Classification of Quadratic Forms

Leena

A dissertation submitted for the partial fulfillment of MS degree

Indian Institute of Science Education and Research Mohali
April 2015

Certificate of Examination

This is to certify that the dissertation titled Classification of Quadratic Forms submitted by Ms.Leena (Reg. No. MP12015) for the partial fulfillment of MS degree 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 Sudesh Kaur Khanduja Dr. Aribam Chandrakant Dr. Amit Kulshrestha (Supervisor)

Dated: 24 April, 2015

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Dr. Amit Kulshrestha at the Indian Institute of Science Education and Research Mohali.
This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bona fide record of original work done by me and all sources listed within have been detailed in the bibliography.

Leena
(Candidate)
Dated: April 24, 2015

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)

Acknowledgement

I am extremely grateful to Dr. Amit Kulshrestha for providing me the opportunity to work under his supervision, for his excellent guidance and for the academic help he has rendered throughout my stay at IISER Mohali.

I would like to thank my friends Cigole Thomas and Prerna Paliwal for their forbearance and support at all times especially at those of distress and disappointments. I can't finish this note without thanking my family for their love and encouragement without which I wouldn't have been where I am now.

Every single person in my life has played a role in making me a better person either in one way or other. I would like to thank all those who has influenced my life with their presence.

Finally, I want to thank IISER Mohali for providing me such a pleasant environment to work.

Leena

Contents

Introduction

Quadratic forms over fields F with $\mathrm{char}(F) \neq 2$ are degree two homogeneous polynomials in finite number of variables. A linear change in these variables produces an *equivalent* quadratic form. In general, over an arbitrary field, or when the number of variables is too large, identifying invariants which classify quadratic forms, up to equivalence, is a difficult task. However, the classification is much easier when the underlying field is a local field. In this case, very few invariants, namely dimension, discriminant and Hasse invariant are enough to make this classification. This, in view of a local-global principle called Hasse-Minkowski theorem, leads to the study of quadratic forms over number fields. In this expository thesis, we aim to study these topics. We also aim to classify small dimensional quadratic forms over arbitrary fields.

Since quadratic forms can be used to construct involutions on matrix algebras, an attempt is also made to study invariants over central simple algebras, and to use them for classification of involutions of first type.

Chapter 1

Quadratic Forms

1.1 Introduction

Throughout this chapter F denote a field of characteristic $\neq 2$ and F^* will denote the multiplicative group of F.

Definition 1.1.1 An (n-ary) *quadratic form* over a field F is a polynomial in n variables over F that is homogeneous of degree 2.
Matrix Notation: By definition, a quadratic form f is of the type

$$f(X_1, ..., X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j \in F[X_1, ..., X_n] = F[X].$$

To make the coefficients symmetric, it is wonted to rewrite f as

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

where $a'_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$. In this way, f ascertains uniquely a symmetric matrix (a'_{ij}), which we shall denote by M_f. In terms of matrix notations, we have

$$f(X) = (X_1, ..., X_n).M_f. \begin{pmatrix} X_1 \\ . \\ . \\ . \\ X_n \end{pmatrix} = X^t.M_f.X$$

where t is transpose and X is viewed as a column vector.

Definition 1.1.2 Let f and g be two n-ary quadratic forms. We say f is *equivalent* to g (denoted as $f \cong g$) if there exists an invertible matrix $C \in GL_n(F)$ such that $f(X) = g(C.X)$; i.e., $M_f = C^t.M_g.C$.

Apparently, $\cong$ is an equivalence relation.

Example 1.1.3 The quadratic forms $g(X_1, X_2) = X_1X_2$ and $f(X_1, X_2) = X_1^2 - X_2^2$ are equivalent because

$$M_f = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = C^t.M_g.C$$

Definition 1.1.4 Let f be an n-ary quadratic form over F. Then the induced map $Q_f : F^n \to F$ defined as $Q_f(x) := x^t.M_f.x \in F$ where $x \in F^n$ is called the *quadratic map* defined by f.

Observations 1.1.5

1. The quadratic map Q_f determines uniquely the quadratic form f since char(F) $\neq 2$.
2. The map Q_f is quadratic as $Q_f(ax) = a^2Q_f(x)$ for all $x \in F^n$ and $a \in F$.
3. If we polarize Q_f by defining
$$B_f(x, y) = (Q_f(x + y) - Q_f(x) - Q_f(y))/2,$$
then $B_f : F^n \times F^n \to F$ is a symmetric bilinear pairing (i.e. B_f is linear in both variables and $B_f(x, y) = B_f(y, x)$ for all $x, y \in F^n$).
4. If B_f is the symmetric bilinear pairing, then by depolarization we can recapture the quadratic map Q_f; i.e., $Q_f(x) = B_f(x, x)$ for any $x \in F^n$.

If V is an n-dimensional vector space over F and $B : V \times V \to F$ is a symmetric bilinear pairing on V, then we call the pair (V, B) a *quadratic space* . We can associate a quadratic map $q : V \to F$ to the quadratic space (V, B) which is defined as $q(x) = B(x, x)$ for every $x \in V$.

Since q and B determine each other, it is logical to write (V, q) to represent the quadratic space (V, B). If we fix a basis $\{e_1, e_2, ..., e_n\}$ of V over F, then the quadratic space (V, B) induces a quadratic form

$$f(X_1, ..., X_n) = \sum_{i,j} B(e_i, e_j)X_iX_j \quad \text{with } M_f = (B(e_i, e_j))_{ij}; \quad 1 \leq i, j \leq n$$

The quadratic space (V, B) uniquely determines an equivalence class of quadratic forms.

Definition 1.1.6 Two quadratic spaces (V, B) and (V', B') are said to be *isometric* ($\cong$) if there exists a linear isomorphism $\tau : V \to V'$ such that

$$B'(\tau(x), \tau(y)) = B(x, y) \text{ for all } x, y \in V.$$

Such a τ is called an *isometry* .

Example 1.1.7 Let V be a two dimensional F-vector space and B_1, B_2 be two symmetric bilinear pairing defined as below

$$B_1(x, y) = d_1x_1y_1 + d_2x_2y_2$$

$$B_2(x, y) = d_1x_1y_1 + d_2a^2x_2y_2$$

where $x = (x_1, x_2)^t$, $y = (y_1, y_2)^t$ and $d_1, d_2 \in F$; $a \in F^*$.
Then $\tau : V \to V$ defined as $(x_1, x_2) \mapsto (x_1, ax_2)$ is an isometry; i.e., $(V, B_1) \cong (V, B_2)$.

Remark 1.1.8 There is a one to one correspondence between the equivalence classes of n-ary quadratic forms and the isometry classes of n-dimensional quadratic spaces.

Proposition 1.1.1. *Let (V, B) be a quadratic space and M be a symmetric matrix associated with B. Let V^* be the vector space dual of V. Then the following are equivalent:*

1. *M is a non singular matrix.*
2. *$x \mapsto B(\_, x)$ is an isomorphism of $V \to V^*$.*

Proof: For a proof we refer to ([Lam05], page 4).

If (V, B) satisfies either of the above conditions then it is called a *regular* or *non-singular* quadratic space.

Definition 1.1.9 Let (V, B) be a quadratic space and W be a F-vector subspace of V. Then the *orthogonal complement* of W (denoted by $W^\perp$) is defined as

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

The orthogonal complement of V itself is called the *radical* of (V, B) and we denote it by rad(V). One can observe that (V, B) is regular if and only if rad(V) $= 0$.

1.2 Diagonalisation of a Quadratic Form

Definition 1.2.1 The *orthogonal sum* of two quadratic spaces (V_1, B_1) and (V_2, B_2) is a quadratic space (V, B) where $V = V_1 \oplus V_2$ and B is the pairing $V \times V \to F$ given by

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

where $x_1, y_1 \in V_1$ and $x_2, y_2 \in V_2$. We shall denote it by $V_1 \perp V_2$.
Equivalently, in terms of quadratic map, we can define orthogonal sum as

$$q((v_1, v_2)) = q_1(v_1) + q_2(v_2) \quad \text{where } v_i \in V_i; \quad i = 1, 2 \tag{1.1}$$

where q, q_1, q_2 are the quadratic maps associated to the quadratic spaces $(V, B), (V_1, B_1), (V_2, B_2)$ respectively and q is denoted by $q_1 \perp q_2$.

Example 1.2.2 Let $V_1 = V_2 = \mathbb{R}^2$ and $q_1(x, y) = x^2+y^2$, $q_2(x, y) = x^2+xy$. Then, the orthogonal sum of (V_1, q_1) and (V_2, q_2) is the quadratic space (V, q) where $V = \mathbb{R}^4$ and $q(x, y, u, v) = x^2 + y^2 + u^2 + uv$.

Definition 1.2.3 Let (V_1, q_1) and (V_2, q_2) be two quadratic spaces over F. The *tensor product* of these quadratic spaces is a quadratic space (V, q) where $V = V_1 \otimes V_2$ and q is the quadratic map $V \to F$ given by

$$q(v_1 \otimes v_2) = q_1(v_1).q_2(v_2).$$

We denote q by $q_1 \otimes q_2$.

Observation 1.2.4

1. $q_1 \otimes q_2 \cong q_2 \otimes q_1$.
2. $(q_1 \otimes q_2) \otimes q_3 = q_1 \otimes (q_2 \otimes q_3)$.
3. $q \otimes (q_1 \perp q_2) \cong (q \otimes q_1) \perp (q \otimes q_2)$.
4. $\langle a_1, ..., a_m\rangle \otimes \langle b_1, ..., b_n\rangle \cong \langle a_1b_1, ..., a_ib_j, ..., a_mb_n\rangle$.

Definition 1.2.5 Let (V, q) be a quadratic space over F and $d \in F^*$. Then q is said to *represent* an element d if there exist $0 \neq v \in V$ such that $q(v) = d$.
Notation: Let (V, q) be any quadratic space, then

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

2. $\langle d \rangle$ denotes the one dimensional quadratic space (F, q) where the quadratic form is given by $q(x) = dx^2$.

3. A quadratic form of the type $\langle d_1 \rangle \perp \langle d_2 \rangle \perp ... \perp \langle d_n \rangle$; $d_i \in F$; $1 \leq i \leq n$ is denoted by $\langle d_1, d_2, ..., d_n \rangle$. Such a form is called *diagonal form* .

Proposition 1.2.1. *Let (V, q) be any quadratic space and $d \in F^*$. Then $d \in D(V)$ if and only if there exists another quadratic space (V', q') together with an isometry $q \cong \langle d \rangle \perp q'$.*

Proof: "Only if" part: $d \in D(V) \Rightarrow \exists v \in V$ such that $q(v) = d$. If V is not regular, then we can write V as $V = \mathrm{rad(V)} \perp \mathrm{V_1}$ where V_1 is a regular subspace of V. Therefore by equation (1.1), we have $D(V) = D(V_1)$. Thus, we may assume that V is regular. $\langle d \rangle$ is isometric to the quadratic subspace $F.v$ and $(F.v) \cap (F.v)^{\perp} = 0$ (otherwise $v \in \mathrm{rad(V)} = 0$). Thus,

$$q \cong \langle d \rangle \perp q'$$

where q' is the quadratic map defined on $(F.v)^{\perp}$ as $\dim(\mathrm{F.v}) + \dim(\mathrm{F.v})^{\perp} = \dim(\mathrm{V})$.
"If" part: Clearly, d is represented by $\langle d \rangle \perp q'$ and hence $d \in D(V)$.

Corollary 1.2.1. *Any n-ary quadratic form q is isometric to a diagonal form; i.e., $q \cong \langle d_1, d_2, ..., d_n \rangle$ where $d_i \in F$; $1 \leq i \leq n$.*

Proof: If $q = 0$ then q is represented by the diagonal form $\langle 0, 0, ..., 0 \rangle$. If there exists $d \in F^*$ which is represented by q, then by proposition (1.2.1) we have a quadratic space (V', q') such that $q \cong \langle d \rangle \perp q'$. Since $\dim_{\mathrm{F}}(\mathrm{V}') < \dim_{\mathrm{F}}(\mathrm{V})$, by induction on $\dim(\mathrm{V})$ we are done.

1.3 Hyperbolic Spaces and Witt's Theorems

Definition 1.3.1

1. Let (V, q) be a quadratic space. A non-zero vector $v \in V$ is said to be an *isotropic* if $q(v) = 0$, otherwise we say that v is *anisotropic* .

2. The quadratic space (V, q) is said to be *isotropic* if it contains an isotropic vector and is said to be *anisotropic* otherwise.

3. The quadratic space (V, q) is said to be *totally isotropic* if all non-zero vectors in V are isotropic.

Example 1.3.2

1. The quadratic form $q = x_1^2 - x_2^2$ is isotropic over any field F.
2. The quadratic form $q = x_1^2 + x_2^2$ is anisotropic over $\mathbb{R}$.
3. The 1-dimensional quadratic space (V, q) generated by an isotopic vector $0 \neq v \in V$ is a trivial example of totally isotropic space.

Definition 1.3.3 A two dimensional form which is isometric to the diagonal form $\langle 1, -1\rangle$ is called a *hyperbolic plane* . An orthogonal sum of hyperbolic planes is called a *hyperbolic space* .

Definition 1.3.4 A quadratic space (V, q) is said to be *universal* if q represents all the non-zero elements of F.

Example 1.3.5 Hyperbolic plane is an example of universal quadratic space because, for all $a \in F$,

$$a = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2.$$

Proposition 1.3.1. *A regular two dimensional quadratic space* (V, q) *is isotropic if and only if* $q \cong \langle 1, -1\rangle$.

Proof: "Only if" part: Let $\{e_1, e_2\}$ be an orthogonal basis of V over F.Since V is regular, $q(e_i) = d_i \neq 0$; $i = 1, 2$. Let $ae_1 + be_2$ be an isotropic vector, with (say) $a \neq 0$. Then

$$0 = q(ae_1 + be_2) = a^2 d_1 + b^2 d_2$$
$$\Rightarrow d_2 = -(ab^{-1})^2 d_1$$

which implies that $q \cong \langle d_1, d_2\rangle \cong \langle d_1, -(ab^{-1})^2 d_1\rangle \cong \langle d_1, -d_1\rangle$ and the last isometry can be easily observed by example (1.1.7). From example (1.1.3), it follows that $d_1x_1^2 - d_1x_2^2$ is equivalent to $d_1x_1x_2$ and apparently, $d_1x_1x_2$ represents 1. By proposition (1.2.1), we conclude that $q \cong \langle 1, -1\rangle$ and converse of this proposition is obvious (as in example (1.3.2)(1)).

The group of isometries of the quadratic space (V, q) is called an *orthogonal group* which is denoted by $O(V)$.
For an anisotropic vector $y \in V$, the map $\tau_y : V \to V$ given by

$$\tau_y(x) = x - \frac{2B(x, y)}{q(y)}y \quad \text{for every } x \in V$$

is an isometry. The determinant of τ_y is -1.

Theorem 1.3.6. ***(Witt's Decomposition Theorem)*** *Any quadratic space* (V, q) *splits into an orthogonal sum*

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

where (V_t, q_t) *is totally isotropic,* (V_h, q_h) *is hyperbolic and* (V_a, q_a) *is anisotropic. Moreover, the isometry classes of* V_t, V_h, V_a *are all uniquely determined.*

Proof: For a proof we refer to ([Lam05], page 12).

Definition 1.3.7 Let (V, q) be a quadratic space and $(V, q) \cong (V_t, q_t) \perp (V_h, q_h) \perp (V_a, q_a)$ where (V_t, q_t), (V_h, q_h) and (V_a, q_a) have the same meaning as they have in the previous theorem. Then the integer $m = \frac{1}{2}\dim(\mathrm{V_h})$ is called the *Witt index* .

Proposition 1.3.2. *Let* (V, q) *be a quadratic space and* $x, y \in V$ *be such that* $q(x) = q(y) \neq 0$*. Then there exists* $\tau \in O(V)$ *such that* $\tau(x) = y$*.*

Proof: For a proof we refer to ([Lam05], page 14).

Theorem 1.3.8. ***(Witt's Cancellation Theorem)*** *If* q, q_1, q_2 *are arbitrary quadratic forms over* F *such that* $q \perp q_1 \cong q \perp q_2$*, then* $q_1 \cong q_2$*.*

Proof: For a proof we refer to ([Lam05], page 12).

Now, we will introduce the notion of chain equivalence for the diagonal quadratic forms and we will see how isometry and chain equivalence of two quadratic forms are related.

Definition 1.3.9 Let $q = \langle a_1, ..., a_n \rangle$ and $q' = \langle b_1, ..., b_n \rangle$ be two quadratic forms. Then

1. q and q' are said to be *simply equivalent* if $\exists$ two indices i and j, such that
   (a) $\langle a_i, a_j \rangle \cong \langle b_i, b_j \rangle$ and
   (b) $a_k = b_k$ for all $k \neq i, j$.
2. q and q' are said to be *chain equivalent* (denoted as $q \approx q'$) if $\exists$ a sequence of diagonal quadratic forms $q_0, q_1, ..., q_m$ such that $q_0 = q$, $q_m = q'$ and q_i is simply equivalent to q_{i+1} for all $0 \leq i \leq m - 1$.

Theorem 1.3.10. *Let* $q = \langle a_1, ..., a_n \rangle$ *and* $q' = \langle b_1, ..., b_n \rangle$ *be two quadratic forms. Then* $q \cong q' \Leftrightarrow q \approx q'$*.*

Proof: For a proof we refer to ([Lam05], page 16).

Chapter 2

Classification of Quadratic Forms

2.1 Invariants of Quadratic Form

Let (V, q) denotes a quadratic space over a field F with char(F) $\neq 2$ and F^* denotes the multiplicative group of F.

Definition 2.1.1 The *dimension* of a quadratic form q (denoted by dim(q)) is defined as the dimension of the underlying vector space V over F; i.e., $\dim(\mathrm{q}) = \dim_{\mathrm{F}}(\mathrm{V})$.

Proposition 2.1.1. *Let r be any positive integer. Then the following statements are equivalent:*

1. *Any quadratic form of dimension $r+1$ over F is isotropic.*
2. *Any regular quadratic form of dimension r over F is universal.*

Proof: For a proof we refer to ([Lam05], page 11).

Definition 2.1.2 The *determinant* of a quadratic form q (denoted by det(q)) is defined as the square class of the determinant of the symmetric matrix associated with q; i.e.,

$$\det(\mathrm{q}) = \det(\mathrm{M_q}) \times \mathrm{F}^{*2} \in \mathrm{F}^*/\mathrm{F}^{*2}.$$

Observation 2.1.3

1. Determinant of a quadratic form q does not depend on the choice of representative of the isometry class because if we choose two different quadratic forms which belong to the same isometry class then determinant of the associated matrices differ by a square.

2. $\det(q_1 \perp q_2) = \det(q_1).\det(q_2)$.

Definition 2.1.4 The *discriminant* of a quadratic form q (denoted by disc(q)) is defined as the signed determinant; i.e., $\text{disc(q)} = (-1)^{n(n-1)/2}\det(q)$.

2.2 Witt Ring

Let M be a commutative cancellation monoid under addition.Then we can define a relation $\sim$ on $M \times M$ as $(x, y) \sim (x', y') \Leftrightarrow x + y' = x' + y$ where $x, x', y, y' \in M$.

Clearly, this is an equivalence relation on $M \times M$.

Definition 2.2.1 Let M be a commutative cancellation monoid. Then *Grothendieck group* of M (denoted by Groth(M)) is defined as $\text{Groth(M)} = \text{M} \times \text{M}/\sim$ with addition operation on $M \times M$ as $(x, y)+(x', y') = (x+x', y+y')$.

It is easy to check that Groth(M) is a commutative group with the above well defined addition operation. Identity element of Groth(M) is the equivalence class of (x, x); $x \in M$ and inverse of the equivalence class of (x, y) is the equivalence class of (y, x); $x, y \in M$.

We can define an injective map $i : M \to \text{Groth(M)}$ which maps $x \mapsto (x, 0)$.Thus, $M \subseteq \text{Groth(M)}$. We can view an element of Groth(M) as $(x, y) = i(x) - i(y) = x - y$.

Let $f : M \to G$ be a monoid homomorphism where G is an abelian group. Then it induces a group homomorphism $\tilde{f} : \text{Groth(M)} \to \text{G}$ given by $\tilde{f}(x - y) = f(x) - f(y) \in G$; and it is known as the *universal property* of Groth(M).

Let M be a commutative cancellation monoid under addition and it has a commutative multiplication (i.e., M is a commutative semiring). Then we can define multiplication on Groth(M) as $(x, y)(x', y') = (xx'+yy', xy'+yx')$. This multiplication makes Groth(M) a commutative ring.

Let $M(F)$ be the set of all isometry classes of regular quadratic forms over F and binary operations $\perp$ and $\otimes$ are the corresponding addition and multiplication operation on $M(F)$ which makes $M(F)$ into a commutative semiring.

Definition 2.2.2 $\widehat{W}(F) = \text{Groth(M(F))}$ is called the *Witt Grothendieck ring* of quadratic forms over F.

Consider the dimension map dim : M(F) $\to \mathbb{Z}$ which is a semiring homomorphism. Then by "universal property" we can extend this dimension map to a ring homomorphism $\widetilde{\dim} : \widehat{W}(F) \to \mathbb{Z}$ which is defined as $\widetilde{\dim}(q_1 - q_2) = \dim(\text{q}_1) - \dim(\text{q}_2)$. Kernel of $\widetilde{\dim}$ is called the *fundamental ideal* of $\widehat{W}(F)$ and it is denoted by $\widehat{I}F$.

Definition 2.2.3 $W(F) = \widehat{W}(F)/\mathbb{Z}.\mathbb{H}$ is called the *Witt ring* of F; where $\mathbb{H}$ denotes the hyperbolic plane.

Consider the natural projection map $\widehat{W}(F) \to W(F)$. Then image of $\widehat{I}F$ under this map is called the *fundamental ideal* of $W(F)$ and it is denoted by IF.

Proposition 2.2.1. *A quadratic form q represents an element in IF if and only if* dim(q) *is even.*

Proof: "If" part: If dim(q) is even, then we can assume that q is a binary form $\langle a, b\rangle$. Clearly, q is the image of $\langle a\rangle - \langle -b\rangle \in \hat{I}F$ under the natural projection $\widehat{W}(F) \to W(F)$ and therefore, q represents an element in $IF \subseteq W(F)$.
"Only if" part: If q represents an element in IF, then $\widetilde{q} = q_1 - q_2 + m\mathbb{H}$ where $m \in \mathbb{Z}$ and $\dim(\text{q}_1) = \dim(\text{q}_2)$. This implies that $\widetilde{\dim}(q) = \dim(\text{q}_1) - \dim(\text{q}_2) + 2\text{m} = 2\text{m}$.

Corollary 2.2.1. $W(F)/IF \cong \mathbb{Z}/2\mathbb{Z}$.

Proof: We know that $\widetilde{\dim} : \widehat{W}(F) \to \mathbb{Z}$ is a ring epimorphism which induces another ring epimorphism $\dim_0 : \text{W(F)} \to \mathbb{Z}/2\mathbb{Z}$ and $ker(\dim_0) = \text{IF}$ by the proposition (2.2.1).

In the previous section, we have given a monoid homomorphism, namely determinant, det : M(F) $\to \text{F}^*/\text{F}^{*2}$ defined as $q \mapsto \det(\text{q})$. By "universal property", the map det can be extended to $\widetilde{(\det)} : \widehat{W}(F) \to F^*/F^{*2}$ as

$$\widetilde{\det}(q_1 - q_2) = \det(\text{q}_1)\det(\text{q}_2)^{-1} = \det(\text{q}_1)\det(\text{q}_2) \in \text{F}^*/\text{F}^{*2}$$

which is a group homomorphism. We can not factor $\widetilde{(\det)}$ homomorphism through $W(F)$ as $\widetilde{(\det)}(\mathbb{H}) = (-1).F^{*2}$.

We can rectify this, using discriminant map because $\text{disc}(\mathbb{H}) = 1.\text{F}^{*2}$, but discriminant map is not a homomorphism on $W(F)$. To avoid this, we look at discriminant map together with $\dim_0$ and construct a new group which is a $\mathbb{Z}/2\mathbb{Z}$ extension of F^*/F^{*2}, namely,

$$Q(F) = \mathbb{Z}/2\mathbb{Z} \times (F^*/F^{*2}).$$

On $Q(F)$, we can define a binary operation as

$$(e, d).(e', d') = (e + e', (-1)^{ee'}dd')$$

It is easy to check that $Q(F)$ is a group with identity element $(0, 1)$ and inverse of (e, d) is $(e, (-1)^e d)$.

Proposition 2.2.2. $(\dim_0, \text{disc}) : \text{M(F)} \to \text{Q(F)}$ *defines a monoid epimorphism. This can be extended to a group epimorphism* $\widehat{W}(F) \to Q(F)$*. The latter induces a group isomorphism* $f : W(F)/I^2F \cong Q(F)$*.*

Proof: For a proof we refer to ([Lam05], page 31).

Proposition 2.2.3. *Every regular* 2*-dimensional quadratic form over a finite field* F *is universal.*

Proof: We know that $F^*/F^{*2} = \{1, s\}$; where s is a non-square.
Claim: s is a sum of two squares.
Case 1: $-1 \in F^{*2}$.
Then $\langle 1, 1\rangle \cong \langle 1, -1\rangle$, and therefore $\langle 1, 1\rangle$ is universal. So, $\langle 1, 1\rangle$ represents s. Hence s is sum of two squares.
Case 2: $-1 \notin F^{*2}$.
Consider the two sets F^{*2} and $1 + F^{*2}$, which are subsets of F with same cardinality. Since $1 \in F^{*2}$ and $1 \notin 1 + F^{*2}$, therefore $F^{*2} \neq 1 + F^{*2}$ as sets. So $\exists$ an element $1 + z^2 \notin F^{*2}$. Thus by taking s to be $1 + z^2$, the claim follows.
Since 1 and s are the only square classes, therefore there can be at most three nonequivalent 2-dimensional quadratic forms, which are:

$$q_1 = \langle 1, 1\rangle, \quad q_2 = \langle 1, s\rangle, \quad q_1 = \langle s, s\rangle.$$

Using the previous claim, we have $D(q_1) = F^*$, $D(q_3) = F^*$, and apparently, $D(q_2) = F^*$. Hence we are through.

2.3 Brauer Group

2.3.1 Central Simple Algebras

Definition 2.3.1 An *algebra* $\mathcal{A}$ over a field F is defined as an F-vector space equipped with associative F-linear multiplication; i.e., $\lambda(ab) = (\lambda a)b = a(\lambda b)$; where $a, b \in \mathcal{A}$ and $\lambda \in F$.

If $\mathcal{A}$ as an F-vector space is finite dimensional then we say that $\mathcal{A}$ is a *finite dimensional algebra* over F.

Definition 2.3.2 Let $\mathcal{A}$ be an algebra over F. Then

1. It is said to be *central* if center of $\mathcal{A}$ is F; i.e., $Z(\mathcal{A}) = F$.
2. It is said to be *simple* if $\mathcal{A}$ has no two sided ideal other than 0 and $\mathcal{A}$.
3. It is said to be *central simple* if it is both central and simple.

Example 2.3.3 Matrix algebra $\mathbb{M}_n(F)$ is a central simple algebra.

Definition 2.3.4 Let $\mathcal{A}$ and $\mathcal{B}$ are two F- algebras. Then their tensor product (denoted by $\mathcal{A} \otimes \mathcal{B}$) is an F- algebra together with F-algebra homomorphisms $i_{\mathcal{A}}$ and $i_{\mathcal{B}}$

$$\mathcal{A} \xrightarrow{i_{\mathcal{A}}} \mathcal{A} \otimes \mathcal{B} \xleftarrow{i_{\mathcal{B}}} \mathcal{B}$$

where $i_{\mathcal{A}}(a) = a \otimes 1$ and $i_{\mathcal{B}}(b) = 1 \otimes b$; satisfy the following conditions:

1. $i_{\mathcal{A}}(a) i_{\mathcal{B}}(b) = i_{\mathcal{B}}(b) i_{\mathcal{A}}(a)$ for all $a \in \mathcal{A}$ and $b \in \mathcal{B}$.
2. If $\alpha : A \to C$, $\beta : B \to C$ are F-algebra homomorphisms so that
$$\alpha(a)\beta(b) = \beta(b)\alpha(a) \quad \text{for all } a \in A, b \in B,$$
then there is a unique F-algebra homomorphism $\psi : A \otimes B \to C$ such that $\alpha = \psi i_{\mathcal{A}}$ and $\beta = \psi i_{\mathcal{B}}$.

Proposition 2.3.1. *Let $\mathcal{A}$ and $\mathcal{B}$ are two F-algebras. Then there is a map $i : \mathcal{A} \times \mathcal{B} \to \mathcal{A} \otimes \mathcal{B}$ which is bilinear multiplicative and satisfies the following "universal property":*
If $\mathcal{C}$ is an F-algebra and $\varphi : \mathcal{A} \times \mathcal{B} \to C$ is a bilinear multiplicative map, then there exists a unique F-algebra homomorphism $\psi : \mathcal{A} \otimes \mathcal{B} \to \mathcal{C}$ such that $\varphi = \psi \circ i$.

Proof: For a proof we refer to ([Sch85], page 286).

By a map i (as in the above proposition) to be *multiplicative*, we mean

$$i(aa', bb') = i(a, b)i(a', b').$$

Definition 2.3.5 Let $\mathcal{B}$ be a subset of a central simple algebra $\mathcal{A}$. Then *centralizer* of $\mathcal{B}$ in $\mathcal{A}$ is defined as:

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

Proposition 2.3.2. *1. Let $\mathcal{A}'$ and $\mathcal{B}'$ be subalgebras of $\mathcal{A}$ and $\mathcal{B}$ respectively. Then*

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

2. If $\mathcal{A}$ is a central simple algebra over F and $\mathcal{B}$ is a simple F-algebra, then $\mathcal{A} \otimes \mathcal{B}$ is simple.

3. If $\mathcal{A}$ and $\mathcal{B}$ are both central simple algebras, then $\mathcal{A}\otimes\mathcal{B}$ is also a central simple algebra.

Proof: For a proof we refer to ([Lam05], page 80).

Theorem 2.3.6. ***(Wedderburn's Theorem)*** *Let $\mathcal{A}$ be a finite dimensional central simple algebra over F. Then there exists $\mathcal{A} \cong \mathbb{M}_n(D)$ for a suitable division algebra D over F. Moreover, n and D are uniquely determined upto isomorphism.*

Proof: For a proof we refer to ([Sch85], page 282).

Theorem 2.3.7. ***(Skolem Noether Theorem)*** *Let $\mathcal{A}$ be a finite dimensional central simple F-algebra and $\mathcal{B}$ be a finite dimensional simple F-algebra. If $f, g : \mathcal{A} \to \mathcal{B}$ are two F-algebra homomorphisms, then $\exists u \in \mathcal{B}$ such that $f = \mathrm{Int(u)} \circ \mathrm{g}$.*

Proof: For a proof we refer to ([Sch85], page 291).

Corollary 2.3.1. *Every F-algebra automorphism of a central simple algebra $\mathcal{A}$ is inner.*

2.3.2 Brauer Group of a Field

Definition 2.3.8 Let $\mathcal{A}$ and $\mathcal{B}$ be two central simple F-algebras. Then $\mathcal{A}$ and $\mathcal{B}$ are said to be *Brauer equivalent* if there exists a central division algebra D such that $\mathcal{A} \cong \mathbb{M}_m(D)$ and $\mathcal{B} \cong \mathbb{M}_n(D)$ for $m, n \in \mathbb{N}$.

Let $\mathfrak{C}$ denotes the set of all finite dimensional central simple algebras over F. Then it is easy to check that Brauer equivalence defines an equivalence

relation on $\mathfrak{C}$. The set of equivalence classes of $\mathfrak{C}$ will be denoted by Br(F). For $\mathcal{A} \in \mathfrak{C}$, the equivalence class of $\mathcal{A}$ in Br(F) will be denoted by $[\mathcal{A}]$.

Define a binary operation on Br(F) as follows:

$$[\mathcal{A}] \otimes [\mathcal{B}] = [\mathcal{A} \otimes \mathcal{B}] \in \mathfrak{C}.$$

It is easy to check that the above defined binary operation is well defined on Br(F).

Definition 2.3.9 The *opposite ring* of a ring $\mathcal{A}$ (denoted by $\mathcal{A}^{op}$) is itself $\mathcal{A}$ as an additive group but multiplication on $\mathcal{A}^{op}$ is defined as $a^{op} \circ b^{op} = b.a$; where $a, b \in \mathcal{A}$ and $(\cdot)^{op}$ is just a way to represent elements of opposite ring.

Observations 2.3.10

1. $(\mathcal{A}^{op})^{op} = \mathcal{A}$.
2. $\mathcal{A}^{op}$ is a central simple algebra if and only if $\mathcal{A}$ is so.

Theorem 2.3.11. *Let $\mathcal{A}$ be an n dimensional central simple F-algebra. Then $\mathcal{A} \otimes \mathcal{A}^{op} \cong \mathbb{M}_n(F)$.*

Now one can easily check that the binary operation $\otimes$ defines a group structure on Br(F) with identity element $\mathbb{M}_m(F)$ and inverse of $\mathcal{A}$ is $\mathcal{A}^{op}$.

Definition 2.3.12 The set Br(F) is called the *Brauer group* of F with $\otimes$ as its binary operation.

Example 2.3.13 If F is an algebraically closed field, then there does not exist any proper finite dimensional division algebra D over F because otherwise $F(d)$ for $d \in D \setminus F$ will be a non trivial algebraic extension of F. Therefore, Brauer group of an algebraically closed field is trivial.

2.4 Quaternion Algebra

Definition 2.4.1 Let $a, b \in F^*$. Then the *quaternion algebra* (denoted by $(a, b)_F$) is defined as an F-algebra generated by i, j with the following defining relations:

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

It can be easily seen that $(a, b)_F$ is a four dimensional vector space over F with basis $\{1, i, j, ij\}$.

Observation 2.4.2 Let $a, b \in F^*$.

1. $(a,b)_F \cong (\lambda^2 a, \mu^2 b)_F \quad \forall \lambda, \mu \in F^*$.
2. $(a,b)_F \cong (b,a)_F$.

One can easily check that $(a,b)_F$ is a central simple algebra over F.

Definition 2.4.3 Let $x = x_0 + x_1 i + x_2 j + x_3 ij$ be an element of the quaternion algebra $(a,b)_F$; $x_i \in F$. Then *conjugate* of x is defined as $\overline{x} = x_0 - x_1 i - x_2 j - x_3 ij$.

Observation 2.4.4 Let $x, y \in (a,b)_F$. Then

1. $\overline{x_{+}y} = \overline{x} + \overline{y}$.
2. $\overline{x.y} = \overline{y}.\overline{x}$.
3. $\overline{\overline{x}} = x$.

Definition 2.4.5 Let $x = x_0 + x_1 i + x_2 j + x_3 ij$ be an element of the quaternion algebra $(a,b)_F$; $x_i \in F$. Then *norm* of x is defined as $N(x) = x.\overline{x} = x_0^2 - x_1^2 a - x_2^2 b + x_3^2 ab$. The quadratic form $\langle 1, -a, -b, ab\rangle$ is called the *norm form* of the quaternion algebra $(a,b)_F$.

Example 2.4.6 $(-1,-1)_{\mathbb{R}}$ is an example of a quaternion algebra. It is known as *Hamiltonian quaternion* . Let $x = x_0 + x_1 i + x_2 j + x_3 ij \in (-1,-1)_{\mathbb{R}}$; where $x_i \in \mathbb{R}$. Then

$$N(x) = x.\overline{x} = x_0^2 + x_1^2 + x_2^2 + x_3^2 \geq 0.$$

If x is a non zero element of $(-1,-1)_{\mathbb{R}}$, then $N(x) > 0$ and hence

$$x^{-1} = \frac{x_0 - x_1 i - x_2 j - x_3 ij}{x_0^2 + x_1^2 + x_2^2 + x_3^2}.$$

Thus $(-1,-1)_{\mathbb{R}}$ is division ring as every non zero element of $(-1,-1)_{\mathbb{R}}$ is invertible.

Theorem 2.4.7. *Let $\mathcal{A} = (a,b)_F$, $\mathcal{A}' = (a',b')_F$ be two quaternion algebras. Then the following statements are equivalent:*

1. *$\mathcal{A}$ and $\mathcal{A}'$ are isomorphic as F-algebras.*
2. *Their corresponding norm forms are isometric; i.e.,*

$$\langle 1, -a, -b, ab\rangle \cong \langle 1, -a', -b', a'b'\rangle.$$

Proof: For a proof we refer to ([Lam05], page 57).

Definition 2.4.8 An algebra $\mathcal{A} = (a, b)_F$ is said to be *split* if $\mathcal{A} \cong \mathbb{M}_2(F)$.

Theorem 2.4.9. *Let $\mathcal{A} = (a, b)_F$. Then the following statements are equivalent:*

1. *$\mathcal{A}$ splits.*
2. *$\mathcal{A}$ is not a division algebra.*
3. *The binary form $\langle a, b\rangle$ represents 1.*
4. *$a \in N_{F(\sqrt{b})/F}(F(\sqrt{b}))$; where N is the norm form of $\mathcal{A}$.*

Proof: For a proof we refer to ([Lam05], page 58).

Corollary 2.4.1. *For any $a \in F^*$, quaternion algebras $(1, a)_F$ and $(a, -a)_F$ are both split algebras.*

Proof: Clearly, binary form $\langle 1, a\rangle$ represents 1 and hence $(1, a)_F$ splits. Since binary form $\langle a, -a\rangle$ is isotropic, therefore $\langle a, -a\rangle \cong \langle 1, -1\rangle$ (using proposition (1.3.1)). Thus $\langle a, -a\rangle$ represents 1 and hence $(a, -a)_F$ splits.

Proposition 2.4.1. ***(Classification of Binary Forms)*** *Let $q = \langle a, b\rangle$ and $q' = \langle a', b'\rangle$. Then $q \cong q'$ if and only if* $\det(\mathrm{q}) = \det(\mathrm{q}')$ *and $(a, b)_F \cong (a', b')_F$.*

Proof: "Only if" part: Assume that $q \cong q'$; i.e., $\langle a, b\rangle \cong \langle a', b'\rangle$. Then $\det(\mathrm{q}) = \det(\mathrm{q}')$. This implies that $ab = a'b'.F^{*2}$.Therefore, it follows that

$$\langle 1, -a, -b, ab\rangle \cong \langle 1, -a', -b', a'b'\rangle.$$

Hence $(a, b)_F \cong (a', b')_F$ (by theorem (2.4.7)).
"If" part: If $(a, b)_F \cong (a', b')_F$, then $\langle 1, -a, -b, ab\rangle \cong \langle 1, -a', -b', a'b'\rangle$ (using theorem (2.4.7)). Further, $\det(\mathrm{q}) = \det(\mathrm{q}')$ implies that $ab = a'b'F^{*2}$. Then by Witt's Cancellation theorem we have $\langle a, b\rangle \cong \langle a', b'\rangle$; i.e., $q \cong q'$.

Theorem 2.4.10. *Let $a, b, c \in F^*$. Then,*

$$(a, b)_F \otimes (a, c)_F \cong (a, bc)_F \otimes \mathbb{M}_2(F).$$

Proof: For a proof we refer to ([Lam05], page 60).

2.5 Clifford Algebra

Let (V, q) be a quadratic space. Then *tensor algebra* of V (denoted by $T(V)$) is defined as

$$T(V) = \oplus_{r=0}^{\infty} T^r(V)$$

where $T^r(V)$ denotes the r-fold tensor product. Now, we can define multiplication on $T(V)$ as follows:

$$(x_1 \otimes x_2 \otimes ... \otimes x_i).(y_1 \otimes y_2 \otimes ... \otimes y_j) = (x_1 \otimes x_2 \otimes ... \otimes x_i \otimes y_1 \otimes y_2 \otimes ... \otimes y_j) \in T^{i+j}(V)$$

Thus, we have a $\mathbb{Z}$-gradation on $T(V)$ because if $x \in T^i(V)$ and $y \in T^j(V)$, then $x.y \in T^{i+j}(V)$.We can write, $T(V)$ as

$$T(V) = T_{even}(V) \oplus T_{odd}(V)$$

where $T_{even}(V) = T^{2r}(V)$ and $T_{odd}(V) = T^{2r-1}(V)$; $r \geq 0$. Observe that, the subspace $T_{even}(V)$ is a subalgebra of $T(V)$.

Definition 2.5.1 Let (V, q) be a quadratic space, $T(V)$ be the tensor algebra of V and $I(q)$ be the two sided ideal of $T(V)$ generated by the elements $v \otimes v - q(v).1$ for all $v \in V$. Then *Clifford algebra* of q (denoted by $C(V, q)$) is defined as the quotient algebra of $T(V)$ by $I(q)$; i.e., $C(V, q) = \frac{T(V)}{I(q)}$.

Let (V, q) be a quadratic space. Then Clifford algebra $C(V, q)$ satisfies the following *universal property*
Let $\mathcal{A}$ be an F-algebra containing V such that $v^2 = q(v).1$ for all $v \in V$. Then there exists a unique F-algebra homomorphism $\varphi : C(V, q) \to \mathcal{A}$ such that $\varphi(v) = v$; for all $v \in V$.

Let $\varphi : T(V) \to C(V, q)$ be the canonical epimorphism. Then $C(V, q)$ has a $\mathbb{Z}/2\mathbb{Z}$-graded structure because $ker(\varphi)$ lies in the subalgebra $T_{even}(V)$; i.e., we can write

$$C(V, q) = C_0(V, q) \oplus C_1(V, q)$$

where $C_0(V, q)$ denotes the image of $T_{even}(V)$ under φ and $C_1(V, q)$ denotes the image of $T_{odd}(V)$ under φ. It is easy to check that $C_0(V, q)$ is an F-subalgebra of $C(V, q)$ and we call it the *even Clifford algebra* .

Proposition 2.5.1. *Let (V, q) be an n-dimensional quadratic space and $C(V, q)$ be the Clifford algebra of q. If n is even, then $C(V, q)$ is a central simple algebra over F and if n is odd, then $C_0(V, q)$ is a central simple algebra over F.*

Proof: For a proof we refer to ([La73], page 111).

2.6 Some more Invariants

Definition 2.6.1 Let (V, q) be a quadratic space. Then the *Witt invariant* of q (denoted by $c(q)$) is defined as:

$$c(q) = \begin{cases} C_0(V,q) \in \mathrm{Br(F)} & \text{if dim(V) is odd} \\ C_1(V,q) \in \mathrm{Br(F)} & \text{if dim(V) is even} \end{cases}$$

Definition 2.6.2 Let (V, q) be a quadratic space and $\langle a_1, ..., a_n \rangle$ is a diagonalisation of q. Then *Hasse invariant* of q (denoted by $s(q)$) is defined to be the class of $\underset{i<j}{\otimes}(a_i, a_j)_F$ in Br(F). (If $n = 1$, then we take $s(q)$ to be 1.)

Proposition 2.6.1. *The Hasse invariant is well defined; i.e., if $q \cong q'$ then $s(q) = s(q')$.*

Proof: Since we know that diagonalisation of isometric quadratic spaces are chain equivalent, therefore it suffices to check the result for $q \cong \langle a, b, a_3, ..., a_n \rangle$ and $q' \cong \langle c, d, a_3, ..., a_n \rangle$.
Now

$$s(q) = (a,b)_F \underset{i\geq 3}{\otimes} (a, a_i)_F \underset{3\leq i<j\leq n}{\otimes} (a_i, a_j)_F \underset{i\geq 3}{\otimes} (b, a_i)_F$$

and

$$s(q') = (c,d)_F \underset{i\geq 3}{\otimes} (c, a_i)_F \underset{3\leq i<j\leq n}{\otimes} (a_i, a_j)_F \underset{i\geq 3}{\otimes} (d, a_i)_F.$$

Using theorem (2.4.10), we have

$$s(q) = (a,b)_F \otimes (ab, a_1a_2...a_n)_F \underset{3\leq i<j\leq n}{\otimes} (a_i, a_j)_F \text{ in Br(F)}$$

and

$$s(q') = (c,d)_F \otimes (cd, a_1a_2...a_n)_F \underset{3\leq i<j\leq n}{\otimes} (a_i, a_j)_F \text{ in Br(F)}.$$

Since $q \cong q'$, therefore $s(q) = s(q')$.

Observation 2.6.3 It can be easily verified that $s(q \perp q') = s(q)s(q')(\mathrm{det(q)}, \mathrm{det(q')})_\mathrm{F}$.

Proposition 2.6.2. *Let (V, q) be an n-dimensional quadratic space. Then*

$$c(q) = s(q).((-1, \mathrm{det(q)})_\mathrm{F})^\epsilon.((-1,-1)_\mathrm{F})^\delta$$

where $\epsilon = (n-1)(n-2)/2$ and $\delta = (n-2)(n-1)n(n+1)/24$.

Proof: For a proof we refer to ([Lam05], page 116).

Theorem 2.6.4. *Let (V, q) and (V, q') be two quadratic spaces such that* $\dim(\mathrm{q}) = \dim(\mathrm{q}') = \mathrm{n} \leq 3$. *Then the following statements are equivalent:*

1. $q \cong q'$.
2. $\det(\mathrm{q}) = \det(\mathrm{q}')$ *and* $c(q) = c(q')$.
3. $\det(\mathrm{q}) = \det(\mathrm{q}')$ *and* $s(q) = s(q')$.

Proof: We split up the proof in three different cases.
Case 1: $n = 1$
There is nothing to prove.
Case 2: $n = 2$
(1) $\Rightarrow$ (2) is trivial.
(2) $\Rightarrow$ (3) From proposition (2.6.2), we have $c(q) = s(q)$ and $c(q') = s(q')$ and we are through.
(3) $\Rightarrow$ (1) This part of the proof we have already done in proposition (2.4.1).
Case 3: $n = 3$
(1) $\Rightarrow$ (2) is trivial.
(2) $\Rightarrow$ (3) From proposition (2.6.2), we have
$c(q) = s(q).(-1, -\det(\mathrm{q}))_{\mathrm{F}}$ and $c(q') = s(q').(-1, -\det(\mathrm{q}'))_{\mathrm{F}}$.
Since $\det(\mathrm{q}) = \det(\mathrm{q}')$ and $c(q) = c(q')$, therefore $s(q) = s(q')$.
(3) $\Rightarrow$ (1) Let $\det(\mathrm{q}) = \det(\mathrm{q}') = \mathrm{d}$. Observe that $\det(\langle -\mathrm{d}\rangle \otimes \mathrm{q}) = -1$. Then by elementary computation, we have

$$s(\langle -d\rangle \otimes q) = s(q) \otimes (-1, -d)_F \text{ and } s(\langle -d\rangle \otimes q') = s(q') \otimes (-1, -d)_F.$$

Now we can replace q and q' by $\langle -d\rangle \otimes q$ and $\langle -d\rangle \otimes q'$ respectively, if required. We can assume that $\det(\mathrm{q}) = \det(\mathrm{q}') = -1$. We can write

$$q = \langle x, y, -xy\rangle, \quad q' = \langle x', y', -x'y'\rangle.$$

Now $s(q) = (x, y)_F$ and $s(q') = (x', y')_F$. Since $s(q) = s(q')$, therefore by theorem (2.4.7), we have

$$\langle 1, -x, -y, xy\rangle \cong \langle 1, -x', -y', x'y'\rangle.$$

By Witt's cancellation theorem (1.3.8), (on cancelling 1) we get $q \cong q'$.

Proposition 2.6.3. *Suppose that every* 5*-dimensional form is isotropic. Then two quadratic forms q and q' are isometric if and only if* $\dim(\mathrm{q}) = \dim(\mathrm{q}')$, $\det(\mathrm{q}) = \det(\mathrm{q}')$ *and* $s(q) = s(q')$.

Proof: "If" part: If $\dim(q) = \dim(q') = n \leq 3$, the result has been already proved in theorem (2.6.4). Now, we have to prove the result for $\dim(q) = \dim(q') = n \geq 4$. Since every 5-dimensional form is isotropic, therefore the quadratic forms q and q' represents 1 (using proposition (2.1.1)); i.e.,

$$q \cong \langle 1 \rangle \perp \varphi \text{ and } q' \cong \langle 1 \rangle \perp \varphi'.$$

Apparently, $\dim(\varphi) = \dim(\varphi') = n - 1$, $\det(\varphi) = \det(\varphi')$ and $s(\varphi) = s(\varphi')$. By induction hypothesis, we have $\varphi \cong \varphi'$ and hence $q \cong q'$. "Only if" part: There is nothing to prove.

2.7 Hasse Minkowski Theorem

Definition 2.7.1 Let F be any field. Then a *discrete valuation* ν on F is defined as a map $\nu : F^* \to \mathbb{Z}$ such that

1. ν is surjective.
2. $\nu(xy) = \nu(x) + \nu(y)$.
3. $\nu(x + y) \geq min\{\nu(x), \nu(y)\}$

Convention: $\nu(0) = \infty$.

Definition 2.7.2 The *discrete valuation ring* of F (denoted by A) w.r.t. ν is defined as

$$A = \{x \in F^* | \nu(x) \geq 0\}.$$

Observation 2.7.3 The discrete valuation ring A has the unique maximal ideal
$\mathfrak{p} = \{x \in F^* | \nu(x) \geq 1\}$. The ideal $\mathfrak{p}$ is generated by an element $\pi \in A$ such that $\nu(\pi) = 1$. We call π as a *uniformising element* and this π is unique upto units of A.

Definition 2.7.4 Let A be the discrete valuation ring of F w.r.t. ν. Then $A/\mathfrak{p}$ is called the *residue class field* of F.

Definition 2.7.5 Let $0 < \lambda < 1$ be any real number and $x \in F$. Then *non-archimedian* value of x (denoted by $|x|_\nu$) is defined as $|x|_\nu = \lambda^{\nu(x)}$.

Now we can define a metric d on F as $d(x-y) = |x-y|_\nu$. If we choose another value of $0 < \lambda < 1$, then it gives an equivalent metric on F. Completion of the metric space (F, d) is denoted by F_ν.

Now, let us define addition and multiplication operation on F_ν as follows: Let $\{x\}, \{y\} \in F_\nu$, then there exist sequences $\{x_n\}_{n\in\mathbb{N}}$ and $\{y_n\}_{n\in\mathbb{N}}$; $x_n, y_n \in F$ such that $\lim_{n\to\infty} x_n = \{x\}$ and $\lim_{n\to\infty} y_n = \{y\}$. Then

$$\{x\} + \{y\} = \lim_{n\to\infty}(x_n + y_n),$$

$$\{x\}.\{y\} = \lim_{n\to\infty}(x_n.y_n).$$

F_ν is a field with the above defined binary operations.
From now onwards F_ν will denote the completion of F w.r.t. $|\ |_\nu$ with the above defined structure of field.

Definition 2.7.6 A map $|\ | : F \to \mathbb{R}$ is said to be *archimedian* if it satisfies the following properties:

1. $|x| \geq 0$ for all $x \in F$ and $|x| = 0$ iff $x = 0$.
2. $|xy| = |x||y|$ for all $x, y \in F$.
3. $|x + y| \leq |x| + |y|$ for all $x, y \in F$.

Definition 2.7.7 Let $|\ |_1$ and $|\ |_2$ be two absolute values. If $\exists$ a real number α such that $|x|_1 = |x|_2^\alpha$ for all $x \in F$, then we say that $|\ |_1$ and $|\ |_2$ are *equivalent* .

It can be easily seen that the notion defined above is an equivalence relation. The set of equivalence classes is denoted by Ω. Elements of Ω are called *places* . Those elements of Ω which correspond to a non-archimedian absolute value are called *finite places* and those which correspond to an archimedian absolute value are called *infinite places* .

Definition 2.7.8 *Local field* is defined as the completion of a number field (finite field extension of $\mathbb{Q}$) w.r.t. a non-archimedian absolute value. It is also known as *p-adic field*.

Let F be a number field and R be its ring of integers. Then every finite place over F uniquely correspond to prime ideal of R. In particular, every

finite place over $\mathbb{Q}$ correspond to prime integer.
Let $p \in \mathbb{Z}$ be a prime number. Then we have a p-adic valuation on $\mathbb{Q}$ which is given as follows:

$$x \mapsto \begin{cases} p^{-\mathrm{ord_p(x)}} & ; x \neq 0 \\ 0 & ; x = 0 \end{cases}$$

where

$$\mathrm{ord_p(x)} = \begin{cases} m & \text{if } x \in \mathbb{Z} \text{ and } x = p^m n; p \nmid n \\ \mathrm{ord_p(a)} - \mathrm{ord_p(b)} & \text{if } \mathrm{x = a/b, a, b} \in \mathbb{Z}, \mathrm{b} \neq 0 \end{cases}$$

is the p-adic order of x.

Definition 2.7.9 Let F be a local field or complete archimedian field with valuation ν and $a, b \in F^*$. Then the *Hilbert symbol* (denoted by $(a, b)_\nu$) is defined as:

$$(a, b)_\nu = \begin{cases} 1 & \text{if } ax^2 + by^2 = 1 \text{ is solvable in } F \\ -1 & \text{otherwise .} \end{cases}$$

We can simply denote the Hilbert symbol by (a, b).

Example 2.7.10

1. Let $F = \mathbb{C}$. Then $(a, b) = 1$ for all $a, b \in \mathbb{C}^*$.
2. Let $F = \mathbb{R}$. Then $(a, b) = \begin{cases} 1 & \text{if either } a \text{ or } b > 0 \\ -1 & \text{otherwise} \end{cases}$.

Theorem 2.7.11. ***(Hilbert's Reciprocity Law)*** *Let $\mathbb{Q}_p$ be a p-adic field and $a, b \in \mathbb{Q}^*$. Then $(a, b)_p = 1$ for almost all p, and $\prod_p (a, b)_p = 1$.*

Proof: For a proof we refer to ([Ger08], page 98).

Theorem 2.7.12. ***(Hensel's Lemma)*** *Let ν be a complete discrete valuation on F.Let A be the associated valuation ring. For a polynomial $f(x) \in A[x]$, suppose there is an element $\alpha \in A$ such that*

$$|f(\alpha)|_\nu < |f'(\alpha)|_\nu^2.$$

Then there exists an element $\beta \in F$ such that $f(\beta) = 0$.

Proof: For a proof we refer to ([Ger08], page 69).

Theorem 2.7.13. ***(Local Square Theorem)*** *Let ν be a complete discrete valuation on F. Then every element of the form $1+4\pi\alpha$, with π prime and $|\alpha|_\nu \leq 1$, is a square in F.*

Proof: Let $\lambda = 1+4\pi\alpha$, with $\alpha \in A$ and π is prime in A. Consider $f(x) = \pi x^2 + x - \alpha \in A[x]$. Using Hensel's lemma (2.7.12), f has a root $\beta \in F$ and β is of the form $\frac{-1\pm\sqrt{1+\lambda}}{2\pi}$. Therefore, $\sqrt{1+\lambda} \in F$; i.e., $1+4\pi\alpha$ is a square in F.

Theorem 2.7.14. ***(Weak Approximation Theorem)*** *Let T be a set which contains finitely many primes, possibly including ∞. Let $\alpha_p \in \mathbb{Q}_p$ for each $p \in T$. Then for a given real number $\epsilon \geq 0$, there exists $\alpha \in \mathbb{Q}$ such that $|\alpha - \alpha_p|_p < \epsilon$ for all $p \in T$.*

Proof: Let $T = \{p_1, p_2, ..., p_t\}$. We can assume that $t \geq 2$, because $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ for each p.
Claim: There exists an element $\beta \in \mathbb{Q}$ such that $|\beta|_{p_1} \geq 1$ and $|\beta|_{p_i} \leq 1$; for $2 \leq i \leq t$.
If $\infty \notin T$, then $\beta = \dfrac{p_2...p_t}{p_1}$ will do the job.
If $\infty \in T$ and $\infty = p_1$, then choose $\beta = p_2...p_t$.
Lastly, if $\infty \in T - p_1$ and say, $\infty = p_2$, then put $\beta = \dfrac{p_3...p_t}{Kp_1}$, where K is any integer relatively prime to $p_3...p_t$ with $K \geq \dfrac{p_3...p_t}{p_1}$.

By previous claim, we have for each $j \in \{1, ..., t\}$, there exists an element $\beta_j \in \mathbb{Q}$ such that $|\beta_j|_{p_j} \geq 1$ and $|\beta_j|_{p_i} \leq 1$; for $i \neq j$. Then

$$\lim_{n\to\infty} \frac{\beta_j^n}{1+\beta_j^n} = \begin{cases} 1 & \text{w.r.t. } |\ |_{p_j}, \\ 0 & \text{w.r.t. } |\ |_{p_i}, \text{ for } i \neq j. \end{cases}$$

Define

$$c_n = \sum_{j=1}^{t} \frac{\alpha_j \beta_j^n}{1+\beta_j^n}.$$

Thus, we get $\lim\limits_{n\to\infty} c_n = \alpha_j$ w.r.t. $|\ |_{p_j}$; for $1 \leq j \leq t$. For sufficiently large value of n, the job will be done by $\alpha = c_n$.

Theorem 2.7.15. ***(Strong Approximation Theorem)*** *Let T be a set which contains finitely many primes not including ∞. Let $z_p \in \mathbb{Z}_p$ for each $p \in T$. Then for a given real number $\epsilon \geq 0$, there exists $z \in \mathbb{Z}$ such that $|z - z_p|_p < \epsilon$ for all $p \in T$.*

Proof: Since for each $p \in T$, $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, therefore, $\exists z'_p \in \mathbb{Z}$ such that $|z'_p - z_p|_p < \frac{\epsilon}{2}$. Now choose $\nu \in \mathbb{N}$ sufficiently large so that $\frac{1}{p^\nu} < \frac{\epsilon}{2}$ for all $p \in T$. Now using the Chinese Remainder Theorem, there exists $z \in \mathbb{Z}$ such that $z \equiv z'_p(\mathrm{mod} p^\nu)$ for all $p \in T$. Thus we have $|z - z'_p|_p < \frac{\epsilon}{2}$ for all $p \in T$. Therefore,

$$\begin{aligned} |z - z_p|_p &= |z - z'_p + z'_p - z_p|_p \\ &\leq |z - z'_p|_p + |z'_p - z_p|_p \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} \\ &= \epsilon \end{aligned}$$

for all $p \in T$.

Lemma 2.7.1. *Let T be a set which contains finitely many primes, possibly including ∞. Let $t_p \in \mathbb{Q}_p$ for each $p \in T$. Then there exists $t \in \mathbb{Q}$ such that*

1. *$t \in t_p \mathbb{Q}_p^{*2}$ for each $p \in T$;*
2. *$|t|_p = 1$ for all other finite primes, but for at most one exceptional prime p_0.*

Proof: Let $\nu_p = \mathrm{ord_p t_p}$ for each finite prime $p \in T$. Now define,

$$\beta = \pm \prod_{p \in T - \infty} p^{\nu_p} \in \mathbb{Q},$$

where sign of β is same as the sign of t_∞ if $\infty \in T$, otherwise we can choose sign of β arbitrarily. Therefore,

$$|\beta|_p = \begin{cases} |t_p|_p & \text{for all finite } p \in T, \\ 1 & \text{for all finite } p \notin T. \end{cases}$$

Thus, we have $\beta = \epsilon_p t_p$ for some $\epsilon_p \in \mathbb{Z}_p^*$; for all $p \in T - \infty$. Now using the Strong Approximation Theorem (2.7.15), $\exists z \in \mathbb{Z}$ such that $z \equiv \epsilon_p(\mathrm{mod 8p})$ for all $p \in T - \infty$.

$$\begin{aligned} &\Rightarrow z\epsilon_p^{-1} \equiv 1(\mathrm{mod 8p}) \\ &\Rightarrow z\epsilon_p^{-1} = 1 + 8p\alpha \end{aligned}$$

where $\alpha \in \mathbb{Z}_p^*$ (and hence $|2\alpha|_p \leq 1$). By Local Square Theorem (2.7.13), $z \in \epsilon_p \mathbb{Q}_p^{*2}$ for all $p \in T - \infty$.
Since z and $8\prod_{p \in T - \infty} p$ are relatively prime integers, therefore we can use Dirichlet's theorem on primes in an arithmetic progression, according to which there exists a prime number p_0 which satisfies $p_0 \equiv z(\mathrm{mod} 8 \prod_{\mathrm{p} \in \mathrm{T} - \infty} \mathrm{p})$. Since p_0 is a unit w.r.t. $|\ |_{\prod_{p \in T - \infty} p}$, therefore, by again use of Local Square Theorem (2.7.13), we get $p_0 \in z\mathbb{Q}_p^{*2}$ for all $p \in T - \infty$. Thus our job will be done by $t = p_0 \beta$.

Lemma 2.7.2. *Let F be a p-adic field whose residue class field has characteristic $\neq 2$. Let $U = A - \mathfrak{p}$; where $\mathfrak{p}$ is the unique maximal ideal of the discrete valuation ring A. If $a, b, c \in U$, then the quadratic form $\langle a, b, c\rangle$ is isotropic.*

Proof: By Hensel's lemma (2.7.12), we know that a diagonal quadratic form $\langle a_1, a_2, ..., a_r\rangle$; $a_i \in U$, is isotropic if and only if the quadratic form $\langle \overline{a_1}, \overline{a_2}, ..., \overline{a_r}\rangle$ is isotropic over the residue class field $A/\mathfrak{p}$ of characteristic $\neq 2$. Here $\overline{a_i}$ denotes the image of a_i in $A/\mathfrak{p}$.

Since for a p-adic field, the residue class field is finite and every 3-dimensional form over a finite field is isotropic. Hence the result follows.

Theorem 2.7.16. *For any finite prime integer p, every five dimensional quadratic form f over $\mathbb{Q}_p$ is isotropic. Two quadratic forms q and q' over $\mathbb{Q}_p$ are isometric if and only if* $\dim(\mathrm{q}) = \dim(\mathrm{q}')$, $\det(\mathrm{q}) = \det(\mathrm{q}')$ *and $s(q) = s(q')$.*

Proof: We can write, $f = f_1 \perp pf_2$; where either $\dim(\mathrm{f_1}) \geq 3$ or $\dim(\mathrm{f_2}) \geq 3$ with the property that, after diagonalisation, all the diagonal elements of f_1 and f_2 are units in $\mathbb{Q}_p$. Using lemma (2.7.2), we get that either f_1 or f_2 is isotropic and therefore so is f. The last statement of the theorem immediately follows from proposition (2.6.3).

Theorem 2.7.17. ***(Hasse Minkowski Theorem)*** *Let q be a regular quadratic form over the field of rational numbers. Then q is isotropic over $\mathbb{Q}$ if and only if q is isotropic over $\mathbb{Q}_p$ for all prime integers p, including ∞.*

Proof: "Only if" part: If q is isotropic over $\mathbb{Q}$ then it is isotropic over all the field extensions of $\mathbb{Q}$. In particular, q is isotropic over $\mathbb{Q}_p$ for all p.
"If" part: We will prove this part using induction on $\dim(\mathrm{q}) = \mathrm{n}$.
Case 1: $n = 1$
This case does not make any sense because 1-dimensional quadratic form can be either regular or isotropic but not both.
Case 2: $n = 2$
Scaling q by an element that it represents, we may assume that $q = \langle 1, \alpha\rangle$; where $\alpha \in \mathbb{Q}_p^*$. Since q is isotropic over $\mathbb{Q}_p$, therefore $\alpha \in -\mathbb{Q}_p^{*2}$ for all p. Thus we have $\alpha < 0$ and $\mathrm{ord_p}\alpha \equiv 0(\mathrm{mod}2)$ for all $p \neq \infty$. Hence $\alpha \in -\mathbb{Q}^{*2}$ and therefore q is isotropic over $\mathbb{Q}$.
Case 3: $n = 3$
Without loss of generality, we can assume that $q \cong \langle 1, -a, -b\rangle$ where a, b are square free integers and $|a| \leq |b|$. We will solve this case by using induction on $m = |a| + |b|$.
For $m = 2$, we get $q \cong \langle 1, \pm 1, \pm 1\rangle$. Since q is isotropic over $\mathbb{Q}_\infty$, therefore

$q \not\equiv \langle 1,1,1\rangle$. Hence the result holds.
Now we can assume that $m \geq 3$ and that the result is true for $\langle 1,-c,-d\rangle$ with $|c|+|d| < m$. Consider $q \cong \langle 1,-a,-b\rangle$ with $|a| \leq |b|$ and $|b| \geq 2$. Suppose $b = \pm p_1...p_k$ where all the p_i's are distinct primes.
Claim: For each $p \in \{p_1,...,p_k\}$, $a \equiv s^2(\text{modp})$ is solvable for some integer s.
If p divides a, then $s = 0$ is the desired integer.
If p does not divide a, then $a \in \mathbb{Z}_p^*$. Since q is isotropic over $\mathbb{Q}_p$ for all p, therefore there exists a primitive element $(x,y,z) \in \mathbb{Z}_p^3$ such that $x^2 - ay^2 - bz^2 = 0$. We are given that p divides b and so p divides $x^2 - ay^2$. If p divides y then it will contradict the fact that (x,y,z) is a primitive element. Thus we have $y \in \mathbb{Z}_p^*$ and so $ay^2 \equiv x^2(\text{modp})$, which further implies $a \equiv (y^{-1}x)^2(\text{modp})$. Since $T' = \{0,1,...,p-1\}$ is a complete set of representatives for the residue class field $\mathbb{Z}_p/p\mathbb{Z}_p$. Therefore we can choose $s \in T'$ such that $s \equiv y^{-1}x(\text{modp})$ which will give $a \equiv s^2(\text{modp})$, establishing the claim.

Using Chinese Remainder Theorem for rings, we have

$$\frac{\mathbb{Z}}{b\mathbb{Z}} \simeq \prod_{i=1}^{k} \frac{\mathbb{Z}}{p_i\mathbb{Z}}$$

By previous claim, we have that $a \equiv t^2(\text{modb})$ is solvable for some integer t. Therefore, we can write $a + bb' = t^2$ with $t, b' \in \mathbb{Z}$ and $|t| \leq |b/2|$.

$$\Rightarrow b' = b.\Big(\frac{1}{b^2}(t^2-a)\Big) \Rightarrow b' = bN\Big(\frac{t+\sqrt{a}}{b}\Big);$$

where $N : \mathbb{Q}(\sqrt{a}) \to \mathbb{Q}$ is the norm mapping. Since every square is a norm, therefore b' is a norm if and only if so is b. By theorem (2.4.9), we know that a quadratic form $\langle 1,-a,-b\rangle$ is isotropic over F if and only if $b \in N_{F(\sqrt{a})/F}(F(\sqrt{a}))^*$. Now combining the above two statements, we have $q \cong \langle 1,-a,-b\rangle$ is isotropic over F if and only if so is $q' \cong \langle 1,-a,-b'\rangle$. Also,

$$|b'| = \Big|\frac{t^2-a}{b}\Big| \leq \Big|\frac{t^2}{b}\Big| + \Big|\frac{a}{b}\Big| \leq \frac{|b|}{4} + 1 < |b|.$$

From the hypothesis, we have q is isotropic over $\mathbb{Q}_p$ for all prime integers p, which implies that q' is isotropic over $\mathbb{Q}_p$ for all prime integers p. Using the induction hypothesis on m, we get q' is isotropic over $\mathbb{Q}$ and hence q is isotropic over $\mathbb{Q}$.
Case 4: $n = 4$
Let $q \cong \langle a_1,a_2,a_3,a_4\rangle$; where all the a_i's are square free integers. Let

$$T = \{\infty\} \cup \{p : p \text{ divides } 2a_1a_2a_3a_4\}$$

Thus for all $p \notin T$, we have $a_1, a_2, a_3, a_4 \in \mathbb{Z}_p^*$ and hence $(a_i, a_j)_p = 1$; $1 \leq i, j \leq 4$.

Since q is isotropic over $\mathbb{Q}_p$, therefore there exists an element $t_p \in \mathbb{Q}_p^*$ such that $\langle a_1, a_2 \rangle$ represents t_p and $\langle a_3, a_4 \rangle$ represents $-t_p$ over $\mathbb{Q}_p$. Using lemma (2.7.1), there exists $t \in \mathbb{Q}$ and a prime p_0 such that the quadratic forms $\langle a_1, a_2, -t \rangle$ and $\langle a_3, a_4, t \rangle$ are isotropic over $\mathbb{Q}_p$ for all $p \in T$. Moreover, $\langle a_1, a_2, -t \rangle$ and $\langle a_3, a_4, t \rangle$ are isotropic over $\mathbb{Q}_p$ for all $p \notin T \cup \{p_0\}$ as $|a_i|_p = |t|_p = 1$ for all such p. Now combining the above two statements, we get that the quadratic forms $\langle a_1, a_2, -t \rangle$ and $\langle a_3, a_4, t \rangle$ are isotropic over $\mathbb{Q}_p$ for all $p \neq p_0$. From Hilbert's Reciprocity Law (2.7.11), it follows that these quadratic forms are isotropic over $\mathbb{Q}_{p_0}$ as well. Therefore these quadratic forms are isotropic over $\mathbb{Q}$ by the case $n = 3$. Hence q is isotropic over $\mathbb{Q}$.
Case 5: $n \geq 5$
Let $q = q_1 \perp q_2$ where $q_1 = \langle a, b \rangle$ and $q_2 = \langle a_1, a_2, ..., a_r \rangle$; $r = \dim(\mathrm{q}_2) \geq 3$ and $a_i \in \mathbb{Q}$. We consider a_i's as elements of $\mathbb{Q}_p$ for all p. We can assume that all a_i's belong to $\mathbb{Z}_p$ (because we can clear their denominators by multiplying with a suitable square in $\mathbb{Q}$).

Let $S = \{p : q_2 \text{ is anisotropic over } \mathbb{Q}_p\}$. S is a finite set because the set of primes at which the quadratic form q_2 is possibly anisotropic contains $p = \infty$, $p = 2$ and those primes $\neq 2$ at which no three a_i's; $1 \leq i \leq r$ are units in the valuation ring of $\mathbb{Q}_p$ (because of lemma (2.7.2)). Since $q = q_1 \perp q_2$ is isotropic for all prime integers p and hence for all $p \in S$. Thus $\exists t_p \in \mathbb{Q}_p^*$ such that q_1 and q_2 represents t_p and $-t_p$ respectively. Therefore, $\exists \beta_{1p}, \beta_{2p} \in \mathbb{Q}_p^*$ such that $a\beta_{1p}^2 + b\beta_{2p}^2 = t_p$. Now using Weak Approximation Theorem (2.7.14) with the Local Square Theorem (2.7.13), we can choose $\beta_1, \beta_2 \in \mathbb{Q}$ sufficiently close to β_{1p}, β_{2p} so that $t = a\beta_1^2 + b\beta_2^2$ belong to the same square class as of t_p in $\mathbb{Q}_p/\mathbb{Q}_p^{*2}$ for all $p \in S$. Now consider the sub-quadratic form $q' = \langle t \rangle \perp q_2$ of q. For $p \in S$, the quadratic form q_2 represents $-t$ by the choice of $\beta_1, \beta_2 \in \mathbb{Q}$. Thus q' is isotropic for $p \in S$. For $p \notin S$, the quadratic form q_2 is isotropic, then so is q'. Thus, q' is isotropic for all prime integers p and $\dim(\mathrm{q}') = \dim(\mathrm{q}) - 1$. Hence, by induction hypothesis we are done.

Corollary 2.7.1. *Let q be quadratic form with $\dim(\mathrm{q}) \geq 5$. Then q is isotropic over $\mathbb{Q}$ if and only if it is isotropic over $\mathbb{R}$.*

Proof: "If" part: Since $\dim(\mathrm{q}) \geq 5$, therefore q is isotropic over $\mathbb{Q}_p$; for all finite primes p not including ∞ (using theorem (2.7.16)). Since it is given that q is isotropic over $\mathbb{R}$, therefore, by Hasse Minkowski theorem (2.7.17), we get that q is isotropic over $\mathbb{Q}$. Converse part is trivial.

Chapter 3

Involution on Central Simple Algebras

Throughout this chapter F denote a field of characteristic $\neq 2$ and F^* will denote the multiplicative group of F.

3.1 Introduction

Definition 3.1.1 Let $\mathcal{A}$ be a central simple simple algebra over a field F. Then involution on $\mathcal{A}$ is a map $\sigma : \mathcal{A} \to \mathcal{A}$ such that

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

for all $x, y \in \mathcal{A}$. We will denote this pair by $(\mathcal{A}, \sigma)$.

Example 3.1.2

1. Let $(\mathcal{A}, \sigma) = (\mathbb{M}_n(F), t)$; where t denote the transpose map on $\mathbb{M}_n(F)$; i.e., the map $t : \mathbb{M}_n(F) \to \mathbb{M}_n(F)$ is given by $A \mapsto A^t$. Then it is easy to check that the map t is an involution on $\mathbb{M}_n(F)$.
2. Let (V, q) be a non singular quadratic space and let M be a symmetric matrix associated with q. Then we can define a map σ_q on $\mathbb{M}_n(F)$ as : $\sigma_q : \mathbb{M}_n(F) \to \mathbb{M}_n(F)$ such that $\sigma_q(A) = (MAM^{-1})^t$. This map satisfies the following properties:

(a) $\sigma_q(A_1 + A_2) = (M(A_1 + A_2)M^{-1})^t$
$= (M(A_1)M^{-1})^t + (M(A_2)M^{-1})^t$
$= \sigma_q(A_1) + \sigma_q(A_2)$.

(b) $\sigma_q(A_1A_2) = (M(A_1A_2)M^{-1})^t$
$= (MA_1M^{-1}MA_2M^{-1})^t$
$= (MA_2M^{-1})^t(MA_1M^{-1})^t$
$= \sigma_q(A_2)\sigma_q(A_1)$.

(c) $\sigma_q^2(A) = \sigma_q((MAM^{-1})^t)$
$= (M(MAM^{-1})^tM^{-1})^t$
$= (MM^{-1}A^tMM^{-1})^t$
$= A$

for all $A, A_1, A_2 \in \mathbb{M}_n(F)$. Hence, σ_q is an involution and it is known as the *adjoint involution* to the quadratic form q.

Observation 3.1.3 Let σ be an involution on a central simple F-algebra $\mathcal{A}$. Then

1. $\sigma(1) = 1$.
2. $\sigma(a^{-1}) = \sigma(a)^{-1}$ for all $a \in \mathcal{A}$.
3. The map σ is not necessarily an F-linear map.
4. The center F is preserved by σ; i.e., $\sigma(F) = F$.

Definition 3.1.4

1. An involution σ is said to be of *first kind* if it is F-linear. Equivalently, $\sigma(\lambda) = \lambda$ for all $\lambda \in F$.
2. If restriction of involution σ to the center F is an automorphism of order 2, then it is said to be an involution of *second kind*.

Definition 3.1.5 Let σ be an involution on a central simple F-algebra $\mathcal{A}$. Then the *fixed field* of σ (denoted by F^σ) is defined as :

$$F^\sigma := \{\lambda \in F | \sigma(\lambda) = \lambda\}.$$

Observation 3.1.6

1. If σ is an involution of first kind, then $F^\sigma = F$.
2. If σ is an involution of second kind, then F is a separable quadratic extension over F^σ.

Theorem 3.1.7. ***(Albert's Theorem)*** *Let $\mathcal{A}$ be a central simple F-algebra. Then $\mathcal{A}$ has an involution of first kind if and only if $\mathcal{A} \otimes \mathcal{A}$ splits.*

Proof: For a proof we refer to ([KMRT98], page 31).

Theorem 3.1.8. *Let $\mathcal{A}$ be a central simple F-algebra and σ is an involution of first kind on $\mathcal{A}$.*

1. *The map $\sigma_a : \mathcal{A} \to \mathcal{A}$ defined by $x \mapsto a\sigma(x)a^{-1}$ is an involution on $\mathcal{A}$; for $a \in \mathcal{A}$ such that $a = \lambda\sigma(a)$; $\lambda \in F^*$ with $\lambda\sigma(\lambda) = 1$.*
2. *If τ is any other involution of first kind on $\mathcal{A}$, then there exists an invertible element $a \in \mathcal{A}$ with $\sigma(a) = \pm a$ such that $\tau = \sigma_a$ where σ_a is same as in (1).*
3. *If σ and τ are two involutions of first kind on $\mathcal{A}$, then one can uniquely determine $a \in \mathcal{A}$ (as in (2)) upto a scalar factor $\mu \in F^*$.*

Proof:

1. To show that σ_a is an involution on $\mathcal{A}$, we have to verify the three conditions as given in definition (3.1.1). For $x, y \in \mathcal{A}$ and $\lambda \in F^*$, we have

   (a) $\begin{aligned}\sigma_a(x+y) &= a\sigma(x+y)a^{-1} \\ &= a(\sigma(x)+\sigma(y))a^{-1} \\ &= a\sigma(x)a^{-1} + a\sigma(y)a^{-1} \\ &= \sigma_a(x) + \sigma_a(y).\end{aligned}$

   (b) $\begin{aligned}\sigma_a(xy) &= a\sigma(xy)a^{-1} \\ &= a(\sigma(y)\sigma(x))a^{-1} \\ &= a\sigma(y)a^{-1}a\sigma(x)a^{-1} \\ &= \sigma_a(y)\sigma_a(x).\end{aligned}$

   (c) $\begin{aligned}\sigma_a^2(x) &= \sigma_a(a\sigma(x)a^{-1}) \\ &= a\sigma(a\sigma(x)a^{-1})a^{-1} \\ &= a\sigma(a^{-1})\sigma^2(x)\sigma(a)a^{-1} \\ &= \lambda x\lambda^{-1} \\ &= x.\end{aligned}$

Thus σ_a is an involution on $\mathcal{A}$.

2. Let τ be any other involution on $\mathcal{A}$. Then $\sigma \circ \tau$ is an automorphism of $\mathcal{A}$ and hence an inner automorphism (by Skolem Noether Theorem (2.3.7)); i.e., there exists an element $a \in \mathcal{A}$ such that $\sigma \circ \tau(x) = axa^{-1}$
$\Rightarrow \tau(x) = \sigma(a)^{-1}\sigma(x)\sigma(a)$
$\Rightarrow \tau^2(x) = \sigma(a)^{-1}\sigma(\tau(x))\sigma(a)$
$\Rightarrow x = \sigma(a)^{-1}axa^{-1}\sigma(a)$
Hence the inner automorphism induced by $\sigma(a)^{-1}a$ is identity, which is possible only if $\sigma(a)^{-1}a \in F^*$; i.e., $\sigma(a)^{-1}a = \lambda$(say). Then $a = \sigma(a)\lambda$
$\Rightarrow \sigma(a) = a\sigma(\lambda)$
$\Rightarrow \sigma(a) = \sigma(a)\lambda\sigma(\lambda)$
$\Rightarrow \lambda\sigma(\lambda) = 1$
Since σ is an involution of first kind, therefore, $\lambda^2 = 1$; i.e., $\lambda = \pm 1$ and hence $\sigma(a) = \pm a$

3. Let σ and τ are as in (2) and $\sigma_a = \tau = \sigma_b$ for $a, b \in F^*$. Then, for all $x \in \mathcal{A}$,
$a^{-1}\sigma(x)a = b^{-1}\sigma(x)b \quad \Rightarrow \sigma(x) = ab^{-1}\sigma(x)ba^{-1}$
$\Rightarrow ab^{-1} \in F^*$
i.e., $ab^{-1} = \mu$ (say) $\Rightarrow a = \mu b$ and we are through.

3.2 Adjoint Algebra

In §3.1, we have defined the adjoint involution to a given quadratic form q. Now, we want to define an equivalent notion on $\mathrm{End_F(V)} = \mathbb{M}_n(\mathrm{F})$.

Definition 3.2.1 Let (V, B) be a non-singular bilinear space. Then $\hat{B} : V \to V^*$ defined by

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

is an isomorphism of vector spaces. We may then define *adjoint involution* on $\mathrm{End_F(V)}$ (denoted by σ_B) as follows:

$$\sigma_B : \mathrm{End_F(V)} \to \mathrm{End_F(V)}$$

$$f \mapsto \hat{B}^{-1} \circ f^t \circ \hat{B}$$

where $f^t \in \mathrm{End_F(V^*)}$ denotes the transpose of f, which is defined by $\varphi \mapsto \varphi \circ f$ for $\varphi \in V^*$.

Observation 3.2.2

1. Equivalently, we can define $\sigma_B(f)$ by the following property:

$$B(x, f(y)) = B(\sigma_B(f)(x), y) \quad \text{for } x, y \in V,$$

because for $x, y \in V$, we have

$$\sigma_B(f) = \hat{B}^{-1} \circ f^t \circ \hat{B}$$

$$\Leftrightarrow \hat{B} \circ \sigma_B(f) = f^t \circ \hat{B}$$

$$\Leftrightarrow B(x, f(y)) = B(\sigma_B(f)(x), y)$$

2. If B is symmetric or skew symmetric, then σ_B is an involution, as it satisfies all the three conditions given in definition (3.1.1). For $f, g \in \mathrm{End_F(V)}$, we have

(a) $$\begin{aligned}\sigma_B(f+g) &= \hat{B}^{-1} \circ (f+g)^t \circ \hat{B} \\ &= \hat{B}^{-1} \circ (f^t + g^t) \circ \hat{B} \\ &= \hat{B}^{-1} \circ f^t \circ \hat{B} + \hat{B}^{-1} \circ g^t \circ \hat{B} \\ &= \sigma_B(f) + \sigma_B(g).\end{aligned}$$

(b) $$\begin{aligned}\sigma_B(f \circ g) &= \hat{B}^{-1} \circ (f \circ g)^t \circ \hat{B} \\ &= \hat{B}^{-1} \circ (g^t \circ f^t) \circ \hat{B} \\ &= \hat{B}^{-1} \circ g^t \circ \hat{B} \circ \hat{B}^{-1} \circ f^t \circ \hat{B} \\ &= \sigma_B(g) \circ \sigma_B(f).\end{aligned}$$

(c) $$\begin{aligned}\sigma_B^2(f) &= \hat{B}^{-1} \circ (\hat{B}^{-1} \circ f^t \circ \hat{B})^t \circ \hat{B} \\ &= \hat{B}^{-1} \circ \hat{B} \circ f \circ \hat{B}^{-1} \circ \hat{B} \\ &= f.\end{aligned}$$

Thus σ_B is an involution on $\mathrm{End_F(V)}$.

Definition 3.2.3 Let σ_B be the adjoint involution on $\mathrm{End_F(V)}$. Then we call $(\mathrm{End_F(V)}, \sigma_B)$ as the *adjoint algebra* .

Theorem 3.2.4. *The map which associates to each non-singular bilinear space (V, B) its adjoint algebra $(\mathrm{End_F(V)}, \sigma_B)$ induces a one-to-one correspondence between equivalence classes of non-singular bilinear forms on V modulo multiplication by a factor in F^* and involutions of $\mathrm{End_F(V)}$. In particular, involutions of first kind correspond to non-singular bilinear forms which are either symmetric or skew-symmetric.*

Proof: Firstly, we want to show that the map is well defined. From the equivalent definition of adjoint involution as given in observation (3.2.2)(1), we have

$$B(x, f(y)) = B(\sigma_B(f)(x), y);$$

where $f \in \mathrm{End_F(V)}$ and $x, y \in V$.
For $\alpha \in F^*$, we have

$$\alpha B(x, f(y)) = \alpha B(\sigma_{\alpha B}(f)(x), y)$$

$$\Rightarrow B(x, f(y)) = B(\sigma_{\alpha B}(f)(x), y);$$

i.e., $\sigma_B = \sigma_{\alpha B}$. Thus the map $B \mapsto \sigma_B$ from non-singular bilinear forms on V to the set of involutions on $\mathrm{End_F(V)}$ is well defined upto a scalar factor.

Now, we will show that this map is one-one. If B and B' are two non-singular bilinear forms on V such that $\sigma_B = \sigma_{B'}$, then

$$\hat{B}^{-1} \circ f^t \circ \hat{B} = {\hat{B'}}^{-1} \circ f^t \circ \hat{B'}$$

$$\Rightarrow \hat{B'} \circ \hat{B}^{-1} \circ f^t \circ \hat{B} \circ {\hat{B'}}^{-1} = f^t;$$

where $f \in \mathrm{End_F(V)}$ is arbitrary. Therefore, we get $\hat{B'} \circ \hat{B}^{-1} = \beta \in F^*$. Thus, B and B' are scalar multiples of each other.

If B is a fixed non-singular bilinear form on V with adjoint involution σ_B, then for any involution σ of $\mathrm{End_F(V)}$, the composition $\sigma_B \circ \sigma^{-1}$ is an F-linear automorphism of $\mathrm{End_F(V)}$. By Skolem Noether theorem (2.3.7), this automorphism is an inner automorphism; i.e., there exist an invertible element $u \in \mathrm{End_F(V)}$ such that $\sigma_B \circ \sigma^{-1} = \mathrm{Int(u)}$. Thus we have,

$$\mathrm{Int(u^{-1})} \circ \sigma_{\mathrm{B}} = \sigma$$

$$\Rightarrow u^{-1}\sigma_B(f)u = \sigma(f)$$

$$\Rightarrow \sigma_B(f)u = u\sigma(f).$$

Hence σ is the adjoint involution w.r.t. the bilinear form B' defined by

$$B'(x, y) = B(u(x), y).$$

Thus we have proved the first part of the theorem.
Let B be a non-singular bilinear form on V with adjoint involution σ_B. Then the bilinear form B' defined by

$$B'(x, y) = B(y, x) \quad \text{for } x, y \in V$$

has adjoint involution $\sigma_{B'} = \sigma_B^{-1}$. Therefore, σ_B^2 is identity if and only if $\sigma_B' = \sigma_B$; i.e., $B' = \epsilon B$ where $\epsilon^2 = 1$ and this is true if and only if B is symmetric or skew-symmetric.

Let $\mathcal{A}$ be a central simple F-algebra with $\deg(\mathcal{A}) = \mathrm{n}$ and K be an algebraic closure of F. If we extend the scalars to K, then $\mathcal{A} \cong \mathbb{M}_n(K)$. We can view every element $a \in \mathcal{A}$ as a matrix in $\mathbb{M}_n(K)$. Characteristic polynomial of that matrix has coefficients in F and it is called the *reduced characteristic polynomial* of $\mathcal{A}$ which is denoted by

$$\mathrm{Prd}_{\mathcal{A},\mathrm{a}}(\mathrm{X}) = \mathrm{X}^{\mathrm{n}} - \mathrm{s}_1(\mathrm{a})\mathrm{X}^{\mathrm{n}-1} + ... + (-1)^{\mathrm{n}}\mathrm{s}_{\mathrm{n}}(\mathrm{a}).$$

Now, define $\mathrm{Trd}_{\mathcal{A}}(\mathrm{a}) = \mathrm{s}_1(\mathrm{a})$ and $\mathrm{Nrd}_{\mathcal{A}}(\mathrm{a}) = \mathrm{s}_{\mathrm{n}}(\mathrm{a})$. We call $\mathrm{Trd}_{\mathcal{A}}(\mathrm{a})$ and $\mathrm{Nrd}_{\mathcal{A}}(\mathrm{a})$ as *reduced trace* and *reduced norm* of a respectively.

Types of Involutions

Notation: Let σ be an involution of first kind on a central simple F-algebra $\mathcal{A}$. Then

1. $\mathrm{Sym}(\mathcal{A}, \sigma) = \{\mathrm{a} \in \mathcal{A} | \sigma(\mathrm{a}) = \mathrm{a}\}$ denotes the set of symmetric elements in $\mathcal{A}$.

2. $\mathrm{Skew}(\mathcal{A}, \sigma) = \{\mathrm{a} \in \mathcal{A} | \sigma(\mathrm{a}) = -\mathrm{a}\}$ denotes the set of skew-symmetric elements in $\mathcal{A}$.

3. $\mathrm{Symd}(\mathcal{A}, \sigma) = \{\mathrm{a} + \sigma(\mathrm{a}) | \mathrm{a} \in \mathcal{A}\}$ denotes the set of symmetrized elements in $\mathcal{A}$.

4. $\mathrm{Alt}(\mathcal{A}, \sigma) = \{\mathrm{a} - \sigma(\mathrm{a}) | \mathrm{a} \in \mathcal{A}\}$ denotes the set of alternating elements in $\mathcal{A}$.

Observation 3.2.5 Since $\mathrm{char(F)} \neq 2$, therefore $\mathrm{Sym}(\mathcal{A}, \sigma) = \mathrm{Symd}(\mathcal{A}, \sigma)$ and $\mathrm{Skew}(\mathcal{A}, \sigma) = \mathrm{Alt}(\mathcal{A}, \sigma)$. Moreover, $\mathcal{A} = \mathrm{Sym}(\mathcal{A}, \sigma) \oplus \mathrm{Skew}(\mathcal{A}, \sigma)$.

If σ is an involution of first kind on a central simple F-algebra $\mathcal{A}$ and L is any field which contains F, then we can extend σ to an involution of first kind $\sigma_L = \sigma \otimes Id_L$ on $A_L = A \otimes_F L$. In particular, if L is a splitting field of F, then $A_L = \mathrm{End_L(V)}$; where V is an n-dimensional vector space over L and $n = \deg(\mathcal{A})$.

As we have observed in theorem (3.2.4), the involution σ_L is the adjoint involution σ_B w.r.t. some non-singular symmetric or skew-symmetric bilinear

form b on V. We know that $\mathrm{End(V)_L} \cong \mathbb{M}_{\mathrm{n}}(\mathrm{L})$. Let M denotes the associated matrix with B w.r.t. a fixed basis of V. Then

$$B(x, y) = x^t.M.y;$$

where x and y are considered as column vectors and $M^t = M$ if B is symmetric, $M^t = -M$ if B is skew-symmetric. Thus, the involution σ_L can be identified with the involution σ_M, which is defined as:

$$\sigma_M(A) = M^{-1}.A^t.M; \quad \text{where } A \in \mathbb{M}_n(L).$$

Now we can sum up our conclusions by giving the following proposition.

Proposition 3.2.1. *Let σ be an involution of first kind on a central simple F-algebra $\mathcal{A}$ with* $\deg(\mathcal{A}) = \mathrm{n}$. *Let L be any splitting field of F. Let V be an n-dimensional vector space over L. Then there exists a non-singular symmetric or skew symmetric bilinear form B on V and an invertible matrix* $M \in \mathrm{GL_n(L)}$ *such that $M^t = M$ if B is symmetric, $M^t = -M$ if B is skew-symmetric, and*

$$(\mathcal{A}_L, \sigma_L) \cong (\mathrm{End_L(V)}, \sigma_{\mathrm{B}}) \cong (\mathbb{M}_{\mathrm{n}}(\mathrm{L}), \sigma_{\mathrm{M}}).$$

Definition 3.2.6 Let σ be an involution of first kind on a central simple F-algebra $\mathcal{A}$. Let L be any splitting field of F.

1. If for any isomorphism $(A_L, \sigma_L) \cong (\mathrm{End_L(V)}, \sigma_{\mathrm{B}})$, the bilinear form B is symmetric, then we call σ to be an involution of *orthogonal type* .

2. If for any isomorphism $(A_L, \sigma_L) \cong (\mathrm{End_L(V)}, \sigma_{\mathrm{B}})$, the bilinear form B is skew-symmetric, then we call σ to be an involution of *symplectic type* .

Remark 3.2.7 In view of the theorem (3.2.4), one can see that involutions of first kind are either of orthogonal type or of symplectic type.

Proposition 3.2.2. *Let σ be an involution of first kind on a central simple F-algebra $\mathcal{A}$ and degree of $\mathcal{A}$ is n.*

1. *If σ is of orthogonal type, then* $\dim_{\mathrm{F}}(\mathrm{Sym}(\mathcal{A}, \sigma)) = \dfrac{\mathrm{n(n+1)}}{2}$.

2. *If σ is of symplectic type, then* $\dim_{\mathrm{F}}(\mathrm{Skew}(\mathcal{A}, \sigma)) = \dfrac{\mathrm{n(n+1)}}{2}$.

Proof: We identify $(\mathcal{A}, \sigma)$ with $(\mathbb{M}_n(F), \sigma_M)$; where $M \in \mathrm{GL_n(L)}$ such that $M^t = M$ if B is symmetric and $M^t = -M$ if B is skew-symmetric (by theorem (3.2.1)). For $A \in \mathbb{M}_n(F)$, the relation $MA = (MA)^t$ is equivalent to $\sigma_M(A) = A$ if $M^t = M$ and to $\sigma_M(A) = -A$ if $M^t = -M$. Therefore,

$$g^{-1}.\mathrm{Sym(\mathbb{M}_n(F), t)} = \begin{cases} \mathrm{Sym}(\mathcal{A}, \sigma) & \text{if B is symmetric} \\ \mathrm{Skew}(\mathcal{A}, \sigma) & \text{if B is skew- symmetric} \end{cases}$$

As $\dim_{\mathrm{F}}(\mathrm{Sym}(\mathbb{M}_{\mathrm{n}}(\mathrm{F}), \mathrm{t})) = \frac{\mathrm{n(n+1)}}{2}$, hence the result follows.

Proposition 3.2.3. *Let σ be an involution of first kind on a central simple F-algebra $\mathcal{A}$. Let $\sigma' = \mathrm{Int(u)} \circ \sigma$ (existence of u follows from theorem (3.1.8)) be any other involution of first kind on $\mathcal{A}$ with $\sigma(u) = \pm u$; $u \in \mathcal{A}^*$. Then*

1. $\mathrm{Sym}(\mathcal{A}, \sigma') = \mathrm{Symd}(\mathcal{A}, \sigma') = \begin{cases} u.\mathrm{Sym}(\mathcal{A}, \sigma) & \text{if } \sigma(\mathrm{u}) = \mathrm{u} \\ u.\mathrm{Skew}(\mathcal{A}, \sigma) & \text{if } \sigma(\mathrm{u}) = -\mathrm{u}. \end{cases}$

2. $\mathrm{Skew}(\mathcal{A}, \sigma') = \mathrm{Alt}(\mathcal{A}, \sigma') = \begin{cases} u.\mathrm{Skew}(\mathcal{A}, \sigma) & \text{if } \sigma(\mathrm{u}) = \mathrm{u} \\ u.\mathrm{Sym}(\mathcal{A}, \sigma) & \text{if } \sigma(\mathrm{u}) = -\mathrm{u}. \end{cases}$

3. *σ and σ' are of the same type if and only if $\sigma(u) = -u$.*

Proof:

1. For all $x \in \mathcal{A}$, we have

   $$x + \sigma'(x) = u(u^{-1}x + \sigma(x)u^{-1}) = u(u^{-1}x + \sigma(u^{-1}x)) \quad \text{if } \sigma(u) = u$$

   and

   $$x + \sigma'(x) = u(u^{-1}x + \sigma(x)u^{-1}) = u(u^{-1}x - \sigma(u^{-1}x)) \quad \text{if } \sigma(u) = -u.$$

2. For all $x \in \mathcal{A}$, we have

   $$x - \sigma'(x) = u(u^{-1}x - \sigma(x)u^{-1}) = u(u^{-1}x - \sigma(u^{-1}x)) \quad \text{if } \sigma(u) = u$$

   and

   $$x - \sigma'(x) = u(u^{-1}x - \sigma(x)u^{-1}) = u(u^{-1}x + \sigma(u^{-1}x)) \quad \text{if } \sigma(u) = -u.$$

3. The involutions σ and σ' are of the same type if and only if $\dim_{\mathrm{F}}(\mathrm{Sym}(\mathcal{A}, \sigma)) = \dim_{\mathrm{F}}(\mathrm{Sym}(\mathcal{A}, \sigma'))$ (by proposition (3.2.2)) and this condition is true if and only if $\sigma(u) = u$ (using part 1).

Proposition 3.2.4. *Let σ be an involution of first kind and symplectic type on a central simple F-algebra $\mathcal{A}$. Then* $\mathrm{Nrd}_{\mathcal{A}}(\mathrm{s})$ *is a square in F for all $s \in \mathrm{Sym}(\mathcal{A}, \sigma)$.*

Proof: For a proof we refer to ([KMRT98], page 19).

Let $Q = (a, b)_F$ be a quaternion algebra over F. Then the conjugation map on Q (denoted by γ) is an involution in view of the observation (2.4.4). It is an involution of first kind (because $\gamma(a) = a$ for all $a \in F$). Since $\dim_{\mathrm{F}}(\mathrm{Sym}(\mathrm{Q}, \gamma)) = 1$, therefore it is a symplectic involution (because of proposition (3.2.2) and remark (3.2.7)). We call this involution as the *canonical involution* on Q.

Proposition 3.2.5. *Let Q be a quaternion algebra over F and γ be the canonical involution on Q. Then γ is the unique symplectic involution on Q and every orthogonal involution σ on Q is of the form* $\mathrm{Int}(\mathrm{u}) \circ \gamma$*; where $u \in Q^*$ is uniquely determined by σ upto a factor in F^*.*

Proof: By theorem (3.1.8), It falls out that if σ is an involution of first kind on Q, then $\sigma = \mathrm{Int}(\mathrm{u}) \circ \gamma$; where $u \in Q^*$ with $\gamma(u) = \pm u$. If σ is symplectic, then $\gamma(u) = u$ which implies that $\sigma = \gamma$. If σ is orthogonal, then $\gamma(u) = -u$ with $u \in Q^*$.

3.3 Isotropy and Hyperbolicity of Adjoint Algebra

Definition 3.3.1 Let I be a left ideal of a central simple algebra $\mathcal{A}$ over a field F. Then the *annihilator* of I (denoted by I°) is defined as

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

In the similar manner, we can define annihilator of a right ideal. Clearly, I° is a right ideal of $\mathcal{A}$ if I is a left ideal of $\mathcal{A}$ and vice-versa.

Definition 3.3.2 Let σ be an involution on a central simple F-algebra $\mathcal{A}$ and I be a right ideal of $\mathcal{A}$. Then the *orthogonal ideal* of I (denoted by $I^\perp$) w.r.t. σ is defined as

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

It can be clearly seen that $I^\perp$ is a right ideal of $\mathcal{A}$.
One can observe that if I is a right ideal of $\mathcal{A}$, then $\sigma(I)$ is a left ideal and

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

Definition 3.3.3 Let σ be an involution on a central simple F-algebra $\mathcal{A}$ and I be a right ideal of $\mathcal{A}$. Then the ideal I is said to be *isotropic* w.r.t. σ if $I \subseteq I^{\perp}$.

Definition 3.3.4 Let σ be an involution on a central simple F-algebra $\mathcal{A}$. Then $\mathcal{A}$ is said to be *isotropic* if there exist a non zero isotropic ideal of $\mathcal{A}$.

Observation 3.3.5 Let σ be an involution of first kind on a central simple F-algebra $\mathcal{A}$. Then $\exists a \in \mathcal{A}$ such that $\sigma(a).a = 0$ if and only if there exists a non zero isotropic ideal of $\mathcal{A}$.

Definition 3.3.6 A central simple algebra $\mathcal{A}$ with involution σ is said to be *hyperbolic* if there exists a non zero isotropic ideal I of $\mathcal{A}$ such that $\dim_{\mathrm{F}}(\mathrm{I}) = \frac{1}{2}\dim_{\mathrm{F}}(\mathcal{A})$.

Proposition 3.3.1. *A central simple algebra $\mathcal{A}$ with involution σ. Then the following statements are equivalent:*

1. *$\mathcal{A}$ is hyperbolic.*
2. *There exists an idempotent element $e \in \mathcal{A}$ such that $\sigma(e) = 1 - e$.*

Proof: For a proof we refer to ([KMRT98], page 74).

Example 3.3.7 The quaternion algebra Q with canonical involution γ is hyperbolic as

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

is the required idempotent element as mentioned in proposition (3.3.1).

Now, we want to find relation between the isotropy and hyperbolicity of the bilinear space (V, B) and the split algebra with orthogonal involution $(\mathrm{End_F(V)}, \sigma_{\mathrm{B}})$. Let U be a subspace of an n-dimensional vector space V. Then one can easily check that

$$\mathrm{Hom_F(V, U)} = \{\mathrm{f} \in \mathrm{End_F(V)} : \mathrm{f(V)} \subseteq \mathrm{U}\}.$$

is a right ideal of the ring $\mathrm{End_F(V)}$ and $\dim_{\mathrm{F}}(\mathrm{Hom_F(V, U)}) = \dim_{\mathrm{F}}(\mathrm{V}).\dim_{\mathrm{F}}(\mathrm{U})$.

Proposition 3.3.2. *There is a one-to-one correspondence between vector subspaces of V and the right ideals I of the the ring* $\mathrm{End_F(V)}$ *defined by the map $U \mapsto \mathrm{Hom_F(V, U)}$.*

Proof: The map $U \mapsto \mathrm{Hom_F(V, U)}$ is a well defined map from the collection of subspaces of V to the collection of right ideals of the ring $\mathrm{End_F(V)}$. Now it suffices to show that every right ideal I of the ring $\mathrm{End_F(V)}$ is of the form $\mathrm{Hom_F(V, U)}$; for some subspace U of V. Let $\mathcal{S}$ be the collection of all subsets W of V such that $f(V) \subseteq W$; for all $f \in I$. $\mathcal{S}$ is a non empty collection as $V \in \mathcal{S}$. Thus, by Zorn's lemma, $\mathcal{S}$ has the minimal element, say, U. Now, therefore, it is enough to show that U is a subspace of V.

For this, firstly, we will show that for $u \in U$, there exist a $f \in I$ such that $f(v) = u$, for all $v \in V$. Since U is the minimal element of $\mathcal{S}$, therefore, there exist atleast one $g \in I$ such that $g(w) = u$ for some $w \in V$. Now fix w and define the map $h : V \to V$ as $h(v) = w$ for all $v \in V$. Thus $f = g \circ h$ is the required map because I is a right ideal of the ring $\mathrm{End_F(V)}$.

Now let $f_1, f_2 \in I$ be two maps corresponding to $u_1, u_2 \in U$ as defined in the previous paragraph. Since I is a ideal, therefore, $(f_1 + f_2) \in I$ and hence $(f_1 + f_2)(V) = u_1 + u_2 \in U$. It is clear that $0 \in U$. Let $\lambda \in F$, $u \in U$ and f be the same as defined earlier. Then $\lambda f(V) = \lambda u \in U$. Hence U is a subspace of V and we are through.

Proposition 3.3.3. *Let* $\mathrm{(End_F(V), \sigma_B)}$ *be the adjoint algebra for the bilinear space* (V, B) *and* $I = \mathrm{Hom_F(V, W)}$ *for some subspace* W *of* V*. Then*

$$I^{\perp} = \mathrm{Hom_F(V, W^{\perp})}.$$

Proof: If $I = \mathrm{Hom_F(V, W)}$ for some subspace W of V, then for $g \in \mathrm{End_F(V)}$, $f \in \mathrm{Hom_F(V, W)}$ and $x, y \in V$, we have

$$B(f(x), g(y)) = B(\sigma_B(g) \circ f(x), y).$$

Thus, $\sigma_B(g) \circ f = 0$ if and only if $g(y) \in W^{\perp}$ i.e., $g \in \mathrm{Hom_F(V, W^{\perp})}$. Hence, $I^{\perp} = \mathrm{Hom_F(V, W^{\perp})}$.

Theorem 3.3.8. *Let* $\mathrm{(End_F(V), \sigma_q)}$ *be the adjoint algebra of the quadratic space* (V, q)*. Then the algebra* $\mathrm{(End_F(V), \sigma_q)}$ *is isotropic if and only if the quadratic space* (V, q) *is isotropic.*

Proof: "If" part: If (V, q) is an isotropic quadratic space, then there exists a non zero isotopic vector $v \in V$. Consider $I = \mathrm{Hom_F(V, W)}$ where W is the subspace generated by v. Then I is a non-zero ideal of $\mathrm{End_F(V)}$. Now $v \in W^{\perp}$ as v is an isotropic vector of V. Therefore,

$$I = \mathrm{Hom_F(V, W)} \subseteq \mathrm{Hom_F(V, W^{\perp})} = \mathrm{I^{\perp}};$$

i.e., I is a non zero isotropic ideal of $\mathrm{End_F(V)}$ and hence the adjoint algebra $\mathrm{(End_F(V), \sigma_q)}$ is isotropic.

"Only if" part: Let I be a non zero isotropic ideal of $\mathrm{End_F(V)}$. Then $I = \mathrm{Hom_F(V,U)}$, for some subspace U of V (by proposition (3.3.2)). Since I is isotropic, therefore, $I \subseteq I^{\perp}$; i.e., $\mathrm{Hom_F(V,U)} \subseteq \mathrm{Hom_F(V,U^{\perp})}$ which implies that $U \subseteq U^{\perp}$. Since U is a non zero subspace of V, therefore, $\exists 0 \neq v \in U$ such that $q(v) = 0$. Hence, (V, q) is an isotropic quadratic space.

Theorem 3.3.9. *Let* $(\mathrm{End_F(V)}, \sigma_q)$ *be the adjoint algebra of a* $2n$*-dimensional quadratic space* (V, q)*. Then the algebra* $(\mathrm{End_F(V)}, \sigma_q)$ *is hyperbolic if and only if the quadratic space* (V, q) *is hyperbolic.*

Proof: "If" part: If (V, q) is a hyperbolic quadratic space, then $\exists$ an n-dimensional totally isotropic subspace W of V. Consider $I = \mathrm{Hom_F(V,W)}$. Then I is a non zero isotropic ideal of $\mathrm{End_F(V)}$ and $\mathrm{dim_F(I) = dim_F(V).dim_F(W) = 2n^2 = \frac{1}{2}dim_F(End_F(V))}$. Thus the adjoint algebra $(\mathrm{End_F(V)}, \sigma_q)$ is hyperbolic.
"Only if" part: Let I be a non zero isotropic ideal of $\mathrm{End_F(V)}$ with $\mathrm{dim_F(I) = \frac{1}{2}dim_F(End_F(V))}$. Then $I = \mathrm{Hom_F(V,U)}$, for some subspace U of V (by proposition (3.3.2)) with $\mathrm{dim_F(U) = \frac{1}{2}dim_F(V)}$. Since I is isotropic, therefore, $I \subseteq I^{\perp}$; i.e., $\mathrm{Hom_F(V,U)} \subseteq \mathrm{Hom_F(V,U^{\perp})}$ which implies that $U \subseteq U^{\perp}$; i.e., U is a totally isotropic subspace of V with $\mathrm{dim_F(U) = \frac{1}{2}dim_F(V)}$. Thus, the quadratic space (V, q) is hyperbolic.

3.4 Hermitian Forms

In this section, we want to generalize some results of §2 for arbitrary central simple algebra with involution.

Definition 3.4.1 Let $\mathcal{A}$ be a central simple F-algebra and M be a left $\mathcal{A}$-module. Then *reduced dimension* of M (denoted by rdim(M)) is defined as:

$$\mathrm{rdim(M)} = \frac{\mathrm{dim_F(M)}}{\mathrm{deg}\mathcal{A}}.$$

Definition 3.4.2 Let σ be an involution of first kind on a central simple F-algebra $\mathcal{A}$ and M be a right $\mathcal{A}$-module. Then *hermitian form* on M is defined as a map $h : M \times M \to \mathcal{A}$ which satisfies the following properties:

1. h is $\mathcal{A}$-linear in second variable; i.e., $h(x, y\alpha+z\beta) = h(x, y)\alpha+h(x, z)\beta$.
2. $h(x, y) = \sigma(h(y, x))$;

where $\alpha, \beta \in \mathcal{A}$ and $x, y, z \in M$.

Definition 3.4.3 A hermitian form $h : M \times M \to \mathcal{A}$ is called *non-singular* if the map $M \to \mathrm{Hom}_{\mathcal{A}}(\mathrm{M}, \mathcal{A})$ defined as $x \mapsto h(\_, x)$ is bijective.

Proposition 3.4.1. *Let $E \cong \mathrm{End}_{\mathcal{A}}(\mathrm{V})$ for some central division algebra $\mathcal{A}$ over F and some finite dimensional vector space V over $\mathcal{A}$. Let I be a right ideal of E. Then*

$$I = \mathrm{Hom}_{\mathcal{A}}(\mathrm{V}, \mathrm{W})$$

where W is a subspace of V. Furthermore, $\exists$ an idempotent element $e \in E$ such that $I = eE$.

Proof: For a proof we refer to ([KMRT98], page 7).

Theorem 3.4.4. *Let $\mathcal{A}$ be a central simple algebra over a field F with involution τ and M be a right $\mathcal{A}$-module. Let h be a non singular hermitian or skew-hermitian form on M. Then there exists a unique involution σ_h on $\mathrm{End}_{\mathcal{A}}(\mathrm{M})$ which satisfies the following conditions:*

1. *$\sigma_h(\alpha) = \tau(\alpha)$ for all $\alpha \in F$.*
2. *$h(x, f(y)) = h(\sigma_h(f)(x), y)$ for $x, y \in M$.*

Proof: For a proof we refer to ([KMRT98], page 42).

The involution σ_h as defined in the above theorem is called the *adjoint involution* w.r.t. h.

Theorem 3.4.5. *Let $E = \mathrm{End}_{\mathcal{A}}(\mathrm{M})$ be a central simple F-algebra and τ be an involution of first kind on $\mathcal{A}$. Then the map $h \mapsto \sigma_h$ defines a one-to-one correspondence between non singular hermitian and skew-hermitian forms on M w.r.t. τ modulo a scalar factor in F^* and involutions of the first kind on E. Moreover, the involutions σ_h and τ are of the same type if h is hermitian and of opposite types if h is skew-hermitian.*

Proof: For a proof we refer to ([KMRT98], page 43).

Theorem 3.4.6. *Let σ be an involution of first kind on a central simple F-algebra $\mathcal{A}$ and $L = F(\sqrt{a})$ be a quadratic extension of F such that the extended algebra $\mathcal{A}_L$ with involution σ_L is hyperbolic. Then $\exists \alpha \in \mathcal{A}$ such that $\alpha^2 = a$ and $\sigma(\alpha) = -\alpha$.*

Proof: Since σ_L is hyperbolic, therefore there exists an idempotent $e \in \mathcal{A}_L$ such that $\sigma_L(e) = 1 - e$. We can write $e = e_1 \otimes 1 + e_2 \otimes \sqrt{a}$; where $e_1, e_2 \in \mathcal{A}$. Thus

$$\sigma_L(e) = \sigma_L(e_1 \otimes 1 + e_2 \otimes \sqrt{a})$$

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

Since $\sigma_L(e) = 1 - e$, therefore

$$\sigma(e_1) \otimes 1 + \sigma(e_2) \otimes \sqrt{a} = 1 \otimes 1 - (e_1 \otimes 1 + e_2 \otimes \sqrt{a})$$

which implies that $\sigma(e_1) = 1 - e_1$ and $\sigma(e_2) = -e_2$.
Idempotency of e (i.e., $e^2 = e$) implies that

$$(e_1^2 + ae_2^2) \otimes 1 + (e_1e_2 + e_2e_1) \otimes \sqrt{a} = e_1 \otimes 1 + e_2 \otimes \sqrt{a}$$

which implies that $e_1^2 + ae_2^2 = e_1$ and $e_1e_2 + e_2e_1 = e_2$.
Let $I = e_2\mathcal{A}$ be a right ideal of $\mathcal{A}$. Then

$$\begin{aligned} I^{\perp} = (\sigma I)^{\circ} &= \{x \in \mathcal{A} : \sigma(I).x = 0\} \\ &= \{x \in \mathcal{A} : e_2x = 0\} \end{aligned}$$

Let x be any element of $I^{\perp}$. Then we have

$$e_2e_1x = 0$$

$$e_1^2x = e_1x.$$

Thus $e_1x \in I^{\perp}$ for $x \in I^{\perp}$. Hence from the above equations, we get

$$e_1\sigma(x)\sigma(e_1\sigma(x)) = 0$$

$$xe_1\sigma(xe_1) = 0$$

We know that if σ is anisotropic, then for all $x \in \mathcal{A}$, $\sigma(x)x = 0 \Leftrightarrow x = 0$.
Therefore, $xe_1 = 0 = e_1\sigma(x)$. Thus

$$0 = \sigma(xe_1) = \sigma(e_1)\sigma(x) = (1 - e_1)\sigma(x) = \sigma(x)$$

and hence $I^{\perp} = 0$. Since $e_2x \neq 0$ for all $0 \neq x \in \mathcal{A}$, therefore, e_2 is invertible.
Now $e_1e_2^{-1}$ is the desired element, say, α; i.e., $\alpha^2 = a$ and $\sigma(\alpha) = -\alpha$.

Theorem 3.4.7. *Let σ be an involution of first kind on a central simple F-algebra $\mathcal{A}$ and $L = F(\sqrt{a})$ be a quadratic extension of F. If there exists $\alpha \in \mathcal{A}$ such that $\alpha^2 = a$ and $\sigma(\alpha) = -\alpha$, then the extended algebra $\mathcal{A}_L$ with involution σ_L is hyperbolic. Conversely, if σ is an involution of first kind and orthogonal type on a non split central simple F-algebra $\mathcal{A}$ and Witt index of $\mathcal{A}$ is odd, then $\exists \alpha \in \mathcal{A}$ such that $\alpha^2 = a$ and $\sigma(\alpha) = -\alpha$ and the extended algebra $\mathcal{A}_L$ with involution σ_L is hyperbolic.*

Proof: For a proof we refer to ([BFST93], Theorem 3.3).

Theorem 3.4.8. *Let $\mathcal{A}$ be a central simple F-algebra with involution σ and let $\mathcal{A}$ is Brauer equivalent to a quaternion division algebra Q. If σ is an involution of first kind and orthogonal type then $\mathcal{A}$ contains a subalgebra which is isomorphic to Q if and only if σ is hyperbolic over a quadratic field extension $F(\sqrt{a})$ such that Q splits over $F(\sqrt{a})$.*

Proof: For a proof we refer to ([BFST93], Theorem 3.4).

3.5 The Discriminant

The notion of discriminant is related to involutions of orthogonal type. In this section, our aim is to define discriminant of an orthogonal involution σ_b in such a way that the discriminant of σ_b is same as the discriminant of the associated symmetric bilinear form b.

Recall that if (V, b) is a non-singular bilinear space over F and $\dim_{\mathrm{F}}(\mathrm{V}) = \mathrm{n}$, then

1. *determinant* of b is the square class of the determinant of the matrix of b w.r.t. an arbitrary basis $(e_1, e_2, ..., e_n)$ of V; i.e.,

$$\det(\mathrm{b}) = \det(\mathrm{b}(\mathrm{e_i}, \mathrm{e_j}))_{1\leq \mathrm{i,j} \leq \mathrm{n}}.\mathrm{F}^{*2} \in \mathrm{F}^*/\mathrm{F}^{*2}.$$

2. *discriminant* of b is the signed determinant; i.e.,

$$\mathrm{disc}(\mathrm{b}) = (-1)^{\mathrm{n(n-1)/2}}\det(\mathrm{b}) \in \mathrm{F}^*/\mathrm{F}^{*2}.$$

Observation 3.5.1 The discriminant of an orthogonal involution is defined only for central simple algebras of even degree. We know that there is a bijection between involutions of first kind on $\mathrm{End}_{\mathrm{F}}(\mathrm{V})$ and equivalence classes of non singular symmetric or skew-symmetric bilinear forms on V modulo multiplication by a factor in F^*. If $\dim(\mathrm{V})$ is odd, then for $\alpha \in F^*$ we have $\mathrm{disc}(\alpha \mathrm{b}) = \alpha \mathrm{disc}(\mathrm{b})$. Therefore, the discriminant of an orthogonal involution is invariant (and hence well defined) if and only if the $\dim(\mathrm{V})$ is even.

The definition of the discriminant of an orthogonal involution depends on the following proposition:

Proposition 3.5.1. *Let σ be an orthogonal involution on a central simple F-algebra $\mathcal{A}$. If $\deg(\mathcal{A})$ is even, then*

$$\mathrm{Nrd}_{\mathcal{A}}(\mathrm{a}) \equiv \mathrm{Nrd}_{\mathcal{A}}(\mathrm{b}).\mathrm{F}^{*2},$$

where $a, b \in \mathrm{Alt}(\mathcal{A}, \sigma) \cap \mathcal{A}^*$.

Proof: Fix $a, b \in \mathrm{Alt}(\mathcal{A}, \sigma) \cap \mathcal{A}^*$. The involution $\sigma' = \mathrm{Int(a)} \circ \sigma$ is symplectic (by proposition (3.2.3)(3)) and $ab \in \mathrm{Sym}(\mathcal{A}, \sigma')$ (using proposition (3.2.3)(1)). Therefore, $\mathrm{Nrd}_{\mathcal{A}}(\mathrm{ab}) \in \mathrm{F}^{*2}$ (using proposition (3.2.4)) and hence the result follows.

Definition 3.5.2 Let σ be an orthogonal involution on a central simple algebra $\mathcal{A}$ of even degree $n = 2m$ over a field F.

1. The *determinant* of σ (denoted by $\det(\sigma)$) is defined as the square class of the reduced norm of any alternating unit, i.e.,

$$\det(\sigma) = \mathrm{Nrd}_{\mathcal{A}}(\mathrm{a}).\mathrm{F}^{*2} \in \mathrm{F}^*/\mathrm{F}^{*2} \quad \text{for a} \in \mathrm{Alt}(\mathcal{A}, \sigma) \cap \mathcal{A}^{*}.$$

2. The *discriminant* of σ (denoted by $\mathrm{disc}(\sigma)$) is defined as the signed determinant, i.e.,

$$\mathrm{disc}(\sigma) = (-1)^{\mathrm{m}}\det(\sigma) \in \mathrm{F}^*/\mathrm{F}^{*2}.$$

Proposition 3.5.2. *Let $\mathcal{A}$ be a central simple algebra of even degree over a field F.*

1. *Suppose σ is an orthogonal involution on $\mathcal{A}$ and let $u \in \mathcal{A}^*$. If* $\mathrm{Int(u)} \circ \sigma$ *is an orthogonal involution on $\mathcal{A}$, then*

$$\mathrm{disc}(\mathrm{Int(u)} \circ \sigma) = \mathrm{Nrd}_{\mathcal{A}}(\mathrm{u}).\mathrm{disc}(\sigma).$$

2. *Suppose σ is a symplectic involution on $\mathcal{A}$ and let $u \in \mathcal{A}^*$. If* $\mathrm{Int(u)} \circ \sigma$ *is an orthogonal involution on $\mathcal{A}$, then* $\mathrm{disc}(\mathrm{Int(u)} \circ \sigma) = \mathrm{Nrd}_{\mathcal{A}}(\mathrm{u})$.

Proof:

1. Since both σ and $\mathrm{Int(u)} \circ \sigma$ are orthogonal involutions, therefore $\sigma(u) = u$ which implies that $\mathrm{Alt}(\mathcal{A}, \mathrm{Int(u)} \circ \sigma) = \mathrm{u.Alt}(\mathcal{A}, \sigma)$ by (by proposition (3.2.3)(2)) and hence the result follows.

2. Since σ is symplectic and $\mathrm{Int(u)} \circ \sigma$ is orthogonal, therefore $\sigma(u) = -u$ which implies that $u \in \mathrm{Alt}(\mathcal{A}, \mathrm{Int(u)} \circ \sigma)$ and hence the result follows.

Proposition 3.5.3. *Let $\mathcal{A} = \mathrm{End}_{\mathrm{F}}(\mathrm{V})$ be a central simple F-algebra of even degree and σ_b is the adjoint involution on $\mathcal{A}$ w.r.t. some non singular symmetric bilinear form b on V, then*

$$\mathrm{disc}(\sigma_{\mathrm{b}}) = \mathrm{disc(b)}.$$

Proof: Let $\dim(\mathrm{V}) = \mathrm{n} = 2\mathrm{m}$ and $\{e_1, e_2, ..., e_n\}$ be a basis of V which identifies $\mathcal{A}$ with $M_n(F)$ and let M be the symmetric matrix of b w.r.t. the chosen basis. Then, by definition, the involution σ_b is given by

$$\sigma_b = \mathrm{Int}(\mathrm{M}^{-1}) \circ \mathrm{t}$$

where t denotes the transpose involution. Since there exists an alternating matrix of determinant 1, therefore $\mathrm{disc(t)} = (-1)^{\mathrm{m}}$ and hence

$$\mathrm{disc}(\sigma_{\mathrm{b}}) = (-1)^{\mathrm{m}}\mathrm{det}(\mathrm{M}^{-1}).\mathrm{F}^{*2} = \mathrm{disc(b)}.$$

Proposition 3.5.4. *Let σ be an orthogonal involution on a central simple algebra $\mathcal{A}$ of even degree $n = 2m$ over a field F. If σ is hyperbolic, then* $\mathrm{disc}(\sigma) = 1$.

Proof: Let $e \in \mathcal{A}$ be an idempotent element such that $\sigma(e) = 1 - e$. Over a splitting field of $\mathcal{A}$, we can represent e by a diagonal matrix

$$e = \mathrm{diag}(1, ..., 1, 0, ..., 0),$$

because $\mathrm{rdim}(\mathrm{e}\mathcal{A}) = \mathrm{m}$. Since $\sigma(e) = 1 - e$, therefore $2e - 1 \in \mathrm{Alt}(\mathcal{A}, \sigma)$. We can write $2e - 1$, over a splitting field, as

$$2e - 1 = \mathrm{diag}(\underbrace{1, ..., 1}_{\mathrm{m}}, \underbrace{-1, ..., -1}_{\mathrm{m}}).$$

Thus we have $\mathrm{Nrd}_{\mathcal{A}}(2\mathrm{e} - 1) = (-1)^{\mathrm{m}}$ and hence $\mathrm{disc}(\sigma) = 1$.

Proposition 3.5.5. *Let Q be a quaternion algebra over F. Then orthogonal involutions on Q can be classified upto conjugation by their discriminant.*

Proof: Let σ and σ' be two orthogonal involutions on Q having the same discriminant and let γ be the canonical involution on Q. Every orthogonal involution on Q is of the form $\mathrm{Int(s)} \circ \gamma$; for some $s \in \mathrm{Skew}(\mathrm{Q}, \gamma)\backslash\mathrm{F}$ (by proposition (3.2.5)). Thus, we can write $\sigma = \mathrm{Int(s)} \circ \gamma$ and $\sigma' = \mathrm{Int(s')} \circ \gamma$; for some $s, s' \in \mathrm{Skew}(\mathrm{Q}, \gamma)\backslash\mathrm{F}$. By proposition (3.5.2)(2), we have $\mathrm{disc}(\sigma) = \mathrm{Nrd_Q(s).F^{*2}}$ and $\mathrm{disc}(\sigma') = \mathrm{Nrd_Q(s').F^{*2}}$. Thus, we can assume that s and s' have the same reduced norm. Therefore s and s' have the same reduced characteristic polynomial (because $\mathrm{Trd_Q(s)} = 0 = \mathrm{Trd_Q(s')}$). Thus, we get

$$s' = xsx^{-1} = xs\overline{x}.\overline{x}^{-1}x^{-1} = \mathrm{Nrd_Q(x)}^{-1}\mathrm{xs}\gamma\mathrm{(x)},$$

for some $x \in Q^*$. Therefore, for all $y \in Q^*$, we have

$$\begin{aligned}\sigma'(y) = \mathrm{Int(s')} \circ \gamma\mathrm{(y)} &= s'\gamma(y)s'^{-1} \\ &= xs\gamma(x)\gamma(y)\gamma(x)^{-1}s^{-1}x^{-1} \\ &= xs\gamma(x^{-1}yx)s^{-1}x^{-1} \\ &= \mathrm{Int(x)} \circ \sigma \circ \mathrm{Int(x^{-1})(y)}\end{aligned}$$

and we are done.

Bibliography

[BFST93] E. Bayer-Fluckiger, D.B. Shapiro and J.P. Tignol, *Hyperbolic Involutions*, Mathematische Zeitschrift **214** (1993), 461-476.

[Gar11] D.J.H. Garling, *Clifford Algebras: An Introduction*, London Mathematical Society (2011).

[Ger08] Larry J. Gerstein, *Basic Quadratic Forms*, American Mathematical Society (2008).

[Kat07] S. Katok, *p-adic Analysis Compared with Real*, American Mathematical Society, (2007).

[KMRT98] M.A. Knus, A.S. Merkurjev, M. Rost, J.P. Tignol *The Book of Involutions*, American Mathematical Society Colloquium Publications, (1998).

[La73] T.Y. Lam, *Algebraic Theory of Quadratic Forms*, W.A. Benjamin, (1973).

[Lam05] T.Y. Lam, *Introduction to Quadratic Forms over Fields*, American Mathematical Society, (2005).

[Sch85] W. Scharlau, *Quadratic and Hermitian Forms*, Springer-Verlag (1985).

Index