Pfister Factor Conjecture

Parul Gupta

A dissertation submitted for the partial fulfilment of BS-MS dual degree in Science

Indian Institute of Science Education and Research Mohali
May 2012

Certificate of Examination

This is to certify that the dissertation titled "**Pfister Factor Conjecture**" submitted by **Ms. Parul Gupta** (Reg. No. MS07016) for the partial fulfilment 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.

Professor S. K. Khanduja   Dr. Chanchal Kumar   Dr. Amit Kulshrestha
(Supervisor)

Dated: May 8, 2012

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Dr. Amit Kulshrestha at 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 acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Parul Gupta
(Candidate)

Dated: May 8, 2012

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)

Acknowledgment

I am elated to see my final year project has ultimately came through. It has truly been a tryst with "Pfister Factor Conjecture". This work certainly would not have been completed without certain individuals pitching in whenever required. Firstly, I would like to thank my project supervisor Dr. Amit Kulshrestha for giving me an opportunity to work under him. He was the one who first introduced me to the topic and it was really worth the effort, learning the subject. He had very patiently worked on several drafts of the report and suggested several corrections. I am also grateful to his doctoral student Ms. Dilpreet Kaur who helped throughout the year whenever required. She took pains in drafting my thesis from the very beginning.

I am also grateful to Professor Albrecht Pfister as he was generous enough to reply my mails. I owe a especial thanks to Dr. Karim Johannes Becher who was always available through e-mail and helped me in understanding his proof of the conjecture.

It would be unfair to not include my family members who have always been my source of inspiration and backed me up whenever I felt a little low. The emotional support package also came from my friends Achyut, Rajni and Prashant. Moreover, they also helped me with the initial problems which I faced with Latex.

Finally I am thankful to IISER Mohali for providing me such a pleasant environment to work and Department of Science and Technology, India for financial support by giving me INSPIRE fellowship.

Parul Gupta

Introduction

In this expository report, the objects of our interest are quadratic forms and central simple algebras with involutions. The report contains six chapters. First three chapters are devoted to the study of algebraic theory of quadratic forms while in next two chapters we develop the theory of algebras with involutions. In last chapter we discuss a proof of Pfister Factor Conjecture due to Becher [Bec08] and a related conjecture due to Becher.

Let K be a field with characteristic different from 2 and $W(K)$ denote the Witt ring of K. An element in $W(K)$ is a class of quadratic forms represented by an anisotropic quadratic form unique up to isometry. A special class of quadratic forms is that of Pfister forms. These are the forms of the type

$$\langle 1, a_1 \rangle \otimes \langle 1, a_2 \rangle \otimes \ldots \otimes \langle 1, a_n \rangle,$$

where $a_1, a_2, \ldots, a_n \in K^*$. Pfister forms play an important role in the understanding of the structure of Witt rings. The study of Pfister forms, which Pfister himself called multiplicative forms, was initiated by Pfister in his paper [Pfi65]. One of the interesting results in the theory of Pfister forms is the following theorem:

Theorem 0.0.1. *Let φ be a quadratic form over K. Then φ is isometric to an n-fold Pfister form if and only if $\dim \varphi = 2^n$ and for every field extension L/K, φ_L is either anisotropic or hyperbolic.*

A conjecture of Becher is a version of the above theorem in a more general setting of central simple algebras with involutions. A central simple algebra over K is an algebra without non-trivial two sided ideals whose center is K. Endomorphism algebra $\mathrm{End}_K(V)$ of a K-vector space is an example of central simple algebras. On a central simple algebra an involution is an anti-automorphism of order two. In [Alb39] Albert proved the results about existence and classification of involutions on central simple algebras. An involution may not be K-linear. It is of first or second kind according as it is K-linear or not. Involutions of first kind are further classified into orthogonal and symplectic types. Scharlau [Sch85] and Knus-Merkurjev-Rost-Tignol [KMRT98] are good resources for the theory of involutions.

Given a symmetric or skew-symmetric bilinear form $\mathfrak{b} : V \times V \to K$ the equation

$$\mathfrak{b}(x, f(y)) = \mathfrak{b}(\sigma_{\mathfrak{b}}(f)(x), y);\ x, y \in V,\ f \in \mathrm{End}_K(V)$$

defines an involution $\sigma_{\mathfrak{b}}$ on $\mathrm{End}_K(V)$. The algebra $(\mathrm{End}_K(V), \sigma_{\mathfrak{b}})$ is called adjoint algebra of $\mathfrak{b}$. This is a key to connect the theory of quadratic forms with that of involutions. It is therefore natural to look for the results which are analogous in the two theories. Becher's conjecture is one such result which is analogous to theorem 0.0.1.

Becher's Conjecture *Let $(\mathcal{A}, \sigma)$ be a central simple K-algebra with involution first kind. Then the following are equivalent:*

1. $(\mathcal{A}, \sigma) \cong \bigotimes_{i=1}^{n} (Q_i, \sigma_i)$*, where* $(Q_i, \sigma_i); 1 \leq i \leq n$*, are K-quaternion algebras with involution of first kind.*
2. $\deg(\mathcal{A}) = 2^n$ *and for every field extension L/K, the L-algebra $(\mathcal{A}, \sigma)_L$ is either anisotropic or hyperbolic.*

This has been verified is for the case when $\mathcal{A}$ is Brauer equivalent to a quaternion algebra [Bec08]. A major step towards the proof of above conjecture in this special case is the following conjecture [Sha00, Chapter 9]:

Pfister Factor Conjecture *Let $n \in \mathbb{N}$ and let $(Q_1, \sigma_1), \ldots, (Q_n, \sigma_n)$ be K-quaternion algebras with involutions. If $\bigotimes_{i=1}^{n} (Q_i, \sigma_i)$ is a split K-algebra with an involution of first kind, then it is adjoint to a Pfister form.*

Therefore in the process Becher has also established Pfister Factor Conjecture. Various other versions of Pfister Factor Conjecture are available in [Sha00, Chapter 9].

This report provides a self contained description of the proof of the Pfister Factor conjecture given by Becher. In chapter 1 we start with basic notions in algebraic theory of quadratic forms. In chapter 2 we explore quadratic forms over some specific field extensions such as rational function fields, quadratic extensions, function fields of quadratic forms and quaternion algebras. Chapter 3 is dedicated to Pfister forms. In chapter 4 we recall some results for central simple algebras and in chapter 5 we define involutions and give some examples. We also record some necessary results which will be used in the proof of the conjecture. In the last chapter proof of Pfister factor conjecture due to Becher is discussed. The case when $\mathcal{A}$ is Brauer equivalent to a quaternion algebra is also explained.

Contents

Chapter 1

Introduction to Quadratic Forms

In this chapter we define some basic notions in the algebraic theory of quadratic forms. Throughout the text, K denotes a field of characteristic different from 2. In §1 we recall quadratic forms and some of their basic properties. In next section we discuss hyperbolic spaces. In the last section we recall some important theorems due to Witt and define Witt ring of a field with some examples.

1.1 Bilinear and Quadratic Forms

Definition 1.1.1 Let K be a field and V be an n-dimensional vector space over K. A *bilinear form* is a map $\mathfrak{b} : V \times V \to K$ satisfying following properties:

1. $\mathfrak{b}(\alpha v_1 + \beta v_2, w) = \alpha\mathfrak{b}(v_1, w) + \beta\mathfrak{b}(v_2, w)$,
2. $\mathfrak{b}(v, \alpha w_1 + \beta w_2) = \alpha\mathfrak{b}(v, w_1) + \beta\mathfrak{b}(v, w_2)$,

where $\alpha, \beta \in K$ and $v_1, v_2, v, w_1, w_2, w \in V$. Set of all n-dimensional bilinear forms over K is denoted by $\mathcal{B}(V)$.

Example 1.1.2 Let V be an n-dimensional vector space over K and vectors are considered to be column vectors. Let $M_n(K)$ be the set of all $(n \times n)$-matrices over K. For $A \in M_n(K)$, define $\mathfrak{b} : V \times V \to K$ by

$$\mathfrak{b}(x, y) = x^T Ay, \tag{1.1}$$

where $x, y \in V$ are indeterminate column vectors and x^T denotes transpose of x. The above defined map is bilinear as matrix multiplication distributes over addition. Let

$\mathfrak{b} \in \mathcal{B}(V)$ be a bilinear form. Then we can associate an $(n \times n)$-matrix to $\mathfrak{b}$ with respect to a given ordered basis $\boldsymbol{\beta} = \{v_1, v_2, \ldots, v_n\}$ of V as follows

$$A_{\boldsymbol{\beta}} = (\mathfrak{b}(v_i, v_j)), \text{ where } 1 \leq i, j \leq n. \tag{1.2}$$

Theorem 1.1.3. *Let V be an n-dimensional vector space over K. Let $\boldsymbol{\beta} = \{v_1, \ldots, v_n\}$ and $\boldsymbol{\gamma} = \{w_1, \ldots, w_n\}$ be two ordered basis of V. Let P be the transformation matrix from $\boldsymbol{\gamma}$ to $\boldsymbol{\beta}$. Then for any $\mathfrak{b} \in \mathcal{B}(V)$, we have $A_{\boldsymbol{\gamma}} = P^T A_{\boldsymbol{\beta}} P$.*

Proof. We have

$$A_{\boldsymbol{\gamma}} = (\mathfrak{b}(w_i, w_j))$$
$$A_{\boldsymbol{\beta}} = (\mathfrak{b}(v_i, v_j))$$

Let $P = (p_{ij})$ be the transformation matrix from $\boldsymbol{\gamma}$ to $\boldsymbol{\beta}$ coordinates. We have

$$w_i = \sum_{k=1}^{n} p_{ki} v_k, w_j = \sum_{l=1}^{n} p_{lj} v_l.$$

Since $\mathfrak{b}$ is a bilinear form we have

$$\begin{aligned} \mathfrak{b}(w_i, w_j) &= \mathfrak{b}\big(\sum_{k=1}^{n} p_{ki} v_k, \sum_{l=1}^{n} p_{lj} v_l\big) \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} p_{ki} p_{lj} \mathfrak{b}(v_k, v_l) \end{aligned}$$

Hence the identity follows. □

Definition 1.1.4 A bilinear form $\mathfrak{b} \in \mathcal{B}(V)$ is called *symmetric* if $\mathfrak{b}(x, y) = \mathfrak{b}(y, x)$ and *skew-symmetric* if $\mathfrak{b}(x, y) = -\mathfrak{b}(y, x)$ for all $x, y \in V$.

Observe that if a bilinear form is symmetric (resp. skew-symmetric) then associated matrix with respect to any basis of V is also symmetric (resp. skew-symmetric). Conversely, given a symmetric (resp. skew-symmetric) matrix we can construct a symmetric (resp. skew-symmetric) bilinear by using equation 1.1. In this chapter our main concern is about symmetric bilinear forms.

Definition 1.1.5 Let K be a field and n be a natural number. A homogeneous polynomial of degree 2 in n variables with coefficients from K is called an n-ary *quadratic form* over K. Given n mutually commutative variables $x_1, x_2, \ldots x_n$ and scalars $a_{ij} \in K$ $(1 \leq i, j \leq n)$, it can be written as follows:

$$\varphi(x_1, \ldots, x_n) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j. \tag{1.3}$$

We say (V, φ) is a *quadratic space.*

A quadratic form φ can be represented using matrices. Let x be an n-dimensional indeterminate column vector. Let $A = \left(\dfrac{a_{ij} + a_{ji}}{2}\right) \in M_n(K)$. Then

$$\varphi(x_1, \ldots, x_n) = x^T A x. \tag{1.4}$$

The matrix A is called the *associated matrix of coefficients* of φ. Observe that A is a symmetric matrix. Also note that this symmetric matrix is uniquely determined by the quadratic form φ.

Definition 1.1.6 Let φ and ψ be two n-ary quadratic forms over K. We say φ is *isometric* to ψ if there exists an invertible matrix $P \in GL_n(K)$, such that

$$\psi(x) = \varphi(Px).$$

Clearly this is an equivalence relation. Let $\varphi = x^T A x$ and $\psi = x^T B x$ be two n-ary quadratic forms over K. If φ and ψ are equivalent then there exists a $P \in GL_n(K)$ such that

$$\begin{aligned} \psi(x) &= \varphi(Px) \\ \Leftrightarrow x^T B x &= (Px)^T A (Px) \\ \Leftrightarrow x^T B x &= x^T P^T A P x \\ \Leftrightarrow B &= P^T A P. \end{aligned} \tag{1.5}$$

If φ and ψ are isometric quadratic form then we write $\varphi \cong \psi$.

Example 1.1.7 Let V be a two dimensional vector space and $x = (x_1, x_2)^T$ be a two dimensional indeterminate column vector. Let

$$\varphi = x_1^2 - x_2^2$$
$$\psi = 2x_1 x_2$$

Then

$$A_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and

$$A_\psi = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Take

$$P = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & -1 \end{pmatrix}$$

We see that

$$A_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & -1 \end{pmatrix} = P^T A_\psi P.$$

Hence φ and ψ are isometric quadratic forms as they satisfy the equation 1.5.

Let $\varphi(x) = x^T Ax$ be an n-ary quadratic form over K, where A is symmetric. Let x, y be linearly independent indeterminate vectors. We can associate a symmetric bilinear form to the given quadratic form as follows:

$$\mathfrak{b}_\varphi(x, y) = \frac{1}{2}(\varphi(x + y) - \varphi(x) - \varphi(y)) = x^T Ay = y^T Ax. \tag{1.6}$$

Conversely let $\mathfrak{b} \in \mathcal{B}(V)$ be a symmetric bilinear form. Then for a choice of basis of V we can associate a symmetric matrix to $\mathfrak{b}$. Let A_1 and A_2 be two associated matrices with respect to two different bases of V. Let $\varphi_1 = x^t A_1 x$ and $\varphi_2 = x^t A_2 x$ be two quadratic forms. From the fact that A_1 and A_2 both are associated matrices to the same bilinear for different bases it follows that φ_1 and φ_2 are isometric.

1.1.1 Orthogonal Sum

Definition 1.1.8 Let (V_1, φ_1) and (V_2, φ_2) be two quadratic spaces of dimension n_1 and n_2 over K. Let

$$V = V_1 \oplus V_2.$$

Then for $v = v_1 \oplus v_2 \in V$, we define a quadratic form $\varphi : V \to K$ as follows:

$$\varphi(v) = \varphi_1(v_1) + \varphi_2(v_2),$$

where $v_1 \in V_1, v_2 \in V_2$. The $(n_1 + n_2)$-dimensional quadratic space (V, φ) is called *orthogonal sum* of (V, φ_1) and (V, φ_2) . The quadratic form φ is written as $\varphi_1 \oplus \varphi_2$. Let A_1 and A_2 be the associated symmetric matrices of φ_1 and φ_2 respectively then associated symmetric matrix A is of the form

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

In the same manner we can define orthogonal sum of r quadratic spaces for any $r \in \mathbb{N}$.

Conversely, suppose (V, φ) is a quadratic space and $V_1, V_2, \ldots V_r$ are subspaces of V such that $\mathfrak{b}_\varphi(v_i, v_j) = 0$ for $v_i \in V_i$, $v_j \in V_j$ and $i \neq j$. Let $\varphi_i = \varphi|_{V_i}$. Then we can write

$$\varphi \cong \varphi_1 \oplus \varphi_2 \oplus \ldots \oplus \varphi_r$$

Example 1.1.9 Let $V = \mathbb{R}^2$ and $\varphi(x) = 3x_1^2 + 4x_1x_2 + x_2^2$. Let $V_1 = (1, -2)\mathbb{R}$ and $V_2 = (0, 1)\mathbb{R}$. Let $x = (x_1, x_2)^T$ and $y = (y_1, y_2)^T$ are two column vectors in $\mathbb{R}^2$ be two indeterminate vectors then bilinear form associated with given quadratic form will be $\mathfrak{b}_\varphi(x, y) = 3x_1y_1 + 2x_1y_2 + 2x_2y_1 + x_2y_2$. Observe that $\mathfrak{b}_\varphi((1, -2), (0, 1)) = 0$. Now we can write $\varphi = \varphi|_{V_1} \oplus \varphi|_{V_2}$. We have

$$\varphi|_{V_1} = -x_1^2$$
$$\varphi|_{V_2} = x_2^2.$$

Hence we get $\varphi \cong x_1^2 - x_2^2$.

1.1.2 Diagonal Quadratic Forms

Definition 1.1.10 An n-ary quadratic form φ over K is called *diagonal* if coefficients of x_ix_j $(i \neq j; 1 \leq i, j \leq n)$ in equation 1.3 are zero. It has the form

$$\varphi(x) = \sum_{i=1}^{n} a_i x_i^2 \tag{1.7}$$

We denote the diagonal form as follows:

$$\varphi(x) = \langle a_1, a_2, \ldots, a_n \rangle.$$

We notice that

$$\langle a_1, a_2, \ldots, a_n \rangle = \langle a_1 \rangle + \langle a_2 \rangle + \ldots + \langle a_n \rangle.$$

In this case matrix of coefficients is diagonal.

Theorem 1.1.11. *Every quadratic space (V, φ) over K is isometric to an orthogonal sum of one dimensional quadratic spaces.*

Proof. We prove this by induction on dimension of V. If $\dim_K V = 1$ then there is nothing to prove. Suppose $\dim_K V = n$ and theorem is true for $(n-1)$-dimensional spaces.

Case I. If $\varphi(v) = 0$ for all $v \in V$ then result is trivially true as the form is diagonal $\langle 0, \ldots, 0\rangle$ with respect to any basis.

Case II. If $\varphi(v) \neq 0$ for some $v \in V$, say v_1. Let $0 \neq a = \varphi(v_1)$. Consider the subspace V_1 generated by v_1. Define the set of all vectors orthogonal to v_1 as follows:

$$W = V_1^{\perp} = \{w \in V : \mathfrak{b}_\varphi(v_1, w) = 0\}.$$

Clearly W is a subspace of V of $\dim_K W \leq n-1$ as $\mathfrak{b}_\varphi(v_1, v_1) = a \neq 0$ and hence $v_1 \notin W$. Note that the equation $\mathfrak{b}_\varphi(v_1, w) = 0$ gives rise to a linear equation in n-variables, which implies the dimension of the solution space $\dim_K W \geq n-1$. Hence $\dim_K W = n-1$ and we get $V = V_1 \oplus W$. Since $\dim_K W = n-1$, the result follows from the induction hypothesis. □

Remark 1.1.12 Let $a \in K^*$. If there exists a non-zero vector $v \in V$ such that $\varphi(v) = a$ then it is clear from the proof of above theorem that $\varphi \cong \langle a\rangle \oplus \psi$, for some quadratic form ψ with $\dim(\psi) = \dim(\varphi) - 1$.

Corollary 1.1.13. *If the binary form $\langle a, b\rangle$ represents $c \in K^*$ then $\langle a, b\rangle \cong \langle c, abc\rangle$.*

Proof. Since $\langle a, b\rangle$ represents $c \in K^*$, we have $\langle a, b\rangle \cong \langle c, e\rangle$, for some $e \in K^*$. The isometry condition implies that $ce = ab\alpha^2$, where $\alpha \in K^*$. Hence $\langle e\rangle \cong \langle abc\rangle$. □

Notation Let $\varphi = \langle a_1, a_2, \ldots, a_n\rangle$ and $\psi = \langle b_1, b_2, \ldots, b_m\rangle$, we define

1. $\varphi \oplus \psi = \langle a_1, \ldots, a_n, b_1, \ldots, b_m\rangle$ is called orthogonal sum of φ and ψ.
2. $\varphi \otimes \psi = \langle \ldots, a_i b_j, \ldots\rangle$ is called product of φ and ψ.
3. $a\varphi = \langle aa_1, aa_2, \ldots, aa_n\rangle$ for any $a \in K^*$.
4. Let $r \geq 0$ be an integer, then $r \times \varphi = \underbrace{\varphi \oplus \ldots \oplus \varphi}_{\text{r times}}$. and $0 \times \varphi = 0$ is zero form.

Remark 1.1.14 Let (V_1, φ) and (V_2, ψ) be two quadratic spaces where φ and ψ are as above. Then for $v_1 \otimes v_2, v_1' \otimes v_2' \in V_1 \otimes_K V_2$ we have

$$\mathfrak{b}_{\varphi\otimes\psi}(v_1 \otimes v_2, v_1' \otimes v_2') = \mathfrak{b}_\varphi(v_1, v_1')\mathfrak{b}_\psi(v_2, v_2').$$

A reference for this remark is [Lam05, p 17].

1.1.3 Radical and Regularity

Definition 1.1.15 Let (V, φ) be an n-dimensional quadratic space over K. Two vectors v and w in V are called *orthogonal* with respect to φ if $\mathfrak{b}_\varphi(v, w) = 0$

Example 1.1.16 Let $V = \mathbb{R}^2$ and $\varphi = x_1^2 + x_2^2$. The bilinear form associated to φ is $\mathfrak{b}_\varphi(x, y) = x_1y_1 + x_2y_2$. Let $v = (2, 1)$ and $w = (3, -6)$ be two vectors in $\mathbb{R}^2$. Then

$$\mathfrak{b}_\varphi(v, w) = 2 \times 3 + 1 \times -6 = 6 - 6 = 0.$$

Hence v and w are orthogonal vectors.

Definition 1.1.17 Let (V, φ) be an n-dimensional quadratic space over K. Let W be a subspace of V then $(W, \varphi|_W)$ is a quadratic subspace of V. An *orthogonal complement* of $(W, \varphi|_W)$ with respect to φ is set of all those vectors $v \in V$ which are orthogonal to all vectors in W. It is denoted by $W^\perp$.

$$W^\perp = \{v \in V : \mathfrak{b}_\varphi(v, w) = 0,\ \forall\ w \in W\}$$

Example 1.1.18 Orthogonal complement of the trivial subspace 0 of V is V itself as $\mathfrak{b}_\varphi(0, v) = 0$ for all $v \in V$.

Definition 1.1.19 Let (V, φ) be an n-dimensional quadratic space over K. Orthogonal complement of V with respect to φ is called the *radical* of V. It is denoted by $\mathrm{rad}(V)$.

$$\mathrm{rad}\, V = V^\perp = \{v \in V : \mathfrak{b}_\varphi(v, u) = 0,\ \forall\ u \in V\} = \{v \in V : u^t A v = 0,\ \forall\ u \in V\},$$

where A is the symmetric matrix associated with φ.

Definition 1.1.20 Let φ be an n-ary quadratic form over K. Then φ is called *regular* if determinant of the associated matrix A is non zero. Otherwise φ is called *singular*.

Observation 1.1.21 If a quadratic form $\varphi \cong \langle a_1, a_2, \ldots, a_n\rangle$ is singular, then $\det A$ is zero and hence $a_i = 0$ for some i.

Example 1.1.22 Let $\varphi = x^2 + 4xy + 4y^2$. Symmetric matrix associated with φ is

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$$

$\det A = 0$, hence φ is not regular.

$\operatorname{rad}(\mathbb{R}^2, \varphi) = \{u \in \mathbb{R}^2 : u^t A v = 0, \ \forall\ v \in V\}$

$$\begin{pmatrix} u_1 & u_2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = 0$$

$$\Rightarrow (u_1 + 2u_2)v_1 + (2u_1 + 4u_2)v_2 = 0 \Rightarrow u_1 + 2u_2 = 0$$

Hence we get

$$\operatorname{rad}(\mathbb{R}^2, \varphi) = \{u = (u_1, u_2) \in \mathbb{R}^2 : u_1 + 2u_2 = 0\}.$$

Theorem 1.1.23. *A quadratic form φ over K is regular if and only if* $\operatorname{rad}(\varphi) = 0$.

Proof. See [Pfi95, p. 4] □

From now onward all quadratic forms will be considered to be diagonal and regular.

1.2 The Hyperbolic Space

Definition 1.2.1 Let (V, φ) be an n-dimensional quadratic space over K. An element $a \in K$ is said to be *represented* over K if there is a non zero n-dimensional vector v such that

$$\varphi(v) = a.$$

The set of all elements of K represented by φ will be denoted by $D_K(\varphi)$

$$D_K(\varphi) = \{\varphi(v) : 0 \neq v \in V\}.$$

Observation 1.2.2 Observe that if φ and ψ are two isometric quadratic forms over K then $D_K(\varphi) = D_K(\psi)$. Since isometric quadratic forms denote the same set of elements of K, it is enough to study of only one representative of an isometry class. For a field K, identifying all quadratic forms (upto isometry) is a very interesting problem. Proceeding in the direction we have the following definition:

Definition 1.2.3 An n-ary quadratic form φ over K is called *universal* if every element of K can be represented by φ, that is $D_K(\varphi) = K$.

Example 1.2.4

1. Every quadratic form over $\mathbb{C}$ is universal as $\mathbb{C}$ is quadratically closed (moreover $\mathbb{C}$ is algebraically closed).

2. The two dimensional form $\varphi = x_1^2 + x_2^2$ is universal over the finite field $\mathbb{F}_q$ for all primes powers, as every element can be written as sum of two squares in a finite field $\mathbb{F}_q$.

3. The form in second example is not universal over $\mathbb{R}$ as -1 is not represented as $\alpha^2 + \beta^2 > 0$, for $\alpha, \beta \in \mathbb{R}$.

Definition 1.2.5 An n-ary quadratic form φ is called *isotropic* if it represents 0 *i.e.* if there exists an n-dimensional non-zero vector v such that $\varphi(v) = 0$. The vector v is called *isotropic vector*. If φ does not represent zero it is called *anisotropic*.

Example 1.2.6

1. Every form of dimension greater then equal to 3 is isotropic over $\mathbb{F}_q$ for all primes powers q.

2. The two dimensional form $\varphi = x_1^2 + x_2^2$ is anisotropic over $\mathbb{R}$.

3. The two dimensional form $\varphi = x_1^2 - x_2^2$ is isotropic over any field K.

4. The one dimensional form $\varphi = x_1^2$ is anisotropic over any K.

A lot of research work in the field of algebraic theory of quadratic forms is dedicated to develop tools to determine whether a given quadratic form is isotropic over a field or not. In this section we will try to identify equivalence classes of isotropic forms.

Definition 1.2.7 A $2n$-dimensional quadratic form φ is called *hyperbolic* if $\varphi \cong n \times \langle 1, -1 \rangle$.

Definition 1.2.8 Let (V, φ) be quadratic space. Then a subspace W of V is called *totally isotropic* if $\mathfrak{b}_\varphi(W, W) = 0$ *i.e.* for all $x, y \in W$, $\mathfrak{b}_\varphi(x, y) = 0$.

Theorem 1.2.9. *Let (V, φ) be a regular $2n$-dimensional quadratic space. Then the following are equivalent:*

1. *V contains an n-dimensional totally isotropic subspace W.*
2. *$\varphi \cong n \times \langle 1, -1 \rangle$.*

Proof. ($1 \Rightarrow 2$) Suppose V contains an n-dimensional totally isotropic subspace W. Let $\boldsymbol{\beta}$ be a basis of V constructed by extending any basis of W to a basis of V. Then associated matrix of φ is of the form

$$A = \begin{pmatrix} 0 & C \\ C^T & D \end{pmatrix}.$$

Take

$$P = \begin{pmatrix} C^T & \frac{1}{2}(D^T + I) \\ C^T & \frac{1}{2}(D^T - I) \end{pmatrix},$$

where I is an $n \times n$ identity matrix. Observe that

$$A = P^T \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix} P.$$

Therefore $\varphi \cong n \times \langle 1, -1 \rangle$. Conversely, suppose $\varphi \cong n \times \langle 1, -1 \rangle$. For $1 \leq j \leq n$, let w_{2j-1} be the vector whose $2j - 1$ and $2j$ component is 1 and every other component is 0. Clearly $S = \{w_{2j-1} : 1 \geq j \leq n\}$ are isotropic vectors of φ and linearly independent. Therefore the subspace generated by S will be n-dimensional totally isotropic subspace of V. $\square$

Corollary 1.2.10. *A regular two dimensional form φ over K is isotropic if and only if it is of the form $2x_1x_2$, which is equivalent to the form $x_1^2 - x_2^2$.*

Definition 1.2.11 Equivalence class of two dimensional regular isotropic quadratic form over K is called the *hyperbolic plane*. It is denoted by H and $H \cong \langle 1, -1 \rangle$.

Observation 1.2.12

1. In example 1.1.7, we proved that $H \cong 2x_1x_2$. That is the hyperbolic plane has a basis $\{v_1, v_2\}$ such that

$$\mathfrak{b}_H(v_1, v_2) = 1, \mathfrak{b}_H(v_1, v_1) = 0, \mathfrak{b}_H(v_2, v_2) = 0.$$

2. The form $2x_1x_2$ is universal as for any $\alpha \in K$, $x_1 = \frac{1}{2}$ and $x_2 = \alpha$ will fulfil the requirement.

In general for isotropic quadratic forms we have the following result:

Theorem 1.2.13. *An n-ary regular quadratic form φ over K is isotropic if and only if it contains a hyperbolic plane as an orthogonal summand for $n \geq 2$. In other words a regular quadratic space (V, φ) of $\dim V \geq 2$ is isotropic over K if and only if $\varphi = \langle 1, -1 \rangle \oplus \varphi|_W$ for some subspace W of V.*

Proof. Suppose φ is isotropic. Let v_1 be an isotropic vector. Since φ is regular we can choose $u \in V$ such that $\mathfrak{b}_\varphi(v_1, u) = \alpha \neq 0$. Which implies $\mathfrak{b}_\varphi(v_1, \frac{u}{\alpha}) = 1$. Let $w = \frac{u}{\alpha}$. Then clearly v_1 and w are linearly independent. Take $v_2 = w - \frac{\varphi(w)}{2} v_1$. Clearly the pair $\{v_1, v_2\}$ satisfies the conditions of above observation. Then $U = Kv_1 \oplus Kv_2$ is a two dimensional subspace of V and the form $\varphi|_U$ is equivalent to $\langle 1, -1 \rangle$. Also $U^\perp = \{v \in V : \mathfrak{b}_\varphi(u, v) = 0, \ \forall\ u \in U\}$. If we extend $\{v_1, v_2\}$ to a basis of V then the equation $\mathfrak{b}_\varphi(u, v) = 0$ will give rise to a linear equation in two variables which implies that $\dim U^\perp \geq n - 2$. Since U is isometric to the hyperbolic plane, U is regular. It implies that $\operatorname{rad}(U) = \{u' \in U : \mathfrak{b}_\varphi(u, u') = 0, \ \forall\ u \in U\} = 0$. Which implies that $U \cap U^\perp = 0$. Since $\dim(U) = 2$, $\dim(U^\perp) = n - 2$. Take $W = U^\perp$ and the result follows. $\square$

1.3 Witt Ring of a Field

We refer [Pfi95, Chapter 2] for details of the content in this section. In view of the previous sections we have the following theorems of Witt:

Theorem 1.3.1. ***(Cancellation theorem of Witt)*** *Let φ be an n-ary quadratic form. Let φ_1 and φ_2 be two quadratic forms of equal dimensions. If*

$$\varphi \oplus \varphi_1 \cong \varphi \oplus \varphi_2$$

then $\varphi_1 \cong \varphi_2$

Theorem 1.3.2. ***(Decomposition Theorem of Witt)*** *Every regular quadratic form over K has an orthogonal decomposition*

$$\varphi \cong i \times \langle 1, -1 \rangle \oplus \varphi_0$$

where $i \in \mathbb{N}$ and φ_0 is anisotropic over K. The number i is called Witt index and it is uniquely determined by isometry classes of φ and φ_0.

Definition 1.3.3 Let $\varphi \cong i \times \langle 1, -1\rangle \oplus \varphi_0$ and $\psi \cong j \times \langle 1, -1\rangle \oplus \psi_0$ be two quadratic forms over K, where φ_0 and ψ_0 are anisotropic part of φ and ψ. Quadratic forms φ and ψ are called of the *same anisotropic type* if $\varphi_0 \cong \psi_0$. We will denote this relation by $\sim$ and it is clearly an equivalence relation.

Let $S(K)$ be the set of all regular quadratic forms of finite dimensions over K. Then define

$$W(K) = S(K)/\sim$$

to be the set of anisotropic classes of regular quadratic forms over K. Elements of $W(K)$ are called *Witt classes* and denoted by $\tilde{\varphi}$.

We have defined addition $\oplus$ and multiplication $\otimes$ for the elements of $S(K)$. Hence we can naturally define these operations for $W(K)$. Although we have to make sure that definitions are still well defined. Let $\tilde{\varphi}, \tilde{\psi} \in W(K)$, then we define

1. $\tilde{\varphi} \oplus \tilde{\psi} = \widetilde{\varphi \oplus \psi}$
2. $\tilde{\varphi} \otimes \tilde{\psi} = \widetilde{\varphi \otimes \psi}$

Observe that

1. $\langle 1, -1\rangle \oplus \varphi \sim \varphi$
2. $\langle 1, -1\rangle \otimes \varphi \cong \dim(\varphi) \times \langle 1, -1\rangle$

Also observe that $\widetilde{\langle 1\rangle} \otimes \varphi \sim \varphi$. Hence $\oplus$ and $\otimes$ are well defined on $W(K)$.

Theorem 1.3.4. *The set $W(K)$ with above defined addition $\oplus$ and multiplication $\otimes$, is a commutative ring with zero element $0 = \tilde{0}$ and unit element $1 = \widetilde{\langle 1\rangle}$.*

Proof. From the above claim addition and multiplication are well defined. Also, $0 = \tilde{0}$ is zero element and $\widetilde{\langle 1\rangle} = 1$ is unit element. We will first show $W(K)$ is a ring.

1. (Abelian group under addition):
   - Clearly addition is commutative and associative.
   - $0 = \tilde{0}$ is the zero element.
   - Let $\tilde{\varphi} = \widetilde{\langle a_1, a_2, \ldots, a_n\rangle} \in W(K)$ then $\tilde{\varphi}' = \widetilde{\langle -a_1, -a_2, \ldots, -a_n\rangle}$ will be the additive inverse of φ as

$$\tilde{\varphi} \oplus \tilde{\varphi}' = \widetilde{\langle a_1, \ldots, a_n, -a_1, \ldots, -a_n\rangle} \cong \widetilde{\dim \varphi \times \langle 1, -1\rangle} \sim \tilde{0}$$

We will denote additive inverse of $\tilde{\varphi}$ by $\ominus\tilde{\varphi}$

2. (Distributive property): Let$\varphi = \widetilde{\langle a_1, a_2, \dots, a_l\rangle}, \psi = \widetilde{\langle b_1, b_2, \dots, b_m\rangle}$ and $\chi = \widetilde{\langle c_1, c_2, \dots, c_n\rangle}$, then

$$\begin{aligned}
\varphi \otimes (\psi \oplus \chi) &= \widetilde{\langle a_1, a_2, \dots, a_l\rangle} \otimes (\widetilde{\langle b_1, b_2, \dots, b_m\rangle} \oplus \widetilde{\langle c_1, c_2, \dots, c_n\rangle}) \\
&= \widetilde{\langle a_1, a_2, \dots, a_l\rangle} \otimes (\widetilde{\langle b_1, \dots, b_m, c_1, \dots, c_n\rangle}) \\
&= \widetilde{\langle \dots, a_i b_j, \dots, a_i c_k, \dots, \rangle} \\
&= \varphi \otimes \psi \oplus \varphi \otimes \chi
\end{aligned}$$

3. (Associativity and commutativity of multiplication): These two properties will also follow directly from the definition of product.

Hence $W(K)$ is a commutative ring. $\square$

Definition 1.3.5 The ring $W(K)$ is called the *Witt ring* of K and if we ignore multiplication the additive group $W(K)$ is called *Witt group*. Observe that $W(K)$ is collection non isometric anisotropic quadratic forms over K. For better understanding we compute Witt rings of some fields.

Example 1.3.6 Let $K = \mathbb{C}$. As $\mathbb{C}$ is a quadratically closed, only Witt classes over K are 0 and $\langle 1\rangle$. We get $W(\mathbb{C}) = \{\tilde{0}, \widetilde{\langle 1\rangle}\} = \mathbb{Z}/2\mathbb{Z}$.

Proof. Since group of square classes $\mathbb{C}/\mathbb{C}^{*2}$ is trivial, we have $a \in \mathbb{C}^*$ is a square. Hence there is only one non isometric one dimensional form namely $\langle 1\rangle$. Let $\langle a, b\rangle$ be any two dimensional form over $\mathbb{C}$ then $b = -ac^2$ holds for some $c \in \mathbb{C}^*$. Therefore $\langle a, b\rangle \cong \langle 1, -1\rangle$. Hence there are only two non equivalent anisotropic form 0 and $\langle 1\rangle$. Hence $W(\mathbb{C}) = \{\tilde{0}, \widetilde{\langle 1\rangle}\} = \mathbb{Z}/2\mathbb{Z}$.

Example 1.3.7 Let $K = \mathbb{R}$. We have $\tilde{0}$, $n \times \langle 1\rangle$ and $n \times \langle -1\rangle$ are the only non equivalent anisotropic forms. Hence $W(\mathbb{R}) = \mathbb{Z}$.

Proof. Since $\mathbb{R}/\mathbb{R}^{*2} = \{1, -1\}$, any form φ of dimension n is isometric to the form $r \times \langle 1\rangle \oplus (n - r) \times \langle -1\rangle$, for some $0 \le r \le n$. Clearly φ is isotropic if $r \ne 0, n$. Hence non equivalent anisotropic forms over $\mathbb{R}$ are only $\tilde{0}$, $n \times \langle 1\rangle$ and $n \times \langle -1\rangle$ are the only non equivalent anisotropic forms. Hence $W(\mathbb{R}) = \mathbb{Z}$.

Example 1.3.8 Let $K = \mathbb{Z}/p\mathbb{Z}$, where p is an odd prime number. Then

$$W(K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \qquad \text{for } p \equiv (1 \mod 4)$$
$$W(K) \cong \mathbb{Z}/4\mathbb{Z} \qquad \text{for } p \equiv (3 \mod 4)$$

Proof. We know that for any odd prime p, $\dfrac{(\mathbb{Z}/p\mathbb{Z})^*}{(\mathbb{Z}/p\mathbb{Z})^{*2}} = \{1, \epsilon\}$, where ϵ is a non square. Clearly one dimensional non equivalent quadratic forms are $\langle 1\rangle$ and $\langle \epsilon\rangle$. Now we characterize anisotropic forms of dimension two. Let $\varphi = \langle a, b\rangle$ be an anisotropic binary quadratic form. Then for any pair $(x, y) \in K^2$ we have

$$ax^2 + by^2 \neq 0,$$
$$\Leftrightarrow b \neq -a(\tfrac{x}{y})^2,$$

which is same as saying, b and $-a$ do not belong to the same square class. Hence $\varphi \cong \langle 1, -\epsilon\rangle$ or $\varphi \cong \epsilon\langle 1, -\epsilon\rangle$. Hence, any binary anisotropic form φ is equivalent to a scalar multiple of the form $\langle 1, -\epsilon\rangle$. we denote this form by φ_0. Also $1 = 1 \cdot 1^2 - \epsilon \cdot 0^2$ and $\epsilon = a^2 + b^2 \Rightarrow \epsilon = (\frac{\epsilon}{b})^2 - \epsilon(\frac{a}{b})^2$. Since φ_0 represents both 1 and ϵ, $D_K(\varphi_0) = K^*$. Therefore any form of dimension ≥ 3 is isotropic. Hence we have in total four non equivalent anisotropic forms, namely $0, \langle 1\rangle, \langle \epsilon\rangle$ and φ_0, hence $|W(K)| = 4$. Further we determine the ring structure of $W(K)$ depending on prime $p \equiv 1 \mod 4$ or $p \equiv 3 \mod 4$. Let $p \equiv 1 \mod 4$ then -1 is a square modulo 4 and $2 \times \langle 1\rangle = \langle 1, 1\rangle \cong \langle 1, -\rangle \sim 0$. Hence every non-zero element will have order 2 and we get

$$W(K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

If $p \equiv 3 \mod 4$ then -1 is not a square. Clearly $\langle 1, 1\rangle \ncong \langle 1, -1\rangle$. Hence $\langle 1, 1\rangle \sim 0$. Thus the order of $\langle 1\rangle$ is not 2. Hence we get

$$W(K) \cong \mathbb{Z}/4\mathbb{Z}.$$

Chapter 2

Quadratic Forms under Field Extensions

Any quadratic form over a field K can be considered as a quadratic form over a field extension L/K. Isotropic quadratic forms over K remain isotropic over L but converse is not true. In this chapter, we consider some specific field extensions and interesting results in the converse direction. In §1 we present some important results for rational function fields such as Cassel-Pfister representation theorem and subform theorem. As an application in next two sections we study extension of a quadratic form to quadratic field extensions and function fields of quadratic forms. In last section function field of a quaternion algebra is studied and we discuss an excellence result due to Rost.

Notation Let φ be a quadratic form over K. For a field extension L/K the extended form is denoted by φ_L. As the K-form φ can become isotropic over a field extension L/K, anisotropic part of φ_L is denoted by $(\varphi_L)_{an}$. With this notation we have the following definition:

Definition 2.0.9 A field extension L/K is called *excellent* if for any quadratic form φ over K, there exists a quadratic form ψ over K such that $(\varphi_L)_{an}$ is isometric to ψ_L.

2.1 Quadratic Forms under Rational function field

Let $K[t]$ be the ring of polynomials in one variable and $L = K(t)$ be the rational function field. Then we have $K \subset K[t] \subset K(t) = L$. We know that L is a transcendental extension of K.

Proposition 2.1.1. *If φ is anisotropic over K, then φ_L is anisotropic over L.*

Proof. Let φ be an n-ary anisotropic quadratic form over K. Assume that φ is isotropic over $L = K(t)$. Then there exists a non-zero vector $f = (f_1, f_2, \ldots, f_n)$ over L such that $\varphi(f) = 0$. Let g_0 be the common denominator of rational functions f_i's then we have $f_i = \dfrac{g_i}{g_0}$. For n-dimensional vector $0 \neq g = (g_1, g_2, \ldots, g_n)$ over the polynomial ring $K[t]$, $\varphi(g) = g_0^2\varphi(f) = 0$. Let $d(t) = \gcd(g_1, g_2, \ldots, g_n)$. We can write $g_i = d(t)h_i$ for some $h_i \in K[t]$ where h_i's are relatively prime. Let $h = (h_1, h_2, \ldots, h_n)$ then we have $\varphi(g) = d(t)^2\varphi(h)$. Since $d(t) \neq 0$ and $K[t]$ is an integral domain, $\varphi(h) = 0$. Let $c_i = h_i(0)$. Since h_i's are relatively prime, all c_i's cannot be zero because in that case t must divide gcd of h_i's. Let $c = (c_1, c_2, \ldots, c_n)$, where $c_i \in K$. Clearly $c \neq 0$ and $\varphi(c) = 0$ as $\varphi(c) = \lim_{t\to 0} \varphi(h(t)) = 0$. □

Remark 2.1.2 The field extension $K(t)/K$ is excellent.

Proposition 2.1.3. *Let φ be an n-ary regular quadratic form over K and let $c \in K^*$. Then φ represents c over K if and only if $(n+1)$-ary quadratic form $\varphi \oplus \langle -c\rangle$ is isotropic over K.*

Proof. Suppose φ represents c over K then there exists a non-zero vector $v \in V$ such that $\varphi(v) = c$. We have $\varphi(v) - c = 0$, therefore $\varphi \oplus \langle -c\rangle$ is isotropic as we observe that $(\varphi \oplus \langle -c\rangle)(v, 1)^T = 0$.

Conversely, suppose the form $\varphi \oplus \langle -c\rangle$ is isotropic over K. We consider the following two cases:

Case I. If φ itself is isotropic then from theorem 1.2.13 it follows that φ contains the form $\langle 1, -1\rangle$ as an orthogonal summand of it. Then φ is universal and therefore φ represents c over K.

Case II. Suppose φ is anisotropic. Since $\varphi \oplus \langle -c\rangle$ is isotropic there exists a $(n+1)$-dimensional non-zero isotropic vector $(v_1, v_2, \ldots, v_n, v_{n+1})$. Let $0 \neq v = (v_1, v_2, \ldots, v_n)$ then we have $\varphi(v) - cv_{n+1}^2 = 0$. Since φ is anisotropic, $v_{n+1} \neq 0$. Therefore, we have $v' = \dfrac{v}{v_{n+1}} \neq 0$ and $\varphi(v') = c$. □

Proposition 2.1.4. *If φ is an n-ary regular isotropic quadratic form over K then φ represents every element of $K[t]$ over $K(t)$.*

Proof. If φ be an n-ary regular isotropic quadratic form over K then it contains a hyperbolic plane as an orthogonal summand. Hence it is of the form

$$\varphi(x) = 2x_1x_2 + \psi(x_3, \ldots, x_n)$$

Let $p(t) \in K[t]$ then take $x_1 = \frac{1}{2}$, $x_2 = p(t)$ and $x_3 = x_4 = \ldots = x_n = 0$ and the result follows. $\square$

Observe that φ is regular over K if and only if φ_L is regular over L.

Theorem 2.1.5. ***(Cassel-Pfister Representation Theorem)*** *Let φ be an n-ary quadratic form over K. Let $p(t) \in K[t]$ be a non-zero polynomial in one variable. If φ represents $p(t)$ over the field $L = K(t)$, then φ represents $p(t)$ over the polynomial ring $K[t]$.*

Proof. We prove the theorem by induction on dimension of φ. For $n = 1$, we have $\varphi(x) = \langle a \rangle$. From hypothesis of the theorem we have $f \in K(t)$ such that $af^2 = p(t)$. Since $K[t]$ is a unique factorization domain and $f^2 = p(t)/a \in K[t]$, $f \in K[t]$. Suppose the result is true for $\dim(\varphi) \leq n - 1$. We have the following two cases:
Case I. Suppose φ is regular and isotropic. Then the result follows from the previous proposition.
Case II. Suppose φ is a regular anisotropic form. Since φ represents $p(t)$ over L, we have

$$f = \left(\frac{f_1}{f_0}, \frac{f_2}{f_0}, \ldots, \frac{f_n}{f_0}\right) \in L^n,$$

where $f_i \in K[t]$, $0 \leq i \leq n$ and $f_i's$ are relatively prime, such that

$$\varphi\left(\frac{f_1}{f_0}, \frac{f_2}{f_0}, \ldots, \frac{f_n}{f_0}\right) = p(t)$$

Now assume that among all representations of $p(t)$ over $K(t)$ satisfying above properties, f_0 has the minimal degree, say d. If $d = 0$, then we are done. Suppose $d > 0$. Then we construct a representation of $p(t)$ over $K(t)$, whose denominator has a smaller degree. Since φ represents $p(t)$ over L, the $(n+1)$-dimensional form $\psi = \langle -p(t) \rangle \oplus \varphi_L$ is isotropic over L (by proposition 2.1.3) and $(f_0, f_1, \ldots, f_n)$ is the isotropic vector. Since f_0 has smaller degree than $f_1, f_2, \ldots, f_n$, hence applying Euclidean division algorithm we get

$$f_i = f_0 g_i + r_i, \qquad (0 \leq i \leq n)$$

where $g_i, r_i \in K[t]$ and degree of r_i's is less than d. Also $g_0 = 1$ and $r_0 = 0$ (we always assume degree of a zero polynomial to be $-\infty$).

Let $\mathbf{f} = (f_0, f_1, \ldots, f_n)$ and $\mathbf{g} = (g_0, g_1, \ldots, g_n)$. Since $0 = \deg(g_0) < \deg(f_0)$, we have $\psi(\mathbf{g}) \neq 0$ as f_0 was the minimal degree polynomial satisfying that condition.

We know that $\psi(\mathbf{f}) = 0$, therefore $\mathbf{f}$ and $\mathbf{g}$ are linearly independent over L. Take $h = \alpha\mathbf{f} - \beta\mathbf{g}$ with $\alpha = \psi(\mathbf{g}) \neq 0$ and $\beta = 2\mathfrak{b}_\psi(\mathbf{f}, \mathbf{g})$. Since $\mathbf{f}$ and $\mathbf{g}$ are linearly independent and $\alpha \neq 0$, we have $h \neq 0$. Let $h = (h_0, h_1, \ldots, h_n)$. Also

$$\psi(h) = \psi(\alpha\mathbf{f} - \beta\mathbf{g}) = \alpha^2\psi(\mathbf{f}) - 2\alpha\beta\mathfrak{b}_\psi(\mathbf{f}, \mathbf{g}) + \beta^2\psi(\mathbf{g}) = 0$$

Observe that h_0 is not zero. Since $\psi(h) = 0$, $\langle -p(t)\rangle \cdot 0 + \varphi(h_1, h_2 \ldots, h_n) = 0$. In that case $(h_1, h_2 \ldots, h_n)$ is a non zero isotropic vector of φ over L. Since φ is anisotropic, $h_0 \neq 0$. We have

$$\begin{aligned} h_0 &= \alpha f_0 - \beta g_0 \\ &= \alpha f_0 - \beta \\ &= \psi(\mathbf{g}) f_0 - 2\mathfrak{b}_\psi(\mathbf{f}, \mathbf{g}) \\ &= \frac{1}{f_0}(\psi(f_0\ \mathbf{g}) - 2f_0\mathfrak{b}_\psi(\mathbf{f}, \mathbf{g})) \\ &= \frac{1}{f_0}\psi(f_0\mathbf{g} - \mathbf{f}) = \frac{1}{f_0}\psi(r), \end{aligned}$$

where $r = (r_0, r_1, \ldots, r_n)$. Since ψ is a quadratic form, we have

$$\deg(h_0) = 2 \cdot \max_i \deg(r_i) - \deg(f_0) \leq 2(d-1) - d = d - 2 < d.$$

which is a contradiction.

□

Observation 2.1.6

1. (Pfister's generalization) Case 2 of above theorem is true even if coefficients of φ are polynomial in one variable of degree less than or equal to 1. Observe that in the last part of the proof of previous theorem we calculated:

   $$\deg(h_0) = \deg\psi(r) - \deg(f_0) = 1 + 2(d-1) - d = d - 1 < d$$

   which is a contradiction.

2. If φ is isotropic and we take coefficients of φ from $K[t]$ of degree less than or equal to 1, then the theorem does not hold. For example take $\varphi = \langle t, -t\rangle$ and $p(t) = 1$. Observe that φ is isotropic and universal over L but $2tx_1x_2 = 1$ has clearly no solution in $K[t]$.

Generalization of theorem 2.1.5 is not possible for several variables as the proof uses Euclidean algorithm to arrive at a contradiction but $K[t_1, t_2, \ldots, t_n]$ is not even a unique factorization domain. Although we have the following weaker result:

Theorem 2.1.7. ***(Substitution Principle)*** *Let φ be an n-ary quadratic form over a field K. Let φ represents a non zero polynomial $p = p(x_1, x_2, \ldots, x_n) \in K[x_1, x_2, \ldots, x_n]$ over the rational function field $K(x_1, x_2, \ldots, x_n)$ then for $c_1, c_2, \ldots, c_n \in K$, φ represents the element $p(c_1, c_2, \ldots, c_n)$ over K.*

Proof. We prove this by induction on n. For $n = 1$, φ represents $p(t_1)$ over the field $K(t_1)$ and hence over the ring $K[t_1]$. Substitute $t_1 = c_1$ and the result follows for $n = 1$.

Suppose φ represents $p(t_1, t_2, \ldots, t_n)$ over $K(t_1, t_2, \ldots, t_n)$. Then from theorem 2.1.5 it follows that the polynomial $p(t_1, t_2, \ldots, t_n)$ has a representation over the ring $K(t_1, t_2, \ldots, t_{n-1})[t_n]$. Substitute $t_n = c_n$ and note that now φ represents the polynomial $p(t_1, t_2, \ldots, t_{n-1}, c_n)$ over the field $K(t_1, t_2, \ldots, t_{n-1})$ and the theorem follows by induction. □

Theorem 2.1.8. *Let $d, a_1, a_2, \ldots, a_n \in K^*$ and $\varphi = \langle a_1, a_2, \ldots, a_n \rangle$. If $d + a_1 t^2 \in D_{K(t)}(\varphi)$ then either φ is isotropic over K or $d \in D_K(\varphi')$, where $\varphi' = \langle a_2, \ldots, a_n \rangle$*

Proof. Suppose φ is anisotropic. Since $d + a_1 t^2 \in D_{K(t)}(\varphi)$, by theorem 2.1.5 φ represents $d + a_1 t^2$ over the ring $K[t]$. Hence we have $f_1, f_2, \ldots, f_n \in K[t]$ such that

$$a_1 f_1^2 + a_2 f_2^2 + \ldots + a_n f_n^2 = d + a_1 t^2$$

On comparing the terms of highest degree we conclude that $\deg f_i \leq 1$, for all $1 \leq i \leq n$. Let $f_i = b_i + c_i t$. Observe that one of the following equations

$$b_1 + c_1 t = \pm t$$

will certainly have a solution over K as $\operatorname{char} K \neq 2$. Substituting $t = \dfrac{b_1}{\pm 1 - c_1}$ we get

$$\sum_{i=2}^{n} a_i \left(b_i + c_i \left(\frac{b_1}{\pm 1 - c_1} \right) \right)^2 = d$$

Hence $d \in D_K(\varphi')$. □

Corollary 2.1.9. *Let K be a field such that $\varphi = \langle \overbrace{1, \ldots, 1}^{n} \rangle$ is anisotropic over K, then $1 + t_1^2 + t_2^2 + \ldots + t_n^2$ is not a sum of n squares in the rational function field $K(t_1, \ldots, t_n)$.*

Proof. Suppose that $1+t_1^2+t_2^2+\ldots+t_n^2$ is sum of n squares. Which is same as saying that φ represents $1+t_1^2+t_2^2+\ldots+t_n^2$. Let $d=1+t_1^2+t_2^2+\ldots+t_{n-1}^2$, $a_1=1$ and $t_n=t$. Since φ represents $d+t^2$ over $K(t_1,\ldots,t_{n-1})$ and φ is anisotropic, applying the theorem 2.1.8 we get that d is a sum of $n-1$ squares. Also observe that d is anisotropic. Applying the theorem 2.1.8 $n-1$ times we get $1+t_1^2$ is a square over $K(t_1)$. Which is a contradiction as char $K \neq 2$. □

Definition 2.1.10 Let $\varphi \cong \langle a_1, a_2, \ldots, a_n\rangle$ and $\psi \cong \langle b_1, b_2, \ldots, b_m\rangle$ with $m \leq n$ then ψ is called subform of φ if ψ is isometric to an orthogonal summand of φ.

Theorem 2.1.11. ***(The Subform Theorem)*** *Let $\varphi \cong \langle a_1, a_2, \ldots, a_n\rangle$ and $\psi \cong \langle b_1, b_2, \ldots, b_m\rangle$ with $m \leq n$ be two regular quadratic form over K. Suppose φ is anisotropic then ψ is isometric to a subform of φ if and only if for every extension field of L of K we have $D_L(\psi) \subseteq D_L(\varphi)$.*

Proof. Clearly if ψ is isometric to a subform of φ then for every extension field of L of K we have $D_L(\psi) \subseteq D_L(\varphi)$. We prove the converse by induction hypothesis on dimension of ψ. Suppose $D_L(\psi) \subseteq D_L(\varphi)$. If ψ is a zero form then the theorem is clearly true. Suppose $\dim(\psi) = m$ and $\psi = \langle b_1, b_2, \ldots, b_m\rangle$. Since $b_1 \in D_L(\psi)$, $b_1 \in D_L(\varphi)$. Which implies $\varphi \cong \langle b_1\rangle \oplus \varphi'$. Since φ is anisotropic so is φ'. By theorem 2.1.8 we get that $\psi' = \langle b_2, \ldots, b_m\rangle$ is represented by φ' over the field $K(t_2,\ldots,t_n)$. Clearly $D_L(\psi') \subseteq D_L(\varphi')$ and $\dim \psi' = m-1$, hence by induction hypothesis $\varphi' = \psi' \oplus \chi$. Therefore we get $\varphi = \langle b_1\rangle \oplus \varphi' = \langle b_1\rangle \oplus \psi' \oplus \chi = \psi \oplus \chi$. □

2.2 Quadratic Extensions

We refer to [Lam05, Chapter 10] for the content of this section. Throughout this section L denotes a fixed quadratic extension $K(\sqrt{a})/K$, where $a \in K^* \setminus K^{*2}$ and θ denotes the binary form $\langle 1, -a\rangle$ over K. Clearly θ is anisotropic over K and becomes isotropic (essentially hyperbolic) over L. In this section, we will formulate some "nice conditions" for isotropy of a quadratic form over L, in terms of the binary form θ.

Theorem 2.2.1. *Let $L = K(\sqrt{a})$ be a quadratic extension of K and $\theta = \langle 1, -a\rangle$ be an anisotropic binary form over K. Let $\varphi = \langle a_1, \ldots a_n\rangle$ be an anisotropic form over K. Then φ_L is isotropic over L if and only if φ contains a binary subform isometric to $\lambda\theta$ for some $\lambda \in K^*$*

Proof. "If" part is clear. Conversely, suppose $\varphi = \langle a_1, \dots a_n\rangle$ be isotropic over L. Let $0 \neq x + \sqrt{a}y = (x_1 + \sqrt{a}y_1, \dots, x_n + \sqrt{a}y_n)$ be an isotropic vector over L, where $x_i, y_i \in K$. Then we have

$$\varphi(x_1 + \sqrt{a}y_1, \dots, x_n + \sqrt{a}y_n) = 0,$$

which implies

$$\sum_{i=1}^{n}(a_i x_i^2 + a a_i y_i^2) + \sqrt{a}\sum_{i=1}^{n}(a_i x_i y_i) = 0.$$

As $\{1, \sqrt{a}\}$ is a basis of L over K, comparing the coefficients of 1 and $\sqrt{a}$ on both sides, we get the following conditions

$$\begin{aligned}&\sum_{i=1}^{n}(a_i x_i^2 + a a_i y_i^2) = 0\\ &\Rightarrow \varphi(x) = -a\varphi(y),\end{aligned}$$

and

$$\sum_{i=1}^{n}(a_i x_i y_i) = 0 \Rightarrow \mathfrak{b}_\varphi(x, y) = 0.$$

The second condition says that x and y are orthogonal vectors. Since φ is anisotropic, x and y are both non-zero. Therefore subform theorem 2.1.11 implies that φ contains the binary form $\langle\varphi(x), \varphi(y)\rangle = \langle -a\varphi(y), \varphi(y)\rangle = \varphi(y)\theta$, where $\varphi(y) \in K$. $\square$

Theorem 2.2.2. *Let L and θ be as in previous theorem. An anisotropic K-form φ becomes hyperbolic over L if and only if $\varphi \cong \psi \otimes \theta$ for some K-form ψ.*

Proof. "If" part is clear. We prove converse by induction on $m = \dfrac{\dim(\varphi)}{2}$. For $m = 0$ the result is true. If $m > 0$ and φ becomes isotropic over L then by theorem 2.2.1 $\varphi \cong \lambda\theta \oplus \varphi'$, where $\dim \varphi' = 2(m-1)$. Now applying Witt's cancellation theorem, we get $\varphi' \cong (m-1) \times \langle 1, -1\rangle$. By induction hypothesis, $\varphi' \cong \psi' \otimes \theta$ for some K-form ψ'. Hence we get

$$\varphi \cong \lambda\theta \oplus \varphi' \cong \lambda\theta \oplus \psi' \otimes \theta \cong (\langle\lambda\rangle \oplus \psi') \otimes \theta \cong \psi \otimes \theta,$$

where ψ is a K-form. $\square$

Corollary 2.2.3. *For any anisotropic form φ over K, there exists a form ψ_K such that anisotropic part of φ_L is isometric to ψ_L i.e. L/K is excellent.*

Proof. Let φ be an anisotropic quadratic form over K. If φ_L remains anisotropic then the result is true. Suppose φ becomes isotropic over L and $\varphi_L \cong i \times \langle 1, -1 \rangle \oplus (\varphi_L)_{an}$ be the Witt decomposition of φ_L. By theorem 2.2.2, we have an orthogonal decomposition $\varphi_K \cong (q \otimes \theta) \oplus \psi$, for some quadratic forms q and ψ over K and $\dim q = i$. Hence we have

$$\begin{aligned} \varphi_L &\cong ((q \otimes \theta) \oplus \psi)_L \\ &\cong (q \otimes \theta)_L \oplus \psi_L \\ &\cong i \times \langle 1, -1 \rangle \oplus \psi_L, \end{aligned}$$

which is possible if and only if

$$i \times \langle 1, -1 \rangle \oplus (\varphi_L)_{an} \cong i \times \langle 1, -1 \rangle \oplus \psi_L.$$

Hence from the Witt cancellation theorem, it follows that

$$(\varphi_L)_{an} \cong \psi_L.$$

□

2.3 Function Field of a Quadratic Form

In this section we introduce the notion of *function field* associated to a quadratic form. Function field methods are very important for solving problems in the algebraic theory of quadratic forms as they have the important property that a quadratic form becomes isotropic over its function field.

We begin with the observation that an n-ary quadratic form $\varphi(x_1, \ldots, x_n)$ over K, $(n \geq 2)$ is reducible as a polynomial in polynomial ring $K[x_1, x_2, \ldots x_n]$ if and only if $n = 2$ and $\varphi \cong \langle 1, -1 \rangle$. Therefore a quadratic form $\varphi(X)$ over K is irreducible in $K[X]$ if $n \geq 2$ and $\varphi \ncong \langle 1, -1 \rangle$ and the principal ideal $(\varphi(X))$ is a prime ideal.

Definition 2.3.1 The quotient field of the integral domain $K[X]/(\varphi(X))$ is called the *function field* of φ. It is denoted by $K(\varphi)$. Let $\varphi(X) = \langle a_1, a_2, \ldots, a_n \rangle$, then

$$K(\varphi) = K(x_2, \ldots, x_n)\left(\sqrt{\frac{-(a_2 x_2^2 + \ldots a_n x_n^2)}{a_1}}\right)$$

Theorem 2.3.2. *Let φ and ψ be quadratic forms over K. If φ represents 1 and ψ becomes hyperbolic over $K(\varphi)$ then $\varphi(X)\psi \cong \psi$, where $X = (x_1, x_2, \ldots, x_n)$.*

Proof. As φ represents 1, we can write $\varphi \cong \langle 1\rangle \oplus \varphi'$. Let $L = K(\varphi) = K'(\sqrt{-\varphi'(X')})$, where $X' = (x_2, \ldots, x_n)$ and $K' = K(X')$. Since ψ is anisotropic over K, $\psi_{K'}$ is also anisotropic. As ψ_L is hyperbolic, it follows from the theorem 2.2.2 that $\psi_{K'} \cong \rho \otimes \langle 1, \varphi'(X')\rangle$ over K', where ρ is a quadratic form over K'. The form $\langle 1, \varphi'(X')\rangle$ represents $\varphi(X)$ over $K(X)$. By applying subform theorem we get

$$\psi_{K'} \cong \rho \otimes \varphi(X)\langle 1, \varphi'(X')\rangle \cong \varphi(X)(\rho \otimes \langle 1, \varphi'(X')\rangle) \cong \varphi(X)\psi_{K'}$$

□

2.4 Function Field of a Quaternion Algebra

In this section we define function field of a quaternion algebra and present a proof of excellence result for it following Rost's approach [Ros90].

Definition 2.4.1 Let $a, b \in K^*$. A *quaternion algebra* over K is a four dimensional K-algebra with basis $1, i, j, k$ such that

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

This quaternion algebra will be denoted by $(a, b)_K$.
Let $Q = (a, b)_K$ be a quaternion algebra and $(ax^2 + by^2 - 1)$ denote the ideal generated by the associated conic $ax^2 + by^2 - 1$. Then the quotient

$$R = K[x, y]/(ax^2 + by^2 - 1)$$

is an integral domain. The quotient field of R is called the *function field of* Q and we denote it by $K(Q)$.

Definition 2.4.2 Note that $R = K[x] \oplus yK[x]$ as K-vector space. For $f(x), g(x) \in K[x]$, define the map $d : R \to \mathbb{N} \cup \{-\infty\}$ by

$$d(f(x) + yg(x)) = \max(\deg(f(x)), \deg(g(x)) + 1),\ \ \deg 0 = -\infty.$$

Let $R_n = \{r \in R : d(r) \leq n\}$. Then R_n is a K-vector subspace of R. We have $R_0 = K$ and $R_n \cdot R_m \subset R_{n+m}$. Let $r \in R_n$ be a general element then

$$r = \alpha + \sum_{i=1}^{n}(\lambda_i y x^{i-1} + \mu_i x^i), \text{ where } \alpha, \lambda_i, \mu_i \in K.$$

Let V be an m-dimensional vector space over K. Then an element $\Upsilon \in V \otimes_K R_n$ is of the form

$$\begin{aligned}\Upsilon &= (\alpha_1 + \sum_{i=1}^{n}(\lambda_{1i}yx^{i-1} + \mu_{1i}x^i), \dots \alpha_m + \sum_{i=1}^{n}(\lambda_{mi}yx^{i-1} + \mu_{mi}x^i) \\ &= (\alpha_1, \dots, \alpha_m) + (\sum_{i=1}^{n}(\lambda_{1i}yx^{i-1}, \dots, \sum_{i=1}^{n}(\lambda_{mi}yx^{i-1}) + (\sum_{i=1}^{n}\mu_{1i}x^i), \dots, \sum_{i=1}^{n}\mu_{mi}x^i)).\end{aligned}$$

Let $v_0 = (\alpha_1, \dots, \alpha_m), v_i = (\lambda_{1i}, \dots, \lambda_{mi})$ and $w_i = (\mu_{1i}, \dots, \mu_{mi})$ are elements of V. Then we can write above expression as

$$\Upsilon = v_0 + \sum_{i=1}^{n} v_i yx^{i-1} + w_i x^i.$$

Proposition 2.4.3. *Let (V, φ) be an m-dimensional regular and anisotropic quadratic space over K. Let $Q = (a, b)_K$ be a quaternion algebra and $K(Q), R, R_i$ are as above. Suppose there exists $k \in \mathbb{N}$ such that for some $\Upsilon \in V \otimes_K R_k \backslash V \otimes_K R_{k-1}$, $\varphi(\Upsilon) = 0 \in R$. Then there exist vectors $v, w \in V$ such that $\mathfrak{b}_\varphi(v, w) = 0$ and $\varphi(w) = ab\varphi(v)$.*

Proof. Let $\Upsilon \in V \otimes_K R_k \setminus V \otimes_K R_{k-1}, k \in \mathbb{N}$ be such that $\varphi(\Upsilon) = 0 \in R$. We write

$$\Upsilon = v_0 + \textstyle\sum_{i=1}^{n}(v_i yx^{i-1} + w_i x^i),$$

where at least one of the v_n and w_n is not zero. Reading the equation, $\varphi(\Upsilon) = 0$ modulo R_{2k-1}, we get

$$\varphi(\Upsilon) \mod R_{2k-1} = 0 \in R/R_{2k-1}.$$

Substituting the value of Υ, we get

$$\begin{aligned}0 &= \varphi(v_0 + \sum_{i=1}^{n}(v_i yx^{i-1} + w_i x^i)) \mod R_{2k-1} \\ &= \varphi(v_n yx^{n-1} + w_n x^n) \mod R_{2k-1} \\ &= \varphi(v_n)y^2x^{2(n-1)} + \varphi(w_n)x^{2n} + 2\mathfrak{b}_\varphi(v_n, w_n)yx^{2n-1} \mod R_{2k-1} \\ &= (\varphi(v_n)y^2x^{-2} + \varphi(w_n))x^{2n} + 2\mathfrak{b}_\varphi(v_n, w_n)yx^{2n-1} \mod R_{2k-1} \\ &= (-ab\varphi(v_n) + \varphi(w_n))x^{2n} + 2\mathfrak{b}_\varphi(v_n, w_n)yx^{2n-1} \mod R_{2k-1}.\end{aligned}$$

Since x^{2n} and yx^{2n-1} are linearly independent in R/R_{2k-1}, we get $\varphi(w_n) = ab\varphi(v_n)$ and $\mathfrak{b}_\varphi(v_n, w_n) = 0$. □

Theorem 2.4.4. *Assuming hypotheses of previous proposition, the following are true:*

1. *There exists a* 2*-dimensional subspace* W *of* V *such that* $\varphi|_W \cong c\langle 1, ab\rangle$, *for some* $c \in K^*$.

2. *There exists a non-zero vector* $\tilde{\Upsilon} \in V \otimes_K R_{k-1}$ *such that* $\tilde{\varphi}(\tilde{\Upsilon}) = 0$ *where* $\tilde{\varphi} = a(\varphi|_W) \oplus (\varphi|_{W^\perp})$

Proof. 1. From proposition 2.4.3 we have $\varphi(w_n) = ab\varphi(v_n)$. As φ is anisotropic over K, both v_n and w_n are non-zero. Also $\mathfrak{b}_\varphi(v_n, w_n) = 0$. Therefore by theorem 2.1.11 φ contains the subform $\langle \varphi(v_n), \varphi(w_n)\rangle \cong \langle \varphi(v_n), ab\varphi(v_n)\rangle \cong \varphi(v_n)\langle 1, ab\rangle$.

2. Let $W = Kv_n \oplus Kw_n$. Then we can identify W with the two dimensional vector space $\dfrac{K[z]}{(z^2+ab)}$ by $w_n \to a$ and $\alpha = \sqrt{-ab} \to v_n$. Define the map

$$\begin{aligned} N : W &\to K \\ ae + \alpha f &\mapsto (ae)^2 + abf^2. \end{aligned}$$

We have $\Upsilon \in V \otimes_K R_k \backslash V \otimes_K R_{k-1}$ such that $\varphi(\Upsilon) = 0 \in R$. Now write $\Upsilon = s + t$ such that $s \in W \otimes_K R$ and $t \in W^\perp \otimes_K R$. From the construction of W, it is clear that $s \in W \otimes R_k = (ax + \alpha y)x^{k-1} + W \otimes R_{k-1}$ and $t \in W^\perp \otimes_K R_{k-1}$. We consider the following two cases:

Case I $k = 1$. Then $s = (ax+\alpha y)x^{k-1} + W \otimes R_{k-1} = (ax+\alpha y) + W \otimes R_0 = (ax+\alpha y) + W \otimes K = (ax+\alpha y) + W$. Therefore, there exists a $w = a\lambda_1 + \alpha\lambda_2 \in W$ such that

$$s = ax + \alpha y + w.$$

Also, we have

$$\begin{aligned} 0 = \varphi(\Upsilon) &= \varphi(s+t) = \varphi(s) + \varphi(t) \\ &= \varphi(ax + \alpha y + w) + \varphi(t) \\ &= \varphi(ax+\alpha y) + \varphi(w) + \mathfrak{b}_\varphi(ax+\alpha y, w) + \varphi(t) \\ &= c((ax)^2 + aby^2 + (a\lambda_1)^2 + ab\lambda_2^2 + a^2x\lambda_1 + aby\lambda_2) + \varphi(t) \\ &= c(a(ax^2+by^2) + (a\lambda_1)^2 + ab\lambda_2^2 + a^2x\lambda_1 + aby\lambda_2) + \varphi(t) \\ &= c(a + (a\lambda_1)^2 + ab\lambda_2^2 + a^2x\lambda_1 + aby\lambda_2) + \varphi(t) \end{aligned}$$

Reading above equation modulo K, we get

$$0 = a^2 x\lambda_1 + aby\lambda_2 \mod K.$$

As x and y are linearly independent vectors in R over K. Thus $\lambda_1 = 0, \lambda_2 = 0$ and hence $w = 0$ and $s = ax + \alpha y$.

Case II $k \geq 2$. Since $s = (ax + \alpha y)x^{k-1} + W \otimes R_{k-1}$, there exists vectors $w = a\mu_1 + \alpha\mu_2$ and $w' = a\lambda_1 + \alpha y$ in W such that

$$s = (ax + \alpha y)x^{k-1} + (ax + \alpha y)x^{k-2}w + x^{k-1}w' + s',$$

where $s' \in W \otimes_K R_{k-2}$. We have

$$\begin{aligned} 0 &= \varphi(\Upsilon) = \varphi(s + t) = \varphi(s) + \varphi(t) \\ &= \varphi((ax + \alpha y)u + x^{k-1}w' + s') + \varphi(t). \end{aligned}$$

Reading above equation modulo $R_{2(n-1)}$, we get

$$\begin{aligned} 0 &= \varphi((ax + \alpha y)(x^{k-1} + x^{k-2}w) + x^{k-1}w') \mod R_{2(k-1)} \\ &= \varphi((ax + \alpha y)(x^{k-1} + x^{k-2}w)) + \varphi(x^{k-1}w') + \mathfrak{b}_\varphi((ax + \alpha y)u, x^{k-1}w') \mod R_{2(k-1)} \\ &= c(N(ax + \alpha y)N((x^{k-1} + x^{k-2}w)) + 0 + \mathfrak{b}_N((ax + \alpha y)u, x^{k-1}w')) \mod R_{2(k-1)} \\ &= c(a \times 0 + \mathfrak{b}_N((ax + \alpha y)(x^{k-1} + x^{k-2}w), x^{k-1}w') \mod R_{2(k-1)} \\ &= c\mathfrak{b}_N((ax + \alpha y)x^{k-1}, x^{k-1}w') \mod R_{2(k-1)} \\ &= cx^{2(k-1)}\mathfrak{b}_N((ax + \alpha y), w') \mod R_{2(k-1)} \\ &= cx^{2(k-1)}(a^2 x\lambda_1 + aby\lambda_2) \mod R_{2(k-1)} \\ &= ca^2\lambda_1 x^{2k-1} + ab\lambda_2 x^{2(k-1)}y \mod R_{2(k-1)} \end{aligned}$$

As x^{2k-1} and $x^{2k-2}y$ are linearly independent vectors in R/R_{2k-2}, $\lambda_1 = 0, \lambda_2 = 0$. Thus $w = 0$ and $s = (ax + \alpha y)(x^{k-1} + x^{k-2}w) + s'$. Let $\tilde{\varphi} = a(\varphi|_W) \oplus \varphi|_{W^\perp}$. Take $\tilde{\Upsilon} = a^{-1}(ax - \alpha y)s + t$. From above two cases it follows that $\tilde{\Upsilon} \in V \otimes R_{k-1}$. Also

$$\begin{aligned} \tilde{\varphi}(\tilde{\Upsilon}) &= \tilde{\varphi}(a^{-1}(ax - \alpha y)s + t) = \tilde{\varphi}(a^{-1}(ax - \alpha y)s) + \tilde{\varphi}(t) \\ &= a\varphi|_W(a^{-1}(ax - \alpha y)s) + (\varphi|_{W^\perp}(t)) = aN(a^{-1})N(ax - \alpha y)N(s) + \varphi(t) \\ &= \varphi(s) + \varphi(t) = \varphi(s + t) = \varphi(\Upsilon) = 0 \in R. \end{aligned}$$

□

Observation 2.4.5 Let φ be a K-form which is anisotropic over K and become isotropic over $K(Q)$. Then in view of above theorem we have

1. $\varphi \cong c\langle 1, ab\rangle \oplus \varphi'$, for some $c \in K^*$.

2. The form $\varphi_1 \cong a(\varphi|_W) \oplus (\varphi|_{W^\perp}) \cong ac\langle 1, ab\rangle \oplus \varphi' \cong c\langle a, b\rangle \oplus \varphi'$.

Therefore φ and φ_1 represent the same anisotropy class in the Witt ring of $K(Q)$.

Corollary 2.4.6. *Let φ be an anisotropic quadratic form over K. Then there exists a form ψ over K such that anisotropic part of $\varphi_{K(Q)}$ is isometric to $\psi_{K(Q)}$*

Proof. We prove the result by induction on dimension of ϕ_{an}. If $\varphi_{K(Q)}$ is anisotropic then there is nothing to prove. Hence we assume $\varphi_{K(Q)}$ is isotropic. Since $K(Q)$ is a fraction field of R there exists an isotropic vector $0 \neq \Upsilon \in V \otimes_K R_k$, for some $k \in \mathbb{N}$. Let $k \in \mathbb{N}$ be the smallest number with the above property. If $k = 0$ then the quadratic form φ is already isotropic over K, which is not the case. Hence $k \neq 0$. Suppose $k \geq 1$. Since k is finite, applying the previous theorem k' times where $k' \leq k$ we get a K-form ψ such that ψ is isotropic over K and ψ represents the same anisotropy class as φ in the Witt ring of $K(Q)$. Since ψ_K is isotropic, $\dim((\psi)_{an}) < \dim(\varphi)$ and hence the result follows from the induction hypothesis. $\square$

Chapter 3

Pfister Forms

In §1 we define multiplicative and strictly multiplicative forms and give some examples. In next section we define Pfister forms and prove that Pfister forms are either anisotropic or hyperbolic over all field extensions and conversely. In the last section we prove some results for function fields of Pfister forms.

3.1 Multiplicative Forms

Let φ be an n-ary quadratic form over K, where $n \geq 1$. Let $x = (x_1, x_2, \ldots, x_n)^T$ and $y = (y_1, y_2, \ldots, y_n)^T$ be two n-dimensional indeterminate column vectors and $K(x, y)$ be the rational function field associated with x, y.

Definition 3.1.1 An n-ary quadratic form φ over K is said to be *multiplicative* if for x, y we have n-dimensional vector $z = (z_1, z_2, \ldots, z_n)^T$ over $K(x, y)$ such that

$$\varphi(x)\varphi(y) = \varphi(z). \tag{3.1}$$

Observe the fact if a multiplicative form φ represents a and b over a field L/K then φ will also represent the element ab over L. This observation leads us to the following theorem:

Theorem 3.1.2. *A regular quadratic form φ over K is multiplicative if and only if $D_L(\varphi)^*$ is a subgroup of L^*, where L is any extension field of K.*

Proof. Suppose φ is a multiplicative form over K. For any two n-dimensional indeterminate column vectors x, y, the quadratic form φ represents $\varphi(x)\varphi(y)$ over $K(x, y)$.

This implies that φ represents $\varphi(x)\varphi(y)$ over $L(x,y)$ as $K \subseteq L$. From substitution principle it follows that φ represent the element $\varphi(u)\varphi(v)$ over L, where u, v are two n-dimensional vectors over L. Hence for $a, b \in D_L(\varphi)^*$, $ab \in D_L(\varphi)^*$. Let $a \in D_L(\varphi)^*$ then there exists an n-dimensional column vector $u \in L^n$ such that $\varphi(u) = a$. Then

$$\varphi\left(\frac{u}{a}\right) = \frac{1}{a^2}\varphi(u) = \frac{1}{a}.$$

Which implies

$$\frac{1}{a} = \varphi\left(\frac{u}{a}\right) \in D_L(\varphi)^*.$$

Since $D_L(\varphi)^*$ is closed under multiplication and inversion, hence it is a subgroup of L^*.

Conversely, suppose $D_L(\varphi)^*$ is a subgroup of L^* for every extension field L of K. In particular, take the rational function field $L = K(x,y)$ and $\varphi(x), \varphi(y)$ in $D_L(\varphi)$. Then we have $\varphi(x)\varphi(y) \in D_L(\varphi)$. Hence the form φ is multiplicative.

Example 3.1.3 Every regular isotropic form is multiplicative as it is universal over any field and $D_K(\varphi)^* = K^*$.

Definition 3.1.4 An n-ary quadratic form φ over K is called *strictly multiplicative* if there exists a matrix $T_x \in M_n(K(x))$, such that for $z = T_x y$ we have

$$\varphi(x)\varphi(y) = \varphi(z) = \varphi(T_x y) \tag{3.2}$$

Since $K \subset K(x) \subset K(x,y)$, if φ is a quadratic form over K, φ can be considered a quadratic form over $K(x)$. In that case over $K(x)$ we can write

$$\varphi(x)\varphi \cong \varphi \tag{3.3}$$

Let $\varphi(x) = x^t A x$, where $A \in M_n(K)$ is the symmetric matrix of coefficients. In matrix notation, we can express the above condition as follows:

$$\varphi(x)\varphi(y) = \varphi(T_x y) \Leftrightarrow \varphi(x) y^t A y = (T_x y)^t A (T_x y)$$

Hence, in $M_n(K(x))$ we can write

$$\Leftrightarrow y^t(\varphi(x)A)y = (T_x y)^t A (T_x y) \Leftrightarrow \varphi(x)A = T_x^t A T_x.$$

Example 3.1.5

1. The one dimensional form x^2 is multiplicative as well strictly multiplicative. Take $T_x = (x)$.

2. Let $\varphi(x) = x_1^2 + x_2^2$ is multiplicative and as well strictly multiplicative. Let $x = (x_1, x_2)^T$ and $y = (y_1, y_2)^T$. Then we have

$$\varphi(x)\varphi(y) = (x_1^2 + x_2^2)(y_1^2 + y_2^2) = x_1^2y_1^2 + x_1^2y_2^2 + x_2^2y_1^2 + x_2^2y_2^2 = \\ (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2$$

Take $z = (z_1, z_2)^T$ such that $z_1 = x_1y_1 + x_2y_2$ and $z_2 = x_1y_2 - x_2y_1$ in $K(x, y)$. Also observe we can write

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

Hence φ is strictly multiplicative.

3.2 Pfister Forms

Strictly multiplicative quadratic forms have a specific structure which was determined by Pfister in [Pfi65] upto some extent. We begin with the following definition

Definition 3.2.1 Let $n \in \mathbb{N}$ and $a_1, a_2, \ldots, a_n \in K^*$. Then 2^n-dimensional quadratic form $\varphi = \langle 1, a_1\rangle \otimes \langle 1, a_2\rangle \otimes \ldots \otimes \langle 1, a_n\rangle$ is called a *Pfister form* and is denoted by $\langle\langle a_1, a_2, \ldots, a_n\rangle\rangle$.

Theorem 3.2.2. *Let $a_1, a_2, \ldots, a_n \in K^*$ and $k \geq 0$ be an integer, then the Pfister form $\varphi = \langle\langle a_1, a_2, \ldots, a_n\rangle\rangle$ is strictly multiplicative over K.*

Proof. We prove this result by induction on k. For $k = 0$, we have $\varphi = \langle 1\rangle$, $A = (1)$ and $T_x = (x)$ will give the result. Let $\varphi = \langle 1, a_1\rangle \otimes \langle 1, a_2\rangle \otimes \ldots \otimes \langle 1, a_n\rangle$ and suppose φ is strictly multiplicative. Let $\psi = \varphi \otimes \langle 1, a\rangle = \varphi \oplus a\varphi$. Since φ is strictly multiplicative we have $\varphi(x)\varphi = \varphi$ over the field $K(x)$. Substituting this in the previous equation we get

$$\psi = \varphi(x)\varphi \oplus a\varphi(y)\varphi = \langle\varphi(x), a\varphi(y)\rangle \otimes \varphi$$

over the field $K(x,y)$. Since $\langle \varphi(x), a\varphi(y)\rangle$ represents the element $\psi(x,y) = \varphi(x) + a\varphi(y)$ over the field $K(x,y)$, by corollary 1.1.13 we have

$$\begin{aligned}\langle \varphi(x), a\varphi(y)\rangle &= \langle \psi(x,y), a\varphi(x)\varphi(y)\psi(x,y)\rangle \\ &= \psi(x,y)\langle 1, a\varphi(x)\varphi(y)\rangle.\end{aligned}$$

Hence

$$\begin{aligned}\psi &= \psi(x,y)\langle 1, a\varphi(x)\varphi(y)\rangle \otimes \varphi \\ &\cong \psi(x,y)(\varphi \oplus a\varphi(x)\varphi(y)\varphi) \\ &\cong \psi(x,y)(\varphi \oplus a\varphi) \cong \psi(x,y)\psi\end{aligned}$$

This proves the theorem for ψ and we are done. $\square$

Corollary 3.2.3. *For any $n = 2^k$, where $k \geq 0$ is an integer, the form $\varphi = n \times \langle 1\rangle$ is strictly multiplicative.*

Proof. Take $a_i = 1$ for$1 \leq i \leq n$, and the corollary follows from the above theorem. $\square$

Theorem 3.2.4. *Let φ be an n- ary regular anisotropic quadratic form over K. Then following statements are equivalent:*

1. *φ is multiplicative.*
2. *φ is strictly multiplicative.*
3. *φ is a Pfister form.*

Proof. ($1 \Rightarrow 2$) Suppose φ is a multiplicative form then φ represents $\varphi(x)\varphi(y)$ over the field $K(x,y)$. Observe that $D_{K(x)}(\varphi(x)\varphi) \subseteq D_{K(x)}(\varphi)$. Since φ is anisotropic over $K(x)$, $\varphi(x)\varphi$ is isometric to a subform of φ over $K(x)$. Also $\dim \varphi(x)\varphi = \dim \varphi$ over $K(x)$ hence $\varphi \cong \varphi(x)\varphi$ over $K(x)$. Which implies φ is strictly multiplicative.

($2 \Rightarrow 3$) Suppose φ is a strictly multiplicative form of dimension n over K. Let k be the maximal integer such that φ contains the Pfister form $\psi = \langle\langle a_1, a_2, \ldots, a_k\rangle\rangle$ over K. We have to show that $\varphi \cong \psi$.
Suppose $\varphi \cong \psi \oplus \chi$, where $\dim \chi \geq 1$. Let $\chi \cong \langle b, \ldots\rangle$. Since φ is strictly multiplicative form we have

$$\varphi(x)\varphi \cong \varphi \text{ over } K(x)$$

where x is an n-dimensional indeterminate vector. Let $x = (z, \underbrace{0, \dots, 0}_{n-2^k})$, where z is a 2^k dimensional indeterminate vector then by above equation we get

$$\varphi \cong \psi(z)\varphi$$

over $K(z)$. Hence over $K(z)$, we can write

$$\psi \oplus \chi \cong \varphi \cong \psi(z)\varphi \cong \psi(z)\psi \oplus \psi(z)\chi \cong \psi \oplus \psi(z)\chi.$$

From Witt's cancellation theorem we conclude that $\chi \cong \psi(z)\chi$ over $K(z)$. Since χ represents b over K, it will represent $b\psi(z)$ over $K(z)$. Since χ is anisotropic hence by applying the subform theorem we conclude that $b\psi$ is a subform of χ. That is $\chi \cong b\psi \oplus \chi'$ over K. Hence

$$\varphi \cong \psi \oplus b\psi \oplus \chi' \cong \psi \otimes \langle 1, b\rangle \oplus \chi'$$

Which is a contradiction. Hence $\varphi \cong \psi$.

$(3 \Rightarrow 1)$. Theorem **??** implies that every Pfister form is strictly multiplicative and hence multiplicative. □

Observation 3.2.5 Every n-ary regular isotropic form over a field K is always multiplicative as if φ is isotropic it is universal over any field extension of K. Which implies φ will represent $\varphi(x)\varphi(y)$ over $K(x, y)$ and hence multiplicative.

Theorem 3.2.6. *An n-ary regular isotropic quadratic form φ over K is strictly multiplicative if and only if*

$$\varphi \cong i \times \langle 1, -1\rangle$$

Proof. Let φ be an n-ary isotropic strictly multiplicative form over K. Let $\varphi \cong i \times \langle 1, -1\rangle \oplus \varphi_0$ with $i \geq 1$ and φ_0 anisotropic, be the Witt's decomposition of φ. Then over field $K(x)$, we get

$$\begin{aligned} i \times \langle 1, -1\rangle \oplus \varphi_0 &\cong \varphi \\ &\cong \varphi(x)\varphi \\ &\cong \varphi(x)(i \times \langle 1, -1\rangle \oplus \varphi_0) \\ &\cong i \times \varphi(x)\langle 1, -1\rangle \oplus \varphi(x)\varphi_0. \end{aligned}$$

Since $\langle 1, -1\rangle \cong \varphi(x)\langle 1, -1\rangle$, hence applying Witt's cancellation theorem, we get

$$\varphi_0 \cong \varphi(x)\varphi_0 \text{ over } K(x)$$

Suppose $\varphi_0 \neq 0$, then $\dim(\varphi_0) \geq 1$. Let $\varphi_0 = \langle b, \ldots \rangle$ then φ_0 represents $b\varphi(x)$ (from the previous identity). Since φ_0 is anisotropic, using subform theorem we deduce that φ_0 contains $b\varphi$. It is a contradiction as $\dim(\varphi) > \dim(\varphi_0)$.

Conversely, Let $\varphi \cong i \times \langle 1, -1 \rangle$. Clearly $\langle 1, -1 \rangle \cong \varphi(x)\langle 1, -1 \rangle$, for $\varphi(x) \in K(x)$. Which implies $\varphi \cong \varphi(x)\varphi$ over $K(x)$. Hence φ is strictly multiplicative. $\square$

Remark 3.2.7 In theorem 3.2.2 we have proved that every Pfister form is strictly multiplicative. From the above theorem it follows that if a Pfister form is isotropic then it is hyperbolic.

Example 3.2.8 The form $\varphi = x_1x_2 + x_3^2$ is multiplicative but not strictly multiplicative.

Corollary 3.2.9. *If $D_K(n)^* = D_K(n \times \langle 1 \rangle)^*$ is a subgroup of K^* for every field K, then n is a power of 2.*

Proof. Since $D_K(n \times \langle 1 \rangle)^*$ is a subgroup of K^*, theorem 3.1.2 implies that $\varphi = n \times \langle 1 \rangle$ is a multiplicative form. Also φ is anisotropic and hence by theorem 3.2.4 φ is isometric to a Pfister form. Thus $n = 2^k$, for some $k \geq 0$. $\square$

The following theorem is the main result of this chapter:

Theorem 3.2.10. *Let φ be a quadratic form over K. Then φ is isometric to an n-fold Pfister form if and only if $\dim \varphi = 2^n$ and for every field extension L/K, φ_L is either anisotropic or hyperbolic.*

Proof. Suppose φ is isometric to an n-fold Pfister form φ then $\dim(\varphi) = 2^n$. Let L/K be any field extension. If φ_L remain anisotropic then we are done. Otherwise if φ_L is isotropic then by remark 3.2.7 φ_L hyperbolic.

Conversely, suppose $\dim \varphi = 2^n$ and for every field extension L/K, φ_L is either anisotropic or hyperbolic. If φ is hyperbolic over K then we are done. Suppose φ is anisotropic over K. Then for $L = K[\varphi]$, φ_L is isotropic and hence hyperbolic. Hence $\varphi(X)\varphi \cong \varphi$ over rational function field $K(X)$. Since φ is strictly multiplicative and φ is anisotropic, by theorem 3.2.4 it is a Pfister form. $\square$

3.3 Function Fields of Pfister Forms

In chapter 2 we introduced the notion of function field of a quadratic form. Since Pfister form assumes some special properties we see some results for function field of Pfister forms.

Theorem 3.3.1. *Let φ be a Pfister form. Let ψ be an anisotropic form over K. Then ψ becomes hyperbolic over the function field $K(\varphi)/K$ if and only if $\psi \cong \varphi \otimes \rho$ for some quadratic form ρ over K.*

Proof. Suppose ψ becomes hyperbolic over the function field $K(\varphi)/K$. Since φ is a Pfister form it represents 1. Then as the form ψ is anisotropic, theorem 2.3.2 implies that $\varphi(x)\psi \cong \psi$ over $K(X)$. Let ψ represent $a \in K^*$. Then $D_K(a\phi)^* \subseteq D_K(\psi)^*$. Now by subform theorem 2.1.11, $a\varphi$ is a subform of ψ. Thus $\psi \cong a\varphi \oplus \psi_0$ for some K-form ψ_0. Since the forms ψ and φ becomes hyperbolic over the field $K(\varphi)$ so is the form ψ_0. Now applying the induction hypothesis we get $\psi_0 \cong \varphi \otimes \rho_0$ for some K-quadratic form ρ_0. Therefore $\psi \cong a\varphi \oplus \psi_0 \cong a\varphi \oplus \varphi \otimes \rho_0 \cong \varphi \otimes \rho$, where $\rho = \langle a \rangle \oplus \rho_0$.

Since φ becomes isotropic over $K(\varphi)$, being a Pfister form it becomes hyperbolic over $K(\varphi)$ and the converse follows. □

Corollary 3.3.2. *Let φ and ψ be in the previous theorem. If ψ is also a Pfister form then $\psi \cong \varphi \otimes \rho$ for some Pfister form ρ over K.*

Proof. From the previous theorem $\psi \cong \varphi \otimes \rho$ for some K-form ρ. Since ψ and φ are both Pfister forms we can assume that ρ represents 1. Then we can write $\rho \cong \langle 1, a, \ldots \rangle$. Since ψ becomes hyperbolic over $K(\varphi)$, ψ becomes hyperbolic over $K(\varphi \otimes \langle\langle a \rangle\rangle)$. From the previous theorem $\psi \cong \varphi \otimes \langle\langle a \rangle\rangle \otimes \rho'$ for some K-quadratic forms ρ'. By proceeding in the same way we get the result. □

Corollary 3.3.3. *Let Q be a quaternion algebra and $K(Q)$ be its function field. Let φ be an anisotropic quadratic form over K and $N = \langle 1, -a, -b, ab \rangle$ be the norm form of Q. Then $\varphi_{K(Q)}$ is hyperbolic if and only if $\varphi \cong \psi \otimes N$.*

Before proving the corollary we mention the fact that if $N = \langle 1, -a, -b, ab \rangle$ is the norm form of quaternion algebra $Q = (a, b)_K$ then a K-quadratic form φ becomes hyperbolic over $K(Q)$ if and only if it becomes hyperbolic over the function field $K(N)$, see [Lam05, p. 347].

Proof. "If" part is clear. Conversely suppose φ is an anisotropic quadratic form over K and φ becomes hyperbolic over $K(Q)$ if and only if it becomes hyperbolic over the field $K(N)$. Since N is a Pfister and φ becomes hyperbolic over $K(N)$, by theorem 3.3.1

$$\varphi \cong N \otimes \rho$$

For some K quadratic form ρ. $\square$

Chapter 4

Central Simple Algebras

In this chapter we discuss some results in the theory of central simple algebras which shall be used in later chapters. In §1 we present some classic examples of central simple algebras such as matrix algebras and quaternion algebras. In next section tensor product of algebras is defined and some important properties of tensor products of quaternion algebras and matrix algebras are proved. In §3 we explore properties of a central simple algebra over an extention of field of scalars. In the last section we define the notion of Brauer group with some examples.

4.1 Introduction and Examples

Throughout this chapter K denote a field with $\operatorname{char} K \neq 2$ and K^* will denote the multiplicative group of K. All algebras occurring in discussions are finite dimensional over K.

Definition 4.1.1 A K-algebra $\mathcal{A}$ is said to be *simple* if it has no two-sided ideal other than 0 and $\mathcal{A}$. It is said to be *central* if center of $\mathcal{A}$ is equal to K. A K-algebra is a *central simple algebra* if it is both central and simple. Matrix algebras and quaternion algebras, which we define in the following discussion are main examples of central simple algebras.

4.1.1 Matrix Algebra

Let $M_n(K)$ be the collection of all $(n \times n)$ matrices over K. The entry at i^{th} row and j^{th} column of a matrix A is denoted by A_{ij} and identity matrix of $M_n(K)$ is denoted by I_n. As a vector space over K the dimension of $M_n(K)$ is n^2. Moreover, we have a multiplicative structure on $M_n(K)$, which is associative and distributes over addition. Hence $M_n(K)$ forms a K-algebra with usual matrix addition, multiplication and scalar multiplication. The following theorem proves that matrix algebras are central simple.

Theorem 4.1.2. *The matrix algebra $M_n(K)$ has the following properties:*

1. *It has no two sided ideal other than 0 and itself.*

2. *A matrix $A \in M_n(K)$ lies in the center of $M_n(K)$ if and only if A is of the form λI_n. In other words, center of $M_n(K)$ is canonically isomorphic to K.*

Proof. 1. Let E_{ij} denote the matrix whose $(i,j)^{th}$ entry is 1 and all other entries are 0. Observe that

$$E_{ij}E_{kl} = 0 \quad \text{ if } j \neq k$$
$$E_{ij}E_{jl} = E_{il} \text{ if } j = k$$

Let $A \in M_n(K)$ be a non zero matrix with $A_{ij} \neq 0$, then for any $1 \leq k \leq n$ we have

$$A_{ij}^{-1} E_{ki} A E_{jk} = E_{kk}.$$

Therefore any non zero ideal will contain the identity matrix $I_n = \sum_{k=1}^{n} E_{kk}$ and hence it is the whole ring $M_n(K)$.

2. Clearly λI_n lies in center of $M_n(K)$. Conversely, suppose $A \in M_n(K)$ is in the center of $M_n(K)$. Then A commutes with all elements of $M_n(K)$. In particular we have

$$AE_{ij} = E_{ij}A.$$

Hence, for all $1 \leq i, j \leq n$

$$A_{ii} = A_{jj} = \lambda \text{ (say)}$$

and for all $i \neq j$

$$A_{ij} = 0.$$

Thus if A lies in the center then it is of the form λI_n, where $\lambda \in K$.

□

4.1.2 Quaternion Algebra

Recall that for $a, b \in K^*$, a *K-quaternion algebra* $Q = (a, b)_K$ is a K-algebra generated by two elements i, j with the following multiplication rule:

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

In view of the above rules of multiplication in Q, it is easy to observe that Q is a 4-dimensional vector space over K with basis $\{1, i, j, ij\}$. This basis is called *standard basis of Q*.

Proposition 4.1.3. *For $a, b \in K^*$, the following are true:*

1. *$(a, b)_K \cong (\lambda^2 a, \mu^2 b)_K$ for each $\lambda, \mu \in K^*$*
2. *$(a, b)_K \cong (b, a)_K$.*

Proof.

1. Let $\{1, i, j, ij\}$ be the standard basis of $(a, b)_K$. Define $\Theta : (a, b)_K \to (\lambda^2 a, \mu^2 b)_K$ on the basis elements as follows:

$$1 \mapsto 1, \quad i \mapsto \lambda^{-1} i, \quad j \mapsto \mu^{-1} j, \quad ij \mapsto \lambda^{-1}\mu^{-1} ij$$

and extend Θ linearly. Clearly Θ is a K-homomorphism. As all basis elements of $(\lambda^2 a, \mu^2 b)_K$ are in the image of Θ, therefore Θ is surjective. Since dimensions of spaces are equal, hence Θ is an isomorphism.

2. The standard bases of $(a, b)_K$ and $(b, a)_K$ are $(1, i, j, ij)$ and $(1, j, i, ji)$ respectively. Define $\Theta : (a, b)_K \to (b, a)_K$ on the basis elements as follows:

$$1 \mapsto 1, \quad i \mapsto j, \quad j \mapsto i, \quad ij \mapsto ji.$$

and extend it linearly. Then Θ is a K-homomorphism and for the same reason as in (1) it is an isomorphism.

□

Definition 4.1.4 Let $q = x_1 + x_2 i + x_3 j + x_4 ij \in (a, b)_K$ be an element with $x_i \in K$. Then we define *conjugate of q* by $\overline{q} = x_1 - x_2 i - x_3 j - x_4 ij$.

The conjugation defines a map $^- : (a, b)_K \to (a, b)_K$ such that for $q_1, q_2, q \in (a, b)_K$ it satisfies the following properties:

1. $\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$

2. $\overline{q_1 q_2} = \overline{q_2 q_1}$

3. $\overline{\overline{q}} = q$

Definition 4.1.5 Let $q = x_1 + x_2 i + x_3 j + x_4 ij \in (a,b)_K$, $x_i \in K$. The *Norm* of q is defined as $N(q) = q\overline{q} = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 \in K$. The quadratic form $N = \langle 1, -a, -b, ab \rangle$ is called the *norm form* of Q.

Example 4.1.6 Hamilton Quaternion is a classic example of quaternion algebras. Let $K = \mathbb{R}$. Then $Q = (-1,-1)_{\mathbb{R}}$ is a quaternion algebra over $\mathbb{R}$. Also for any $0 \neq x_1 + x_2 i + x_3 j + x_4 ij \in Q$, $N(q) = x_1^2 + x_2^2 + x_3^2 + x_4^2 > 0$. Hence

$$q^{-1} = \frac{x_1 - x_2 i - x_3 j - x_4 ij}{x_1^2 + x_2^2 + x_3^2 + x_4^2}.$$

Since every nonzero element in Q is invertible, Q is a division ring.

Example 4.1.7 The Matrix Algebra ($M_2(K)$) The matrix algebra $M_2(K)$ is a quaternion algebra over K. The quaternion algebra $(1,b)_K \cong M_2(K)$ and isomorphism is given by

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & b \\ -1 & 0 \end{pmatrix},$$

where $\{1, i, j, ij\}$ is the standard basis of $(1,b)_K$

The following theorem gives equivalent conditions for Q being split *i.e.* $Q \cong M_2(K)$.

Theorem 4.1.8. *Let $Q \cong (a,b)_K$ be a quaternion algebra. The following statements are equivalent:*

1. *$Q \cong M_2(K)$.*

2. *Q is not a division algebra.*

3. *The norm form of Q has a non-trivial zero.*

Proof. ($1 \Rightarrow 2$) is clear.
($2 \Rightarrow 3$) Suppose Q is not a division algebra then there exists a $0 \neq q \in Q$, which is non invertible. Since an element of Q is non invertible if and only if its norm is non-zero. Therefore in this case $N(q) = 0$. Hence norm form has a non trivial zero and hence the implication follows.

($3 \Rightarrow 1$) Now suppose norm form has a non trivial zero. Let $x_1^2 - x_2^2 a - x_3^2 b + x_4^2 ab = 0$, where $x_k \neq 0$ at least for some $1 \leq k \leq 4$. We have the following cases:

- If x_3 and x_4 are both 0. Observe that in this case x_1 and x_2 are both non-zero as one dimensional form is always anisotropic over any field. Hence we get

$$x_1^2 - x_2^2 a = 0 \Rightarrow a = \left(\frac{x_1}{x_2}\right)^2$$

  Hence $(a, b)_K \cong (1, b)_K \cong M_2(K)$ follows from proposition 4.1.3 and example 4.1.7.

- If at least one of the x_3 and x_4 is non-zero. Let $\{1, i, j, ij\}$ be the standard basis of $(a, b)_K$. Then

$$\begin{aligned}
0 &= (x_1^2 - x_2^2 a) - b(x_3^2 - x_4^2 a) \\
\Rightarrow b &= (x_1^2 - x_2^2 a)/(x_3^2 - x_4^2 a) \\
&= N(x_1 + x_2 i)N(x_3 + x_4 i)^{-1} \\
&= N((x_1 + x_2 i)(x_3 + x_4 i)^{-1}) \\
&= \alpha^2 - a\beta^2,
\end{aligned}$$

  for some $\alpha, \beta \in K$. Let $u = rj + sij \in Q$, where $r = \dfrac{\alpha}{\alpha^2 - a\beta^2}$ and $s = \dfrac{\beta}{\alpha^2 - a\beta^2}$. Then $u^2 = br - abs^2 = 1$. Also, observe $ui = -iu$, hence $\{1, u, i, ui\}$ forms a basis of $Q = (a, b)_K$. Hence $(a, b)_K \cong (1, a)_K \cong M_2(K)$ follows from example 4.1.7.

$\square$

Corollary 4.1.9. *For any $a \in K$, the following are true:*

1. *$(a, -a)_K \cong M_2(K)$.*
2. *If $a \neq 0, 1$, then $(a, 1 - a)_K \cong M_2(K)$*

Proof.

1. The norm form $\langle 1, -a, a, -a^2 \rangle \cong \langle 1, -1 \rangle \oplus a \langle 1, -1 \rangle$ of $(a, -a)_K$ is isotropic. Hence by previous theorem $(a, -a)_K \cong M_2(K)$.
2. If $a \neq 0, 1$ then $a, 1 - a \neq 0$. The norm form of $(a, 1-a)_K$ is $\langle 1, -a, a-1, a-a^2 \rangle$. Observe that $(1, 1, 1, 0)$ is an isotropic vector. Therefore $(a, 1 - a)_K \cong M_2(K)$

$\square$

Corollary 4.1.10. *For $a \in K^*$, the quaternion algebra $(-1, a)_K \cong M_2(K)$ if and only if $a \in K$ is a sum of two squares in K.*

Proof. From the previous theorem $(-1, a) \cong M_2(K)$ if and only if $\langle 1, 1, -a, -a \rangle$ is isotropic. Which is possible if and only if $\langle 1, 1, -a, -a \rangle \cong \langle 1, -1, \rangle \oplus \langle c, d \rangle$ if and only if $\langle c \rangle \cong \langle -d \rangle$. Therefore $\langle 1, 1, -a, -a \rangle \cong \langle 1, -1, c, -c \rangle$. Which implies $\langle 1, 1, -a, -a \rangle$ is hyperbolic. Hence the form $\langle 1, 1, -a \rangle$ is isotropic and we are done.

□

Remarks 4.1.11 Let $Q = (a, b)_K$. Then

1. Any element $q = x_1 + x_2 i + x_3 j + x_4 ij \in (a, b)_K$ is in center of Q if and only if q commutes with all basis elements. Which is possible if and only if $q \in K$. Hence center of $Q = (a, b)_K$ is K.

2. Quaternion algebra $Q = (a, b)_K$ is simple as Q is either a division algebra or isomorphic to $M_2(K)$. In both cases Q is simple.

4.2 Tensor Product

In this section we define tensor product and recall some important resutls of tensor product of matrix algebras and quaternion algebras.

Definition 4.2.1 Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ be K-algebras. A map $B : \mathcal{A} \times \mathcal{B} \to \mathcal{C}$ is called *balanced* if for all $a, a' \in \mathcal{A}, b, b' \in \mathcal{B}$ and $\lambda \in K$ it satisfies the following properties:

1. $B(a, b + b') = B(a, b) + B(a, b')$

2. $B(a + a', b) = B(a, b) + B(a', b)$

3. $B(a\lambda, b) = B(a, \lambda b)$

Definition 4.2.2 If $\mathcal{A}$ and $\mathcal{B}$ are K-algebras then *tensor product* of $\mathcal{A}$ and $\mathcal{B}$ is a pair $(\mathcal{T}, \tau)$, where $\mathcal{T}$ is a K-algebra and $\tau : \mathcal{A} \times \mathcal{B} \to \mathcal{T}$ is a balanced map such that for any other such pair $(\mathcal{S}, \delta)$, there exists a unique K-algebra homomorphism $h : \mathcal{T} \to \mathcal{S}$ such that $\delta = h \circ \tau$.

Remarks 4.2.3

1. Tensor product of two algebras $\mathcal{A}$ and $\mathcal{B}$ over K exists and we denote it by $\mathcal{A} \otimes_K \mathcal{B}$.

2. The tensor product of algebras is commutative and associative *i.e.*

   (a) $\mathcal{A} \otimes_K K \cong \mathcal{A}$.

   (b) $\mathcal{A} \otimes_K \mathcal{B} \cong \mathcal{B} \otimes_K \mathcal{A}$.

   (c) $\mathcal{A} \otimes_K (\mathcal{B} \otimes_K \mathcal{C}) \cong (\mathcal{A} \otimes_K \mathcal{B}) \otimes_K \mathcal{C}$.

3. If $\mathcal{A}$ is a K-algebra with basis $\{a_1, a_2, \dots a_m\}$ and $\mathcal{B}$ is K-algebra with basis $\{b_1, b_2 \dots b_n\}$ then the set $\{a_i \otimes b_j : 1 \leq i \leq m, 1 \leq i \leq n\}$ constitutes a basis of $\mathcal{A} \otimes \mathcal{B}$.

4.2.1 Tensor Product and Matrix Algebras

Theorem 4.2.4. *Let $\mathcal{A}$ be a finite dimensional K-algebra. Then*

$$M_n(K) \otimes_K \mathcal{A} \cong M_n(\mathcal{A})$$

Proof. Define the map $B : M_n(K) \times \mathcal{A} \to M_n(\mathcal{A})$ such that any pair $(M, a) \in M_n(K) \times \mathcal{A}$ maps to the matrix whose $(i,j)^{th}$ entry is $M_{ij} \cdot a$. Clearly the map B is a balanced map. Hence there exists a unique K-homomorphism $h : M_n(K) \otimes_K \mathcal{A} \to M_n(\mathcal{A})$ such that the following diagram commutes:

$$\begin{tikzcd}
M_n(K) \times \mathcal{A} \arrow[r, "B"] \arrow[d, "\tau"'] & M_n(\mathcal{A}) \\
M_n(K) \otimes \mathcal{A} \arrow[ur, "h"'] &
\end{tikzcd}$$

We show h is an isomorphism. Let E_{ij} be the matrix whose $(i,j)^{th}$ entry is 1 and all other entries are 0. For any $a \in \mathcal{A}$, $B(E_{ij}, a)$ is the matrix in $M_n(\mathcal{A})$ whose $(i,j)^{th}$ entry is a and all other entries are 0. Hence B is surjective. As h is the unique homomorphism such that $B = h \circ \tau$ therefore h is surjective. Since A is finite dimensional algebra over K, $\dim M_n(\mathcal{A}) = \dim M_n(K) \otimes_K \mathcal{A}$, h is injective. $\square$

Corollary 4.2.5. $M_m(K) \otimes_K M_n(K) \cong M_{mn}(K)$.

4.2.2 Tensor Product of Quaternion Algebras

Proposition 4.2.6. *Let $Q_1 = (a,b)_K$ and $Q_2 = (a,b')_K$ be two quaternion algebras. Then*

$$Q_1 \otimes_K Q_2 \cong (a,bb')_K \otimes_K M_2(K).$$

Proof. Let $\{1,i,j,k\}$ and $\{1,i',j',k'\}$ be the standard bases of quaternion algebras Q_1 and Q_2 respectively. To prove the result, we construct a basis of quaternion algebra (a,bb') as a subalgebra of $Q_1 \otimes Q_2$.
Let $I = i \otimes 1$ and $J = j \otimes j'$. Consider the 4-dimensional subspacce Q_3 of $Q_1 \otimes_K Q_2$ with basis $\{1, I, J, IJ\}$. Since Q_3 is multiplicatively closed it is a subalgebra and observe that

$$\begin{aligned}
I^2 &= (i \otimes 1)(i \otimes 1) = i^2 \otimes 1 = a \otimes 1 = a(1 \otimes 1),\\
J^2 &= (j \otimes j')(j \otimes j') = (j^2 \otimes j'^2) = b \otimes b' = bb' \otimes 1 = bb'(1 \otimes 1),\\
IJ &= (i \otimes 1)(j \otimes j') = ij \otimes j' = -ji \otimes j' = -(j \otimes j')(i \otimes 1) = -JI.
\end{aligned}$$

Clearly Q_3 is a quaternion algebra and $Q_3 \cong (a,bb')_K$.

Let $I' = (1 \otimes j')$ and $J' = i \otimes i'j'$ and Q_4 be a 4-dimensional subspace of $Q_1 \otimes_K Q_2$ with basis $\{1, I', J', I'J'\}$. Since Q_4 is also multiplicatively closed and hence a subalgebra and observe that

$$\begin{aligned}
I'^2 &= (1 \otimes j')(1 \otimes j') = 1 \otimes j'^2 = 1 \otimes b' = b,\\
J'^2 &= (i \otimes i'j')(i \otimes i'j') = (i^2 \otimes -i'^2 j'^2) = a \otimes -ab' = -a^2 b' \otimes 1 = -a^2 b',\\
I'J' &= (1 \otimes j')(i \otimes i'j') = i \otimes -i'j'^2 = -(i \otimes i'j')(1 \otimes j') = -J'I'.
\end{aligned}$$

Hence Q_4 is a quaternion algebra and $Q_4 \cong (b', -a^2 b')_K \cong (b', -b')$. From corollary 4.1.9, $Q_4 \cong M_2(K)$.

Consider the map $\Theta : Q_3 \times_K Q_4 \to Q_1 \otimes_K Q_2$ defined as $\Theta(q_3, q_4) = q_3 \cdot q_4$. Hence by the definition of tensor product there exists a unique map h such that the following diagram is commutative:

$$\begin{tikzcd}
Q_3 \times Q_4 \arrow[r, "\Theta"] \arrow[d, "\tau"'] & Q_1 \otimes_K Q_2 \\
Q_3 \otimes_K Q_4 \arrow[ur, "h"'] &
\end{tikzcd}$$

Clearly the map θ is surjective, therefore h is surjective. Since $\dim_K Q_3 \otimes_K Q_4 = \dim_K Q_1 \otimes_K Q_2$, h has to be injective. Hence the result follows. $\square$

Corollary 4.2.7. *Let $Q = (a,b)_K$. Then the biquaternion algebra $Q \otimes_K Q \cong M_4(K)$.*

Proof. $(a,b)_K \otimes_K (a,b)_K \cong (a,b^2) \otimes_K M_2(K) \cong (a,1)_K \otimes_K M_2(K) \cong M_2(K) \otimes_K M_2(K) \cong M_4(K)$. $\square$

4.3 Central Simple Algebras

In this section we further develop the theory of central simple algebras. Basic references for the content in this section are [Sch85, Chapter 8] and [KMRT98, Chapter 1].

4.3.1 Centers and Tensor Products

Let $\mathcal{A}$ be a central simple algebra over K and $\mathcal{B}$ be a subset of $\mathcal{A}$. Then we define *centralizer of $\mathcal{B}$ in $\mathcal{A}$* as follows:

$$Z_{\mathcal{A}}(\mathcal{B}) = \{a \in \mathcal{A} : ab = ba \text{ for all } b \in \mathcal{B}\}.$$

Proposition 4.3.1. *Let $\mathcal{A}$ and $\mathcal{B}$ be two K-algebras. For subalgebras $\mathcal{A}' \subseteq \mathcal{A}$ and $\mathcal{B}' \subseteq \mathcal{B}$, we have*

$$Z_{\mathcal{A}\otimes\mathcal{B}}(\mathcal{A}' \otimes_K \mathcal{B}') = Z_{\mathcal{A}}(\mathcal{A}') \otimes_K Z_{\mathcal{B}}(\mathcal{B}').$$

Proof. We show the following inclusions:

(a) $Z_{\mathcal{A}\otimes\mathcal{B}}(\mathcal{A}' \otimes_K \mathcal{B}') \subseteq Z_{\mathcal{A}}(\mathcal{A}') \otimes_K Z_{\mathcal{B}}(\mathcal{B}')$.

(b) $Z_{\mathcal{A}}(\mathcal{A}') \otimes_K Z_{\mathcal{B}}(\mathcal{B}') \subseteq Z_{\mathcal{A}\otimes\mathcal{B}}(\mathcal{A}' \otimes_K \mathcal{B}')$.

(a) Let $x \in Z_{\mathcal{A}\otimes\mathcal{B}}(\mathcal{A}' \otimes_K \mathcal{B}')$ and $\{b_1, b_2, \ldots, b_n\}$ be a basis of $\mathcal{B}$. We write

$$x = x_1 \otimes b_1 + x_2 \otimes b_2 + \ldots + x_n \otimes b_n,$$

where $x_i \in \mathcal{A}, 1 \leq i \leq n$ are uniquely determined. As x commutes with every element of $\mathcal{A}' \otimes_K \mathcal{B}'$,for every $a \in \mathcal{A}'$ it will commute with $a \otimes 1$. Hence

$$(a \otimes 1)x = x(a \otimes 1)$$
$$\Rightarrow ax_1 \otimes b_1 + ax_2 \otimes b_2 + \ldots ax_n \otimes b_n = x_1 a \otimes b_1 + x_2 a \otimes b_2 + \ldots + x_n a \otimes b_n.$$

Since such representation of any element in $\mathcal{A}' \otimes_K \mathcal{B}'$ is unique, for all $1 \leq i \leq n$, $ax_i = x_i a$ and hence $x_i \in Z_{\mathcal{A}}(\mathcal{A}')$. Thus we get $x \in Z_{\mathcal{A}}(\mathcal{A}') \otimes_K \mathcal{B}$. Let $\{c_1, c_2, \ldots c_r\}$ be a basis of $Z_{\mathcal{A}}(\mathcal{A}')$. Then we write

$$x = c_1 \otimes z_1 + c_2 \otimes z_2 + \ldots + c_r \otimes z_r,$$

where $z_j \in \mathcal{B}, 1 \leq j \leq r$ are uniquely determined. For every $b \in \mathcal{B}'$, x will commute with $(1 \otimes b)$. Hence

$$(1 \otimes b)x = x(1 \otimes b)$$
$$\Rightarrow c_1 \otimes bz_1 + c_2 \otimes bz_2 + \ldots c_r \otimes bz_r = c_1 \otimes z_1 b + c_2 \otimes z_2 b + \ldots + c_r \otimes z_r b.$$

By the same argument as above we have $z_j \in Z_{\mathcal{B}}(\mathcal{B}')$ for all $1 \leq j \leq r$. Hence $x \in Z_{\mathcal{A}}(\mathcal{A}') \otimes_K Z_{\mathcal{B}}(\mathcal{B}')$. Which implies $Z_{\mathcal{A}\otimes\mathcal{B}}(\mathcal{A}' \otimes_K \mathcal{B}') \subseteq Z_{\mathcal{A}}(\mathcal{A}') \otimes_K Z_{\mathcal{B}}(\mathcal{B}')$.

(b) This is clear from the definition of tensor product and centralizer.

□

Corollary 4.3.2. *If K-algebras $\mathcal{A}$ and $\mathcal{B}$ are central then $\mathcal{A} \otimes_K \mathcal{B}$ is central.*

Proposition 4.3.3. *If $\mathcal{A}$ is a central simple algebra and $\mathcal{B}$ is simple, then $\mathcal{A} \otimes_K \mathcal{B}$ is simple.*

Proof. We show that every non zero ideal of $\mathcal{A} \otimes_K \mathcal{B}$ is equal to itself. Let I be a non zero ideal of $\mathcal{A} \otimes_K \mathcal{B}$ and $\{b_1, b_2, \ldots, b_n\}$ be a basis of $\mathcal{B}$. Then it contain a non-zero element. We choose an element $0 \neq x \in I$ with representation

$$x = a_1 \otimes b_1 + a_2 \otimes b_2 + \ldots + a_r \otimes b_r$$

such that r is the smallest amongst all such representations of all elements of I. We have the following cases:

(a) When $r = 1$. Then $x = a \otimes b$. Let I_a be the two sided ideal of $\mathcal{A}$ generated by a. Then being a non zero ideal of $\mathcal{A}$, $I_a = \mathcal{A}$, as $\mathcal{A}$ is simple. That is $1 \in I_a$ and hence there exist finite $a_i, a_i' \in \mathcal{A}$ such that

$$\sum_i a_i a a_i' = 1$$
$$\Rightarrow \sum_i (a_i \otimes 1)(a \otimes b)(a_i' \otimes 1) = 1 \otimes b.$$

Hence $1 \otimes b \in I$. Since $\mathcal{B}$ is also simple, by the same argument we say $1 \otimes 1 \in I$.

(b) If $r > 1$. Then a_r and a_{r-1} are linearly independent, otherwise

$$a_r = \lambda a_{r-1}$$
$$\Rightarrow a_{r-1} \otimes b_{r-1} + a_r \otimes b_r = a_{r-1} \otimes (\lambda b_{r-1} + b_r).$$

Which contradicts the minimality of r. We can assume that a_r is 1 as $\mathcal{A}$ is simple. Since $\mathcal{A}$ is central, there exists an element in $\mathcal{A}$ such that

$$aa_{r-1} \neq a_{r-1}a.$$

Consider the following element

$$(a \otimes 1)x - x(a \otimes 1) = (aa_1 - a_1a) \otimes b_1 + \ldots + (aa_{r-1} - a_{r-1}a) \otimes b_{r-1}.$$

Since $b_1, \ldots, b_r$ are linearly independent and $aa_{r-1} - a_{r-1}a \neq 0$, right hand side of the above equation is not zero. Therefore the element $(a \otimes 1)x - x(a \otimes 1)$ is a non zero element of I with smaller r. which is a contradiction and hence $r = 1$.

□

Theorem 4.3.4. *If $\mathcal{A}$ and $\mathcal{B}$ are central simple algebras then $\mathcal{A} \otimes_K \mathcal{B}$ is also a central simple algebra.*

Proof. The theorem is an immediate consequence of propostion 4.3.1 and 4.3.3. □

4.3.2 Fundamental Theorems

We refer [Sch85, Chapter 8] for content of this section. In theorem 4.1.2 we proved that the matrix algebra is a central simple algebra. In a similar manner we can prove that for a central division algebra and $n \in \mathbb{N}$, matrix algebra $M_n(D)$ is central simple. In fact the converse is also true. In 1907, Wedderburn proved the following result:

Theorem 4.3.5. *Let $\mathcal{A}$ be a simple ring. Then $\mathcal{A} \cong M_n(D)$ for a suitable division ring D. Furthermore, n and D are uniquely determined upto isomorphism.*

Another important result in our context is Skolem-Noether theorem which relates algebra homomorphisms and inner automorphisms.

Definition 4.3.6 Let $\mathcal{A}$ be a K-algebra and u be an invertible element of $\mathcal{A}$. Then the map $Int(u) : \mathcal{A} \to \mathcal{A}$ defined by $x \mapsto uxu^{-1}$ is an automorphism of $\mathcal{A}$. Automorphisms of this kind are called *inner automorphisms* of $\mathcal{A}$.

Theorem 4.3.7. ***(Skolem-Noether, 1927)*** *Let $\mathcal{A}$ be a finite dimensional simple K-algebra and $\mathcal{B}$ be a finite dimensional simple K-algebra. If $f, g : \mathcal{A} \to \mathcal{B}$ are two K-algebra homomorphisms, then there exists an invertible element $u \in \mathcal{B}$ such that $f = Int(u) \circ g$.*

Corollary 4.3.8. *Every automorphism of a central simple algebra $\mathcal{A}$ is an inner automorphism.*

Notation If $\mathcal{A}$ is a central simple algebra over K and L/K is a field extension then $\mathcal{A}_L$ will denote the L-algebra $\mathcal{A} \otimes_K L$ with scalar multiplication defined through the map $l \mapsto 1 \otimes l$, for $l \in L$.

Proposition 4.3.9. *The L-algebra $\mathcal{A}_L$ satisfies the following properties:*

1. $\dim_K(\mathcal{A}) = \dim_L(\mathcal{A}_L)$.

2. *If $\mathcal{A}$ is a central simple algebra over K and L/K is a field extension then $\mathcal{A}_L$ is a central simple algebra over L.*

Proof. 1. Let $\{a_1.a_2, \dots, a_n\}$ and $\{l_1, l_2, \dots, l_m\}$ be K-bases of $\mathcal{A}$ and L respectively. Let $x \in \mathcal{A}_L$ be an arbitary element. Then

$$\begin{aligned} x &= \sum_{j=1}^{m} (\sum_{i=1}^{n} (\lambda_{ij} a_i) \otimes l_j) \\ &= \sum_{j=1}^{m} l_j (\sum_{i=1}^{n} (\lambda_{ij} a_i) \otimes 1) \\ &= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} (\lambda_{ij} l_j) \right) (a_i \otimes 1). \end{aligned}$$

Hence $\{a_1 \otimes 1, a_2 \otimes 1, \dots, a_n \otimes 1\}$ forms a L-basis of $\mathcal{A}_L$ and therefore

$$\dim_L(\mathcal{A}_L) = \dim_K(\mathcal{A}) = n.$$

2. This is true in view of 4.3.1 and 4.3.3

□

Definition 4.3.10 Let $\mathcal{A}$ be a central simple algebra over K. An extension field L over K is called a *splitting field* of $\mathcal{A}$ if $\mathcal{A}_L \cong M_n(L)$.

Remarks 4.3.11 Let $\mathcal{A}$ be a central simple algebra.

1. Let L be any algebraically closed field then upto isomorphism there is only one division algebra over L namely itself. Hence from Wedderburn's theorem any central simple algebra over L is isomorphic to $M_n(L)$. In particular algebraic closure of a field K is a splitting field of any central simple algebra $\mathcal{A}$ over K. Therefore the set of splitting field is non-empty.

2. Let L be any splitting field of K. In view of the property (1) we have

$$\dim_K(\mathcal{A}) = \dim_L(\mathcal{A}_L) = \dim_L(M_n(L)) = n^2,$$

   for some $n \in \mathbb{N}$. It follows that dimension of any central simple algebra is a square.

3. All division algebras are central simple over their centers hence in view of (2) $\dim_K D$ is a square.

4.4 Brauer Group of a Field

Let $\mathscr{C}(K)$ be the collection of all finite dimensional central simple algebras over K.

Definition 4.4.1 Two central simple algebras $\mathcal{A}$ and $\mathcal{B}$ are called *Brauer equivalent* if there exists a central division algebra D and $m, n \in \mathbb{N}$ such that $\mathcal{A} \cong M_m(D)$ and $\mathcal{B} \cong M_n(D)$.

Clearly it is an equivalence relation on the set $\mathscr{C}(K)$. The set of equivalence classes will be denoted by $Br(K)$ and for $\mathcal{A} \in \mathscr{C}(K)$ the equivalence class of $\mathcal{A}$ in $\mathrm{Br}(K)$ will be denoted by $[\mathcal{A}]$.

Remark 4.4.2 Observe that Br (K) is infact collection of isomorphism classes of finite dimensional central division algebras over K. Let $\mathcal{A}, \mathcal{B} \in \mathscr{C}(K)$ then by theorem 4.3.4 tensor product $\mathcal{A} \otimes_K \mathcal{B} \in \mathscr{C}(K)$. Define

$$[\mathcal{A}] \otimes [\mathcal{B}] = [\mathcal{A} \otimes_K \mathcal{B}].$$

In view of Wedderburn's theorem and properties of tensor products we have that if $\mathcal{A}$ and $\mathcal{B}$ are Brauer equivalent to $\mathcal{A}'$ and $\mathcal{B}'$ respectively then $\mathcal{A} \otimes_K \mathcal{B}$ will be Brauer equivalent to $\mathcal{A}' \otimes_K \mathcal{B}'$. Therefore product of equivalence classes is well defined. Our aim is to prove that $\mathrm{Br}(K)$ is an abelian group. Proceeding in the direction we have the following definition

Definition 4.4.3 Let $\mathcal{A}$ be a ring. Then the *opposite ring* $\mathcal{A}^{op}$ is defined by $\mathcal{A}^{op} = \mathcal{A}$ with addition is as in $\mathcal{A}$ and multiplication is $a \circ b = ba$.

Observation 4.4.4

1. Every left (right) ideal of $\mathcal{A}$ is a right (left) ideal of $\mathcal{A}^{op}$.

2. $\mathcal{A}^{op}$ is central or simple or a division ring if and only if $\mathcal{A}$ is.

3. $\mathcal{A} = (\mathcal{A}^{op})^{op}$.

Theorem 4.4.5. *Let $\mathcal{A}$ be a central simple algebra over K. Then $\mathcal{A} \otimes \mathcal{A}^{op} \cong M_n(K)$ where $n = \dim(\mathcal{A})$.*

Proof. We will prove as K-algebras $\mathcal{A} \otimes \mathcal{A}^{op} \cong \mathrm{End}_K(\mathcal{A})$. Let $a, b, x \in \mathcal{A}$. Define the map

$$\Psi_{a,b} : \mathcal{A} \to \mathcal{A}$$
$$\Psi_{a,b}(x) = axb$$

Clearly $\Psi_{a,b}$ is an endomorphism of the K-vector space $\mathcal{A}$. This defines a map

$$\Phi : \mathcal{A} \times \mathcal{A}^{op} \to \mathrm{End}_K(\mathcal{A}).$$
$$\Phi(a, b) = \psi_{a,b}$$

The map Φ is clearly a balanced map, hence the definition of tensor product there exists a unique algebra homomorphism $h : \mathcal{A} \otimes \mathcal{A}^{op} \to \mathrm{End}_K(\mathcal{A})$. Since $\mathcal{A} \otimes_K \mathcal{A}^{op}$ is simple h is injective. Since the dimensions are equal h is surjective.

□

Claim The set $\mathrm{Br}(K)$ is an abelian group with the above defined binary operation.

Proof. Let $\mathcal{A}, \mathcal{B}, \mathcal{C} \in \mathscr{C}(K)$.

1. As $\mathcal{A} \otimes (\mathcal{B} \otimes \mathcal{C}) \cong (\mathcal{A} \otimes \mathcal{B}) \otimes \mathcal{C}$ and $\mathcal{A} \otimes \mathcal{B} \cong \mathcal{B} \otimes \mathcal{A}$ the above defined product is associative and commutative.

2. If $\mathcal{A} \cong M_n(D)$ then $\mathcal{A} \otimes M_m(K) \cong M_n(D) \cong M_m(K) \cong M_mn(D)$. Therefore the class of $M_m(K)$ is the identity element for this product.

3. If $\mathcal{A}$ is a central simple algebra then $\mathcal{A}^{op}$ defined in the previous section is also a central simple algebra and $[\mathcal{A}] \otimes [\mathcal{A}^{op}] = [\mathcal{A} \otimes \mathcal{A}^{op}] = [\mathrm{End}_K(\mathcal{A})] = [M_n(K)]$, where $n = \dim_K(\mathcal{A})$. Hence class of opposite algebra is inverse of $[\mathcal{A}]$.

$\square$

Example 4.4.6 If K is an algebraically closed field then any finite dimensional division algebra D over K will be equal to K. As if that is not the case then for any $d \in D \setminus K$, $K(d)$ will be a proper algebraic extension of K, which is not possible. Therefore Brauer group of an algebaically closed field is trivial.

Example 4.4.7 In 1905, Wedderburn proved that every finite division algebra is a field. Any finite dimensional division algebra D over a finite field K is also finite, and hence itself a field. Any proper division algebra D cannot be central as center of D is equal to D. Therefore the Brauer group of a finite field is trivial.

Theorem 4.4.8. *(Frobenius, 1878) The only finite dimensional division algebra over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$, where $\mathbb{H}$ is Hamilton quaternion $(-1, -1)_{\mathbb{R}}$.*

Example 4.4.9 As a consequence of above theorem we have that the only central division algebras over $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{H}$, the set of Hamiltonian quaternions. Hence, $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$.

Chapter 5

Involutions and Quadratic Forms

In this chapter we explore the connections between quadratic forms and central simple algebras with involutions. In §1 we introduce the notion of an involution and mention various results concerning the classification of involutions of first kind. In the next section we present some important examples of involutions, namely the adjoint involution on a split algebra, canonical involution on quaternion algebras and the product of canonical involutions on the split biquaternion algebra. In §3, the notion of isotropy and hyperbolicity of involutions is defined and analogy of these notions with those in the algebraic theory of quadratic forms is established. In last section we describe analogical results for non split central simple algebras and record their connection with hermitian forms.

5.1 Involution on Central Simple Algebra

Throughtout this chapter K will denote a field with $\operatorname{char} K \neq 2$ and by a K-algebra $\mathcal{A}$, we shall mean a finite dimensional K-algebra.

Definition 5.1.1 An *involution* on a central simple K-algebra $\mathcal{A}$ is a map $\sigma : \mathcal{A} \to \mathcal{A}$ satisfying for each $x, y \in \mathcal{A}$, the following conditions:

1. $\sigma(x + y) = \sigma(x) + \sigma(y)$
2. $\sigma(xy) = \sigma(y)\sigma(x)$
3. $\sigma^2(x) = x$

Remarks 5.1.2

1. The map σ need not be a K-linear.
2. The map σ preserves the center K: $\sigma(K) = K$.

5.1.1 Classification of Involution

In view of previous remark we have two possibilities:

1. Involution σ is K-linear, in which case σ is said to be an involution of *first kind*.
2. Involution σ is the non-trivial automorphism of K of order 2, in which case σ is said to be an involution of *second kind*.

Examples 5.1.3

1. **Transpose map** On $M_n(K)$, the map $T : M_n(K) \to M_n(K)$ given by $A \to A^T$ satisfies the following conditions:

   (a) $(A + B)^T = A^T + B^T$

   (b) $(AB)^T = B^T A^T$

   (c) $(A^T)^T = A$

   Hence T is an involution on $M_n(K)$.

2. **Adjoint Involution on Matrix algebra** Let (V, φ) be a regular quadratic space and A be a matrix of coefficient of φ for some choice of basis of V. Define the map $\sigma_\varphi : M_n(K) \to M_n(K)$ as follows: $\sigma_\varphi(G) = (AGA^{-1})^T$. Then σ_φ satisfies the following properties:

   (a) $$\begin{aligned}\sigma_\varphi(G_1 + G_2) &= (A(G_1 + G_2)A^{-1})^T \\ &= (AG_1A^{-1})^T + (AG_2A^{-1})^T \\ &= \sigma_\varphi(G_1) + \sigma_\varphi(G_2).\end{aligned}$$

   (b) $$\begin{aligned}\sigma_\varphi(G_1G_2) &= (AG_1G_2A^{-1})^T \\ &= (AG_1A^{-1}AG_2A^{-1})^T \\ &= (AG_2A^{-1})^T(AG_1A^{-1})^T \\ &= \sigma_\varphi(G_2)\sigma_\varphi(G_1).\end{aligned}$$

(c) $$\begin{aligned}\sigma_\varphi^2(G) &= \sigma_\varphi(\sigma_\varphi(G)) \\ &= (A(\sigma_\varphi(G))A^{-1})^T \\ &= (A(AGA^{-1})^T A^{-1})^T \\ &= (A(A^{-1})^T G^T A^T A^{-1})^T \\ &= G.\end{aligned}$$

Therefore σ_φ is an involution. It is called the *adjoint involution* of the quadratic form φ.

3. Let $(\mathcal{A}, \sigma)$ be a central simple K-algebra with involution. Then $(a_{ij}) \to (\sigma(a_{ij}))^T$ defines an involution on $M_n(K) \otimes_K \mathcal{A} \cong M_n(\mathcal{A})$.

Definition 5.1.4 For an involution σ on a central simple K-algebra $\mathcal{A}$ the *fixed field* of σ is the field $K^\sigma := \{\lambda \in K : \sigma(\lambda) = \lambda\}$.

Clearly if σ is of the first kind then $K^\sigma = K$ otherwise K is a separable quadratic extension over K^σ. Now onwards in this chapter we shall only be concerned about the involutions of first kind.

Before we proceed, to make sure that the set of involution on a K-algebra $\mathcal{A}$ is non-empty we record a theorem of Albert.

Theorem 5.1.5. *A central simple K-algebra $\mathcal{A}$ has an involution of the first kind if and only if $\mathcal{A} \cong \mathcal{A}^{op}$ where $\mathcal{A}^{op}$ denotes the algebra opposite to $\mathcal{A}$.*

For a proof of this theorem we refer to [Sch85, Chapter 8].

Let a central simple K-algebra $\mathcal{A}$ admit an involution of the first kind. The following theorem asserts that any other involution on $\mathcal{A}$ can be obtained from σ by twisting it with an inner automorphism.

Theorem 5.1.6. *Let $(\mathcal{A}, \sigma)$ be a central simple K-algebra with involution. Then the following statements are true:*

1. *Let $a \in \mathcal{A}$ be an element satisfying the condition $a = \lambda\sigma(a)$, for some $\lambda \in K$ such that $\lambda\sigma(\lambda) = 1$. Then the map $\sigma_a : \mathcal{A} \to \mathcal{A}$ defined by $x \to a\sigma(x)a^{-1}$ is an involution on $\mathcal{A}$.*

2. *If τ is any other involution on $\mathcal{A}$ then there exists an invertible element $a \in \mathcal{A}$ such that $a = \pm\sigma(a)$ and $\tau = \sigma_a$, where σ_a is as in 1.*

3. *If σ and τ are involutions of first kind then $a \in \mathcal{A}$ (as in 2) is uniquely determined upto a scalar factor $\mu \in K^*$.*

Proof. 1. To prove this we just have to check properties of an involution given in definition 5.1.1.

- $\sigma_a(x+y) = a(\sigma(x)+\sigma(y))a^{-1} = a\sigma(x)a^{-1} + a\sigma(y)a^{-1} = \sigma_a(x) + \sigma_a(y)$.
- $\sigma_a(xy) = a(\sigma(y)\sigma(x))a^{-1} = a\sigma(y)a^{-1}a\sigma(x)a^{-1} = \sigma_a(y)\sigma_a(x)$.
- $\sigma_a^2(x) = a\sigma(a\sigma(x)a^{-1})a^{-1} = a\sigma(a^{-1})\sigma^2(x)\sigma(a)a^{-1} = \lambda\sigma^2(x)\lambda^{-1} = x$.

Hence σ_a is an involution.

2. Let τ be any other involution on $\mathcal{A}$. Then the composition $\tau \circ \sigma$ will be an inner automorphism. By Skolem-Noether theorem 4.3.7. Hence there exists an invertible element $a \in \mathcal{A}$ such that for every $x \in \mathcal{A}$

$$\sigma \circ \tau(x) = axa^{-1} \Rightarrow \tau(x) = \sigma(axa^{-1}) = \sigma(a)^{-1}\sigma(x)\sigma(a).$$

As $\tau^2(x) = x$, for all $x \in \mathcal{A}$, from above equation, we get

$$x = \sigma(a)^{-1}\sigma(\tau(x))\sigma(a) = \sigma(a)^{-1}\sigma(a^{-1}\sigma(x)a)\sigma(a) = \sigma(a)^{-1}axa^{-1}\sigma(a).$$

Hence the inner automorphism induced by the element $\sigma(a)^{-1}a$ is identity, which is possible only when $\sigma(a)^{-1}a$ is an element of K^*, say λ. Then $\sigma(a)^{-1}a = \lambda$. Thus $a = \sigma(a)\lambda$ and $\sigma(a) = \sigma(\lambda)a$. Therefore $a = \lambda\sigma(\lambda)a \Rightarrow \lambda\sigma(\lambda) = 1$. Therefore $\lambda = \pm 1$ and $a = \pm\sigma(a)$.

3. Let σ and τ are as in (2) and $a, b \in \mathcal{A}^*$ such that $\sigma_a = \tau = \sigma_b$. Then

$$\begin{aligned} a^{-1}\sigma(x)a &= b^{-1}\sigma(x)b \\ \Rightarrow \sigma(x) &= ab^{-1}\sigma(x)ba^{-1} \end{aligned}$$

Since $\mathcal{A}$ is central simple, above is possible only if $ab^{-1} \in K^*$. Therefore $ab^{-1} = \mu \Rightarrow a = \mu b$ and hence we are done.

□

Let $(\mathcal{A}, \sigma)$ be a K-algebra with an involution, define

$$\mathcal{A}^{+} = \{x \in \mathcal{A} : \sigma(x) = x\}.$$
$$\mathcal{A}^{-} = \{x \in \mathcal{A} : \sigma(x) = -x\}.$$

As char $K \neq 2$, any element $a \in \mathcal{A}$ can be written as

$$a = \frac{1}{2}(a + \sigma(a)) + \frac{1}{2}(a - \sigma(a)).$$

Hence we can write $\mathcal{A} = \mathcal{A}^{+} \oplus \mathcal{A}^{-}$. Let $(\mathcal{A}, \sigma)$ be a central simple K-algebra with involution of first kind and L/K be any field extension. Then write $\mathcal{A}_L$ for the L-algebra $\mathcal{A} \otimes_K L$ and σ_L for the map $\sigma \otimes id : \mathcal{A}_L \to \mathcal{A}_L$, where id is identity map on L. The following is immediate:

- $\dim_K(\mathcal{A}) = \dim_L(\mathcal{A}_L)$
- $\dim_K(\mathcal{A}^{+}) = \dim_L(\mathcal{A}_L^{+})$

With this notation we have the following:

Theorem 5.1.7. *Let $(\mathcal{A}, \sigma)$ be a K-algebra with involution of first kind and $\dim_K \mathcal{A} = n^2$. Then $\dim_K(\mathcal{A}^{+})$ is either equal to $\dfrac{1}{2}(n(n+1))$ or $\frac{1}{2}(n(n-1))$.*

Proof. Let L be a splitting field of $\mathcal{A}$. Then $\mathcal{A}_L = \mathcal{A} \otimes_K L \cong M_n(L)$. Observe that $(\mathcal{A}_L, \sigma_L)$ is an L-algebra with involution. It is sufficient to prove the result for $M_n(L)$ as $\dim_L(M_n(L)^{+}) = \dim_K(\mathcal{A}^{+})$. Suppose σ_L is the transposition involution then the set of all symmetric matrices forms a subspace $\mathcal{S}$ of $M_n(L)$ of $\dim_L(\mathcal{S}) = \frac{1}{2}(n(n+1))$. Otherwise, by theorem 5.1.6 every other involution σ on $\mathcal{A}_L$ is equal to T_a, for some $a \in M_n(L)$ with $a = \pm a^T$. Consider the subspace $a\mathcal{S}$ of $M_n(L)$. For any symmetric matrix $A \in \mathcal{S}$ we have $T_a(aA) = a(aA)^T a^{-1} = \pm aA$. Conversely, let A be a matrix satisfying the condition $T_a(A) = \pm A$. Then $a^{-1}A = \pm(a^{-1}A)^T$. Consider the matrix $B = a^{-1}A \in M_n(L)$, then $A = aB$ and B is either symmetric matrix or skew-symmetric matrix. Hence if a is symmetric then $\mathcal{A}_L^{+} = a\mathcal{S}$ and $\dim_L(a\mathcal{S}) = \frac{1}{2}(n(n+1))$. If a is skew symmetric then $\mathcal{A}^{-} = a\mathcal{S}$ and $\dim_L(a\mathcal{S}) = \frac{1}{2}(n(n+1))$. Hence $\dim_L(A_L)^{+} = \frac{1}{2}(n(n-1))$ and we are done. ☐

Definition 5.1.8 An involution σ is said to be of the *orthogonal type* if $\dim_K(A^{+}) = \frac{n(n+1)}{2}$ and of the *symplectic type* if $\dim_K(A^{+}) = \frac{n(n-1)}{2}$.

It is easy to check that in 5.1.3 the transpose involution T has the fixed subspace $M_n(K)^{+} = \{A \in M_n(K) : A^T = A\}$, which has dimension $\dfrac{n(n+1)}{2}$. Thus T is of the orthogonal type. Similarly the adjoint involution σ_φ in 5.1.3 is an involution of the orthogonal type.

Remarks 5.1.9

1. As type of an involution does not change if we extend the field of scalars, an involution σ on a central simple K-algebra $\mathcal{A}$ is symplectic if and only if for every field extension L/K, the involutionσ_L on $\mathcal{A}_L$ is symplectic. In particular for a splitting field L of $\mathcal{A}$, $\mathcal{A}_L \cong M_n(L)$ and a non singular skew symmetric matrix exists only for even dimensions. Therefore of first kind can exist only when $\dim_K(\mathcal{A})$ is even.

2. All symplectic involutions on the split algebra $M_{2n}(K)$ are isomorphic as all skew-symmetric regular matrices are congruent. We refer to [Bak02, Cor. 8.25, P.231] for a proof.

5.2 Examples

In this section, we give some important examples of involutions of first kind. Some of the results of this section will be used in the proof of Pfister factor conjecture.

5.2.1 Adjoint Involution on $\mathrm{End}_K(V)$

In 5.1.3, we have defined the notion of adjoint involution to a given quadratic form (V, φ). We begin the section with an equivalent definition of adjoint involution on $\mathrm{End}_K(V) \cong M_n(K)$.

Definition 5.2.1 Let $(V, \mathfrak{b})$ be a nonsingular bilinear space. Then the bilinear form $\mathfrak{b}$ induces a map $\hat{\mathfrak{b}} : V \to V^*$ defined by

$$\hat{\mathfrak{b}}(x)(y) = \mathfrak{b}(x, y) \text{ for } x, y \in V.$$

Here V^* denotes the space dual to V consisting of linear functionals on V. Since $\mathfrak{b}$ is nonsingular, $\hat{\mathfrak{b}}$ is an isomorphism of V and V^* [Lam05, Prop. I.1.2]. The *adjoint involution* on $\mathrm{End}_K(V)$ is defined as follows:

$$\begin{aligned} \sigma_{\mathfrak{b}} : \mathrm{End}_K(V) &\to \mathrm{End}_K(V), \\ f &\mapsto \hat{\mathfrak{b}}^{-1} f^t \hat{\mathfrak{b}}, \end{aligned}$$

where $f^t \in \mathrm{End}_K(V^*)$ is transpose of f given by $\xi \mapsto \xi \circ f$ for $\xi \in V^*$.

Observation 5.2.2 For any pair $x, y \in V$ and $f \in End_K(V)$

$$\begin{aligned} &\sigma_{\mathfrak{b}}(f) = \hat{\mathfrak{b}}^{-1} \circ f^t \circ \hat{\mathfrak{b}} \\ \Leftrightarrow &\hat{\mathfrak{b}} \circ \sigma_{\mathfrak{b}}(f) = f^t \circ \hat{\mathfrak{b}} \\ \Leftrightarrow &\mathfrak{b}(x, f(y)) = \mathfrak{b}(\sigma_{\mathfrak{b}}(f)(x), y). \end{aligned}$$

Claim $\sigma_{\mathfrak{b}}$ is an involution.

Proof. For $f, g \in \mathrm{End}_K(V)$

1. $\sigma_{\mathfrak{b}}(f+g) = \hat{\mathfrak{b}}^{-1} \circ (f+g)^t \circ \hat{\mathfrak{b}} = \hat{\mathfrak{b}}^{-1} \circ (f^t + g^t) \circ \hat{\mathfrak{b}} = \hat{\mathfrak{b}}^{-1} \circ f^t \circ \hat{\mathfrak{b}} + \hat{\mathfrak{b}}^{-1} \circ g^t \circ \hat{\mathfrak{b}} = \sigma_{\mathfrak{b}}(f) + \sigma_{\mathfrak{b}}(g)$.
2. $\sigma_{\mathfrak{b}}(f \circ g) = \hat{\mathfrak{b}}^{-1} \circ (f \circ g)^t \circ \hat{\mathfrak{b}} = \hat{\mathfrak{b}}^{-1} \circ g^t \circ f^t \circ \hat{\mathfrak{b}} = \hat{\mathfrak{b}}^{-1} \circ g^t \circ \hat{\mathfrak{b}} \circ \hat{\mathfrak{b}}^{-1} f^t \circ \hat{\mathfrak{b}} = \sigma_{\mathfrak{b}}(g) \circ \sigma_{\mathfrak{b}}(f)$.
3. As $\mathfrak{b}$ is symmetric or skew symmetric, we have
$\sigma_{\mathfrak{b}}^2(f) = \hat{\mathfrak{b}}^{-1} \circ (\hat{\mathfrak{b}}^{-1} \circ f^t \circ \hat{\mathfrak{b}})^t \circ \hat{\mathfrak{b}} = \hat{\mathfrak{b}}^{-1} \circ \hat{\mathfrak{b}} \circ f \circ \hat{\mathfrak{b}}^{-1} \circ \hat{\mathfrak{b}} = f$.

Hence, $\sigma_{\mathfrak{b}}$ is an involution.

Definition 5.2.3 The algebra $(\mathrm{End}_K(V), \sigma_{\mathfrak{b}})$ with involution is called the *adjoint algebra* of $(V, \mathfrak{b})$.

Theorem 5.2.4. *The map which associates to each nonsingular bilinear space* $(V, \mathfrak{b})$ *its adjoint algebra* $(\mathrm{End}_K(V), \sigma_{\mathfrak{b}})$ *induces a bijection between equivalence classes of nonsingular bilinear forms on* V *up to multiplication by a factor in* K^* *and involutions of first kind on* $\mathrm{End}_K(V)$.

Proof. We first show that the map given in the theorem is well defined. From the definition of adjoint involution we have

$$\mathfrak{b}(x, f(y)) = \mathfrak{b}(\sigma_{\mathfrak{b}}(f)(x), y)$$

where $f \in \mathrm{End}_K(V)$ and $x, y \in V$. For $\alpha \in K^*$, we have $\alpha\mathfrak{b}(x, f(y)) = \alpha\mathfrak{b}(\sigma_{\alpha\mathfrak{b}}(f)(x), y)$. Thus $\mathfrak{b}(x, f(y)) = \mathfrak{b}(\sigma_{\alpha\mathfrak{b}}(f)(x), y)$ and $\sigma_{\mathfrak{b}} = \sigma_{\alpha\mathfrak{b}}$. Therefore the map from the set of nonsingular bilinear forms on V to the set of adjoint algebras is well defined up to a scalar factor.

Now we will show that this map is one-to-one. Let $\mathfrak{b}, \mathfrak{b}'$ be two nonsingular bilinear forms on V such that $\sigma_{\mathfrak{b}} = \sigma_{\mathfrak{b}'}$. Let $f \in \mathrm{End}_K(V)$. Then $\hat{\mathfrak{b}}^{-1} f^t \hat{\mathfrak{b}} = \hat{\mathfrak{b}'}^{-1} f^t \hat{\mathfrak{b}'} \Rightarrow \hat{\mathfrak{b}'}\hat{\mathfrak{b}}^{-1} f^t \hat{\mathfrak{b}}\hat{\mathfrak{b}'}^{-1} = f^t$. Since f is arbitary $\hat{\mathfrak{b}'}\hat{\mathfrak{b}}^{-1} \in K^*$, say $\hat{\mathfrak{b}'}\hat{\mathfrak{b}}^{-1} = \alpha \in K^*$. Hence $\mathfrak{b}, \mathfrak{b}'$ are scalar multiples of each other.

Let $\mathfrak{b}$ be a fixed nonsingular bilinear form on V with adjoint involution $\sigma_{\mathfrak{b}}$. Then for any linear involution σ of $\mathrm{End}_K(V)$, the composite $\sigma_{\mathfrak{b}} \circ \sigma^{-1}$ is K-linear automorphism of $\mathrm{End}_K(V)$. By the Skolem-Noether theorem 4.3.7 these automorphisms are inner automorphisms. Therefore there exists an invertible element $u \in \mathrm{End}_K(V)$ such that $\sigma_{\mathfrak{b}} \circ \sigma^{-1} = \mathrm{Int}(u)$, where $\mathrm{Int}(u)$ is inner automorphism of $\mathrm{End}_K(V)$. Therefore

$$\mathrm{Int}(u^{-1}) \circ \sigma_{\mathfrak{b}} = \sigma \Rightarrow \ u^{-1}\sigma_{\mathfrak{b}}(f)u = \sigma(f) \Rightarrow \sigma_{\mathfrak{b}}(f)u = u\sigma(f).$$

Hence by definition σ is adjoint involution to the bilinear form

$$\mathfrak{b}'(x, y) = \mathfrak{b}(u(x), y).$$

□

Remarks 5.2.5

1. Let (V, φ) be a regular quadratic space over K with associated bilinear form $\mathfrak{b}_\varphi$. Then the involutions σ_φ and $\sigma_{\mathfrak{b}_\varphi}$ on $\mathrm{End}_K(V)$ are same. Adjoint algebra of (V, φ) is denoted by $\mathrm{Ad}\,\varphi$.

2. Let (V_1, φ_1) and (V_2, φ_2) are two regular quadratic spaces then $\mathrm{Ad}(\varphi_1 \otimes \varphi_2) \cong \mathrm{Ad}(\varphi_1) \otimes \mathrm{Ad}(\varphi_2)$.

   Proof. In 1.1.14 we saw that for $v_1, v_1' \in V_1$ and $v_2, v_2' \in V_2$ we have $\mathfrak{b}_{(\varphi_1\otimes\varphi_2)}(v_1 \otimes v_2, v_1' \otimes v_2') = \mathfrak{b}_{\varphi_1}(v_1, v_1')\mathfrak{b}_{\varphi_2}(v_2, v_2')$. Let $\{f_1, f_2, \ldots, f_n\}$ be a basis of $\mathrm{End}_K(V_1)$ and $\{g_1, g_2, \ldots, g_m\}$ be a basis of $\mathrm{End}_K(V_2)$. Then $\{f_i \otimes g_j : 1 \le i \le n, 1 \le j \le m\}$ constitutes a basis of $\mathrm{End}_K(V)$.

$$\begin{aligned}
\mathfrak{b}_{(\varphi_1\otimes\varphi_2)}(v_1 \otimes v_2, (f_i \otimes g_j)v_1' \otimes v_2') &= \mathfrak{b}_{(\varphi_1\otimes\varphi_2)}(v_1 \otimes v_2, f_i(v_1') \otimes g_j(v_2') \\
&= \mathfrak{b}_{\varphi_1}(v_1, f_i(v_1'))\mathfrak{b}_{\varphi_2}(v_2, g_j(v_2')) \\
&= \mathfrak{b}_{\varphi_1}(\sigma_{\varphi_1}(f_i)(v_1), v_1')\mathfrak{b}_{\varphi_2}(\sigma_{\varphi_1}(g_j)(v_2), v_2') \\
&= \mathfrak{b}_{(\varphi_1\otimes\varphi_2)}(\sigma_{\varphi_1}(f_i) \otimes \sigma_{\varphi_2}(g_j)(v_1 \otimes v_2), v_1' \otimes v_2') \\
&= \mathfrak{b}_{(\varphi_1\otimes\varphi_2)}(\sigma_{\varphi_1\otimes\varphi_2}(f_i \otimes g_j)(v_1 \otimes v_2), v_1' \otimes v_2').
\end{aligned}$$

   Hence the result is proved. □

Let $Q = (a,b)_K$ be a K-quaternion algebra. In §4.1.2, we have defined conjugation map on Q and have shown that it is an involution. Since it is a K-linear map it defines an involution of first kind. Moreover $\dim_K Q^+ = 1$ and hence it is of symplectic type. This conjugation involution on Q is called the *cannonical involution.* Let L be a splitting field of Q, then $Q \simeq M_2(L)$. Define

$$\gamma : M_2(L) \to M_2(L)$$

as follows

$$\gamma \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} x_4 & -x_2 \\ -x_3 & x_1 \end{pmatrix}; x_i \in L$$

Clearly γ is an involution. Observe that if Q splits over K, then γ is same as the conjugation map on Q.

Proposition 5.2.6. *The canonical involution on a quaternion algebra Q is the unique symplectic involution on Q. Every orthogonal involution σ on Q is of the form $\sigma = \mathrm{Int}(u) \circ \gamma$, where $u \in Q^*$ is uniquely determined by σ up to a factor in K^*.*

Proof. From theorem 5.1.6, it follows that every involution of the first kind σ on Q is of the form $\sigma = \mathrm{Int}(u) \circ \gamma$, where u is an invertible element of Q such that $\gamma(u) = \pm u$. If σ is orthogonal then $\gamma(u) = -u$. If σ is symplectic then $\gamma(u) = u$ and $u \in K^*$. Therefore $\sigma = \gamma$. ☐

Observation 5.2.7 Let (Q_1, σ_1) and (Q_2, σ_2) be quaternion algebras with involution of first kind.

1. If σ_1 and σ_2 are orthogonal, then $(Q_1, \sigma_1) \otimes (Q_2, \sigma_2)$ is an algebra with orthogonal involution.

2. If σ_1 is symplectic and σ_2 is orthogonal, then $(Q_1, \sigma_1) \otimes (Q_2, \sigma_2)$ is an algebra with symplectic involution.

3. If σ_1 and σ_2 are symplectic, then $(Q_1, \sigma_1) \otimes (Q_2, \sigma_2)$ is an algebra with orthogonal involution.

Proof. For $q_1 \in Q_1, q_2 \in Q_2$, we have $\sigma_1 \otimes \sigma_2(q_1 \otimes q_2) = \sigma_1(q_1) \otimes \sigma_2(q_2)$. Hence

1. $$\begin{aligned} \dim_K(Q_1 \otimes_K Q_2)^+ &= \dim_K Q_1^+ \times \dim_K Q_2^+ + \dim_K Q_1^- \times \dim_K Q_2^- \\ &= 3 \times 3 + 1 \times 1 \\ &= 10 = \frac{4(4+1)}{2} \end{aligned}$$

2. $$\begin{aligned}\dim_K(Q_1 \otimes_K Q_2)^+ &= \dim_K Q_1^+ \times \dim_K Q_2^+ + \dim_K Q_1^- \times \dim_K Q_2^- \\ &= 1 \times 3 + 3 \times 1 \\ &= 6 = \frac{4(4-1)}{2}.\end{aligned}$$

3. $$\begin{aligned}\dim_K(Q_1 \otimes_K Q_2)^+ &= \dim_K Q_1^+ \times \dim_K Q_2^+ + \dim_K Q_1^- \times \dim_K Q_2^- \\ &= 1 \times 1 + 3 \times 3 \\ &= 10 = \frac{4(4+1)}{2}.\end{aligned}$$

□

Theorem 5.2.8. *Any product of two quaternion algebras with symplectic involution is isomorphic to a product of two quaternion algebras with orthogonal involution.*

Proof. Let (Q_1, σ_1) and (Q_2, σ_2) be two quaternion K-algebras with symplectic involutions. Let $Q_1 = (a, b)_K$ and $Q_2 = (a', b')_K$. Then $(Q_1, \sigma_1) \otimes_K (Q_2, \sigma_2)$ is a central simple algebra with orthogonal involution.

Denote the quaternion bases of Q_1 and Q_2 by $1, i, j, ij$ and $1, i', j', i'j'$ respectively. Consider the following subspaces of $(Q_1 \otimes Q_2)$:

$$Q_3 = (1 \otimes 1)K \oplus (i \otimes 1)K \oplus (j \otimes j')K \oplus (ij \otimes j')K.$$
$$Q_4 = (1 \otimes 1)K \oplus (1 \otimes j')K \oplus (i \otimes i'j')K \oplus ((-b'i) \otimes i')K.$$

Being closed under multiplication, Q_3 and Q_4 are subalgebras of $Q_1 \otimes_K Q_2$.
Define the map $\Theta : Q_3 \otimes_K Q_4 \to Q_1 \otimes_K Q_2$ as $q_3 \otimes q_4 \to q_3 q_4$, where $q_3 \in Q_3$ and $q_4 \in Q_4$. Since the standard basis elements of $(Q_1 \otimes_K Q_2)$ are in image of Θ. Hence Θ is surjective. As $\dim_K(Q_1 \otimes_K Q_2) = \dim_K(Q_3 \otimes_K Q_4)$. Therefore Θ is also injective. Hence $Q_1 \otimes_K Q_2 \cong Q_3 \otimes_K Q_4$.

Also observe $\sigma_3 = (\sigma_1 \otimes \sigma_2)|_{Q_3}$ and $\sigma_4 = (\sigma_1 \otimes \sigma_2)|_{Q_4}$ are orthogonal involutions on Q_3 and Q_4 respectively. Clearly $(Q_1, \sigma_1) \otimes_K (Q_2, \sigma_2) \cong (Q_3, \sigma_3) \otimes_K (Q_4, \sigma_4)$

□

Theorem 5.2.9. *Let (Q, γ) be a quaternion algebra with involution. Then the biquaternion algebra $(Q, \gamma) \otimes (Q, \gamma)$ is adjoint to the norm form $N = \langle 1, -a, -b, ab \rangle$.*

Proof. Since the norm form $\langle 1, -a, -b, ab\rangle \cong \langle 1, -a\rangle \otimes \langle 1, -b\rangle$, from remark 5.2.5, we have

$$\operatorname{Ad} N \cong \operatorname{Ad}(\langle 1, -a\rangle) \otimes \operatorname{Ad}(\langle 1, -b\rangle).$$

Let $(M_2(K), \sigma_1) = \operatorname{Ad}(\langle 1, -a\rangle)$ and $(M_2(K), \sigma_2) = \operatorname{Ad}(\langle 1, -b\rangle)$. Let (Q_3, σ_3) and (Q_4, σ_4) be as in previous theorem. From example 4.1.7, $Q_3 \cong (1, a)_K \cong M_2(K)$ and isomorphism is given by:

$$1\otimes 1 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad j\otimes j \to \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad i\otimes 1 \to \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \quad ij\otimes j \to \begin{pmatrix} 0 & a \\ -1 & 0 \end{pmatrix}$$

The involution $\sigma_3 = \gamma \otimes \gamma|_{Q_3}$ fixes all basis elements except $i \otimes 1$ and $\sigma_3(i \otimes 1) = -(i \otimes 1)$. Hence the involution σ_3 is given by

$$\sigma_3\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_3\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$\sigma_3\begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -a \\ -1 & 0 \end{pmatrix}, \quad \sigma_3\begin{pmatrix} 0 & a \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ -1 & 0 \end{pmatrix}$$

The adjoint involution σ_1 on $M_2(K)$ is given by:

$$\sigma_1\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1/a \end{pmatrix}\begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -a \end{pmatrix} = \begin{pmatrix} x_1 & -ax_3 \\ -x_2/a & x_4 \end{pmatrix}$$

kronecker product Hence on the basis elements σ_1 acts as follows:

$$\sigma_1\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$\sigma_1\begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -a \\ -1 & 0 \end{pmatrix}, \quad \sigma_1\begin{pmatrix} 0 & a \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ -1 & 0 \end{pmatrix}$$

Therefore σ_1 and σ_3 are same as images of the basis elements are same under the two. Similarly, $Q_4 \cong (b, -a^2b)_K \cong (1, b)_K \cong M_2(K)$ and $\sigma_2 = \sigma_4$. Now in the view of remark 5.2.5, we are done. □

5.3 Isotropy and Hyperbolicity of Involutions

In this section we will develop analogous notions for isotropy and hyperbolicity of central simple algebras with involutions.

Definition 5.3.1 For every left ideal I of a central simple algebra $\mathcal{A}$ over a field K, the *annihilator of I*, I° is defined by

$$I^\circ = \{x \in \mathcal{A} : Ix = 0\}$$

The set I° is a right ideal. Similarly, for a right ideal I of $\mathcal{A}$, the *annihilator of I* is defined by

$$I^\circ = \{x \in \mathcal{A} : xI = 0\}$$

Clearly I° is a left ideal of $\mathcal{A}$.

Definition 5.3.2 Let $(\mathcal{A}, \sigma)$ be a central simple algebra with involution of first kind and I be a right ideal in $(\mathcal{A}, \sigma)$. The *orthogonal ideal* of I with respect to σ is defined by

$$I^\perp = \{x \in \mathcal{A} : \sigma(x) \cdot I = 0\}$$

$I^\perp$ is clearly a right ideal. Observe that for a right ideal I, $\sigma(I)$ will be left ideal and

$$\sigma(I)^\circ = \{x \in \mathcal{A} : \sigma(I) \cdot x = 0\} = \{x \in \mathcal{A} : \sigma(x) \cdot I = 0\} = I^\perp.$$

Definition 5.3.3 Let $(\mathcal{A}, \sigma)$ be a central simple algebra with involution over a field K. A right ideal I of $\mathcal{A}$ is called *isotropic* with respect to the involution σ if $I \subseteq I^\perp$.

Observation 5.3.4 Let $(\mathcal{A}, \sigma)$ be a central simple algebra with involution of any kind. Then there exists $a \in \mathcal{A}$ such that $a\sigma(a) = 0$ if and only if there exists a non zero isotropic ideal of $\mathcal{A}$.

Definition 5.3.5 A central simple algebra with involution $(\mathcal{A}, \sigma)$ is called *isotropic* if it satisfies any of the equivalent condition in the above observation.

Definition 5.3.6 A central simple algebra with involution $(\mathcal{A}, \sigma)$ is called *hyperbolic* if it contains an isotropic ideal such that $\dim_K(I) = \frac{1}{2}\dim_K \mathcal{A}$.

Proposition 5.3.7. *The following are equivalent*

1. $(\mathcal{A}, \sigma)$ *is hyperbolic.*

2. *There exists an idempotent such that* $\sigma(e) = 1 - e$

Proof. [KMRT98, prop. 6.7] □

Example 5.3.8 The quaternion algebra with canonical involution (Q, γ) is hyperbolic.

Proof. The element

$$e = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

is a desired idempotent. □

5.3.1 Isotropy and Hyperbolicity of Adjoint Involutions

In the previous section we saw that to a given bilinear space $(V, \mathfrak{b})$ we can associate a central simple algebra with an involution of first kind namely $(\mathrm{End}_K(V), \sigma_{\mathfrak{b}})$. In this section we find relation between the isotropy and hyperbolicity of quadratic forms discussed in §1.2 and split algebras with orthogonal involutions. Let V be an n-dimensional vector space over field K, then $\mathrm{End}_K(V) \cong M_n(K)$. We first establish relation between subspaces of vector space V and ideals of the endomorphism ring of V. Let $U \subseteq V$ be a subspace of V. We have following set

$$\mathrm{Hom}_K(V, U) = \{f \in \mathrm{End}_K(V) | f(V) \subseteq U\}$$

Claim For a subspace U of V, the space $\mathrm{Hom}_K(V, U)$ is a right ideal of the ring $\mathrm{End}_K(V)$ and $\dim_K(\mathrm{Hom}_K(V, U)) = \dim_K(U) \cdot \dim_K(V)$.

Proof. 1. Let $f, g \in \mathrm{Hom}_K(V, U)$. Since U is a subspace of V, we have

$$f + g(V) = f(V) + g(V) \subseteq U + U = U.$$

Hence $f + g \in \mathrm{Hom}_K(V, U)$. Clearly $0 \in \mathrm{Hom}_K(V, U)$.

2. For $\theta \in \mathrm{End}_K(V)$ and $f \in \mathrm{Hom}_K(V, U)$, the map $f \circ \theta \in \mathrm{Hom}_K(V, U)$

Hence $\mathrm{Hom}_K(V, U)$ is a right ideal of $\mathrm{End}_K(V)$. Clearly $\dim_K(\mathrm{Hom}_K(V, U)) = \dim_K(U) \cdot \dim_K(V)$. □

We have a well defined map from the collection of all subspaces of V to the collection of right ideals of the endomorphism ring $\mathrm{End}_K(V)$. We have the following proposition:

Proposition 5.3.9. *The map $U \to \mathrm{Hom}_K(V, U)$ defines a one-one correspondence between subspaces of V and right ideals I of the ring $\mathrm{End}_K(V)$.*

Proof. To prove the proposition it is enough to show that every right ideal I is of the form $\mathrm{Hom}_K(V, U)$, for some subspace U of V. Let S be the collection of all subsets $W \subseteq V$ such that $f(V) \subseteq W, \forall f \in I$. Clearly S is non empty as $V \in S$. Let U be the minimal element of S. Proposition will be proved if we show that U is a subspace of V.

We first show that for an element $u \in U$ there exist a $f \in I$ such that $f(v) = u$, for all $v \in V$. Since U is minimal, there exists atleast one $g \in I$, such that $g(w) = u$ for some $w \in V$. Now for this fixed w define the map $\theta : V \to V$ as $\theta(v) = w$, for all $v \in V$. Since I is a right ideal, $f = g \circ \theta \in I$ is the desired map.

Now let $u_1, u_2 \in U$ and $f_1, f_2 \in I$ are maps as in above paragraph. As I is a ideal $f_1 + f_2 \in I$. Which implies $f_1 + f_2(V) = u_1 + u_2 \in U$. Clearly $0 \in U$. Let $\lambda \in K$ and $u \in U$. If f be the map as in above paragraph then $\lambda f(V) = \lambda u \in U$. Therefore U is a subspace of V and we are done.

□

The following proposition establishes a relation between orthogonal ideals of $\mathrm{End}_K(V)$ and orthogonal subspaces of V.

Proposition 5.3.10. *If $(\mathcal{A}, \sigma) = (\mathrm{End}_K(V), \sigma_{\mathfrak{b}})$, for some bilinear space $(V, \mathfrak{b})$ and $I = \mathrm{Hom}_K(V, W)$ for some subspace $W \subset V$, then*

$$I^{\perp} = \mathrm{Hom}_K(V, W^{\perp})$$

Proof. Suppose $I = \mathrm{Hom}_K(V, W)$ for some subspace $W \subset V$. For every $g \in \mathrm{End}_K(V)$, $f \in \mathrm{Hom}_K(V, W)$ we have $f(x) \in W$. For $x, y \in V$

$$\mathfrak{b}(f(x), g(y)) = \mathfrak{b}(\sigma(g) \circ f(x), y)$$

Therefore, $\sigma(g) \circ f = 0$ if and only if $g(y) \in W^{\perp}$. Hence $g \in \mathrm{Hom}_K(V, W^{\perp})$ and $I^{\perp} = \mathrm{Hom}(V, W^{\perp})$.

□

Theorem 5.3.11. *Let (V, φ) be an n-dimensional quadratic space. Then the adjoint algebra $(\mathcal{A}, \sigma) = (\mathrm{End}_K(V), \sigma_{\varphi})$ is isotropic if and only if the quadratic space (V, φ) is isotropic.*

Proof. Suppose (V, φ) is an isotropic quadratic space. Then there exists an isotropic vector $0 \neq v \in V$. Let W be the subspace of V generated by v then taking $I = \mathrm{Hom}_K(V, W)$ will be a non-zero ideal of $\mathrm{End}_K(V)$. Since v is an isotropic vector,

$v \in W^\perp$. Therefore $I = \mathrm{Hom}_K(V, W) \subseteq \mathrm{Hom}_K(V, W^\perp) = I^\perp$. Hence I is an isotropic ideal of $\mathrm{End}_K(V)$.

Conversely, suppose there exists a non-zero isotropic ideal I of $\mathrm{End}_K(V)$. By proposition 5.3.9, $I = \mathrm{Hom}_K(V, W)$, for some subspace W of V. As I is an isotropic ideal $I \subseteq I^\perp$. Which implies $\mathrm{Hom}_K(V, W) \subseteq \mathrm{Hom}_K(V, W^\perp) \Rightarrow W \subseteq W^\perp$. As $W \neq 0$, there exists a non-zero vector $v \in W$ and $\varphi(v) = 0$. Hence (V, φ) is isotropic. □

Theorem 5.3.12. *Let (V, φ) be a $2n$-dimensional quadratic space. Then the adjoint algebra $(End_K(V), \sigma_\varphi)$ is hyperbolic if and only if the quadratic space (V, φ) is hyperbolic.*

Proof. Suppose (V, φ) is a hyperbolic quadratic space. Then there exists n-dimensional totally isotropic subspace W of V. Let $I = \mathrm{Hom}_K(V, W)$. Then I will be a non-zero ideal of $\mathrm{End}_K(V)$ and $\dim_K I = \dim_K V \dim_K W = 2n^2 = \frac{1}{2}(4n^2) = \frac{1}{2}\dim_K(\mathrm{End}_K(V))$.

Conversely, suppose there exists a non-zero isotropic ideal I of $\mathrm{End}_K(V)$ with $\dim_K(I) = \frac{1}{2}\dim_K \mathrm{End}_K(V)$. By proposition 5.3.9, $I = \mathrm{Hom}_K(V, W)$, for some subspace W of V with $\frac{1}{2}\dim_K(V)$. Hence $\mathrm{Hom}_K(V, W) \subseteq \mathrm{Hom}_K(V, W^\perp) \Rightarrow W \subseteq W^\perp$ and W is a totally isotropic subspace of V with $\dim_K(W) = \frac{1}{2}\dim_K(V)$. Now the theorem follows from proposition 1.2.9. □

5.4 Hermitian Forms and Involutions

In §2 we saw that split algebras with involution of first kind are adjoint to quadratic forms. In this section we briefly record some analogous results for arbitrary central simple algebras with involution. We begin with the following theorem

Theorem 5.4.1. *Let $\mathcal{A}$ be a K-algebra and M be a non zero minimal left $\mathcal{A}$-module. Then there is a canonical isomorphism $\mathcal{A} \cong \mathrm{End}_D(M)$ with $D = \mathrm{End}_{\mathcal{A}}(M)$.*

Remark 5.4.2 The algebra $\mathcal{A}$ is Brauer equivalent to the K-division algebra D.

Definition 5.4.3 Let $(\mathcal{A}, \sigma)$ be an algebra with involution and M be a left $\mathcal{A}$-module. A *hermitian form* on M is a map $h : M \times M \to \mathcal{A}$ satisfying the following properties:

(a) The map h is $\mathcal{A}$ linear in first variable *i.e.* for $x, y, z \in M$ and $\alpha, \beta \in \mathcal{A}$, $h(\alpha x + \beta y, z) = \alpha h(x, z) + \beta h(y, z)$.

(b) $h(y, x) = \sigma(h(x, y))$.

Observe that the map h is bilinear over $\mathbb{Z}$ and that $h(\alpha x, y\beta) = \alpha h(x, y)\sigma(\beta)$. Given a hermitian form $h : M \times M \to \mathcal{A}$, we define a map $M \to \hom_{\mathcal{A}}(M, \mathcal{A})$ by $x \mapsto h(\_, x)$. If this map is bijective then hermitian form is called *non-singular*. In this section we mention generalization of some results of the previous section:

Proposition 5.4.4. *Let $\mathcal{A} \cong \mathrm{End}_D(V)$ be a central simple algebra and I be a right ideal of $\mathcal{A}$. Then I is of the form*

$$I = \mathrm{Hom}_D(V, W),$$

where W is some subspace of V. Moreover, there exists an idempotent $e \in \mathcal{A}$ such that $I = e\mathcal{A}$.

Proof. See [KMRT98, prop. 1.12] □

Theorem 5.4.5. *Let (D, τ) be a central division K-algebra with involution. Let h be a nonsingular hermitian or skew-hermitian form on M. Then there exists a central simple algebra $(\mathrm{End}_D(M), \sigma_h)$, where σ_h is the unique involution satisfying the following conditions:*

1. *For $\alpha \in K$, $\sigma_h(\alpha) = \tau(\alpha)$*

2. *For $x, y \in M$, $h(x, f(y)) = h(\sigma_h(f)(x), y)$*

The involution σ_h is called the adjoint involution with respect to h.

Proof. See [KMRT98, Prop. 4.1, Chapter 1] □

Theorem 5.4.6. *Let $\mathcal{A} = \mathrm{End}_D(M)$ be a central simple K-algebra. Let τ be an involution of the first kind on D. Then the map $h \mapsto \sigma_h$ defines a one-one correspondence between nonsingular hermitian and skew-hermitian forms on M with respect to τ up to a scalar factor in K^* and involutions of the first kind on $\mathcal{A}$. Moreover the involution τ and σ are of the same type if h is hermitian and of opposite types if h is skew-hermitian.*

Proof. See [KMRT98, Theorem 4.2, Chapter 1] □

Theorem 5.4.7. *Let $(\mathcal{A}, \sigma)$ be a central simple K-algebra with involution of first kind. Let $L = K(\sqrt{a})$ be a quadratic extension such that the extended algebra $(\mathcal{A}_L, \sigma_L)$ is hyperbolic. Then there exist $\alpha \in \mathcal{A}$ such that $\alpha^2 = a$ and $\sigma(\alpha) = -\alpha$.*

Proof. As σ_L is hyperbolic there exists an idempotent $e \in \mathcal{A}_L$ such that $\sigma_L(e) = 1 - e$. Write $e = e_1 \otimes 1 + e_2 \otimes \sqrt{a}$, where $e_1, e_2 \in \mathcal{A}$. We get

$$\begin{aligned}
\sigma_L(e) &= \sigma_L(e_1 \otimes 1 + e_2 \otimes \sqrt{a}) \\
&= \sigma_L(e_1 \otimes 1) + \sigma_L(e_2 \otimes \sqrt{a}) \\
&= \sigma(e_1) \otimes id(1) + \sigma(e_2) \otimes id(\sqrt{a}) \\
&= \sigma(e_1) \otimes 1 + \sigma(e_2) \otimes \sqrt{a}.
\end{aligned}$$

As $\sigma_L(e) = 1 - e$, we have

$$\begin{aligned}
\sigma(e_1) \otimes 1 + \sigma(e_2) \otimes \sqrt{a} &= 1 \otimes 1 - (e_1 \otimes 1 + e_2 \otimes \sqrt{a}) \\
&\Rightarrow \begin{cases} \sigma(e_1) = 1 - e_1 \\ \sigma(e_2) = -e_2 \end{cases}
\end{aligned}$$

Also e is an idempotent, $e^2 = e$ implies

$$\begin{aligned}
(e_1^2 + a{e_2}^2) \otimes 1 + (e_1 e_2 + e_2 e_1) \otimes \sqrt{a} &= e_1 \otimes 1 + e_2 \otimes \sqrt{a} \\
&\Rightarrow \begin{cases} e_1^2 + a{e_2}^2 = e_1 \\ e_1 e_2 + e_2 e_1 = e_2 \end{cases}
\end{aligned}$$

Let I be the right ideal $e_2\mathcal{A}$, then the annihilator

$$\begin{aligned}
I^\perp = (\sigma I)^0 &= \{x \in \mathcal{A} : \sigma(I)x = 0\} \\
&= \{x \in \mathcal{A} : e_2 x = 0\}
\end{aligned}$$

Let x be any element in $I^\perp$. Then we have the following equations

$$\begin{aligned}
e_2 e_1 x &= 0 \\
{e_1}^2 x &= e_1 x
\end{aligned}$$

Observe that for $x \in I^\perp$, $e_1 x \in I^\perp$. Thus from the above equations we get the following

$$\begin{aligned}
e_1 \sigma(x) \sigma(e_1 \sigma(x)) &= 0 \\
x e_1 \sigma(x e_1) &= 0
\end{aligned}$$

Since σ is anisotropic, for all $x \in \mathcal{A}$, $\sigma(x)x = 0$ if and only if $x = 0$. Therefore $xe_1 = e_1\sigma(x) = 0$. But $0 = \sigma(xe_1) = \sigma(e_1)\sigma(x) = (1 - e_1)\sigma(x) = \sigma(x)$. Which implies $x = 0$ and hence $I^{\perp} = 0$. As $e_2x \neq 0$ for all non zero x in $\mathcal{A}$ therefore e_2 is invertible. Now take $\alpha = e_1{e_2}^{-1}$. Clearly $\alpha^2 = e_1{e_2}^{-1}e_1{e_2}^{-1}$ □

Using this fact we can prove the following theorem

Theorem 5.4.8. *Let $(\mathcal{A}, \sigma)$ be a central simple K-algebra with involution of first kind and $L = K(\sqrt{a})$ be a quadratic field extension. If there exists $\alpha \in \mathcal{A}$ such that $\alpha^2 = a$ and $\sigma(\alpha) = -\alpha$ then the extended algebra $(\mathcal{A}_L, \sigma_L)$ is hyperbolic. Conversely If $(\mathcal{A}, \sigma)$ is a central simple K-algebra with involution of first kind and orthogonal type such that $\mathcal{A}$ is not split and its Witt index is odd then there exists $\alpha \in \mathcal{A}$ such that $\alpha^2 = a$ and $\sigma(\alpha) = -\alpha$ and the extended algebra $(\mathcal{A}_L, \sigma_L)$ is hyperbolic.*

Proof. see [BFST93, Theorem 3.3] □

Theorem 5.4.9. *Let $(\mathcal{A}, \sigma)$ be a central simple K-algebra Brauer equivalent to a quaternion division algebra Q. If σ is an involution of first kind, orthogonal type then $\mathcal{A}$ contains a subalgebra isomorphic to Q if and only if σ becomes hyperbolic over a quadratic field extension $K(\sqrt{a})$ such that Q splits over $K(\sqrt{a})$.*

Proof. see [BFST93, Theorem 3.4] □

5.4.1 The Jacobson Correspondence

For the contents of this section we refer to [Jac40]. Let $(\mathcal{A}, \sigma)$ be a central simple K-algebra with involution and M be a finite dimensional free $\mathcal{A}$-module with $\dim_{\mathcal{A}}(M) = n$. Let $\{u_1, u_2, \ldots, u_n\}$ be a basis of M over $\mathcal{A}$. Let $A = (h(u_i, u_j))$ be the matrix of coefficients of h. The matrix A satisfies the condition $A = \sigma(A)^T$, where $\sigma(A) = (\sigma(h(u_i, u_j))$. If B be the coefficient matrix of h for any other basis $\{v_1, v_2, \ldots, v_n\}$ of M over $\mathcal{A}$ then A and B are *cogredient* that is there exists an invertible matrix P in $M_n(\mathcal{A})$ such that $B = (\sigma(P))^T AP$.

Definition 5.4.10 Two hermitian forms h_1 and h_2 are called *isometric* if their coefficient matrices are cogredient.

Let $Q = (a, b)_K$ be a quaternion algebra with canonical involution γ and norm form N. Let M be a free module over Q of dimension n and $h : M \times M \to Q$ be a hermitian form. The hermitian form h gives rise to a K-quadratic form $\psi_h : M \to K$ defined by $\psi_h(x) = h(x, x) \in K$ as $h(x, x) = \overline{h(x, x)}$. The K-quadratic space (M, ψ_h)

is $4n$-dimensional and $\psi_h \cong N \otimes \varphi_h$ for some K-quadratic form φ_h, where N denotes the norm form of Q. The quadratic form φ_h is called the *underlying quadratic form* of h. Conversely, let $\psi \cong N \otimes \varphi$ be a $4n$-dimensional quadratic form over K. Then $(M, \psi) \cong (Q \otimes V, N \otimes \varphi)$, where V is an n-dimensional vector space oveer K. Since Q is a left module over itself, we regard $Q \otimes V$ as a left Q-module and define a hermitian form associated to ψ as follows:

$$h_\psi(x, y) = \mathfrak{b}_\psi(x, y) - \frac{i}{a}\mathfrak{b}_\psi(x, iy) - \frac{j}{b}\mathfrak{b}_\psi(x, jy) - \frac{ij}{ab}\mathfrak{b}_\psi(x, ijy).$$

The hermitian form h_ψ is n-dimensional over Q and h_ψ is called the *extension* of φ over (Q, γ). The two associations $h \to \psi_h$ and $\psi \to h_\psi$ are inverses of each other. We have the following result due to Jacobson:

Theorem 5.4.11. *Two non-singular hermitian spaces over (Q, γ) are isometric if and only if their underlying quadratic spaces are isometric over K.*

5.4.2 Witt Ring of Hermitian Forms

We refer to [Sch85, Chapter 7] for defintions of this section. One has the notion of orthogonal sum, totally isotropic subspace and anisotropy of hermitian forms. Moreover cancellation and decomposition theorems hold for hermitian forms. Let (D, σ) be a central division algebra with involution. Then Witt ring of (D, σ) is defined to be the collection of non-isometric anisotropic hermitian forms and we denote it by $W(D, \sigma)$. We have the following theorem

Theorem 5.4.12 (prop. 3.3, [PSS01])**.** *Let Q be a quaternion algebra over a field K and let τ be the orthogonal involution on Q. Let $K(Q)$ be the function field of Q. Then the canonical homomorphism*

$$W(Q, \tau) \to W(Q \otimes K(Q), \tau \otimes 1)$$

is injective.

Chapter 6

Pfister Factor Conjecture

The main result of this chapter is Pfister Factor Conjecture and a proof of it due to Becher [Bec08]. In §1 we explain this conjecture, its history and a related conjecture again due to Becher. This conjecture attempts at relating properties of Pfister forms and products of quaternion algebras with involutions. In §2 we describe various results from the theory of quadratic forms and central simple algebras which shall be used in the proof of main result of the chapter. Finally in §3 we present the proof of the main result.

6.1 Introduction

In §5.2.1, we have seen that to a given bilinear space a split central simple algebra with involution of first kind can be associated. In view of this, it is natural to consider results from the algebraic theory of quadratic forms and look for their counterparts in the theory of central simple algebras. One such instance is the following result due to Pfister:

Theorem 6.1.1 (See 3.2.10)**.** *Let φ be a quadratic form over K. Then φ is isometric to an n-fold Pfister form if and only if $\dim \varphi = 2^n$ and for every field extension L/K, φ_L is either anisotropic or hyperbolic.*

Motivated by this theorem, Becher conjectured the following:

Conjecture *Let $(\mathcal{A}, \sigma)$ be a central simple K-algebra with involution first kind. Then the following are equivalent:*

1. $(\mathcal{A}, \sigma) \cong \bigotimes_{i=1}^{n} (Q_i, \sigma_i)$, *where* $(Q_i, \sigma_i); 1 \leq i \leq n$ *are* K*-quaternion algebras with involution of first kind.*

2. $\deg \mathcal{A} = 2^n$ *and for every field extension* L/K*, the* L*-algebra* $(\mathcal{A}, \sigma)_L$ *is either anisotropic or hyperbolic.*

Becher also verified this conjecture in the special case when A is Brauer equivalent to a quaternion algebra. In the process he proved the following conjecture [Sha00, Chapter 9]:

Theorem 6.1.2 (Pfister Factor Conjecture)**.** *Let* $n \in N$ *and let* $(Q_1, \sigma_1), \ldots, (Q_n, \sigma_n)$ *be* K*-quaternion algebras with involutions. If* $\bigotimes_{i=1}^{n} (Q_i, \sigma_i)$ *is a split* K*-algebra with an involution of first kind, then it is adjoint to a Pfister form.*

Originally the above conjecture was posed in terms of similarities of quadratic forms by Shapiro around 1975. He had also proved the conjecture for specific cases where $n \leq 5$ and also for arbitrary n for some specific fields such as number fields [Sha00, See chapter 9]. In [Sha00], Shapiro reformulated the problem in terms of algebras with involutions. Initially it seemed that this version of conjecture is hard to work with. Different proofs were given till then for specific cases $n \leq 5$ for this version of the conjecture. In 2008, Becher gave a surprisingly elementary proof of the Pfister factor conjecture.

In next section we record some results to be used in the proof of Pfister Factor Conjecture in general and that of Becher's conjecture in a special case.

6.2 Some Important Results

6.2.1 An Exact Sequence of Witt Groups

Let Q be a quaternion algebra and $K(Q)$ be the generic splitting field of Q. In §2.4 we proved that the function field of a quaternion algebra $K(Q)$ is excellent over K. That is for a given quadratic form φ over K there exists a quadratic form ψ over K such that $(\varphi_{K(Q)})_{an} \cong \psi_{K(Q)}$.

Let $W(K)$ and $W(K(Q))$ denote Witt rings of K and $K(Q)$ respectively. Then we have a natural map

$$\Phi : W(K) \to W(K(Q))$$
$$\varphi \mapsto \varphi_{K(Q)}.$$

With this notation we have the following

Lemma 6.2.1. *A quadratic form φ over $K(Q)$ represents a class in $W(K)$ if and only if it represents a class in image of the map Φ.*

Proof. Suppose φ represents a class in $W(K)$ then clearly φ represents a class in the image of Φ. Conversely, suppose φ represents a class in image of Φ. Then class of φ in $W(K(Q))$ is same as class of $(\varphi_{K(Q)})_{an}$. Since $K(Q)/K$ is excellent $(\varphi_{K(Q)})_{an} \cong \psi$ for some quadratic form ψ over K and hence we are done. $\square$

We now discuss how K-valuations on $K(Q)$ are useful for our purpose. We refer to appendix (page 85) for basics on valuations. Let v be any K-valuation on $K(Q)$ and $\mathcal{O}_v, \mathfrak{m}_v, \kappa_v$ denote the valuation ring, maximal ideal of $\mathcal{O}_v$, residue class field respectively. For each valuation v we have second residue maps $\partial_v^2 : W(K(Q)) \to W(\kappa_v)$ (see appendix). Since the complete system of inequivalent valuations of $K(Q)/K$ consists of a countably infinite set of non-archimedean valuations and these valuations are all discrete (see [Has10, p. 332]), we define the *total residue map* as follows:

$$\partial^2 : W(K(Q)) \to \bigoplus_{v,\infty} W(\kappa_v)$$
$$\partial^2([\varphi]) = (\partial_{v_1}^2([\varphi]), \partial_{v_2}^2([\varphi]), \ldots)$$

Since $K(Q)$ and κ_v are extensions of K, the Witt groups $W(K(Q))$ and $W(\kappa_v)$ can be regarded as $W(K)$ modules. Then with the above notations we have the following theorem

Theorem 6.2.2 (Theorem 6b [Pfi93])**.** *The following is an exact sequence of $W(K)$-modules:*

$$0 \to \varphi W(K) \xrightarrow{i} W(K) \xrightarrow{\Phi} W(K(Q)) \xrightarrow{\partial^2} \bigoplus_{v} W(\kappa_v) \to C \to 0,$$

Where $\varphi \cong \langle 1, -a, -b, ab\rangle$ and $i : \varphi W(K) \to W(K)$ is inclusion map. The maps Φ and ∂^2 are as above and C is cokernel of ∂^2.

6.2.2 An Excellence Result

All notations are as before. Recall that a quaternion algebra $Q = (a,b)_K$ splits over K if and only if norm form has non trivial zero (see 4.1.8). Therefore the algebra $Q_{K(Q)}$ is split as the norm form $\langle 1, -a, -b, ab\rangle$ is isotropic over the field $K(Q)$. The field $K(Q)$ is called *generic splitting field* of Q. Using this property we prove the following result:

Proposition 6.2.3. *Let $Q = (a,b)_K$ be a quaternion algebra over K and v be a K-valuation on $K(Q)$ with residue class field κ_v, then Q splits over κ_v.*

Proof. To prove the proposition it is enough to prove that the equation $ax^2 + by^2 = 1$ is solvable over κ_v. Consider the quadratic form $ax^2 + by^2 - z^2$. Since this quadratic form is isotropic over $K(Q)$ it has an isotropic vector, say (x_0, y_0, z_0). Observe that $v(z_0) \geq \min(v(x_0), v(y_0))$. We consider the following two cases:

1. when $v(z_0) = v(x_0)$. Then

   $$a\left(\tfrac{x_0}{z_0}\right)^2 + b\left(\tfrac{y_0}{z_0}\right)^2 = 1$$

   Let $x' = \dfrac{x_0}{z_0}, y' = \dfrac{y_0}{z_0}$. Then

   $$ax'^2 + by'^2 = 1$$

   As $v(x') = 0$, reading modulo $\mathfrak{m}_v$ we conclude that the form $ax^2 + by^2$ represents 1 over κ_v.

2. $v(x_0) \leq v(y_0) < v(z_0)$. We have

   $$\begin{aligned} ax_0^2 &= z_0^2 - by_0^2 \\ \Rightarrow v(ax_0^2) &= v(z_0^2 - by_0^2) \\ \Rightarrow v(a) + 2v(x_0) &\geq \min(2v(z_0), v(-b) + 2v(y_0)) \\ \Rightarrow v(x_0) &\geq \min(v(z_0), v(y_0)) \\ \Rightarrow v(x_0) &\geq v(y_0) \end{aligned}$$

   Hence we get $v(x_0) = v(y_0)$. Let $v(x_0) = v(y_0) = r$ and $\pi \in K(Q)$ be such that $v(\pi) = 1$. Let $x_0' = \pi^{-r}x_0$ and $y_0' = \pi^{-r}y_0$. Then

   $$ax_0'^2 + by_0'^2 = (z_0\pi^{-r})^2$$

Reading above equation mod $\mathfrak{m}_v$, we get

$$ax_0'^2 + by_0'^2 = 0 \quad \bmod (\mathfrak{m}_v).$$

Hence the two dimensional form $\langle a, b\rangle$ is isotropic over κ_v and hence hyperbolic. Therefore it will represent 1 and the desired quadratic form is isotropic and we are done in this case too.

These are essentially the cases as other cases follow from symmetry of the quadratic form $ax^2 + by^2 = z^2$ in variable x and y. □

Lemma 6.2.4. *Let v be any K-valuation on $K(Q)$. Let M be the completion of $K(Q)$ with respect to v. If κ_v is the residue class field and L is relative algebraic closure of K in M then L is embedded into κ_v and κ_v/L is finite purely inseparable extension.*

Proof. **Step 1** Let $\alpha \in L$. Then α will satisfy a polynomial over K, say

$$f(x) = a_0 + a_1x + \ldots + x^n.$$

Substituting $x = \alpha$, we get

$$\begin{aligned} 0 &= a_0 + a_1\alpha + \ldots + \alpha^n \\ \Rightarrow \alpha^n &= -(a_0 + a_1x + \ldots + a_{n-1}x^{n-1} \\ \Rightarrow nv(\alpha) &= v(a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}) \\ &\geq \min(v(a_0), v(a_1) + v(\alpha), \ldots, v(a_{n-1}) + (n-1)v(\alpha)) \\ &= \min(0, v(\alpha), \ldots, (n-1)v(\alpha)). \end{aligned}$$

Which implies $v(\alpha) = 0$. Hence L is embedded in κ_v.
Step 2 We show that the field extension κ_v/L is finite. Let t be an element of $K(Q)$ such that $v(t) = 1$. Then $L((t))$, the field of formal Laurent series (in the variable t) over L. As $L((t))$ is complete with respect to v, and $L \subseteq M, t \in M$ therefore $L((t))$ is contained in M.

Since t is a trascedental element of $K(Q)$, $K(t)/K$ is transcedental. Also we know that $K(Q)/K$ has transcedence degree 1, therefore $K(Q)/K(t)$ will be a finite extension. Adjoining generators of the extension $K(Q)/K(t)$ to $L((t))$, we obtain a finite extension M' of $L((t))$ contained in M. In fact, as a finite extension of a complete field M' is complete. Since M' contains $K(Q)$, the completion of $K(Q)$ must be contained in M'. Hence $M = M'$. Which implies that M is a finite extension of $L((t))$. Since $M/L((t))$ is unramified with respect to v, hence by fundamental equality, $[\kappa_v : L] = [M : L((t))]$ and κ_v/L is a finite extension.

Step 3 In this step we show that the extension κ_v/L is purely inseparable. Let $\kappa_v = \mathcal{O}_v/\mathfrak{m}_\mathfrak{v}$, where $\mathcal{O}_v$ is the valuation ring and $\mathfrak{m}_\mathfrak{v}$ is the maximal ideal of $\mathcal{O}_v$. Let $\mu + \mathfrak{m}_\mathfrak{v} \in \kappa_v$ with $v(\mu) \geq 0$ be any separable element over L. Let minimal polynomial of $\mu + \mathfrak{m}_\mathfrak{v}$ over L is $f(x)$. Then we have $f(\mu) \equiv 0 \mod \mathfrak{m}_\mathfrak{v}$. Since f(x) is separable over L, $f'(\mu) \not\equiv 0 \mod \mathfrak{m}_v$ and $f'(\mu)$ is a unit in $\mathcal{O}_v$. Therefore by Hensel's lemma (see appendix) there exists a unique solution $\mu' \in \mathcal{O}_v$ such that $f(\mu') = 0$ and $\mu' \equiv \mu \mod \mathfrak{m}_\mathfrak{v}$. As $\mu' \in M$ is algebraic over K, μ' belongs to L. Therefore, the element $\mu + \mathfrak{m}_\mathfrak{v}$ already belongs to L. This shows that the residue field is a purely inseparable extension of L. □

Proposition 6.2.5. *If φ is a Pfister form then $\partial_v^2(\varphi)$ is either 0 or scalar multiple of ∂_v^1.*

Proof. We will prove this by induction. If φ is 1-fold Pfister form then the result is clearly true. Now suppose φ is a k-fold Pfister form. Let $\psi = \varphi \otimes \langle 1, a\rangle$. Then $\psi = \varphi \oplus a\varphi$ and $\partial_v^2(\psi) = \partial_v^2(\varphi \oplus a\varphi)$. Suppose $\partial_v^2(\psi) \neq 0$. Then

$$\begin{aligned}\partial_v^2(\psi) &= \partial_v^2(\varphi \oplus a\varphi)\\ &= \partial_v^2(\varphi) \oplus \partial_v^2(a\varphi)\\ &= \partial_v^2(\varphi) \oplus \partial_v^2(\langle a\rangle)\partial_v^2(\varphi).\end{aligned}$$

We have the following two cases

1. $\partial_v^2(\langle a\rangle) = 0$. Then $\partial_v^2(\psi) = \lambda\langle 1, \bar{a}\rangle \otimes \partial_v^1(\varphi) = \lambda \cdot \partial_v^1(\psi)$.
2. $\partial_v^2(\langle a\rangle) = \langle \bar{a}\rangle$. Then $\partial_v^2(\psi) = \lambda\langle 1, \bar{\pi}\bar{\lambda}\bar{a}\rangle \otimes \partial_v^1(\varphi) = \lambda \cdot \partial_v^1(\psi)$.

□

Theorem 6.2.6. *(Springer's Theorem) Let L/K be an extension of odd degree. If a K-quadratic form φ is anisotropic over K then φ_L is anisotropic over L.*

Proof. See [Lam05, p. 194] □

The following theorem is an important tool in proving the main conjecture.

Theorem 6.2.7. *Let $(\mathcal{A}, \sigma)$ be a central simple algebra with orthogonal involution over K. Let $\mathcal{A} \cong M_n(Q)$, where $n \in \mathbb{N}$ and Q is a K-quaternion algebra Q. If*

$(\mathcal{A},\sigma)_{K(Q)}$ is adjoint to a Pfister form over $K(Q)$ then there exists a Pfister form ψ over K such that $(\mathcal{A},\sigma)_{K(Q)} \cong \operatorname{Ad}\psi_{K(Q)}$.

Proof. Let $(\mathcal{A},\sigma)$ be a central simple K-algebra with orthogonal involution and $\mathcal{A} \cong M_n(Q)$. Let $\wp$ be a Pfister form over $K(Q)$ such that $(\mathcal{A},\sigma)_{K(Q)} \cong \operatorname{Ad}\wp$. Let $W(K)$, $W(K(Q))$ and Φ be as in the §6.2.1. By lemma 6.2.1, it is enough to show that $\wp$ denotes a class in the image of the natural map Φ. By theorem 6.2.2, image of Φ is equal to the kernel of the product of all second residue maps $\partial_v^2 : W(K(Q)) \to W(\kappa_v)$, where v is a K-valuation on $K(Q)$ and κ_v is its residue class field. Therefore it is enough to show that $\partial_v^2(\wp) = 0 \in W(\kappa_v)$ for every K-valuation v on $K(Q)$.

Let v be a K-valuation on $K(Q)$ with residue field κ_v. Since $K(Q)$ is splitting field of Q, by proposition 6.2.3 Q also splits over κ_v. Let (M, v') be the completion of $(K(Q), v)$. Then the residue class field of (M, v') will be equal to κ_v and hence $\partial_v^2(\wp) = \partial_v^2(\wp_M)$. Let L be the relative algebraic closure of K in M. Then by proposition 6.2.3, the field extension L/K is naturally embedded into κ_v/K. Also by lemma 6.2.4, κ_v/L is finite purely inseparable. Since $K \subseteq L$, $\operatorname{char} L \neq 2$. Hence κ_v/L is an odd degree extension. Therefore, by Springer's theorem 6.2.6 Q already splits over L. Now by 5.2.4, there exists a quadratic form φ over L such that $(\mathcal{A},\sigma)_L \cong \operatorname{Ad}\varphi$. Therefore $(\mathcal{A},\sigma)_M \cong \operatorname{Ad}(\varphi_M) \cong \operatorname{Ad}(\wp_M)$. Therefore $\wp_M \cong \lambda\varphi_M$, for some $\lambda \in M$. Observe that $\partial_v^2(\varphi) = 0$, as φ is defined over L. Hence $0 = \partial_v^2(\varphi) = \partial_v^2(\lambda\wp_M)$. If $v'(\lambda) = 0$ then $0 = \partial_v^2(\wp_M) = \partial_v^2(\wp)$ and in this case we are done. If $v'(\lambda) \neq 0$ then $0 = \partial_v^1(\wp_M) = \partial_v^1(\lambda\wp)$. Since $\wp$ is a Pfister form, by lemma 6.2.5, $\partial_v^2(\wp)$ will be scalar multiple of $\partial_v^1(\wp)$ and $\partial_v^2(\wp) = 0$ and we are done. □

Theorem 6.2.8. *Let $(\mathcal{A},\sigma)$ be an algebra with orthogonal involution over K. Assume that $\mathcal{A}$ is Brauer equivalent to a quaternion algebra Q. Then $(\mathcal{A},\sigma)$ is hyperbolic if and only if $(\mathcal{A},\sigma)_{K(Q)}$ is hyperbolic.*

Proof. The result follows from 5.4.12. □

6.3 A Proof of Pfister Factor Conjecture

We saw in remark 5.1.9 all split symplectic involutions are isomorphic and hence if $(\mathcal{A},\sigma)$ is a split central simple algebra with symplectic involution in conjecture 6.1 then $(\mathcal{A},\sigma) \cong (Q,\gamma) \otimes (Q_2,\sigma_2) \otimes \ldots \otimes (Q_n,\sigma_n)$, where γ is canonical involution on Q and σ_i's are orthogonal involutions. Since for every field extension L/K the (Q,γ) is hyperbolic (see example 5.3.8) the algebra $(\mathcal{A},\sigma)$ is hyperbolic for every field extension

L/K. Therefore conjecture is true in this case. The following theorem verifies the conjecture for split orthogonal case.

Theorem 6.3.1. *Let $n \in \mathbb{N}$ and let $(Q_1, \sigma_1), \ldots, (Q_n, \sigma_n)$ be K-quaternion algebras with involutions. If $\bigotimes_{i=1}^{n}(Q_i, \sigma_i)$ is a split K-algebra with orthogonal involution, then it is adjoint to a Pfister form.*

Proof. Since $\bigotimes_{i=1}^{n}(Q_i, \sigma_i)$ is an algebra with orthogonal involution, from observation 5.2.7 it follows that the number of symplectic factors (Q_i, σ_i) is even. Also by theorem 5.2.8, any product of two quaternion algebras with symplectic involution is isomorphic to a product of two quaternion algebras with orthogonal involution. Hence we can assume that all factors in the product are orthogonal.

We prove the result by induction on n. Let $n = 1$. Then (Q, σ) is a split quaternion algebra with orthogonal involution. That is $(Q, \sigma) \cong (M_2(K), \sigma) \cong (M_2(K), \sigma_\varphi)$, for some 2-dimensional quadratic form φ over K. Hence the statement is true. Assume that result holds for n. We want to prove the result for $n + 1$. Let $(Q_1, \sigma_1), \ldots, (Q_{n+1}, \sigma_{n+1})$ are K-quaternion algebras with orthogonal involutions such that $\bigotimes_{i=1}^{n+1}(Q_i, \sigma_i)$ splits. Let $(\mathcal{A}, \sigma) = \bigotimes_{i=1}^{n}(Q_i, \sigma_i)$ and $(Q, \tau) = (Q_{n+1}, \sigma_{n+1})$. Then $\mathcal{A}$ is Brauer equivalent to Q. As $(\mathcal{A}, \sigma) \otimes (Q, \tau)$ is split, $(\mathcal{A}, \sigma) \otimes (Q, \tau) \cong \mathrm{Ad}(\varphi)$, for some quadratic form φ over K. Since $K(Q)$ is generic splitting field of Q that is $Q \otimes_K K(Q) \cong M_2(K(Q))$, the algebra $(\mathcal{A}, \sigma)_{K(Q)}$ is a split algebra. Hence by induction hypothesis, $(\mathcal{A}, \sigma)_{K(Q)}$ is adjoint to a Pfister form and theorem 6.2.7 shows that $(\mathcal{A}, \sigma)_{K(Q)} \cong \mathrm{Ad}(\psi_{K(Q)})$ for an n-fold Pfister form ψ defined over K.

If $(\mathcal{A}, \sigma)$ is hyperbolic then $(\mathcal{A}, \sigma) \otimes (Q, \tau)$ is also hyperbolic and φ is hyperbolic $(n + 1)$-fold Pfister form. In this case we are done. Therefore assume $(\mathcal{A}, \sigma)$ is not hyperbolic. By theorem 2, $(\mathcal{A}, \sigma)_{K(Q)}$ is not hyperbolic. Hence the Pfister form $\psi_{K(Q)}$ is not hyperbolic and therefore anisotropic. Consider the function field $L = K(\psi)$. Then $\psi_{L(Q)}$ is an isotropic Pfister form and hence hyperbolic. Therefore $(\mathcal{A}, \sigma)_{L(Q)} \cong \mathrm{Ad}(\psi_{L(Q)})$ is hyperbolic. By theorem 6.2.8 $(\mathcal{A}, \sigma)_L$ is hyperbolic. Therefore $(\mathcal{A}, \sigma)_L \otimes_L (Q, \tau)_L$ becomes hyperbolic. Since $(\mathcal{A}, \sigma)_L \otimes (Q, \tau)_L \cong \mathrm{Ad}(\varphi_L)$ the quadratic form φ_L is hyperbolic. Hence

$$(\varphi)_{an} \cong \beta \otimes \psi$$

for some quadratic form β over K. Also observe $\dim \varphi = 2^{n+1}$ and $\dim \psi = 2^n$ and hence $\dim \beta \leq 2$. We have the following cases

- If $\dim \beta = 0$. Then anisotropic part is zero and φ is hyperbolic $(n + 1)$-fold Pfister form.

- If $\dim\beta = 2$. Then $\varphi \cong \beta\otimes\psi = \wp$. Then $(\mathcal{A},\sigma)\otimes(Q,\tau) \cong \mathrm{Ad}(\varphi) \cong \mathrm{Ad}(\wp)$, where $\wp$ is an $(n+1)$-fold Pfister form.

- If $\dim\beta = 1$. Then $(\varphi)_{an} \cong c\psi$, for some $c \in K^*$. Therefore φ contains 2^n-dimensional hyperbolic form. Hence $\varphi_{K(Q)}$ is isotropic but not hyperbolic. Therefore φ is not similar to a Pfister form. However $(Q,\tau)_{K(Q)} \cong \mathrm{Ad}(\theta)$, where θ is a 1-fold Pfister form. Therefore $(\mathcal{A},\sigma)_{K(Q)}\otimes(Q,\tau)_{K(Q)} \cong \mathrm{Ad}(\theta\otimes\psi)_{K(Q)} \cong \mathrm{Ad}(\varphi_{K(Q)})$ and $\varphi_{K(Q)}$ is similar to $(\theta\otimes\psi)_{K(Q)}$. Since $(\theta\otimes\psi)_{K(Q)}$ is an $(n+1)$-fold Pfister form, $\varphi_{K(Q)}$ is similar to a Pfister form. This is a contradiction. Hence $\dim\beta \neq 1$.

□

Corollary 6.3.2. *Let Q be a K-quaternion algebra. Let $(\mathcal{A},\sigma)$ be a central simple K-algebra with symplectic involution such that $\mathcal{A}$ is Brauer equivalent to Q and* $\deg(\mathcal{A}) = 2^n$ *with $n \in \mathbb{N}$. Let γ denote the canonical involution of Q. Then the following are equivalent:*

1. *$(\mathcal{A},\sigma)$ is a product of quaternion algebras with involutions.*
2. *$(\mathcal{A},\sigma)\otimes_K(Q,\gamma)$ is adjoint to a Pfister form.*
3. *$(\mathcal{A},\sigma) \cong (Q,\gamma)\otimes_K \mathrm{Ad}(\wp)$, for some Pfister form $\wp$ over K.*
4. *For any field extension L/K, the L-algebra $(\mathcal{A},\sigma)_L$ is either anisotropic or hyperbolic.*

Proof.

- ($1 \Rightarrow 2$) Let $(\mathcal{A},\sigma) \cong \bigotimes_{i=1}^r (Q_i,\sigma_i)$ be a central simple algebra with symplectic involution. Since (Q,γ) is a quaternion algebra with symplectic involution, the product algebra $(\mathcal{A},\sigma)\otimes(Q,\gamma)$ is a central simple algebra with orthogonal involution and hence by previous theorem $(\mathcal{A},\sigma)\otimes(Q,\gamma)$ is adjoint to a Pfister form over K.

- ($2 \Rightarrow 3$) Since Q splits over $K(Q)$, the algebra $(Q,\gamma)_{K(Q)}$ is hyperbolic and hence the product $(\mathcal{A},\sigma)\otimes(Q,\gamma)$ is hyperbolic. As $(\mathcal{A},\sigma)\otimes(Q,\gamma)$ is adjoint to a Pfister form ψ over K, $\psi_{K(Q)}$ is hyperbolic. Let N be the norm form of Q then by corollary 3.3.3 it follows that $\psi \cong N\otimes\wp$ for some Pfister form $\wp$ over K.

  Since $\mathcal{A}$ is Brauer equivalent to Q, $\mathcal{A} \cong M_m(K)\otimes_K Q$, where $m = 2^{n-1}$. Therefore $(\mathcal{A},\sigma) \cong (Q,\gamma)\otimes\mathrm{Ad}(\varphi)$ for some K-quadratic form φ which represents

1. Therefore $\mathrm{Ad}(\psi) \cong (\mathcal{A}, \sigma) \otimes (Q, \gamma) \cong \mathrm{Ad}(N \otimes \varphi)$. Since ψ is a Pfister form and $N \otimes \varphi$ represents 1 it follows that $N \otimes \varphi \cong \psi$. Therefore we get $N \otimes \varphi \cong N \otimes \wp$. Therefore the forms φ and $\wp$ extend to the same hermitian form over (Q, γ) and hence by theorem 5.4.11 the quadratic form φ and $\wp$ are isometric. This proves the implication.

- $(3 \Rightarrow 1)$ This is clear as for a Pfister form $\wp$, $\mathrm{Ad}(\wp)$ is product of quaternion algebras.

- $(3 \Rightarrow 4)$ Now suppose $(\mathcal{A}, \sigma) \cong (Q, \gamma) \otimes_K \mathrm{Ad}(\wp)$, for some Pfister form $\wp$ over K. Observe that $(\mathcal{A}, \sigma)$ is isotropic or hyperbolic if and only if the product algebra $(\mathcal{A}, \sigma) \otimes (Q, \gamma)$ is isotropic or hyperbolic. This is possible if and only if the quadratic form $N \otimes \wp$ is isotropic or hyperbolic. Let L/K be any field extension. Then $(\mathcal{A}, \sigma)_L$ is isotropic or hyperbolic if and only if the quadratic form $(N \otimes \wp)_L$ is isotropic or hyperbolic. Since $N \otimes \wp$ is a Pfister form, the form $(N \otimes \wp)_L$ is either anisotropic or hyperbolic. Therefore $(\mathcal{A}, \sigma)_L$ is either anisotropic or hyperbolic.

- $(4 \Rightarrow 1)$ As a K-algebra $(\mathcal{A}, \sigma) \otimes_K (Q, \gamma)$ is split with orthogonal involution hence adjoint to a K-quadratic form say ψ. Let L/K be any field extension. The L-algebra $(\mathcal{A}, \sigma)_L$ is either anisotropic or hyperbolic if and only if the L-algebra $(\mathcal{A}, \sigma)_L \otimes_L (Q, \gamma)_L$ is either anisotropic or hyperbolic. This is possible if and only if ψ_L is either anisotropic or hyperbolic. Therefore ψ is a Pfister form and hence $(\mathcal{A}, \sigma)$ is a product of quaternion algebras.

□

Theorem 6.3.3. *Let $(\mathcal{A}, \sigma)$ be a central simple algebra with orthogonal involution over K. Assume that $(\mathcal{A}, \sigma)$ is Brauer equivalent to a quaternion algebra Q over K and $\deg(\mathcal{A}) = 2^n$ with $n \geq 1$. Then the following are equivalent:*

1. *$(\mathcal{A}, \sigma)$ is a product of quaternion algebras with involutions.*

2. *$(\mathcal{A}, \sigma) \otimes_K (Q, \gamma)$ is adjoint to a Pfister form.*

3. *$(\mathcal{A}, \sigma) \cong (Q, \tau) \otimes_K \mathrm{Ad}(\wp)$, where τ is an orthogonal involution on Q and $\wp$ is some $(n-1)$-fold Pfister form over K.*

4. *For any field extension L/K, the L-algebra $(\mathcal{A}, \sigma)_L$ is either anisotropic or hyperbolic.*

Proof. 1. ($1 \Rightarrow 2$) Since $(\mathcal{A},\sigma)$ is Brauer equivalent to Q, the algebra $(\mathcal{A},\sigma)_{K(Q)}$ is split. As $(\mathcal{A},\sigma)$ is a product of quaternion algebras with involutions $(\mathcal{A},\sigma)_{K(Q)}$ is also product of quaternion algebras and implication follows from the split case.

2. ($2 \Rightarrow 4$) Suppose $(\mathcal{A},\sigma)_{K(Q)}$ is adjoint to a Pfister form. Let L/K be any field extension such that $(\mathcal{A},\sigma)_L$ is not hyperbolic. We show that $(\mathcal{A},\sigma)_L$ is anisotropic. Since $(\mathcal{A},\sigma)_L$ is not hyperbolic, from 6.2.8 it follows that $(\mathcal{A},\sigma)_{L(Q)}$ is not hyperbolic. As $(\mathcal{A},\sigma)_{K(Q)}$ is adjoint to a Pfister form and $L(Q)$ is an extension of $K(Q)$, the algebra $(\mathcal{A},\sigma)_{L(Q)}$ is anisotropic. Hence $(\mathcal{A},\sigma)_L$ is anisotropic and we are done.

3. ($4 \Rightarrow 2$) Let φ be a quadratic form over $K(Q)$ with $(\mathcal{A},\sigma)_{K(Q)} = \mathrm{Ad}(\varphi)$. Then $\dim(\varphi) = \deg(\mathcal{A}) = 2n$. With the assumption of 4 it follows that φ_L is anisotropic or hyperbolic for any field extension $L/K(Q)$. Therefore φ is similar to a Pfister form $\wp$ over $K(Q)$, and then $(\mathcal{A},\sigma)_{K(Q)} = \mathrm{Ad}(\varphi) = \mathrm{Ad}(\wp)$.

4. ($2 \Rightarrow 3$) Assume that $(\mathcal{A},\sigma)_{K(Q)}$ is adjoint to a Pfister form. Then by the excellence result 6.2.7, $(\mathcal{A},\sigma)_{K(Q)} = \mathrm{Ad}(\wp_{K(Q)})$ for an n-fold Pfister form $\wp$ over K. Let γ denote the canonical involution on Q. Then in view of theorem 5.4.6 $(\mathcal{A},\sigma)$ is adjoint to a skew-hermitian form h of rank 2^{n-1} over (Q,γ). Let $\delta \in Q^*$ be an element represented by h. Then δ is a pure quaternion. Let $d = \delta^2 \in K^*$. As $\sigma\delta = -\delta$, by theorem 5.4.8 the extended algebra $(\mathcal{A},\sigma)$ is hyperbolic. Also note that $(\mathcal{A},\sigma)_{K(\sqrt{d})}$ is split as Q splits over $K(\sqrt{d})$. Therefore $(\mathcal{A},\sigma)_{K(\sqrt{d})} = \mathrm{Ad}(\wp_{K(\sqrt{d})})$, and $\wp_{K(\sqrt{d})}$ is hyperbolic. Hence theorem 2.2.2 implies that $\wp \cong \langle 1,-d\rangle \otimes \rho$ over K for some $(n-1)$-fold Pfister form ρ. Let τ be orthogonal involution on Q with $\tau(\delta) = -\delta$. Then by theorem 5.4.9 $\mathcal{A}$ contains an σ invariant subalgebra isomorphic to (Q,τ). The centraliser of this subalgebra is then split and also σ-invariant (see [Sch85, p. 311]). Since $\mathcal{A}$ is Brauer equivalent to Q and τ is orthogonal $(\mathcal{A},\sigma) \cong (Q,\tau) \otimes (\mathcal{A}',\sigma')$, where $(\mathcal{A}',\sigma')$ is a split K-algebra with orthogonal involution hence there exists a quadratic form say ν such that $(\mathcal{A}',\sigma') \cong \mathrm{Ad}(\nu)$. Therefore $(Q,\tau) \otimes \mathrm{Ad}(\nu)$. Let h' be the extended hermitian form of ν over (Q,τ) such that $(\mathcal{A},\sigma)$ is adjoint to h'. Since $(Q,\tau)_{K(Q)}$ is adjoint to the quadratic form $\langle 1,-d\rangle$ over $K(Q)$, we have $(\mathcal{A},\sigma)_{K(Q)} \cong \mathrm{Ad}(\langle 1,-d\rangle \otimes \nu)$. In view of theorem 5.2.4 we can assume that ν represents 1. Hence $(\langle 1,-d\rangle \otimes \nu)_{K(Q)} \cong \wp_{K(Q)}$. Therefore the two algebras $Q \otimes \mathrm{Ad}(\rho)$ and $Q \otimes \mathrm{Ad}(\nu)$ are isomorphic over $K(Q)$. Hence from theorem 5.4.12

it follows that ρ and ν are isometric and hence $(\mathcal{A}, \sigma) \cong (Q, \tau) \otimes \mathrm{Ad}(\rho)$. This completes the proof.

5. $(3 \Rightarrow 1)$ Obvious.

$\square$

Appendix A

Valuation Theory

Definition A.0.4 Let S be a set. An order on S is a binary relation $\leq$ for all $a, b, c \in S$, satisfying following conditions:

1. $a \leq a$
2. $a \leq b, b \leq a \Rightarrow a = b$
3. $a \leq b, b \leq c \Rightarrow a \leq c$
4. $a \leq b$ or $b \leq a$

$(S, \leq)$ is called an ordered set.

An ordered abelian group is an abelian group $(G, +)$ with an order relation $\leq$ on G satisfying the following:

$$a \leq b \Rightarrow a + c \leq b + c$$

where $a, b, c \in G$. This condition make sure that order relation respects the group operation.

Example A.0.5 $(\mathbb{R}, +, \leq)$ is an ordered abelian group with usual ordering. Let K be a field.

We recall some basic definitions and results of valuation theory which are used in proving further results.

Definition A.0.6 Let Γ be an ordered abelian group and ∞ be a symbol satisfying the condition

$$\infty = \infty + \infty = \gamma + \infty = \infty + \gamma, \ \forall \gamma \in \Gamma.$$

A *valuation* v is a surjective map

$$v : K \to \Gamma \cup \{\infty\}$$

such that for all $x, y \in K$

$$v(x) = \infty \Rightarrow x = 0,$$
$$v(xy) = v(x) + v(y),$$
$$v(x + y) \geq \min(v(x), v(y)).$$

Observation A.0.7

1. $v(1) = v(1 \cdot 1) = v(1) + v(1) = 2v(1) \Rightarrow v(1) = 0$
2. $v(x \cdot x^{-1}) = v(1) \Rightarrow v(x) + v(x^{-1}) = 0 \Rightarrow v(x^{-1}) = -v(x)$
3. $v(-x) = v(-1) + v(x) = v(x)$
4. If $v(x) < v(y)$ then $v(x + y) = v(x)$.
   As $v(x) < v(y)$ therefore $v(x) = v(x + y - y) \geq \min(v(x + y), v(y)) \geq v(x + y)$.
   Also $v(x + y) \geq \min(v(x), v(y)) = v(x)$. Hence $v(x + y) = v(x)$.

Definitions A.0.8 Let $v : K \to \Gamma \cup \{\infty\}$ be a valuation. Then the set

$$\mathcal{O}_v = \{x \in K | v(x) \geq 0\}$$

forms a subring of K and it is called *valuation ring* of K. Observe that the set

$$\mathfrak{m}_v = \{x \in K | v(x) > 0\}$$

is a maximal ideal of $\mathcal{O}_v$. Define the *residue class field* of a valuation v as

$$K_v = \mathcal{O}_v / \mathfrak{m}_v.$$

The image of the valuation map is called *value group*. If value group is isomorphic to the additive group of integers then we say valuation is *discrete*. All valuation we consider here are discrete.

Definition A.0.9 Let L/K be a field extension and v and w are valuations on K and L respectively. The valuation w is said to be an *extension of* v if $w|_K = v$.

Definition A.0.10 Let (K, v) be a valued field. A sequence $(a_k)_{k\geq 0}$ is said to be Cauchy with respect to the valuation v if

$$\lim_{m,n\to\infty} v(a_n - a_m) = 0.$$

and convergent to a in K with respect to valuation v if

$$\lim_{n\to\infty} v(a - a_n) = 0.$$

Definition A.0.11 Let (K, v) be a valued field. Then K is called complete if every Cauchy sequence converges in K.

Theorem A.0.12. *For every valued field (K, v), upto valuation isomorphism there exists one and only one valuation extension (M, v') which is complete and in which K is dense.*

Proof. See [EP05, p. 50]. □

This unique extension is called *completion* of (K, v).

Theorem A.0.13. *Residue class fields and value groups of (K, v) and (M, v') are canonically isomorphic.*

Proof. See [EP05, p. 52]. □

Theorem A.0.14. *(Hensel's Lemma) Let (K, v) be a complete valued field and $f(x)$ be a polynomial with coefficients in $\mathcal{O}_v$. Then if $a \in \mathcal{O}_v$ satisfies*

$$f(a) \cong 0 \mod \mathfrak{m}$$
$$f'(a) \ncong 0 \mod \mathfrak{m}$$

then there exists $b \in K$ such that

$$f(b) = 0 \text{ and } b \cong a \mod \mathfrak{m}.$$

Proof. See [EP05, p. 88]. □

First and Second Residue Homomorphisms

Let v be a trivial valution on a field K. Then the valuation ring is $\mathcal{O}_v$ is equal to K and K is itself complete with respect to v. Let L/K be an extension field. By a *K-valuation* on L we mean a valuation which is trivial on K. In that case K is embedded in L_v. We have the following important theorem

Theorem A.0.15. *(Springer, Knebusch). Let (K, v) be a discrete valued field. Let π be an element of $\mathcal{O}_v$ such that $v(\pi) = 1$. Then a quadratic form $\varphi \cong \langle a_1, \ldots, a_n\rangle$ has unique representation as $\langle \pi^{r_1}u_1, \ldots, \pi^{r_n}u_n\rangle$ where u_i's are invertible in $\mathcal{O}_v$ and for a fixed integer k = 1 or 2, there is one and only one additive homomorphism*

$$\partial_v^k : W(K) \to W(K_v)$$

defined as each coefficient $\langle \pi^{r_i}u_i\rangle$ maps to either $\langle \bar{u}_i\rangle$ or 0 according as $r_i \cong k \mod 2$ or $r_i \ncong k \mod 2$.

Proof. See [MH73, p. 85] □

The homomorphisms ∂_v^1 and ∂_v^2 from $W(K)$ to $W(K_v)$ are called *first* and *second residue homomorphism* associated with valuation v.
Observe that ∂_v^1 is independent of the choice of π but ∂_v^2 is not independent of the choice of π. Let π_1, π_2 be two uniformizers of v. If for a quadratic form φ over L, image of the second residue map are $\bar{\varphi}_1$ and $\bar{\varphi}_2$ with respect to π_1 and π_2 respectively, then $\varphi_1 \cong \lambda\varphi_2$, with $v(\lambda) = 0$.

Bibliography

[Alb39] A. A. Albert, *Structure of algebras*, no. XXIV, American Mathematical Society colloquium Publications, 1939.

[Bak02] A. Baker, *Matrix groups : An introduction to lie group theory*, Springer Undergraduate Mathematics Series, 2002.

[Bec08] K. J. Becher, *A proof of the pfister factor conjecture*, Inventiones Mathematicae **173** (2008), 1–6.

[BFST93] E. Bayer-Fluckiger, D.B. Shapiro, and J.-P. Tignol, *Hyperbolic involutions*, Mathematische Zeitschrift **214** (1993), 461–476.

[EP05] A.J. Engler and A. Prestel, *Valued field*, Springer-Verlag, 2005.

[Has10] H. Hasse, *Number theory*, Springer, 2010.

[Jac40] N. Jacobson, *A note on hermitian forms*, Bulletin of the American Mathematical Society **46** (1940), no. 4, 264–268.

[KMRT98] M.-A. Knus, A. S. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, 1998.

[Lam05] T. Y. Lam, *Introduction to quadratic forms over fields*, American Mathematical Society, 2005.

[MH73] J. Milnor and D. Husemoller, *Symmetric bilinear forms*, Springer-Verlag, 1973.

[Pfi65] A. Pfister, *Multiplicative qudratische formen*, Archiv Der Mathematik **16** (1965), 363–370.

[Pfi93] ———, *Quadratic lattices in function fields of genus 0*, Proceedings of the London Mathematical Society **66** (1993), no. 3, 257–278.

[Pfi95] ______, *Quadratic forms with applications to algebraic geometry and topology*, Cambridge University Press, 1995.

[PSS01] R. Parimala, R. Sridharan, and V. Suresh, *Hermitian analogue of a theorem of springer*, Journal of Algebra **243** (2001), no. 3, 780–789.

[Ros90] M. Rost, *On quadratic forms isotropic over the function field of a conic*, Mathematische Annalen **288** (1990), no. 3, 511–513.

[Sch85] W. Scharlau, *Quadratic and hermitian forms*, Springer-Verlag, 1985.

[Sha00] D. B. Shapiro, *Compositions of quadratic forms*, no. 33, De Gruyter Expositions in Mathematics, 2000.

Index