1 is trivial, then we already have the desired result since $h_L \cong \lambda h_L$. So assume that both of them are nontrivial.

We know that D_L is an $L-$ division algebra by Lemma 9.4.1. Then we have $\lambda h_{0,L} \perp \lambda h_{1,L} = \lambda h_L \cong h_L = h_{0,L} \perp h_{1,L}$ and $\nu_L(\lambda) \in \{0, 1\}$. Every element in the diagonalization of h_0 (resp. h_1) has value 0 (resp. $\frac{1}{2}$) over L. By Theorem 7.3.6 we have $h_{0,L} \cong \lambda h_{0,L}$ and $h_{1,L} \cong \lambda h_{1,L}$. □

By Remark 8.3.2 and Lemma 9.4.2, we may assume that either $h = h_0$ or $h = h_1$, i.e., h is either unramified or ramified.

Subcase 4.1, when h is unramified.

By Remark 7.3.5 we have

$$h =< \alpha_1 x, \dots, \alpha_n x >,$$

where $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K{}^*$.

The restriction of the involution τ to the field $K(x)$ is a unitary involution, which we denote by τ (abusing notation). We define the following unitary unit hermitian form over $(K(x), \tau)$

$$h' :=< \alpha_1 x, \dots, \alpha_n x > \quad over \;\; (K(x), \tau).$$

The hermitian form h' will only be used in subcase 4.1.

Lemma 9.4.3. The unitary group $U(h')$ is a subgroup of the special orthogonal group $O^+(h)$.

Proof. Let $g \in U(h')$, so once we fix a linear representation $U(h') \longrightarrow GL_n(K(x))$, we can view g as a matrix, which belongs to $GL_n(K(x))$. In fact, g is also an element of $GL_n(D)$ as $GL_n(K(x)) \subset GL_n(D)$. Let H be the diagonal matrix $diag(\alpha_1 x, \dots, \alpha_n x)$ representing h' (and h). Also let σ_h be the involution on $M_n(D)$ adjoint to h, and $\sigma_{h'}$ be the involution on $M_n(K(x))$ adjoint to h'. Both of these involutions are given by the map $M \mapsto H\tau(M^t)H^{-1}$, where M^t means transpose of M, and by $\tau(M^t)$ we mean the matrix obtained by the action of τ on all entries of M^t. The element g satisfies the equation $g\sigma_{h'}(g) = Id$. By taking the determinant of both sides we have $N_{K(x)/K}(det\ g) = 1$. The group $O^+(h)$ is defined as:

$$O^+(h) := \{f \in GL_n(D) | f\sigma_h(f) = Id, \;\; and \; Nrd(f) = 1\}.$$

So the element g clearly lies in $O^+(h)$ as well, which shows that $U(h') \subset O^+(h)$. □

Note that the unitary group $U(h')$ has a subgroup $SU(h')$, which in fact can be viewed as a subgroup of $O^+(h)$ by Lemma 9.4.3. Let o_K be the induced map $o_K : H^1(K, SU(h')) \to H^1(K, O^+(h))$.

Lemma 9.4.4. Kernel of the maps o_K and o_L are trivial.

Proof. Let $[\mathfrak{h}] \in \operatorname{Ker}(o_K)$. The set $H^1(K, O^+(h))$ consists of the isometry classes of regular skew-hermitian forms over (D, τ) with the same discriminant as h. So $\mathfrak{h}$ is a unitary hermitian form over $(K(x), \tau)$ which is isometric to the skew-hermitian form h after extending the scalars from $K(x)$ to D. This in particular means that $\mathfrak{h}$ is a unit hermitian form by Theorem 7.3.6. By [15, Theorem 2.12], $\overline{\mathfrak{h}} \cong \overline{h'}$ as unitary hermitian forms over $(k(\overline{x}), \overline{\tau})$.

Again, by [15, Theorem 2.12], we have $\mathfrak{h} \cong h'$ as unitary hermitian forms over $(K(x), \tau)$. Therefore $\mathrm{Ker}(o_K)$ is trivial.

A similar argument as above works for o_L, since D_L is an $L-$ division algebra by Lemma 9.4.1. $\square$

Let H be the preimage of the group $SU(h')$ under the morphism $Spin(h) \longrightarrow O^+(h)$.

Lemma 9.4.5. Let H^0 be the connected component of H. Then the restriction of the map $Spin(h) \longrightarrow O^+(h)$ to H^0 is an isomorphism of algebraic groups $H^0 \cong SU(h')$.

Proof. The connected component H^0 of H has the structure $H^0 = R_u(H^0) \rtimes {H^0}_{red}$ over K^{sep}, where $R_u(H^0)$ is its unipotent radical and ${H^0}_{red}$ is a reductive subgroup. Under the morphism $H^0 \to SU(h')$ the unipotent radical of H^0 is being mapped to the unipotent radical of $SU(h')$, which is trivial because $SU(h')$ is a semisimple group. Hence $R_u(H^0) \subset$ Ker $(H^0 \to SU(h'))$, and since the kernel is finite, $R_u(H^0)$ is trivial. So the connected component H^0 is reductive, and it is an almost direct product of a central torus S and its semisimple part, i.e., $H^0 = S \cdot [H^0, H^0]$. But then since S is in the kernel of the morphism $H \to SU(h')$, it is trivial because the kernel is finite. Therefore, H^0 is semisimple. So the map $H^0 \longrightarrow SU(h')$ is isomorphism since $SU(h')$ is simply connected and does not admit any nontrivial covering. $\square$

Let $Z_1 = \mu_2$ be the central subgroup in $Spin(h)$ which is the kernel of the map $Spin(h) \longrightarrow O^+(h)$. Note that $Z_1 \cap H^0 = \{1\}$ by Lemma 9.4.5.

We need to consider the cases below separately based on the parity of n, the dimension of h:

Subcase 4.1.1 : n is even.

The center of the group $O^+(h)$ is μ_2, which is a central subgroup of $SU(h')$ as well. Let us denote by Z_2 its pre-image in H^0. On the other hand we know that the center of $Spin(h)$, i.e., Z, has the structure $R_{F/K}(\mu_2) = R_{(K\times K)/K}(\mu_2) = \mu_2 \times \mu_2$ (since $disc(h)$ is trivial we have $F = K \times K$). So Z_2 has to be one of the components μ_2 of Z, and the other μ_2 component is Z_1. We have $Z = Z_1 \times Z_2$.

Proof of the main theorem in subcase 4.1.1:

Proof. Consider the following diagram:

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & Z_1 & \longrightarrow & Z = Z_1 \times Z_2 & \longrightarrow & Z_2 & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & Z_1 & \longrightarrow & Z_1 \times SU(h') & \longrightarrow & SU(h') & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & Z_1 & \longrightarrow & Spin(h) & \longrightarrow & O^+(h) & \longrightarrow & 1
\end{array}
$$

Now we apply Lemma 8.5.1: Put
$G_1 := Z_1$
$G_2 := Z$
$G_3 := Z_2$
$G_4 := Z_1 \times SU(h')$
$G_5 := SU(h')$
$G_6 := Spin(h)$
$G_7 := O^+(h)$

We need to show that conditions (a),(b),(c), and (d) are satisfied:

(a) We know that $u \in \mathrm{Ker}(o_L \circ \chi_L \circ g_L)$, and $\mathrm{Ker}(o_L)$ is trivial by Lemma 9.4.4. Therefore, $u \in \mathrm{Ker}(\chi_L \circ g_L)$.

(b) This is equivalent to the H^1- variant of the norm principle for the pair $(Z_2, SU(h'))$ which holds by [1], as $SU(h')$ is an algebraic group of type A_n.

(c) It is equivalent to Knebusch norm principle.

(d) The map $\eta : H^1(-, Z_1) \times H^1(-, Z_2) \to H^1(-, Z_1) \times H^1(-, SU(h'))$ can be written as the product of the identity map $id : H^1(-, Z_1) \to H^1(-, Z_1)$ and the map $\chi : H^1(-, Z_2) \to H^1(-, SU(h'))$. Then the same argument as in part (b) above shows that $cor_{L/K}(\mathrm{Ker}(\eta_L)) \subset \mathrm{Ker}(\eta_K)$. □

Subcase 4.1.2: n is odd.

Let $\tilde{U}$ be the pre-image of the group $U(h')$ under the morphism $Spin(h) \to O^+(h)$. Recall that H is the preimage of the group $SU(h')$ under the morphism $Spin(h) \longrightarrow O^+(h)$.

Lemma 9.4.6. The connected component $\tilde{U}^0$ is an almost direct product of H^0 (the connected component of H) and a central torus S. In particular, $\tilde{U}^0$ is reductive. The torus S is being mapped to the norm one torus ${R_{K(x)/K}}^{(1)}(\mathbb{G}_m)$ under the morphism $Spin(h) \to O^+(h)$ with kernel $Z_1 = \mu_2$. Furthermore, $Z \subset S$.

Proof. The connected group $\tilde{U}^0$ has an almost direct product structure $\tilde{U}^0 = R_u(\tilde{U}^0)\cdot\tilde{U}^0_{red}$ over K^{sep} where $R_u(\tilde{U}^0)$ is its unipotent radical and $\tilde{U}^0_{red}$ is a reductive subgroup. Under the morphism $\tilde{U}^0 \to U(h')$ the unipotent radical of $\tilde{U}^0$ is being mapped to the unipotent radical of $U(h')$, which is trivial because $U(h')$ is a reductive group. Hence $R_u(\tilde{U}^0) \subset \text{Ker}\,(\tilde{U}^0 \to U(h'))$, and since the kernel is finite, $R_u(\tilde{U}^0)$ is trivial. So the connected component $\tilde{U}^0$ is reductive, and it is an almost direct product of a central torus S and its semisimple part, i.e., $\tilde{U}^0 = S\cdot[\tilde{U}^0,\tilde{U}^0]$.

On the other hand, the unitary group $U(h')$ is an almost direct product of the central torus ${R_{K(x)/K}}^{(1)}(\mathbb{G}_m)$ and the special unitary group $SU(h')$, i.e., $U(h') = {R_{K(x)/K}}^{(1)}(\mathbb{G}_m)\cdot SU(h')$.

Under the map $\tilde{U}^0 \to U(h')$, the central torus S goes to ${R_{K(x)/K}}^{(1)}(\mathbb{G}_m)$, and the semisimple part of $\tilde{U}^0$, i.e., $[\tilde{U}^0,\tilde{U}^0]$, goes to the semisimple part of $U(h')$, i.e., $SU(h')$. Since the group $SU(h')$ is simply connected, the covering $[\tilde{U}^0,\tilde{U}^0] \to SU(h')$ has to be trivial, so

$$\tilde{U}^0 = S\cdot H^0.$$

The center of the group $O^+(h)$, which is μ_2, is in fact a subgroup of ${R_{K(x)/K}}^{(1)}(\mathbb{G}_m)$: once we fix a linear representation $O^+(h) \to GL_n(D)$, the nontrivial element of the center of $O^+(h)$ is in fact the diagonal matrix $diag(-1,\dots,-1)$, whose determinant (i.e., -1) has reduced norm 1, so this element belongs to ${R_{K(x)/K}}^{(1)}(\mathbb{G}_m)$. This implies that the preimage of ${R_{K(x)/K}}^{(1)}(\mathbb{G}_m)$, i.e., S, contains Z (the center of $Spin(h)$), and we have an exact sequence

$$1 \to Z_1 \to S \to {R_{K(x)/K}}^{(1)}(\mathbb{G}_m) \to 1.$$

□

Lemma 9.4.7. The multiplier λ belongs to $N_{L(x)/L}(L(x)^*)$.

Proof. Since n is odd, the determinant of h is of the form αx^n, for a unit $\alpha \in \mathcal{O}_K$ (recall that $h \cong h_0$). So the discriminant extension of L is $L(x)$ ($L(x) \cong L[t]/ < t^2 - Nrd_{D_L/L}(det\ h) >$). Recall that $Z = \text{Ker}(Norm : R_{L(x)/L}(\mu_4) \longrightarrow \mu_4)$ ([19, Page 332]), and $H^1(L,Z) = U(L)/U_0(L)$, where $U \subseteq \mathbb{G}_m \times R_{L(x)/L}\mathbb{G}_m$ is the subgroup defined by

$$U(L) \coloneqq \{(q,p) \in L^* \times L(x)^* | q^4 = Norm_{L(x)/L}(p)\}$$

and $U_0 \subseteq U$ is the subgroup defined by

$$U_0(L) \coloneqq \{(N_{L(x)/L}(p), p^4) | p \in L(x)^*\}.$$

The map $g_L : H^1(L,Z) \to H^1(L,\mu_2)$ sends $[q,p]$ to $[N_{L(x)/L}(p_0)]$, where $p_0 \in L(x)^*$ is such that $p_0\psi(p_0)^{-1} = q^{-2}p$ (see [13, Section 13]). Since λ is in the image of the map g_L, then it belongs to $N_{L(x)/L}(L(x)^*)$. □

Proof of the main theorem in subcase 4.1.2:

Proof. Consider the following diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & Z_1 & \longrightarrow & Z & \longrightarrow & Z_2 & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & Z_1 & \longrightarrow & S & \longrightarrow & {R_{K(x)/K}}^{(1)}(\mathbb{G}_m) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & Z_1 & \longrightarrow & Spin(h) & \longrightarrow & O^{+}(h) & \longrightarrow & 1
\end{array}$$

Now we apply Lemma 8.5.1: Put
$G_1 := Z_1$
$G_2 := Z$
$G_3 := Z_2$
$G_4 := S$
$G_5 := {R_{K(x)/K}}^{(1)}(\mathbb{G}_m)$
$G_6 := Spin(h)$
$G_7 := O^{+}(h)$

We need to show that conditions (a),(b),(c), and (d) are satisfied:

(a) By Lemma 9.4.7, we know that the multiplier λ belongs to $N_{L(x)/L}(L(x)^*)$. By Hilbert theorem 90, we have $H^1(L, {R_{K(x)/K}}^{(1)}(\mathbb{G}_m)) = L^*/N_{L(x)/L}(L(x)^*)$, hence $\chi_L([\lambda]) = 1$. Therefore, $u \in \mathrm{Ker}(\chi_L \circ g_L)$.

(b) This is true due to commutativity of ${R_{K(x)/K}}^{(1)}(\mathbb{G}_m)$.

(c) It is equivalent to Knebusch norm principle.

(d) It holds because of commutativity of S.

□

Subcase 4.2, when $h = h_1$ is ramified.

By Remark 7.3.5 we can assume that

$$h =< (\beta_1 + \gamma_1 x)y, \ldots, (\beta_n + \gamma_n x)y >,$$

where $\beta, \ldots, \beta_n, \gamma_1, \ldots, \gamma_n \in \mathcal{O}_K$ and the elements $\beta_i + \gamma_i x$ are all units.

Consider the following orthogonal involution on D:

$$\tau_y : D \longrightarrow D$$

$$s \mapsto y^{-1}\tau(s)y.$$

Elements in the subfield $K(x)$ are invariant under τ_y. Then

$$h' :=< \beta_1 + \gamma_1 x, \dots, \beta_n + \gamma_n x >$$

is a unit quadratic form over $K(x)$. The following is a unit hermitian form over (D, τ_y) (since the elements of the maximal subfield $K(x)$ are invariant under τ_y):

$$h'' =< \beta_1 + \gamma_1 x, \dots, \beta_n + \gamma_n x > .$$

The quadratic form h' is in fact the restriction of the hermitian form h'' to $K(x)^n$.

Let $H = diag(\beta_1 + \gamma_1 x, \dots, \beta_n + \gamma_n x)$ be the diagonal matrix representing h' (or h''). Then the skew-symmetric matrix Hy (with respect to the canonical involution τ) represents h.

Let σ_h and $\sigma_{h''}$ be the corresponding adjoint involutions on $M_n(D)$. Then for all $M \in M_n(D)$ we have

$$\begin{aligned}\sigma_{h''}(M) &= H\tau_y(M^t)H^{-1}\\ &= Hy\tau(M^t)y^{-1}H^{-1}\\ &= Hy\tau(M^t)(Hy)^{-1}\\ &= \sigma_h(M).\end{aligned}$$

Hence the algebraic groups $O^+(h)$ and $O^+(h'')$ (respectively, $Spin(h)$ and $Spin(h'')$) are identical. So it is enough to show the norm principle for the pair $(Z, Spin(h''))$ over L/K (abusing notation, we denote the center of $Spin(h'')$ by Z as well).

Note that the forms h' and h'' will only be used in subcase 4.2.

Let $G := R_{K(x)/K}(O^+(h'))$.

Lemma 9.4.8. *G is a subgroup of $O^+(h'')$.*

Proof. Let $g \in G(K)$. By the natural identification $G(K) = O^+(h')(K(x))$ and abusing notation, we view g as an element in $O^+(h')(K(x))$. Once we fix a linear representation $O^+(h') \longrightarrow GL_n(K(x))$, we can view g as a matrix, which belongs to $GL_n(K(x))$. In fact, g is also an element of $GL_n(D)$ as $GL_n(K(x)) \subset GL_n(D)$. Recall that the matrix H represents both h' and h''. Furthermore $\sigma_{h''}$ is the involution on $M_n(D)$ adjoint to h'', and $\sigma_{h'}$ is the involution on $M_n(K(x))$ adjoint to h'. The involution $\sigma_{h''}$ is given by the map $M \mapsto H\tau_y(M^t)H^{-1}$, and the involution $\sigma_{h'}$ is the restriction of $\sigma_{h''}$ to $M_n(K(x))$ (so it is given by the same formula). The element g satisfies the equation $g\sigma_{h'}(g) = Id$ and $N_{K(x)/K}(det\ g) = 1$. Clearly, g lies in the group $O^+(h'')$ since

$$O^+(h'') := \{f \in GL_n(D) | f\sigma_{h''}(f) = Id,\ and\ Nrd(f) = 1\}.$$

□

Let o_K be the induced map $o_K : H^1(K,G) \to H^1(K,O^+(h''))$.

Lemma 9.4.9. Kernel of the map o_K is trivial. Furthermore, if D_L is an $L-$division algebra, then kernel of the map o_L is also trivial.

Proof. Let $[\mathfrak{h}] \in \operatorname{Ker}(o_K)$. By the identification $H^1(K,G) = H^1(K(x),O^+(h'))$, we can view $\mathfrak{h}$ as a quadratic form over $K(x)$ which is isometric to the hermitian form h'' after extending the scalars from $K(x)$ to D. This in particular means that $\mathfrak{h}$ is a unit quadratic form by Theorem 7.3.6. By [15, Theorem 2.12], $\overline{\mathfrak{h}} \cong \overline{h''}$ as unitary hermitian forms over $(k(\overline{x}),\overline{\tau_y})$. Note that the field $k(\bar{x})$ is element-wise invariant under the involution $\overline{\tau_y}$, so we can view both $\overline{\mathfrak{h}}$ and $\overline{h''}$ as quadratic forms over $k(\overline{x})$.

By Springer's decomposition theorem for quadratic forms, we have $\mathfrak{h} \cong h'$ over $K(x)$. Therefore $\operatorname{Ker}(o_K)$ is trivial.

A similar argument works for o_L, if D_L is an $L-$division algebra. □

Since $G = R_{K(x)/K}(O^+(h'))$, we have $C(G) = R_{K(x)/K}(C(O^+(h'))) = R_{K(x)/K}(\mu_2)$ and $|C(G)| = 4$. Also $G(K(x)) = O^+(h')(K(x)) \times O^+(\widetilde{h'})(K(x))$ (direct product), where $\widetilde{h'} =< \beta_1 - \gamma_1 x, \dots, \beta_n - \gamma_n x >$. Over the algebraic closure G is isomorphic to the direct product of two copies of ${O_n}^+$ and the center of each of these components is μ_2.

Let G' be the preimage of the group G under the morphism $Spin(h'') \longrightarrow O^+(h'')$:

$$\begin{array}{ccccc} & & 1 & & 1 \\ & & \downarrow & & \downarrow \\ & & \mu_2 & \xrightarrow{id} & \mu_2 \\ & & \downarrow & & \downarrow \\ 1 & \longrightarrow & G' & \longrightarrow & Spin(h'') \\ & & \downarrow & & \downarrow \\ 1 & \longrightarrow & G & \longrightarrow & O^+(h'') \\ & & \downarrow & & \downarrow \\ & & 1 & & 1 \end{array}$$

Over the algebraic closure, we denote by ${O_m}^+$, $Spin_m$, and C_m the special orthogonal group, the spinor group, and the even Clifford algebra of any $m-$ dimensional quadratic form, respectively (for any $m \in \mathbb{N}$). We have $G(\overline{K}) \cong {O_n}^+(\overline{K}) \times {O_n}^+(\overline{K})$. The pre-image of each component ${O_n}^+$ of G under the map $Spin_{2n} \to {O_{2n}}^+$ is $Spin_n$. So there is a surjective map $Spin_n \times Spin_n \to G'$ which means that G' is an almost direct product of two copies of $Spin_n$, i.e., $G' = Spin_n \cdot Spin_n$. The kernel of the map $Spin_n \times Spin_n \to G'$ consist of all pairs (w, w^{-1}) where w is an element in the intersection of the two components $Spin_n$. Let us view such an element (w, w^{-1}) in C_{2n}. The element w then belongs to each component C_n of the product $C_n \cdot C_n$ inside C_{2n}, but we know that the two copies of C_n have only the scalars in common. Furthermore, based on the explicit realization of elements in the even Clifford algebra (see [3, Section 2.2] and [2, Corollary 4.10.19]), the only scalars which belong to each component $Spin_n$ are the elements in μ_2. In conclusion, the intersection of the two components $Spin_n$ in the almost direct product $Spin_n \cdot Spin_n$ is μ_2. The center of G' is isomorphic to the almost direct product of $C(Spin_n)$ with itself, the intersection being μ_2. Hence $C(G')$ is an abelian group of order 8 (Note that $|C(Spin_n)| = 4$) containing $Z = C(Spin(h''))$. Finally we get the following diagram, whose vertical arrows are inclusion and the rows are exact:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_2 & \longrightarrow & Z & \longrightarrow & \mu_2 & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & Spin(h'') & \longrightarrow & O^+(h'') & \longrightarrow & 1
\end{array}$$

Note that G and G' are both semisimple (in particular connected), because of their structure as direct or almost direct products of semisimple groups over the algebraic closure. Also the inclusion $\mu_2 \to G$ is induced via the diagonal embedding of μ_2 into the center of G (over the algebraic closure), i.e.,

$$\mu_2 \to R_{K(x)/K}(\mu_2) = C(G) \to G.$$

Lemma 9.4.10. The H^1- variant of the norm principle holds for the pair (Z, G') over L/K.

Proof. Let

$$\overline{h'} :=< \overline{\beta_1 + \gamma_1 x}, \dots, \overline{\beta_n + \gamma_n x} >$$

be the residue quadratic form over $k(\overline{x})$. By our assumption, the H^1-variant of the norm principle holds for the pair $(C(Spin(\overline{h'})), Spin(\overline{h'}))$ over $k(\overline{x})$. By [4, Theorem 5.1], the H^1-variant of the norm principle holds for the pair $(C(Spin(h')), Spin(h'))$ over $K(x)$. Then the proof of Theorem 4.3.1 ($2 \implies 1$) shows that the H^0- variant of the norm principle holds for the group $\Omega(h')$ over $K(x)$; this is obtained by assuming that the reductive and the semisimple groups in the proof of Theorem 4.3.1 are $\Omega(h')$ and $Spin(h')$, respectively. By [1, Lemma 2.6], the H^0- variant of the norm principle holds for the group $R_{K(x)/K}(\Omega(h'))$ over K. The same argument as in the proof of Theorem 4.3.1 ($1 \implies 2$) shows that the H^1- variant of the norm principle holds for the pair $(C(R_{K(x)/K}(Spin(h'))), R_{K(x)/K}(Spin(h')))$ over K. Note that the group $R_{K(x)/K}(Spin(h'))$ is the commutator subgroup of $R_{K(x)/K}(\Omega(h'))$:

$$R_{K(x)/K}(Spin(h')) = R_{K(x)/K}([\Omega(h'), \Omega(h')]) = [R_{K(x)/K}(\Omega(h')), R_{K(x)/K}(\Omega(h'))].$$

By Lemma 4.4.3, the H^1- variant of the norm principle holds for the pair $(C(G'), G')$ over K, since $R_{K(x)/K}(Spin(h'))$ is the simply connected cover of G' (this follows from the covering $Spin(h'') \to O^+(h''))$. Since $C(G')$ contains Z, by applying Lemma 4.4.1 we obtain the H^1- variant of the norm principle for the pair (Z, G') over K, in particular over L/K. □

Lemma 9.4.11. The H^1- variant of the norm principle holds for the pair (μ_2, G) over L/K.

Proof. Scharlau's norm principle for quadratic forms states that the H^0- variant of the norm principle holds for the group $GO(h')$ over $K(x)$. By [1, Lemma 2.6], the H^0- variant of the norm principle holds for the group $R_{K(x)/K}(GO(h'))$ over K.

Repeating the argument in the proof of Theorem 4.3.1 (by assuming that the reductive group and the semisimple group in the proof of Theorem 4.3.1 are $R_{K(x)/K}(GO(h'))$ and $G = R_{K(x)/K}(O^+(h'))$ respectively), we obtain the H^1- variant of the norm principle for the pair $(C(G), G)$ over K; note that the group G is the commutator subgroup of $R_{K(x)/K}(GO(h'))$:

$$G = R_{K(x)/K}(O^+(h')) = R_{K(x)/K}([GO(h'), GO(h')]) = [R_{K(x)/K}(GO(h')), R_{K(x)/K}(GO(h'))].$$

Since $C(G)$ contains $\mu_2 = C(O^+(h''))$, by applying Lemma 4.4.1 we conclude that the H^1- variant of the norm principle holds for the pair (μ_2, G) over K, in particular over L/K. □

We split the rest of the argument is case 4.2 into two subcases:

Subcase 4.2.1, when D_L is an $L-$ division algebra.

Proof of the main theorem in subcase 4.2.1:

Proof. Recall that it is enough to show the norm principle for the pair $(Z, Spin(h''))$ over L/K. Consider the following diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_2 & \longrightarrow & Z & \longrightarrow & \mu_2 & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & Spin(h'') & \longrightarrow & O^+(h'') & \longrightarrow & 1
\end{array}$$

Now we apply Lemma 8.5.1: Put
$G_1 := \mu_2$

$G_2 := Z$
$G_3 := \mu_2$
$G_4 := G'$
$G_5 := G$
$G_6 := Spin(h'')$
$G_7 := O^+(h'')$

We need to show that conditions (a),(b),(c), and (d) are satisfied:

(a) We know that $u \in \mathrm{Ker}(o_L \circ \chi_L \circ g_L)$, and $\mathrm{Ker}(o_L)$ is trivial by Lemma 9.4.9. Therefore, $u \in \mathrm{Ker}(\chi_L \circ g_L)$.

(b) This was proved in Lemma 9.4.11.

(c) It is equivalent to Knebusch norm principle for qaudratic forms.

(d) This was proved in Lemma 9.4.10.

□

Subcase 4.2.2, when D_L is split.

When D_L splits then $L \cong K(x)$, the unique unramified field extension of K in D_K (see Lemma 8.1.2). Once we fix an isomorphism $D_L \cong M_2(L)$, we have a Morita correspondence between m dimensional hermitian forms over D_L (with respect to the involution τ_y) and $2m$ dimensional quadratic forms over L, up to scalars in L, for any $m \in \mathbb{N}$. Recall that

$$h'' =< \beta_1 + \gamma_1 x, \dots, \beta_n + \gamma_n x > .$$

Under Morita equivalence, the one dimensional hermitian form $< \beta_i + \gamma_i x >$ corresponds to the quadratic form $\theta < \beta_i + \gamma_i x, -(\beta_i - \gamma_i x)\pi >$ for a scalar $\theta \in L$. Since Morita equivalence respects direct sums, the form h'' corresponds to the quadratic form $\mathfrak{h} := \theta h' \perp (-\theta\pi\widetilde{h'})$ over L. The element λ is a multiplier for h over L, so it is a multiplier for h'' over L as well. The hermitian form $h'' \perp (-\lambda h'')$ is hyperbolic over L, hence the quadratic form $\mathfrak{h} \perp (-\lambda\mathfrak{h})$ is hyperbolic over L (again, because Morita equivalence respects scalar products, orthogonal sums, and hyperbolicity). So λ is a multiplier for $\mathfrak{h}$ over L, and therefore it is also a multiplier for the quadratic form $\theta^{-1}\mathfrak{h} = h' \perp (-\pi\widetilde{h'})$. We have the L-isometry of quadratic forms

$$h_L{}' \perp (-\pi\widetilde{h_L{}'}) \cong \lambda h_L{}' \perp (-\lambda\pi\widetilde{h_L{}'}).$$

We split the rest of the proof in subcase 4.2.2 into two parts: when λ is a uniformizer of L, and then the case that λ is a unit in L.

Subcase 4.2.2.1, when λ is a uniformizer of L.

Proof of the main theorem in subcase 4.2.2.1:

Proof. By Springer's decomposition theorem we have $-\pi\widetilde{h_L}' \cong \lambda h_L'$, hence $\mathfrak{h}_L \cong < 1, \lambda > \otimes(\theta h_L')$ and $PGO^+(\mathfrak{h})(L)$ is R-trivial by [4, Lemma 4.2]. Therefore $PGO^+(h'')(L)$ and $PGO^+(h)(L)$ are also R–trivial and we are done by Theorem 5.1.2.

□

Subcase 4.2.2.2, when λ is a unit in L.

Proof of the main theorem in subcase 4.2.2.2:

Proof. By Springer's decomposition theorem we have the following L isometries of quadratic forms:

$$h_L' \cong \lambda h_L' \quad \text{and} \quad \widetilde{h_L}' \cong \lambda \widetilde{h_L}'.$$

Recall that it is enough to show the norm principle for the pair $(Z, Spin(h''))$ over L/K. Consider the following diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_2 & \longrightarrow & Z & \longrightarrow & \mu_2 & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & Spin(h'') & \longrightarrow & O^+(h'') & \longrightarrow & 1
\end{array}$$

Now we apply Lemma 8.5.1: Put
$G_1 := \mu_2$
$G_2 := Z$
$G_3 := \mu_2$
$G_4 := G'$
$G_5 := G$
$G_6 := Spin(h'')$
$G_7 := O^+(h'')$

We need to show that conditions (a),(b),(c), and (d) are satisfied:

(a) The image of $[\lambda]$ under the following map

$$\chi_L : H^1(L, \mu_2) \to H^1(L, G) = H^1(L, O^+(h')) \times H^1(L, O^+(\widetilde{h}'))$$

is the pair $([\lambda h'], [\lambda \widetilde{h}']) = ([h'], [\widetilde{h}']) = 1 \in H^1(L, G)$. So $u \in \mathrm{Ker}(\chi_L \circ g_L)$.

(b) This was proved in Lemma 9.4.11.

(c) It is equivalent to Knebusch norm principle for quadratic forms.

(d) This was proved in Lemma 9.4.10.

□

By analyzing cases 1, 2, 3, and 4 in this chapter, we have completed the proof of the main theorem, i.e., Theorem 8.0.1.

9.5 Applications and open questions

We now discuss a consequence of the main theorem of this dissertation (Theorem 8.0.1). As mentioned in Section 1.2, the norm principle for spinor groups $Spin(h)$ is known when the skew-hermitian form h is defined over a field k where k is a number field, finite field, or local field. Consider the affine curve $\mathbb{A}^1$ defined over k, with function field $k(t)$. The completion of the field $k(t)$ with respect to the $t-$adic valuation is $k((t))$, the field of formal Laurent series, which is a complete discretely valued field with residue field k. Using the main theorem (Theorem 8.0.1) and by induction, we conclude the following:

Theorem 9.5.1. Let k be a number field, finite field (of charactersitic different from 2), or local field, and $K = k((t_1))\cdots((t_n))$. Let (D, τ) be a quaternion algebra with symplectic involution defined over K, and h be a skew-hermitian form defined over (D, τ). Then the norm principle holds for the group $Spin(h)$.

Even though the norm principle looks like a technical statement, it provides us with a powerful tool to deal with the behavior of algebraic groups under extensions of the base field. For example, Gille used the norm principle to prove the following statement: if G is a group of type E_6 or E_7 which is split over coprime degree extensions of the base field, then G is split itself. The norm principle for $GL_1(D)$, where D is a central simple algebra, was used by Parimala while working with H^3. The Tits-Weiss conjecture and the Kneser-Tits conjecture for some groups of type E_7 and E_8 was proved by Alsaody, Chernousov, and Pianzola, where the norm principle was used. Lastly, using the norm principle one can give a short alternative proof of the Bayer-Lenstra theorem on hyperbolicity of hermitian or skew-hermitian forms.

We end the dissertation with some related open questions:

- Let k be a number field, C be a smooth projective curve defined over k, and q be a quadratic form defined over the function field $k(C)$. Does the norm principle hold for $Spin(q)$ over $k(C)$?

- Let K be a complete discretely valued field with residue field k and $char\ k \neq 2$. Assume that the norm principle holds for $Spin(h_1)$ for every regular skew-hermitian form h_1 over any central simple algebra with symplectic involution (D_1, τ_1) defined over any finite extension of k. Does the norm principle hold for $Spin(h)$ for every regular skew-hermitian form h over any central simple algebra with symplectic involution (D, τ) over K?

  An affirmative answer to the above question generalizes the main result of this dissertation to spinor groups of skew-hermitian forms over arbitrary central simple algebras.

- Let K be a complete discretely valued field with residue field k. Assume that the norm principle holds for every semisimple linear algebraic group defined over any finite extension of k. Does the norm principle hold for all semisimple linear algebraic groups defined over K?

- In the norm principles, the statements are about the inclusion of some sets in other sets. When do we obtain equalities? More precisely, what can we say about the inclusions of these sets? For example, in the H^0 -variant of the norm principle (see Definition 1.2.1), is it possible to characterize $\mathrm{Im}(N_{L/K} \circ f_L)$ in $\mathrm{Im}\, f_K$?

Bibliography

[1] P. Barquero and A. Merkurjev, *Norm principle for reductive algebraic groups*, Algebra, arithmetic and geometry, Part I, II (Mumbai, 2000), Tata Inst. Fund. Res. Stud. Math., vol. 16, Tata Inst. Fund. Res., Bombay, 2002, pp. 123–137. MR 1940665

[2] Grégory Berhuy, *An introduction to Galois cohomology and its applications*, London Mathematical Society Lecture Note Series, vol. 377, Cambridge University Press, Cambridge, 2010, With a foreword by Jean-Pierre Tignol. MR 2723693

[3] Nivedita Bhaskhar, *R-equivalence and norm principles in algebraic groups*, ProQuest LLC, Ann Arbor, MI, 2016, Thesis (Ph.D.)–Emory University. MR 3593322

[4] Nivedita Bhaskhar, Vladimir Chernousov, and Alexander Merkurjev, *The norm principle for type D_n groups over complete discretely valued fields*, Trans. Amer. Math. Soc. **372** (2019), no. 1, 97–117. MR 3968764

[5] Armand Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991. MR 1102012

[6] V. Chernousov and A. Merkurjev, *R-equivalence and special unitary groups*, J. Algebra **209** (1998), no. 1, 175–198. MR 1652122

[7] Antonio J. Engler and Alexander Prestel, *Valued fields*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005. MR 2183496

[8] Philippe Gille, *La R-équivalence sur les groupes algébriques réductifs définis sur un corps global*, Inst. Hautes Études Sci. Publ. Math. (1997), no. 86, 199–235 (1998). MR 1608570

[9] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. MR 2266528

[10] James E. Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics, No. 21, Springer-Verlag, New York-Heidelberg, 1975. MR 396773

[11] Nikita A. Karpenko, *Hyperbolicity of orthogonal involutions*, Doc. Math. (2010), no. Extra vol.: Andrei A. Suslin sixtieth birthday, 371–392, With an appendix by Jean-Pierre Tignol. MR 2804259

[12] Max-Albert Knus, *Quadratic and Hermitian forms over rings*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 294, Springer-Verlag, Berlin, 1991, With a foreword by I. Bertuccioni. MR 1096299

[13] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998, With a preface in French by J. Tits. MR 1632779

[14] T. Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, RI, 2005. MR 2104929

[15] Douglas W. Larmour, *A Springer theorem for Hermitian forms*, Math. Z. **252** (2006), no. 3, 459–472. MR 2207754

[16] A. S. Merkurjev, *R-equivalence and rationality problem for semisimple adjoint classical algebraic groups*, Inst. Hautes Études Sci. Publ. Math. (1996), no. 84, 189–213 (1997). MR 1441008

[17] Yevsey A. Nisnevich, *Espaces homogènes principaux rationnellement triviaux et arithmétique des schémas en groupes réductifs sur les anneaux de Dedekind*, C. R. Acad. Sci. Paris Sér. I Math. **299** (1984), no. 1, 5–8. MR 756297

[18] Alex Ondrus, *Minimal anisotropic groups of higher real rank*, Michigan Math. J. **60** (2011), no. 2, 355–397, With an appendix by V. Chernousov and A. Merkurjev. MR 2825267

[19] Vladimir Platonov, Andrei Rapinchuk, and Igor Rapinchuk, *Algebraic groups and number theory. Vol. I*, Cambridge Studies in Advanced Mathematics, vol. 205, Cambridge University Press, Cambridge, [2023] ©2023, Second edition [of 1278263], The translation of the first Russian edition was prepared by Rachel Rowen. MR 4615820

[20] Winfried Scharlau, *Quadratic and Hermitian forms*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 270, Springer-Verlag, Berlin, 1985. MR 770063

[21] Jean-Pierre Serre, *Galois cohomology*, english ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, Translated from the French by Patrick Ion and revised by the author. MR 1867431

[22] Jean-Pierre Tignol and Adrian R. Wadsworth, *Value functions on simple algebras, and associated graded rings*, Springer Monographs in Mathematics, Springer, Cham, 2015. MR 3328410

[23] Adrian R. Wadsworth, *Extending valuations to finite-dimensional division algebras*, Proc. Amer. Math. Soc. **98** (1986), no. 1, 20–22. MR 848866

[24] William C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York-Berlin, 1979. MR 547117