Springer's Theorem and Its Analogues

Rahul Kumar Choudhary

Department of Mathematical Science

Indian Institute of Science Education and Research Mohali

April 2014

Certificate of Examination

This is to certify that the dissertation titled **Springer's Theorem and its Analogues** submitted by **Rahul Kumar Choudhary** (Reg. No. MS09102) for the partial fulfillment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Prof. Sudesh K. Khanduja   Dr. Mahender Singh   Dr. Amit Kulshrestha
(Supervisor)

Dated: April 25, 2014

Declaration

The work presented in this dissertation has been carried out by me under the guidance of **Dr. Amit Kulshrestha** at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due reference to the literature, and acknowledgement of collaborative research and discussions.

Rahul Kumar Choudhary
(Candidate)
: April 25, 2014

In my capacity as the supervisor of the candidate's project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Dr. Amit Kulshrestha
(Supervisor)
Dated: April 25, 2014

Acknowledgment

I am jubilant to see that my final year project work has came through. In this regard, I would like to thank my Project supervisor Dr. Amit Kulshrestha for giving me the opportunity to work under his guidance, introducing me to the topic and supporting me morally. The topic has really been worth this hard work.

I would also like to thank Prof. Sudesh Kaur Khanduja and Dr. Mahender Singh for his valuable suggestions. I would also express my gratitude towards institute facilities and such a nice environment for research work.

I would be ungrateful to not include my family members who always supported me emotionally with their encouraging and motivational words. I would not forget to thank my friends Iswarya, Jyosmita, Rahul, Amit, Leena and Saksham who backed me up throughout.

Rahul Kumar Choudhary

Notation

$\mathbb{R}$	Field of real numbers
$\mathbb{Z}$	Ring of integers
$\mathbb{Q}$	Field of rational numbers
$\mathbb{H}$	Hyperbolic space
q	Quadratic form
b	Bilinear form
h	Hermitian form
s	Sesquilinear form
$D(q)$	Elements represented by q
A	Algebra
D	Division algebra
H	Quaternion algebra
$*$	Involution on a ring
σ	Involution on an algebra
$k(C)$	Function field associated to the conic C
$k((t))$	Field of formal Laurent series over field k

Abstract

In the algebraic theory of quadratic forms a fundamental result due to Springer was given in 1952. Let k be a field with $char k \neq 2$, Springer proved that if a quadratic form q over k acquires an *isotropy* in odd degree extension of k then q has an isotropy over k. Springer's theorem has been generalized in various way, similar problems have been posed for hermitian forms over finite dimensional central simple algebra over k with involutions. The weak version of Springer's theorem for hermitian forms was proved by Bayer-Fluckiger and Lenstra [3]. The strong version of Springer's theorem for hermitian forms is still an open question. We will see an example of anisotropic hermitian form over central division algebra with involution of type of second kind(unitary involution) which becomes isotropic over an odd degree extension.

Contents

Chapter 1

Quadratic and Bilinear Forms

The study of bilinear forms was arised due to classification of matrices over a field k. The classification of alternating and symmetric matrices can be parametrized by bilinear forms. If A and B are matrices then they are congruent if $A = P^T BP$ for some invertible matrix P. To study the congruence class of matrices and diagonalization can be reduced to bilinear forms. The study of quadratic forms arose from the investigation of homogeneous polynomial of degree 2. We will use a coordinate free approach to study these forms. In this chapter we are assuming that $char k \neq 2$.

1.1 Bilinear forms

Definition Let V be a finite dimensional vector space over a field k. A *bilinear form* on V is a map $b : V \times V \to k$ satisfying for all $v, v', w, w' \in V$ and $c \in k$,

$$b(v + v', w) = b(v, w) + b(v', w);$$
$$b(v, w + w') = b(v, w) + b(v, w');$$
$$b(cv, w) = cb(v, w) = b(v, cw).$$

The bilinear form is called *symmetric* if $b(v, w) = b(w, v)$ for all $v, w \in V$ and is called *alternating* if $b(v, v) = 0$ for all $v \in V$. If b is an alternating form, expanding $b(v+w, v+w)$ shows that b is *skew symmetric*, i.e. $b(v, w) = -b(w, v)$ for all $v, w \in V$.

We define the *dimension of the bilinear form* to be the integer $\dim(V)$. We write it as $\dim(b)$. We say that b is a bilinear form over k if b is a bilinear form on a finite dimensional vector space over k and the vector space which supports b is denoted by V_b.

Definition Let $V^* := \mathrm{Hom}_k(V, k)$ denote the dual space of V. A bilinear form b on V is called *nondegenerate* if $l : V \to V^*$ defined by $v \mapsto l_v : w \mapsto b(v, w)$ is an isomorphism.

Let b be a bilinear form on V and $\{v_1, v_2, v_3, \cdots, v_n\}$ be a basis for V. Then b is determined by the matrix $(b(v_i, v_j))$ and the form is nondegenerate if and only if $(b(v_i, v_j))$ is invertible. Conversely any matrix B in the $n \times n$ matrix ring $M_n(k)$ determines a bilinear form on V.

Definition An *isometry* f between two bilinear forms b_i, $i = 1,2$, is a linear isomorphism

$$f : V_{b_1} \to V_{b_2}$$

such that

$$b_1(v, w) = b_2(f(v), f(w)) \text{ for all } v, w \in V_{b_1}.$$

If such an isometry exists, we write $b_1 \simeq b_2$ and say that b_1 and b_2 are *isometric.*

1.2 Structure theorem on Bilinear forms

Let b be a symmetric or alternating bilinear form on V. We say $v, w \in V$ are *orthogonal* if $b(v, w) = 0$. Let $W, U \subset V$ be subspaces. Define the *orthogonal complement* of W by

$$W^\perp := \{v \in V \mid b(v, w) = 0 \text{ for all } w \in W\}.$$

This is a subspace of V. We say W is *orthogonal* to U if $W \subseteq U^\perp$, equivalently $U \subseteq W^\perp$. If $V = W \oplus U$ is a direct sum of subspaces with $W \subseteq U^\perp$, we write $b = b\mid_W \perp b\mid_U$ and say b is the *(internal) orthogonal sum* of $b\mid_W$ and $b\mid_U$.

Definition The subspace $V^\perp$ is called the *radical* of b and denoted by *rad b*. The orthogonal complement of V itself is called *"radical"* of (V, b) and is denoted by $radV = V^\perp$.

The form b is nondegenerate if and only if $rad\ b = 0$.

If K/k is a field extension, let $V_K := K \otimes_k V$, a vector space over K. We have the standard embedding $V \to V_K$ by $v \mapsto 1 \otimes v$. Let b_K denote the extension of b to V_K, so $b_K\ (a \otimes v, c \otimes w) = acb(v, w)$ for all $a, c \in K$ and $v, w \in V$. The form b_K is of the same type as b. Moreover, $radb_K = (radb)_K$, hence b is nondegenerate if and only if b_K is nondegenerate.

Let q be a quadratic form on V. We say that q is *totally singular* if its polar form b_q is zero. If $chark \neq 2$, then q is totally singular if and only if q is the zero quadratic form. If $chark = 2$ this may not be true. Define the *quadratic radical* of q by

$$rad(q) := \{v \in radb_(q) \mid q(v) = 0\}.$$

This is a subspace of $rad(b_q)$. We say that q is regular if $rad(q) = 0$. If $chark \neq 2$, then $rad(q) = rad(b_q)$. In particular, q is regular if and only if its polar form is non-degenerate. If $chark = 2$, this may not be true.
By above definition we have a result that every anisotropic quadratic form is regular. So we can conclude that the bilinear space (V, b) is regular. $\Leftrightarrow$ rad V = 0.

Proposition 1.1. *Let b be a symmetric or alternating bilinear form on V. Let W be a subspace such that $b\mid_W$ is nondegenerate. Then $b = b\mid_W \perp b\mid_{W^\perp}$. In particular, if b is also nondegenerate, then so is $b\mid_{W^\perp}$.*

For proof see [4] (chapter 1).

Corollary 1.1. *Let b be a symmetric bilinear form on V. Then*

$$b = b\mid_{rad(b)} \perp b\mid_{V_1} \perp \cdots \perp b\mid_{V_n} \perp b\mid_W$$

with V_i a 1-dimensional subspace of V and $b\mid_{V_i}$ non-degenerate for all $i \in [1, n]$ and $b\mid_W$ a nondegenerate alternating subform on a subspace W of V.

If $chark \neq 2$, then, in the corollary 1.1, $b\mid_W$ is symmetric and alternating hence $W = \{0\}$. In particular, every symmetric bilinear form b has an *orthogonal basis*, i.e., a basis $\{v_1, ..., v_n\}$ for V_b satisfying $b(v_i, v_j) = 0$ if $i \neq j$. The form is non-degenerate if and only if $b(v_i, v_i) \neq 0$ for all i.
Let $a \in k$. Denote the bilinear form on k given by $b(v, w) = avw$ for all $v, w \in k$ by $\langle a\rangle_b$ or simply $\langle a\rangle$. In particular, $\langle a\rangle \simeq \langle b\rangle$ if and only if $a = b = 0$ or $ak^{*2} = bk^{*2}$ in k^*/k^{*2}. Denote

$$\langle a_1\rangle \perp \langle a_2\rangle \cdots \perp \langle a_n\rangle \text{ by } \langle a_1, a_2, \cdots, a_n\rangle_b \text{ or simply by } \langle a_1, a_2, \cdots, a_n\rangle.$$

We call such a form a *diagonal form.* A symmetric bilinear form b isometric to a diagonal form is called *diagonalizable.* Consequently, b is diagonalizable if and only if b has an orthogonal basis. Note that det $\langle a_1, a_2, \cdots, a_n\rangle = a_1 a_2 .....a_n\ k^{*2}$ if $\mathrm{a}_i \in k^*$ for all i. From corollary 1.1 we conclude that every bilinear form b on V satisfies

$$b \simeq \mathrm{r}\langle 0\rangle \perp \langle a_1, a_2, \cdots, a_n\rangle \perp b'$$

with $\mathrm{r} = dim(radb)$ and b' an alternating form and $a_i \in k^*$ for all i. In particular, if $char k \neq 2$, then every symmetric bilinear form is diagonalizable.

Definition Let b be a bilinear form on V over k. Let

$$D(b) := \{b(v, v) \mid v \in V \text{ with } b(v, v) \neq 0\},$$

the set on non-zero values of b and

$$G(b) := \{\mathrm{a} \in k^* \mid ab \simeq b\ \},$$

a group called *the group of similarity factors of* b. Also set

$$\overline{D(b)} := D(b) \cup \{0\}.$$

We say that elements in $\overline{D(b)}$ are *represented by b.*

Proposition 1.2. *Let b be a symmetric bilinear form. If $D(b) \neq \phi$, then b is diagonalizable. In particular, a non-zero symmetric bilinear form is diagonalizable if and only if it is not alternating.*

Corollary 1.2. *Let b be a symmetric bilinear form over k. Then $b \perp \langle 1\rangle$ is diagonalizable.*

Corollary 1.3. *Every anisotropic bilinear form is diagonalizable.*

For details of above results see [4] (chapter 1).

1.3 Introduction to Quadratic forms and matrices

An quadratic form over a field k is a polynomial f in n variables over k that is homogeneous of degree 2.

$$f(x_1, x_2, \cdots, x_n) = \sum_{i,j=1}^{n} a_{i,j} X_i X_j \in k[X_1, \cdots, X_n] = k[X].$$

for making the coefficients symmetric, we rewrite f as

$$f(X) = \sum_{i,j=1}^{n} \frac{1}{2}(a_{ij} + a_{ji}) X_i X_j$$

denote $a_{ij}^{'} = \frac{1}{2}(a_{ij} + a_{ji})$, in this way f determines uniquely a symmetric matrix $(a_{ij}^{'}$ which we shall denote by M_f. So in terms of matrix notations

$$f(X) = X^t M_f X$$

where X is viewed as a column vector.

f and g are *equivalent* n-ary quadratic forms if $(f \cong g)$ $f(x) = g(cx)$ for some $c \in GL_n(k)$. Since

$$\begin{aligned} g(cx) &= (cx)^t M_g (cx) \\ &= x^t c^t M_g c x \\ &= \mathrm{x}^t(\mathrm{c}^t \mathrm{M}_g \mathrm{c})\mathrm{x} \\ &= f(x) = x^t M_f x. \end{aligned}$$

so $M_f = c^t M_g c$.

Example 1.1. *Let $g(x_1, x_2) = x_1 x_2$ and $f(x_1, x_2) = x_1^2 - x_2^2$. clearly both quadratic forms are equivalent via mapping $x_1 \mapsto x_1 + x_2$ and $x_2 \mapsto x_1 - x_2$.*

Any quadratic form gives rise to a map $q_f : k^n \mapsto k$, defined by $q_f(x) = x^t M_f x \in k$ called *quadratic map* defined by q.
In terms of quadratic maps the notion of equivalance of forms f and g amounts to the existance of a linear automorphism C of k^n such that $q_f(x) = q_g(cx)$ for every column tuple x.
Quadratic map q_f determines uniquely the quadratic form f. If $q_f = q_g$ as maps from k^n to k then $M_f = M_g$.

Definition Let V be a finite dimensional vector space over k. A *quadratic form* on V is a map $q : V \to k$ satisfying:

1. $q(av) = a^2 q(v)$ for all $v \in V$ and $a \in k$.

2. (Polar Identity) $b_q : V \times V \to k$ defined by

$$b_q(v, w) = \frac{q(v+w) - q(v) - q(w)}{2}$$

   is a symmetric bilinear form.

The bilinear form b_q is called the *polar form* of q. We call $dim(V)$ the *dimension of the quadratic form* and also write it as $\dim q$. We write q is a quadratic form over k if q is a quadratic form on a finite dimensional vector space over k and denote the underlying space by V_q.

Let $q_b : V \to k$ be defined by $q_b(v) = b(v, v)$ for all $v \in V$. Then q_b is a quadratic form and its polar form b_{q_b} is $b + b^t$. We call q_b the *associated quadratic form of b.*

Let q_1 and q_2 be two quadratic forms. An *isometry* f is a linear map $f : V_{q_1} \to V_{q_2}$ such that $q_1(v) = q_2(f(v))$ for all $v \in V_{q_1}$. If such an isometry exists, we write $q_1 \simeq q_2$ and say that q_1 and q_2 are *isometric.*

Example 1.2. *Let $q_1 = x_1 x_2$ and $q_2 = x_1^2 - x_2^2$ be two quadratic forms over $\mathbb{R}^2$. Then q_1 and q_2 are isometric via the map $f : \mathbb{R} \to \mathbb{R}$ with $f(u, v) = (\frac{(u^2+v^2)}{2}, \frac{(u^2-v^2)}{2})$.*

Notation

1. Let $a \in k$. The quadratic form on k given by $q(v) = av^2$ for all $v \in k$ will be denoted by $\langle a \rangle_q$ or simply $\langle a \rangle$.

2. Let $a, b \in k$. The 2-dimensional quadratic form on k^2 given by $q(x, y) = ax^2 + xy + by^2$ will be denoted by $[a, b]$. The corresponding matrix for q in the standard basis is

$$A = \begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix}$$

while the corresponding matrix for b_q is

$$B = \begin{pmatrix} 2a & 1 \\ 1 & 2b \end{pmatrix}$$

$$= \text{A} + A^t.$$

1.3.1 Properties of Quadratic Forms

These are some basic properties of quadratic forms

1. $q_f(ax) = a^2 q_f(x)$.
2. *'Polarization'* of q_f is

$$b_f(x,y) = \frac{(q_f(x+y) - q_f(x) - q_f(y))}{2}$$

thus

$$= \frac{((x+y)^t M_f (x+y) - x^t M_f x - y^t M_f y)}{2}$$
$$= \frac{(x^t M_f y + y^t M_f x)}{2}$$
$$= x^t M_f y.$$

so clearly $b_f(x,y)$ is a symmetric bilinear form.
Depolarization of $b_f(x,y)$ is $q_f(x) = b_f(x,x) \; \forall \; x \in k^n$.

Let V is any finite dimensional vector space over k and b is a symmetric bilinear mapping $b : V \times V \to k$. Then we call (V,b) or (V,q) is a "*quadratic space*" and associated quadratic map is $q(x) = q_f(x) = b_f(x,x) \; \forall \; x \in k^n$.
Quadratic spaces (V,b) determines equivalance class of quadratic forms q_f.

Theorem 1.1. *The following statements are equivalent*

1. *M is a non singular matrix.*
2. *$x \mapsto b(,x)$ defines an isomorphism $V \to V^*$, where V^* denotes the dual space of V.*
3. *For $x \in V$, $b(x,y) = 0 \ \forall \ y \in V$ implies $x = 0$.*

Let S is subspace of V then $(S, b \mid_{(S\times S)})$ is also a quadratic space. Orthogonal complement of S is defined by

$$S^{\perp} = \{x \in V \mid B(x,S) = 0\}.$$

Theorem 1.2. *Let (V,b) is a regular quadratic space and S is a subspace of V. Then following holds*

1. $\dim(S) + \dim(S^{\perp}) = \dim(V)$.
2. $(S^{\perp})^{\perp} = S$.

Proof Let $q : V \to V^*$ be the linear isomorphism defined in theorem 1.1. Then $S^{\perp}$ is precisely the subspace of V annihilated by the functionals in $q(S)$.
By the usual duality theory in linear algebra, we have

$$\begin{aligned}\dim(S^{\perp}) &= \dim(V^*) - \dim(q(S))\\ &= \dim(V) - \dim(S),\end{aligned}$$

Since q is an isomorphism. This establishes (1).
Applying this twice we get

$$\dim((S^{\perp})^{\perp}) = \dim(V) - (\dim(V) - \dim(S)) = \dim(S)$$

Since $(S^{\perp})^{\perp} \supseteq S$, from this (2) follows.

1.4 Diagonalization of Quadratic forms

Definition Let q is a quadratic form over k and $d \in k^*$. Then we say that q represents d if there exists $x_1, x_2, x_3, \cdots, x_n \in k$ such that $q(x_1, x_2, \cdots, x_n) = d$.

We shall write $D(q) = D_k(q)$ to denote the set of values in k^* represented by q. If (V,q) is a quadratic space then

$$D(q) = \{d \in k^* \mid \exists v \in V \text{ such that } q_b(v) = d\}.$$

If $a, d \in k^*$ then clearly $d \in D(q) \Leftrightarrow a^2 d \in D(q)$. So $D(q)$ consists of a union of cosets of k^* modulo k^{*2}.
we shall call k^*/k^{*2} the *group of square classes* of k. $D(q)$ is a subset of group of square classes of k and it is closed under inverse as $(d^{-1}) = (d^{-1})^2 d \in D(q)$.
In general $D(q)$ is not a subgroup of k^*. $D(q)$ may not contain 1 , even if it contains then it may fail to be closed under multiplication.

Example 1.3. *Consider the quadratic form $q = x^2 + y^2 + z^2$ over $\mathbb{Q}$. Here $D(q)$ consists of (non-zero) rational numbers which are sum of three squares of rational numbers. Clearly 1,2,1/2,14 $\in D(q)$, but 1/2 $\times$ 14 $=$ 7 $\notin D(q)$.*

Hence in view of this example $D(q)$ may not be a subgroup of k^*.
If $D(q)$ is a subgroup of k^* then we say q is a *group form* over k.

1.5 Orthogonal Sums

If (V_1, b_1) , (V_2, b_2) are quadratic spaces, we may form (V, b) where $V = V_1 \oplus V_2$ and b is the pairing $V \times V \to k$, given by

$$b((x_1, x_2), (y_1, y_2)) = b_1(x_1, y_1) + b_2(x_2, y_2).$$

clearly b is symmetric and bilinear so (V, b) is a new quadratic space.
We have $b(V_1, V_2) = 0$ and $b \mid_{(V_i \times V_i)} = b_i$ for i = 1,2. So (V, b) is denoted by $V_1 \perp V_2$.

Example 1.4. *Let $q_1 = x^2 + 2y^2$ and $q_2 = 5xy - z^2$ are two quadratic forms. Then the orthogonal sum of these will be $q_1 \perp q_2 = u^2 + 2v^2 + 5xy - z^2$.*

Notation Isometry class of the 1-dimensional space corresponding to the quadratic form dx^2 is denoted by $\langle d \rangle$.

Corollary 1.4. *Let (V, b) is a quadratic space and q is quadratic form associated to b. For $d \in k^*$, $d \in D(V)$ or $D(q)$ if and only if there exists another quadratic space (V', b') together with an isometry $V \simeq \langle d \rangle \perp V'$.*

Proof If we have $V \simeq \langle d \rangle \perp V'$, then $d \in D(\langle d \rangle \perp V') = D(V)$. Conversely, suppose that $d \in D(V)$, so there exists $v \in V$ with $q(v) = d$ (where $q = q_b$). We first make a reduction to the case where V is regular. Take any subspace W such that $V = radV \oplus W = radV \perp W$. We have $D(V) = D(W)$ and W is clearly regular. We may thus assume that V itself is regular. The quadratic subspace $q.v$ is isometric to $\langle d \rangle$ and $(q.v) \cap (q.v)^{\perp} = 0$.
Since

$$dim(q.v) + dim(q.v)^{\perp} = dimV$$

By theorem 1.2, we conclude that $V \simeq \langle d \rangle \perp V'$.

Lemma 1.1. *If (V, b) is any quadratic space over k then there exists scalars* $d_1, d_2, d_3, \cdots, d_n \in k$ *such that $V \simeq \langle d_1 \rangle \perp \langle d_2 \rangle \perp \cdots \perp \langle d_n \rangle$.*

Theorem 1.3. *If (V, b) is a quadratic space and S is a regular subspace then*

1. *$V = S \perp S^{\perp}$.*

2. *If T is a subspace of V such that $V = S \perp T$ then $T = S^{\perp}$.*

for further details see [7] (chapter 1)

Corollary 1.5. *Let (V, b) be a regular quadratic space then a subspace S is regular if and only if there exists $T \subseteq V$ such that $V = S \perp T$.*

Definition *Determinant of a nonsingular quadratic form q* is defined by $d(q) = det.(M_q)\ (k^*)^2$. Where M_q is the matrix associated to the quadratic space (V, q).

If $q_1 \simeq q_2$ then $d(q_1) = d(q_2)$ and $d(q_1 \perp q_2) = d(q_1)d(q_2) \in k^*/(k^*)^2$. Let (V, b) is a regular quadratic space to the equivalance class of q. if $V \simeq \langle d_1, d_2, \cdots, d_n \rangle$ is a diagonalization of V then $d(q) = d_1 d_2 d_3 \cdots d_n (k^*)^2 = d(V)$. Note that determinant is an invariant of the isometry class of a nondegenerate bilinear form.

Definition Let k be an ordered field. A quadratic space (V, q) is called positive definite if $q(x) > 0$ for all $x \neq 0$. It is called negative definite if $q(x) < 0$ for all $x \neq 0$.

Theorem 1.4. *(Inertia theorem of Jacobi and Sylvester)*
Let (V, q) be a quadratic space over an ordered field. Then there exists $V = V^+ \perp V^-$ where (V^+, q_{V^+}) is positive and (V^-, q_{V^-}) is negative definite. The dimensions of V^+ and V^- are independent of the chosen orthogonal decomposition.

Definition Let P be an ordering of k and q a quadratic space over k. We define $sign_P(q) := dim(V^+) - dim(V^-)$. This invariant is called the signature of q.

Let $q^{'}$ be a sub-form of a quadratic form q. The restriction of q on $(V_{q^{'}})^{\perp}$ (with respect to the polar form b_q) is denoted by $q^{'\perp}$ and is called the *complementary form* of $q^{'}$ in q. If $V_q = W \oplus U$ is a direct sum of vector spaces with $W \subset U^{\perp}$, we write $q = q \mid_W \perp q \mid_U$ and call it an *internal orthogonal sum.* So $q(w+u) = q(w) + q(u)$ for all $w \in W$ and $u \in U$. Note that $q \mid_U$ is a sub-form of $(q \mid_W)^{\perp}$.

Chapter 2

Quadratic forms over Field extensions and Springer's Theorem

A basic result in Artin-Schreier theory is that an ordering on a formally real field extends to an ordering on a finite algebraic extension of odd degree, equivalently if the bilinear form $n\langle 1\rangle$ is anisotropic over k for any integer n, it remains so over any finite extension of odd degree. Witt conjectured that any anisotropic symmetric bilinear form remains anisotropic under a odd degree extension (if $char k \neq 2$). This was first shown to be true by Springer in 1952. This is in fact true without a characteristic assumption for both quadratic and symmetric bilinear forms. In this chapter we will generalize the notion of quadratic forms in field extensions and prove Springer's theorem for quadratic forms.

2.1 Isotropy and Anisotropy

Definition Let v be a nonzero vector in a quadratic space (V, b). We say that v is an *isotropic vector* if $b(v, v) = 0$. (or equivalently $q(v) = 0$) and say that v is *anisotropic* otherwise. A quadratic form (or quadratic space) is called *universal* if it represents all the nonzero elements of k.

Definition The quadratic space (V, b) is said to be *isotropic* if it contains a (non-zero) isotropic vector and is said to be *anisotropic* otherwise (anisotropic spaces are necessarily regular). We say (V, b) is *totally isotropic* if all nonzero vectors in V are isotropic (i.e. $b = 0$).

Example 2.1. *Let* $q_1 = {x_1}^2 - {x_2}^2$ *be a quadratic form on* $\mathbb{R}^2$ *over* $\mathbb{R}$*. Clearly* q_1 *is an isotropic form because* $(x_1, x_2) = (1, 1) \in \mathbb{R}^2$ *is an isotropic vector.*

Theorem 2.1. *Let* (V, q) *be a 2-dimensional quadratic space then following are equivalent*

1. V *is regular and isotropic space.*
2. V *is regular space with* $d(V)$ = *-1.*k^{*2}.
3. V *is isometric to* $\langle 1, -1\rangle$.
4. V *corresponds to the equivalence class of the binary quadratic form* x_1x_2.

For further details see [7].

2.2 Hyperbolic Plane and Hyperbolic Spaces

The isometry class of 2-dimensional quadratic space as in theorem 2.1 are called *hyperbolic planes* and are denoted by $\mathbb{H}$, an orthogonal sum of $\mathbb{H}$ will be called *hyperbolic space.*

Theorem 2.2. *If* (V, b) *is a regular quadratic space then*

1. *Every totally isotropic subspace* $U \subseteq V$ *of positive dimension* r *is contained in a hyperbolic subspace* $T \subseteq V$ *of dimension* $2r$.

2. V *is isotropic iff* V *contains a hyperbolic plane.*

3. V *is isotropic* $\Rightarrow V$ *is universal.*

For proof see [7].

Corollary 2.1. *Let* q *be a regular quadratic form and* $d \in k^*$*. Then* $d \in D(q)$ *iff* $q \perp \langle -d\rangle$ *is isotropic.*

Corollary 2.2. *Let* q_1, q_2 *be regular forms of positive dimensions then* $q = q_1 \perp q_2$ *is isotropic iff* $D(q_1) \bigcap -D(q_2) \neq \phi$.

Corollary 2.3. *For positive integer* r *following statements are equivalent*

1. *Any regular quadratic form of dimension r over field k is universal.*

2. *Any quadratic form of dimension $r+1$ over field k is isotropic.*

for details see [7] (chapter 1).

Remark 2.1. *Let q be a quadratic form on V over k. Then the associated polar form b_q is not the zero form if and only if there are two vectors v, w in V satisfying $b(v, w) = 1$. In particular, if q is a non-zero binary form, then $q \simeq [a, b]$ for some $a, b \in k$.*

Let q be a quadratic form on V over k. If $q = q_b$ for some symmetric bilinear form b, then q is isotropic if and only if b is. In addition, if $char k \neq 2$, then q is isotropic if and only if its polar form b_q is. However, if $char k = 2$, then every $0 \neq v \in V$ is an isotropic vector for b_q.

Definition If (V, b) is a bilinear space over k, define $(V, b)_K$ by

$$(V, b)_K = (V \otimes_k K, b_K)$$
$$b_K(x \otimes \alpha, y \otimes \beta) = \alpha b(x, y)\beta \ ; \ \ x, y \in V, \alpha, \beta \in K.$$

2.3 Witt's Theorems

Theorem 2.3. *(Witt's cancellation theorem) If q, q_1, q_2 are arbitrary quadratic forms then $q \perp q_1 \simeq q \perp q_2 \Rightarrow q_1 \simeq q_2$.*

Proof Let $q \perp q_1 \simeq q \perp q_2$,
Step(1) Cancellation holds if q is totally isotropic and q_1 is regular. In fact, let M_1, M_2 be the symmetric matrices associated with q_1 and q_2. The hypothesis implies that

$$\alpha = \begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix}$$

is congruent to

$$\beta = \begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix}$$

so there exists an invertible matrix

$$E = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

such that $\alpha = \mathrm{E}^t \beta \mathrm{E}$

$$\begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix} = \begin{pmatrix} A & C \\ B & D \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

$$= \begin{pmatrix} * & * \\ * & D^t M_2 D \end{pmatrix}$$

In particular, $M_1 = \mathrm{D}^t M_2 \mathrm{D}$. Since M_1 is non singular, so is D and hence M_1 and M_2 are congruent. This gives $q_1 \simeq q_2$.

Step(2) Cancellation holds if q is totally isotropic. To see this, diagonalize q_1, q_2 and assume that q_1 has exactly r zero coefficient in the diagonalization, while q_2 has exactly r zero or more. Rewriting the hypothesis, we have

$$q \perp \mathrm{r} \langle 0 \rangle \perp q_1' \simeq q \perp r \langle 0 \rangle \perp q_2'$$

since q_1' is regular, step(1) implies that $q_1' \simeq q_2'$. By tagging on r terms of $\langle 0 \rangle$. We conclude that $q_1 \simeq q_2$.

Step(3) (General case) Let $\langle a_1, a_2, \cdots, a_n \rangle$ be a diagonalization of q. Inducting on n, we are reduced to the case $n = 1$. The case $a_1 = 0$ has been handled in step(2), so we assume that $q = \langle a_1 \rangle, a_1 \neq 0$. The hypothesis now reads $\langle a_1 \rangle \perp q_1 \simeq \langle a_1 \rangle \perp q_2$. The cancellation theorem is clearly equivalent to the following result.

Theorem 2.4. *Witt's decomposition theorem Any quadratic space (V, q) splits into an orthogonal sum*

$$(V_t, q_t) \perp (V_h, q_h) \perp (V_a, q_a)$$

where V_t is totally isotropic, V_h is hyperbolic (or zero), V_a is anisotropic (" Witt decomposition"). Furthermore, the isometry types of V_t, V_h, V_a are uniquely determined.

Proof For existance take any subspace V_0 such that

$$V = rad(V) \oplus V_0 = rad(V) \perp V_0.$$

Then $V_t = rad(V)$ is totally isotropic, and V_0 is regular. If V_0 is isotropic, we may write $V_0 = V_1 \perp \mathbb{H}_1$ by theorem 2.2 where $\mathbb{H}_1 \simeq \mathbb{H}$. If V_1 is again isotropic, we may further write $V_0 = \mathbb{H}_2 \perp V_2$, where $\mathbb{H}_2 \simeq \mathbb{H}$. After a finite number of steps, we achieve a decomposition

$$V_0 = (\mathbb{H}_1 \perp \mathbb{H}_2 \perp \cdots \perp \mathbb{H}_r) \perp V_a \ (r \geq 0).$$

where $\mathbb{H}_1 \perp \mathbb{H}_2 \perp \cdots \perp \mathbb{H}_r = V_h$ is hyperbolic (or zero), and V_a is anisotropic. This proves the existence part.
To deduce the uniqueness part, suppose V has another "Witt decomposition" $V = (V_t)' \perp (V_h)' \perp (V_a)'$. Since $(V_t)'$ is totally isotropic and $(V_h)' \perp (V_a)'$ is regular, we have

$$\text{rad}(V) = \text{rad}((V_t)') \perp \text{rad}((V_h)' \perp (V_a)') = (V_t)'.$$

so $(V_t)' = V_t$. By the cancellation theorem we have now $V_h \perp V_a \simeq (V_h)' \perp (V_a)'$. Write $V_h \simeq m.\ \mathbb{H}$ (orthogonal sum of m copies of $\mathbb{H}$) and $(V_h)' \simeq m'\ \mathbb{H}$. By cancelling $\mathbb{H}$ one a time, we conclude that $m = m'$ since V_a, $(V_a)'$ are both anisotropic. After all m hyperbolic have been cancelled, we arrive at $V_a \simeq (V_a)'$. This completes the proof.

2.4 Springer's Theorem

Theorem 2.5. *Let $k \subseteq K$ be an extension of odd degree. If an quadratic form q over k is anisotropic over k, then q_K is anisotropic over K.*

Proof Suppose K/k is a counter example with $n = [K : k]$ minimal. Clearly $n>1$, and $K = k(x)$ for some x. Let $p(t) \in k[t]$ be the minimal polynomial of x over k. Since q_K is isotropic, there is an equation

$$q(g_1(t), g_2(t), g_3(t), \cdots, g_d(t)) = p(t)h(t) \in k[t].$$

where $d = \dim(q)$; $m = max_j$ $\{\deg g_j\} \leqslant n - 1$; and the g_j's are not all zero. We may assume that no irreducible polynomial $f(t)$ divides all g_j (for otherwise $f^2|h$ and we could have cancelled out f^2 from above equation). This condition means that Σ_j

$k[t].g_j(t) = k[t]$, so in particular, the g_j's, can't have a common zero in the algebraic closure $\overline{k}$ of k. Since q itself is anisotropic. The L.H.S. of above equation has degree $2m \leq 2n-2$. So $h(t)$ has odd degree $\leqslant n-2$. Now we pick any root y in closure of k of an irreducible odd degree factor of h in $k[t]$. Plugging y into that equation we see that $(g_1(y), g_2(y) \cdots g_d(y))$ is an anisotropic vector for $q_{k(y)}$. But by choice, $[k(y):k]$ is odd and $\leqslant n-2$, which contradicts the minimal choice of n. Hence q_K is anisotropic over K.

There many ways to prove Springer's theorem but the given proof can be refer to [4].

Corollary 2.4. *Let K/k be as in theorem 2.5 and let $a \in k^*$ for any quadratic form q_o over k, q_o represents a over k if and only if q_o represents a over K.*

Lemma 2.1. *Let b be an anisotropic bilinear form over k . If K/k is purely transcendental, then b_K is anisotropic.*

Proof First suppose that $K = k(t)$, the field of rational functions over k in the variable t. Suppose that $b_{k(t)}$ is isotropic. Then there exist a vector $0 \neq v \in V_{b_{k(t)}}$ such that $b_{k(t)}(v, v) = 0$. Multiplying by an appropriate non-zero polynomial, we may assume that $v \in k[t] \otimes_k V$. Write $v = v_0 + t \otimes v_1 + \cdots + t_n \otimes v_n$, with v_1 , $\cdots$,v_n $\in V$ and $v_n \neq 0$. As the t^{2n} coefficient $b(v_n, v_n)$ of $b(v, v)$ must vanish but v_n is an isotropic vector of b, a contradiction.
If K/k is finitely generated, then the result follows by induction on the transcendence degree of K over k. In the general case, if b_K is isotropic there exists a finitely generated purely transcendental extension K_0 of k in K with b_{K_0} isotropic, a contradiction. Therefore lemma is proved.

Example 2.2. *The Field Extension $\mathbb{Q}(i)$ over $\mathbb{Q}$ which has an even degree 2. The basis of $\mathbb{Q}(i)$ over $\mathbb{Q}$ is (1,i). Consider the quadratic form $f(x, y) = x^2 + y^2$. As there is no non-zero solution of $f(x, y)$ over $\mathbb{Q}$ so $f(x, y)$ is anisotropic over $\mathbb{Q}$. Clearly $f(x, y)$ is isotropic over $\mathbb{Q}(i)$ because if we take elements (non-zero) $x = 1$, $y = i$ in $\mathbb{Q}(i)$, then $f(x, y) = 0$.*

This shows that Springer Theorem is not true for even degree extensions.

Chapter 3

Central Simple Algebras and Involutions

The foundations of the theory of central simple algebras go back to the great algebraists of the dawn of the twentieth century, we merely mention here the names of Wedderburn, Dickson and Emmy Noether. We may characterize central simple algebras as those nite dimensional algebras which become isomorphic to some full matrix ring over a nite extension of the base eld. It will be shown in this chapter that the classification of in- volutions on simple algebras is almost identical with the classification of hermitian forms over division algebras. There are many interesting connections between the theory of quadratic and hermitian forms on the one hand and the theory of simple algebras and involutions on the other. After having some basic knowledge about central simple algebras and involutions on it, we will use these results in next chapter.

3.1 Central Simple Algebras

Definition A finite dimensional algebra over a field k is a k- vector space equipped with a not necessarily commutative but associative k- linear multiplication.

Definition A finite dimensional *algebra* A over a field k is called *division algebra* if each non-zero element of A has a two-sided multiplicative inverse.

Definition Centre $Z(A)$ of a k-algebra A is the k-subalgebra consisting of elements $x \in A$ satisfying $xy = yx$ for all $y \in A$. A k-algebra A is called *simple* if it has no

two-sided ideal other than 0 and A. A is *central* if centre equals k.
If an algebra is *Simple* as well as *Central*, then it is called *Central Simple algebra.*

Note that if A is a division algebra then $Z(A)$ is a field.

Example 3.1. *The field of complex numbers* $\mathbb{C}$ *is a central simple algebra over* $\mathbb{R}$.

Example 3.2. *The algebra* $M_n(D)$ *is a central simple algebra over* D *where* D *is any division algebra.*

Definition Let R be a ring. An R-module $M \neq 0$ is called simple if it has no submodules other than 0 and M. The ring R is called simple if it has no two-sided ideals other than 0 and R.

Lemma 3.1. *(Schur's lemma) If* M *is a simple* R*-module, the endomorphism ring* $A = End_R(M)$ *is a skew field.*

If A is a k-algebra and α is an invertible element of A, then $x \mapsto \alpha x \alpha^{-1}$ is an automorphism of A. Automorphisms of this kind are called inner automorphisms.

Theorem 3.1. *(Skolem, Noether) Let* A *be a central simple algebra over* k *and* B *a simple* k *-algebra. Let* $\sigma, \tau : B \to A$ *be two algebra homomorphisms. Then there exists an inner automorphism* φ *of* A *such that* $\tau = \varphi\sigma$ *.*

for proof and further details see [8].

Corollary 3.1. *If* B *is a simple subalgebra of the central simple algebra* A*, then* $\dim(A)$ *is a multiple of* $\dim(B)$.

Corollary 3.2. *If* A *is a central simple algebra over* k*, then* $\dim_k(A)$ *is a square. If* A *is a central division algebra* D *of dimension* d^2*, then the maximal commutative subfields of* D *are exactly* d*-dimensional. They coincide with their centralizers.*

Corollary 3.3. *If* A *is a central simple algebra over* k *and* K/k *a field extension then* A_K *is a central simple algebra over* K*.*

Definition If A is a central simple algebra over k, every extension field K of k such that A_K splits is called a splitting field of A.

Theorem 3.2. *Let* A *be a central simple algebra over* k *and* K *a field extension of* k *contained in* A*. If* B *denotes the centralizer of* K*, then* $A_K \sim B$*. In particular, if* A *is a skew field and* K *a maximal commutative subfield of* A*, then* K *is a splitting field.*

Theorem 3.3. *Let D be a division algebra with center k. Then there is a maximal commutative sub field which is separable over k. Every central simple algebra has a separable splitting field. Every central simple algebra over a separably closed field splits.*

Let A be an n^2-dimensional central simple algebra over k. Let K be an arbitrary splitting field and choose an isomorphism $i : A_K = A \otimes_k K \cong M(n, K)$. We consider A to be contained in A_K . For every matrix $a \in M(n, K)$ we have the characteristic polynomial

$$\chi(X, a) = \chi_K(X, a) = det(XI - a) \in K[X]$$

$$\chi(X, a) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_0.$$

Definition Let A be a central simple algebra over k. For every $a \in A$ the polynomial $\chi(X, a) \in k[X]$ is called the characteristic polynomial of a. The coefficient $(-1)^n\alpha_0$ is called the *reduced norm* of a and $-\alpha_{n-1}$ is called the *reduced trace*. We will use the notations $n(a)$ and $S(a)$ for the reduced norm and trace, respectively.

Lemma 3.2. *If $a \in A$, then $\chi(X, a)$ is independent of the choice of the splitting field and has coefficients in k.*

3.2 Quaternion Algebras

Definition For any two elements $a, b \in k^\times$, we define the *quaternion algebra* (a, b) as the 4-dimensional k-algebra with basis $\{1, i, j, ij\}$, multiplication being determined by

$$i^2 = a,\ j^2 = b, ij = -ji.$$

Example 3.3. *For $a = -1$ and $b = -1$. The algebra $(-1, -1)$ is a algebra of quaternions over $\mathbb{R}$ with basis $\{1, i, j, ij\}$ and multiplication is determined by $i^2 = -1$, $j^2 = -1$, $ij = -ji$.*

Definition The *associated conic* $C(a, b)$ of a quaternion algebra (a, b) is the projective plane curve defined by the homogeneous equation

$$ax^2 + by^2 = z^2$$

where x, y, z are the homogeneous coordinates in the projective plane $\mathbf{P}^2$.

Definition A quaternion algebra over k is called split if it is isomorphic to matrix algebra $M_2(k)$ as a k-algebra.

Lemma 3.3. *For a quaternion algebra (a, b) the following statements are equivalent*

1. *The algebra (a, b) is split.*
2. *The algebra (a, b) is not a division algebra.*
3. *The norm map $n : (a, b) \to k$ has a non-trivial zero.*
4. *The element b is a norm from the field extension $k(\sqrt{a}) \mid k$.*

The proof of above lemma is given in [9] (chapter 1). Let k be the finite field with q elements where q is odd. Then any quaternion algebra (a, b) over k is split.

Lemma 3.4. *Let (a, b) be a quaternion algebra over k. Then (a, b) is split over k if and only if $(a, b) \otimes_k k(t)$ is split over $k(t)$. where $k(t)$ is field of rational functions over k.*

A k-algebra which is isomorphic to a tensor product of two quaternion algebra over k is called *biquaternion algebra*.

3.3 Involutions on Algebras and their classifications

Definition Let R be a ring. A map $* : R \to R$ is called an *involution* if $(x + y)^* = x^* + y^*$, $(xy)^* = y^* x^*$, $x^{**} = x$ for all $x, y \in R$. The pair $(R, *)$ is called a ring with involution.

Definition Let A be an algebra over a field k, then

$$\sigma : A \to A$$

is called involution on A if

- $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$

- $\sigma(\alpha\beta) = \sigma(\beta)\sigma(\alpha)$
- $\sigma^2 = id \ \forall \ \alpha, \ \beta \in A$.

Example 3.4. *$M_n(\mathbb{R})$ is an algebra over $\mathbb{R}$. Then the map*

$$\sigma : M_n(\mathbb{R}) \to M_n(\mathbb{R})$$

given by $\sigma(A) = A^T$ is an involution on $M_n(\mathbb{R})$. Let k be a field of $char \neq 2$ and let k_s be a separable closure of k. All algebras considered in this section are assumed to be finite dimensional over k, and all modules are supposed to be of finite type. Let K be an extension of k, with $[K : k] \leq 2$.
Let A be a central simple algebra over K, and let $\sigma : A \to A$ be a k-linear involution. Suppose that k is the fixed field of σ in K. Then σ is said to be of the first kind if $K = k$, of the second kind if $[K : k] = 2$. We say that σ is a K/k-involution. Set $A_{k_s} = A \otimes k_s$. Then $A_{k_s} \simeq End_{k_s}(V)$, for some k_s vector space V. If σ is of the first kind, then the extension σ_{k_s} of σ to k is given by conjugation with a symmetric or an alternating form on V. We say that σ is of *orthogonal type* in the first case and of *symplectic type* in the second.
An involution of the second kind is also called a *unitary involution*.

Remark 3.1. *If A is a k-algebra one does not require the involution to be k-linear. However, it is obvious that any involution σ maps the center $Z(A)$ onto itself. Since $\sigma|Z(A)$ is an automorphism of order at most 2 it maps every sub field of center $Z(A)$ onto itself. Therefore $\sigma(k) = k$. We now distinguish two possibilities*

1. *$\sigma|k$ is the identity, that is σ is k-linear. In this case σ is said to be of the first kind.*
2. *$\sigma|k$ is not the identity, that is $\sigma|k$ is a non-trivial automorphism σ of k. In this case σ is σ-semilinear, that is $\sigma(\lambda x) = (\lambda)\sigma(x)$ for all $x \in A$, $\lambda \in k$. The involution is said to be of the second kind. If K denotes the fixed field of σ, we get the separable quadratic extension K/k.*

Definition Let A is an k- algebra and σ is an involution on A. We define the maps

$$tr : A \to A \text{ by } tr(x) = x + \sigma(x) \text{ for } x \in A$$
$$n : A \to A \text{ by } n(x) = x\sigma(x) \text{ for } x \in A.$$

then σ is called standard involution if the following conditions hold

1. k is fixed under σ, i.e. $fix(\sigma) \supset k$.
2. $tr(x) \in k$ and $\sigma(x) \in k$ for every $x \in A$.

Let A be a quaternion algebra over the field k. Then the conjugation involution is the only linear map $\sigma : A \to A$ such that $\sigma(1) = 1$ and $\sigma(x)x \in k$ for all $x \in A$.

Example 3.5. *If $A = M_n(\mathbb{R})$, then the transpose map is an anti-automorphism which is standard if and only if $n = 1$, the adjoint map is a standard involution for $n = 2$ but is not R-linear for $n = 3$.*

Lemma 3.5. *If (a, b) is a quaternion algebra over field k and $n(x)$ is the norm of x then $n(x.y) = n(x).n(y)$ for all $x, y \in (a, b)$.*

Theorem 3.4. *Let A be a central simple algebra of dimension n^2 over k and σ an involution. Then*

1. *If $char(k) \neq 2$ then $A = A^+ \oplus A^-$.*
2. *If σ is of the second kind, then $dim_k(A^+) = dim_k(A^-) = n^2$.*
3. *If σ is of the first kind, then either $dim_k(A^+) = (1/2)n(n+1)$ or $= (1/2)n(n-1)$. If $char(k) = 2$ one has always $dim_k(A^+) = (1/2)n(n+1)$.*

Definition Let σ be an involution of the first kind on a central simple algebra A of dimension n^2. This involution is called of *orthogonal type* if $dim(A^+) = (1/2)n(n+1)$ and *symplectic type* if $dim_k(A^+) = (1/2)n(n-1)$. (Hence in characteristic 2 only the orthogonal type occurs.) Involutions of the second kind are called *unitary*.

The theory of classification of involutions is well explained in [8] (chapter 8).

Theorem 3.5. *Let A be a central simple k-algebra admitting a K/k-involution. Let B be a simple subalgebra and let σ be a K/k-involution on B. Then σ can be extended to an involution on A.*

We can have a look at proof in [8] (chapter 8).

An involution σ on a skew field k is called of first kind if σ is the identity on $Z(k)$, the center of k. Otherwise the involution is called of second kind. In the later case $\sigma|Z(k)$ is an automorphism of order 2.

Let us define $Z_0 := \{\alpha \in Z(k) \mid \sigma(\alpha) = \alpha\}$. Thus $Z(k) = Z_0$ for involutions of the first kind and $Z(k)/Z_0$ is a separable quadratic extension for involutions of the second kind. We say in both cases that σ is an $Z(k)/Z_0$-involution. In particular, σ is a Z_0-linear map.

Chapter 4

Hermitian Analogue of Springer's Theorem

The algebraic theory of quadratic forms and hermitian forms is related in many contexts. So the question that, can the main results proved in theory of quadratic forms be generalzed also to the theory of hermitian forms? In this chapter we will have a look at generalization of Springer's theorem for hermitian forms and will give some examples where it is not true in general. For this hermitian analogue we have used the theory of Witt groups and involutions on division algebras.

4.1 Hermitian Forms

In this chapter we will use some terminology that is not defined yet in above chapters. So this chapter will begin with some definitions which will be used in order to prove some main results of hermitian analogue of Springer's theorem.

Definition *Algebraic Variety* is a set of solutions of a system of polynomial equations over reals or complex numbers. We define the *function field* of an algebraic variety V consists of objects which are interpreted as rational functions of V.

Another definition of function field is a special case of transcendental extensions of fields. For a given field k, a function field over k is a field extension K of k such that there is atleast one element $x \in K$ that is transcendental over k.

p-adic field of $char \neq 2$ is the quotient field of complete discrete valuation ring with a finite residue class field k. Therefore such type of field is either a finite algebraic extension of a field $\mathbb{Q}_p$ of p-adic numbers or a field of formal power series $k((t))$ with finite constant field k.

Field of formal Laurent series over k with coefficients from k (i.e. The set of all formal series of the form $\sum_{n \geq N} a_n t^n$ where $a_n \in k$ and $n \in \mathbb{Z}$. The ring of formal power series over k is denoted by $k[[t]]$.

In this chapter we will consider ***p-adic field*** as local field of characterstic zero.

Let k be a field and K/k is a finitely generated extension. The ***transcendence degree*** $tr.deg.(K/k)$ is defined as the cardinality of a maximal subset of elements of K algebraically independent over k, such a maximal subset is called a ***transcendence basis*** of K/k. If K is the function field of a variety V over k then dimension of V is defined to be $tr.deg.(K/k)$.

Definition Let R be a ring with an involution $*$. A sesquilinear mapping or a sesquilinear form on an R-module M is a map $s : M \times M \to R$ which satisfies the following conditions:

- $s(x + y, z) = s(x, z) + s(y, z)$,
- $s(x, y + z) = s(x, y) + s(x, z)$,
- $s(x, y\alpha) = s(x, y)\alpha$, $s(x\alpha, y) = \alpha^* s(x, y)$.

for all $x, y \in M$ and $\alpha \in R$. The transpose s^* of a sesquilinear map is defined by $s^*(x, y) = s(y, x)^*$. It is clearly sesquilinear.

Definition Let A be a central simple algebra over a field k and let M be a finitely generated right $A - module$. Suppose that $\sigma : A \to A$ is an involution on A. A ***hermitian form*** on M w.r.t. the involution σ on A is a bi-additive map

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

subject to the following conditions:

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

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

Definition The *rank* n of a hermitian form (V, h) is by definition the dimension of the D-vector space V, $n = \dim(V)$.

4.2 Witt groups

Definition Let $\epsilon = \pm 1$. An $\epsilon - hermitianform$ (V, h) over (A, σ) consists of a right A-module V and a biadditive map $h : V \times V \to A$ such that

- $h(xa, yb) = \sigma(a)h(x, y)b$
- $h(y, x) = \epsilon\sigma(h(x, y))$.

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

Let $V^* = Hom_A(V, A)$ be the dual of V. The form h induces a map $\tilde{h} : V \to V^*$ which we call the *adjoint of h.* The left A-module V^* is regarded as a right A-module through the involution σ on A. Then $\tilde{h} : V \to V^*$ is A-linear. We say that h is *nondegenerate* if $\tilde{h}$ is an isomorphism. A non-degenerate ϵ hermitian form is also called an ϵ- hermitian space.
Let (V, h) and $(V^{'}, h^{'})$ be two ϵ- hermitian forms. The *orthoqonal sum* $(V, h) \oplus (V^{'}, h^{'})$ is by definition the form $(V \oplus V^{'}, h \oplus h^{'})$, where

$$(h \oplus h^{'})(v + v^{'}, w + w^{'}) = h(v, w) + h^{'}(v^{'} + w^{'})$$

where $v, w \in V$ and $v^{'}, w^{'} \in V^{'}$.

Definition Let $\hat{W}^{\epsilon}(A, \sigma)$ be the *Grothendieck group* of the isomorphism classes of non-degenerate ϵ- hermitian forms with respect to orthogonal sums. A form (V, h) is said to be *hyperbolic* if there exists a sub A-module W of V such that $W = W^{\perp}$. The Witt group $W^{\epsilon}(A, \sigma)$ is the quotient of $\hat{W}^{\epsilon}(A, \sigma)$ by the subgroup generated by hyperbolic forms.

If $\epsilon = 1$, an ϵ- hermitian form is said to be a hermitian form, and we set $W^{\epsilon}(A, \sigma) = W(A, \sigma)$.

If $A = k$ and σ is the identity, then $W(A, \sigma)$ is the usual Witt group of non-degenerate quadratic forms, denoted by $W(k)$. We have a ring structure on $W(k)$, induced by the tensor product of quadratic forms. The ideal of even dimensional forms is denoted by $I(k)$.

The definition of hyperbolic spaces carries over in the obvious way:
If M is finitely generated, then we define

$$\mathbb{H}(M) := (M \oplus M^*, \mathbb{H}_M)$$

$$\mathbb{H} = \mathbb{H}_M : (M \oplus M^*) \times (M \oplus M^*) \to R$$

$$\mathbb{H}((x \oplus f), (y \oplus g)) = f(y) + \lambda(g(x))^*.$$

It is easily shown that $\mathbb{H}$ is actually a λ-hermitian form. In particular we have

$$\begin{aligned} \mathrm{H}((\mathrm{x} \oplus f)\alpha, (y \oplus g)) &= (f\alpha)y + \lambda g(x\alpha)^* \\ &= \alpha^*(f(y)) + \alpha^*\lambda(g(x))^* \\ &= \alpha^*\mathbb{H}((x \oplus f, y \oplus g) \\ \mathrm{H}((\mathrm{x} \oplus f), (y \oplus g)) &= (f(y) + \lambda(g(x))^*)^{**} \\ &= \lambda(g(x)) + \lambda(f(y))^*)^* \\ &= \lambda\mathbb{H}((y \oplus g), (x \oplus f))^*. \end{aligned} \tag{4.1}$$

We now define the Grothendieck group and the Witt group for hermitian forms. The orthogonal sum $(M, h) \perp (M', h') := (M \oplus M', h \oplus h')$ defines an addition on the set of isometry classes of regular λ-hermitian forms. With this operation the set of isometry classes is a semigroup. The Grothendieck group of this semigroup is denoted by $\hat{W}(R) = \hat{W}^\lambda(R, *)$. Thus its elements are the differences $[M, h] - [M', h']$, where $[M, h]$ denotes the element given by the isometry class of the space (M, h). The Witt group $W(R) = W^\lambda(R, *)$ is the factor group of $\hat{W}(R)$ by the subgroup generated by all $[\mathbb{H}(M)]$. We will denote the Grothendieck group by $\hat{W}$.

Every λ-hermitian form which can be written as $h = s + \lambda s^*$ where s is a sesquilinear form, is called even (or sometimes trace-valued). If R is commutative and $* = id$, we speak of bilinear forms, and for $\lambda = 1$ of symmetric bilinear forms, and for $\lambda = -1$ of skew symmetric bilinear forms. Even skew symmetric bilinear forms, that is those of form $b = s - s^*$ are called alternating.

Theorem 4.1. *(Pfister). The Witt group $W(K)$ and the Witt-Grothendieck group $\hat{W}(K)$ do not contain non-zero elements of odd order.*

See the proof in [8].

Let (V, h) be a non-degenerate ϵ- hermitian form over (A, σ). Let $E = End_A(V)$. Then E is a central simple algebra over K. The form h defines an involution $\tau_h : E \to E$ by $h(ex, y) = h(x, \tau_h(e)(y))$ for all $x, y \in V$ and for all $e \in E$. We call τ_h the ***adjoint involution*** of E with respect to h.

Let $H(A, \sigma)$ denote the category of non-degenerate ϵ- hermitian forms over (A, σ), with $\epsilon = \pm 1$. Let $a \in A^*$ be such that $\sigma(a) = \epsilon' a$, where $\epsilon' = \pm 1$. Then $Int(a^{-1})\sigma$ is again an involution on A. We have an equivalence of categories

$$\phi_a : H^{\epsilon}(A, Int(a^{-1})\sigma) \to H^{\epsilon\epsilon'}(A, \sigma)$$

which attaches to an ϵ- hermitian space (M, h) over $(A, Int(a^{-1})\sigma)$, the $\epsilon\epsilon'$ hermitian space (M, ah) where ah is defined by $(ah)(u, v) = ah(u, v)$.

The adjoint involutions τ_h and $\tau_{\phi(h)}$ coincide on $End_A(M)$. Further, the equivalence ϕ_a, induces an isomorphism

$$\phi_a : W^{\epsilon}(A, Int(a^{-1})\sigma) \to W^{\epsilon\epsilon'}(A, \sigma)$$

In particular, if σ and τ are two involutions of A of the same kind and type, there exists $a \in A^*$ with $\tau(a) = a$ and $\tau = Int(a^{-1})\sigma$. Therefore $\phi(a)$, induces an isomorphism

$$W(A, \tau) \simeq W(A, \sigma)$$

4.2.1 Morita equivalence

Let (V, f) be a hermitian space over (A, σ). Let $f : V \to V^*$ be the adjoint map. Let $E = End(V)$ and let τ_f be the involution induced by f. For $\alpha \in E$, we have

$$\tau_f(\alpha) = \tilde{f}^{-1}\alpha^*\tilde{f}$$

where α^* is the transpose of α. We have a left E-module structure on V which commutes with the right A-module structure. We regard V^* as a left E-module via the involution τ_f on E. Similarly, given a right E-module M, we regard M^* as a right E-module via τ_f. We have an equivalence of categories, called Morita equivalence

$$\phi_f : H(E,\tau_f) \to H(A,\sigma)$$

defined as follows :
Let (M,b) be a hermitian space over (E,τ_f). The right A-modules $M^* \otimes_E V^*$ and $Hom_A(M \otimes_E V, A)$ are identified via the map

$$(g \otimes h)(m \otimes v) = H(g(m)v)$$

for $g \in M^*, h \in V^*, m \in M$ and $v \in V$.
Set

$$\phi_f(M,b) = (M \otimes_E V, fb) \ .$$

where fb is the (A,σ) hermitian form on $M \otimes_E V$ whose adjoint $\tilde{fb}$ is $b\tilde{f} \otimes \tilde{f}$. More explicitly,

$$fb(m_1 \otimes v_1, m_2 \otimes v_2) = [\tilde{b} \otimes \tilde{f}((m_1 \otimes v_1)](m_2 \otimes v_2) = (\tilde{b}(m_1)\tilde{f}(v_1))(m_2, v_2)$$
$$= \tilde{f}(v_1)(\tilde{b}(m_1)(m_2)v_2) = f(v_1, b(m_1,m_2)v_2) \text{ for } m_1, m_2 \in M \text{ and } v_1, v_2 \in V.$$

For furhter details see [1] (section 1).

4.2.2 Exact sequence of Witt groups

Let A be a central simple algebra with an involution σ (of either kind). Let K be the centre of A and let k be the fixed field of $\sigma \mid K$. Let us assume that there exists a subfield $L \subset A$ which is a quadratic extension of K and which is stable by σ. Suppose that the restriction of σ to L is the identity if σ is of the first kind. Let $\lambda \in L$ be such that $\lambda^2 \in K$ and $L = K(\lambda)$. Let $\hat{A}$ be the commutant of L in A.

Lemma 4.1. *There exists $\mu \in A^*$ such that $\sigma(\mu) = -\mu$ and that $Int(\mu)$ restricts to the non-trivial automorphism σ_0 of L/K.*

Proof case 1 Suppose that σ is of the second kind. Let σ_1 be the restriction of σ to L. Then $\sigma_0\sigma_1$ is an automorphism of L which restricts to the non-trivial automorphism of K over k. So there exists an involution τ on A which restricts to $\sigma_0\sigma_1$ on L. There exists $\mu \in A^*$ such that $\tau = Int(\mu)\sigma$. We have $\sigma(\mu) = \epsilon\mu$ with $\epsilon \in K^*$ such that $N_{K/k}(\epsilon) = 1$. Suppose that $\epsilon \neq -1$. Let $\delta \in K^*$ such that $\epsilon = \delta^{-1}\overline{\delta}$, denoting the non-trivial automorphism of K/k. Replacing μ by $\delta^{-1}\mu$, we assume that $\sigma(\mu) = \mu$. Let $v \in \hat{A}^*$ such that $\tau(v) = -v$. Then $\sigma(v\mu) = -v\mu$. The restriction of

$Int(v\mu)$ to L is equal to the restriction of $Int(v)\tau\sigma$ to L, which is simply σ_0 by the choice of v and of τ.

case 2 Suppose that σ is of the first kind, of symplectic type, and that $[A : k] = 4$. Then A is a quaternion algebra, and we take $\mu \in A^*$ such that $\mu\lambda = -\lambda\mu, \mu^2 \in k$.

case 3 Suppose that σ is of the first kind, of orthogonal type, and that $[A : k] = 4$. Let σ_1 be the canonical involution of the quaternion algebra A. There exists $\mu \in A^*$ such that $Int(\mu)\sigma_1 = \sigma$. Then $\sigma(\mu) = -\mu = \sigma_1(\mu)$ since σ is orthogonal and $Int(\mu) \mid L = \sigma_1$.

case 4 Suppose that σ is of the first kind, and $[A : k] > 4$. Recall that $\hat{A}$ is the commutant of L in A. Then $\hat{A}$ is central over L and is non-commutative since $[A : k] > 4$. Let τ be an involution on A which extends the automorphism σ_0 of L/K. We have $\tau = Int(\mu)\sigma$ where $\mu \in A^*$ is such that $\sigma(\mu) = \pm\mu$. If $\sigma(\mu) = +\mu$, we chose $v \in \hat{A}^*$ with $\tau(v) = -v$. Then $\sigma(v\mu) = -v\mu$, and $Int(v\mu)$ restricts to σ_0 on L.

This proves the lemma.

Let $A, \sigma, K, k, L, \hat{A}, \sigma_0, \lambda$ and μ be as defined above. Let $\tau = Int(\mu)\sigma$. Then $\tau \mid L = \sigma_0$ if σ is of the first kind. We have $\tau(\mu) = -\mu$. Let $\tau_1 = \tau \mid \hat{A}$, and $\tau_2 = (Int(\mu^{-1})\tau) \mid_{\hat{A}} = \sigma \mid_{\hat{A}}$. Then τ_1 is of the second kind, and τ_2 is of the same kind as σ. Let F_σ be the fixed field of σ in L, and let F_τ be the fixed field of τ in L.

We have $A = \hat{A} \oplus \mu\hat{A}$. Let $\pi_1 : A \to \hat{A}$ be the L-linear projections $\pi_1(\alpha + \mu\beta) = \alpha, \pi_2(\alpha + \mu\beta) = \beta$, for all $\alpha, \beta \in \hat{A}$. The maps π_i induce homomorphisms

$$\pi_1 : W(A, \tau) \to W(\hat{A}, \tau_1),$$
$$\pi_2 : W^{-1}(A, \tau) \to W(\hat{A}, \tau 2).$$

We have a homomorphism

$$\rho : W(\hat{A}, \tau_1) \to W^{-1}(A, \tau)$$

induced by scalar extension of an $(\hat{A}, \tau_1)$-form multiplied by λ to an (A, τ)-form. For all $x \in A$, with $\tau_i(x) = x$, we have

$$\rho(\langle x \rangle) = \langle \lambda \rangle.$$

We then have an exact sequence

$$W(A,\tau) \to W(\hat{A},\tau_1) \to W^{-1}(A,\tau) \to W(\hat{A},\tau_2).$$

Since $\tau(\mu) = -\mu$, we have an isomorphism

$$\phi_\mu^{-1} : W^{-1}(A,\tau) \to W(A,\tau)$$

given by $\phi_\mu^{-1}(h) = \mu^{-1}h$. We replace $W^{-1}(A,\tau)$ in the above exact sequence by $W(A,\sigma)$ via φ_μ, and rewrite it as

$$(*)\ W(A,\tau) \to W(\hat{A},\tau_1) \to W^{-1}(A,\sigma) \to W(\hat{A},\tau_2).$$

where $\hat{\rho} = \phi_\mu^{-1}\rho$ and $\hat{\pi}_2 = \pi_2\phi_\mu$. Now we are referring to (*) as the exact sequence of Witt groups.

Corollary 4.1. *Let h and $h^{'}$ be two non-degenerate hermitian forms over the same free right A-module V. Then (V,h) and $(V,h^{'})$ are isomorphic.*

Let K be a field of characteristic not equal to 2. Let A be a central simple algebra over K with an involution τ (first or second kind). Assume that there exist $\lambda,\mu \in A^*$ such that $\tau(\lambda) = -\lambda$, $\tau(\mu) = -\mu$, $\mu\lambda = -\lambda\mu$ and $L = K(\lambda)$ is a quadratic extension of K. Let $\hat{A}$ be the commutant of L in A. It is easy to see that $\mu\hat{A}\mu^{-1} = \hat{A}$, $\mu^2 \in \hat{A}$, $\tau(\hat{A}) = \hat{A}$ and $A = \hat{A} \oplus \mu\hat{A}$. Let $\tau_1 = \tau \mid_{\hat{A}}$ and let τ_2 be the involution $Int(\mu^{-1})\tau_1$ on $\hat{A}$. We have the following L-linear projections

$$\pi_1 : A \to \hat{A},\ \pi_1(\alpha + \mu\beta) = \alpha$$
$$\pi_2 : A \to \hat{A},\ \pi_2(\alpha + \mu\beta) = \beta$$

for $\alpha,\beta \in \hat{A}$. If $h : V \times V \to A$ is an ϵ-hermitian space over (A,τ).
we define $h_i : V \times V \to \hat{A}$ by $h_i(x,y) = \pi_i(h(x,y))$. Then $h = h_1 + \mu h_2$. It is easily verified that h_1 is an ϵ-hermitian space over $(\hat{A},\tau_1)$ and that h_2 is a $-\epsilon$-hermitian space over $(\hat{A},\tau_2)$. For $x,y \in V$, we have the following identities:

$$h_1(x\mu,y) = -\mu^2 h_2(x,y)$$
$$h_1(x,y\mu) = \mu h_2(x,y)\mu$$
$$h_1(x\mu,y\mu) = -\mu h_2(x,y)\mu.$$

The assignments $h \mapsto h_1$ and $h \mapsto h_2$ induce homomorphisms

$$\pi_1 : W^\epsilon(A,\tau) \to W^\epsilon(\hat{A},\tau_1)$$
$$\pi_2 : W^\epsilon(A,\tau) \to W^{-\epsilon}(\hat{A},\tau_2)$$

Lemma 4.2. *Let V be an A-module and let $h_1 : V \times V \to \hat{A}$ be an ϵ-hermitian space over $(\hat{A},\tau_1)$. Define $h : V \times V \to A$ by $h(x,y) = h_1(x,y) - \mu^{-1}h_1(x\mu,y)$. Then h is an ϵ-hermitian space over (A,τ) if and only if $h_1(x,y\mu) + \mu^{-1}h_1(x\mu,y) = 0$ for all $x,y \in V$.*

Proof If h is ϵ-hermitian over (A,τ), then by (*), for $x, y \in V$, we have $h_1(x, y\mu)\mu^{-1} = \mu h_2(x,y) = -\mu^{-1}h_1(x\mu, y)$. Conversely, suppose h_1 satisfies the given condition. Using the relation $h_1(x,y) = \epsilon\tau_1(h_1(y,x))$ and $\tau\mid_{\hat{A}} = \tau_1$, it is easy to see that, for $x, y \in V$, $h(x,y) = \epsilon\tau(h(y,x))$. From the definition of h it is clear that $h(x\mu, y) = \tau(h(x,y))$ for all $x, y \in V$. Since h_1 is τ_1-semilinear in the first variable, h is τ-semilinear in the first variable. Therefore h is an ϵ-hermitian space over (A,τ). So the lemma is proved.

We now define a homomorphism

$$\rho : W^{\epsilon}(\hat{A}, \tau_1) \to W^{-\epsilon}(A,\tau)$$

Let $f : V \times V \to \hat{A}$ be an ϵ-hermitian space on $\hat{A}$.
We define $h : V \otimes_{\hat{A}} A \times V \otimes_{\hat{A}} A \to A$ as follows :
we write $V \otimes_{\hat{A}} A = V \oplus V\mu$, now for $x_1, x_2, y_1, y_2 \in V$,

$$h(x_1 \oplus y_1\mu, x_2 \oplus y_2\mu) = \lambda(f(x_1,x_2) + f(x_1,y_2)\mu + \mu f(y_1,x_2) + \mu f(y_1,y_2)\mu)$$

In other words, h is defined by λf on V and extended by sesquilinearity on $V \oplus V\mu$. The map $f \mapsto h$ yields a homomorphism

$$\rho : W^{\epsilon}(\hat{A}, \tau_1) \to W^{-\epsilon}(A,\tau).$$

Theorem 4.2. *With the notation above, the sequence*

$$W^{\epsilon}(A,\tau) \xrightarrow{\pi_1} W^{\epsilon}(\hat{A},\tau_1) \xrightarrow{\rho} W^{-\epsilon}(A,\tau) \xrightarrow{\pi_2} W^{\epsilon}(\hat{A},\tau)_2$$

For proof of theorem 4.2 see [1] (Appendix 2).

4.3 Hermitian Analogue

Proposition 4.1. *Suppose (A,σ) is a central simple k-algebra with involution and K/k is an odd degree field extension. If $(A \otimes_k K, \sigma_K)$ is hyperbolic, then (A,σ) is hyperbolic.*

This is a weak analogue of Springer's theorem but the strong version of Springer's theorem is still open.

Theorem 4.3. *Suppose (A,σ) and (B,τ) are central simple k-algebras with involution of the first kind. If $degB$ is odd and $(A,\sigma) \otimes (B,\tau)$ is hyperbolic, then (A,σ) is hyperbolic.*

Since we have some knowledge of an exact sequence of Witt groups of hermitian forms over quaternion algebras. A brief summary is given below,
Let H be a quaternion algebra over k and let τ be the canonical involution on H. Let $L = k(\lambda)$ be a maximal commutative subfiled of H, with $\lambda^2 = a \in k^*$. Let $\mu \in H$ be such that $\mu\lambda = -\lambda\mu$ and $\mu^2 = b \in k^*$. Then $H = L \oplus \mu L$. Let τ_0 be the non-trivial automorphism over L over k. We have the L-linear projections

$$\pi_1 : H \to L,\ \pi_1(\alpha + \mu\beta) = \alpha,$$
$$\pi_2 : H \to L,\ \pi_2(\alpha + \mu\beta) = \beta$$

for $\alpha, \beta \in L$. If $h : V \times V \to H$ is an ϵ - hermitian form over (H, τ), we define $h_i : V \times V \to L$, by $h_i(x, y) = \pi_i(h(x, y)$ as in the above section. Then $h = h_1 + \mu h_2$. Since $h(x\mu, y) = \sigma(\mu)h(x, y) = -\mu h(x, y)$, we have $h_2(x, y) = -b^{-1}h_1(x\mu, y)$. It is easy to see that $\pi_1(h) = h_1 : V \times V \to L$ is an ϵ-hermitian form over L and that $\pi_2(h) = h_2 : V \times V \to L$ is an $-\epsilon$-symmetric form over L. Further, π_1 and π_2 induce homomorphisms

$$\pi_1 : W^\epsilon(H, \tau) \to W^\epsilon(L, \tau_0)$$
$$\pi_2 : W^\epsilon(H, \tau) \to W^{-\epsilon}(L)$$

Let

$$\rho : W(L, \tau_0) \to W^{-1}(H, \tau)$$

be the homomorphism defined as follows :
Let $f : V \times V \to L$ be a hermitian space over (L, τ_0). Write $V \otimes_L H = V \oplus V\mu$. Define

$$\rho(f) : V \otimes_L H \times V \otimes_L H \to H$$

by

$$\rho(f)(x_1 + y_1\mu, x_2 + y_2\mu) = \lambda(f(x_1, x_2) + f(x_1, y_2)\mu + \mu f(y_1, x_2) + \mu f(y_1, y_2)\mu),$$

for $x_1, x_2, y_1, y_2 \in V$. Then we have the following

Theorem 4.4. *With the notation as above, the sequence*

$$0 \longrightarrow W(H, \tau) \xrightarrow{\pi_1} W(L, \tau_0) \xrightarrow{\rho} W^{-1}(H, \tau) \xrightarrow{\pi_2} W(L)$$

is exact.

For proof see [1]. Now we have the following lemma.

Lemma 4.3. *Let H be a quaternion algebra over a field k and let τ be the canonical involution on H. Let C be the conic associated to H and let $k(C)$ be the function field of C. Let L be a maximal commutative subfield of H. Then the sequence*

$$W(H,\tau) \xrightarrow{\pi_1} W(L,\tau_0) \longrightarrow W(L \otimes k(C), \tau_0 \otimes 1)$$

is exact.

Proof Let n_H denote the norm form of the quaternion algebra H over k and let n_L denote the norm form of the field extension L over k. We have the following identifications, for the proofs of which we refer to

$$W(H,\tau) = n_H.W(k),$$

$$W(L,\tau_0) = n_L.W(k),$$

$$W(L \otimes k(C), \tau_0 \otimes 1) = n_L.W(k(C)).$$

Since L splits H, n_L is a sub-form of n_H and $n_H W(k)$ is contained in $n_L W(k)$. With these identifications, it is easy to see that the sequence in the lemma coincides with the sequence

$$n_H.W(k) \longrightarrow n_L.W(k) \longrightarrow n_L.W(k(C)),$$

with the canonical homomorphisms. Hence to prove the lemma, it is enough to show that the above sequence is exact. By [8] (chapter 4), the kernel of the map $W(k) \to W(k(C))$ is $n_H.W(k)$. This proves the lemma.

Proposition 4.2. *Let H be a quaternion algebra over a field k and let τ be the canonical involution on H. Let C be the conic associated to H and let $k(C)$ be the function field of C. Then the canonical homomorphism*

$$W^{-1}(H,\tau) \to W^{-1}(H \otimes k(C), \tau \otimes 1)$$

is injective.

Proof For a field extension E of k, let H_E denote the quaternion algebra $H \otimes_k E$ and let τ_E denote the standard involution on H_E. We have the following commutative diagram

$$\begin{array}{ccccccc} 0 \to & W(H,\tau) & \xrightarrow{\pi_1} & W(L,\tau_0) & \xrightarrow{\rho} & W^{-1}(H,\tau) & \xrightarrow{\pi_2} & W(L) \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 \to & W(H_{k(C)},\tau_{k(C)}) & \xrightarrow{\pi_1} & W(L(C),\tau_0) & \xrightarrow{\rho} & W^{-1}(H_{k(C)},\tau_{k(C)}) & \xrightarrow{\pi_2} & W(L(C)) \end{array} \tag{4.2}$$

with exact rows (by theorem 4.4), where L and τ_0 are as in theorem 4.4. Let h be a (-1)-hermitian form over (H,τ) such that $h \otimes k(C)$ is hyperbolic over $H_{k(C)} = H \otimes k(C)$. Since $L(C) = L \otimes k(C)$ is a rational function field in one variable over L, the map $W(L) \to W(L \otimes k(C))$ is injective by [8]. Therefore, by the above diagram, there exists $f \in W(L,\tau_0)$ such that $\rho(f) = h$. Since $H \otimes k(C) \simeq M_2(k(C))$, by Morita equivalence, we have $W(H \otimes k(C), \tau \otimes 1) = W^{-1}(k(C)) = 0$. Thus, by theorem 4.4, the map $W(L \otimes k(C), \tau_0 \otimes 1) \xrightarrow{\rho} W^{-1}(H \otimes k(C), \tau \otimes 1)$ is injective. Since $h \otimes k(C)$ is hyperbolic, it follows that $f \otimes k(C)$ is hyperbolic. Therefore by lemma 4.3 there exists $h' \in W(H,\tau)$ such that $f = \pi_1(h')$. Since $\rho\pi_1 = 0$, we have $h = \rho(f) = \rho\pi_1(h') = 0$. This proves the proposition.

Corollary 4.2. *Let h be (σ,ϵ)-hermitian space over A. Then the anisotropic part of $h \otimes k(C)$ extends from k.*

Corollary 4.3. *Let H, τ are as in proposition 4.2. Let h be a (-1)-hermitian form over (H,τ). If $h \otimes k(C)$ is isotropic, then h is isotropic.*

Proof Suppose that $h \otimes k(C)$ is isotropic. Let $h \otimes k(C) = h_1 \perp h_2$, with h_1 anisotropic and h_2 hyperbolic (-1)-hermitian spaces over $(H \otimes k(C), \tau \otimes 1)$. By the "excellence result" 4.2 , there exists a (-1)-hermitian space h' over (H, τ) such that $h' \otimes k(C) = h_1$. Then $(h^{\perp} - h') \otimes k(C)$ is hyperbolic, so that by proposition 4.2 , $h^{\perp} - h'$ is hyperbolic. Since the rank of h' is strictly less than that of h, it follows that h is isotropic.

Theorem 4.5. *Let H be a quaternion algebra over a field of characteristic not equal to 2 and let σ be an involution on H. Let h be a hermitian form over (H, σ). Suppose that h is isotropic over $H \otimes_k M$ for some odd degree extension M of k. Then h is isotropic over H.*

Proof Let h be a hermitian form over (H, σ) with $h \otimes M$ isotropic for some odd degree extension M of k. Let τ be the standard involution on H.
Suppose that $\sigma = \tau$. Let V be the underlying H-vector space of h. Since $\tau(h(x,x)) = h(x,x)$ for every $x \in V$ and τ, the standard involution on H, it follows that $h(x,x) \in k$ for every $x \in V$. Thus the map $q_h : V \to k$ given by $q_h(x) = h(x,x)$ for $x \in V$ is a quadratic form over k. Clearly h is isotropic if and only if q_h is isotropic. Thus the result in this case follows from Springer's theorem for quadratic forms.
Suppose that $\sigma \neq \tau$. Let $u \in H^*$ be such that $\tau = int(u)\sigma$. Then $\tau(u) = -u$. Let $h_1 = uh$. Then h_1 is a (-1)-hermitian form over (H, τ). Moreover h is isotropic if and only if h_1 is isotropic. Let C be the conic associated to H. Since $H \otimes k(C) \simeq M_2(k(C))$, by the Morita equivalence, $h_1 \otimes k(C)$ corresponds to a quadratic form q over $k(C)$. Since $h \otimes k(C) \otimes M$ is isotropic, $q \otimes M$ is isotropic and hence q is isotropic over $k(C)$. Thus, by the Morita equivalence $h_1 \otimes k(C)$ is isotropic. By corollary 4.3 , h_1 and hence h are isotropic. This completes the proof of the theorem.

Corollary 4.4. *Let H and σ be as in theorem 4.5 . If M is an odd degree extension of k, then the canonical homomorphism*

$$W^{\epsilon}(H, \sigma) \to W^{\epsilon}(H \otimes M, \sigma \otimes id)$$

is injective.

This result was given by Bayer-Fluckiger and Lenstra.

Let A be a central simple algebra over k with an involution σ. According to Bayer-Fluckiger [3], σ is isotropic if there exists a nonzero $a \in A$ such that $\sigma(a)a = 0$. Therefore we can interpret our result in terms of isotropy of involutions.

Corollary 4.5. *Let H be as in theorem 4.5. Let $A = M_n(H)$, let $n \geq 1$, and let σ be an involution on A of first kind. If σ is isotropic in an odd degree extension of k, then σ is isotropic.*

Proof The involution σ on A corresponds to a hermitian form h over (H, σ') for some involution σ' on H of the first kind. Further, σ is isotropic if and only if h is isotropic [3] (Corollary 1.8). The corollary follows from theorem 4.5.

4.4 General aspects of hermitian analogue

In this section we have given an example of an odd degree division algebra D over a field K with an involution σ of the second kind over k and an anisotropic hermitian form h over (D, σ) which is isotropic over a degree 2 extension and over an odd degree extension of k.

Proposition 4.3. *Let k be a p-adic field containing all pth roots of unity and let F be a ramified quadratic extension of k. Then there exists a central division algebra over $F((t))$ of degree a power of p, which has an involution of the second kind.*

Let p be an odd prime number and let k be a p-adic field. Let F be a ramified quadratic extension of k. Let D be a division algebra over $F((t))$ of degree a power of p, with an involution σ of the second kind. Such a division algebra exists by proposition 4.3. Let $\lambda \in k^*$ be such that λ is not a norm from F^*. Let $h = \langle 1, -\lambda \rangle$ be the rank 2 hermitian form over (D, σ).

Theorem 4.6. *Let k, F, D, σ and h be as above. Then h is anisotropic over D, and there exist finite extensions K_1 and K_2 of $k((t))$ such that K_1 is a quadratic extension, K_2 is an extension of odd degree, and h is isotropic over $D \otimes_{k((t))} K_i$ for $i = 1, 2$. In* *particular, the group $U(h)$ of isometries of h is anisotropic over $k((t))$ and isotropic over K_1 and K_2.*

Proof Suppose that h is isotropic over D. Then, there exists $u \in D^*$ such that $\lambda = u\sigma(u)$. By taking the reduced norm on both sides, we get that λ^{p^r} is a norm from $F((t))^*$, where p^r is the degree of D. Since p is odd and $F((t))$ is a quadratic extension of $k((t))$, it follows that λ is a norm from $F((t))$. Since $\lambda \in k$, it follows that λ is a norm from a unit in $F[[t]]$. By putting $t = 0$, it is easy to see that λ is a norm from F^*, leading to a contradiction to the assumption on λ. Thus h is anisotropic over D. Let $k_1 = k(\sqrt{\lambda})$ and $K_1 = k_1((t))$. Then, clearly h is isotropic over $D \otimes_{k((t))} K_1$. Let K_2 be an extension of $k((t))$ of odd degree such that $D \otimes_{k((t))} K_2$ is a split algebra [1]. Then, by Morita equivalence $h \otimes K_2$ corresponds to a hermitian form over $F((t)) \otimes_{k((t))} K_2$, which corresponds to a quadratic form q over K_2. Since K_2 a finite extension of $k((t))$, by Hensel's lemma, every quadratic form over k_2 of rank 9 is isotropic. Since $p \geq 3$, it follows that the rank of q is at least 12 [6] (Theorem 4.6). Thus q is isotropic, and, hence, by Morita equivalence, h is isotropic. This completes the proof of the theorem.

Remark 4.1. *Let D, σ be as in theorem 4.6 and let $v \in D^*$ be such that $\sigma(v) = v$. Then the rank one hermitian form $\langle v \rangle$ over (D, σ) is anisotropic. If $p \geq 5$, then as in the theorem 4.6 , it follows that $\langle v \rangle$ is isotropic over an odd degree extension. However, there is no quadratic extension or more generally an extension of degree a power of 2, over which $\langle v \rangle$ is isotropic.*

Remark 4.2. *Let k and F be as in proposition 4.3. Then as in theorem 4.6, one can show that there exist division algebras over $F(t)$ of degrees powers of p, which have involutions of second kind. Recently, in [6], it was shown that every quadratic form over a function field in one variable over a p-adic field, $p \neq 2$, of rank at least 11 is isotropic [6] (Theorem 4.5). Using this result one can replace $k((t))$ in theorem 4.6 by $k(t)$.*

Remark 4.3. *In view of theorem 4.6, it appears that the correct analogue of Springer's theorem for hermitian form over involutorial division algebras should be the following: Let D be a central division algebra over K with a K/k-involution σ of any kind. Let n be the degree of D over K. If a hermitian form h over (D, σ) acquires an isotropy in a finite extension L of k of degree coprime with $2n$, does h have an isotropy already over k?*

In the algebraic theory of quadratic forms these type of questions will be arise in context of analogues of Springer's theorem.

Bibliography

[1] E. Bayer-Fluckiger, R. Parimala, Galois cohomology of the classical groups over fields of cohomological dimension ≤ 2, Invent. Math. (1995), 195-229.

[2] E.Bayer-Fluckiger, H.W. Lenstra, Forms in odd degree extensions and self-dual normal bases, Amer. J. Math. 112(1989), 359-373.

[3] E.Bayer-Fluckiger, D.B. Schapiro, J.P. Tignol, Hyperbolic involutions, Math. Z. (1993), 461-476.

[4] R. Elman , N. Karpenko N., A. Merkurjev *The algebraic and geometric theory of quadratic forms* 2008.

[5] R. Parimala, R. Sridharan, V. Suresh *Hermitian Analogue of a Theorem of Springer*, Journal of Algebra 243, 780-789, 2001.

[6] R. Parimala, V. Suresh, Isotropy of quadratic forms over function fields of p-adic curves, Publ. I. H. E. S. 88 (1998), 129-150.

[7] T.Y. Lam *Introduction to quadratic forms over fields*, American Mathematical Society 2000.

[8] W. Scharlau, "Quadratic and Hermitian Forms," Grundlehren der mathematischen Wissenschaften, Vol. 270, Springer-Verlag, Berlin/Heidelberg/New York, 1985.

[9] P. Gille, T. Szamuely "Central Simple Algebra and Galois Cohomology", Cambridge studies in advanced mathematics 101, Cambridge University Press, 2006.