Pfister Numbers of Quadratic Forms

Kritika Singhal

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

Indian Institute of Science Education and Research Mohali
April 2014

Certificate of Examination

This is to certify that the dissertation titled **Pfister Numbers of Quadratic Forms** submitted by **Ms. Kritika Singhal** (Reg. No. MS09072) for the partial fulfillment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Kapil H. Paranjape Dr. Varadharaj R. Srinivasan Dr. Amit Kulshrestha
(Supervisor)

Dated: April 24, 2014

Declaration

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

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Kritika Singhal
(Candidate)

Dated: April 24, 2014

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

Dr. Amit Kulshrestha
(Supervisor)

Acknowledgment

There are many people behind the successful completion of my master's thesis. I feel extremely happy to thank these people. The first person I want to thank is my supervisor Dr. Amit Kulshrestha for introducing me to this topic and helping me at each and every step of understanding it. I feel fortunate to be his student and receive his guidance, not only in mathematics but in other academic decisions as well. I also thank his doctoral student, Ms. Dilpreet Kaur for helping me with LaTeX.

I thank Dr. Varadharaj R. Srinivasan for his course on "Structure of Algebras" which helped me understand many concepts of this project and Prof. I B S Passi for his courses on algebra which provided me with an adequate background for the project.

I cannot forget to thank my family for their constant support and invaluable guidance. Without their help, I would not have been able to complete my project so efficiently. I also thank my friends at IISER Mohali for lifting up my spirits whenever required.

Finally, I thank IISER Mohali for providing me a pleasant work environment and the Department of Science and Technology, India for giving me INSPIRE fellowship.

Kritika Singhal

Contents

Chapter 1

Quadratic Forms

We start by defining quadratic forms and properties of isotropy, anisotropy and hyperbolicity of quadratic forms. The main results of this chapter come in the end when we define Witt ring of a field and compute Witt rings for certain fields.

1.1 Definition

Let K be a field with characteristic different from 2. Let V be an n dimensional vector space over K. An n-ary quadratic form over K is a polynomial f in n variables over K that is homogenous of degree 2. The general form of f is given as

$$f(x_1, x_2, \ldots, x_n) = \sum_{i,j} a_{ij} x_i x_j$$

here $a_{ij} \in K$. We may rewrite f as

$$f(x_1, x_2, \ldots, x_n) = \sum_{i,j} \frac{1}{2}(a_{ij} + a_{ji}) x_i x_j$$

in order to make the coefficients symmetric.
Then, f identifies uniquely with a matrix $M_f = \left(\frac{1}{2}(a_{ij} + a_{ji})\right)_{i,j}$ which turns out to be a symmetric matrix. In matrix notation, for $X = (x_1, x_2, \ldots, x_n)$, $f(X)$ can be

written as

$$f(X) = \begin{pmatrix} x_1 & . & . & . & . & x_n \end{pmatrix} M_f \begin{pmatrix} x_1 \\ . \\ . \\ . \\ . \\ x_n \end{pmatrix}$$

Two n-ary quadratic forms f and g are said to be equivalent if there exists a matrix $C \in GL_n(F)$ such that $f(X) = g(CX)$. In matrix notation, we have $f(X) = X^t M_f X$ where t stands for transpose. Thus, if f and g are equivalent then

$$\begin{aligned} f(X) &= g(CX) \\ \Leftrightarrow X^t M_f X &= (CX)^t M_g CX \\ \Leftrightarrow X^t M_f X &= X^t C^t M_g CX \\ \Leftrightarrow M_f &= C^t M_g C \end{aligned}$$

Thus, two quadratic forms are equivalent if and only if their respective symmetric matrices are congruent. In such case, we write $f \cong g$. For example, the 2-dimensional quadratic forms $f(X) = X_1^2 - X_2^2$ and $g(X) = 2X_1X_2$ over $\mathbb{R}$ are equivalent since

$$M_f = \begin{pmatrix} 1/2 & 1 \\ 1/2 & -1 \end{pmatrix} M_g \begin{pmatrix} 1/2 & 1/2 \\ 1 & -1 \end{pmatrix}$$

where $M_f = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $M_g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

The equivalence of forms is an equivalence relation and divides the set of quadratic forms over K into equivalence classes.

Let K^n denote the space of n-tuples, given the usual K vector space structure. Any element x of K^n is of the form $x = \sum_i x_i e_i$ where $x_i \in K$ and $(e_i)_i$ is the usual basis set.

Every n-ary quadratic form f gives rise to a map

$$Q_f : K^n \to K$$

given by

$$Q_f(x) = x^t M_f x$$

The map Q_f is called the *quadratic map* defined by f.
Two quadratic forms f and g with quadratic maps Q_f and Q_g are said to be equivalent if there exists a linear automorphism $C : K^n \to K^n$ such that

$$Q_f(x) = Q_g(C.x)$$

for every n- tuple $x \in K^n$.
In fact, Q_f uniquely determines the quadratic form f. This is because if $Q_f = Q_g$ as maps from K^n to K then, for any i, we have

$$(M_f)_{ii} = Q_f(e_i) = Q_g(e_i) = (M_g)_{ii}$$

and

$$Q_f(e_i + e_j) - Q_f(e_i) - Q_f(e_j) = 2M_f(e_{ij}) = 2M_g(e_{ij})$$

for all i, j. Thus $M_f = M_g$ and hence $f = g$. The quadratic map Q_f satisfies the following properties:

- Q_f is quadratic in the sense that $Q_f(ax) = a^2 Q_f(x)$ for every $a \in K$ and $x \in K^n$. This is because
$$Q_f(ax) = (ax)^t M_f(ax) = a^2 x^t M_f x$$

- If, for $x, y \in K^n$, we define
$$B_f(x, y) = \frac{Q_f(x + y) - Q_f(x) - Q_f(y)}{2}$$
Then, we observe that $B_f(x, y) = B_f(y, x)$ and B_f is linear in both variables x and y. Such a map is called a *symmetric bilinear map*. We discuss more about such maps in next section.

1.2 Bilinear forms

Let V be a vector space over field K. A map $B : V \times V \to K$ is called a bilinear map if it satisfies the following properties:

- $B(\alpha x_1 + \beta x_2, y) = \alpha B(x_1, y) + \beta B(x_2, y)$
- $B(x, \alpha y_1 + \beta y_2) = \alpha B(x, y_1) + \beta B(x, y_2)$

for all $x, y \in V$ and $\alpha, \beta \in K$. Given quadratic form f, the map B_f defined above is a bilinear map since

$$Q_f(x+y) - Q_f(x) - Q_f(y) = (x+y)^t M_f(x+y) - x^t M_f x - y^t M_f y$$

$$= x^t M_f y + y^t M_f y = 2x^t M_f y = 2y^t M_f x$$

since M_f is symmetric. Thus, we get

$$B_f(x, y) = x^t M_f y$$

Note that $B_f(x, x) = Q_f(x)$ for every $x \in K^n$. Thus, given a bilinear map, we can get back the corresponding quadratic map.
We now define a quadratic space (V, B) . Let V be a finite dimensional K-vector space and $B : V \times V \to K$ be a symmetric bilinear pairing on V. Then, we call the pair (V, B) a *quadratic space* and associate to it the quadratic map

$$q = q_B : V \to K$$

given by

$$q(x) = B(x, x),\ x \in\ V$$

As above, we have

$$q(ax) = a^2 q(x),\ q(x+y) - q(x) - q(y) = 2B(x, y)$$

for $x, y \in V$. Since q and B determine each other, we can even write (V, q) to denote the quadratic space.
If we choose a basis $(e_1, e_2, \ldots, e_n)$ for V, where $n = \dim(V)$ then, the quadratic form on V is given by

$$f(x_1, \ldots, x_n) = \sum_{i,j} B(e_i, e_j) x_i x_j$$

with $M_f = (B(e_i, e_j))_{i,j}$.
If we choose a different basis say $(w_1, w_2, \ldots, w_n)$ then the quadratic form obtained is given by

$$g(x_1, x_2, \ldots, x_n) = \sum_{i,j} B(w_i, w_j) x_i x_j$$

However, the two forms f and g are equivalent. This is because

$$\begin{aligned} B(w_i, w_j) &= B(\sum_{k=1}^{n} a_{ki}e_k, \sum_{l=1}^{n} a_{lj}e_l) \\ &= \sum_{k,l} a_{ki}B(e_k, e_l)a_{lj} \\ &= A^t B(e_i, e_j)A \end{aligned}$$

where $A = (a_{kl}) \in GL_n(K)$ is the change of basis matrix. Thus, the quadratic space (V, B) uniquely determines the equivalence class of the quadratic form f.
Two quadratic spaces (V, B) and (V', B') are said to be *isometric* ($\cong$)if there exists a linear isomorphism $\gamma : V \to V'$ such that

$$B(x, y) = B'(\gamma(x), \gamma(y)) \ \forall \ x, y \in V$$

In fact, it is obvious that

$$(V, B) \cong (V', B') \leftrightarrow (f_B) = (f_{B'})$$

1.3 Regular Quadratic Spaces

Let (V, B) be a quadratic space and S be a subspace of V. Then $(S, B \mid S \times S)$ also gives a quadratic space. Define

$$S^{\perp} = \{x \in V : B(x, y) = 0 \ \forall \ y \in S\}$$

$S^{\perp}$ is called the *orthogonal complement* of S. The orthogonal complement of V is called the *radical* of V and is denoted by $\mathrm{rad}(V)$. A quadratic space (V, B) is called *regular* if $\mathrm{rad}(V) = 0$.

Theorem 1.3.1. *The following are equivalent:*

1. *M_f is a non-singular matrix, where $M_f = B(e_i, e_j)_{i,j}$, $(e_i)_i$ being the basis of the quadratic space (V, B).*
2. *$x \to B(, x)$ defines an isomorphism $V \to V^*$ where V^* denotes the vector space dual of V.*
3. *For $x \in V$, $B(x, y) = 0$ for all $y \in V$ implies $x = 0$.*

We note that any of the above statements can be taken as a definition of regular quadratic space. The proof of this result is trivial and is therefore skipped.
The zero quadratic space is also considered regular since it satisfies statements (2) and (3) of the above theorem. Every subspace of a regular quadratic space may not be regular.

Theorem 1.3.2. *Let (V, B) be a regular quadratic space and S be a subspace of V. Then*

1. $\dim(S) + \dim(S^\perp) = \dim(V)$ *(Dimension Formula)*
2. $(S^\perp)^\perp = S$

Proof. Let $\phi : V \to V^*$ be the linear isomorphism defined by $\phi(x)(y) = B(y, x)\ \forall x, y \in V$. We know that $S^\perp = \{x \in V : B(x, S) = 0\}$. Thus, $S^\perp$ is the subspace of V for which the linear functions in $\phi(S)$ are equal to 0. Then, by the duality theory in linear algebra, we get

$$\dim(S^\perp) + \dim(\phi(S)) = \dim(V^*)$$

$$\dim(S^\perp) + \dim(S) = \dim(V)$$

This proves (1).
Applying (1) twice, we get

$$\dim(S^\perp)^\perp + \dim S^\perp = \dim V$$

Since $S \subseteq (S^\perp)^\perp$, we get $S = (S^\perp)^\perp$. □

1.4 Orthogonal sums

Let (V_1, B_1) be an n_1-dimensional and (V_2, B_2) be an n_2-dimensional quadratic space. The *orthogonal sum* of (V_1, B_1) and (V_2, B_2) is the n_1+n_2-dimensional quadratic space (V, B) such that $V = V_1 \oplus V_2$ and $B : V \times V \to F$ is given by

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

Note that $B(V_1, V_2) = 0$ and $B \mid V_i \times V_i = B_i$. The quadratic space (V, B) is denoted by $V_1 \perp V_2$. The corresponding quadratic form q_B is given by

$$q_B(x_1, x_2) = B((x_1, x_2), (x_1, x_2)) = B_1(x_1, x_1) + B_2(x_2, x_2) = q_{B_1}(x_1) + q_{B_2}(x_2)$$

We can similarly define orthogonal sum of n quadratic spaces, $n \in \mathbb{N}$.
If A_1 is the symmetric matrix corresponding to (V_1, B_1) and A_2 is the symmetric matrix corresponding to (V_2, B_2) then, the block diagonal matrix $\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$ is the symmetric matrix corresponding to (V, B).

Theorem 1.4.1. *The quadratic space $(V_1 \perp V_2, B)$ is regular if and only if both V_1 and V_2 are regular.*

Proof. The symmetric matrix of (V, B) is non singular if and only if the symmetric matrices of both (V_1, B_1) and (V_2, B_2) are non-singular. □

1.5 Diagonalization of Quadratic Forms

Let $\dot{K}$ denote the group of units in the field K. Let f be an n-ary quadratic form over K and $d \in \dot{K}$. We say that f *represents* d if there exists an n-tuple $(x_1, \ldots, x_n), x_i \in K$ such that

$$f(x_1, \ldots, x_n) = d$$

The set of values in $\dot{K}$ represented by f is denoted by $D_K(f) = D(f)$.
We observe that for $a, d \in \dot{K}$, $d \in D(f)$ if and only if $a^2 d \in D(f)$. Thus, $D(f)$ consists of cosets $a\dot{K}^2$, $a \in \dot{K}$. The set $D(f)$ is closed under taking inverses since, if $a \in D(f)$ then $a^{-1} = (a^{-1})^2 a$ also belongs to $D(f)$.
In general, $D(f)$ is not a subgroup of $\dot{K}$. If (V, B) is a quadratic space then we use $D(V)$ to denote values in $\dot{K}$ represented by the corresponding quadratic form of V.
For $d \in K$, we shall write $\langle d \rangle$ to denote the isometry class of 1-dimensional vector space corresponding to the quadratic form dX^2. Clearly, $\langle d \rangle$ is regular if and only if $d \in \dot{K}$.

Theorem 1.5.1. *Let (V, B) be a quadratic space, and $d \in \dot{K}$. Then $d \in D(V)$ if and only if there exists another quadratic space (V', B') together with an isometry $V \cong \langle d \rangle \perp V'$.*

Proof. Let $V \cong \langle d \rangle \perp V'$. Then, $d \in D(\langle d \rangle \perp V')$. Hence, $d \in D(V)$.
Conversely, suppose that $d \in D(V)$. Then, we write $V = \text{rad}(V) \perp W$ where W is a subspace of V. Let $d \in D(V)$. Then, there exists $v \in V$ such that

$$q_B(v) = d = B(v, v)$$

Let $v = x \oplus y$ where $x \in \text{rad}(V)$ and $y \in W$. Then

$$q_B(v) = q_B(x) + q_B(y) = B(x, x) + B(y, y) = B(y, y) = d$$

Thus, $d \in D(W)$. This implies that $D(V) \subseteq D(W)$. The reverse inclusion is trivial and therefore, we get $D(V) = D(W)$. Since W is regular, we may assume that V is regular. The quadratic subspace $K.v$ is isometric to $\langle d \rangle$ since

$$B(av, av) = a^2 d \ \forall \ a \in K$$

Since $d \in \dot{K}$ therefore $\langle d \rangle$ is regular. We get

$$\implies K.v \cap (K.v)^{\perp} = 0$$

From Theorem 1.3.2, we have

$$\dim(V) = \dim(K.v) + \dim(K.v)^{\perp}$$

Thus we conclude that

$$V \cong \langle d \rangle \oplus (K.v)^{\perp}$$

This completes the proof. □

Theorem 1.5.2. *If (V, B) is any quadratic space over K, then there exist scalars $d_1, \ldots, d_n \in K$ such that $V \cong \langle d_1 \rangle \perp \langle d_2 \rangle \perp \ldots \perp \langle d_n \rangle$.*

Proof. If $D(V)$ is empty, then V can be written as an orthogonal sum of zeroes. Let $D(V)$ be non-empty and let $0 \neq d \in D(V)$. By the theorem above, $V \cong \langle d \rangle \perp V'$. The result now follows by induction on $\dim(V')$. □

Theorem 1.5.3. *If (V, B) is a quadratic space (not necessarily regular) and S is a regular subspace of V, then the following hold:*

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

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

Proof. We write $S = \langle x_1 \rangle \perp \langle x_2 \rangle \perp \ldots \perp \langle x_n \rangle$ where $x_i \in \dot{K}$. Since S is regular, therefore $\text{rad}(S) = 0$. For any $z \in V$ consider

$$y = z - \sum_{i=1}^{n} \left(\frac{B(z, x_i)}{B(x_i, x_i)} \right) x_i$$

The denominator is non-vanishing since $x_i \in S$ and S is regular. Then

$$B(y, x_i) = B(z, x_i) - \sum_{i=1}^{n} \left(\frac{B(z, x_i)}{B(x_i, x_i)} \right) B(x_i, x_i) = 0$$

The above relation holds for all i. Therefore, $y \in S^{\perp}$.
Since $z \in V$ and $\sum_{i=1}^{n} \left(\frac{B(z, x_i)}{B(x_i, x_i)} \right) x_i \in S$, we get $V = S \oplus S^{\perp}$. If T is a subspace of V such that $V = S \perp T$ then using $V = S \perp S^{\perp}$, we get $T \subseteq S^{\perp}$. The dimension formula for subspaces of V gives

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

Thus, $T = S^{\perp}$. □

Theorem 1.5.4. *Let (V, B) be a regular quadratic space. Then a subspace S of V is regular if and only if there exists $T \subseteq V$ such that $V = S \perp T$.*

Proof. Let $S \subseteq V$ be regular. Then, taking $T = S^{\perp}$, the result follows from the previous theorem. Now suppose that $V = S \perp T$. Then $\text{rad}(S) = S \cap S^{\perp}$. We know that $S^{\perp} \subseteq T$. So $\text{rad}(S) \subseteq S \cap T \subseteq \text{rad}(V)$. Since $\text{rad}(V) = 0$, we get $\text{rad}(S) = 0$. Therefore S is regular. □

Let f be a non-singular quadratic form over a field K. We define *determinant* of f as

$$\det(f) = \det(M_f).\dot{K}^2$$

where M_f is the symmetric matrix associated to f. If g is another quadratic form isometric to f, then $M_g = C^t M_f C$ for some $C \in GL_n(K)$. We get

$$\det(g) = \det(M_g).\dot{K}^2 = \det(M_f)\det(C)^2.\dot{K}^2 = \det(f)$$

Thus, isometric quadratic forms have same determinant. For a diagonal quadratic space (V, B),

$$V = \langle d_1 \rangle \perp \langle d_2 \rangle \perp \ldots \perp \langle d_n \rangle$$

with corresponding quadratic form f,

$$\det(f) = d_1 d_2 \ldots d_n . \dot{K}^2$$

This determinant is sometimes denoted by $d(V)$.

1.6 Isotropic and Hyperbolic quadratic forms

Let (V, B) be a quadratic space and q_B be the associated quadratic form. The space (V, B) is called *isotropic* if there exists $v \in V, v \neq 0$ such that $q(v) = 0$. The vector v is then called the *isotropic vector*. If there does not exist any non-zero vector $v \in V$ for which $q(v) = 0$ then (V, B) is called *anisotropic* quadratic space. The space (V, B) is called *totally isotropic* if $q(v) = 0$ for all $v \in V$.

Theorem 1.6.1. *Let (V, q) be a 2-dimensional quadratic space. The following statements are equivalent:*

1. *V is regular and isotropic.*
2. *V is regular, with $d(V) = -1.\dot{K}^2$.*
3. *V is isometric to $\langle -1, 1 \rangle$.*
4. *V corresponds to the equivalence class of binary quadratic form $X_1 X_2$.*

Proof. (3) $\Leftrightarrow$ (4)
It has been proved in an example given before.
(1) $\Longrightarrow$ (2)
Let (x_1, x_2) be an orthogonal basis of V. Then, since V is regular, $q(x_i) = d_i \neq 0$ for $i = 1, 2$. Let $v = ax_1 + bx_2, a, b \in K, a \neq 0$ be an isotropic vector. Then

$$q(v) = q(ax_1 + bx_2) = a^2 d_1 + b^2 d_2 = 0$$

$$\Longrightarrow d_1 = -\left(\frac{b^2}{a^2}\right) d_2$$

Since $d(V) = d_1 d_2 \dot{K}^2$, we get

$$d(V) = -\left(\frac{b^2}{a^2}\right) d_2^2 \dot{K}^2$$

This gives $d(V) = -1.\dot{K}^2$.
(2) $\Longrightarrow$ (3)
Since $d(V) = -1.\dot{K}^2$, V is isometric to $\langle -a, a\rangle$ for some non zero $a \in K$. We have

$$aX_1^2 - aX_2^2 \cong aX_1X_2$$

Since aX_1X_2 takes all values in K, we get $1 \in D(V)$.

$$\Longrightarrow V \cong \langle 1\rangle \perp \langle -1\rangle \cong \langle 1, -1\rangle$$

(3) $\Longrightarrow$ (1)
The quadratic form $\langle -1, 1\rangle$ is isotropic since the corresponding quadratic form is $X_1^2 - X_2^2$. It is regular because the corresponding symmetric matrix is non-singular. □

The isometry class of a 2-dimensional quadratic space satisfying the above conditions is called the *hyperbolic plane*. The hyperbolic plane is denoted by $\mathbb{H}$. An orthogonal sum of hyperbolic planes is called a *hyperbolic space* .
A quadratic space (V, B) is called *universal* if $D(V) = \dot{K}$.

Theorem 1.6.2. *Let (V, B) be a regular quadratic space. Then:*

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

2. *V is isotropic if and only if V contains a hyperbolic plane (necessarily as an orthogonal summand).*

3. *V is isotropic implies V is universal.*

Proof. (1) $\Longrightarrow$ (2)
Let V be isotropic. Then, there exists $v \in V$ such that $q(v) = 0$. Let $S = \mathrm{Span}_K(v)$. Then $\dim(S) = 1$ and $S \subseteq V$ is totally isotropic. By (1), S is contained in a hyperbolic subspace $T \subseteq V$ of dimension 2. Thus V contains a hyperbolic plane.
Conversely, any hyperbolic plane is isometric to $\langle 1, -1\rangle$ and is therefore isotropic.
(2) $\Longrightarrow$ (3)

Let V be isotropic. Then, V contains a hyperbolic plane. Since the quadratic form corresponding to a hyperbolic plane is X_1X_2, we get that V is universal.
We now prove (1) by induction on r. Let $\{x_1, x_2, \ldots, x_r\}$ be an orthogonal basis of U and let S be the subspace of V spanned by $\{x_2, \ldots, x_r\}$. Then $U^\perp \subseteq V^\perp$. Since V is regular,

$$\dim(U^\perp) = \dim(V) - \dim(U) < \dim(V) - \dim(S) = \dim(S^\perp)$$

Thus, $\dim(S^\perp) > \dim(U^\perp)$.
This implies that there exists $y \in V$ such that y is orthogonal to $x_2, \ldots, x_r$ but not to x_1, i.e. $B(y, x_1) \neq 0$. Therefore, x_1 and y are linearly independent vectors.
We now consider the subspace $H = \mathrm{Span}_K(x_1, y)$. Then,

$$d(H) = det \begin{pmatrix} 0 & B(x_1, y) \\ B(y, x_1) & B(y, y) \end{pmatrix} = -B(x_1, y)^2.\dot{K}^2 = -1.\dot{K}^2$$

By previous theorem, H is isometric to $\langle 1, -1\rangle$. The space H is regular and therefore, we can write $V = H \perp V'$ where $V' = H^\perp$ and contains $\{x_2, \ldots, x_r\}$. Then, V' is regular since V is and $\dim(V') < \dim(V)$. The result now follows from induction on $\dim(V)$. □

Theorem 1.6.3 (First Representation Theorem). *Let q be a regular quadratic form over a vector space V and $d \in \dot{K}$. Then, $d \in D(V)$ if and only if $q \perp \langle -d\rangle$ is isotropic over K.*

Proof. Let

$$q = d_1X_1^2 + d_2X_2^2 + \ldots + d_nX_n^2,\ d_i \in \dot{K}$$

If $d \in D(V)$, then it is trivial that $q \perp \langle -d\rangle$ is isotropic. Conversely, suppose that $q \perp \langle -d\rangle$ is isotropic. Then, there exist $(x_1, x_2, \ldots, x_n, x_{n+1}), x_i \in K$ such that

$$d_1x_1^2 + d_2x_2^2 + \ldots + d_nx_n^2 - dx_{n+1}^2 = 0$$

If $x_{n+1} \neq 0$ then,

$$d = d_1\left(\frac{x_1}{x_{n+1}}\right)^2 + \ldots + d_n\left(\frac{x_n}{x_{n+1}}\right)^2$$

Thus, $d \in D(V)$. If $x_{n+1} = 0$, then q is isotropic and hence universal. Again, we get $d \in D(V)$. □

Theorem 1.6.4. *Let q_1, q_2 be regular quadratic forms of positive dimensions over vector spaces V_1 and V_2 respectively. Then $q = q_1 \perp q_2$ is isotropic if and only if*

$$D(V_1) \cap -D(V_2) \neq \phi$$

Proof. Let

$$q_1 = d_1X_1^2 + \ldots + d_nX_n^2$$

and

$$q_2 = a_1Y_1^2 + \ldots + a_nY_n^2$$

If $q_1 \perp q_2$ is isotropic then, there exist vectors $x_i, y_i \in K$ such that

$$\sum_{i=1}^{n} d_i x_i^2 + \sum_{i=1}^{n} a_i y_i^2 = 0$$

We get

$$\sum_{i=1}^{n} d_i x_i^2 = -\sum_{i=1}^{n} a_i y_i^2$$

and therefore,

$$D(V_1) \cap -D(V_2) \neq \phi$$

Conversely, suppose there exists $a \in D(V_1) \cap -D(V_2), a \in K, a \neq 0$. Then, for some non-zero x and y, $q_1(x) = a$ and $q_2(y) = -a$. Thus,

$$q(x, y) = q_1(x) + q_2(y) = a - a = 0$$

Hence, q is isotropic. □

Corollary 1.6.5. *For a positive integer r, the following statements are equivalent over a field K:*

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

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

Proof. (1) $\Longrightarrow$ (2)
Let $q \perp \langle a \rangle, a \in \dot{K}$ be a quadratic form of dimension $r + 1$ corresponding to the quadratic space (V, B). If $q \perp \langle a \rangle$ is not regular then, there exists

$$0 \neq x \in \mathrm{rad}(q \perp \langle a \rangle)$$

and therefore, $q \perp \langle a \rangle$ is isotropic. If $q \perp \langle a \rangle$ is regular, then q is regular and hence universal. Therefore, $q(x) = -a$ for some vector x and thus $q \perp \langle a \rangle$ is isotropic.
(2) $\Longrightarrow$ (1)
The proof follows identically. □

1.7 Witt's Decomposition and Cancellation Theorem

Theorem 1.7.1 (Witt's Cancellation Theorem). *Let q, q_1 and q_2 be arbitrary quadratic spaces such that $q \perp q_1 \cong q \perp q_2$. Then $q_1 \cong q_2$.*

Proof. We may assume that the quadratic forms q, q_1 and q_2 are diagonalized (see [Pfi95]). Let

$$q = \langle a_1, a_2, \ldots, a_m \rangle$$

where m is the dimension of q and let $r(q)$ denote the rank of the corresponding matrix of q. Then, number of zeroes among a_i's is equal to $m - r(q)$. Since dimensions and ranks remain unchanged under isometries, we get $\dim(q_1) = \dim(q_2) = n$ and $r(q_1) = r(q_2)$. Assume that q_1 and q_2 are regular(if not, take out zeroes from q_1 and q_2 and attach them to q). Without loss of generality, we take $\dim(q) = 1$ and $q = \langle a \rangle, a \neq 0$. Then,

$$\langle a \rangle \perp q_1 \cong \langle a \rangle \perp q_2$$

Thus, there exists an $(n+1) \times (n+1)$ matrix T such that

$$(a \perp q_1)(TX) = (a \perp q_2)X$$

Let $X = \begin{pmatrix} x_0 \\ y \end{pmatrix}$ where $y \in K^n$ is a column vector and $T = \begin{pmatrix} t & u \\ v & B \end{pmatrix}$ where $v, u \in K^n, t \in K$ and $B \in M_n(K)$. Then

$$(a \oplus q_1) \begin{pmatrix} tx_0 + u.y \\ vx_0 + By \end{pmatrix} = (a \oplus q_2) \begin{pmatrix} x_0 \\ y \end{pmatrix}$$

$$\Rightarrow a(tx_0 + u.y)^2 + q_1(vx_0 + By) = ax_0^2 + q_2(y)$$

Since $\mathrm{char}(K) \neq 2$, we get

$$tx_0 + u.y = \pm x_0$$

Then, $x_0 = \dfrac{u.y}{\pm 1 - t} \in K$. Let $w = \dfrac{u}{\pm 1 - t}$. We get

$$q_1((v.w)y + By) = q_2(y)$$

$$q_1((v.w + B)y) = q_2(y)$$

$$\implies q_1 \cong q_2$$

□

Theorem 1.7.2 (**Witt's Decomposition Theorem**). *Let (V, q) be any quadratic space. Then V can be decomposed as*

$$V = V_t \perp V_h \perp V_a$$

where V_t is totally isotropic, V_h is hyperbolic and V_a is anisotropic. Moreover, the decomposition is unique upto isometry.

Proof. Write $V = \text{rad}(V) \perp V_0$. Then, $\text{rad}(V)$ is totally isotropic and V_0 is regular. If V_0 is isotropic then, $V_0 = H_1 \perp V_1$ where H_1 is hyperbolic. If V_1 is isotropic then, $V_1 = H_2 \perp V_2$ where H_2 is hyperbolic and so on. Thus, we arrive at

$$V_0 = H_1 \perp H_2 \perp \ldots \perp H_m \perp V_a$$

where V_a is anisotropic. We get $V = V_t \perp V_h \perp V_a$.
For uniqueness, we use Witt's Cancellation Theorem. Let $V = V_t' \perp V_h' \perp V_a'$. Since V_t' is totally isotropic and $V_h' \perp V_a'$ is regular,

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

$$\implies V_t' \cong V_t,\ V_h' \perp V_a' \cong V_h \perp V_a$$

Let $V_h' = m'H$ and $V_h = mH$. Then, $m' = m$ and we get $V_h' \cong V_h$ and $V_a' \cong V_a$. □

The index $m' = \dfrac{1}{2}(\dim(V_h))$ is called *Witt index* of V.

1.8 Witt Ring of a Field

We begin this section by introducing some notations.
Let $\phi = \langle a_1, a_2, \ldots, a_n \rangle$ and $\psi = \langle b_1, b_2, \ldots, b_m \rangle$ be quadratic forms over K. Then

1. $\phi \oplus \psi = \langle a_1, \ldots, a_n, b_1, \ldots, b_m \rangle$ is the *orthogonal sum* of ϕ and ψ.
2. $\phi \otimes \psi = \langle a_1 b_1, a_1 b_2, \ldots, a_i b_j, \ldots, a_n b_m \rangle$ is the product of ϕ and ψ.
3. $\alpha\phi = \langle \alpha a_1, \ldots, \alpha a_n \rangle$ for all $\alpha \in \dot{K}$.
4. For any $s \in \mathbb{N}$, $s \times \phi = \phi \oplus \phi \oplus \ldots \oplus \phi$, the sum being taken s times.

Let

$$\phi = i \times \langle 1, -1 \rangle \oplus \ \phi_0$$

and

$$\psi = j \times \langle 1, -1 \rangle \oplus \ \psi_0$$

be two regular quadratic forms over K, ϕ_0 and ψ_0 being the anisotropic parts of ϕ and ψ respectively (Such an orthogonal decomposition follows from Witt's Decomposition Theorem).
Quadratic Forms ϕ and ψ are called of the *same anisotropic type* if

$$\phi_0 \cong \psi_0$$

This relation is denoted by $\sim$ and is clearly an equivalence relation.
Let $S(K)$ denote the set of all finite dimensional regular quadratic forms over field K. Then, the *Witt ring of* K is defined as

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

the set of anisotropic classes of regular quadratic forms over K. Elements of $W(K)$ are called *Witt classes* and denoted by $\tilde{\phi}$. The operations of addition($\oplus$) and multiplication($\otimes$) are defined naturally for elements of $W(K)$.
Let $\tilde{\phi}$, $\tilde{\psi} \in W(K)$. Then, define

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

We have to check that the above relations are well-defined. For this, we make the following observations:

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

The second observation follows from

$$\langle 1,-1\rangle \otimes \langle a\rangle \;\cong\; \langle a,-a\rangle \;\cong\; \langle 1,-1\rangle$$

for every $a \in \dot{K}$. Thus, the relations $\oplus$ and $\otimes$ are well-defined.
It remains to show that $W(K)$ is a ring. It is clear that 0 is the additive identity and since $\langle\tilde{1}\rangle \otimes \phi \cong \phi$, it follows that $\langle\tilde{1}\rangle$ is the multiplicative identity.
Addition and multiplication are both commutative and associative. For a quadratic form

$$\tilde{\phi} = \langle a_1, \widetilde{a_2, \ldots, a_n}\rangle$$
$$-\tilde{\phi} = \langle -a_1, \widetilde{-a_2, \ldots, -a_n}\rangle$$

is the additive inverse since

$$\tilde{\phi} \oplus -\tilde{\phi} = \langle a_1, a_2, \ldots, a_n, \widetilde{-a_1}, -a_2, \ldots, -a_n\rangle$$

is isotropic. It remains to prove that multiplication is distributive.
Consider quadratic forms $\phi = \langle a_1, \widetilde{a_2, \ldots, a_n}\rangle$, $\psi = \langle b_1, \widetilde{b_2, \ldots, b_n}\rangle$ and $\chi = \langle c_1, \widetilde{c_2, \ldots, c_n}\rangle$. Then

$$\begin{aligned}
\phi \otimes \psi \oplus \chi &= \langle \widetilde{a_1, \ldots, a_n}\rangle \otimes \langle \widetilde{b_1, \ldots, b_n}\rangle \oplus \langle \widetilde{c_1, \ldots, c_n}\rangle \\
&= \langle \widetilde{a_1, \ldots, a_n}\rangle \otimes \langle b_1, \ldots, \widetilde{b_n, c_1}, \ldots, c_n\rangle \\
&= \langle \ldots, a_i \widetilde{b_j, \ldots, a_i c_l}, \ldots\rangle \\
&= \phi \otimes \psi \oplus \phi \otimes \chi
\end{aligned}$$

This proves that $W(K)$ is a commutative ring. The ring $W(K)$ is called the *Witt ring of field* K and if we ignore multiplication, then the additive group $W(K)$ is called the *Witt group of* K. We now compute Witt rings for some fields.

Theorem 1.8.1. *The following hold:*

1. $W(\mathbb{C}) = \dfrac{\mathbb{Z}}{2\mathbb{Z}}$
2. $W(\mathbb{R}) = \mathbb{Z}$
3. *Let* $K = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ *where* p *is an odd prime number. Then*

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

for $p \equiv 1 \ (mod\ 4)$ *and*

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

for $p \equiv 3 \ (mod\ 4)$

Proof. 1. Let $K = \mathbb{C}$. We know that $\mathbb{C}$ is algebraically closed. Hence, the group of square classes $\frac{\dot{\mathbb{C}}}{\dot{\mathbb{C}}^2}$ is trivial and so the only non-isometric anisotropic quadratic forms over $\mathbb{C}$ are 0 and $\langle 1 \rangle$. Thus, $W(\mathbb{C}) = \{\tilde{0}, \langle \tilde{1} \rangle\} = \frac{\mathbb{Z}}{2\mathbb{Z}}$.

2. Let $K = \mathbb{R}$. Then, the group

$$\frac{\dot{\mathbb{R}}}{\dot{\mathbb{R}}^2} = \{1, -1\}$$

Thus, the non-isometric anisotropic quadratic forms are of the type $n \times \langle 1 \rangle$ and $n \times \langle -1 \rangle$ for some $n \in \mathbb{N}$. As a result, $W(\mathbb{R}) = \mathbb{Z}$.

3. Let $K = \frac{\mathbb{Z}}{p\mathbb{Z}}$. We use the fact that for every odd prime p, there are $\left(\frac{p-1}{2}\right)$ quadratic residues and $\left(\frac{p-1}{2}\right)$ quadratic non-residues modulo p (see [Bur89]). Thus

$$\frac{\dot{\mathbb{Z}/p\mathbb{Z}}}{(\dot{\mathbb{Z}/p\mathbb{Z}})^2} = \{1, \epsilon\}$$

where ϵ is a quadratic non-residue modulo p. Therefore, the one-dimensional anisotropic quadratic forms are $\langle 1 \rangle$ and $\langle \epsilon \rangle$.
We now determine the anisotropic quadratic forms of dimension 2. Let $\phi = \langle a, b \rangle$ be a quadratic form of dimension 2. Then ϕ is anisotropic if for all $(x, y) \in K$,

$$ax^2 + by^2 \neq 0$$

$$b \neq -a\left(\frac{x^2}{y^2}\right)$$

i.e. b and $-a$ do not belong to the same square class. As a result, ϕ is isometric to a scalar multiple of $\langle 1, -\epsilon \rangle$.
Let $\phi_0 = \langle 1, -\epsilon \rangle$. Since the sets K^2 and $\epsilon - K^2$ have $\frac{p+1}{2}$ elements each, their intersection is non-empty. Therefore, there exist $c, d \in K$ such that

$$c^2 = \epsilon - d^2$$

Thus, we can write

$$\epsilon = \left(\frac{\epsilon}{d}\right)^2 - \epsilon\left(\frac{c}{d}\right)^2$$

Since ϕ_0 represents both 1 and ϵ, we get $D_K(\phi_o) = \dot{K}$ and therefore, every quadratic form q with $\dim(q) \geq 3$ is isotropic. We therefore get 4 non-isometric anisotropic quadratic forms

$$0, \langle 1\rangle, \langle \epsilon\rangle, \phi_0$$

For $p \equiv 1 \mod 4$, -1 is a square modulo p and thus

$$2\langle 1\rangle = \langle 1, 1\rangle \cong \langle 1, -1\rangle \sim 0$$

Therefore, every non-zero element has order 2 and so

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

For $p \equiv 3 \mod 4$, -1 is not a square modulo p and so

$$2\langle 1\rangle = \langle 1, 1\rangle$$

is anisotropic. Thus, every non-zero element has order 4 and we get

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

□

Chapter 2

Quadratic Forms under Field Extensions

In this chapter, we study the properties of isotropy and anisotropy of quadratic forms over field extensions. The main results of this chapter are Cassel-Pfister representation theorem and subform theorem. In §2, we use these theorems to obtain results on quadratic forms over quadratic extensions. Finally, in §3, we describe the function field of a quadratic form.

2.1 Quadratic forms under Rational function field

Let ϕ be a quadratic form over K and let L/K be a field extension. Then ϕ_L represents the quadratic form ϕ extended to L and $(\phi_L)_{an}$ denotes the anisotropic part of ϕ_L. A field extension L/K is called *excellent* if for every quadratic form ϕ over K, there exists a quadratic form ψ over K such that $(\phi_L)_{an}$ is isometric to ψ_L.

Theorem 2.1.1. *Let ϕ be an n-dimensional anisotropic quadratic form over K. Then, ϕ_L is anisotropic over $L = K(t)$, where $K(t)$ denotes the polynomial ring over K in one variable.*

Proof. Suppose ϕ_L is isotropic over L, then there exists $f = (f_1, f_2, \ldots, f_n) \in K(t)$ such that $\phi(f) = 0$. Let $f_i = \left(\frac{g_i}{g_0}\right)$ where g_0 is the common denominator, $g_0 \neq 0$. Let $g = (g_1, g_2, \ldots, g_n)$. Then

$$\phi(f) = \phi(g_1, g_2, \ldots, g_n)$$

$$\phi(g) = g_0^2.\phi(f) = 0$$

Let $d = \gcd(g_1, g_2, \ldots, g_n)$. Then, $g_i = dh_i$ where h_i's are relatively prime.

$$\phi(g) = d^2.\phi(h) = 0$$

Since $K(t)$ is an integral domain, we get $\phi(h) = 0$ where $h = (h_1, h_2, \ldots, h_n)$. Let $c_i = h_i(0)$ and $c = (c_1, c_2, \ldots, c_n)$. All c_i's cannot be zero since h_i's are relatively prime and $\gcd(h_1, h_2, \ldots, h_n) = 1$. We have

$$\phi(c) = \lim_{t \to 0} \phi(h(t)) = 0$$

This contradicts the statement that ϕ is anisotropic over K. Hence ϕ_L is anisotropic over L. □

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

Theorem 2.1.3. *Let ϕ be an n-ary regular isotropic quadratic form over K. Then ϕ represents every element of $K[t]$ over $K(t)$.*

Proof. Since ϕ is regular and isotropic over K, for $x = (x_1, x_2, \ldots, x_n)$, we can write

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

where ψ is another quadratic form over K. Then, for $p(t) \in K[t]$, taking $x_1 = 1/2, x_2 = p(t)$ and $x_3 = x_4 = \ldots = x_n = 0$, we get the result. □

Theorem 2.1.4 (Cassel-Pfister Representation Theorem). *Let ϕ be an n-ary quadratic form over K and let $p(t) \in K[t]$ be a non-zero polynomial. If ϕ represents $p(t)$ over the field $L = K(t)$, then ϕ represents $p(t)$ over the polynomial ring $K[t]$.*

Proof. We prove this result be induction on $\dim(\phi)$.
If $\dim(\phi) = 1$, then $\phi = \langle a \rangle, a \in \dot{K}$. There exists $f \in K(t)$ such that $af^2 = p(t)$. Since $K(t)$ is a unique factorization domain and $\left(\frac{p(t)}{a}\right) \in K[t]$, we get $f \in K[t]$.
Let the result hold for all quadratic forms q with $\dim(q) < n$. Let ϕ be a quadratic form of dimension n.

- Case 1 - ϕ is regular and isotropic. Then,

$$\phi = 2x_1x_2 + \langle x_3, \ldots, x_n \rangle, \ x_i \in \dot{K}$$

Taking $x_1 = p(t), x_2 = 1/2$ and $x_3 = x_4 = \ldots = x_n = 0$, we get $p(t) \in D_{K[t]}(\phi)$.

- Case 2 - ϕ is regular and anisotropic. Let

$$\phi\left(\frac{f_1}{f_0}, \frac{f_2}{f_0}, \ldots, \frac{f_n}{f_0}\right) = p(t),\ f_i \in K(t)$$

We choose f_i's such that f_0 is of minimal degree. We will prove the theorem by contradiction. Let d denote the degree of f_0. If $d = 0$, we are done.
Let $d > 0$. By Euclidean algorithm,

$$f_i = g_i f_0 + r_i$$

where $g_0 = 1, r_0 = 0$ and $\deg(r_i) < d$.
Let ψ denote the quadratic form $\langle -p(t) \rangle \oplus \phi$. Then for

$$f = (f_0, f_1, \ldots, f_n)$$

we get $\psi(f) = 0$. Let $g = (g_0, g_1, \ldots, g_n)$. Then, $\psi(g) \neq 0$ since $\deg(g_0) < d$. Let $h = \alpha f - \beta g$, where $\alpha = \psi(g)$ and $\beta = 2B_\psi(f, g)$. Then

$$\begin{aligned} \psi(h) &= \psi(\alpha f - \beta g) \\ &= \alpha^2\psi(f) + \beta^2\psi(g) - 2\alpha\beta B_\psi(f, g) \\ &= \alpha^2.0 + \beta^2\psi(g) - \psi(g)\beta^2 = 0 \end{aligned}$$

We have

$$h_0 = \alpha f_0 - \beta g_0 = \psi(g) f_0 - \beta$$

Then, $h_0 \neq 0$ since in such a case, $\phi(h_1, h_2, \ldots, h_n) = 0$ which implies that ϕ is isotropic, a contradiction. Therefore,

$$\begin{aligned} h_0 &= \psi(g) f_0 - 2B_\psi(f, g) \\ &= \frac{1}{f_0}(\psi(g) f_0^2 - f_0 2B_\psi(f, g)) \\ &= \frac{1}{f_0}(\psi(f_0 g) - f_0 2B_\psi(f, g)) \end{aligned}$$

$$= \frac{1}{f_0}(\psi(f_0 g) - 2B_\psi(f, gf_0))$$

$$= \frac{1}{f_0}(\psi(f) - 2B_\psi(f, gf_0) + \psi(gf_0))$$

$$= \frac{1}{f_0}(\psi(f - gf_0) + 2B_\psi(f, gf_0) - 2B_\psi(f, gf_0)) = \frac{1}{f_0}\psi(r)$$

As a result, we get

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

This gives a contradiction. Hence the result is proved.

□

Remark 2.1.5. If ϕ is isotropic and we take coefficients of ϕ from $K[t]$ of degree less than or equal to 1, then the theorem does not hold. For example, take $\phi = \langle t, -t\rangle$ and $p(t) = 1$. Then, ϕ is isotropic and hyperbolic but the equation $2tx_1x_2 = 1$ has no solution in $K[t]$.

The result cannot be generalized for several variables since the proof makes use of the fact that the polynomial ring is a Euclidean domain, however $K[t_1, t_2, \ldots, t_n]$ is not even a unique factorization domain. But we still have the following weaker result:

Theorem 2.1.6 (Substitution Principle). *Let ϕ be an n-ary quadratic form over K. If ϕ represents $p(x_1, x_2, \ldots, x_n) \in K[x_1, x_2, \ldots, x_n]$ over $K(x_1, x_2, ..., x_n)$, then for $c_1, c_2, \ldots, c_n \in K$, ϕ represents $p(c_1, c_2, \ldots, c_n)$ over K.*

Proof. We prove the result by induction on n.
For $n = 1$, the statement of the theorem says that ϕ represents $p(t_1)$ over $K(t_1)$. Then, ϕ represents $p(t_1)$ over $K[t_1]$ and taking $t_1 = c_1$, we get that ϕ represents $p(c_1)$ over K.
Let ϕ represent $p(t_1, t_2, \ldots, t_n)$ over $K(t_1, t_2, \ldots, t_n)$. Then ϕ represents $p(t_1, t_2, \ldots, t_n)$ over $K(t_1, t_2, \ldots, t_{n-1})[t_n]$. Taking $t_n = c_n$, we get that ϕ represents $p(t_1, t_2, \ldots, t_{n-1}, c_n)$ over $K(t_1, \ldots, t_{n-1})$. The result now follows from induction hypothesis. □

Theorem 2.1.7. *Let $d, a_1, a_2, \ldots, a_n \in \dot{K}$ and $\phi = \langle a_1, a_2, \ldots, a_n\rangle$. If $d + a_1t^2 \in D_{K(t)}(\phi)$ then either ϕ is isotropic over K or $d \in D_K(\phi')$, where $\phi' = \langle a_2, \ldots, a_n\rangle$.*

Proof. Suppose ϕ is anisotropic. Since $d + a_1t^2 \in D_{K(t)}(\phi)$, then by theorem 2.1.4, ϕ represents $d + a_1t^2$ over the ring $K[t]$. Hence, there exist $f_1, f_2, \ldots, f_n \in K[t]$ such

that

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

On comparing the degrees of polynomials on two sides of the equation, we infer that $\deg(f_i) \leq 1$. Let $f_i = b_i + c_i t$. Then

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

Since $\text{char}(K) \neq 2$, one of the above two equations certainly has a solution in K. Substituting $t = \dfrac{b_1}{\pm 1 - c_1}$, we get

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

This implies $d \in D_K(\phi')$. □

Corollary 2.1.8. *Let K be a field such that the n dimensional quadratic form $\phi = \langle 1, 1, \ldots, 1 \rangle$ is anisotropic over K, then $1 + t_1^2 + t_2^2 + \ldots + t_n^2$ is not a sum of n squares in the rational function field $K(t_1, t_2, \ldots, t_n)$.*

Proof. Suppose for $x_i \in K(t_1, t_2, \ldots, t_n)$,

$$1 + t_1^2 + t_2^2 + \ldots + t_n^2 = x_1^2 + x_2^2 + \ldots + x_n^2$$

Then, on applying theorem 2.1.7 $n - 1$ times, we arrive at the equation $x_n^2 = 1 + t_n^2$. This equation does not have a solution in K and this proves that our initial assumption was false. □

Let $\phi = \langle a_1, a_2, \ldots, a_n \rangle$ and $\psi = \langle b_1, b_2, \ldots, b_n \rangle$ be two quadratic form over a field K with $m \leq n$. Then ψ is called a *subform* of ϕ if ψ is isometric to an orthogonal summand of ϕ.

Theorem 2.1.9 (Subform Theorem). *Let $\phi = \langle a_1, a_2, \ldots, a_n \rangle$ and $\psi = \langle b_1, b_2, \ldots, b_n \rangle$ be two regular quadratic forms with $m \leq n$. If ϕ is anisotropic, then ψ is isometric to a subform of ϕ if and only if for every extension L over K, $D_L(\psi) \subseteq D_L(\phi)$.*

Proof. We prove the result by induction on $\dim(\psi) = m$. If $\psi = 0$, then there is nothing to prove.
Let ψ be isometric to a subform of ϕ. Then, $D_L(\psi) \subseteq D_L(\phi)$ for all extensions L/K.

Let for every extension L/K, $D_L(\psi) \subseteq D_L(\phi)$. Since $b_1 \in D_L(\psi)$ therefore $b_1 \in D_L(\phi)$. Hence, we can write $\phi = \langle b_1 \rangle \oplus \phi'$. Since ϕ is anisotropic, so is ϕ'. We have

$$D_L(\psi) \subseteq D_L(\phi)$$

Therefore,

$$D_L(\psi) \subseteq D_L(\langle b_1 \rangle \oplus \phi')$$

where

$$\psi = \langle b_1 \rangle \oplus \langle b_2, \ldots, b_n \rangle$$

As a result, $\psi' = \langle b_2, \ldots, b_m \rangle$ is represented by ϕ' over $K(t_2, \ldots, t_n)$. Now, we have $\dim(\psi') = m - 1$. By induction hypothesis,

$$\psi \cong \langle b_1 \rangle \oplus \phi' \cong \langle b_1 \rangle \oplus \psi' \oplus \chi \cong \psi \oplus \chi$$

This proves the theorem. □

2.1.1 Quadratic Extensions

Throughout this section, L refers to the field extension $K(\sqrt{a})/K$ where $a \in \dfrac{\dot{K}}{\dot{K}^2}$ and θ is the quadratic form $\langle 1, -a \rangle$. Note that θ is isotropic over L but not over K.

Theorem 2.1.10. *Let $L = K(\sqrt{a})$ be a field extension where $a \in \dfrac{\dot{K}}{\dot{K}^2}$ and θ be the quadratic form as above. Let $\psi = \langle a_1, a_2, \ldots, a_n \rangle$ be a quadratic form which is anisotropic over K. Then ψ_L is isotropic if and only if ψ has a binary subform isometric to $\lambda\theta$ for some $\lambda \in \dot{K}$.*

Proof. Suppose ψ has a binary subform isometric to $\lambda\theta$ for some $\lambda \in \dot{K}$. Then

$$\psi \cong \lambda\theta \oplus \chi \cong \lambda\langle 1, -a \rangle \oplus \chi \cong \langle \lambda, -a\lambda \rangle \oplus \chi$$

The form $\langle \lambda, -a\lambda \rangle$ is isotropic over L and so ψ_L is isotropic.
Conversely, suppose ψ_L is isotropic. Let

$$(x_1 + \sqrt{a}y_1, x_2 + \sqrt{a}y_2, \ldots, x_n + \sqrt{a}y_n) \neq 0$$

be an isotropic vector. Then

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

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

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

We get $\psi(x) = -a\psi(y)$ and $b_\psi(x, y) = 0$. Since ψ is anisotropic over K, therefore $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ are both non-zero. Now, consider the regular quadratic form $\langle\psi(x), \psi(y)\rangle = \gamma$. Since $D_L(\gamma) \subseteq D_L(\psi)$ for all extensions L/K, using subform theorem, we get that γ is isometric to a subform of ψ. Thus,

$$\gamma = \langle\psi(x), \psi(y)\rangle = \langle -a\psi(y), \psi(y)\rangle = \psi(y)\langle 1, -a\rangle = \psi(y)\theta$$

where $\psi(y) \in K$. This proves the theorem with $\lambda = \psi(y)$. □

Theorem 2.1.11. *Let L and θ be as in previous theorem. An anisotropic K-form ϕ becomes hyperbolic over L if and only if $\phi \cong \psi \otimes \theta$ for some K-form ψ.*

Proof. The 'if' part is trivial. We prove the converse by induction on $m = \dfrac{\dim(\phi)}{2}$. For $m = 0$, the result is true. If $m > 0$ and ϕ becomes isotropic over L then by Theorem 2.1.10,

$$\phi \cong \lambda\theta \oplus \phi'$$

where $\dim(\phi') = 2(m-1)$. Now applying Witt's Cancellation theorem, we get $\phi' \cong (m-1) \times \langle 1, -1\rangle$. By induction hypothesis, $\phi' \cong \psi' \otimes \theta$ for some K-form ψ'. Hence we get

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

where ψ is a K-form. □

Corollary 2.1.12. *For any anisotropic form ϕ over K, there exists a form ψ_K such that anisotropic part of ϕ_L is isometric to ψ_L i.e. L/K is excellent.*

Proof. Let ϕ be an anisotropic quadratic form over K. If ϕ_L remains anisotropic over L, then the result is true. Suppose ϕ becomes isotropic over L and

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

be the Witt decomposition of ϕ_L. By theorem 2.8, we have an orthogonal decomposition

$$\phi_K \cong (q \otimes \theta) \oplus \psi$$

for some quadratic forms q and ψ over K, $\dim(q) = i$ and θ is the quadratic form given in the previous theorem. Hence we have

$$\phi_L \cong ((q \otimes \theta) \oplus \psi)_L$$

$$\cong (q \otimes \theta)_L \oplus \psi_L$$

$$\cong i \times \langle 1, -1 \rangle \oplus \psi_L$$

which is possible if and only if

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

Hence from the Witt Cancellation theorem, it follows that

$$(\phi_L)_{an} \cong \psi_L$$

□

2.2 Function Field of a Quadratic Form

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

$$K(\phi) = K(x_2, \ldots, x_n)\left(\sqrt{\frac{-(a_2x_2^2 + \ldots + a_nx_n^2)}{a_1}}\right)$$

Basically, the function field of a quadratic form is the field over which the form becomes isotropic.

Theorem 2.2.1. *Let ϕ and ψ be quadratic forms over K. If ψ represents 1 and ψ becomes hyperbolic over $K(\phi)$ then $\phi(X)\psi \cong \psi$, where $X = (x_1, x_2, \ldots, x_n)$.*

Proof. As ϕ represents 1, we can write $\phi \cong \langle 1 \rangle \oplus \phi'$. Let

$$L = K(\phi) = K'(\sqrt{-\phi'(X')})$$

where $X' = (x_2, \ldots, x_n)$ and $K' = K(X')$. Since ψ is anisotropic over K, $\psi_{K'}$ is also anisotropic. As ψ_L is hyperbolic, it follows from Theorem 2.1.11 that $\psi_{K'} \cong \rho \otimes \langle 1, \phi'(X')\rangle$ over K', where ρ is a quadratic form over K'. The form $\langle 1, \phi'(X')\rangle$ represents $\phi(X)$ over $K(X)$. By applying subform theorem we get

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

Hence, the result is proved. □

Chapter 3

Pfister Forms

This chapter gives an introduction to Pfister forms which form a major part of our study. In §1, we define multiplicative and strictly multiplicative quadratic forms. In §2, we determine the conditions under which the Pfister forms become multiplicative or strictly multiplicative. Subsequently, we study important results on isotropy and hyperbolicity of Pfister forms.

3.1 Multiplicative Forms

An n-ary quadratic form ϕ over K is said to be *multiplicative* if for indeterminate vectors $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ there exists a vector $z = (z_1, z_2, \ldots, z_n)$ with $z_i \in K(x, y)$ such that $\phi(x)\phi(y) = \phi(z)$.

Theorem 3.1.1. *A regular quadratic form ϕ over K is multiplicative if and only if $D(\dot{\phi}_L)$ is a subgroup of $\dot{L}$ for every extension L over K.*

Proof. Let $D(\dot{\phi}_L)$ be a subgroup of $\dot{L}$ for every extension L/K. Then for $a, b \in D(\dot{\phi}_L)$, $ab \in D(\dot{\phi}_L)$ i.e. if there exist u and v in L for which $\phi_L(u) = a$ and $\phi_L(v) = b$ then there exists $w \in L$ such that $\phi_L(w) = ab$.

$$\implies \phi_L(u)\phi_L(v) = \phi_L(w)$$

Hence ϕ is multiplicative.
Conversely, let ϕ be multiplicative. This implies that for indeterminate column vectors x and y, ϕ represents $\phi(x)\phi(y)$ over $K(x, y)$. Since $K \subseteq L$, therefore ϕ represents $\phi(x)\phi(y)$ over $L(x, y)$. By Substitution principle, there exist $u, v \in L$ such that ϕ

represents $\phi(u)\phi(v)$ over L. Thus, for $a, b \in D(\phi_L)$, $ab \in D(\phi_L)$. Also, if $a \in D(\phi_L)$ and $\phi(u) = a$ for $u \in L$, then

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

This implies that $\frac{1}{a} \in D(\phi_L)$.
Hence, we infer that $D(\dot{\phi_L})$ is a subgroup of $\dot{L}$. □

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

$$\phi(x)\phi(y) = \phi(z) = \phi(T_x y)$$

In matrix notation, if A is the matrix associated to ϕ, then

$$\phi(x)y^t Ay = (T_x y)^t A(T_x y)$$

$$y^t \phi(x) Ay = y^t T_x^t A T_x y$$

$$\implies \phi(x)A = T_x^t A T_x$$

Examples

1. The one dimensional quadratic form x^2 is strictly multiplicative. Here $A = (1)$ and $T_x = x$. For $z = T_x(y) = xy$,

$$\phi(z) = (xy)^2 = z^2 = \phi(x)\phi(y)$$

2. The two-dimensional quadratic form $\phi(x) = x_1^2 + x_2^2$ is strictly multiplicative. Taking $x = (x_1, x_2)$, $y = (y_1, y_2)$, we get

$$\phi(x)\phi(y) = (x_1^2 + x_2^2)(y_1^2 + y_2^2)$$

$$= x_1^2y_1^2 + x_1^2y_2^2 + x_2^2y_1^2 + x_2^2y_2^2$$

$$= x_1^2y_1^2 + x_2^2y_2^2 + 2x_1x_2y_1y_2 + x_1^2y_2^2 + x_2^2y_1^2 - 2x_1x_2y_1y_2$$

$$= (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2$$

Let $z = (x_1y_1 + x_2y_2, x_1y_2 - x_2y_1)$. Then for $T_x = \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix}$,

$$\phi(z) = \phi(T_x y) = \phi(x)\phi(y)$$

3.2 Pfister Forms

For $a_1, a_2, \ldots, a_n \in \dot{K}, n \in \mathbb{N}$, the 2^n dimensional quadratic form

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

is called a *Pfister Form*. It is denoted by $\langle\langle a_1, a_2, \ldots, a_n \rangle\rangle$.

Theorem 3.2.1. *The Pfister form $\langle\langle a_1, a_2, \ldots, a_n \rangle\rangle, n \geq 0$ with $a_i \in \dot{K}$ is strictly multiplicative over K.*

Proof. We proceed by induction on n. For $n = 0$, we have $\phi = \langle 1 \rangle$. Then, $A = (1)$ and $T_x = x$ does the job.
Let the result be true for $\phi = \langle 1, a_1 \rangle \otimes \ldots \otimes \langle 1, a_n \rangle$.
Let

$$\psi = \langle 1, a \rangle \otimes \phi = \langle \phi, \phi a \rangle = \phi \oplus a\phi$$

Let A be the matrix associated with ϕ. Since ϕ is strictly multiplicative, we have $\phi(x)\phi = \phi$. Therefore,

$$\psi = \phi(x)\phi \oplus a\phi(y)\phi$$

$$= \langle \phi(x)\phi, a\phi(y)\phi \rangle$$

The matrix associated with ψ is $B = \begin{pmatrix} A & 0 \\ 0 & aA \end{pmatrix}$ and

$$\psi(x, y) = \begin{pmatrix} x^t & y^t \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & aA \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \phi(x) + a\phi(y)$$

Since $\langle \phi(x), a\phi(y) \rangle$ represents $\psi(x, y)$ over K, so we have

$$\langle \phi(x), a\phi(y) \rangle \cong \langle \psi(x, y), \psi(x, y)\phi(x)a\phi(y) \rangle \cong \psi(x, y)\langle 1, a\phi(x)\phi(y) \rangle$$

Using

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

we get

$$\psi \cong \psi(x,y) \otimes \langle 1, a\phi(x)\phi(y)\rangle \otimes \phi$$

$$\cong \psi(x,y) \otimes \langle \phi, a\phi(x)\phi(y)\phi\rangle$$

$$\cong \psi(x,y) \otimes \langle \phi, a\phi\rangle \cong \psi(x,y)\psi$$

Thus, ψ is strictly multiplicative. □

Theorem 3.2.2. *Let ϕ be an n-ary regular anisotropic quadratic form over K. The following are equivalent:*

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

Proof. $(1 \implies 2)$
Since ϕ is multiplicative, ϕ represents $\phi(x)\phi(y)$ over $K(x,y)$ where $x, y \in K^n$. Therefore, $D(\phi(x)\phi) \subseteq D(\phi)$. Since ϕ is anisotropic over K, by subform theorem $\phi(x)\phi$ is isometric to a subform of ϕ. But $\dim(\phi(x)\phi) = \dim(\phi)$. Hence, $\phi(x)\phi \cong \phi$ and therefore ϕ is strictly multiplicative.
$(2 \implies 3)$
Let ϕ be strictly multiplicative and let

$$\psi = \langle\langle a_1, a_2, \ldots, a_k\rangle\rangle$$

be the maximal Pfister form contained in ϕ. We have to show that $\phi \cong \psi$.
Let $\phi = \psi \oplus \chi$ where $\dim(\chi) \geq 1$. Let $\chi \cong \langle b, \ldots\rangle$ where $b \in \dot{K}$. Since ϕ is strictly multiplicative, we have $\phi(x)\phi \cong \phi$ over $K(x)$.
Let $x = (z, 0, \ldots, 0)$ where z is a non zero element in K^{2^k} and there are $n - 2^k$ zeroes. Then $\psi(z)\phi \cong \phi$. Using the fact that Pfister forms are strictly multiplicative, we get

$$\psi \oplus \chi \cong \phi \cong \psi(z)\phi \cong \psi(z)(\psi \oplus \chi) \cong \psi(z)\psi \oplus \psi(z)\chi \cong \psi \oplus \psi(z)\chi$$

By Witt's Cancellation theorem, $\chi \cong \psi(z)\chi$. Since χ represents b over K, it represents $b\chi(z)$ over $K(z)$. So $D_{K(z)}(b\chi) \subseteq D_{K(z)}(\chi)$. Since χ is anisotropic, by subform theorem $b\chi$ is isometric to a subform of χ. Therefore, $\chi \cong b\psi \oplus \chi'$, where χ' is a

quadratic form. Hence

$$\phi \cong \psi \oplus \chi \cong \psi \oplus b\psi \oplus \chi' \cong \psi \otimes < 1, b > \oplus \chi'$$

which is a contradiction since ψ was the maximal Pfister form contained in ϕ. This contradiction arises because we assumed that $\dim(\chi) \geq 1$. Thus, $\phi \cong \psi$ and ϕ is a Pfister form.
$(3 \Longrightarrow 1)$
Every Pfister form is strictly multiplicative by theorem 3.2.1 and every strictly multiplicative form is multiplicative. □

We observe that every n-ary regular isotropic form ϕ over field K is multiplicative since ϕ, being isotropic is universal and so $D_K(\phi) = \dot{K}$.

Theorem 3.2.3. *An n-ary regular isotropic quadratic form ϕ over K is strictly multiplicative if and only if*

$$\phi \cong i \times \langle 1, -1 \rangle, i \in \mathbb{N}$$

Proof. Let ϕ be a regular isotropic quadratic form which is strictly multiplicative and let

$$\phi = i \times \langle 1, -1 \rangle \oplus \phi_0$$

be the Witt decomposition of ϕ where $0 \neq \phi_0$ is the anisotropic part of ϕ and $\dim(\phi_0) \geq 1$. Since ϕ is strictly multiplicative, $\phi \cong \phi(x)\phi$ over $K(x)$. Therefore,

$$i \times \langle 1, -1 \rangle \oplus \phi_0 \cong \phi(x)(i \times \langle 1, -1 \rangle \oplus \phi_0) \cong i \times \phi(x)\langle 1, -1 \rangle \oplus \phi(x)\phi_0$$

Since $\langle 1, -1 \rangle \cong \phi(x)\langle 1, -1 \rangle$, using Witt's Cancellation theorem, we get $\phi_0 \cong \phi(x)\phi_0$. Let $\phi_0 = \langle b, \ldots \rangle$ where $b \in \dot{K}$. Then, ϕ_0 is anisotropic and since $D_K(b\phi) \subseteq D_K(\phi_0)$ using subform theorem, we get that $b\phi$ is a subform of ϕ_0. This gives a contradiction since by assumption, $\dim(\phi) > \dim(\phi_0)$. Thus, we get $\phi_0 = 0$ and $\phi \cong i \times \langle 1, -1 \rangle$.
Conversely, let $\phi \cong i \times \langle 1, -1 \rangle$. Since $\langle 1, -1 \rangle \cong \phi(x)\langle 1, -1 \rangle$, $\phi(x)\phi \cong \phi$ over $K(x)$ and so $\phi(x)$ is strictly multiplicative. □

Theorem 3.2.4. *Let ϕ be a quadratic form over K. Then, ϕ is isometric to an n-fold Pfister form if and only if $dim(\phi) = 2^n$ and for every field extension L/K, ϕ_L is either anisotropic or hyperbolic.*

Proof. Let ϕ be a Pfister form. Then, $\dim(\phi) = 2^n,\ n \in \mathbb{N}$ and let L/K be a field extension. If ϕ_L is anisotropic, we are done. If ϕ_L is isotropic, then ϕ being a Pfister

form is strictly multiplicative and hence it is hyperbolic.
Conversely, let $\dim(\phi) = 2^n$ and for every field extension L/K, ϕ is either hyperbolic or anisotropic. If ϕ is hyperbolic, we are done. Let ϕ be anisotropic. Then, for $L = K(\phi)$, ϕ is isotropic over L and hence hyperbolic. So $\phi(x)\phi \cong \phi$ over the rational function field $K(x)$. Since ϕ is strictly multiplicative and anisotropic over K, by theorem 3.2.2, ϕ is a Pfister form. □

Chapter 4

Galois Cohomology

In this chapter, we define the cohomology groups obtained by the action of a group G on a set A. This set can either be a group or a module. In many cases, the group G will be a Galois group. For a subgroup H of the group G, we define inflation, restriction and corestriction maps. Subsequently, we define cup-products of elements of cohomology groups which give us higher cohomology groups.

4.1 Introduction

Let G be a group acting on a set A. For an element $a \in A$ and $g \in G$ we denote by ${}^g a$ or $g.a$, the element of A obtained by the action of g on a. Thus, we have a map

$$f : G \times A \to A$$

where $f(g, a) = {}^g a = g.a$. Such a set A is called a *G-set* since G acts on this set. If the G-set A has the structure of a group and if the action of G respects the group structure of A, then A is called a *G-group*. Therefore, in a G-group we have

$${}^g(ab) = {}^g a \, {}^g b \; \forall \; a, b \in A, g \in G$$

Let G be a set and A be a group. Then with notations as above, we define

$$H^0(G, A) = A^G = \{a \in A : {}^g a = a \; \forall \; g \in G\}$$

The set $H^0(G, A)$ is therefore equal to the stabilizer of A in G. Now, we define the first cohomology set $H^1(G, A)$. Before that, we need to introduce few more objects. A 1-*cocycle* of G into A is a map $f : G \to A$ such that

$$f(st) = f(s)s.f(t) \ \forall \ s, t \in G$$

where $s.f(t)$ denotes the action of s on $f(t)$. The set of 1-cocycles is denoted by $Z^1(G, A)$. We can define an equivalence relation on $Z^1(G, A)$. Two 1-cocycles f and g are said to be *equivalent* if there exists $c \in A$ such that

$$g(s) = c^{-1} f(s)s.c \ \forall \ s \in G$$

This is indeed an equivalence relation and divides $Z^1(G, A)$ into equivalence classes. This set of equivalence classes is defined to be the *first cohomology set* $H^1(G, A)$. Alternatively, we can define another set $B^1(G, A)$ as the set of elements of $Z^1(G, A)$ which are equivalent to the trivial map i.e. the map $\theta \in Z^1(G, A)$ which takes every element of G to identity in A. Such elements are called 1-*coboundaries of* G *in* A. If A is Abelian, then both $Z^1(G, A)$ and $B^1(G, A)$ are groups. In fact, $B^1(G, A)$ becomes a normal subgroup of $Z^1(G, A)$. In such case, $H^1(G, A)$ is the quotient group

$$H^1(G, A) = \frac{Z^1(G, A)}{B^1(G, A)}$$

Given groups A and B and sets G and H with maps $\alpha : A \to B$ and $\beta : H \to G$ we can define a map

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

as

$$\theta(f) = \alpha \circ f \circ \beta$$

In such a case, the maps α and β are said to be *compatible*.

Now we define the cohomology sets associated with a Galois extension. Let k be a field and k_s be the separable closure of k. Let Γ_k denote the Galois group of the extension k_s/k. Let A be any group with discrete topology on which Γ_k acts continuously. Then, we define

$$H^0(k, A) = H^0(\Gamma_k, A) = A^{\Gamma_k}$$

Similarly we define

$$Z^1(k, A) = Z^1(\Gamma_k, A),\ B^1(k, A) = B^1(\Gamma_k, A)$$

and

$$H^1(k, A) = H^1(\Gamma_k, A)$$

Here $H^1(k, A)$ is called the *first cohomology set of* Γ_k *with values in* A . The definitions of $H^0(k, A)$ and $H^1(k, A)$ make sense for finite Galois extensions as well. In fact, we have

$$H^1(k, A) = \lim_{\to K}(H^1(\Gamma_{K/k}, A^{\Gamma_k}))$$

where K runs over finite Galois extensions of k and $\Gamma_{K/k}$ denotes the Galois group associated with the extension K/k. The set $Z^1(k, A)$ consists of an element f where $f : \Gamma_k \to A$ is such that $f(s) = 1 \in A$ for all $s \in \Gamma_k$. Such an f is called the *distinguished element* of $Z^1(k, A)$ and its cocycle class is the *distinguished element* of $H^1(k, A)$ denoted by 1. Therefore, $Z^1(k, A)$ is a *pointed set* .

For an Abelian group A, we define the *second cohomology group* $H^2(k, A)$.
A *normailzed* 2*-cocycle* of Γ_k with values in A is a continuous map

$$f : \Gamma_k \times \Gamma_k \to A$$

such that $f(1, 1) = 1$ and for $s_1, s_2, s_3 \in \Gamma_k$,

$$s_1.(f(s_2, s_3))f(s_1s_2, s_3)^{-1}f(s_1, s_2s_3)f(s_1, s_2)^{-1} = 1$$

A *normalized* 2*-coboundary* of Γ_k with values in A is a continuous map

$$\delta h : \Gamma_k \times \Gamma_k \to A$$

for which there exists a 1-cocycle $h : \Gamma_k \to A$ such that

$$\delta h(s, t) = s.(h(t))h(st)^{-1}h(s)\ \forall\ s, t \in \Gamma_k$$

Note that every 2-coboundary is a 2-cocycle (The statement holds only if h is a 1-cocycle and A is Abelian). The 2-cocycles form an Abelian group under the operation

$$(f + g)(s_1, s_2) = f(s_1, s_2)g(s_1, s_2)$$

where $s_1, s_2 \in \Gamma_k$. The group of 2-cocycles is denoted by $Z^2(k, A)$ and the 2-coboundaries form a normal subgroup of $Z^2(k, A)$ denoted by $B^2(k, A)$. The quotient $\dfrac{Z^2(k, A)}{B^2(k, A)}$ is called the *second cohomology group of* Γ_k *with values in* A and is denoted by $H^2(k, A)$.

4.2 Exact sequences of cohomology groups

A *morphism* of pointed sets A and B with distinguished elements a and b respectively is a set-theoretic map $\alpha : A \to B$ such that $\alpha(a) = b$. Then we have

$$\ker(\alpha) = \{x \in A \ : \ \alpha(x) = b\}$$

Let C be a pointed set with distinguished element c. Then the sequence

$$A \ \stackrel{\alpha}{\to} \ B \ \stackrel{\beta}{\to} \ C$$

is *exact* if $\text{img}(\alpha) = \ker(\beta)$ where $\text{img}(\alpha) = \{b \in B : b = \alpha(a), a \in A\}$. The exactness of the sequence

$$B \ \stackrel{\beta}{\to} \ C \ \stackrel{\gamma}{\to} \ 1$$

implies $\text{img}(\beta) = \ker(\gamma)$ i.e. $\text{img}(\beta) = C$ which is equivalent to β being surjective. The exactness of the sequence

$$1 \ \stackrel{\gamma}{\to} \ A \ \stackrel{\beta}{\to} \ B$$

implies $\text{img}(\gamma) = \ker(\beta) = a$.

Let B be a Γ_k-group i.e. Γ_k acts on the group B and let A be a Γ_k-subgroup of B. We consider A and B as pointed sets with their group identities acting as distinguished elements. The set $\dfrac{B}{A}$ of left cosets of A in B is a pointed Γ_k-set with induced action. Let S^{Γ_k} denote the set of fixed points of S under action from group Γ_k. The image of B^{Γ_k} under the map $B \to \dfrac{B}{A}$ is $\left(\dfrac{B}{A}\right)^{\Gamma_k}$. We define a map $\delta_0 : \left(\dfrac{B}{A}\right)^{\Gamma_k} \to H^1(k, A)$ as follows:

For $bA \in \left(\dfrac{B}{A}\right)^{\Gamma_k}$, we set $\delta_0(bA) = [f]$ where $f \in H^1(k, A)$ is the map $f(s) = b^{-1}s.b$ for $s \in \Gamma_k$ and $s.b$ denoting the action of s on b. We first show that $f \in Z^1(k, A)$.

$$f(st) = b^{-1}st.b = b^{-1}s.bs.b^{-1}st.(b) = b^{-1}s.bs.b^{-1}t.b = f(s)s.f(t)$$

Thus, f is indeed a cocycle. The image of the coset $bA \in \left(\frac{B}{A}\right)^{\Gamma_k}$ is class of $f \in H^1(k, A)$. The map f depends only on b, thus bA gives an equivalence class in $Z^1(k, A)$. Let $f = \delta_0(b)$ and $g = \delta_0(c)$ in $H^1(k, A)$ be such that $f \sim g$ i.e. f and g differ by a coboundary. Then, there exists $a \in A$ such that

$$f(s) = a^{-1}g(s)s.a = a^{-1}c^{-1}s.c\ s.a = (ca)^{-1}s.ca$$

Thus, we get that $b = ca$ i.e. b and c belong to the same coset of A in B.

Theorem 4.2.1. *The following sequence of pointed sets is exact:*

$$1 \xrightarrow{\alpha} A^{\Gamma_k} \xrightarrow{i} B^{\Gamma_k} \xrightarrow{\pi} \left(\frac{B}{A}\right)^{\Gamma_k} \xrightarrow{\delta_0} H^1(k, A) \xrightarrow{\gamma} H^1(k, B)$$

Proof. 1. Exactness at A^{Γ_k} - We know that $\text{img}(\alpha) = a$ and

$$ker(i) = \{x \in A^{\Gamma_k} \ : \ i(x) = a\}$$

Since A^{Γ_k} is a subset of B^{Γ_k}, the map i is injective and $\ker(i) = a$. Thus $\text{img}(\alpha) = \ker(i)$.

2. Exactness at B^{Γ_k} - Since i is injective, $\text{img}(i) = A^{\Gamma_k}$. The map π is the projection map and $\ker(\pi)$ contains those elements in B^{Γ_k} which belong to A and are fixed by Γ_k. Thus $\text{img}(i) = \ker(\pi)$.

3. Exactness at $\left(\frac{B}{A}\right)^{\Gamma_k}$ - Let $bA \in \ker(\delta_0)$. Then $\delta_0(bA)$ is the trivial cocycle of $Z^1(k, A)$. This implies that there exists $a \in A$ such that for all $s \in \Gamma_k$

$$b^{-1}s.b = a^{-1}s.a$$

$$s.b\ (s.a)^{-1} = ba^{-1}$$

$$s.(ba)^{-1} = ba^{-1}$$

Thus, $ba^{-1} \in B^{\Gamma_k}$. The element $ba^{-1} \in B^{\Gamma_k}$ maps to the coset $bA \in \left(\frac{B}{A}\right)^{\Gamma_k}$. Thus, $bA \in \text{img}(\pi)$. We get $\ker(\delta_0) \subseteq \text{img}(\pi)$. The reverse inclusion is trivial. Hence, $\ker(\delta_0) = \text{img}(\pi)$.

4. Exactness at $H^1(k, A)$ - Let $f \in H^1(k, A)$ be such that $f \in \ker(\gamma)$. Then there exists $b \in B$ such that $f(s) = b^{-1}s.b \in A$ for all $s \in \Gamma_k$. This implies that $bA = (s.b)A$ for all $s \in \Gamma_k$. Thus, $bA \in \left(\frac{B}{A}\right)^{\Gamma_k}$ and $\delta_0(bA)$ is the class of f in $H^1(k, A)$. This proves the exactness at $H^1(k, A)$.

□

If A is a normal subgroup of B then the quotient group $\frac{B}{A}$ is also a Γ_k group. Let $C = \frac{B}{A}$. The above result can then be extended as:

Theorem 4.2.2. *The following sequence is exact:*

$$1 \xrightarrow{\alpha} A^{\Gamma_k} \xrightarrow{i} B^{\Gamma_k} \xrightarrow{\pi} C^{\Gamma_k} \xrightarrow{\delta_0} H^1(k, A) \xrightarrow{\gamma} H^1(k, B) \xrightarrow{\beta} H^1(k, C)$$

Proof. We have to establish exactness at $H^1(k, B)$. Let $f \in Ker(\beta)$. This implies that there exists $c \in C$ such that $f(s) = c^{-1}s.c \in A$ for all $s \in \Gamma_k$. Consider

$$f : \Gamma_k \to A$$

given by $f(s) = c^{-1}s.c$. Then, $f \in \text{img}(\alpha)$. Thus $\ker(\beta) = \text{img}(\alpha)$. □

If A is the central subgroup of B then we can define $H^2(k, A)$ and a map

$$\delta_1 : H^1(k, C) \to H^2(k, A)$$

Let $h \in Z^1(k, C)$. Since $\pi : B \to \frac{B}{A} = C$ is the projection map, we can choose a map $\beta : \Gamma_k \to B$ such that $h(s) \in C$ is the image of $\beta(s) \in B$ under π. Then, we define

$$\gamma : \Gamma_k \times \Gamma_k \to A$$

as $\gamma(s, t) = \beta_s s.\beta_t \beta_{st}^{-1}$. It is trivial to check that γ is a 2-cocycle of Γ_k with values in A. We then define $\delta_1([h]) =$ class of γ in $H^2(k, A)$ where $[h]$ denotes the class of h in $H^1(k, C)$. Note that the class of γ does not depend on the choice of β.

Theorem 4.2.3. *The following sequence is exact:*

$$1 \to A^{\Gamma_k} \to B^{\Gamma_k} \to C^{\Gamma_k} \xrightarrow{\delta_0} H^1(k, A) \to H^1(k, B) \to H^1(k, C) \xrightarrow{\delta_1} H^2(k, A)$$

where A is a central subgroup of B and $C = \frac{B}{A}$.

Proof. In view of Proposition 4.2.2, we only need to check exactness at $H^1(k, C)$. Let $[h] \in Ker(\delta_1)$. Then $\delta_1([h])$ = trivial class in $H^2(k, A)$. From previous statements, we know that $\delta_1([h])$ is the class of γ in $H^2(k, A)$ where

$$\gamma(s, t) = \beta_s s.(\beta_t)\beta_{st}^{-1}$$

for $\beta \in Z^1(k, B)$. Since $[h] \in Ker(\delta_1)$, we have

$$\gamma(s, t) = s(\alpha_t)\alpha(st)^{-1}\alpha(s)$$

for some $\alpha : \Gamma_k \to A$. Thus $\beta_s\alpha_s^{-1}$ is an element of $Z^1(k, B)$. We know that $\pi(\beta(s)) = h(s)$. Since $\alpha(s)$ takes values in A, therefore $\beta(s)\alpha(s)^{-1}$ is equivalent to $h(s)$ as elements of $Z^1(k, C)$. Thus, there exists $a \in C$ such that

$$\beta(s)\alpha(s)^{-1} = a^{-1}h(s)s.a \ \forall \ s \in \Gamma_k$$

Hence, $\beta(s)\alpha(s)^{-1}$ and $h(s)$ belong to the same coset of B in A. This proves the exactness at $H^1(k, C)$. □

4.3 Hilbert Theorem 90

Let K be a finite Galois extension of k and let $\Gamma_{K/k}$ be the Galois group. The multiplicative group $\dot{K}$ is a $\Gamma_{K/k}$-group with action defined as

$$s.a = s(a) \ \forall \ s \in \Gamma_{K/k}, a \in \dot{K}$$

Theorem 4.3.1. *For K, k and $\Gamma_{K/k}$ as above, $H^1(\Gamma_{K/k}, \dot{K}) = 1$.*

Proof. We want to show that every 1-cocycle $a : \Gamma_{K/k} \to \dot{K}$ is a coboundary i.e. a is equivalent to the trivial cocycle.
Let $a : \Gamma_{K/k} \to \dot{K}$ be a cocycle. By Dedekind's theorem (see 2.12, [Mor96]), $\Gamma_{K/k}$ is linearly independent over K. Thus $\sum_{s\in\Gamma_{K/k}} a(s)s \neq 0$ since $a \neq 0$. This implies that there exist $\alpha, \beta \in \dot{K}$ such that $\sum_{s\in\Gamma_{K/k}} a(s)s(\alpha) = \beta$. For any $t \in \Gamma_{K/k}$, we have

$$\sum t(a(s)s(\alpha)) = t(\beta)$$

$$\sum t(a(s))ts(\alpha) = t(\beta)$$

Since a is a cocycle, we have $a(ts) = a(t)t(a(s))$. Thus $t(a(s)) = a(t)^{-1}a(ts)$. Therefore, we get

$$\sum_{s\in\Gamma_{K/k}} a(t)^{-1}a(ts)ts(\alpha) = t(\beta)$$

$$a(t)^{-1}\sum_{s\in\Gamma_{K/k}} a(ts)ts(\alpha) = t(\beta)$$

$$a(t)^{-1}\beta = t(\beta)$$

$$a(t) = \beta t(\beta)^{-1}$$

Thus we have shown that a is a coboundary. This completes the proof. □

We now study some applications of Hilbert Theorem 90. Consider the group $\mathrm{GL}(n, K)$ of $n \times n$ invertible matrices over K. The action of $\Gamma_{K/k}$ on $\mathrm{GL}(n, K)$ is given by action of the Galois group $\Gamma_{K/k}$ on entries of matrices. We have the following result:

Theorem 4.3.2. $H^1(\Gamma_{K/k}, \mathrm{GL}(n, K)) = 1$

Proof. Let $f \in H^1(\Gamma_{K/k}, \mathrm{GL}(n, K))$. For any $\beta \in M_n(K)$, define $\alpha = \sum_{s\in\Gamma_{K/k}} f(s)s(\beta)$. Here $\alpha \neq 0$ since by Dedekind's theorem $\Gamma_{K/k}$ is linearly independent over $\mathrm{GL}(n, K)$ and $f \neq 0$. For any $t \in \Gamma_{K/k}$, we have

$$t(\alpha) = \sum_{\Gamma_{K/k}} t(f(s))ts(\beta)$$

We use $f(ts) = f(t)t(f(s))$ to get

$$t(\alpha) = \sum_{s\in\Gamma_{K/k}} f(t)^{-1}f(ts)ts(\beta)$$

Then,

$$t(\alpha) = f(t)^{-1}\alpha$$

$$f(t) = \alpha t(\alpha^{-1})$$

This proves that $f \in B^1(\Gamma_{K/k}, \mathrm{GL}(n, K))$. We are done if we show that $\alpha \in \mathrm{GL}(n, K)$ for any choice of $\beta \in M(n, K)$. This is proved as follows:
For $x \in K^n$, define

$$\gamma(x) = \sum_{s\in\Gamma_{K/k}} f(s)(s(x)) \in K^n$$

We will show that $\gamma(x)$ generates K^n as a K-vector space as x runs over K^n. Let $u(x)$ be a linear form which vanishes on all $\gamma(x), x \in K^n$. Then, for all $a \in K$, $u(\gamma(ax)) = 0$. We have

$$0 = u(\gamma(ax)) = u\left(\sum_s f(s)s(ax)\right)$$

$$= u\left(\sum_s f(s)s(a)s(x)\right)$$

$$= u\left(\sum_s s(a)f(s)s(x)\right)$$

$$= \sum_s s(a)u(f(s)s(x))$$

$$0 = \sum_s u(f(s)s(x))s(a)$$

The above statement holds for all $a \in K$. Thus, $\sum_s u(f(s)s(x))s = 0$. By Dedekind's theorem,

$$u(f(s)s(x)) = 0 \ \forall \ s \in \Gamma_{K/k}$$

This implies that

$$f(s)u(s(x)) = 0$$

for all $s \in \Gamma_{K/k}$. Since $f(s)$ is invertible, $u(s(x)) = 0$ for all $s \in \Gamma_{K/k}$. Thus, u is identically zero. Therefore, the only linear form which vanishes identically on all $\gamma(x)$ is the zero form. Consequently, $\gamma(x)$ spans K^n as K-vector space.
Let $(x_1, x_2, \ldots, x_n)$ be vectors in K^n such that $\gamma(x_i) = y_i$ are linearly independent. Let $(e_i), 1 \leq i \leq n$ be the standard basis of K-vector space K^n. Let $\beta \in M(n, K)$ be the matrix of x_i's with respect to the standard basis $\{e_i\}_{i=1}^n$. Then

$$\alpha(e_i) = \left(\sum f(s)s(\beta)\right)(e_i)$$

$$= \sum f(s)s(\beta(e_i))$$

$$= \sum f(s)s(x_i)$$

$$= \gamma(x_i) = y_i$$

Since $\{y_i\}_{i=1}^n$ are linearly independent, the matrix corresponding to the transformation $x \to \alpha(x)$ is invertible. Hence, $\alpha \in \mathrm{GL}(n, K)$. □

Corollary 4.3.3. $H^1(\Gamma_{K/k}, \mathrm{SL}(n, K)) = 1$

Proof. Consider the exact sequence

$$1 \to \mathrm{SL}(n, K) \to \mathrm{GL}(n, K) \to \dot{K} \to 1$$

By Theorem 4.2.2, we obtain the following exact sequence,

$$1 \to \mathrm{SL}(n, k) \to \mathrm{GL}(n, k) \to \dot{k} \to H^1(\Gamma_{K/k}, \mathrm{SL}(n, K)) \to H^1(\Gamma_{K/k}, \mathrm{GL}(n, K))$$

Since the map $\det : \mathrm{GL}(n, k) \to \dot{k}$ is surjective and $H^1(\Gamma_{K/k}, \mathrm{GL}(n, K)) = 1$, we get $H^1(\Gamma_{K/k}, \mathrm{SL}(n, K)) = 1$. □

Given a Galois extension K/k and $\alpha \in K$, we define $\mathrm{norm}(\alpha) = \prod_i \sigma_i(\alpha)$ where σ_i run over elements of the group $\mathrm{Gal}(K/k)$.

Corollary 4.3.4. *Let K/k be a finite cyclic extension, say of degree n and let σ be a generator of $\mathrm{Gal}(K/k)$. Then, for $a \in K$, $\mathrm{norm}(a) = 1$ if and only if $a = \sigma(b)b^{-1}$.*

Proof. Let $a = \sigma(b)b^{-1}$. Then,

$$\mathrm{norm}(a) = a\sigma(a)\sigma^2(a).....\sigma^{n-1}(a)$$

$$= \sigma(b)b^{-1}\sigma^2(b)\sigma(b^{-1})\sigma^3(b)\sigma^2(b^{-1}).....\sigma^n(b)\sigma^{n-1}(b^{-1}) = 1$$

Conversely, suppose that $\mathrm{norm}(a) = 1$. Then, the assignment $\sigma \to a$ can be used to define a 1-cocycle $f : G \to A$ (We can check that f is indeed a 1-cocycle). Since, $H^1(\Gamma_{K/k}, \dot{K}) = 1$, there exists $b \in A$ such that $f(\sigma) = b^{-1}\sigma(b)$. Thus, we get $a = b^{-1}\sigma(b)$. □

4.4 Defining higher cohomology groups

We refer to [Ber10] for this section. Let Γ_k and A be as in section 4.1. Additionally, we assume that A is a Γ_k-*module* i.e. A is commutative as a Γ_k group. Let $n \geq 0$. We set $C^0(\Gamma_k, A) = A$ and for $n \geq 1$, we denote by $C^n(\Gamma_k, A)$, the set of continuous maps from Γ_k^n to A.

We now define $d_n : C^n(\Gamma_k, A) \to C^{n+1}(\Gamma_k, A)$.
For $n = 0$ and $\sigma \in \Gamma_k$, define

$$d_0(a)(\sigma) = \sigma.a - a$$

For $n \geq 1$,

$$d_n(\alpha)(\sigma_1, \ldots, \sigma_{n+1}) = \sigma_1.\alpha(\sigma_2, \ldots, \sigma_{n+1}) + \sum_{i=1}^{n} (-1)^i \alpha(\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_{n+1}) + (-1)^{n+1}\alpha(\sigma_1, \ldots, \sigma_n$$

where α is a map from Γ_k^n to A and $\sigma_i \in \Gamma_k$.

Definition 4.4.1. - *An n-cocycle of* Γ_k *with values in* A *is a map* $\alpha \in C^n(\Gamma_k, A)$ *satisfying*

1. $d_n(\alpha) = 0$
2. $\alpha(\sigma_1, \ldots, \sigma_n) = 0$ *if* $\sigma_i = 1$ *for any* i.

Definition 4.4.2. - *An n-coboundary of* Γ_k *with values in* A *is a map* $\alpha \in C^n(\Gamma_k, A)$ *for which there exists a map* $\beta \in C^{n-1}(\Gamma_k, A)$ *such that*

1. $d_{n-1}(\beta) = \alpha$
2. $\beta(\sigma_1, \ldots, \sigma_n) = 0$ *if* $\sigma_i = 1$ *for any* i.

For $n = 1$, only the first condition is required to hold.
Note that for $n = 1, 2$, the above definitions coincide with our previous definitions of $H^1(k, A)$ and $H^2(k, A)$. The set of n-cocycles and n-coboundaries form Abelian subgroups of $C^n(\Gamma_k, A)$. We denote the set of n-cocycles by $Z^n(\Gamma_k, A)$ and the set of n-coboundaries by $B^n(\Gamma_k, A)$. We observe that for every $n \geq 1$, $B^n(\Gamma_k, A) \subseteq Z^n(\Gamma_k, A)$. Thus, the n-th cohomology group $H^n(\Gamma_k, A)$ is given by

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

4.5 Cup-products

Let G be a group and A and B be groups with discrete topology on which G acts continuously. The cup product of an element from $H^1(G, A)$ with an element of

$H^1(G, B)$ gives an element of $H^2(G, A \otimes_{\mathbb{Z}} B)$. Since the tensor product is taken over $\mathbb{Z}$, it is mandatory that the G groups involved in the cup - product are Abelian. We first define the action of G on $A \otimes_{\mathbb{Z}} B$. For $\sigma \in G$ and $a \otimes b \in A \otimes_{\mathbb{Z}} B$, define $\sigma.(a \otimes b) = \sigma.a \otimes \sigma.b$. Let $\alpha \in Z^p(G, A)$ and $\beta \in Z^q(G, B)$. Then we define,

$$\alpha \cup \beta : G^{p+q} \to A \otimes_{\mathbb{Z}} B$$

as

$$(\sigma_1, \sigma_2, \ldots, \sigma_{p+q}) \mapsto \alpha(\sigma_1, \ldots, \sigma_p) \otimes \sigma_1\sigma_2 \ldots \sigma_p\beta(\sigma_{p+1}, \ldots, \sigma_{p+q})$$

Theorem 4.5.1. *The element $\alpha \cup \beta$ is a $(p+q)$-cocycle of G with values in $A \otimes_{\mathbb{Z}} B$. Moreover, $\alpha \cup \beta$ gives a map*

$$H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes_{\mathbb{Z}} B)$$

$$\cup : ([\alpha], [\beta]) \to [\alpha \cup \beta]$$

This map is $\mathbb{Z}$-bilinear. The cohomology class $[\alpha \cup \beta]$ depends only on the cohomology classes $[\alpha]$ and $[\beta]$. In addition, after identifying the $\mathbb{Z}$-modules $B \otimes_{\mathbb{Z}} A$ and $A \otimes_{\mathbb{Z}} B$ canonically, we have

$$[\alpha] \cup [\beta] = (-1)^{pq}[\beta] \cup [\alpha] \ \ \forall \ \ [\alpha] \in H^p(G, A), [\beta] \in H^q(G, B)$$

Proof. Using the expression for $d_n(\alpha)$, one can show that

$$d_{p+q}(\alpha \cup \beta) = d_p(\alpha) \cup \beta + (-1)^p \alpha \cup d_q(\beta)$$

Since both α and β are cocycles, $d_p(\alpha) = d_q(\beta) = 0$. Thus, from the above equation, we get $d_{p+q}(\alpha \cup \beta) = 0$. Hence, $\alpha \cup \beta$ is a $(p+q)$-cocycle.

In order to show that the cohomology class $[\alpha \cup \beta]$ depends only on the cohomology classes $[\alpha]$ and $[\beta]$, we have to show that $\alpha \cup \beta$ is a coboundary if one of α or β is a coboundary.
Let α be a coboundary. Then, there exists $\gamma \in C^{p-1}(G, A)$ such that $d_{p-1}(\gamma) = \alpha$. We have

$$d_{p+q-1}(\gamma \cup \beta) = d_{p-1}(\gamma) \cup \beta + (-1)^p \gamma \cup d_q(\beta)$$

Since β is a q-cocycle, $d_q(\beta) = 0$. Therefore,

$$d_{p+q-1}(\gamma \cup \beta) = d_{p-1}(\gamma) \cup \beta = \alpha \cup \beta$$

Thus, $\alpha \cup \beta$ is a coboundary. The proof proceeds similarly when β is a coboundary. The rest of the proof is technical and long and is therefore skipped. We refer to [Ber10] for further details. □

Definition 4.5.2. *The map $\cup$ is called a cup-product.*

Let C be another G-module and let $\theta : A \times B \to C$ be a $\mathbb{Z}$-bilinear map satisfying

$$\theta(\sigma.a, \sigma.b) = \sigma.\theta(a, b) \ \forall \ a \in A, b \in B, \sigma \in G$$

Then, θ induces a map of G-modules $A \otimes_{\mathbb{Z}} B \to C$ satisfying

$$\theta(\sigma.a \otimes \sigma.b) = \sigma.\theta(a \otimes b)$$

Therefore, we get a map

$$\theta^* : H^n(G, A \otimes_{\mathbb{Z}} B) \to H^n(G, C)$$

given by

$$f \to \theta \circ f$$

It is trivial to check that $\theta \circ f \in H^n(G, C)$ whenever $f \in H^n(G, A \otimes_{\mathbb{Z}} B)$. Further, we get another map

$$\cup_\theta : H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, C)$$

given by

$$([\alpha], [\beta]) \to \theta^*([\alpha \cup \beta])$$

Thus, we have $[\alpha] \cup_\theta [\beta] = \theta^*([\alpha \cup \beta]) = [\theta \circ (\alpha \cup \beta)]$. The map $\cup_\theta$ is called the *cup-product relative to θ*.

4.6 Inflation, Restriction and Corestriction

4.6.1 Inflation and Restriction

Let $f : G \to G'$ be a homomorphism of groups. Let A be a G-module and A' be a G'-module. Then A' can be made into a G-module by defining

$$g.a = f(g)a \ \forall \ g \in G, a \in A'$$

Let $\phi : A \to A'$ be a homomorphism of G-modules. Then the pair (f, ϕ) is called a *compatible pair* . This pair induces a natural homomorphism

$$\theta : C^n(G', A') \to C^n(G, A)$$

given by $\gamma \mapsto \delta$ where

$$\delta(g_1, g_2, \ldots, g_n) = \theta \circ \gamma \circ f(g_1, g_2, \ldots, g_n)$$

The sets $C^n(G, A)$ refer to the set of all continuous maps from G^n to A. This map naturally induces a map from $H^n(G', A') \to H^n(G, A)$ for $n \geq 1$.

Examples:

1. Let H be a subgroup of the group G and $f : H \hookrightarrow G$ be the inclusion map. Let $\phi = Id : A \to A$ be the identity map on G-module A. Then, (f, ϕ) is a compatible pair and we get maps

   $$\theta : C^n(G, A) \to C^n(H, A)$$

   and

   $$H_\theta : H^n(G, A) \to H^n(H, A)$$

   We know that $H^0(G, A) = A^G$ and $H^0(H, A) = A^H$. Thus, for $n = 0$, we get the inclusion $A^G \hookrightarrow A^H$. The homomorphism $H_\theta : H^n(G, A) \to H^n(H, A)$ is called the *restriction homomorphism* and is denoted by *res*.

2. Let H be a normal subgroup of G. Consider the projection map $f : G \to \dfrac{G}{H}$. If A is a G-module, then A^H is a $\dfrac{G}{H}$-module. Let $\phi : A^H \hookrightarrow A$ be the inclusion map. Then, the induced homomorphism

   $$H_\theta : H^n\left(\frac{G}{H}, A^H\right) \to H^n(G, A)$$

   is called the *inflation homomorphism* and is denoted by *inf*. For $n = 0$, $H^0(G, A) = A^G$ and $H^0\left(\dfrac{G}{H}, A^H\right) = A^G$. Thus, we get the identity map $A^G \to A^G$.

Proposition 4.6.1. *The restriction homomorphism is functorial i.e. if $f : A \to A'$ is a homomorphism of G-modules , then the diagram*

$$\begin{array}{ccc} H^n(G,A) & \xrightarrow{H^n(G,f)} & H^n(G,A') \\ \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} \\ H^n(H,A) & \xrightarrow{H^n(H,f)} & H^n(H,A') \end{array}$$

is commutative.

Proposition 4.6.2. *Restriction homomorphism commutes with connecting homomorphisms of exact sequences i.e. if*

$$0 \to A' \to A \to A'' \to 0$$

is an exact sequence of G-modules, then the diagram

$$\begin{array}{ccc} H^n(G,A'') & \xrightarrow{\delta^n} & H^{n+1}(G,A') \\ \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} \\ H^n(H,A'') & \xrightarrow{\delta^n} & H^{n+1}(H,A') \end{array}$$

is commutative.

Proposition 4.6.3. *The inflation homomorphism is functorial i.e. if $f : A \to A'$ is a homomorphism of G-modules , then the diagram*

$$\begin{array}{ccc} H^n\left(\frac{G}{H}, A^H\right) & \xrightarrow{H^n\left(\frac{G}{H},f\right)} & H^n\left(\frac{G}{H}, A'^H\right) \\ \downarrow{\scriptstyle inf} & & \downarrow{\scriptstyle inf} \\ H^n(G,A) & \xrightarrow{H^n(G,f)} & H^n(G,A') \end{array}$$

is commutative.

Proposition 4.6.4. *Inflation homomorphism commutes with connecting homomorphisms of exact sequences i.e. if*

$$0 \to A' \to A \to A'' \to 0$$

is an exact sequence of G-modules such that the induced sequence

$$0 \to A'^H \to A^H \to A''^H \to 0$$

is exact, then the diagram

$$\begin{array}{ccc} H^n\left(\frac{G}{H}, A''^H\right) & \xrightarrow{\delta^n} & H^{n+1}\left(\frac{G}{H}, A'^H\right) \\ \downarrow{\scriptstyle inf} & & \downarrow{\scriptstyle inf} \\ H^n(G, A'') & \xrightarrow{\delta^n} & H^{n+1}(G, A') \end{array}$$

is commutative.

Theorem 4.6.5. *Let H be a normal subgroup of G and let A be a G-module. If $H^i(H, A) = 0$ for $1 \leq i \leq n-1$(in particular, there is no condition for $n = 1$), then the sequence*

$$0 \ \to \ H^n\left(\frac{G}{H}, A^H\right) \ \xrightarrow{inf} \ H^n(G, A) \ \xrightarrow{res} \ H^n(H, A)$$

is exact.

The proof can be found in [Dal06]. An important consequence of the above result is the following theorem:

Corollary 4.6.6. *Let K/k be a finite Galois extension with Galois group G. Let H be a subgroup of G and K^H be the fixed field of H. Then, the following sequence is exact:*

$$0 \ \to \ H^2\left(\frac{G}{H}, \dot{K}^H\right) \ \xrightarrow{inf} \ H^2(G, \dot{K}) \ \xrightarrow{res} \ H^2(H, \dot{K})$$

Proof. Since H is the Galois group of the extension K/K^H, from Hilbert Theorem 90, $H^1(H, \dot{K}) = 0$. The theorem now follows from the above result. □

4.6.2 Corestriction

Let G be a group and H be a subgroup of finite index in G. Let A be a G-module. Then, A is also an H-module. Let $\{x_i\}_{i \in I}$ be a set of right coset representatives of H in G, I being an indexing set. We define a map

$$\theta : \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A) \to A$$

by $\theta(f) = \sum_{i\in I} x_i^{-1} f(x_i)$. Here, $\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)$ is the ring of all $\mathbb{Z}[H]$-module homomorphisms from $\mathbb{Z}[G]$ to A.
Note that θ does not depend on the choice of coset representatives. In fact, if $x_i = h_i y_i$, then

$$\theta(f) = \sum_{i\in I} (h_i y_i)^{-1} f(h_i y_i)$$

$$= \sum_{i\in I} y_i^{-1} h_i^{-1} h_i f(y_i) = \sum_{i\in I} y_i^{-1} f(y_i)$$

Here, we have used that f is $\mathbb{Z}[H]$-linear. We observe that θ is functorial and therefore, we get maps

$$H^n(\theta) : H^n(G, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)) \to H^n(G, A)$$

Lemma 4.6.7 (Shapiro). *Let H be a subgroup of G and let A be an H-module. Then, we have isomorphisms*

$$s_A^n : H^n(G, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)) \cong H^n(H, A) \ \forall \ n \geq 0$$

each of which is functorial in A.

By Shapiro's Lemma, we have

$$(s_A^n)^{-1} : H^n(H, A) \cong H^n(G, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A))$$

Composing the two maps, we get

$$H^n(\theta) \circ (s_A^n)^{-1} : H^n(H, A) \to H^n(G, A)$$

The above homomorphism is called *corestriction homomorphism.*
For $n = 0$, we get a map $A^H \to A^G$ given by $m \to \sum_{i\in I} x_i m$. Such a map is called an *averaging map.*

Theorem 4.6.8. *Let G be a group and H be a subgroup of finite index in G. Then the composite map*

$$cores \circ res : H^n(G, A) \to H^n(G, A)$$

is multiplication by $[G : H]$ for all $n \geq 0$.

Proof. For $n = 0$, the composite $cores \circ res$ is the map from $A^G \hookrightarrow A^H \to A^G$ given by $a \to \sum_{i\in I} x_i a = ra$ since $x_i a = a$ for $a \in A^G$. Here, $r = [G : H]$. Since both *cores*

and res are functorial and commute with connecting homomorphisms, it follows that $cores \circ res$ is multiplication by $[G : H]$ for all $n \geq 0$. $\square$

Chapter 5

Central Simple Algebras

In this chapter, we define central simple algebras over a field K and study quaternion algebras in detail. We try to establish a link between the second cohomology group $H^2(K, \mu_2)$ and the Brauer group $Br(K)$ of a field K. Further, we define involutions on central simple algebras and classify these involutions on basis of certain properties.

Let K be a field and $\mathcal{A}$ be a finite-dimensional K-algebra. Then $\mathcal{A}$ is called a *central simple algebra* over K if center$(\mathcal{A}) = K$ and $\mathcal{A}$ does not have any proper non-zero two sided ideals.

Examples:

1. Let V be an n-dimensional vector space over field K. Then, the ring End(V) of K-endomorphisms of V is a central simple algebra over K.
2. The four-dimensional *quaternion algebra* , $A = \left(\frac{a,b}{K}\right)$, $a, b \in \dot{K}$ is a central simple algebra over K. We refer to section 4.7.2 for details on quaternion algebras.

An algebra $\mathcal{A}$ over a field K is a *division algebra* if every non-zero element in $\mathcal{A}$ is invertible. We have the following result for central simple algebras over a field K.

Theorem 5.0.9. *For an algebra $\mathcal{A}$ over a field K, the following conditions are equivalent:*

1. *$\mathcal{A}$ is central simple.*

2. *There is a field L containing K such that*

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

for some n.

3. *If Ω is an algebraically closed field containing K, then*

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

for some n.

4. *There is a finite dimensional central division algebra D over K and an integer r such that $\mathcal{A} \cong M_r(D)$. Moreover, such a division algebra D is uniquely determined upto isomorphism.*

A field $L \supseteq K$ for which $\mathcal{A} \otimes_K L \cong M_n(L)$ is called a *splitting field* of $\mathcal{A}$. Thus, every central simple algebra admits a splitting field. Note that $\dim_K(\mathcal{A}) = n^2$. The integer n here is called the *degree of* $\mathcal{A}$. The degree of the division algebra D for which $\mathcal{A} \cong M_r(D)$ is called the *index of* $\mathcal{A}$.

Theorem 5.0.10. *The following statements hold for finite dimensional algebras over a field K.*

1. *If $\mathcal{A}$ is a central simple algebra over K and $\mathcal{B}$ is a simple algebra over K, then $\mathcal{A} \otimes_K \mathcal{B}$ is a simple algebra over K.*

2. *If both $\mathcal{A}$ and $\mathcal{B}$ are central simple algebras over K, then so is $\mathcal{A} \otimes_K \mathcal{B}$.*

Let S denote the set of central simple algebras over field K. Then, S is a commutative monoid with multiplication defined by taking tensor product over K and with K being the identity element. Two central simple algebras $\mathcal{A}$ and $\mathcal{B}$ over field K are said to be *Brauer equivalent* if

$$\mathcal{A} \otimes M_n(K) \cong \mathcal{B} \otimes M_m(K) \ for\ some\ n, m \in \mathbb{N}$$

The above relation is an equivalence relation on the set S and divides S into equivalence classes. The operation $[\mathcal{A}] \circ [\mathcal{B}] = [\mathcal{A} \otimes \mathcal{B}]$ is well-defined. The set S under this equivalence relation forms a group called the *Brauer group of* K denoted by $\mathrm{Br}(K)$. The class of matrix algebras over K forms the identity element of $\mathrm{Br}(K)$.

Theorem 5.0.11. *For any K-algebra, let $\mathcal{A}^{op}$ denote the opposite algebra of $\mathcal{A}$. If $\mathcal{A}$ is a central simple algebra, so is $\mathcal{A}^{op}$, and $\mathcal{A} \otimes \mathcal{A}^{op} \cong \mathrm{End}(\mathcal{A})$(the algebra of linear endomorphisms of $\mathcal{A}$). In particular, $\mathrm{Br}(K)$ forms an Abelian group, with $[\mathcal{A}]^{-1} = [\mathcal{A}^{op}]$ for any central simple algebra $\mathcal{A}$.*

Examples[[Lam05]]:

1. For $K = \mathbb{R}$, $\mathrm{Br}(\mathbb{R}) = \{\pm 1\}$, with the non-trivial element being the real quaternion algebra.

2. If F is a finite field or F is an algebraic extension of the rational function field $\mathbb{C}(x)$, then $\mathrm{Br}(F) = 0$.

5.1 Involutions

In this section, we define involutions on a central simple algebra $\mathcal{A}$ and the reduced norm of an element $a \in \mathcal{A}$.

Let L denote an algebraic closure of K and let $\mathcal{A}$ be a central simple algebra over K of degree n. Then, we have

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

We fix a K-algebra monomorphism $f : \mathcal{A} \otimes_K L \to M_n(L)$ and identify every element $a \in \mathcal{A}$ with a matrix say $M_a \in M_n(L)$. The characteristic polynomial of M_a has coefficients in K and is independent of embedding of $\mathcal{A}$ in $M_n(L)$. The determinant of M_a is called the *reduced norm of a* and is denoted by $\mathrm{nrd}_{\mathcal{A}}(a)$ while the trace of M_a is called the *reduced trace of a* denoted by $\mathrm{trd}_{\mathcal{A}}(a)$.

An *involution* on a central simple algebra $\mathcal{A}$ over a field K is a map $\sigma : \mathcal{A} \to \mathcal{A}$ satisfying the following properties:

1. $\sigma(a + b) = \sigma(a) + \sigma(b) \ \forall \ a, b \in \mathcal{A}$

2. $\sigma(ab) = \sigma(b)\sigma(a) \ \forall \ a, b \in \mathcal{A}$

3. $\sigma^2(a) = a \ \forall \ a \in \mathcal{A}$

We observe that the center of $\mathcal{A}$ i.e. K is preserved under σ. Thus, σ restricted to K is either the identity map or an automorphism of order 2. If σ restricted to K is identity, then σ is called an *involution of first kind* while if σ restricted to K is an automorphism of order 2, we say that σ is an *involution of second kind* .

We now describe involutions of first kind, which are of two types- orthogonal and symplectic.
Let V be a finite dimensional vector space over field K. A bilinear form

$$b : V \times V \to K$$

is called *non-singular* if the matrix associated to b with respect to a basis of V is invertible. Alternatively, we can say that the induced map

$$\hat{b} : V \to V^*$$

given by $\hat{b}(v)(u) = b(v, u)$ is an isomorphism of vector spaces. Here, the space V^* denotes the dual space of V. If b is non-singular, then for $f \in \mathrm{End}_K(V)$, we define

$$\sigma_b(f) = \hat{b^{-1}} \circ f^t \circ \hat{b}$$

where f^t called the *transpose* of f is a map

$$\hat{f} : V^* \to V^*$$

given by $\hat{f}(g) = g \circ f$. The map $\sigma_b : \mathrm{End}_K(V) \to \mathrm{End}_K(V)$ is an anti-automorphism known as *adjoint involution* of $\mathrm{End}_K(V)$ with respect to the bilinear form b. We then have the following result.

Theorem 5.1.1. *The map which associates to each non-singular bilinear form b on V its adjoint involution σ_b induces a one to one correspondence between equivalence classes of non-singular bilinear forms on V modulo multiplication by a factor in $\dot{K}$ and linear anti-automorphisms of* $\mathrm{End}_K(V)$. *Under this correspondence, K-linear involutions on* $\mathrm{End}_K(V)$ *correspond to non-singular bilinear forms which are either symmetric or skew-symmetric.*

We now use the above theorem to obtain an adjoint involution on central simple algebra $\mathcal{A}$.
Let $\mathcal{A}$ be a central simple algebra over K and σ be an involution of first kind on $\mathcal{A}$. Let $(\mathcal{A}', \sigma')$ be another central simple algebra with involution. Then, a homomorphism from $(\mathcal{A}, \sigma)$ to $(\mathcal{A}', \sigma')$ is a map $f : \mathcal{A} \to \mathcal{A}'$ such that

$$f \circ \sigma = \sigma' \circ f$$

Let L be a splitting field of $\mathcal{A}$ i.e. $\mathcal{A} \otimes_K L \cong M_n(L)$ where n is the degree of $\mathcal{A}$. Then, the involution σ can be extended to $\mathcal{A}_L$ by making it constant on scalars i.e. the involution σ_L on $\mathcal{A} \otimes_K L$ can be defined as $\sigma_L = \sigma \otimes id_L$. Since $\mathcal{A}_L = \mathrm{End}_K(V)$ for some n-dimensional vector space V over L, using the above theorem, we get that σ_L is the adjoint involution σ_b with respect to some non-singular bilinear form b on V, which can either be symmetric or skew-symmetric.

Since b is non-singular, if we take a basis of V over L, then the matrix corresponding to b, say m is invertible, i.e. $m \in GL_n(L)$. Therefore, we get an involution σ_m on $M_n(L)$ given by

$$\sigma_m(a) = m^{-1}a^t m \ \forall \ a \in M_n(L)$$

Therefore, we get the following result.

Theorem 5.1.2. *Let $(\mathcal{A}, \sigma)$ be a central simple K-algebra of degree n with involution of the first kind and let L be a splitting field of $\mathcal{A}$. Let V be an L-vector space of dimension n. There is a non-singular symmetric or skew-symmetric bilinear form b on V and an invertible matrix $m \in GL_n(L)$ such that $m^t = m$ if b is symmetric and $m^t = -m$ if b is skew-symmetric, and*

$$(A_L, \sigma_L) \cong (\mathrm{End}_L(V), \sigma_b) \cong (M_n(L), \sigma_m)$$

This result gives another important result.

Corollary 5.1.3. *For all $a \in \mathcal{A}$, the elements a and $\sigma(a)$ have the same reduced characteristic polynomial. In particular, $Trd_{\mathcal{A}}(\sigma(a)) = Trd_{\mathcal{A}}(a)$ and $Nrd_{\mathcal{A}}(\sigma(a)) = Nrd_{\mathcal{A}}(a)$ for all $a \in \mathcal{A}$.*

Proof. The theorem follows directly from the observation that every $a \in \mathcal{A}$ corresponds to a matrix $g \in M_n(L)$ and for every such matrix $\sigma_m(g) = m^{-1}g^t m$, the characteristic polynomial of $\sigma_m(g)$ being the same as that of g. □

We now define the sets of symmetric, skew-symmetric, alternating and symmetrized elements in (A, σ).

$$Sym(\mathcal{A}, \sigma) = \{a \in \mathcal{A} \mid \sigma(a) = a\}$$

$$Skew(\mathcal{A}, \sigma) = \{a \in \mathcal{A} \mid \sigma(a) = -a\}$$

$$Alt(\mathcal{A}, \sigma) = \{a - \sigma(a) \mid a \in \mathcal{A}\}$$

$$Symd(\mathcal{A}, \sigma) = \{a + \sigma(a) \mid a \in \mathcal{A}\}$$

If $\text{char}(K) \neq 2$, then $Sym(\mathcal{A}, \sigma) = Symd(\mathcal{A}, \sigma)$ and $Skew(\mathcal{A}, \sigma) = Alt(\mathcal{A}, \sigma)$.

Definition 5.1.4. *A bilinear form $b : V \times V \to K$ is said to be alternating if for every $v \in V$, $b(v, v) = 0$.*

We are now in a position to define orthogonal and symplectic involutions. An involution σ of the first kind on a central simple algebra $\mathcal{A}$ is said to be *symplectic* if for every splitting field L of $\mathcal{A}$ and every isomorphism $(\mathcal{A}_L, \sigma_L) \cong (\text{End}_K(V), \sigma_b)$, the bilinear form b is alternating. On the other hand, σ is *orthogonal* if for every splitting field L of $\mathcal{A}$ and every isomorphism $(\mathcal{A}_L, \sigma_L) \cong (\text{End}_K(V), \sigma_b)$, the bilinear form b is non-alternating.

5.2 Quaternion Algebras

Let $a, b \in \dot{K}$. A *quaternion algebra* $\left(\frac{a,b}{K}\right)$ is a four-dimensional K-algebra with generators $\{i, j\}$ and defining relations

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

Theorem 5.2.1. *The set $\{1, i, j, ij\}$ forms a basis of the algebra $\left(\frac{a,b}{K}\right)$ over K.*

Proof. Let Ω be the algebraic closure of K and let $\alpha, \beta \in \Omega$ be such that $\alpha^2 = a$ and $\beta^2 = b$. Consider matrices $A_1, A_2 \in \mathbb{M}_2(\Omega)$ given by $A_1 = \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix}$ and $A_2 = \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix}$. Then, $A_1^2 = aI$, $A_2^2 = bI$ and $A_1A_2 = -A_2A_1$. Thus, the map

$$\phi : \left(\frac{a,b}{K}\right) \to \mathbb{M}_2(\Omega)$$

given by $i \to A_1$, $j \to A_2$ is a homomorphism. Since the set (I, A_1, A_2, A_1A_2) is linearly independent over Ω, therefore $(1, i, j, ij)$ is linearly independent over K. Hence, the set $(1, i, j, ij)$ forms a basis of $\left(\frac{a,b}{K}\right)$ over K. □

Note that the quaternion algebra $\left(\frac{a,b}{K}\right)$ is symmetric in a, b i.e. $\left(\frac{a,b}{K}\right) \cong \left(\frac{b,a}{K}\right)$ and functorial in K, i.e. for any field extension L/K,

$$L \otimes \left(\frac{a,b}{K}\right) \cong \left(\frac{a,b}{L}\right)$$

We now state some more results about quaternion algebras.

Theorem 5.2.2. *The following statements hold for quaternion algebras over K:*

1. $\left(\frac{a,b}{K}\right) \cong \left(\frac{ax^2,by^2}{K}\right)$ *for any* $a, b, x, y \in \dot{K}$.
2. $\left(\frac{-1,1}{K}\right) \cong \mathbb{M}_2(K)$
3. *The center of* $\left(\frac{a,b}{K}\right)$ *is* K.
4. $\left(\frac{a,b}{K}\right)$ *is a simple algebra.*

Proof. 1. Let $\{1, i, j, ij\}$ be a basis for $\left(\frac{a,b}{K}\right)$ and $\{1, i', j', i'j'\}$ be a basis for $\left(\frac{ax^2,by^2}{K}\right)$. Then,

$$i^2 = a,\ j^2 = b,\ i'^2 = ax^2,\ j'^2 = by^2$$

Consider a map

$$\phi : \left(\frac{ax^2,by^2}{K}\right) \to \left(\frac{a,b}{K}\right)$$

given by $i' \to xi$ and $j' \to yj$. This map gives the required isomorphism between the two algebras.

2. Let $(1, i, j, ij)$ be a basis for $\left(\frac{-1,1}{K}\right)$. Then, the map

$$\theta : \left(\frac{-1,1}{K}\right) \to \mathbb{M}_2(K)$$

given by $i \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $j \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is an isomorphism.

3. Let Ω be the algebraic closure of K. Then, by functorial property of quaternion algebras, $\Omega \otimes \left(\frac{a,b}{K}\right) \cong \left(\frac{a,b}{\Omega}\right)$. Since Ω is algebraically closed, the equations $ax^2 = 1$ and $by^2 = -1$ are solvable in Ω. Thus,

$$\left(\frac{a,b}{\Omega}\right) \cong \left(\frac{-1,1}{\Omega}\right) \cong \mathbb{M}_2(\Omega)$$

Since center$(\mathbb{M}_2(\Omega)) = \Omega$, therefore center$\left(\frac{a,b}{K}\right) = K$.

4. The matrix algebra $\mathbb{M}_2(\Omega)$ does not have proper ideals, thus $\left(\frac{a,b}{K}\right)$ does not have any proper ideal.

□

Consider an element $v = \alpha + \beta i + \gamma j + \delta k$ in the algebra $A = \left(\frac{a,b}{K}\right)$ with basis $\{1, i, j, k\}$. We define *conjugate* of v as

$$\bar{v} = \alpha - \beta i - \gamma j - \delta k$$

The element v is called a *pure quaternion* if $\alpha = 0$. The K-space of pure quaternions is denoted by A_0.

Theorem 5.2.3. *A quaternion $0 \neq v \in A$ is pure if and only if $v \notin K$ and $v^2 \in K$.*

Proof. The proof follows from straightforward calculations. □

We observe that if $v \in A_0$, then $\bar{v} = -v$. With every quaternion algebra A, we can associate a quadratic form q in the following manner:
For $x \in A$,

$$\overline{xy} = \bar{y}\bar{x},\ \overline{x+y} = \bar{x} + \bar{y},\ \bar{\bar{x}} = x$$

For $x \in A$, define

$$\text{norm}(x) = x\bar{x},\ \text{trace}(x) = x + \bar{x}$$

Define a bilinear form B on A as

$$B(x,y) = \frac{x\bar{y} + y\bar{x}}{2} = \frac{\text{trace}(x\bar{y})}{2}$$

For $x = p+qi+rj+sk$, $\text{norm}(x) = p^2 - q^2a - r^2b - s^2ab$ and $\text{trace}(x) = 2p$. Thus, both $\text{norm}(x) \in K$ and $\text{trace}(x)$ are elements of K. Hence, $B(x,y) \in K$. By definition,

$B(x, y)$ is symmetric and homogeneous of degree 2. Thus, (A, B) gives a quadratic space over K. If q is the associated quadratic form then,

$$q(x) = B(x, x) = \frac{x\bar{x} + \bar{x}x}{2} = x\bar{x} = \text{norm}(x)$$

The quadratic form associated with A is isometric to the Pfister form $\langle\langle -a, -b\rangle\rangle$. Therefore, the form $q = \langle\langle -a, -b\rangle\rangle$ is called the *norm form of A*.

Theorem 5.2.4. *For* $A = \left(\frac{a, b}{K}\right)$, *the following statements are equivalent:*

1. $A \cong \left(\frac{1, -1}{K}\right)$.
2. *A is not a division algebra.*
3. *A is isotropic as a quadratic space.*
4. *A is hyperbolic as a quadratic space.*
5. A_0 *is isotropic as a quadratic space.*
6. $\langle 1, -a\rangle \otimes \langle 1, -b\rangle = 0$ *in* $W(K)$.
7. *The binary form* $\langle a, b\rangle$ *represents* 1.
8. $a \in N_{L/K}(L)$, *where* $L = K(\sqrt{b})$, *and* $N_{L/K}$ *is the field norm.*

If any of these conditions holds for A, we say that A is split or that A splits over K.

Proof. We use the following results in our proof[[Lam05]]:

1. An element $v \in A$ is invertible if and only if $\text{norm}(v) \neq 0$.
2. A Pfister form is isotropic if and only if it is hyperbolic.

These results establish the equivalence of statements 1 to 7. Now, we prove that $7 \leftrightarrow 8$. We assume that $b \notin \dot{K}^2$. Let L be the quadratic extension $K(\sqrt{b})$. Then, for any element $x + y\sqrt{b} \in L$, $\text{norm}(x + y\sqrt{b}) = x^2 - by^2$. Thus, $a \in N_{L/K}(L)$ implies that $a \in D_K(\langle 1, -b\rangle)$ which further implies that the binary form $\langle a, b\rangle$ represents 1. The reverse implication follows from reversing these arguments. □

Definition 5.2.5. *A biquaternion algebra over a field K is the tensor product of two quaternion algebras over K. It forms a* 16 *dimensional central simple algebra over K.*

Theorem 5.2.6. *For $a, b, c \in \dot{K}$, we have*

$$\left(\frac{a,b}{K}\right) \otimes \left(\frac{a,c}{K}\right) \cong \left(\frac{a,bc}{K}\right) \otimes \mathbb{M}_2(K)$$

Thus, we have

$$\left(\frac{a,b}{K}\right) \otimes \left(\frac{a,b}{K}\right) \cong \left(\frac{a,b^2}{K}\right) \otimes \mathbb{M}_2(K) \cong \left(\frac{a,1}{K}\right)$$

From Theorem 4.7.10, we deduce that $\left(\frac{a,1}{K}\right)$ splits over K and thus, every division quaternion algebra is an element of order 2 in $\mathrm{Br}(K)$. Thus, the set of quaternion algebras over field K has order 2 in $\mathrm{Br}(K)$. In fact, it is true that 2-torsion Brauer group of a field K, denoted by ${}_2\mathrm{Br}(K)$ is generated by the set of division quaternion algebras over K.

5.3 $H^2(K, \mu_2)$ and $\mathbf{Br}(K)$

In this section, we define Witt ring $W(K)$ of a field K in a different manner than defined in Section 1.8. Additionally, we understand how quadratic forms, basically Pfister forms are related to elements of cohomology groups which further establishes a relation between ${}_2\mathrm{Br}(K)$ and $H^2(K, \mu_2)$.
Consider the set $M(K)$ of isometry classes of regular quadratic forms over K. Then, $M(K)$ is a ring under the operations of addition($\perp$) and multiplication($\otimes$). We give an equivalence relation on the set $M(K) \times M(K)$. For $(x, y), (x', y') \in M(K) \times M(K)$, we say that $(x, y) \sim (x', y')$ if and only if

$$x + y' = x' + y$$

The above relation is indeed an equivalence relation on the set $M(K) \times M(K)$.

Definition 5.3.1. *The Grothendieck group of $M(K)$ is defined as*

$$\mathrm{Groth}(M(K)) = \frac{M(K) \times M(K)}{\sim}$$

We define addition on Groth$(M(K))$ as

$$(x, y) + (x', y') = (x + x', x + y')$$

The addition in Groth$(M(K))$ is well defined. The additive identity is the equivalence class of elements $(\alpha, \alpha), \alpha \in M(K)$. The additive inverse of (x, y) is given by (y, x). Thus, Groth$(M(K))$ becomes a group under addition. We now define a map

$$i : M(K) \to \text{Groth}(M(K))$$

given by $x \to (x, 0)$. The map i is injective. Therefore,

$$M(K) \hookrightarrow \text{Groth}(M(K))$$

We have

$$(x, y) = i(x) - i(y) = i(x - y)$$

Thus, we can identify Groth$(M(K))$ by elements of type $x - y$ where $x, y \in M(K)$. Since elements of $M(K)$ are quadratic forms, we have

$$\text{Groth}(M(K)) = \{q_1 - q_2 \mid q_1, q_2 \in M(K)\}$$

The ring Groth$(M(K)) = W\hat{(}K)$ is called the *Witt Grothendieck ring* of quadratic forms over field K. We now give homomorphisms on Groth$(M(K))$.
Let G be a group and $\theta : M(K) \to G$ be a group homomorphism. Then, θ induces a map

$$\bar{\theta} : \text{Groth}(M(K)) \to G$$

given by

$$\bar{\theta}(q_1 - q_2) = \theta(q_1) - \theta(q_2)$$

We can check that $\bar{\theta}$ is again a group homomorphism.
Consider a homomorphism

$$\dim : M(K) \to \mathbb{Z}$$

given by $q \to \dim(q)$. This homomorphism induces another homomorphism

$$\overline{\dim} : \text{Groth}(M(K)) \to \mathbb{Z}$$

given by $q_1 - q_2 \to \dim(q_1) - \dim(q_2)$. The kernel of the map $\overline{\dim}$ is called the *fundamental ideal* of $W\hat{(}K)$ and is denoted by $I(\hat{K})$. Thus, $I(\hat{K})$ consists of elements of type $q_1 - q_2$ such that $\dim(q_1) = \dim(q_2)$.

Theorem 5.3.2. *The ideal $I(\hat{K})$ is generated by elements of type $\langle a\rangle - \langle 1\rangle$, $a \in \dot{K}$.*

Proof. Let $q_1 - q_2 \in I(\hat{K})$. Then $\dim(q_1) = \dim(q_2) = n$(say). Let $q_1 = \langle a_1, a_2, \ldots, a_n\rangle$ and $q_2 = \langle b_1, b_2, \ldots, b_n\rangle$. Then

$$q_1 - q_2 = \sum_i (\langle a_i\rangle - \langle b_i\rangle) = \sum_i (\langle a_i\rangle - \langle 1\rangle) - (\langle b_i\rangle - \langle 1\rangle)$$

$$= \sum_i (\langle a_i\rangle - \langle 1\rangle) - \sum_i (\langle b_i\rangle - \langle 1\rangle$$

Hence the theorem is proved. □

We recall that $\mathbb{H}$ denotes the hyperbolic space over field K which consists of finite products of quadratic forms of type $\langle 1, -1\rangle$. The quotient $\dfrac{W\hat{(}K)}{\mathbb{Z}.\mathbb{H}}$ gives the isometry classes of regular quadratic forms which are anisotropic over K. Thus, the quotient $\dfrac{W\hat{(}K)}{\mathbb{Z}.\mathbb{H}} = W(K)$ is the Witt ring of field K. The image of $I(\hat{K})$ under the projection $W\hat{(}K) \to W(K)$ is denoted by $I(K)$. The ideal $I(\hat{K})$ consists of elements $q_1 - q_2$ such that $\dim(q_1 - q_2) = 0$. Since $\dim(\mathbb{H}) = 2$, therefore $I(\hat{K}) \cap \mathbb{Z}.\mathbb{H} = 0$. Thus, we get $I(\hat{K}) \cong I(K)$.

The above theorem says that $I(K)$ is generated by Pfister forms of type $\langle 1, a\rangle, a \in \dfrac{\dot{K}}{\dot{K}^2}$. We define the powers of fundamental ideal $I^m(K)$ as ideals generated by m-fold Pfister forms given by $\langle\langle a_1, a_2, \ldots, a_m\rangle\rangle, a_i \in \dfrac{\dot{K}}{\dot{K}^2}$.

Theorem 5.3.3. *A quadratic form $q \in I(K)$ if and only if $\dim(q)$ is even.*

Proof. Let $q \in I(K)$. Then $q = q_1 - q_2 + m\mathbb{H}$ where $\dim(q_1) = \dim(q_2)$. Thus, $\dim(q) = 2m$. Conversely, let $q \in W(K)$ be such that $\dim(q)$ is even. Then, q is a binary form of type $\langle a, b\rangle = \langle a\rangle - \langle -b\rangle \in I(\hat{K})$. Thus, $q \in I(K)$. □

Thus, $I(K)$ consists of even dimensional quadratic forms of $W(K)$. Therefore, we get an isomorphism $\dfrac{W(K)}{I(K)} \cong \dfrac{\mathbb{Z}}{2\mathbb{Z}}$.

We now give another homomorphism of $W(K)$. Define a map

$$d : M(K) \to \frac{\dot{K}}{\dot{K}^2}$$

given by $q \to d(q)$ where $d(q)$ denotes the determinant of q. Since $d(q_1 \perp q_2) = d(q_1)d(q_2)$, d is a homomorphism. We observe that $d(\mathbb{H}) = -1.\dot{K}^2$. Since the map d does not factor through $W(F)$, we make a modification and define *signed determinant* of q as

$$d_{\pm}(q) = (-1)^{n(n-1)/2} \in \frac{\dot{K}}{\dot{K}^2}$$

where $n = \dim(q)$. Then $d_{\pm} : M(K) \to \dfrac{\dot{K}}{\dot{K}^2}$ gives the desired map. We have $d_{\pm}(\mathbb{H}) = 1.\dot{K}^2$ but now the relation $d_{\pm}(q_1 \perp q_2) = d_{\pm}(q_1)d_{\pm}(q_2)$ does not hold. In order to restore the homomorphism between $M(K)$ and $\dfrac{\dot{K}}{\dot{K}^2}$, we define a larger group $Q(K) = \dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\dot{K}}{\dot{K}^2}$. The operation of multiplication in $Q(K)$ is defined as

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

The element $(0, 1)$ serves as the multiplicative identity while $\left(e, (-1)^e \dfrac{1}{d}\right)$ serves as the multiplicative inverse of (e, d). The inclusion $d \hookrightarrow (0, d)$ identifies $\dfrac{\dot{K}}{\dot{K}^2}$ as a subgroup of $Q(K)$. Therefore, we have the isomorphism

$$\frac{Q(K)}{\dot{K}/\dot{K}^2} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$$

Theorem 5.3.4. *The map* $(\dim_0, d_{\pm})$ *defines a monoid epimorphism from* $M(K)$ *to* $Q(K)$. *This extends to a group epimorphism from* $W(K)$ *to* $Q(K)$ *and thus, we get* $\dfrac{W(K)}{I^2(K)} \cong Q(K)$.

Proof. The map $(\dim_0, d_{\pm}) : M(K) \to Q(K)$ is given by $q \to (\dim_0(q), d_{\pm}(q))$ where $\dim_0(q) = \dim(q) \mod 2$ and $d_{\pm}(q)$ is the signed determinant of q. We can check that $(\dim_0, d_{\pm})$ is indeed a homomorphism. It is surjective since for every $a \in \dot{K}$, we have

$$(\dim_0, d_{\pm})(\langle a \rangle) = (1, a\dot{K}^2)$$

and

$$(\dim_0, d_{\pm})(\langle 1, a \rangle) = (0, a\dot{K}^2)$$

We observe that elements of type $\langle 1, a \rangle \otimes \langle 1, b \rangle$ are mapped to the identity element $(0, 1)$ of $Q(K)$. The ideal generated by such elements in $W(K)$ is denoted by $I^2(K)$.

Therefore, we get a homomorphism $f : \dfrac{W(K)}{I^2(K)} \to Q(K)$. We now show that the inverse map $g : Q(K) \to \dfrac{W(K)}{I^2(K)}$ is also a homomorphism.
Define $g(0,a) = \langle 1, -a\rangle \mod I^2(K)$ and $g(1,a) = \langle a\rangle \mod I^2(K)$. Then

$$g[(0,a).(0,b)] = g[(0,ab)] = \langle 1, -ab\rangle \equiv \langle 1, a, 1, b\rangle \mod I^2(K)$$

Thus, $g[(0,a).(0,b)] = g[(0,a)] \perp g[(0,b)]$. Similarly, we have

$$g[(1,a).(1,b)] = g[(0,-ab)] = \langle 1, ab\rangle \equiv \langle a, b\rangle \mod I^2(K)$$

$$= g[(1,a)] \perp g[(1,b)]$$

and

$$g[(0,a).(1,b)] = g[(1,ab)] = \langle ab\rangle \equiv \langle 1, -a, b\rangle \mod I^2(K)$$

$$= g[(0,a)] \perp g[(1,b)]$$

Therefore, $g : Q(K) \to \dfrac{W(K)}{I^2(K)}$ is a homomorphism. By definition, we have $f \circ g = g \circ f = id$. As a result, $Q(K) \cong \dfrac{W(K)}{I^2(K)}$. □

The restriction of the isomorphism $\dfrac{W(K)}{I^2(K)} \cong \dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\dot{K}}{\dot{K}^2}$ to $I(K)$ induces an isomorphism

$$\frac{I(K)}{I^2(K)} \cong \frac{\dot{K}}{\dot{K}^2}$$

We now consider the exact sequence

$$\{1\} \to \{1, -1\} \to \dot{K}^s \to \dot{K}^s \to \{1\}$$

where K^s denoted the separable closure of K and the map $\dot{K}^s \to \dot{K}^s$ is given by $x \to x^2$. We consider the long homology exact sequence obtained from the above exact sequence and use Hilbert Theorem 90 to obtain the isomorphism

$$\frac{\dot{K}}{\dot{K}^2} \cong H^1(K, \mu_2)$$

Thus, we have

$$\frac{I(K)}{I^2(K)} \cong H^1(K, \mu_2)$$

Similarly, we try to describe the quotient $\dfrac{I^2(K)}{I^3(K)}$. We know that $I^2(K)$ is generated by 2-fold Pfister forms i.e. quadratic forms of type $\langle\langle a, b\rangle\rangle = \langle 1, a\rangle \otimes \langle 1, b\rangle$. Thus, every element of $\dfrac{I^2(K)}{I^3(K)}$ is given by the class $\overline{\langle\langle a, b\rangle\rangle}$. We define a map

$$\alpha : \frac{I^2(K)}{I^3(K)} \to H^2(K, \mu_2)$$

given by $\alpha(\overline{\langle\langle a, b\rangle\rangle}) = (a) \cup (b)$. This map is well defined and is therefore a homomorphism.

We saw before that $\langle\langle -a, -b\rangle\rangle$ is the norm form of quaternion algebra $\left(\dfrac{a, b}{K}\right)$ and that quaternion algebras over K are the only elements of ${}_2\mathrm{Br}(K)$. We define another map

$$\beta : \frac{I^2(K)}{I^3(K)} \to {}_2\mathrm{Br}(K)$$

given by $\overline{\langle\langle a, b\rangle\rangle} \to \left(\dfrac{-a, -b}{K}\right)$. Then, β is a homomorphism. It was proved by Merkurjev that the maps α and β are isomorphisms. We thus have

$$\frac{I^2(K)}{I^3(K)} \cong H^2(K, \mu_2) \cong {}_2\mathrm{Br}(K)$$

We refer to [Lam05] for further details on above isomorphisms.

Chapter 6

Invariants of Quadratic Forms

This chapter discusses three invariants of quadratic forms which are dimension, determinant and Clifford invariant. All these invariants have a cohomological description in terms of Stiefel-Whitney invariants which is included in the chapter.

6.1 Dimension, Determinant and Clifford Invariant

Let K be a field. Let $S(K)$ denote the set of isometry classes of quadratic forms over K. Then, to every class in $S(K)$, we can associate certain maps which are called *invariants*.

The first invariant is the *dimension of a quadratic form* q. The dimension of a quadratic form q remains fixed under every isometry of q. In fact, we can define a map

$$\dim : W(K) \to \frac{\mathbb{Z}}{2\mathbb{Z}}$$

given by $q \mapsto \dim(q) \mod 2$. This map is a homomorphism and gives the isomorphism

$$\frac{W(K)}{I(K)} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$$

The second invariant is the *determinant of a quadratic form* q. The determinant of $q = \langle a_1, a_2, a_3, ..., a_n \rangle$ is defined as

$$d(q) = a_1 a_2 .....a_n \mod \dot{K}^2$$

The square class of $d(q)$ remains unchanged under every isometry of q. However, the map

$$\det : S(K) \to \frac{\dot{K}}{\dot{K}^2}$$

given by $q \to \det(q)$ does not factor through the hyperbolic space $\mathbb{H}$. Therefore, we define *signed determinant of* q as

$$d_{\pm}(q) = (-1)^{n(n-1)/2} d(q) \in \frac{\dot{K}}{\dot{K}^2}$$

Now, we get a homomorphism

$$d_{\pm} : W(K) \to \frac{\dot{K}}{\dot{K}^2}$$

given by $q \mapsto d_{\pm}(q)$. The two invariants mentioned above have already been discussed in Chapter 1 and therefore we will not talk much about them.
The main subject of this section is *Clifford Invariant* which is nothing but the Clifford algebra associated to a quadratic form q.

6.1.1 Clifford Algebra

Let V be a finite dimensional vector space over a field K. The tensor algebra $T(V)$ of V is given by

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

The *Clifford algebra* of q denoted by $C(V, q)$ is defined as

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

where (V, q) is a quadratic space and $I(q)$ denotes the ideal of $T(V)$ generated by elements $\{v \otimes v - q(v),\ v \in V\}$. Thus, for every $v \in C(V, q)$, we have $v \otimes v = q(v)$.
The algebra $C(V, q)$ satisfies the following universal property :
For every K-algebra $\mathcal{A}$ with a map $\alpha : V \to \mathcal{A}$ for which $\alpha(v^2) = q(v)$, there exists a unique map $\bar{\alpha} : C(V, q) \to \mathcal{A}$ such that the diagram

$$\begin{array}{ccc} V & \xrightarrow{\ i\ } & C(V,q) \\ \downarrow{\scriptstyle \alpha} & \swarrow_{\bar{\alpha}} & \\ \mathcal{A} & & \end{array}$$

is commutative (see [Sch85]). The space $T(V)$ has $\oplus_{r=0}^{\infty} T^{2r}(V) = T_{even}(V)$ and $\oplus_{r=o}^{\infty} T^{2r+1}(V) = T_{odd}(V)$ as subspaces.
Let $\eta : T(V) \to C(V,q)$ denote the canonical homomorphism. Then, $\ker(\eta) = I(q) \subseteq T_{even}(V)$. Thus, $C(V,q)$ has a structure of $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)$-graded algebra. We write

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

where $C_0(V,q) = \eta(T_{even}(V))$ and $C_1(V,q) = \eta(T_{odd}(V))$. The algebra $C_0(V,q)$ is called the *even Clifford algebra* of (V,q).
Examples:

1. Let V be the one-dimensional quadratic space over K with basis $\{x\}$ and quadratic form $q = \langle a \rangle$. Then, $I(q)$ is the ideal generated by $x^2 - a$ and the Clifford algebra $C(V,q) = \dfrac{K[x]}{(x^2 - a)}$.

2. Let V be as above and q be the zero quadratic form on V i.e. $q(x) = 0$. Then, $I(q)$ is the ideal generated by $x \otimes x$ and $C(V,q)$ is same as the exterior algebra on V.

We now state two theorems which give us the Clifford Invariants.

Theorem 6.1.1. *Suppose* $\dim(V)$ *is odd,* $\delta = d_{\pm}(V)$ *denotes the signed determinant of* (V,q) *and* $Z(C(V,q))$ *denotes the center of Clifford algebra* (V,q)*. Then*

1. $C_0(V,q)$ *is a central simple algebra over* K*, and* $C(V,q) \cong (C_0(V,q)) \otimes K(\sqrt{\delta})$.

2. *If* $\delta \notin \dot{K}^2$*, then* $Z(C(V,q)) \cong K(\sqrt{\delta})$*, and* $C(V,q)$ *is a central simple algebra over* $K(\sqrt{\delta})$.

3. *If* $\delta \in \dot{K}^2$*, then* $Z(C(V,q)) \cong K \times K$*, and* $C(V,q) \cong C_0(V,q) \times C_0(V,q)$.

Theorem 6.1.2. *Suppose* $\dim(V) = n$ *is even,* $\delta = d_{\pm}V$ *denotes the signed determinant of* (V,q) *and* $Z(C(V,q))$ *denotes the center of Clifford algebra* (V,q)*. Then*

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

2. *If* $\delta \notin \dot{K}^2$*, then* $Z(C_0(V,q)) \cong K(\sqrt{\delta})$*, and* $C_0(V,q)$ *is a central simple algebra over* $K(\sqrt{\delta})$.

3. *If* $\delta \in \dot{K}^2$*, then* $Z(C_0(V,q)) \cong K \times K$.

A proof of these theorems can be found in [5, [Lam05]]. From the above theorems, we deduce that if (V, q) is an even dimensional quadratic space, then $C(V, q)$ is a central simple algebra over K and if (V, q) is an odd dimensional quadratic space, then $C_0(V, q)$ is a central simple algebra over K. These, in fact, give the Clifford invariants.

Definition 6.1.3. *If q is even dimensional, then $C(V, q)$ is the Clifford invariant while if q is odd dimensional, then $C_0(V, q)$ is the Clifford invariant.*

6.2 Invariants in Cohomological Language

In this section, we study the cohomological definitions of quadratic invariants. We define the Stiefel-Whitney classes, each of which gives an invariant space(see [GMS03]).

Let q be a quadratic form of dimension n over K, given by $q = \langle a_1, a_2, \ldots, a_n \rangle$. For indeterminates $X = (X_1, X_2, \ldots, X_n)$, the i^{th} elementary symmetric polynomial in X_i's is defined as

$$f_0(X) = 1$$

$$f_1(X) = X_1 + X_2 + \ldots + X_n$$

$$f_2(X) = \sum_{i,j=1, i<j, i\neq j}^{n} X_i X_j$$

$$f_3(X) = \sum_{i,j,k=1, i<j<k, i\neq j\neq k}^{n} X_i X_j X_k$$

$$\vdots$$

$$f_n(X) = X_1 X_2 \ldots X_n$$

Definition 6.2.1. *The i^{th} Stiefel-Whitney invariant $w_i(q)$ is defined as the ith elementary symmetric polynomial in a_i's computed in the commutative ring $H(K)$ given by*

$$H(K) = \oplus_i H^i(K, \mu_2)$$

Thus, we have

$$w_0(q) = 1$$

$$w_1(q) = \sum_{i=1}^{n} (a_i) = (a_1 a_2 \ldots a_n) = (d(q))$$

$$w_2(q) = \sum_{i,j=1,i<j,i\neq j}^{n} (a_i).(a_j)$$

$$\vdots$$

$$w_n(q) = (a_1).(a_2)\dots(a_n)$$

Here, (a_i) denotes the cohomological class $(a_i) \in H^1(K,\mu_2) \cong \dfrac{\dot{K}}{\dot{K}^2}$ while . is the operation of taking cup-products. We recall that the isomorphism $H^1(K,\mu_2) \cong \dfrac{\dot{K}}{\dot{K}^2}$ has already been established in chapter 4. Each $w_i(q) \in H^i(K,\mu_2)$. The w_i's are indeed invariant for a quadratic form q.

Theorem 6.2.2. *Each $w_i(q)$ gives an invariant of q. For $q \in I(K)$, $w_1(q) = d_{\pm}(q)$ and for $q \in I^2(K)$, $w_2(q) = C(V,q)$.*

Proof. By definition, $w_1(q) = d_{\pm}(q)$ for $q \in I(K)$. We now prove the theorem for $q \in I^2(K)$. We know that $H^2(K,\mu_2) \cong {}_2Br(K)$. Thus, $w_2(q) \in {}_2Br(K)$. Let $q \in I^2(K)$ be a 4-dimensional quadratic form. Then q is generated by 2-fold Pfister forms. Hence, we may assume that

$$q = \langle 1, -c\rangle \otimes \langle 1, -d\rangle$$

Then, $w_2(q) = (-c) \cup (-d)$. The element $(-c) \cup (-d)$ has image $\left(\dfrac{c,d}{K}\right)$ in ${}_2Br(K)$. We are done if we show that $C(V,q)$ is the quaternion algebra $\left(\dfrac{c,d}{K}\right)$. We refer to [[Lam05], 5, 3.1] for this description.
Each $w_i(q)$ is invariant for q for higher values of i as well, however the proof for higher values is technical and long and is therefore skipped. □

Chapter 7

Pfister Numbers of Quadratic Forms

In this section, we try to give bounds on 1*-Pfister number and* 2*-Pfister number of quadratic forms. In §1 the technique of combinatorial analogue is used to determine Pfister numbers of Pfister elements. These Pfister elements help us to determine Pfister numbers of quadratic forms in §2. Finally, in §3 we determine Pfister numbers of quadratic forms of dimension* 6 *using their Stiefel-Whitney invariants and give conditions for* 2*-Pfister number of a quadratic form to be less than* 4*.*

7.1 Introduction

We refer to [PST09] for this chapter. Throughout this chapter, we assume that K is a field of characteristic not equal to 2 and K contains square root of -1. As a consequence, the quadratic form $\langle 1, 1\rangle$ becomes isotropic over K. We use the same notation q for a quadratic form as well as its Witt equivalence class in $W(K)$ i.e. the Witt ring of K. The fundamental ideal of $W(K)$ is denoted by $I(K)$ while $I^m(K)$ denotes the m^{th} power of the fundamental ideal.

We know that $I(K)$ is generated by the Pfister forms $\langle 1, a_i\rangle, a_i \in \dfrac{\dot{K}}{\dot{K}^2}$(refer to chapter 5). Thus, $I^m(K)$ is generated by m-fold Pfister forms i.e. quadratic forms of type

$$\langle 1, a_1\rangle \otimes \langle 1, a_2\rangle \otimes \ldots \otimes \langle 1, a_m\rangle,\ a_1, a_2, \ldots, a_m \in \frac{\dot{K}}{\dot{K}^2}$$

We define *m-Pfister number* $Pf_m(q)$ of a quadratic form $q \in W(K)$ as the least number of terms in decomposition of q as a sum of m-fold Pfister forms.

For $m, n \geq 1$, the *(m,n)-Pfister number* $Pf_K(m,n)$ is defined as the supremum of m-Pfister number $Pf_m(q)$, where q runs over quadratic forms of dimension n in $I^m(L)$ as L runs over field extensions of K.

In a paper by Brosnan, Reichstein and Vistoli [BRV10], it was established that for quadratic forms in $I(K)$, $Pf_K(1,n) \leq n$ and for quadratic forms in $I^2(K)$, $Pf_K(2,n) \leq n-2$. These results are proved in this paper using a combinatorial analogue. Moreover, it is shown that for a quadratic form q_0 of dimension n and having trivial discriminant, $Pf_2(q_0) = n-2$.

7.2 A combinatorial analogue

Let V be an arbitrary vector space over the field $\mathbb{F}_2$ with 2 elements. We consider the group algebra $\mathbb{F}_2[V]$ as a combinatorial analogue of the Witt ring of K. The explanation for this identification is provided below. We refer to [Lam05] for this part.

Consider a complete discretely valued field E with valuation v such that for any $a \in E$,

$$v(a) = m \; if \; a = \pi^m u, \; u \in U$$

where U is the group of units in E. The element π satisfies $v(\pi) = 1$ and therefore is called *uniformizer* of E.

Let

$$A = \{x \in E \; : \; v(x) \geq 0\}$$

Then, A is a subring of E and is called the *valuation ring* of E. The ring A is a local ring with maximal ideal

$$M = \{x \in E \; : \; v(x) \geq 1\}$$

The field $\bar{E} = \dfrac{A}{M}$ is called the *residue class field of* A. For an element $a \in A$, $\bar{a} = a + M$ denotes the image of a in $\dfrac{A}{M}$.

Consider a map

$$i : \frac{\dot{\bar{E}}}{\dot{\bar{E}}^2} \to \frac{\dot{E}}{\dot{E}^2}$$

given by $i(\bar{u}) = u\dot{E}^2$. The map i is well defined because if $\bar{u_1} = \bar{u_2}$, then $i\left(\frac{\bar{u_1}}{\bar{u_2}}\right) = 1\dot{E}^2$. Thus, $u_1\dot{E}^2 = u_2\dot{E}^2$.
Now, we consider the sequence

$$1 \to \frac{\dot{\bar{E}}}{\dot{\bar{E}}^2} \to \frac{\dot{E}}{\dot{E}^2} \xrightarrow{v} \frac{\mathbb{Z}}{2\mathbb{Z}} \to 0$$

Then, $\ker(v) = \{a \in \frac{\dot{E}}{\dot{E}^2} : v(a)\ is\ odd\ \}$. We have

$$\text{img}(i) = i\left(\frac{\dot{\bar{E}}}{\dot{\bar{E}}^2}\right) = \{\dot{E}^2, u_1\dot{E}^2, u_2\dot{E}^2, \ldots\}$$

where $u_1, u_2, \ldots$ are non-square elements of $\dot{E}$. Since $v(u_i\dot{E}^2) = 1$ for all non-square elements of $\dot{E}$, we get $\text{img}(i) = \ker(v)$. Hence, the above sequence is exact. Further, there exists a map

$$\phi : \frac{\mathbb{Z}}{2\mathbb{Z}} \to \frac{\dot{E}}{\dot{E}^2}$$

given by $\phi(1) = \pi\dot{E}^2$. Then, we have $\phi \circ v = v \circ \phi = Id$. Thus, the above sequence is split-exact.
The map i gives a homomorphism from $\hat{W}(\bar{E})$ to $\hat{W}(E)$ where $\hat{W}(E)$ is the Witt-Grothendieck ring associated with the field E.
We define another map $j : \hat{W}(\bar{E}) \to \hat{W}(E)$ given by

$$j(\langle \bar{u_1}, \bar{u_2}, \ldots, \bar{u_s}\rangle) = \pi\langle u_1, u_2, \ldots, u_s\rangle$$

Then, j is a ring homomorphism. The map

$$(i, j) : \hat{W}(\bar{E}) \oplus \hat{W}(\bar{E}) \to \hat{W}(E)$$

given by

$$(i, j)(\langle \bar{u_1}, \bar{u_2}, \ldots, \bar{u_r}\rangle \oplus \langle \bar{u_{r+1}}, \ldots, \bar{u_s}\rangle) = \langle u_1, u_2, \ldots, u_r\rangle \oplus \langle u_{r+1}, \ldots, u_s\rangle$$

is also a ring homomorphism. Since $j(\mathbb{H}) = \pi\mathbb{H} = \mathbb{H}$, we conclude that

$$(i, j) : \frac{\hat{W}(\bar{E}) \oplus \hat{W}(\bar{E})}{\mathbb{Z}.(\mathbb{H}, -\mathbb{H})} \to \hat{W}(E)$$

is a ring homomorphism. Here $\mathbb{Z}.(\mathbb{H}, -\mathbb{H})$ denotes the ideal generated by hyperbolic space $\mathbb{H}$ in the ring $\hat{W}(\bar{E}) \oplus \hat{W}(\bar{E})$. In fact, the above map is an isomorphism. In order to prove this, we define a map

$$\theta : \hat{W}(E) \to \frac{\hat{W}(\bar{E}) \oplus \hat{W}(\bar{E})}{\mathbb{Z}.(\mathbb{H}, -\mathbb{H})}$$

given by

$$\langle u_1, u_2, \ldots, u_r, u_{r+1}, \ldots, u_s\rangle \to \langle \bar{u_1}, \bar{u_2}, \ldots, \bar{u_r}\rangle \perp \pi\langle \bar{u_{r+1}}, \ldots, \bar{u_s}\rangle$$

The map θ is the inverse map of (i, j). Hence, $W(E) \cong W(\bar{E}) \oplus W(\bar{E})$. Since $i(W(\bar{E})) \subseteq W(E)$, we can say that $W(\bar{E})$ sits inside $W(E)$. We now identify $W(\bar{E}) \subseteq W(E)$ by $i(W(\bar{E}))$. The subgroup $(\langle\pi\rangle - 1)(W(\bar{E}))$ is an ideal in $W(E)$ because

$$\langle u\rangle(\langle\pi\rangle - 1)W(\bar{E}) = (\langle\pi\rangle - 1)W(\bar{E})$$

and

$$\langle\pi\rangle(\langle\pi\rangle - 1)W(\bar{E}) = (1 - \langle\pi\rangle)W(\bar{E})$$

Thus $W(E) \cong W(\bar{E}) \oplus (\langle\pi\rangle - 1)W(\bar{E})$. Since

$$(\langle\pi\rangle - 1)(\langle\pi\rangle - 1) = \langle\pi^2, -\pi, -\pi, 1\rangle$$

$$= \langle 1, 1, -\pi, -\pi\rangle = 0$$

the order of $(\langle\pi\rangle - 1)$ in $W(E)$ is 2. Thus,

$$W(E) \cong W(\bar{E})\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)$$

For $\bar{E} = \mathbb{C}$, we get $W(E) \cong \mathbb{F}_2\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)$. Thus, we can identify $W(K)$ with $\mathbb{F}_2[V]$ where V is an $\mathbb{F}_2$ vector space.
A vector $v \in V$ is identified with the element $X^v \in \mathbb{F}_2[V]$. Thus, we have

$$\mathbb{F}_2[V] = \{\sum_{v\in V} a_v X^v \ : \ a_v \in \mathbb{F}_2\}$$

where $a_v \neq 0$ for all but finitely many $v \in V$, $X^0 = 1$ and $X^{v_1}.X^{v_2} = X^{v_1+v_2}$. Consider group homomorphisms

$$\epsilon_0 : \mathbb{F}_2[V] \to \mathbb{F}_2$$

given by

$$\sum_{v\in V} a_v X^v \to \sum_{v\in V} a_v$$

and

$$\epsilon_1 : \mathbb{F}_2[V] \to V$$

given by

$$\sum_{v\in V} a_v X^v \to \sum_{v\in V} a_v v$$

ϵ_0 is called the *augmentation map* . The kernel of ϵ_0 is denoted by $I(V)$. Since ϵ_0 is a ring homomorphism, $I(V)$ is an ideal and is generated by elements of type $1+X^v, v \in V$. Such elements are called *1-fold Pfister elements* of $\mathbb{F}_2[V]$. The elements of type

$$(1 + X^{v_1})(1 + X^{v_2}).....(1 + X^{v_m})$$

are called *m-fold Pfister elements* of $\mathbb{F}_2[V]$. We define $I^m(V)$ as the ideal of $\mathbb{F}_2[V]$ generated by m-fold Pfister elements. For $\xi = \sum_{v\in V} a_v X^v \in \mathbb{F}_2[V]$, we define the *support of* ξ denoted by $D(\xi)$ as

$$D(\xi) = \{v \in V \ : \ a_v \neq 0\} \subseteq V$$

Theorem 7.2.1. *Let $\xi \in \mathbb{F}_2[V]$ be a non-zero element and let $d = |D(\xi)|$ be the cardinality of support of ξ.*

1. *If $\xi \in I[V]$, then $d \geq 2$ and there exist 1-fold Pfister elements $\pi_1, \pi_2, \ldots, \pi_p$ such that*

   $$\xi = \pi_1 + \pi_2 + \ldots + \pi_p$$

   and $p \leq d$. If moreover $0 \in D(\xi)$, the same property holds with $p \leq d - 1$.

2. *If $\xi \in I[V]$ and $\epsilon_1(\xi) = 0$, then $d \geq 4$ and there exist 2-fold Pfister elements $\pi_1, \pi_2, \ldots, \pi_p$ such that*

   $$\xi = \pi_1 + \pi_2 + \ldots + \pi_p$$

   and $p \leq d - 2$. If moreover $0 \in D(\xi)$, the same property holds with $p \leq d - 3$.

Proof. 1. Since $\xi \neq 0$, therefore $d \neq 0$. We observe that $d \equiv \epsilon_0(\xi) \mod 2$ and since $\xi \in I[V]$, we have $\epsilon_0(\xi) = 0$. Thus, d is even. Hence $d \geq 2$. We get

$$\xi = \sum_{v \in D(\xi)} X^v = \sum_{v \in D(\xi)} 1 + X^v$$

Thus, ξ can be written as sum of d 1-fold Pfister elements. If $0 \in D(\xi)$, then $1 + X^0 = 0$ is included in the sum. Thus, $p \leq d - 1$.

2. Since $\xi \in I[V]$, d is even. Let $d = 2$. Then,

$$\xi = X^{v_1} + X^{v_2}$$

where $v_1 \neq v_2, v_1, v_2 \in V$. Since $\epsilon_1(\xi) = 0$, we get $v_1 + v_2 = 0$. Thus, $v_1 = -v_2 = v_2$. This implies that $\xi = 0$. Therefore, $d \geq 4$.
We prove the result by induction on d. We first assume that $0 \in D(\xi)$. Then, since $d \geq 4$, there exist distinct $u, v \in D(\xi)$.
Define

$$\xi' = (1 + X^u)(1 + X^v) + \xi$$

Then,

$$D(\xi') \subseteq D(\xi) \setminus \{u, v, 0\} \cup \{u + v\}$$

As a result, $|D(\xi')| \leq d - 2$. By induction, there exist 2-fold Pfister elements $\pi_1, \pi_2, \ldots, \pi_p$ such that

$$\xi' = \pi_1 + \pi_2 + \ldots + \pi_p,\ p \leq d - 4$$

Then,

$$\xi = \pi_1 + \pi_2 + \ldots + \pi_p + (1 + X^u)(1 + X^v)$$

Thus, ξ can be written as a sum of p 2-fold Pfister elements, where $p \leq d - 3$.
Let $0 \notin D(\xi)$. As above, we define

$$\xi' = (1 + X^u)(1 + X^v) + \xi$$

Then,

$$D(\xi') \subseteq D(\xi) \setminus \{u, v\} \cup \{0, u + v\}$$

Since $0 \in D(\xi')$, we get $|D(\xi')| \leq d$. By induction hypothesis, there exist p 2-fold Pfister elements $\pi_1, \pi_2, \ldots, \pi_p$ such that

$$\xi' = \pi_1 + \pi_2 + \ldots + \pi_p,\ p \leq d-3$$

Then,

$$\xi = \pi_1 + \pi_2 + \ldots + \pi_p + (1+X^u)(1+X^v)$$

Thus, ξ can be written as a sum of p 2-fold Pfister elements with $p \leq d-2$. Hence, the result is proved.

□

Corollary 7.2.2. $I^2[V] = \{\xi \in I[V] : \epsilon_1(\xi) = 0\}$

Proof. From the proof of first part of Theorem 6.2.1, we can conclude that $I[V]$ is spanned by 1-fold Pfister elements i.e. elements of type $(1+X^v)$. Therefore, $I^2[V]$ is spanned by 2-fold Pfister elements i.e. elements of type $(1+X^{v_1})(1+X^{v_2})$. For each such element, $\epsilon_1[(1+X^{v_1})(1+X^{v_2})] = 0$. Thus, we get

$$I^2[V] \subseteq \{\xi \in I[V] \mid \epsilon_1(\xi) = 0\}$$

If $\xi \in I[V]$ satisfies $\epsilon_1(\xi) = 0$, then second part of Theorem 6.2.1 shows that $\xi \in I^2[V]$. Hence, the result is proved. □

Theorem 7.2.3. *For $\xi \in I[V]$, we have*

$$Pf_1(\xi) = \begin{cases} |D(\xi)| & \text{if } 0 \notin D(\xi), \\ |D(\xi)| - 1 & \text{if } 0 \in D(\xi). \end{cases}$$

Here, $Pf_1(\xi)$ is defined as the least number of terms occurring in decomposition of ξ as a sum of 1-fold Pfister elements.

Proof. Let $p = Pf_1(\xi)$. Then, $\xi = \sum_{i=1}^{p}(1+X^{v_i}) = p + \sum_{i=1}^{p} X^{v_i}$. Therefore, $D(\xi) \subseteq \{0, v_1, v_2, \ldots, v_p\}$. We get $|D(\xi)| \leq p$ if $0 \notin D(\xi)$ and $|D(\xi)| \leq p+1$ if $0 \in D(\xi)$. The reverse inequalities follow from Theorem 6.2.1. □

Now, we talk about 2-Pfister numbers of quadratic forms $q \in I^2(K)$. We already know (from first part of Theorem 6.2.1) that for $\xi \in I^2[V]$,

$$Pf_2(\xi) \leq \begin{cases} |D(\xi)| - 2 & \text{if } 0 \notin D(\xi), \\ |D(\xi)| - 3 & \text{if } 0 \in D(\xi). \end{cases}$$

We now give a specific element $\xi_e \in \mathbb{F}_2[V]$ for which $Pf_2(\xi_e) = |D(\xi_e)| - 2$. Before that, we make some remarks.

Remark 7.2.4. For vector spaces V and W, a map $\phi : V \to W$ induces a map

$$\phi^* : \mathbb{F}_2[V] \to \mathbb{F}_2[W]$$

given by

$$\phi^* \left(\sum_{v \in V} a_v X^v \right) \to \sum_{v \in V} a_v X^{\phi(v)}$$

We observe that for every $m \geq 1$, image of an m-fold Pfister element in $\mathbb{F}_2[V]$ is an m-fold Pfister element in $\mathbb{F}_2[W]$. Thus, $Pf_m(\phi^*(\xi)) \leq Pf_m(\xi)$.

Consider an $\mathbb{F}_2$-vector space V of dimension $n > 1$, and let $e = \{e_i\}_{i=1}^n$ be a basis for V. Define $e_0 = \sum_{i=1}^n e_i$. Let

$$\xi_e = n + 1 + \sum_{i=0}^{n} X^{e_i}$$

Then, we observe that $\epsilon_0(\xi_e) = 0$ and $\epsilon_1(\xi_e) = 0$. Therefore, from Theorem 6.2, we get $\xi_e \in I^2[V]$. Note that for even n

$$D(\xi_e) = \{e_0, e_1, ..., e_n, 0\}$$

and for odd n

$$D(\xi_e) = \{e_0, e_1, ..., e_n\}$$

From Theorem 6.2.1, we get

$$Pf_2(\xi_e) \leq n - 1$$

if n is odd and

$$Pf_2(\xi_e) \leq n - 1$$

if n is even. We shall show that $Pf_2(\xi_e) = n - 1$.

Theorem 7.2.5. $Pf_2(\xi_e) = n - 1$

Proof. Let $n = 2$. Then

$$\xi_e = 1 + X^{e_1} + X^{e_2} + X^{e_1 e_2} = (1 + X^{e_1})(1 + X^{e_2})$$

We get $Pf_2(\xi_e) = 1$. Hence, theorem holds for $n = 2$.
Let $n = 3$. Then

$$\xi_e = X^{e_1} + X^{e_2} + X^{e_3} + X^{e_1} X^{e_2} X^{e_3}$$

Since $0 \notin D(\xi_e)$, ξ_e is not a 2-fold Pfister element. Hence, $Pf_2(\xi_e) > 1$. Since $Pf_2(\xi_e) \leq 2$, we get $Pf_2(\xi_e) = 2$. Thus, theorem holds for $n = 3$.
We now prove the result for $n > 3$. Let $p = Pf_2(\xi_e)$ and let $\pi_1, \pi_2, \ldots, \pi_p$ be 2-fold Pfister elements such that

$$\xi_e = \pi_1 + \pi_2 + \ldots + \pi_p$$

Then, $D(\xi_e) \subseteq \cup_{i=1}^{p} D(\pi_i)$. This implies that $e_n \in D(\pi_i)$ for some i. Let $e_n \in D(\pi_p)$. Then,

$$\pi_p = 1 + X^{e_n} + X^{v} + X^{e_n + v}$$

for some $v \in V$.
Let $W \subseteq V$ be the $\mathbb{F}_2$ span of $e_1, e_2, \ldots, e_{n-1}$. Let $f_0 = \sum_{i=1}^{n-1} e_i \in W$. The set $f = (e_i)_{i=1}^{n-1}$ forms a basis of W and we can construct ξ_f as

$$\xi_f = n + X^{f_0} + \sum_{i=1}^{n-1} X^{e_i}$$

Consider a linear map $\phi : V \to W$ given by

$$\phi(e_i) = e_i \; for \; 1 \leq i \leq n - 1$$

$$\phi(e_n) = 0$$

The map ϕ induces a ring homomorphism

$$\phi^* : \mathbb{F}_2[V] \to \mathbb{F}_2[W]$$

Consequently, $\phi^*(X^{e_n}) = 1$. Since $\phi(e_0) = f_0$, it follows that $\phi(\xi_e) = \xi_f$. Thus, we can write

$$\xi_f = \phi^*(\pi_1) + \phi^*(\pi_2) + \ldots + \phi^*(\pi_p)$$

Note that $\phi^*(\pi_p) = 0$. As a result, $Pf_2(\xi_f) \leq p-1$. Since $\dim(W) = n-1$, by induction hypothesis, $Pf_2(\xi_f) = n-2$. This implies that

$$n-2 \leq p-1$$

Hence, $n-1 \leq p$. The reverse inequality $p \leq n-1$ already holds. We get $p = n-1$. Hence the result is proved. □

7.3 Pfister Numbers of Generic Forms

Let K be a field of characteristic $\neq 2$ that contains square root of -1. Let $V_K = \dfrac{\dot{K}}{\dot{K}^2}$. V_K can be realized as a vector space over $\mathbb{F}_2$. We define a map $\phi : V_K \to W(K)$ given by $\phi(a\dot{K}^2) = \langle a \rangle$, $a \in \dot{K}$. Then, ϕ is a homomorphism and thus, induces a surjective $\mathbb{F}_2$-algebra homomorphism

$$\phi^* : \mathbb{F}_2[V_K] \to W(K)$$

The map ϕ^* carries 1-fold Pfister elements in $\mathbb{F}_2[V_K]$ to 1-fold Pfister forms in $W(K)$. As a result, image of m-fold Pfister elements in $\mathbb{F}_2[V_K]$ is m-fold Pfister forms in $W(K)$. Therefore, from remark 7.2.4, we have

$$Pf_m(\phi^*(\xi)) \leq Pf_m(\xi) \ \forall \ \xi \in \mathbb{F}_2[V_K], \ m \geq 1$$

Theorem 7.3.1. *Let q be a quadratic form of dimension n over a field K as above.*

1. *If $q \in I(K)$, then $Pf_1(q) \leq n$. Moreover, if q represents 1, then $Pf_1(q) \leq n-1$.*
2. *If $q \in I^2(K)$, then $Pf_2(q) \leq n-2$. Moreover, if q represents 1, then $Pf_2(q) \leq n-3$.*

Proof. 1. Let $q = \langle a_1, a_2, \ldots, a_n \rangle$. Consider an element

$$\xi = a_1\dot{K}^2 + a_2\dot{K}^2 + \ldots + a_n\dot{K}^2 \in \mathbb{F}_2[V_K]$$

Then, $\phi^*(\xi) = q$ and $D(\xi) = \{a_1\dot{K}^2, a_2\dot{K}^2, \ldots, a_n\dot{K}^2\}$. We get $|D(\xi)| = n$. If $q \in I(K)$, then n is even and $\xi \in I[V_K]$. Thus, $Pf_1(\xi) = n$. Since $Pf_1(\phi^*(\xi)) \leq Pf_1(\xi)$, we get $Pf_1(q) \leq n$.
If q represents 1, then $0 \in D(\xi)$ and therefore $Pf_1(\xi) = n-1$. This implies that $Pf_1(q) \leq n-1$.

2. If $q \in I^2(K)$, then n is even and $a_1, a_2, \ldots, a_n \in \dot{K}^2$. Thus, $\epsilon_1(\xi) = 0$. From corollary 6.2.2, we get $\xi \in I^2[V_K]$. We have $D(\xi) = \{a_1\dot{K}^2, a_2\dot{K}^2, \ldots, a_n\dot{K}^2\}$. Thus, $Pf_2(\xi) \leq n-2$ if $0 \notin D(\xi)$. If q represents 1, then $0 \in D(\xi)$ and $Pf_2(q) \leq Pf_2(\xi) \leq n-3$. Hence, the theorem is proved.

□

Illustration

- Let $q = \langle a_1, a_2, \ldots, a_n\rangle$. If $q \in I(K)$, then n is even and q is Witt equivalent to $\left(\frac{n}{2}\right) \times \langle 1, -1\rangle \oplus q$. Therefore, we can write

$$q = \langle 1, a_1\rangle - \langle 1, -a_2\rangle + \ldots - \langle 1, -a_n\rangle = \langle\langle a_1\rangle\rangle - \langle\langle -a_2\rangle\rangle + \ldots - \langle\langle -a_n\rangle\rangle$$

  We get $Pf_1(q) = n$. If any of the a_i's is a square, then the Pfister number further decreases.

- If q represents 1, then we have $q = \langle 1, a_1, a_2, \ldots, a_{n-1}\rangle$. In this case, q is Witt equivalent to $\left(\frac{n-2}{2}\right) \times \langle 1, -1\rangle \oplus q$. Therefore, we get

$$q = \langle\langle a_1\rangle\rangle - \langle\langle a_2\rangle\rangle + \ldots - \langle\langle -a_{n-2}\rangle\rangle + \langle\langle a_{n-1}\rangle\rangle$$

  We get $Pf_1(q) = n-1$. If any of the a_i's is a square, then the Pfister number further decreases.

- Let $q = \langle a_1, a_2, \ldots, a_{n-1}, a_1a_2\ldots a_{n-1}\rangle$ and let n be even. Then, $q \in I^2(K)$. We calculate $Pf_2(q)$ for $n = 4$ and $n = 6$.
  If $n = 4$, then $q = \langle a_1, a_2, a_3, a_1a_2a_3\rangle$. We can write

$$q = \langle 1, a_1, a_2, a_1a_2\rangle \oplus \langle -1, -a_1a_2, a_3, a_1a_2a_3\rangle = \langle\langle a_1, a_2\rangle\rangle - \langle\langle a_1a_2, -a_3\rangle\rangle$$

  Therefore, $Pf_2(q) = 2$.
  Let $\dim(q) = 6$. Then, $q = \langle a_1, a_2, a_3, a_4, a_5, -a_1a_2a_3a_4a_5\rangle$. The negative sign appears because in this case, $d(q) = -1\dot{K}^2$. We can write

$$\begin{aligned} q &= \langle 1, a_1, a_2, a_1a_2, -1, a_3, a_4, -a_3a_4, 1, a_5, -a_1a_2, -a_1a_2a_5, -1, a_3a_4, a_1a_2a_5, -a_1a_2a_3a_4a_5\rangle \\ &= \langle\langle a_1, a_2\rangle\rangle - \langle\langle -a_3, -a_4\rangle\rangle + \langle\langle a_5, -a_1a_2\rangle\rangle - \langle\langle -a_3a_4, -a_1a_2a_5\rangle\rangle \end{aligned}$$

  Therefore, $Pf_2(q) = 4$.

- We are left with the case for $q \in I^2(K)$ and simultaneously representing 1. The explanation for this case proceeds similarly as above and is therefore skipped.

We conclude that theorem 7.3.1 holds even for fields not containing square root of -1 since in the above illustration we have nowhere used the assumption that $\sqrt{-1} \in K$. We now try to construct quadratic forms for which the upper bound of n-Pfister number is reached.
Let n be an integer greater than 1. Consider n independent indeterminates $x_1, x_2, \ldots, x_n$ over K . Let $x_0 = x_1x_2x_3 \ldots x_n$. Let $L = K(x_1, x_2, \ldots, x_n)$. Consider quadratic forms

$$q = \langle x_1, x_2, \ldots, x_n \rangle,\ q_0 = \langle x_0, x_1, \ldots, x_n \rangle$$

$$q' = \langle 1, x_1, x_2, \ldots, x_n \rangle,\ q'_0 = \langle 1, x_0, x_1, \ldots, x_n \rangle$$

If n is even, then $q \in I(L)$ and $q'_0 \in I^2(L)$. If n is odd, $q' \in I(L)$ and $q_0 \in I^2(L)$.

Theorem 7.3.2. *If n is even, then*

$$Pf_1(q) = n \text{ and } Pf_2(q'_0) = n - 1$$

If n is odd, then

$$Pf_1(q') = n \text{ and } Pf_2(q_0) = n - 1$$

Proof. Let Ω be the algebraic closure of K. Consider the field

$$F = \Omega((x_1))((x_2)) \ldots ((x_n))$$

i.e. the field of iterated Laurent series. We want to establish an isomorphism

$$W(F) \cong \mathbb{F}_2 \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \right)^n$$

We refer to section 7.2 for this description.
We use this isomorphism to identify Pfister forms in $W(F)$ with Pfister elements in $\mathbb{F}_2 \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \right)^n$. The isomorphism ψ maps $W(\Omega)$ to $\mathbb{F}_2$ and quadratic form $\langle x_i \rangle$ to X^{e_i}, where e_i is the ith basis element of the vector space $\left(\frac{\mathbb{Z}}{2\mathbb{Z}} \right)^n$, $1 \leq i \leq n$. The $(x_1, x_2, ..., x_n)$-adic valuation on F yields an isomorphism

$$\frac{\dot{F}}{\dot{F}^2} \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \right)^n$$

This isomorphism maps $x_i\dot{F}^2$ to e_i. Let $e_0 = \sum_{i=1}^{n} e_i$. We have

$$q = \langle x_1, x_2, \ldots, x_n \rangle,\ q_0 = \langle x_0, x_1, \ldots, x_n \rangle$$

$$q' = \langle 1, x_1, \ldots, x_n \rangle,\ q'_0 = \langle 1, x_0, x_1, \ldots, x_n \rangle$$

Then,

$$\psi(q_F) = \sum_{i=1}^{n} X^{e_i},\ \psi(q_{0F}) = \sum_{i=0}^{n} X^{e_i}$$

$$\psi(q'_F) = 1 + \sum_{i=1}^{n} X^{e_i},\ \psi(q'_{0F}) = 1 + \sum_{i=0}^{n} X^{e_i}$$

Define

$$\xi_e = n + 1 + \sum_{i=0}^{n} X^{e_i} \in \mathbb{F}_2 \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \right)^n$$

If n is even, then $\xi_e = \psi(q'_{0F})$ and if n is odd, $\xi_e = \psi(q_{0F})$. The isomorphism ψ maps m-fold Pfister elements to m-fold Pfister forms and thus preserves the m-Pfister number of elements. From Theorem 6.2.4, we have $Pf_2(\xi_e) = n - 1$. Thus,

$$Pf_2(q'_{0F}) = n - 1$$

when n is even, and

$$Pf_2(q_{0F}) = n - 1$$

when n is odd. Also,

$$Pf_1(q_F) = n$$

for even n, and

$$Pf_1(q'_F) = n$$

for odd n. This implies that when n is even

$$Pf_2(q'_0) \geq n - 1\ ,\ Pf_1(q) \geq n$$

and when n is odd,

$$Pf_2(q_0) \geq n - 1\ ,\ Pf_1(q') \geq n$$

The reverse inequalities follow from Theorem 6.3.1. Hence, the theorem is proved. □

Corollary 7.3.3. *$Pf_K(1, m) = m$ for every even integer $m \geq 2$ and $Pf_K(2, m) = m - 2$ for every even integer $m \geq 4$.*

Proof. We recall that $Pf_K(m,n)$ is the supremum of m-Pfister number of quadratic forms q of dimension n in $I^m(L)$ as L runs over field extensions of K.
If m is even, the quadratic form q above with dimension m satisfies $q \in I(K)$ and $Pf_1(q) = m$. Thus, $Pf_K(1,m) \geq m$.
For $m \geq 4$, consider the quadratic form q_0 defined above with dimension $m = n+1$. The form $q_0 \in I^2(K)$ and satisfies $Pf_2(q_0) = n-1 = m-2$. Thus, $Pf_K(2,m) \geq m-2$. The reverse inequalities follow from Theorem 6.3.1. Thus, we conclude that for m even,

$$Pf_K(1,m) = m,\ m \geq 2$$

and

$$Pf_K(2,m) = m-2,\ m \geq 4$$

□

7.4 Low-dimensional Forms

We now talk about quadratic forms of dimension 6. These forms are characterized using their Stiefel-Whitney invariants $w(q)$ and the Pfister numbers are obtained accordingly.

Theorem 7.4.1. *Let q be an anisotropic quadratic form of dimension 6. We assume that $q \in I^2(K)$ and q represents 1. If $w_4(q) = 0$, then $Pf_2(q) = 2$. If $w_4(q) \neq 0$, then $Pf_2(q) = 3$.*

Proof. From Theorem 6.3.1, we know that for an anisotropic quadratic form of dimension n, $Pf_2(q) \leq n-3$, if q represents 1. Thus, if q has dimension 6 and represents 1, then $Pf_2(q) \leq 3$. It is obvious that $Pf_2(q) \neq 1$. Thus, $Pf_2(q)$ is either 2 or 3. It is sufficient to prove that $Pf_2(q) = 2$ if and only if the Stiefel-Whitney invariant $w_4(q) = 0$.
We first assume that $Pf_2(q) = 2$. Then,

$$q = \langle a, b, ab, c, d, cd \rangle$$

We can write $q = q_1 \perp q_2$ where $q_1 = \langle 1, a, b, ab \rangle$ and $q_2 = \langle 1, c, d, cd \rangle$. Then, we have

$$w_4(q) = \sum_{i+j=4} w_i(q_1) w_j(q_2)$$

As a result, $w_4(q) = (a) \cup (b) \cup (c) \cup (d)$. Since q represents 1, the form $\langle 1 \rangle \perp q$ is isotropic. The 4-fold Pfister form $\langle\langle a, b, c, d \rangle\rangle$ which contains $\langle 1 \rangle \perp q$ as a subform becomes isotropic. Since every isotropic Pfister form is hyperbolic, we get that $\langle\langle a, b, c, d \rangle\rangle$ is hyperbolic. Hence, the Stiefel-Whitney invariant

$$(a) \cup (b) \cup (c) \cup (d) = 0$$

Conversely, let $w_4(q) = 0$. Since q represents 1, we assume that $q = \langle 1, a, b, c, d, abcd \rangle$. Then, $w_4(q) = (a) \cup (b) \cup (c) \cup (d) = 0$. We use the following result from [Ara75]:
Let $e^n_{q,F} : I^n(F) \to H^n F$ be defined as

$$\langle 1, -a_1 \rangle \otimes \langle 1, -a_2 \rangle \otimes \ldots \otimes \langle 1, -a_n \rangle \to (a_1) \cup (a_2) \cup \ldots \cup (a_n)$$

Let ρ and σ be two 4-fold Pfister forms over F. Suppose that $e^4_F(\sigma) = e^4_F(\rho)$. Then $\rho \cong \sigma$.
We take the 4-fold Pfister form $\langle\langle a, b, c, d \rangle\rangle$ as σ and the hyperbolic form $\langle\langle 1, 1, 1, 1 \rangle\rangle$ as ρ. Then

$$e^4_F(\sigma) = (a) \cup (b) \cup (c) \cup (d) = 0 = e^4_F(\rho)$$

Thus, $\langle\langle a, b, c, d \rangle\rangle$is hyperbolic. As a result, its 9-fold subform $q \perp \langle ab, ac, ad \rangle$ is isotropic. Hence, q represents a non-zero element of type $a(bx^2 + cy^2 + dz^2)$ where $x, y, z \in \dot{K}$.
Let $b' = bx^2 + cy^2 + dz^2$. Since the form $\langle b, c, d \rangle$ represents b', we can find $c', d' \in \dot{K}$ such that

$$\langle b, c, d \rangle \cong \langle b', c', d' \rangle$$

Then, $bcd = b'c'd'$ modulo $\dot{K}^2$. Thus,

$$\langle 1, a, b, c, d, abcd \rangle \cong \langle 1, a, b', c', d', ab'c'd' \rangle$$

Since q is anisotropic, the form $\langle 1, a, b' \rangle$ is anisotropic. Thus, the 2-fold Pfister form $\langle\langle a, b' \rangle\rangle$ is anisotropic. This is because if $\langle\langle a, b' \rangle\rangle$ were isotropic, then it would have been hyperbolic and so every 3-dimensional subform of $\langle\langle a, b' \rangle\rangle$ would have been isotropic, which is not the case.
Since q represents ab', the form $q \perp \langle ab' \rangle$ is isotropic. Hence, $\langle\langle a, b' \rangle\rangle$ represents a non-zero element $c'r^2 + d's^2 + ab'c'd't^2$, $r, s, t \in \dot{K}$. Let $c'' = c'r^2 + d's^2 + ab'c'd't^2 \in \dot{K}$

and let $d'' \in \dot{K}$ be such that

$$\langle c', d', ab'c'd' \rangle \cong \langle c'', d'', ab'c''d'' \rangle$$

Then, $q = \langle 1, a, b', c'', d'', ab'c''d'' \rangle$. Since $\langle\langle a, b' \rangle\rangle$ represents c'', the form $\langle\langle a, b', c'' \rangle\rangle$ is isotropic and hence hyperbolic. Therefore, its 5-dimensional subform $\langle 1, a, b', c'', abc'' \rangle$ is isotropic. Consequently, $\langle 1, a, b', c'' \rangle$ represents $ab'c''$. Thus,

$$\langle 1, a, b', c'' \rangle \cong \langle ab'c'', u, v, uv \rangle$$

for some $u, v \in \dot{K}$. We get

$$q = \langle ab'c'', u, v, uv, d'', ab'c''d'' \rangle = \langle\langle u, v \rangle\rangle \perp \langle\langle ab'c'', d'' \rangle\rangle$$

Thus, $Pf_2(q) = 2$. Hence, the result is proved. □

We now discuss effects of scaling on the Pfister number of an anisotropic quadratic form of dimension 6. If a, b, c, d, e are indeterminates over K and

$$q = \langle a, b, c, d, e, abcde \rangle$$

then by Theorem 6.3.2, $Pf_2(q) = 4$. On scaling q by a, we get

$$\langle a \rangle q = \langle 1, ab, ac, ad, ae, bcde \rangle$$

We can view the elements ab, ac, ad, ae as indeterminates over K and again by using Theorem 6.6, we get $Pf_2(\langle a \rangle q) = 3$. Thus, scaling q by a 1-dimensional subform reduces its Pfister number.
Now, consider

$$\langle abc \rangle q = \langle bc, ac, ab, abcd, abce, de \rangle$$

Then

$$\langle abc \rangle q = \langle\langle ab, ac \rangle\rangle \perp \langle\langle abce, de \rangle\rangle$$

Thus, $Pf_2(\langle abc \rangle q) = 2$. In fact, it is true that scaling q by the discriminant of any of its 3-dimensional subform reduces the Pfister number to 2. Therefore, we are now interested in studying the conditions required for $Pf_2(\langle \lambda \rangle q) = 2$ where $\lambda \in \dot{K}$ and q is an anisotropic form of dimension 6.

Let $q = \langle\langle a, b \rangle\rangle \perp \langle\langle c, d \rangle\rangle$. The form q is assumed to have $Pf_2(q) = 2$ since any

quadratic form of dimension 6 can be written as a scalar multiple of a quadratic form with 2-Pfister number equal to 2. The biquaternion algebra associated with q is denoted by $D = (a,b)_K \otimes (c,d)_K$. We refer to sections 5.2 and 5.3 for this description.

Theorem 7.4.2. *For $\lambda \in \dot{K}$, $Pf_2(\langle\lambda\rangle q) = 2$ if and only if λ^2 is the reduced norm of some σ-symmetric element in the biquaternion algebra D i.e. $\lambda^2 = \mathrm{nrd}_D(u)$ for some $u \in Sym(D,\sigma)$. Here, the involution σ on D is the tensor product of the conjugation involutions on $(a,b)_K$ and $(c,d)_K$.*

Proof. The proof of this theorem uses several results from [KMRT98] which are stated in the appendix. Let $(a,b)_K^0$(resp. $(c,d)_K^0$) denote the K-vector space of pure quaternions in $(a,b)_K$(resp. $(c,d)_K$). Then,

$$Skew(D,\sigma) = ((a,b)_K^0 \otimes 1) \oplus (1 \otimes (c,d)_K^0)$$

Define a linear operator p_σ on $Skew(D,\sigma)$ as

$$p_\sigma(x \otimes 1 + 1 \otimes y) = x \otimes 1 - 1 \otimes y$$

for $x \in (a,b)_K^0$ and $y \in (c,d)_K^0$. Then $q_\sigma(s) = sp_\sigma(s)$ defines a quadratic form on $Skew(D,\sigma)$ given by

$$q_\sigma \cong \langle a, b, ab, c, d, cd\rangle = q$$

Let $Pf_2(\langle\lambda\rangle q) = 2$ for some $\lambda \in \dot{K}$. We fix a decomposition

$$\langle\lambda\rangle q = \langle\langle a', b'\rangle\rangle \perp \langle\langle c', d'\rangle\rangle$$

Using [[Lam05], ch.5, 3.1], we get that Clifford algebras of q and $\langle\lambda\rangle q$ are isomorphic. Since D is Brauer-equivalent to Clifford algebra of q, we conclude that

$$D = (a', b')_K \otimes (c', d')_K$$

Let σ' denote the orthogonal involution on D given by taking tensor product of conjugation involutions of $(a', b')_K$ and $(c', d')_K$. From Theorem $A.0.4$, there exists a unit $u \in Sym(D,\sigma)$ such that

$$\sigma'(x) = u\sigma(x)u^{-1} \ \forall \ x \in D$$

We define a linear operator $p_{\sigma'}$ and a quadratic form $q_{\sigma'}$ on $Skew(D,\sigma')$ in the same way as p_σ and q_σ to get

$$q_{\sigma'} \cong \langle\lambda\rangle q$$

We observe that

$$Skew(D,\sigma') = uSkew(D,\sigma) = Skew(D,\sigma)u^{-1}$$

We define a linear operator p' on $Skew(D,\sigma')$ as

$$p'(s') = up_\sigma(s'u) \ \forall \ s' \in Skew(D,\sigma')$$

Then, p' satisfies

$$s'p'(s') = s'up_\sigma(s'u) = q_\sigma(s'u) \in K$$

Using Theorem $A.0.5$, we deduce that p' is a multiple of $p_{\sigma'}$ i.e. there exists $\lambda_1 \in \dot{K}$ such that $p' = \lambda_1 p_{\sigma'}$. It follows that

$$s'p'(s') = \lambda_1 q_{\sigma'}(s') \ \forall \ s' \in Skew(D,\sigma')$$

The map $s' \to s'u$ is an isometry. Therefore, $\langle\lambda_1\rangle q_{\sigma'} \cong q_\sigma$. Hence, $\langle\lambda_1\lambda\rangle q \cong q$. This implies that $\langle\lambda_1\lambda\rangle$ is a multiplier of similitude of q(refer to appendix for this part). Since λ_1^2 is also a multiplier and the set of multipliers forms a group, we get that $\lambda\lambda_1^{-1}$ is a multiplier of a similitude of q. From Theorem $A.0.6$, we may find $\lambda_2 \in \dot{K}$ and $v \in \dot{D}$ such that

$$\lambda\lambda_1^{-1} = \lambda_2^2 \mathrm{nrd}_D(v)$$

On the other hand, for $s' \in Skew(D,\sigma')$, we have $q_\sigma(s'u)^2 = \mathrm{nrd}_D(s'u)$ and $q_{\sigma'}(s')^2 = \mathrm{nrd}_D(s')$ from Theorem $A.0.7$. Thus, we get $\lambda_1^2 = \mathrm{nrd}_D(u)$. So

$$\lambda^2 = \lambda_1^2\lambda_2^4 \mathrm{nrd}_D(v)^2 = \mathrm{nrd}_D(\lambda_2 vu\sigma(v))$$

Since $\lambda_2 vu\sigma(v) \in Sym(D,\sigma)$, this is the desired element i.e. we have found an element $\lambda_2 vu\sigma(v) \in Sym(D,\sigma)$ satisfying $\lambda^2 = \mathrm{nrd}(\lambda_2 vu\sigma(v))$.
Conversely, let $\lambda^2 = \mathrm{nrd}_D(u)$ for some $u \in Sym(D,\sigma)$. We define an orthogonal involution σ' on D as $\sigma' = Int(u) \circ \sigma$. Using Theorem $A.0.8$, we deduce that $disc(\sigma') = \mathrm{nrd}_D(u) = \lambda^2$. From Theorem $A.0.9$, we may find quaternion subalgebras

$(a', b')_K, (c', d')_K \subseteq D$ such that

$$D = (a', b')_K \otimes (c', d')_K$$

the involution σ' being the tensor product of conjugation involutions on $(a', b')_K$ and $(c', d')_K$. We may, then define, $p_{\sigma'}$ and $q_{\sigma'}$ as before and we have

$$q_{\sigma'} \cong \langle a', b', a'b', c', d', c'd' \rangle$$

On the other hand, we define a linear operator p_0 and a quadratic form q_0 on $Skew(D, \sigma)$ by

$$p_0(s') = \lambda^{-1} u p_\sigma(s'u)$$

and

$$q_0(s') = \lambda^{-1} q_\sigma(s'u) \ \forall \ s' \in Skew(D, \sigma')$$

By definition, we have

$$q_0 \cong \langle \lambda \rangle q_\sigma \cong \langle \lambda \rangle q$$

Moreover, $s'p_0(s') = q_0(s') \in K$ for $s' \in Skew(D, \sigma)$, hence p_0 is a multiple of $p_{\sigma'}$.
We have $p_0 = \mu p_{\sigma'}$ for some $\mu \in \dot{K}$. Hence, $q_0 = \mu q_{\sigma'}$.
For $s' \in Skew(D, \sigma')$, we have

$$p_0^2(s') = \lambda^{-2} u p_\sigma(u p_\sigma(s'u)u) = \lambda^{-2} \mathrm{nrd}_D(u) p_\sigma^2(s'u) u^{-1}$$

Since $p_\sigma^2 = id$ and $\mathrm{nrd}_D(u) = \lambda^2$, it follows that $p_0^2 = Id$. Since $p_{\sigma'}^2 = Id$, we get $\mu = \pm 1$. Therefore,

$$q_0 = \langle \pm 1 \rangle q_{\sigma'} \cong q_{\sigma'}$$

We get

$$\langle \lambda \rangle q = \langle a', b', a'b', c', d', c'd' \rangle$$

Hence $Pf_2(\langle \lambda \rangle q) = 2$. □

Theorem 7.4.3. *Let $q \in I^2(K)$ be an anisotropic quadratic form of dimension 6. Then, $Pf_2(q) \leq 3$ if and only if there exists a 4-dimensional quadratic form q_1 and scalars $\mu, \mu', \nu \in \dot{K}$ such that*

1. $q \cong q_1 \perp \langle \mu \rangle \langle\langle \nu \rangle\rangle$
2. $Pf_2(q_1 \perp \langle \mu' \rangle \langle\langle \nu \rangle\rangle) \leq 2$

3. $\langle\langle \mu, \mu', \nu \rangle\rangle = 0$

Proof. Let $Pf_2(q) \leq 3$. Then, we can write

$$q = \langle\langle a, b \rangle\rangle \perp \langle\langle c, d \rangle\rangle \perp \langle\langle e, f \rangle\rangle$$

$$q = \langle a, b, ab, c, d, cd \rangle \perp \langle 1, e, f, ef \rangle$$

Since $\dim(q) = 6$, there exists a quadratic form $\langle \mu \rangle\langle 1, \nu \rangle$ which is a subform of both $\langle a, b, ab, c, d, cd \rangle$ and $\langle 1, e, f, ef \rangle$. This implies that

$$\langle a, b, ab, c, d, cd \rangle = q_1 \perp \langle \mu \rangle\langle 1, \nu \rangle$$

where $\dim(q_1) = 4$. We get

$$Pf_2(q_1 \perp \langle \mu \rangle\langle 1, \nu \rangle) \leq 2$$

We also have

$$\langle 1, e, f, ef \rangle = \langle a_1, a_2 \rangle \perp \langle \mu \rangle\langle 1, \nu \rangle$$

Comparing discriminants on both sides, we get

$$a_1 a_2 \equiv \nu \dot{K}^2$$

Thus, $a_1 a_2 = \nu \mu'^2$ for some $\mu' \in \dot{K}$. This gives

$$\langle 1, e, f, ef \rangle = \langle \mu' \rangle\langle 1, \nu \rangle \perp \langle \mu \rangle\langle 1, \nu \rangle$$

Adding the two equations above, we get

$$q = q_1 \perp \langle \mu' \rangle\langle 1, \nu \rangle$$

The quadratic form $\langle \mu', \mu \rangle\langle 1, \nu \rangle$ represents 1 and therefore $\langle 1, \mu, \mu', \mu\nu, \mu'\nu \rangle$ is isotropic. Since $\langle 1, \mu, \mu', \mu\nu, \mu'\nu \rangle$ occurs as a subform of $\langle\langle \mu, \mu', \nu \rangle\rangle$, we get

$$\langle\langle \mu, \mu', \nu \rangle\rangle = 0$$

Conversely, suppose there exists a 4-dimensional quadratic form q and scalars $\mu, \mu', \nu \in \dot{K}$ such that $1, 2$ and 3 hold. Then, $\langle\langle \mu, \mu', \nu \rangle\rangle = 0$ implies

$$\langle 1, \mu \rangle \otimes \langle 1, \mu' \rangle \otimes \langle 1, \nu \rangle = \langle 1, \mu, \mu', \nu \rangle \otimes \langle 1, \nu \rangle = \langle 1, \nu, \mu, \mu\nu, \mu', \mu'\nu, \mu\mu', \mu\mu'\nu \rangle$$

is isotropic. Therefore,

$$q_1 \perp \langle \mu \rangle \langle 1, \nu \rangle \perp \langle \mu' \rangle \langle 1, \nu \rangle = q_1 \perp \langle 1, \nu \rangle \perp \langle \mu, \mu' \rangle \langle 1, \nu \rangle$$

$$\Rightarrow q_1 \perp \langle \mu' \rangle \langle 1, \nu \rangle = q_1 \perp \langle 1, \nu \rangle \langle 1, \mu\mu' \rangle \perp \langle \mu \rangle \langle 1, \nu \rangle$$

Thus, $Pf_2(q) \leq 3$. Hence, the result is proved. □

It is difficult to give an illustration for the above theorem because of the following results(see [BS66]).

Theorem 7.4.4 (Chevalley-Warning Theorem)**.** *Let $f(x_1, \ldots, x_n)$ be a quadratic form with integer coefficients. If $n \geq 3$, then the congruence*

$$f(x_1, \ldots, x_n) \equiv 0 \mod p$$

has a non-zero solution.

Theorem 7.4.5. *Any quadratic form q over the field $\mathbb{Q}_p$ of p-adic numbers in five or more variables always has a non-zero solution.*

Theorem 7.4.6 (Hasse-Minkowski Theorem). *A quadratic form q over $\mathbb{Q}$ is isotropic if and only if it is isotropic over $\mathbb{Q}_p$ for all q and over $\mathbb{R}$.*

As a consequence, for $K = \mathbb{Q}, \mathbb{Q}_p, \mathbb{F}_p, \mathbb{R}$, every quadratic form of dimension 6 is isotropic over $K(\sqrt{-1})$.

Appendix A

Some important theorems

We refer to [KMRT98] for proofs of the following theorems.

Theorem A.0.7. *Let $\mathcal{A}$ be a central simple algebra over a field K and let σ be an orthogonal involution on $\mathcal{A}$. Then*

1. *For each unit $u \in \dot{\mathcal{A}}$ such that $\sigma(u) = \pm u$, the map $Int(u) \circ \sigma$ is an involution of first kind on $\mathcal{A}$. Here $Int(u)$ refers to the inner automorphism given by $x \to uxu^{-1}$.*

2. *Conversely, for every involution σ' of the first kind on $\mathcal{A}$, there exists some $u \in \dot{\mathcal{A}}$ uniquely determined upto a factor in $\dot{K}$ such that $\sigma' = Int(u) \circ \sigma$ and $\sigma(u) = \pm u$.*

Theorem A.0.8. *Let σ be an orthogonal involution on a biquaternion K-algebra $\mathcal{A}$. There exists a linear endomorphism*

$$p_\sigma : Skew(\mathcal{A}, \sigma) \to Skew(\mathcal{A}, \sigma)$$

which satisfies the following two conditions:

1. *$xp_\sigma(x) = p_\sigma(x)x \in K \ \forall \ x \in Skew(\mathcal{A}, \sigma)$*

2. *An element $x \in Skew(\mathcal{A}, \sigma)$ is invertible if and only if $xp_\sigma(x) \neq 0$.*

The endomorphism p_σ is uniquely determined upto a factor in $\dot{K}$. More precisely, if $p_{\sigma'} : Skew(\mathcal{A}, \sigma) \to Skew(\mathcal{A}, \sigma)$ is a linear map such that $xp_{\sigma'}(x) \in K$ for all $x \in Skew(\mathcal{A}, \sigma)$ (or $p_{\sigma'}(x)x \in K$ for all $x \in Skew(\mathcal{A}, \sigma)$), then

$$p_{\sigma'} = \lambda p_\sigma$$

for some $\lambda \in K$.

Definition A.0.9. *Let* $(\mathcal{A}, \sigma)$ *be a central simple algebra over* K *with involution* σ. *A similitude of* $(\mathcal{A}, \sigma)$ *is an element* $g \in \mathcal{A}$ *such that*

$$\sigma(g)g \in \dot{K}$$

The scalar $\sigma(g)g$ *is called the multiplier of* g *and is denoted by* $\mu(g)$. *The set of all similitudes of* $(\mathcal{A}, \sigma)$ *forms a subgroup of* $\dot{\mathcal{A}}$.

Theorem A.0.10. *Let* $\mathcal{A}$ *be a central simple algebra over* K. *The multipliers of similitudes of* $(\mathcal{A}, \sigma, f)$ *are given by*

$$G(\mathcal{A}, \sigma, f) = \dot{K}^2 \mathrm{nrd}_E(\dot{E})$$

where $C(\mathcal{A}, \sigma, f) \cong E \times E^{op}$, E *being a central simple* K *algebra of degree* 4.

Theorem A.0.11. *Let* σ *be an orthogonal involution on a biquaternion* K*-algebra* $\mathcal{A}$. *Let* p_σ *be a non-zero linear endomorphism of* $Skew(\mathcal{A}, \sigma)$ *such that* $xp_\sigma(x) \in K \ \forall \ x \in Skew(\mathcal{A}, \sigma)$ *and let* $q_\sigma : Skew(\mathcal{A}, \sigma) \to K$ *be the quadratic map defined by*

$$q_\sigma(x) = xp_\sigma(x) \ \forall \ x \in Skew(\mathcal{A}, \sigma)$$

Then, there exists some $d_\sigma \in \dot{K}$ *such that*

1. $q_\sigma(x)^2 = d_\sigma \mathrm{nrd}_{\mathcal{A}}(x) \ \forall \ x \in Skew(\mathcal{A}, \sigma)$
2. $p_\sigma^2 = d_\sigma . id_{Skew(\mathcal{A}, \sigma)}$

Theorem A.0.12. *Let* $\mathcal{A}$ *be a central simple algebra of even degree* $n = 2m$ *over a field* K. *Suppose* σ *is an orthogonal involution on* $\mathcal{A}$ *and let* $u \in \dot{\mathcal{A}}$. *If* $Int(u) \circ \sigma$ *is an orthogonal involution on* $\mathcal{A}$, *then*

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

where

$$disc(\sigma) = (-1)^m det(\sigma) \in \frac{\dot{K}}{\dot{K}^2}$$

and

$$det(\sigma) = \mathrm{nrd}_{\mathcal{A}}(a).\dot{K}^2 \in \frac{\dot{K}}{\dot{K}^2} \ for \ a \in Alt(\mathcal{A}, \sigma) \cap \dot{\mathcal{A}}$$

Theorem A.0.13. *Every central simple algebra $\mathcal{A}$ of degree 4 and exponent 2 is a biquaternion algebra.*

Bibliography

[Ara75] Jón Kr. Arason, *Cohomologische invarianten quadratischer Formen*, J. Algebra **36** (1975), no. 3, 448–491. MR 0389761 (52 #10592)

[Ber10] Grégory Berhuy, *An introduction to Galois cohomology and its applications*, London Mathematical Society Lecture Note Series, vol. 377, Cambridge University Press, Cambridge, 2010, With a foreword by Jean-Pierre Tignol. MR 2723693 (2011i:12010)

[BRV10] Patrick Brosnan, Zinovy Reichstein, and Angelo Vistoli, *Essential dimension, spinor groups, and quadratic forms*, Ann. of Math. (2) **171** (2010), no. 1, 533–544. MR 2630047 (2011f:11053)

[BS66] A. I. Borevich and I. R. Shafarevich, *Number theory*, Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20, Academic Press, New York-London, 1966. MR 0195803 (33 #4001)

[Bur89] David M. Burton, *Elementary number theory*, second ed., W. C. Brown Publishers, Dubuque, IA, 1989. MR 990017 (90e:11001)

[Dal06] Chandan Singh Dalawat, *Some aspects of the functor K_2 of fields*, J. Ramanujan Math. Soc. **21** (2006), no. 2, 129–151. MR 2243064 (2007b:19002)

[GMS03] Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series, vol. 28, American Mathematical Society, Providence, RI, 2003. MR 1999383 (2004f:11034)

[KMRT98] M.-A. Knus, A. S. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, 1998.

[Lam05] T. Y. Lam, *Introduction to quadratic forms over fields*, American Mathematical Society, 2005.

[Mor96] Patrick Morandi, *Field and Galois theory*, Graduate Texts in Mathematics, vol. 167, Springer-Verlag, New York, 1996. MR 1410264 (97i:12001)

[Pfi95] Albrecht Pfister, *Quadratic forms with applications to algebraic geometry and topology*, London Mathematical Society Lecture Note Series, vol. 217, Cambridge University Press, Cambridge, 1995. MR 1366652 (97c:11046)

[PST09] R. Parimala, V. Suresh, and J.-P. Tignol, *On the Pfister number of quadratic forms*, Quadratic forms—algebra, arithmetic, and geometry, Contemp. Math., vol. 493, Amer. Math. Soc., Providence, RI, 2009, pp. 327–338. MR 2537109 (2010g:11065)

[Sch85] W. Scharlau, *Quadratic and hermitian forms*, Springer-Verlag, 1985.

Index