Quadratic Forms and Milnor's Conjecture

Narendran E

This document contains notes on quadratic forms and Milnor's Conjecture made as part of my Master's thesis under Prof Utsav Choudhury during the 6th semester of my MMath program at Indian Statistical Institute.
We first introduce quadratic forms on vector spaces and study properties concerning the decomposition of the quadratic forms. We follow this by introducing a group structure on the set of quadratic forms over a field.
Later we study Milnor K-theory of a field and relation between Milnor K-theory and Witt rings. In the final section we prove the case $n = 1$ of Milnor's conjecture, concerning the relation between Milnor K-theory and Galois cohomology.

Quadratic Forms

An (n-ary) quadratic form over a field F(char $\neq 2$) is a polynomial f in n variables over FF that is homogeneous of degree 2. It can be written as

$$f(X_1,\ldots,X_n) = \sum_{i,j=1} a_{ij}X_iX_j = F[X]$$

We can rewrite the above as $\sum_{i,j}\frac{1}{2}(a_{ij}+a_{ji})X_iX_j = \sum_{i,j}a'_{ij}X_iX_j$ to get an expression with symmetric coefficients. This deteremines an unique symmetric matrix $M_f = (a'_{ij})$. So in-terms of matrix notation we have $f(X) = X^tM_fX$.

Two quadratic forms are said to be equivalent, if $\exists C \in GL_n(F)$ such that $f(X) = g(C\cdot X)$. In terms of their symmetric matrices, we have $M_f = C^tM_gC$.
An example is the equivalence of the forms $f = X_1^2 - X_2^2$ and $g = X_1X_2$, with the matrix $C = \left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)$

A quadratic form f gives rise to a map $Q_f : F^n \to F$ defined by $Q_f(x) := x^tM_fx$ called as the *quadratic map* defined by f. The quadratic map Q_f determines uniquely the quadratic form f. For if $Q_f = Q_g$ then it follows that $M_f = M_g$ and $f = g$.(Here char$F \neq 2$)

Let us observe some properties of the quadratic map:

1. $Q_f(ax) = a^2Q_f(x)$
2. We polarize Q_f by setting $B_f(x,y) = \frac{1}{2}[Q(x+y) - Q(x) - Q(y)]$. Then B_f is a symmetric bilinear pairing. The quadratic map Q_f can be obtained from the bilinear form by defining $Q_f(x) = B_f(x,x)$.

1.1 Quadratic spaces

The pair (V,B) is called a quadratic space if V is a finite dimensional space and $B : V\times V \to F$ is a symmetric bilinear pairing on V. We associate a quadratic map $q_B : V \to F$ given by $q(x) = B(x,x)$. Since q and B determine each other we can denote the space as (V,q). The quadratic space gives rise to a quadratic form $f = \sum_{i,j}B(e_i,e_j)X_iX_j$. The quadratic space uniquely determines the equivalence class of quadratic forms. Since if we choose another basis $\{e'_i\}$ then the matrices of the forms are related by the change of basis matrix.

Two quadratic spaces $(V,B),(V',B')$ are isometric if there exists an isomorphism $\tau : V \to V'$ such that $B'(\tau(x),\tau(y)) = B(x,y)$. Thus $(V,B) \cong (V',B') \iff (f_B) = (f'_B)$. Thus there is a one-one correspondence between the equivalence classes of n-ary quadratic forms and the isometry classes of n-dimensional quadratic spaces.

Let (V,B) be a quadratic space, and let M be a symmetric matrix associated to one of the forms in the equivalence class (f_B).

Proposition. *The following statements are equivalent:*

1. *M is a nonsingular matrix.*
2. *$x \mapsto B(\_,x)$ 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 that $x = 0$.*

Proof.

$1 \implies 2$ Since M is non singular there exists some $v \in V$ such that $B(v,x) \neq 0$. Thus the linear map $x \mapsto B(-,x)$ is injective and hence an isomorphism.

$3 \implies 1$ If M is singular then there exists non zero v such that $Mv = 0$. Then $B(v,e_i) = 0$ for all i. This implies $v = 0$ and that is a contradiction.

□

Proposition. *For a regular quadratic space (V,B) and a subspace S, we have*

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

Proof. Consider the map $x \mapsto (B,x)$ from $V \to V^*$. $S^{\perp}$ is annihilated by all the functionals in $\phi(S)$. So we have $\dim S^{\perp} = \dim V^* - \dim \phi(S) = \dim V - \dim S$

□

1.2 Diagonalization of quadratic forms

A quadratic form f represents $d \in \dot{F}$ if there exists $x_i \in F$ such that $f(x_1,\ldots x_n) = d$. $D(f)$ denotes the set of values in $\dot{F}$ represented by f.Note that $d \in D(f)$ iff $a^2 d \in D(f)$.

$D(f)$ in general need not be a group. For example $f = x^2 + y^2 + z^2$ has $1,2,2^{-1},14 \in D(f)$, but $7 \notin D(f)$.

If $(V_1,B_1),(V_2,B_2)$ are quadratic spaces, we may form (V,B), where $V = V_1 \oplus V_2$, and B is the pairing $V \times V \to F$ given by

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

This implies

$$q_B(x_1,x_2) = q_B(x_1) + q_B(x_2)$$

Theorem 1.2.1. *Let (V,B) be a quadratic space, and $d \in \dot{F}$. Then $d \in D(V)$ iff there exists another quadratic space (V',B') together with an isometry $V \cong \langle d \rangle \perp V'$.*

Here $\langle d \rangle$ denotes the isometry class of one dimensional vector spaces corresponding to the quadratic form dX_1^2.

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

$$\dim(F \cdot v) + \dim(F \cdot v)^{\perp} = \dim V$$

by dimnension formula, we conclude that $V \cong \langle d \rangle \perp (F \cdot v)^{\perp}$.

□

Corollary 1.2.1.1. *If (V,B) is any quadratic space then there exists $d_i \in F$ such that $V \cong \langle d_1 \rangle + \cdots + \langle d_n \rangle$. So the quadratic form is equal to the form $d_1X_1^2 + \cdots + d_nX_n^2$.*

Proof. If $D(V)$ is empty, then $B \equiv 0$ and V is isometric to an orthogonal sum of $\langle 0 \rangle$'s. If there exists some $d \in D(V)$, then $V \cong \langle d \rangle \perp V'$ for some (V',B'), and the proof proceeds by induction on $\dim V$. □

Corollary 1.2.1.2. *If (V,B) is a quadratic space (not necessarily regular) and S is a regular subspace, then:*

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

Proof. (1) $\Rightarrow$ (2). If $V = S \perp T$, then, clearly, $T \subseteq S^{\perp}$. But $\dim T = \dim V - \dim S = \dim S^{\perp}$ by (1) (not by dimension formula), so we must have $T = S^{\perp}$.
(1) Since $S \cap S^{\perp} = \operatorname{rad} S = 0$, it suffices to show that V is spanned by S and $S^{\perp}$. By 2.4, S has an orthogonal basis $x_1, \ldots, x_p$, and the regularity of S implies that $B(x_i,x_i) \neq 0$ for all i. Given any $z \in V$, consider the vector

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

We have

$$\begin{aligned} B(y,x_j) &= B(z,x_j) - \sum_{i=1}^{p} \frac{B(z,x_i)}{B(x_i,x_i)} B(x_i,x_j) \\ &= B(z,x_j) - \frac{B(z,x_j)}{B(x_j,x_j)} B(x_j,x_j) = 0 \end{aligned}$$

Thus, $y \in S^{\perp}$, and

$$z = y + \sum_{i=1}^{p} \frac{B(z,x_i)}{B(x_i,x_i)} x_i \in S \perp S^{\perp}$$

□

Corollary 1.2.1.3. *Let (V,B) be a regular quadratic space. Then a subspace S is regular iff there exists $T \subset V$ such that $V = S \perp T$.*

The determinant of a non singular quadratic form is defined as $d(f) = \det(M_f) \cdot \dot{F}^2$ as an element of $\dot{F}/\dot{F}^2$. The determinant is same on the equivalence class of quadratic forms. Also $d(f_1 \perp f_2) = d(f_1)d(f_2)$.

1.3 Hyperbolic planes and Hyperbolic spaces

A nonzero vector v in a quadratic space (B,V) is called isotropic vector if $B(v,v) = 0$. Otherwise it is called an anisotropic vector. A quadatic space is isotropic if it contains an isotropic vector.(V,B) is totally isotropic if all the nonzero vectors are isotropic, i.e. $B \equiv 0$

Theorem 1.3.1. *Let (V,q) be a 2 -dimensional quadratic space. The following four statements are equivalent:*

1. *V is regular and isotropic.*
2. *V is regular, with $d(V) = -1 \cdot \dot{F}^2$.*
3. *V is isometric to $\langle 1,-1\rangle$.*
4. *V corresponds to the equivalence class of the binary quadratic form X_1X_2.*

The isometry class of quadratic spaces satisfying the above conditions is called hyperbolic plane, denoted by $\mathbb{H}$. The orthogonal sum of such planes is called hyperbolic space and the corresponding orthogonal sum is $X_1X_2 + \cdots + X_{2m-1}X_{2m}$.

Proof. $(1) \Rightarrow (2)$: Let x_1, x_2 be an orthogonal basis for V. Regularity of V implies that $q(x_i) = d_i \neq 0 (i = 1,2)$. Let $ax_1 + bx_2$ be an isotropic vector, with (say) $a \neq 0$. Then

$$\begin{aligned} 0 = q(ax_1 + bx_2) = a^2d_1 + b^2d_2 &\Longrightarrow d_1 = -\left(ba^{-1}\right)^2 \cdot d_2 \\ &\Longrightarrow d(V) = d_1d_2 \cdot \dot{F}^2 = -1 \cdot \dot{F}^2 \end{aligned}$$

$(2) \Rightarrow (3)$: Under the hypothesis (2), we have clearly a diagonalization, $V \cong \langle a,-a\rangle$ for some $a \in \dot{F}$. By the argument in 1.1, we know that $aX_1^2 - aX_2^2$ is equivalent to aX_1X_2. The latter clearly represents all elements in $\dot{F}$. In particular, (V,q) itself represents 1. By the Representation Criterion, we conclude that $V \cong \langle 1,-1\rangle$. □

The isometry class of the 2-dimensional quadratic spaces satisfying the above conditions is called the hyperbolic plane.

A quadratic form is universal if it represents all the nonzero elements of F.

Theorem 1.3.2. *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 iff V contains a hyperbolic plane (necessarily as an orthogonal summand, by 1.2.1.2).*

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

Proof. We prove (1) by induction on r. Take any basis $x_1,\ldots,x_r$ in U, and let S be the span of $x_2,\ldots,x_r$. Of course, $U^\perp \subseteq S^\perp$. Since V is regular, we get

$$\dim S^\perp = \dim V - \dim S > \dim V - \dim U = \dim U^\perp$$

This means that there exists a vector y_1 that is orthogonal to $x_2,\ldots,x_r$, but not orthogonal to x_1. In particular, x_1, y_1 are linearly independent vectors (since x_1 is isotropic). The subspace $H_1 = Fx_1 + Fy_1$ has determinant

$$d(H_1) = \begin{vmatrix} 0 & B(x_1,y_1) \\ B(x_1,y_1) & B(y_1,y_1) \end{vmatrix} \cdot \dot{F}^2 = -1 \cdot F^2$$

so $H_1 \cong \mathbb{H}$ by Theorem 3.2. We have thus a splitting $V = H_1 \perp V'$, where $V' = H_1^\perp$ contains $x_2,\ldots,x_r$ (1.2.1.2). Since V' is regular (Corollary 1.3.2), the proof proceeds by induction.
(1) $\Rightarrow$ (2) is clear by putting $r = 1$ in (1).
(2) $\Rightarrow$ (3) is follows because the form X_1X_2 corresponding to $\mathbb{H}$ is universal.

□

The hyperbolic plane $\mathbb{H}$ is isotropic and regular. So it is universal.

Theorem 1.3.3 (First Representation theorem)**.** *If q is a regular form and $d \in \dot{F}$. Then $d \in D(q) \iff q \perp \langle -d \rangle$ is isotropic.*

Proof. $q(x) = \sum_i a_i x_i^2$. Then $q(x) = d$ implies that $\sum_i a_i x_i^2 + (-d)(1)^2 = 0$.
$\iff q \perp \langle -d \rangle$ is isotropic.
Conversely if $x_1,\ldots,x_n$ is an isotropic vector then $a_1x_1^2 + \cdots + dx_{n+1}^2 = 0$.
If x_{n+1} is non zero then this gives a representation of d If $x_{n+1} = 0$ then $(x_1,\ldots,x_n)$ is an isotropic vector for q. This implies q is universal. □

A simple application of the previous theorem is the following corollary

Corollary 1.3.3.1. *For a positive integer r, the following are equivalent*

1. *regular quadratic form of* $\dim r$ *is universal.*

2. *quadratic form of* $\dim r + 1$ *is isotropic.*

1.4 Witt's Decomposition Theorem

Theorem 1.4.1. *Any quadratic space (V,q) can be decomposed into*

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

where V_t, V_h, V_a are totally isotropic, hyperbolic and anisotropic subsapces respectively and the isometry types of these spaces are uniquely determined.

We introduce some notations and prove Witt's cancellation theorem before proving this theorem.

For a quadratic space (V,B,q) denote by $O(V)$ the group of isometris of (V,q). For every anisotropic vector $y \in V$, define

$$\tau_y = x - 2\frac{2B(x,y)}{q(y)}y \in O(V)$$

1. τ_y is an endomorphism.
2. $\tau_y|_{(F.y)^\perp} = Id$
3. $\det \tau_y = -1$
4. $\{\tau_y | q(y) \neq 0\}$ is closed under conjugation.

Theorem 1.4.2 (Witt's Cancellation theorem)**.** *If q, q_1, q_2 are quadratic forms and $q \perp q_1 \cong q \perp q_2$ then $q_1 \cong q_2$*

Proof.

Step 1 Cancellation holds if q is totally isotropic and q_1 is regular. In fact, let M_1, M_2 be the symmetric matrices associated with q_1 and q_2. The hypohhesis implies that $\begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix}$ is congruent to $\begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix}$, so there exists an invertible matrix $E = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ such that

$$\begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix} = E^t \begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix} E = \begin{pmatrix} * & * \\ * & D^t M_2 D \end{pmatrix}$$

In particular, $M_1 = D^t M_2 D$. Since M_1 is nonsingular, so is D, and hence M_1, M_2 are congruent. This gives $q_1 \cong q_2$.

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

$$q \perp r\langle 0\rangle \perp q_1' \cong q \perp r\langle 0\rangle \perp q_2'.$$

Since q_1' is regular, Step 1 implies that $q_1' \cong q_2'$. By tagging on r terms of $\langle 0\rangle$, we conclude that $q_1 \cong q_2$.

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

□

Now we can prove Witt's decompsition theorem

Proof. For existence, take any subspace V_0 such that

$$V = \mathrm{rad}(V) \perp V_0.$$

Then $V_t = \mathrm{rad}\, V$ is totally isotropic, and V_0 is regular. If V_0 is isotropic, we may write $V_0 = H_1 \perp V_1$ (by 1.3.2), where $H_1 \cong \mathbb{H}$. If V_1 is again isotropic, we may further write $V_1 = H_2 \perp V_2$, where $H_2 \cong \mathbb{H}$. After a finite number of steps, we get

$$V_0 = (H_1 \perp \cdots \perp H_r) \perp V_a \quad (r \geq 0),$$

where $H_1 \perp \cdots \perp H_r = V_h$ is hyperbolic (or zero), and V_a is anisotropic. This proves the existence part.

To establish the uniqueness part, suppose V has another "Witt decomposition," $V = V_t' \perp V_h' \perp V_a'$. Since V_t' is totally isotropic and $V_h' \perp V_a'$ is regular, we have

$$\mathrm{rad}\, V = \left(\mathrm{rad}\, V_t'\right) \perp \mathrm{rad}\left(V_h' \perp V_a'\right) = V_t'$$

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

□

Proposition. *If $q = \langle a, b\rangle$ and $q' = \langle c, d\rangle$. Then $q \cong q'$ iff $d(q) = d(q')$ and q and q' represents a common element $e \in \dot{F}$*

Proof. If $d(q) = d(q')$ and $e \in D(q) \cap D(q')$, then by the representation criterion, $q \cong < e, e' >$ for some $e' \in \dot{F}$. Taking determinants, $ab = ee' mod \dot{F}^2$. So we have $q \cong < e, abe >$. Similarly, $q' \cong < e, cde >$. $ab = cd mod \dot{F}^2$. So $q \cong q'$ □

Simple equivalence for diagonal forms:- $q = \langle a_1, \ldots, a_n\rangle$ and $a' = \langle b_1 \ldots, b_n\rangle$
q and q' are simply equivalent if there exists i, j such that

1. $\langle a_i, a_j\rangle \simeq \langle b_i, b_j\rangle$
2. $a_k = b_k$ when $k \notin \{i, j\}$

Two diagonal forms are chain equivalent if there exists a sequence of diagonal forms $f_0, \ldots f_m$ such that $f_0 = f$ and $f_m = g$ and each f_i is simply equivalent to f_{i+1}.
Clearly $f \approx g$ implies $f \cong g$. Witt's chain equivalence theorem says the converse is true.

Theorem 1.4.3. *If f and g are arbitrary diagonal forms, then $f \cong g \implies f \approx g$.*

Proof. Say $f = \langle a_1, \ldots, a_n\rangle, g = \langle b_1, \ldots, b_n\rangle$. Note that if σ is a permutation of the indices $\{1, 2, \ldots, n\}$, and $f^\sigma = \left\langle a_{\sigma(1)}, \ldots, a_{\sigma(n)}\right\rangle$, then $f \approx f^\sigma$. This follows from the observation that the full symmetric group on $\{1, \ldots, n\}$ is generated by the transpositions. Since $f \cong g$, the two forms, f and g, have the same number of zero terms in their diagonalizations. It is, therefore, sufficient to show that the "regular parts" of f and g are chain-equivalent. We may thus assume that f, g are both

regular, that is, a_i, b_j are all nonzero. The argument is by induction on n. There is nothing to prove if $n = 1, 2$, so we consider $n \geq 3$ in the following.

Among all diagonal forms that are chain-equivalent to f, choose an $f' = \langle c_1, \ldots, c_n \rangle$ such that some $\langle c_1, \ldots, c_p \rangle$ represents b_1, and p is smallest possible. (The existence of f' follows from the Well-Ordering Principle.) *We* claim that $p = 1$. In fact, suppose the contrary. Write $b_1 = c_1 e_1^2 + \cdots + c_p e_p^2$ $(p \geq 2)$. By the minimality of p, no subsum in this summation can be equal to zero. In particular, $d = c_1 e_1^2 + c_2 e_2^2 \neq 0$. By 2.3, $\langle c_1, c_2 \rangle \cong \langle d, c_1 c_2 d \rangle$. Thus,

$$\begin{aligned} f \approx f' &= \langle c_1, c_2, c_3, \ldots, c_n \rangle \\ &\approx \langle d, c_1 c_2 d, c_3, \ldots, c_p, \ldots, c_n \rangle \\ &\approx \langle d, c_3, \ldots, c_p, \ldots, c_n, c_1 c_2 d \rangle \end{aligned}$$

and $b_1 = d + c_3 e_3^2 + \cdots + c_p e_p^2$ is already represented by $\langle d, c_3, \ldots, c_p \rangle$, which has dimension $p-1$, contradicting the choice of p. We have thus shown that $p = 1$. Hence $\langle c_1 \rangle \cong \langle b_1 \rangle$, and so $f \approx \langle b_1, c_2, \ldots, c_n \rangle$. By Witt's Cancellation Theorem,

$$\langle b_1, c_2, \ldots, c_n \rangle \cong \langle b_1, b_2, \ldots, b_n \rangle \Longrightarrow \langle c_2, \ldots, c_n \rangle \cong \langle b_2, \ldots, b_n \rangle$$

By the inductive hypothesis, this implies that $\langle c_2, \ldots, c_n \rangle \approx \langle b_2, \ldots, b_n \rangle$. So finally, $f \approx \langle b_1, c_2, \ldots, c_n \rangle \approx \langle b_1, b_2, \ldots, b_n \rangle = g$.

□

Proposition. *Let $\phi = << a_1, \ldots, a_n >>$ be an n-fold Pfister form and $b \in D_F(\phi')$ where $\phi = 1 + \phi'$, then there exists $b_2, \ldots, b_n$ such that $\phi \approx << b, b_2, \ldots, b_n >>$*

$<< a_1, \ldots a_n >>$ and $<< b_1, \ldots, b_n >>$ are p-equivalent if there exists i, j such that $<< a_i, a_j >> \approx << b_i, b_j >>$ and $a_k = b_k \, \forall k$

Proof. If $n = 1$ then $\phi = < 1, a_1 >$ then we have $< b > \cong < a_1 >$. Then $\phi \cong < b, a_1 >$
Let $\tau = << a_1, \ldots a_{n-1} >> \cong < 1 > + \tau'$
Then $\phi \cong \tau < 1, a_n > \cong \tau \perp < a_n > \tau$. So $\phi' \cong \tau' \perp < a_n > \tau$.
$b \in D_F \phi'$, then there exists $x \in D_f \tau' \cup \{0\}$ and $y \in D_F(\tau) \cup \{0\}$ such that $b + x + a_n y$. Let $y = t^2 + y_0$ for some $y_0 \in D_F(\tau') \cup \{0\}$

Case 1 $y = 0$, then $0 \neq b = x \in D_F(\tau')$. By inductive hypothesis, $\exists d_2, \ldots, d_n \in \dot{F}$ such that $\tau \approx << x, d_2, \ldots, d_{n-1} >>$
Thus $\phi \approx << x, d_2, \ldots, d_{n-1}, a_n >> = << b, d_2, \ldots, d_{n-1}, a_n >>$

Case 2 $y \neq 0$. We claim that $\phi \approx << a_1, \ldots, a_{n-1}, a_n y >>$.
If $y_0 = 0$, $y = t^2$ then we are done. If $y_0 \neq 0$ then $\tau \approx << y_0, c_2, \ldots, c_{n-1} >>$
$\phi \approx << y_0, c_2, \ldots c_{n-1}, a_n >>$
$\approx << y_0, c_2, \ldots c_{n-1}, a_n(t^2 + y_0) >>$ [1]
$\approx << b, d_2, \ldots, d_{n-1}, a_n y >>$

Corollary 1.4.3.1. *If a Pfister form is isotropic, then it is hyperbolic*

[1] $x \in D(<< a >>), << a, b >> \approx < 1, a > \perp < b > < x, xa > \approx << a, bx >>$

Proof. Since ϕ contains a hyperbolic form, $-1 \in D_f(\phi')$ by Witt's Cancellation theorem. So $\phi \approx << -1, \cdots >>$ which is hyperbolic

□

□

Grothendieck Witt Rings

Let $M(F)$=isometry class of nonsinglar quadratic forms over field F. Id (V,B,q_1) and (W,B_2,q_2) are two vector spaces. Then the "multiplication" is given by the tensor product. If $V = V_1 \otimes V_2$ then the bilinear form on V is given by

$$B : V \times V \to F$$

$$(V_1 \otimes w_1, v_2 \otimes w_2) \mapsto B(v_1,w_1)B(v_2,w_2)$$

This is a dim mn vector space. The Kronecker product of matrices gives the matrix of bilinear form for V.

The operations $\perp$ and $\otimes$ give $M(F)$ a semiring structures. We want to introduct a group structure on $M(F)$.

Defihne a relation on $M \times M$, $(x,y) \sim (x',y')$ iff $x+y' = x'+y$. The Wtt's cancellation law in M makes $\sim$ an equivalence relation.

Define $\text{Groth}(M) = M \times M/\sim$ with $(x,y)+(x',y') = (x+x', y+y')$. It is a simple observation that $[(x,y)]+[(y,x)] = [(0,0)]$. This makes $\text{Groth}(M)$ into a group. We can view M as a subset of $\text{Groth}(M)$

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

$$x \mapsto (x,0)$$

So $(x,y) = x-y$ in $\text{Groth}(M)$. Since M has multiplication operation $(\otimes)$ which makes it into a semiring, then $(x,y)(x',y') = (xx'+yy', yx'+xy')$ makes $Groth(M)$ into a ring.

This $\text{Groth}(M) = \widehat{W}(F)$ is called the Witt-Grothendieck ring of quadratic forms over field F. Every element of $\widehat{W}(F)$ is of the form $q_1 - q_2$. The map $\dim : M(F) \to \mathbb{Z}$ extends to a map from $\widehat{W}(F) \to \mathbb{Z}$ because of the universal property, where we have $\dim(q_1-q_2) = \dim q_1 - \dim q_2$. The kernel of this dimension map is called the fundamental ideal, $\widehat{I}(F)$. This gives us

$$\frac{\widehat{W}(F)}{\widehat{I}(F)} \cong \mathbb{Z}$$

Proposition. *$\widehat{I}(F)$ is generated by expressions of the form $\{\langle a\rangle - \langle 1\rangle\}$ where $a \notin F$*

Proof. For $q \in \widehat{I}(F)$, $q = q_1 - q_2$ and $\dim q_1 = \dim q_2$. So if we write $q_1 =< a_1, \cdots, a_n >$ and $q_2 =< b_1, \cdots, b_n >$, then $q = \sum < a_i > -1 - \{< b_i - 1 >\}$

□

Proposition. *If q represens a regualr quadratic form, then* $q \otimes \mathbb{H} = \dim q \cdot \mathbb{H}$

SO $\mathbb{Z}\mathbb{H}$ is an ideal of $\widehat{W}(F)$ consisting of all hyperbolic spaces and their inverses.

$$W(F) = \frac{\widehat{W}(F)}{\mathbb{Z}\mathbb{H}}$$

is defined as the Witt ring of F.

Theorem 2.0.1. *Elements of* $W(F)$ *are in one to one correspondence with the isometry class of all anisotropic forms.*

Proof. Note that $\langle -a \rangle = -\langle a \rangle$ in $W(F)$. So every element of $W(F)$ is represented by some form q. From decomposition theorem we know $q = q_a \perp q_h$ and q_h is zero in $W(F)$. □

We have a natural map from $\widehat{W}(F) \to W(F)$. The image of the ideal $\widehat{I}(F)$ under this map is denoted as $IF = \frac{\widehat{I}(F)}{\mathbb{Z}\mathbb{H}}$ and is called the fundamental ideal of $W(F)$.Since $\dim \mathbb{H} = 2$, $\mathbb{Z} \cap \widehat{I}(F) = \{0\}$. This implies $\widehat{I}(F) \cong IF$.

Proposition. *A form q represents an element in IF and only if* $\dim q$ *is even*

Proof. If q is an even dimensional quadratic form, we may assume that it is a binary form, say, $q = \langle a, b \rangle$. Then q is the image of $\langle a \rangle - \langle -b \rangle \in \widehat{I}F$ under the natural projection $\widehat{W}(F) \to W(F)$. By definition, this says that $q \in IF \subseteq W(F)$.
COnversely suppose q represents an element in IF, then $q = q_1 - q_2 + m\mathbb{H} \in \widehat{W}(F)$, where $m \in \mathbb{Z}$ and $\dim q_1 = \dim q_2$. Applying the map dim, we see that $\dim q = 2m$. □

The ring epimorphism $\dim : \widehat{W}(F) \to \mathbb{Z}$ induces another epimorphism $\widehat{W}(F)/\mathbb{Z} \cdot \mathbb{H} = W(F) \to \mathbb{Z}/2\mathbb{Z}$, which we shall denote by dimo. By the above proposition, $\ker(\dim_0) = IF$, so we obtain:

Corollary 2.0.1.1. $\dim_0$ *defines an isomorphism* $W(F)/IF \cong \mathbb{Z}/2\mathbb{Z}$.

2.1 Square Class Groups

We can define a monoid homomorphism $d : M(F) \to \dot{F}/\dot{F}^2$ by

$$d(q_1 - q_2) = d(q_1)d(q_2)^{-1} = d(q_1)d(q_2)$$

(d is the determinant of a quadratic form as defined earlier)this extends to a group homomorphism from $\widehat{W}(F)$ to $\dot{F}/\dot{F}^2$.

If q is a non singular form of dimension n, define the signed determinant of q by

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

.

Define

$$Q(F) = \mathbb{Z}_2 \times (\dot{F}/\dot{F}^2)$$

as a set and define the binary operation

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

The identity element is $(0,1)$ and $(e,d)^{-1} = (e,(-1)^e d)$
$Q(F)$ is a split extension if and only if -1 is a square element modulo F.

Proposition.

$$(\dim_0, d_\pm) : MF \to QF$$

is a monoid epimorphism, this extends to a group homomorphism

$$(\dim_0, d_\pm) : \widehat{W}(F) \to QF$$

This induces isomorphism

$$f : \frac{WF}{I^2F} \xrightarrow{\simeq} QF$$

Proof. . The map $M(F) \to Q(F)$ sends a form q to

$$(\dim_0 q, d_\pm(q)) \in Q(F)$$

To check that it is a monoid homomorphism, we calculate as follows (where $\dim q = n$, and $\dim q' = n'$) :

$$\begin{aligned}
&(\dim_0\ , d_\pm)(q) \cdot (\dim_0, d_\pm)\left(q'\right) \\
&\quad = \left(n, (-1)^{n(n-1)/2} d(q)\right)\left(n', (-1)^{n'(n'-1)/2} d\left(q'\right)\right) \\
&\quad = \left(n+n', (-1)^{nn'}(-1)^{[n(n-1)+n'(n'-1)]/2} \cdot d(q) d\left(q'\right)\right) \\
&\quad = \left(n+n', (-1)^{(n+n')(n+n'-1)/2} \cdot d\left(q \perp q'\right)\right) \\
&\quad = (\dim_0, d_\pm)\left(q \perp q'\right) \in Q(F)
\end{aligned}$$

Further, $M(F) \to Q(F)$ is clearly an epimorphism, since

$$(\dim_0, d_\pm)(\langle a \rangle) = \left(1, a \cdot \dot{F}^2\right) \text{ and } (\dim_0, d_\pm)(\langle 1, -a \rangle) = \left(0, a \cdot \dot{F}^2\right).$$

is the identity element of $Q(F)$, we get an induced epimorphism $W(F) \to Q(F)$. We claim that this homomorphism is trivial on I^2F. IF is additively generated by binary forms $\langle 1, a \rangle$, so I^2F is additively generated by the four-dimensional forms $\langle 1, a \rangle \otimes \langle 1, b \rangle$. But

$$(\dim_0, d_\pm)(\langle 1, a, b, ab \rangle) = \left(0, (-1)^0 \cdot a \cdot b \cdot ab\dot{F}^2\right) = (0,1)$$

so we obtain an epimorphism $f : W(F)/I^2F \to Q(F)$. We shall show that f is an isomorphism, by constructing an inverse $g : Q(F) \to W(F)/I^2F$. We simply set

$$g(0,a) = \langle 1, -a \rangle \left(\operatorname{mod} I^2F\right), \quad g(1,a) = \langle a \rangle \left(\operatorname{mod} I^2F\right),$$

and carry out the following computation:

$$\begin{aligned} g[(0,a)(0,b)] &= g(0,ab) = \langle 1,-ab\rangle \equiv \langle 1,-a,1,-b\rangle \\ &\equiv g(0,a)+g(0,b) \left(\operatorname{mod} I^2F\right) \\ g[(1,a)(1,b)] &= g(0,-ab) = \langle 1,ab\rangle \equiv \langle a,b\rangle \\ &\equiv g(1,a)+g(1,b) \left(\operatorname{mod} I^2F\right) \\ g[(0,a)(1,b)] &\equiv g(1,ab) = \langle ab\rangle \\ &\equiv \langle 1,-a,b\rangle \equiv g(0,a)+g(1,b) \left(\operatorname{mod} I^2F\right) \end{aligned}$$

Hence, g is a group homomorphism. Clearly, $f \circ g$ is the identity map on $Q(F)$, that is, g splits the surjection f. But, by $g(1,a) \equiv \langle a\rangle \left(\operatorname{mod} I^2F\right)$, g is onto. It follows immediately that f and g are inverse isomorphisms of each other.

□

An obvious corollary of the above proposition is

Corollary 2.1.0.1 (Pfister)**.** *I^2F consists of classes of even dimensionla forms q for which $d(q) = (-1)^{n(n-1)/2}$*

Corollary 2.1.0.2 (Pfister)**.** *The restriction of $f : \frac{WF}{I^2F} \to QF$ induces an isomorphism from $\frac{IF}{I^2F} \to \frac{\dot{F}}{\dot{F}^2}$*

2.2 Some Elementary Computations

In this section, we wish to compute a few Witt rings to illustrate the general theory.

Proposition. *F is a quadratically closed field iff* $\dim : \widehat{W}(F) \to \mathbb{Z}$ *is an isomorphism , In this case $WF = \mathbb{Z}_2$*

Proof. $q = \langle a_1,\ldots,a_n\rangle = \left\langle b_1^2,\ldots,n^2\right\rangle = \dim q\langle 1\rangle$
So the map $\dim : \widehat{W}(F) \to \mathbb{Z}$ is an isomorphism.
Conversely if dim is an isomorphism then $\dim\langle a\rangle = \dim\langle 1\rangle$. This implies $\langle a\rangle = \langle 1\rangle$ □

A field F with $|\frac{\dot{F}}{\dot{F}^2}| = 2$ is called Euclidean field. The two square classes are represented by $1,-1$.

Proposition. *Let $F = \mathbb{R}$ (or any "euclidean" field). Then:*

1. *There exist exactly two anisotropic forms at each (positive) dimension. For dimension $n > 0$, these are $n\langle 1\rangle$ and $n\langle -1\rangle$.*
2. *$W(F) \cong \mathbb{Z}$.*
3. *(Sylvester's Law of Inertia) Two (nonsingular) forms over F are equivalent iff they have the same dimension and the same signature*
4. *$\widehat{W}(F) \cong \mathbb{Z} \oplus \mathbb{Z}$. As a ring, $\widehat{W}(F)$ is isomorphic to the integral group ring $\mathbb{Z}[G]$ of a 2-element group. G.*

Proof. 1. $\frac{\dot{F}}{\dot{F}^2} = \pm 1$. So if $q = n\langle 1\rangle + m\langle -1\rangle$, then for q to be an isotropic n or m has to be 0.

2. $x \in WF$, then $x = \langle q\rangle$ for some anisotorpic form , the from the previos result $q = n\langle 1\rangle$ for some n in $\mathbb{Z}$.This gives an isomorphism from $WF \to \mathbb{Z}$.

3. Suppose $q = r\langle 1\rangle \perp n - r\langle -1\rangle = s\langle 1\rangle \perp + n - s\langle -1\rangle (s \geq r)$
Passing to WF we get $r\langle 1\rangle - (n-r)\langle -1\rangle = s\underline{1} - (n-s)\text{-}\underline{1}$. From previous result we get $r = s$.

   The signature of q is defined to be $n_+ - n_-$ where n_+ is the number of positive trems and n_- is the number iof negative terms.

   So $q \simeq q'$ implies they have same dimesnion and signature.

   Conversely, supoose $q = r\langle 1\rangle \perp s\langle -1\rangle$ and $q' = m\langle 1\rangle \perp + n\langle -1\rangle$ have the same signature, then $m+n = r+s$ and $2n - \dim q = 2r - \dim q'$ and this gives $m = r$ and $n = s$.

4. We need to show $\langle 1\rangle, \langle -1\rangle$ form a $\mathbb{Z}$ basis for $\widehat{W}(F)$. It is clear that they space $\widehat{W}(F)$.
Suppose $a\langle 1\rangle + b\langle -1\rangle = 0$ in $\widehat{W}(F)$. This implies $a = b$ in WF, which is $a = b = 0$

□

It follows from (4) above that $\widehat{I}(F)$ is a free abelian group generated by $\langle 1\rangle - \langle -1\rangle$

Theorem 2.2.1. *Assume that every binary form over the field F is universal. Then*

1. *two quadratic forms are isometric iff they have the same dimension and the same determinant;*
2. *$\widehat{I}^2F \cong I^2F = 0$ and $\widehat{I}F \cong IF \cong \dot{F}/\dot{F}^2$; and*
3. *$W(F) \cong Q(F)$ as rings, and $\widehat{W}(F) = \mathbb{Z} \oplus \widehat{I}F$ with trivial multiplication on $\widehat{I}F$.*

Proof. 1. $\langle a_1, a_2\rangle \simeq \langle 1, a_1a_2\rangle$ since $\langle a_1, a_2\rangle$ is universal (Similar to the proof of Witt's chain equivalence theorem to get this form). By induction we can get $\langle a_1, a_2, \ldots a_n\rangle \simeq \langle 1, \ldots d(q)\rangle$

2. $\widehat{I}(F)^2$ is is additively generated by

$$(\langle a_1\rangle - \langle 1\rangle)(\langle a_2\rangle - \langle 1\rangle) = \langle a_1a_2\rangle + \langle 1\rangle - \langle a_1\rangle - \langle a_2\rangle = 0,$$

   so $\widehat{I}^2F = 0$, proving the first part of (2). It follows that

$$\widehat{I}F \cong IF \cong IF/I^2F \cong \dot{F}/\dot{F}^2,$$

3. Finally, the isomorphism $W(F) \cong Q(F)$ in (3) follows from 2.1, and the description of $\widehat{W}(F)$ follows from the (split) exact sequence

$$0 \to \widehat{I}F \to \widehat{W}(F) \xrightarrow{\dim} \mathbb{Z} \to 0.$$

□

Corollary 2.2.1.1. *Let F be a finite field $\mathbb{F}_q$. Then*
If $q \cong 1$ mod4 then $WF \simeq \mathbb{Z}_2[\dot{F}/\dot{F}^2]$
if $q \cong 3$ mod4 then $WF \simeq \mathbb{Z}_4$

Proof. $Q(F)$ is a split extension in the first case and a non-split extension in the second case. In second case, we know that $|WF| = 4$, and $0, \langle 1\rangle, \langle 1,1\rangle, \langle -1\rangle$ are 4 anisotropic forms ($\langle 1,1,1\rangle = \langle -1\rangle$). So $WF \simeq \mathbb{Z}_4$

In the first case $0, \langle 1\rangle, \langle s\rangle, \langle 1,s\rangle$ are 4 forms and $3 = \langle 1,1\rangle = 0$ in WF. So $WF \simeq \mathbb{Z}_2[\dot{F}/\dot{F}^2]$(If we identify, $\dot{F}/\dot{F}^2$ with $\{1, \underline{s}\}$).

□

We have previously seen that sums of squares in general are not group forms. The following lemma provides a situation where forms are indeed group forms.

Lemma 2.2.2. *Over any field F, any binary form $q = \langle 1, a\rangle$ is a group form.*

Proof. A direct proof results by checking the formula

$$\left(x^2 + ay^2\right)\left(z^2 + aw^2\right) = (xz - ayw)^2 + a(xw + yz)^2$$

We will provide an alternative proof using a different technique. Consider the quadratic algebra $K = F[x]/\left(x^2 + a\right)$, which has an F-basis $\{1, \theta\}$ where $\theta^2 = -a$. With respect to this basis, multiplication by $x + y\theta$ on K has the matrix $\begin{pmatrix} x & -ay \\ y & x \end{pmatrix}$. Thus, the "algebra norm" of $x + y\theta \in K$ is given by the determinant of this matrix:

$$\mathrm{N}_{K/F}(x + y\theta) = x^2 + ay^2 \quad (\forall x, y \in F).$$

Since the algebra norm is multiplicative, $q = \langle 1, a\rangle$ is a group form. Indeed, we have $D(q) = \mathrm{N}_{K/F}(\mathrm{U}(K))$, which is a subgroup of $\dot{F}$. □

Proposition. *Let $F = k(t)$, where k is any algebraically closed field. Then any binary quadratic form q over F is universal.*

Proof. We may assume that $q = \langle 1, f\rangle$, where $f \in \dot{F}$. The $\mathbb{F}_2$-vector space $\dot{F}/\dot{F}^2$ has a basis $\left\{(t-b)\dot{F}^2 : b \in k\right\}$, so by the previous lemma, it suffices to show that $t - b \in D(q)$ for any $b \in k$. After a change of variables, we are reduced to showing that $t \in D(q)$, or equivalently, that $\langle 1, -t, f\rangle$ is isotropic. Another application of the same trick enables us to assume that $f = t - c$, where $c \in k$. For such an f, the isotropy of the form $\langle 1, -t, f\rangle$ follows from the equation $(\sqrt{c})^2 - t + f = 0$.

□

Proposition. *Let]phi =<< $a_1, \ldots, a_n$ >> be an n fold Pfister form and $b \in D_F(\phi')$(where $\phi = 1 \oplus \phi'$)Then there exists $b_1, \cdots_n$ such that $\phi \approx$<< $b, b_2, \ldots, b_n$ >>*

2.3 Presentation of Witt Ring

We consider $\widehat{W}(F)$ as a commutative ring. The elements $\langle a\rangle (a \in \dot{F})$ generate $\widehat{W}(F)$, and satisfy the following obvious properties:

$(R_0 1)$ $\langle 1\rangle = 1$ (= the identity of the ring)

$(R_0 2)$ $\langle a\rangle \cdot \langle b\rangle = \langle ab\rangle \quad (a,b \in \dot{F})$

$(R_0 3)$ $\langle a\rangle + \langle b\rangle = \langle a+b\rangle \cdot (1+\langle ab\rangle)$, where $a,b,a+b \in \dot{F}$.

We claim that these are all the only relations among the smbols $\langle a\rangle$, $a \in \dot{F}$.To state it precisely,

Theorem 2.3.1. *Let $\mathscr{F}$ be the free commutative ring generated by the symbols $[a](a \in \dot{F})$. Let $\mathscr{R}$ be the ideal of $\mathscr{F}$ generated by the elements*

$R_0 1$ $[1]-1$

$R_0 2$ $[ab]-[a]\cdot[b] \quad (a,b \in \dot{F})$

$R_0 3$ $[a]+[b]-[a+b]\cdot(1+[ab]) \quad (a,b,a+b \in \dot{F})$ *content...*

Then, the factor ring $X = \mathscr{F}/\mathscr{R}$ is isomorphic to $\widehat{W}(F)$.

Proof. Define a ring homomorphism $f_0 : \mathscr{F} \to \widehat{W}(F)$, that takes $[a] \mapsto < a >$. $f(\mathscr{R}) = 0$, so we have a homomorphism $f : \mathscr{F}/\mathscr{R} \to \widehat{W}(F)$.
To define an inverse to this map let us begin with defining a monoid homomorphism $g : M(F) \to X$.We set $g(q) = [a_1] + \cdots + [a_n]$ where $q =< a_1, \ldots, a_n >$ is the diagonalisation of q. Suppose $q =< b_1, \ldots, b_n >$ is another diagonalisation, we must show that $\sum[a_i] = \sum[b_i] \in X$. By Witt's Chain equivalence theorem, we may suppose that $< a_1, \ldots, a_n >$ is simply equivalent to $< b_1, \ldots, b_n >$.Without loss of generality, we may assume that $a_i = b_i$ for $i \geq 3$ and $< a_1, a_2 > \cong < b_1, b_2 >$. So it suffices to show that

$$\langle a_1, a_2\rangle \cong \langle b_1, b_2\rangle \Longrightarrow [a_1]+[a_2] = [b_1]+[b_2] \in X$$

Claim: For every $a \in X$, $[a^2] = 1 \in X$
Proof: Since $a + a = 2a \neq 0, (R_0 3)$ implies

$$[a]+[a] = [2a]\cdot\left(1+\left[a^2\right]\right) \in X.$$

Also by $R_0 2$ we have

$$\begin{aligned} [a]+[a] &= [a]\cdot([1]+[1]) \\ &= [a]\cdot[2]\cdot(1+[1]) \quad (\text{ by } (R3)) \\ &= [2a]\cdot(1+[1]) \in X \quad (\text{ by } (R2)) \end{aligned}$$

From $R_0 2$ we infer that every $[a]$ is a unit in X, so we have $[a^2] = 1 \in X$ ■

Since $< a_1, a_2 > \cong < b_1, b_2 >$, we have

$$\begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \begin{pmatrix} x & z \\ y & w \end{pmatrix}$$

It follows, $b_1 = a_1x^2 + a_2y^2$ and taking determinant $a_1a_2 = b_1b_2c^2$ for some $c \in \dot{F}$.

case 1 $x = 0$, or $y = 0$. Suppose, for instance, $x = 0 (y = 0$ is similar). Then $b_1 = a_2 y^2 \Rightarrow [b_1] = \left[a_2 y^2\right] = [a_2] \in X$. On the other hand,

$$[a_1] = \left[b_2 \cdot \frac{b_1}{a_2} \cdot c^2\right] = \left[b_2 y^2\right] = [b_2] \in X.$$

case 2 $x \neq 0, y \neq 0$. Then, in X, we have

$$\begin{aligned}
[a_1] + [a_2] &= \left[a_1 x^2\right] + \left[a_2 y^2\right] \\
&= \left[a_1 x^2 + a_2 y^2\right] \cdot \left(1 + \left[a_1 a_2 (xy)^2\right]\right) \\
&= [b_1] \cdot (1 + [b_1 b_2]) \\
&= [b_1] + [b_2]
\end{aligned}$$

Thus, $g : M(F) \to X$ is well-defined, and is clearly a monoid homomorphism. By the universal property of $\widehat{W}(F), g$ extends to a group homomorphism $g : \widehat{W}(F) \to X$, which is an inverse for $f : X \to \widehat{W}(F)$.This proves that f is a ring isomorphism.

□

Milnor K-Theory

Definition Let F be a commutative field. The Milnor-Witt K-theory of F is the graded associative ring $K_*^{MW}(F)$ generated by the symbols $[u]$, for each unit $u \in F^\times$, of degree $+1$, and one symbol η of degree -1 subject to the following relations:

R1 (Steinberg Relation)For each $a \in F^\times - \{1\} : [a] \cdot [1-a] = 0$

R2 For each pair $(a,b) \in (F^\times)^2 : [ab] = [a] + [b] + \eta \cdot [a] \cdot [b]$

R3 For each $u \in F^\times : [u].\eta = \eta \cdot [u]$

R4 Set $h := \eta \cdot [-1] + 2$. Then $\eta \cdot h = 0$

The quotient ring $K_*^{MW(F)}/\eta$ is the Milnor K-theory $K_*^M(F)$ (as defined by Milnor). Then the relation R2 becomes additive in $K_*^M(F)$.

$$[ab] = [a] + [b]$$

$K_*^W(F) = K_*^{MW}(F)/h$ is called the Witt K-theory of F.
A simple observation here is that the following isomorphism holds true,

$$\frac{\oplus_{n\geq 0}(K_1^{MW}(F))^n}{\langle [a]\cdot[1-a]\rangle_{a\in \dot{F}}} \cong K_{\geq 0}^{MW}(F)$$

We establish some useful facts. For any unit $a \in F^\times$, we set $< a >= 1 + \eta[a] \in K_0^{MW}(F)$. Note that $h = 1 + < -1 >$.

Lemma 3.0.1. *Let $(a,b) \in (F^\times)^2$ be units in F.The,*

1. $[ab] = [a] + < a >.\ [b] = [a].\ < b > + [b]$
2. $< ab >=< a > .\ < b >; K_0^{MW}(F)$ *is central in* $K_*^{MW}(F)$
3. $< 1 >= 1$ *in* $K_0^{MW}(F)$ *and* $[1] = 0$ *in* $K_1^{MW}(F)$
4. $< a >$ *is a unit in* $K_0^{MW}(F)$ *whose inverse is* $< a^{-1} >$
5. $\left[\frac{a}{b}\right] = [a] - < \frac{a}{b} > .[b]$. *In particular one has:* $\left[a^{-1}\right] = - < a^{-1} > \cdot [a]$

Proof. 1. Proof of 1) is obvious to see

2. Elements $\langle a\rangle$ are central because $\langle a\rangle[b] = [b]\langle a\rangle$(follows from the previous fact)

3. Multiplying R4 by$[1]$ we get $(<1>-1)\cdot(<-1>+1) = 0 \implies <1>= 1$. By 1) we have now $[1] = [1]+<1>\cdot[1] = [1]+1$. $[1] = [1]+[1]$; thus $[1] = 0$

4. 4) follws from 2) and 3)

5. 5) is a consequence of the previous facts .

□

Lemma 3.0.2. *1. For each $n \geq 1$, the group $K_n^{MW}(F)$ is generated by the products of the form $[u_1]\ldots.[u_n]$, with the $u_i \in F^\times$.*

2. For each $n \leq 0$, the group $K_n^{MW}(F)$ is generated by the products of the form $\eta^n.\ <u>$, with $u \in F^\times$. In particular the product with $\eta : K_n^{MW}(F) \to K_{n-1}^{MW}(F)$ is always surjective if $n \leq 0$.

Proof. Proof. The group $K_n^{MW}(F)$ is generated by the products of the form $\eta^m \cdot [u_1]\ldots..[u_\ell]$ with $m \geq 0, \ell \geq 0, \ell - m = n$ and with the u_i 's units. The relation R2 can be rewritten $\eta\cdot[a]\cdot[b] = [ab]-[a]-[b]$. This easily implies the result using the fact that $<1>= 1$.

□

We know $h-1+\langle -1\rangle$. Set $\varepsilon = -\langle -1\rangle \in K_0^{MW}(F)$. So $\eta h = 0$ is same as $\varepsilon\eta = \eta$.

We have the following observations

Lemma 3.0.3. *1. For $a \in F^\times$: $[a]\cdot[-a] = 0$ and $<a>+<-a>= h$*

2. For $a \in F^\times$: $[a]\cdot[a] = [a]\cdot[-1] = \varepsilon[a][-1] = [-1]\cdot[a] = \varepsilon[-1][a]$;

3. For $a \in F^\times$ and $b \in F^\times$: $[a].[b] = \varepsilon\cdot[b]\cdot[a]$

4. For $a \in F^\times$: $<a^2>= 1$

Corollary 3.0.3.1. *The graded $K_0^{MW}(F)$-algebra $K_*^{MW}(F)$ is ε-graded commutative: for any element $\alpha \in K_n^{MW}(F)$ and any element $\beta \in K_m^{MW}(F)$ one has*

$$\alpha.\beta = (\varepsilon)^{n.m}\beta.\alpha$$

Proof. It is enough to check this on the generators: $[a][b], [a]\eta, \eta\cdot\eta$, which follows from the relations in $K_*^{MW}(F)$.

□

$\langle u\rangle$ is an element of $K_0^{MW}(F)$ and it satisfies all the relations of the Grothendieck-Witt ring. To prove R_03 we may assume that $u+v = 1$(since $\langle u\rangle$ is multiplicative in u, we can multiply by $<1/u+v>$ if necessary).

Thus we get an epimorphism from

$$\phi_0 : \widehat{W}(F)(F) \twoheadrightarrow K_0^{MW}(F)$$

For $n > 0$, the multiplication by η^n induces map

$$\eta^n : K_0^{MW}(F) \to K_{-n}^{MW}(F)$$

This map kills h (since $h\eta = 0$) and thus we get an epimorphism

$$\phi_{-n} : W(F) \twoheadrightarrow K_{-n}^{MW}(F)$$

Note:$h = 1 + \langle -1 \rangle = \langle 1 \rangle + \langle -1 \rangle = \mathbb{H}$, so $\widehat{W}(F)/h \cong WF$

Lemma 3.0.4. *For each field F and $n \geq 0$, ϕ_{-1} is an isomorphism.*

We introduce Morel's J^*-construction,before going ahead with the proof, which will play a prominent role in our study of Milnor-Witt K-theory . Milnor's homomorphisms are defined as

$$\alpha_n : K_n^M(F) \to I^n(F)/I^{n+1}(F)$$

$$[a_1][a_2]\cdots[a_n] \mapsto (< a_1 > -1)\cdots(< a_n > -1) + I^{n+1}F$$

(The forms $< a_1 > -1)\cdots(< a_n > -1)$ are called Pfister forms) Let us write $i^nF := I^n(F)/I^{n+1}(F)$. Now define J^nF as the fiber product, i.e., $J^nF := I^nF \times_{i^nF} K_n^MF$. If we interpret $I^n(F)$ as $W(F)$ for $n \leq 0$, then we get $J^n(F) = W(F)$ for $n < 0$, and

$$J^0(F) = W(F) \times_{\mathbb{Z}/2\mathbb{Z}} \mathbb{Z} \cong GW(F).$$

We define $\eta := 1 \in J^{-1}(F) = W(F)$. Further, let $[a] := (\langle a \rangle - 1, [a]) \in J^1(F) \subset I(F) \times K_1^M(F)$. It is straightforward to check that the Milnor-Witt relations(R1-R4) hold amongst these terms in $J^*(F)$. Thus we get a homomorphism of graded rings $K_*^{MW}(F) \to J^*(F)$ taking η to η and $[a]$ to $[a]$. It is clear that this map is surjective in degrees $n \leq 0$, and in degree $n = 1$. It follows that $K_*^{MW}(F) \to J^*(F)$ is surjective in all degrees.

Proof. Proof of 3.0.4.ϕ_{-n} is surjective.For $n > 0$ the composite map

$$W(F) \twoheadrightarrow K_{-n}^{MW}(F) \twoheadrightarrow J^{-n}(F) = W(F)$$

$$\langle u \rangle \mapsto \eta^n \langle u \rangle \mapsto \langle u \rangle$$

is identity. For $n = 0$, the composite

$$\widehat{W}(F) \twoheadrightarrow K_0^{MW}(F) \twoheadrightarrow J^0(F) = \widehat{W}(F)$$

is also identity.This proves the lemma. □

Lemma 3.0.5. *Let $a \in F^\times$ and let $n \in \mathbb{Z}$ be an integer. Then the following formula holds in $K_1^{MW}(F)$:*

$$[a^n] = n_\varepsilon [a]$$

where for $n \geq 0$, where $n_\varepsilon \in K_0^{MW}(F)$ is defined as follows

$$n_\varepsilon = \sum_{i=1}^{n} < (-1)^{(i-1)} >$$

(and satisfies for $n > 0$ the relation $n_\varepsilon =< -1 > (n-1)_\varepsilon + 1)$ and
where for $n \leq 0$,

$$n_\varepsilon := - < -1 > (-n)_\varepsilon.$$

Proof. The proof follows by induction, from the observation: $[a^n] = \left[a^{n-1}\right] + [a] + \eta \left[a^{n-1}\right][a]$ as well as $\left[a^{-1}\right] = - < a > [a] = -([a] + \eta [a][a])$. □

Proposition. *Let F be a field in which any unit is a square. Then the epismorphism $K_*^{MW}(F) \to K_*^M(F)$ is an epimorphism in degree ≥ 0, and $K_*^{MW}(F) \to K_*^W(F)$ is an isomorphism in degree < 0.*
In fact $I^n(F) = 0$ for $n > 0$ and $I^n(F) = W(F) = \mathbb{Z}/2$ for $n \leq 0$.

Proof. Since -1 is a square, we have $\langle -1 \rangle = 1$, so that $h = 2$ and relation R4 becomes $2\eta = 0$. By the previous lemma, $\eta \left[a^2\right] = 2\eta [a]$, so $\eta \left[a^2\right] = 0$. Since any unit is a square, $\eta [b] = 0$ for all b, so that relation R2 becomes $[ab] = [a] + [b]$. Thus in degree $\geq 0, K_*^M$ and K_*^{MW} have the same generator and relations. In degree < 0, we know that $K_n^{MW}(F) \cong W(F)$. Since $h = 2, K_n^W(F) \cong W(F)/2W(F)$. But it is known that for a field in which every unit is a square, $W(F) \cong \mathbb{Z}/2\mathbb{Z}$. So that taking the quotient by 2 will be an isomorphism.

□

3.1 Relation between Milnor K-theory and Witt Rings

The K-theory modulo 2 of F is the quotient

$$k_*^M F = K_*^M F / 2K_*^M F$$

We use the same notation $[a_1], \ldots, [a_n]$ for a symbol in $K_n^M F$ and its class modulo $2K_n^M F$. The presentation of $K_\star^M F$ by generators and relations extends to Milnor's K-theory modulo 2 as follows. The classes $[a]$, with $a \in F^\times$, generate the graded ing $k_\star^M F$; and they satisfy the following relations:

k1 $[ab] = [a] + [b]$

k2 $[a][1-a] = 0$

k3 $2[a] = 0$

The witt ring WF has a filtration given by $I^n F$. We define the graded Witt ring $GW_* F$ as the graded ring associated to this filtration,

$$GW_* F = \oplus_{n \geq 0} I^N F / I^{n+1} F$$

Theorem 3.1.1. *There is a homomorphism*

$$\alpha_\star : k_\star F \to GW_\star F,$$

mapping the symbol $[a]$ *to the Pfister form* $\langle\langle a\rangle\rangle =< a, -1 >$. *Moreover, the map* $\alpha_\star$ *is surjective*

Proof. As defined earlier, $\alpha_\star$ is the Milnor's homomorphisms and it is clearly surjective, as I^nF are generated by Pfister forms. We are left to prove that $\alpha_\star$ is well defined.It suffices to check that the relations k1,k2,k3 also hold in the graded Witt ring.
Consider $a, b \in F^\times$. If $a \neq 1$, the form

$$\langle\langle a, 1-a\rangle\rangle = \langle 1, -a, -(1-a), a(1-a)\rangle$$

is isotropic, hence hyperbolic. So we have $\langle\langle a, 1-a\rangle\rangle = 0$ in the Witt ring $W(F)$. The other relations hold true in $GW_\star F$. Since $\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle = \langle\langle ab\rangle\rangle + \langle\langle a, b\rangle\rangle \in W(F)$. and $\langle\langle a, b\rangle\rangle \in I^2F$, we get $\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle = \langle\langle ab\rangle\rangle \in IF/I^2F$.
Similarly, $2\langle\langle a\rangle\rangle = \langle\langle a, -1\rangle\rangle \in I^2F$, so that $2\langle\langle a\rangle\rangle = 0 \in IF/I^2F$.

□

3.2 Norm and Residue maps

Restriction map Consider a field extension E/F, the inclusion $F \to E$ induces maps $\text{res}_{E/F}$: $K_*^M F \to K_M^* E$ and $k_*^M F \to k_M^* E$. The map takes a symbol $\{a_1, \ldots, a_n\}$ to itself viewed as an element of $K_M^* E$ or $k_M^* E$.

Residue Map Consider a field L with a valuation map $v : L^\times \to \mathbb{Z}$ and residue field F.The homomorphism v can be viewed as homomorphism

$$K_1^M F \to K_0^M F$$

Let $\mathscr{O}$ be the valuation ring, and $\mathscr{O}^\times$ be the set of units and $p \in \mathscr{O}$ be a prime element, so $v(p) = 1$.

Proposition. *For all* $n \geq 1$ *there is a unique morphism , called the residue map*

$$\partial_v : K_n^M L \to K_{n-1}^M F$$

satisfying $\partial_v(\{a, u_2, \ldots, u_n\}) = v(a)\{\bar{u_2}, \ldots \bar{u_n}\}$ *(where* $\bar{u}_i$ *is the image of* u_i *in the residue field* F*) for all units* u_i

Proof. By properties of the valuation map the residue homomorphism ∂_v satisfies

$$\begin{aligned}
&\partial_v(\{p, u_2, \ldots, u_n\}) = \{\bar{u}_2, \ldots, \bar{u}_n\}, \text{ and} \\
&\partial_v(\{u_1, \ldots, u_n\}) = 0
\end{aligned}$$

for all prime elements p and units u_i. Since every $a \in L^\times$can be written uniquely $a = p^i u$, where $i = v(a)$, for some unit $u \in \mathscr{O}^\times$. Since $\{p\}\{p\} = \{p\}\{-1\}$, $K_n^M L$ is generated by symbols $\{p, u_2, \ldots, u_n\}$, and $\{u_1, \ldots, u_n\}$ for units $u_1, \ldots, u_n \in \mathscr{O}^\times$. Hence, if such a morphism exists,

the condition guarantees its uniqueness.
Consider the ring $K_\star^M F[\eta]$, generated by $K_\star^M F$ and by an additional element η satisfying:

$$\eta^2 = \{-1\}\eta \text{ and } \eta\alpha = -\alpha\eta \text{ for all } \alpha \in K_1 F.$$

We let η be of degree 1, so that $K_\star^M F[\eta]$ is graded and satisfies

$$K_n^M F[\eta] = K_n F \oplus \eta K_{n-1} F.$$

Let us fix a prime element π, and consider the map

$$d_\pi : K_1^M L \mapsto L_1(F), \quad \left\{\pi^i u\right\} \mapsto \{\bar{u}\} + \eta i$$

It clearly induces a morphism $K_1^M L^{\otimes n} \to K_n^M F[\eta]$. For all $a \in L^\times, a \neq 1$, the map $d_\pi^{\otimes 2}$ maps $\{a\} \otimes \{1-a\}$ to zero.

Therefore, the morphism $d_\pi^{\otimes n}$ factors through $K_n^M L$. Composing with the projection

$$K_n^M F \oplus \eta K_{n-1}^M F \mapsto K_{n-1}^M F,$$

we get a well-defined morphism

$$\partial_\pi : K_n^M F \mapsto K_{n-1}^M F.$$

Moreover, since $d_\pi\left(\left\{\pi^i u_1\right\}\right) = \{\bar{u}_1\} + \eta i$, and $d_\pi(\{u_i\}) = \{\bar{u}_i\}$ for all $u_1, \ldots, u_n \in \mathscr{O}^\times$, we have $\partial_\pi(\{a, u_2, \ldots, u_n\}) = v(a)\{\bar{u}_2, \ldots, \bar{u}_n\}$, for all $a \in L^\times$. In particular, it follows from this formula that ∂_π does not depend on the choice of π, and can be denoted by ∂_v.

□

Norm map Let E/F be a field extension of finite degree. The norm homomorphism $N : E^\times \to F^\times$ can be viewed as a morphism

$$N_{E/F} : K_1^M E \to K_1^M F$$

In fact there exists a norm homomorphism for every n,

$$N_{E/F} : K_n^M E \to K_n^M F$$

Milnor's Conjecture for $n = 1$

In this section our main goal would be to prove the Milnor's conjecture in degree 1. We will also prove that the degree 2 graded Witt group is isomorphic to the degree 2 graded Milnor groups mod 2

Let $\overline{e_0} : WF/IF \to \mathbb{Z}/2\mathbb{Z}$ denote the isomorphism given by $\dim q \mod 2$. and $\overline{e_1} : IF/I^2F \to \dot{F}/\dot{F}^2$ denote the isomorphism in 2.1.0.2
Let $f_1 : F^\times/F^{\times 2} \to I(F)/I^2(F)$ be given by $aF^{\times 2} \mapsto \langle\langle a\rangle\rangle + I^2(F)$.This is inverse to $\overline{e_1}$.

Lemma 4.0.1. *Let $\langle\langle a,b\rangle\rangle$ and $\langle\langle c,d\rangle\rangle$ be isometric bilinear 2-fold Pfister forms. Then $\{a,b\} = \{c,d\}$ in $k_2(F)$.*

Proof. If the form $\langle\langle a,b\rangle\rangle$ is hyperbolic, then $\{a,b\} = 0$ in $k_2(F)$. Therefore, we may assume that $\langle\langle a,b\rangle\rangle$ is anisotropic. Using Witt Cancellation, we see that $c = ax^2 + by^2 - abz^2$ for some $x,y,z \in F$. If $c \notin aF^{\times 2}$, let $u = y^2 - az^2 \neq 0$. Then $\langle\langle a,b\rangle\rangle (\simeq \langle 1,-a,-b,ab\rangle \simeq \langle 1,-a,-by^2,abx^2\rangle \simeq \langle 1,-a,-bw,abw\rangle) \simeq \langle\langle a,bw\rangle\rangle \simeq \langle\langle c,-abw\rangle\rangle$ and $\{a,b\} = \{a,bw\} = \{c,-abw\}$ in $k_2(F)$ [1]. Hence we may assume that $a = c$. By Witt Cancellation, $\langle -b,ab\rangle \simeq \langle -d,ad\rangle$, so $bd \in D(\langle\langle a\rangle\rangle)$, i.e., $bd = x^2 - ay^2$ in F for some $x,y \in F$. Thus $\{a,b\} = \{a,d\}$ by the last footnote.

□

Proposition. *The homomorphism*

$$e_2 : I^2(F) \to k_2(F) \quad \text{given by} \quad \langle\langle a,b\rangle\rangle \mapsto \{a,b\}$$

is a well-aefined surjection with $\mathrm{Ker}(e_2) = I^3(F)$. *Moreover, e_2 induces an isomorphism*

$$\bar{e}_2 : I^2(F)/I^3(F) \to k_2(F)$$

Proof. By previous lemma, the map is well-defined. Since

$$\langle\langle a,b,c\rangle\rangle = \langle\langle a,c\rangle\rangle + \langle\langle b,c\rangle\rangle - \langle\langle ab,c\rangle\rangle,$$

we have $I^3(F) \subset \mathrm{Ker}(e_2)$. As $\bar{e}_2$ and f_2 are inverses of each other, the result follows.

□

[1] $\{a, x^2 - ay^2\} = 0$ for $a \neq 0$ and $x^2 - ay^2 \neq 0$. So $\{a,b\} = \{a+b, ab(a+b)\}$ for $a+b \neq 0$

Stiefel-Whitney map We provide an alternate proof of the above using Stiefel-Whitney map.

Let $M(F)$ be the free abelian group on the set of isometry classes of nondegenerate 1-dimensional quadratic forms. Then we have a group homomorphism

$$w : M(F) \to k_*(F)[[t]]^\times \quad \langle a \rangle \mapsto 1 + \{a\}t$$

If $a, b \in F^\times$ satisfy $a + b \neq 0$, we have

$$\begin{aligned} w(\langle a \rangle + \langle b \rangle) &= (1 + \{a\}t)(1 + \{b\}t) \\ &= 1 + (\{a\} + \{b\})t + \{a, b\}t^2 \\ &= 1 + \{ab\}t + \{a, b\}t^2 \\ &= 1 + \left\{ab(a+b)^2\right\}t + \{a+b, ab(a+b)\}t^2 \\ &= w(\langle a+b \rangle + \langle ab(a+b) \rangle) \end{aligned}$$

Since $\langle a \rangle + \langle b \rangle = \langle a + b \rangle + \langle ab(a+b) \rangle$ for all $a, b \in F^\times$ satisfying $a + b \neq 0$, we get a group homomorphism

$$w : \widehat{W}(F) \to k_*(F)[[t]]^\times$$

This homomorphism is called the total Stiefel-Whitney map.We state the following lemma without proof,

Lemma 4.0.2. *Let $\alpha = (\langle 1 \rangle - \langle a_1 \rangle) \cdots (\langle 1 \rangle - \langle a_n \rangle)$ in $\widehat{W}(F)$. Let $m = 2^{n-1}$. Then*

$$w(\alpha) = \left(1 + \{a_1, \ldots, a_n, \underbrace{-1, \ldots, -1}_{m-n}\}t^m\right)^{-1}.$$

Proof. [**Mek**] Ch 1, Section 5

□

Let $w_0(\alpha) = 1$ and $w(\alpha) = 1 + \sum_{i \geq 1} w_i(\alpha)t^i$ for $\alpha \in \widehat{W}(F)$. The map $w_i : \widehat{W}(F) \to k_i(F)$ is called the i^{th} Stiefel-Whitney class. Let $\alpha, \beta \in \widehat{W}(F)$. As $w(\alpha + \beta) = w(\alpha)w(\beta)$, for every $n \geq 0$, we have the Whitney Sum Formula

$$w_n(\alpha + \beta) = \sum_{i+j=n} w_i(\alpha)w_j(\beta)$$

If we let $m = 2^{n-1}$ and $\alpha = (\langle 1 \rangle - \langle a_1 \rangle) \cdots (\langle 1 \rangle - \langle a_n \rangle)$, by the previous lemma we have $w_i(\alpha) = 0$ for $i \in [1, m-1]$. Then using Whitney Sum formula we get $w_j(\hat{I}^n(F)) = 0$ for $j \in [1, m-1]$.

Let $j : \widehat{I}(F) \to I(F)$ be the isomorphism sending $\langle 1 \rangle - \langle a \rangle \mapsto \langle\langle a \rangle\rangle$, and $\tilde{w}_m : I^n(F) \xrightarrow{j^{-1}} \widehat{I}^n(F) \xrightarrow{w_m|_{\hat{I}^n(F)}} k_m(F)$. From the previous observation we see that $\tilde{w}_i = e_i$ for $i = 1, 2$. The map $\tilde{w}_m : I^n(F) \to k_m(F)$ is a group homomorphism with $I^{n+1}(F) \subset \mathrm{Ker}(\tilde{w}_m)$ so it induces a homomorphism

$$\bar{w}_m : I^n(F)/I^{n+1}(F) \to k_m(F).$$

We have $\bar{w}_i = \bar{e}_i$ for $i = 1,2$. The composition $\bar{w}_m \circ f_n$ is multiplication by $\{\underbrace{-1,\ldots,-1}_{m-n}\}$. In particular, $\bar{w}_1$ and $\bar{w}_2$ are isomorphisms, i.e.,

$$I^2(F) = \mathrm{Ker}\,(\tilde{w}_1) \quad \text{and} \quad I^3(F) = \mathrm{Ker}\,(\tilde{w}_2)$$

and

$$\widehat{I}^2(F) = \mathrm{Ker}\left(w_1|_{\widehat{I}(F)}\right) \quad \text{and} \quad \widehat{I}^3(F) = \mathrm{Ker}\left(w_2|_{\widehat{I}^2(F)}\right)$$

4.1 Galois Cohomology and Hilbert 90

Let G be a group. A G-module is an abelian group A together with an action of G, i.e., a map $G \times A \to A$ such that

1. $\sigma(a+a') = \sigma a + \sigma a'$ for all $\sigma \in G, a, a' \in M$;
2. $(\sigma\tau)(a) = \sigma(\tau a)$ for all $\sigma, \tau \in G, a \in A$
3. $1_G a = a$ for all $a \in A$

Thus we get a homomorphism $G \to \mathrm{Aut}(A)$.
Let

$$C^r(G,A) := \mathrm{Maps}\,(G^r, A)$$

an element of $C^r(G,A)$ is a function f of r variables in G,

$$f(\sigma_1,\ldots,\sigma_r) \in A$$

and is called an r-cochain. There is a sequence

$$\cdots \to 0 \to 0 \to C^0(G,A) \xrightarrow{\delta_0} C^1(G,A) \xrightarrow{\delta_1} C^2(G,A) \xrightarrow{\delta_2} \cdots$$

Here $C^0(G,A) = A$, since an element f of $C^0(G,A)$ is given by the value of f_0 at the unique element g^0 in G^0. The maps δ are defined by

$$\begin{aligned}
(\delta f_0)(\sigma) &= \sigma f_0(g^0) - f_0(g^0), \\
(\delta f_1)(\sigma,\tau) &= \sigma f_1(\tau) - f_1(\sigma\tau) + f_1(\sigma), \\
(\delta f_2)(\sigma,\tau,\rho) &= \sigma f_2(\tau,\rho) - f_2(\sigma\tau,\rho) + f_2(\sigma,\tau\rho) - f_2(\sigma,\tau)
\end{aligned}$$

and so on. Note that $\delta \circ \delta = 0$. The cohomology groups are given by

$$H^r(G,A) = \ker \delta_r / \operatorname{im} \delta_{r-1} \subset C^r(G,A) / \operatorname{im} \delta_{r-1}.$$

Cocycles are elements of the kernel of δ, and coboundaries are elements of the image of δ. We have

$$\begin{aligned}
H^0(G,A) &= A^G \\
H^1(G,A) &= \frac{\text{crossed-homomorphisms}}{\text{principal crossed-homomorphisms}}
\end{aligned}$$

Theorem 4.1.1 (Hilbert 90)**.** *Let E be a Galois extension of F with group G; then $H^1(G,E^\times)=0$.*

Proof. Let f be a crossed homomorphism $G\to E^\times$. In multiplicative notation, this means that

$$f(\sigma\tau)=f(\sigma)\cdot\sigma(f(\tau)),\quad \sigma,\tau\in G,$$

and we have to find a $\gamma\in E^\times$ such that $f(\sigma)=\frac{\sigma\gamma}{\gamma}$ for all $\sigma\in G$. Because the $f(\tau)$ are nonzero, the independence of characters($\{\chi_1,\cdots,\chi_n\}:G\to F$, then $\sum a_i\chi_i=0\implies a_i=0\forall i$) implies that

$$\sum_{\tau\in G} f(\tau)\tau : E\to E$$

is not the zero map, i.e., there exists an $\alpha\in E$ such that

$$\beta\overset{\text{def}}{=}\sum_{\tau\in G} f(\tau)\tau\alpha\neq 0.$$

But then, for $\sigma\in G$,

$$\begin{aligned}\sigma\beta&=\sum_{\tau\in G}\sigma(f(\tau))\cdot\sigma\tau(\alpha)\\&=\sum_{\tau\in G}f(\sigma)^{-1}f(\sigma\tau)\cdot\sigma\tau(\alpha)\\&=f(\sigma)^{-1}\sum_{\tau\in G}f(\sigma\tau)\sigma\tau(\alpha)\end{aligned}$$

which equals $f(\sigma)^{-1}\beta$ because, as τ runs over G, so also does $\sigma\tau$. Therefore, $f(\sigma)=\frac{\beta}{\sigma(\beta)}=\frac{\sigma(\beta^{-1})}{\beta^{-1}}$. □

Let E be a Galois extension of F with Galois group G. We define the norm of an element $\alpha\in E$ to be

$$\mathrm{N}(\alpha)=\prod_{\sigma\in G}\sigma\alpha.$$

For $\tau\in G$,

$$\tau(\mathrm{N}\alpha)=\prod_{\sigma\in G}\tau\sigma\alpha=\mathrm{N}\alpha$$

and so $\mathrm{N}(\alpha)\in F$. The map

$$\alpha\mapsto\mathrm{N}(\alpha):E^\times\to F^\times$$

is a homomorphism.

Let $f:G\to A$ be a crossed homomorphism. For any $\sigma\in G$,

$$\begin{aligned}f\left(\sigma^2\right)&=f(\sigma)+\sigma f(\sigma)\\f\left(\sigma^3\right)&=f\left(\sigma\cdot\sigma^2\right)=f(\sigma)+\sigma f(\sigma)+\sigma^2 f(\sigma)\\&\cdots\\f\left(\sigma^n\right)&=f(\sigma)+\sigma f(\sigma)+\cdots+\sigma^{n-1}f(\sigma)\end{aligned}$$

Thus, if G is a cyclic group of order n generated by σ, then a crossed homomorphism $f : G \to A$ is determined by its value, x say, on σ, and x satisfies the equation

$$x + \sigma x + \cdots + \sigma^{n-1} x = 0 \tag{4.1}$$

Moreover, if $x \in M$ satisfies the above equation, then the formulas $f\left(\sigma^i\right) = x + \sigma x + \cdots + \sigma^{i-1} x$ define a crossed homomorphism $f : G \to M$. Thus, for a finite cyclic group $G = \langle \sigma \rangle$, there is a one-to-one correspondence

$$\{ \text{ crossed homs } f : G \to M \} \overset{f \leftrightarrow f(\sigma)}{\longleftrightarrow} \{ x \in M \text{ satisfying} 4.1 \}$$

.

Theorem 4.1.2 (Hilbert's 90)**.** *Let E be a finite cyclic extension of F, and let σ generate* $\mathrm{Gal}(E/F)$. *Let $\alpha \in E^\times$; if $\mathrm{N}_{E/F}\alpha = 1$, then $\alpha = \beta/\sigma\beta$ for some $\beta \in E$.*

Proof. Let $m = [E : F]$. Since $\mathrm{N}(\alpha) = 1$, $\alpha \cdot \sigma\alpha \cdots \sigma^{m-1}\alpha = 1$, and so (from the aobve observation) there is a crossed homomorphism $f : \langle \sigma \rangle \to E^\times$ with $f(\sigma) = \alpha$. Theorem 4.1.1 now shows that there is a γ with $f(\sigma) = \sigma\gamma/\gamma$. Setting $\beta := \gamma^{-1}$,we have

$$f(\sigma) = \beta/\sigma(\beta)$$

as desired □

Cup product If M and N are two Galois modules, then $M \otimes N$ is also a galois module, via the action $g \cdot (a \otimes b) = ga \otimes gb$. We define the cup product on chains as

$$C^i(G,M) \otimes C^j(G,N) \overset{\smile}{\longrightarrow} C^{i+j}(G, M \otimes N)$$

$f \smile f'(g_1, \cdots g_{i+j}) = f(g_1 \ldots g_i) \otimes g_1 \ldots g_i f'(g_{i+1}, \ldots g_{i+j})$. This induces a map on the cohomology groups,

$$H^i(G,M) \otimes H^j(G,N) \overset{\smile}{\longrightarrow} H^{i+j}(G, M \otimes N)$$

Restriction and Corestriction map [2]Let M be a G Galois module over and H be a subgroup of G. This defines a restriction map

$$\mathrm{Res}_{G/H} : H^n(G,M) \to H^n(H,M)$$

by restricting the G–cocycles to H. If we have an arbitrary field extension K over F, then there is a restriction homomorphism from $G = Gal(K_{\mathrm{sep}}) \to H = Gal(F_{\mathrm{sep}})$.
If M is a G module, then there is a restriction homomorphism

$$r_{K/F} : H^n(H,M) \to H^n(G,M)$$

In degree 0 it coincides with the map $M^G \to M^H$.

[2][**Mek**] 99.C

If H is a subgroup of finite index of G, then there exists a homomorphism from $M^H \to M^G$, $m \mapsto \sum_{g\in G/H} gm$.
If K/F is a finite separable extension, then $G = Gal(K)$ is a subgroup of finite index of $H = Gal(F)$. For ever $n \geq 0$ there is a natural corestriction homomorphism

$$c_{K/F} : H^n(G,M) \to H^n(H,M)$$

In degree 0 it coincides with the map mentioned above.
If H is a subgroup of finite index, then we have a map

$$T : H^0(H,M) \to H^0(G,M)$$

defined by $m \mapsto \sum_{g\in G/H} gm$ and this can be extended to a map $H^n(H,M) \to H^n(G,M)$.

There is a projection formula that holds on the cup product that is:
$c_{K/F}(\alpha_L \cdot \beta) = \alpha \cdot c_{K/F}(\beta)$ for all $\alpha \in H^i(Gal(F_{sep}),M)$ and $\beta \in H^j(Gal(L_{sep}),M)$.

4.2 Relation with k-theory

Norm Residue Homomorphism We will consider Galois cohomology groups of F with coefficients in Galois module $\mathbb{Z}/2\mathbb{Z}$ with trivial action of $G = gal(E/F)$. We have the following exact sequence of Galois modules

$$1 \to \mathbb{Z}/2\mathbb{Z} \to E^\times \xrightarrow{x\mapsto x^2} \mathbb{E}^\times \to 1$$

which gives a cohomology long exact sequence

$$1 \to \mathbb{Z}/2\mathbb{Z} \to E^\times \to E^\times \to H^1(F,\mathbb{Z}/2\mathbb{Z}) \to H^1(F,E^\times)$$

By Hilbert 90, we get the last term = 1 and hence the isomorphism

$$F^\times/F^{\times 2} \to H^1(F,\mathbb{Z}/2\mathbb{Z})$$

Identifying $F^\times/F^{\times 2}$ with $k_1^M(F)$, we get an isomorphism

$$h^1 : k_1^M(F) \to H^1(F,\mathbb{Z}/2\mathbb{Z})$$

Let us denote by (a) the image $H^1(\{a\})$. Since $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ is canonnically isomorphic to $\mathbb{Z}/2\mathbb{Z}$, the cup product induces a map $H^i(F) \times H^j(F) \to H^{i+j}(F)$. This map defines a product on the graded ring $H^*(F)$.We will use $(a_1,\dots a_n)$ to denote the element $(a_1)\dots(a_n) \in H^n(F)$. Thus the isomorphism $h^1 : k_1^M F \to H^1(F,\mathbb{Z}/2\mathbb{Z})$ extends uniquely to a homomorphism of graded rings

$$h : k_*^M F \to H^*(F,\mathbb{Z}/2\mathbb{Z})$$

This is called the norm residue homomorphism.

Proof. Clearly the map h^1 induces maps $k_n^F \to H^n(F,\mathbb{Z}/2\mathbb{Z})$. So we have to check that the relations of Milnor k-theory holds in Galois cohomology.
Since h^1 is an isomorphism, we clearly have $(ab) = (a) + (b)$ and $2(a) = (a^2) = 0$ in $H^1(F)$.
If $a \in F^{\times 2}$ then $(a)\cdot(1-a) = 0$. If not, let $b \in E$ a square root of a and $K = F(b)$. $c_{K/F}(1-b) = (1-b)(1+b) = 1-a$. By the projection formula, $(a)\cdot(1-a) = (a)\cdot c_{K/F}(1-b) = c_{K/F}((a)\cdot(1-b)) = c_{K/F}((b^2)\cdot(1-b)) = 0$. □

References

[Lam] Lam, T. Y. Introduction to quadratic forms over fields.

[Mek] The Algebraic and Geometric Theory of Quadratic Forms, Richard Elman,Nikita Karpenko, Alexander Merkurjev

[Mor] $\mathbb{A}^1$- Algebraic Topology over a field, Fabien Morel