SYMMETRIC INNER PRODUCTS IN CHARACTERISTIC 2

John Milnor

Let F be a field of characteristic 2. This paper will classify the nondegenerate symmetric inner product modules over F, and describe the structure of the associated Witt ring W(F) as defined by Knebusch [3].

1. *Introduction*

The concept of symmetric bilinear form (= symmetric inner product) is closely related to the concept of quadratic form. In fact in the classical case, working over a field of characteristic different from 2, the two concepts are completely equivalent. But in dealing with more general rings, the symmetric bilinear form seems to be the simpler and more natural object of study. (Compare Serre [7, p. 6].)

Recently M. Knebusch has defined and studied a "Witt ring" W(A) associated with any commutative ring A. The elements of W(A) are equivalence classes of symmetric inner product modules over A. We will study this Knebusch-Witt ring for the special case of a field F of characteristic 2. The subfield $S \subset F$ consisting of all squares in F will play an important role. Thus if F has finite degree $d = 2^k$ over S, then the additive group of W(F) is canonically isomorphic to the group consisting of all S-rational points in a certain algebraic group whose identity component is an open subset of a rational variety of dimension $d(d-1)/2$ over S. The ring W(F) is local, and its unique maximal ideal $\mathfrak{J}$ satisfies the condition $\mathfrak{J}^k \neq 0$, but $\mathfrak{J}^{k+1} = 0$. The proofs are based on a Clifford algebra $C = C(F)$ which is canonically associated with F.

I am indebted to W. Scharlau for very useful discussions.

2. *Inner product modules and the Witt ring*

Let A be a commutative ring with unit. An *inner product module* X over A will mean a finitely generated projective A-module together with a symmetric bilinear inner product,

$$x \cdot y \in A$$

for x, y $\in$ X, which is *non-degenerate* in the following strong sense. The homomorphism

$$h : X \to \mathrm{Hom}_A(X,A)$$

adjoint to the inner product, defined by $h(x)(y) = x \cdot y$, must be bijective.

(An elementary topological application may help to motivate this concept: Let M^2 be a closed connected surface. Then the homology $H_1(M^2;Z/2Z)$ is an inner product module over $Z/2Z$, using the intersection number as inner product. In fact the isomorphism class of this inner product module provides a complete invariant for the surface. Similarly the inner product module $H_2(M^4;Z)$ over Z provides a complete invariant, up to homotopy type, for an oriented simply connected 4-dimensional manifold M^4. Compare [4].)

Starting with the monoid consisting of all isomorphism classes of inner product modules over the ring A, one can form the Grothendieck ring, which we denote by $\hat{W}(A)$. This consists of all formal differences $X - X'$ of inner product modules, where $X - X'$ is set equal to $Y - Y'$ if and only if the orthogonal direct sum $X \oplus Y' \oplus Z$ is isomorphic to $X' \oplus Y \oplus Z$ for some Z. (Compare [7], [3].) The sum operation in $\hat{W}(A)$ corresponds to the orthogonal direct sum of modules, and the product operation to the tensor product of modules.

An inner product module is called *hyperbolic* if it splits as the direct sum of two self-annihilating submodules. The hyperbolic modules generate an ideal in $\hat{W}(A)$. Following Knebusch, the quotient of $\hat{W}(A)$ by this ideal is called the *Witt ring* W(A). This coincides with the classical Witt ring in the case of a field of characteristic $\neq 2$.

For any inner product module X, let $-X$ denote the inner product module formed from X by reversing the sign of every inner product. Note the isomorphism

$$X \oplus (-X) \oplus X \cong X \oplus (\text{hyperbolic module}).$$

In fact the diagonal submodule

$$D(X \oplus (-X) \oplus X) \subset X \oplus (-X) \oplus X$$

is canonically isomorphic to X, and the orthogonal complement of this submodule is hyperbolic, since it splits as the direct sum of $D(X \oplus (-X)) \oplus 0$ and $0 \oplus D((-X) \oplus X)$, each of which is self annihilating. Passing to the Witt ring, it follows that the identity

$$X + (-X) = 0$$

is satisfied in W(A).

Now suppose that as ring A we choose a field F of characteristic 2. Then the theory undergoes several drastic simplifications. Thus the isomorphism $X \cong -X$ implies that every element of the Witt ring W(F) has order 2. Furthermore the quadratic function

$$q(x) = x \cdot x$$

from X to F is now an additive homomorphism. Hence its image $q(X) \subset F$ is a finite dimensional vector space over the subfield $S = F^2$ consisting of all squares in F. This image q(X) will be called the *value space* of X. Note that X is hyperbolic if and only if $q(X) = 0$.

If q(X) contains a non-zero field element f, then clearly X splits as an orthogonal direct sum

$$X \cong \langle f \rangle \oplus X' .$$

Here $\langle f \rangle$ denotes the one-dimensional inner product module spanned by a single vector x with $q(x) = f$. By induction, this leads to a direct sum decomposition

$$X \cong \langle f_1 \rangle \oplus \ldots \oplus \langle f_n \rangle \oplus H;$$

with H hyperbolic. (Compare [2, p. 23].)

It follows easily that the square of every element in the Witt ring is either 0 or 1. Those elements with square 0 (corresponding to inner product modules of even rank) form a maximal ideal, which we denote by $\mathcal{J} \subset W(F)$. Since every element not in $\mathcal{J}$ is a unit, we see that W(F) is a local ring. (Compare [3, §10]. Pfister proves the corresponding statement for fields of characteristic $\neq 2$, assuming only that -1 is a sum of squares.)

3. *The Clifford algebra C*

Again let F be a field of characteristic 2, and let $S = F^2$ be the subfield consisting of all squares in F. The degree d of F over S is either a power of 2 or infinite.

We will think of F as a quadratic vector space over S, using the function

$$f \mapsto f^2 \in S$$

as canonical S-quadratic mapping from F to S. Hence we can form the Clifford algebra $C = C(F)$ associated with this quadratic vector space. (See for example [1, p. 139].) This is a $(Z/2Z)$ – graded algebra,

$$C = C_0 \oplus C_1 ,$$

of dimension 2^d over S. By definition, C is generated (as a ring) by the image of a canonical S-linear embedding, which we denote by

$$c : F \to C_1 .$$

If $\{a_1,\ldots,a_d\}$ forms a basis for F over S, then the products $c(a_{i_1})\ldots c(a_{i_p})$ with $i_1 < \ldots < i_p$ form a basis for C over S. The square of each generator c(f) of C is equal to f^2 times the identity element $1 \in C_0$. (Caution. Note that $c(f)c(g) \neq c(fg)$, and that $c(1) \neq 1$.)

It will be convenient to identify S with the set of S multiples of the identity element. This Clifford algebra C has the unusual property of being commutative. It follows easily that the square of *every* element of C belongs to the ground field S. Clearly those elements with square zero form a maximal ideal $\mathfrak{M}$, and those elements with square different from zero are units. Thus C is a local ring. Note that the quotient algebra $C/\mathfrak{M}$ over S is canonically isomorphic to F.

4. *The additive structure of* W(F)

Now we will relate the Witt ring of a field F of characteristic 2 to the Clifford algebra C over the subfield S.

An element of C is called *decomposable* if it can be written as a product $c(f_1)\ldots c(f_k)$ with $f_i \in F$. Let $C^\bullet$ be the group of all units in C, and let $S^\bullet$ be the subgroup consisting of all non-zero elements of S.

THEOREM 1. *The additive group of* W(F) *is canonically isomorphic to the multiplicative group consisting of all decomposable elements in the quotient* $C^\bullet/S^\bullet$.

Thinking of C as a vector space over S, each element of $C^\bullet/S^\bullet$ can of course be identified with a line through the origin in C. It follows that W(F) is canonically embedded in the projective space consisting of all lines through the origin in C.

While proving Theorem 1, we will also prove the following.

THEOREM 2. *Every element of* W(F) *is represented by one, and up to unique isomorphism only one, anisotropic inner product module* X_0.

(Compare [3, §8.2.1]. An inner product module is *anisotropic* if $q^{-1}(0) = 0$.)

The proofs will be based on the following elementary remark. If (c_{ij}) is a symmetric $n \times n$ matrix over a commutative ring of characteristic 2, let c(i) stand for the diagonal entry c_{ii}, and let c(ij) stand for the *square* of the off-diagonal entry c_{ij}.

LEMMA 1. *The determinant of* (c_{ij}) *is equal to* $\sum c(P_1)\ldots c(P_k)$, *to be summed over all partitions of the set* $\{1,\ldots,n\}$ *into one and two element subsets:*

$$\{1,\ldots,n\} = P_1 \cup \ldots \cup P_k .$$

Proof. This is just the classical formula $\det(c_{ij}) = \sum \pm c_{1\pi(1)}\cdots c_{n\pi(n)}$ together with the remark that the term corresponding to a permutation π cancels the term corresponding to π^{-1} unless $\pi = \pi^{-1}$.

Now consider an inner product module X over F. Choosing a basis $x_1,\ldots,x_r$ for X, consider the $r \times r$ matrix (c_{ij}) over C whose ij-th entry is

$$c_{ij} = c(x_i \cdot x_j) .$$

The determinant of this matrix will be called the *Clifford determinant of* X. This determinant belongs either to C_1 or to C_0 according as the rank r is odd or even.

LEMMA 2. *The Clifford determinant of* X *is a decomposable unit of* C, *well defined up to multiplication by units of* S. *Furthermore every decomposable unit of* C *occurs as the Clifford determinant of some* X.

Thus, setting $\Delta(X) = \det(c_{ij})S^{\bullet}$. it is evident that the function Δ extends to a well-defined homomorphism

$$\Delta : W(F) \to C^{\bullet}/S^{\bullet}.$$

Proof of Lemma 2. We must see what happens to the determinant of (c_{ij}) when we change the basis for X. If one basis vector x_h of X is replaced by a multiple fx_h then clearly:

$$c_{hh} \text{ is replaced by } f^2c_{hh} ,$$

$$(c_{ih})^2 \text{ is replaced by } f^2(c_{ih})^2 \text{ for } i \neq h ,$$

and c_{ij} is left unchanged for $i, j \neq h$. Using Lemma 1, it follows that the determinant of (c_{ij}) is multiplied by the element $f^2 \in S^{\bullet}$.

Now consider an elementary change of basis in which some x_h is replaced by $x_h + x_k$, with $h \neq k$. Then:

$$c_{hh} \text{ is replaced by } c_{hh} + c_{kk},$$

$$(c_{ih})^2 \text{ is replaced by } (c_{ih})^2 + (c_{ik})^2 \text{ for } i \neq h,$$

and c_{ij} is left unchanged for $i, j \neq h$. Hence the determinant of this new matrix car be expressed as a sum

$$\det(c_{ij}) + \det(c'_{ij})$$

where (c'_{ij}) is a singular symmetric matrix in which the h-th row is equal to the k-th row. In other words, the determinant remains unchanged. Since every basis change can be built up out of these two particular types of basis change, this proves that $\Delta(X)$ is well defined.

Finally, if

$$X \cong \langle a_1\rangle \oplus \ldots \oplus \langle a_n\rangle \oplus H ,$$

where H has inner product matrix $\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$ with respect to a suitable basis, then clearly

$$\Delta(X) = c(a_1) \ldots c(a_n)S^{\bullet}$$

is decomposable. Since any decomposable unit can be obtained in this way, this proves Lemma 2.

LEMMA 3. *An anisotropic inner product module is determined up to (unique) isomorphism by its Clifford determinant* $\Delta \in C^{\bullet}/S^{\bullet}$.

Proof. Consider two anisotropic modules, say

$$X \cong \langle a_1\rangle \oplus \ldots \oplus \langle a_m\rangle$$

and

$$Y \cong \langle b_1\rangle \oplus \ldots \oplus \langle b_n\rangle ,$$

with $\Delta(X) = \Delta(Y)$. We will prove by induction on m that $X \cong Y$.

Since X is anisotropic, the field elements $a_1, \ldots, a_m$ must be linearly independent over S. Similarly $b_1, \ldots, b_n$ are linearly independent over S.

Case 1. Suppose that the $m + n$ field elements $a_1, \ldots, a_m$, $b_1, \ldots, b_n$ are all linearly independent over S. Then the relation

$$c(a_1) \ldots c(a_m) \in c(b_1) \ldots c(b_n) S^{\bullet}$$

in the Clifford algebra implies that $m = n = 0$, so that $X \cong Y \cong 0$.

(Note in particular that if $m = 0$, then we are certainly in Case 1. So this case starts the induction.)

Case 2. Otherwise, there must exist some field element $f \neq 0$, which belongs both to the value space $Sa_1 + \ldots + Sa_m$ of X and to the value space $Sb_1 + \ldots + Sb_n$ of Y. It follows easily that

$$X = \langle f \rangle \oplus X', \quad Y = \langle f \rangle \oplus Y',$$

where X' and Y' are (necessarily anisotropic) submodules. Since $\Delta(X') = \Delta(Y')$, it follows by induction that $X' \cong Y'$, and hence $X \cong Y$.

The isomorphism is unique, since each element of X is uniquely characterized by its image $x \cdot x \in F$. This proves Lemma 3.

LEMMA 4. *Every inner product module* X *over* F *can be expressed as an orthogonal direct sum*

$$X \cong X_0 \oplus Y \oplus Y \oplus H,$$

with X_0 *anisotropic and with* H *hyperbolic.*

Proof by induction on the rank of X. If $x \cdot x = 0$ for every element of X, then X is hyperbolic, and we are finished. Otherwise $X \cong \langle f \rangle \oplus X'$ for some f and X'. Setting

$$X' \cong X_0' \oplus Y' \oplus Y' \oplus H'$$

by induction, there are two possibilities. If f belongs to the value space $q(X_0')$, then X_0' also splits as a sum $\langle f \rangle \oplus X_0''$, so that

$$X \cong X_0'' \oplus (\langle f \rangle \oplus Y') \oplus (\langle f \rangle \oplus Y') \oplus H',$$

as required. On the other hand if f does not belong to $q(X_0')$, then the direct sum $\langle f \rangle \oplus X_0'$ is anisotropic, and

$$X \cong (\langle f \rangle \oplus X_0') \oplus Y' \oplus Y' \oplus H',$$

as required. This proves Lemma 4.

Combining Lemmas 3 and 4, we have evidently proved Theorem 2. For the sum $Y \oplus Y \oplus H$ has trivial Clifford determinant, and represents the zero element of the Witt ring.

Theorem 1 follows also. For if $\Delta(X) = \Delta(X_0 \oplus Y \oplus Y \oplus H) = \Delta(X_0)$ is the identity element of $C^{\bullet}/S^{\bullet}$, then $X_0 = 0$, and hence X represents the zero element of $W(F)$.

We are now ready to classify inner product modules. Given X, let X_0 be the unique anisotropic module which satisfies $\Delta(X_0) = \Delta(X)$, and hence represents the same element of $W(F)$ as X.

THEOREM 3. *An inner product module* X *over* F *is characterized up to isomorphism by its associated anisotropic module* X_0, *by its value space* $q(X)$ *which must contain* $q(X_0)$, *and by its rank* r *which must have the form*

$$2 \dim_S q(X) - \operatorname{rank} X_0 + 2h$$

for some integer $h \geq 0$.

(Here $2h$ is the rank of any maximal hyperbolic subspace.)

The proof will be given in outline only. First note the identity

(1) $\langle a \rangle \oplus \langle b \rangle \oplus \langle b \rangle \cong \langle a \rangle \oplus \langle f^2a+b \rangle \oplus \langle f^2a+b \rangle$.

In fact if x, y, z are mutually orthogonal vectors with

$$x \cdot x = a, \quad y \cdot y = z \cdot z = b,$$

then the three vectors $x' = x + (y+z)fa/b$, $y' = fx+y$, and $z' = fx'+z$ are mutually orthogonal, with

$$x'\cdot x' = a, \quad y'\cdot y' = z'\cdot z' = f^2a+b\,.$$

(Compare [2, p. 24].)

Similarly note the identity

(2) $\langle a\rangle \oplus \langle a\rangle \oplus \langle a\rangle \cong \langle a\rangle \oplus$ (hyperbolic).

For if x,y,z are orthogonal with $x\cdot x = y\cdot y = z\cdot z = a$, then the three vectors $x+y+z$, $x+y$, and $x+z$ have the required inner products. (Compare §2.)

Now, starting with Lemma 4, and noting that the anisotropic summand X_0 is determined by $\Delta(X) = \Delta(X_0)$, it is not difficult to reduce X to a normal form depending only on X_0, $q(X)$, and the rank. This proves Theorem 3.

Now suppose that the degree d of F over S is finite. Let $P(C)$ denote the (2^d-1)-dimensional projective space over S consisting of all lines through the origin in C. We have defined a canonical embedding

$$\Delta : W \to P(C),$$

the image $\Delta(W)$ consisting of all lines which are decomposable.

THEOREM 4. *This set $\Delta(W) \subset P(C)$ of decomposable lines through the origin is precisely the set of* S*-rational points of a certain non-singular algebraic set Σ defined over* S. *This algebraic set Σ consists of two components, each of which is a rational variety of dimension* $d(d-1)/2$.

The two components of Σ are of course just the closures of the two subsets

$$\Delta(\mathcal{J}) \subset P(C_0) \quad\text{and}\quad \Delta(W-\mathcal{J}) \subset P(C_1),$$

corresponding to inner product modules of even rank or of odd rank respectively.

Proof. Choose a basis $f_1,\ldots,f_d$ for F over S. For each subset $I = \{i_1,\ldots,i_m\} \subset \{1,\ldots,d\}$, let e_I denote the product $c(f_{i_1})\ldots c(f_{i_m})$ in C. Evidently these products e_I form a basis for C over S.

We may assume that the field S is infinite. For if S is finite then

Next we will construct a rational parametrization of an open subset of $\Delta(W)$. Let X be an anisotropic inner product module, and suppose first that its image space $q(X)$ is the entire field F. (This is equivalent to the assumption that X has rank $r = d$.) Then there exists a unique basis $x_1,\ldots,x_d$ for X so that $q(x_i) = f_i$. Setting

$$c(x_i\cdot x_j) = c_{ij}\,,$$

the diagonal entries of the matrix (c_{ij}) are just the generators $c(f_1),\ldots,c(f_d)$, and the squares of the off-diagonal entries c_{ij} are completely arbitrary elements $(x_i\cdot x_j)^2$ of S. (See the argument below.)

Let $D-I$ stand for the complement of I in the index set $D = \{1,2,\ldots,d\}$. It will be convenient to define field elements $s_I \in S$ by setting

$$\det(c_{ij}) = \sum s_I\, e_{D-I}.$$

These coefficients s_I can be read off easily from Lemma 1. Thus the coefficient $s_\emptyset$ of $e_D = c(f_1)\ldots c(f_d)$ is equal to 1. Furthermore, for $i \neq j$ the coefficient $s_{\{i,j\}}$ of $e_{D-\{i,j\}}$ is equal to c_{ij}^2. For any set I consisting of $2m$ elements the coefficient s_I is now given by

(3) $s_I = \sum s_{P_1}\ldots s_{P_m}$, to be summed over all partitions of I into two element subsets: $I = P_1 \cup \ldots \cup P_m$. Finally, if I has an odd number of elements, then $s_I = 0$.

Thus the determinant of (c_{ij}) is completely specified by the $d(d-1)/2$ elements $s_{\{i,j\}}$ of S. Clearly the inner products $x_i\cdot x_j$, with $i \neq j$, can be completely arbitrary* elements of F. Hence their squares $s_{\{i,j\}}$ can be

*We must check that the resulting inner product matrix is non-singular. But a symmetric matrix over F whose diagonal entries are linearly independent over S can For if it were then the associated (degenerate) inner product completely arbitrary elements of S. Thus we have established a one-to-one correspondence between the subset of W(F) consisting of all anisotropic X with $q(X) = F$ and the set consisting of all $d(d-1)/2$-tuples of elements $s_{\{i,j\}}$ of S.

Now consider the invariant

$$\Delta(X) = (\det c(x_i \cdot x_j))S^\bullet$$

in the projective space P(C). We continue to assume that X is anisotropic of maximal rank d. Setting

$$\Delta(X) = (\sum s_I\, e_{D-I})S^\bullet ,$$

it is evident that the homogeneous coordinates s_I must satisfy the homogeneous equations

$$(3') \quad (s_\emptyset)^{m-1} s_I = \sum s_{P_1} \cdots s_{P_m}$$

with $s_\emptyset \neq 0$. (Again this is to be summed over all partitions of I into two element subsets.)

On the other hand, if X is an anisotropic module of rank $r < d$ then choosing an arbitrary basis $x_1, \ldots, x_r$ for X, an easy computation shows that the algebra element

$$\det(c(x_i \cdot x_j)) = \sum s_I\, e_{D-I}$$

satisfies the equation $s_\emptyset = 0$. Thus the argument above has given a rational parametrization precisely of the "open" subset of

$$\Delta(W) \subset P(C)$$

consisting of all $(\sum s_I\, e_{D-I})S^\bullet$ in Δ(W) for which $s_\emptyset \neq 0$.

To prove Theorem 4, we must give an analogous parametrization, for each $J \subset D$, of the open set consisting of all $(\sum s_I\, e_{D-I})S^\bullet$ in Δ(W)

for which $s_J \neq 0$. But multiplication by e_J gives rise to an involution of P(C) which carries Δ(W) onto itself, and transforms the open set $s_J \neq 0$ onto the open set $s_\emptyset \neq 0$. The corresponding homogeneous equation

$$(4) \quad s_J^{\,m-1} s_{I+J} = \sum s_{P_1+J} \cdots s_{P_m+J}$$

for $s_J \neq 0$ now follows. Here I+J stands for the symmetric difference $(I \cup J) - (I \cap J)$, and again we sum over partitions of I into two element subsets. The coordinate s_{I+J} is zero if I has an odd number of elements.

Note that the equation (3′) is actually valid for every point

$$(\sum s_I\, e_{D-I})S^\bullet$$

in Δ(W), even when $s_\emptyset = 0$. In fact if the given point lies in

$$\Delta(W) \cap P(C_1),$$

then evidently both sides of (3′) are zero. So it suffices to consider a point in $\Delta(W) \cap P(C_0)$. Choose some index set J for which $s_J \neq 0$. Normalizing the homogeneous coordinates by setting $s_J = 1$, the remaining coordinates can then be expressed as polynomial functions of $d(d-1)/2$ among them, by (4). Substituting these polynomial functions into (3′), we obtain an identity between polynomial functions which is valid wherever the polynomial function $s_\emptyset$ is not zero. Since $s_\emptyset$ is not identically zero on the set $s_J \neq 0$, and since the field S is infinite, it follows that (3′) is valid everywhere. Similarly the equations (4) are valid throughout Δ(W).

To work within the usual framework of algebraic geometry, we must choose some large algebraically closed extension $\Omega \supset S$, and consider points $(\sum \omega_I\, e_{D-I})\Omega^\bullet$ with coefficients in Ω. The equations (4) define an algebraic set Σ in the projective space $P(\Omega \otimes C)$ over Ω, and it is now easy to check that each of the two components of Σ is rational and

Remark. The set $\Delta(W)$ can also be described as the set of S-rational points of an algebraic group G, which is an open subset of Σ. Recall that $\mathfrak{M}$ denotes the maximal ideal in C. Evidently the product operation in C gives rise to a well-defined polynomial product operation in the open set $P(C) - P(\mathfrak{M})$. Extending the field S of scalars to the algebraically closed field Ω, consider the algebra $\Omega \otimes C$ and its maximal ideal $\mathfrak{M}'$. Clearly $P(\Omega \otimes C) - P(\mathfrak{M}')$ is a commutative algebraic group defined over S. The relatively closed subset $G = \Sigma - \Sigma \cap P(\mathfrak{M}')$ is also an algebraic group, and the set of S-rational points of G is precisely $\Delta(W)$.

5. *The multiplicative structure of* W(F).

Recall that $\mathfrak{J} \subset W(F)$ denotes the unique maximal ideal. We will consider the successive powers

$$\mathfrak{J} \supset \mathfrak{J}^2 \supset \mathfrak{J}^3 \supset \ldots$$

THEOREM 5. *If the degree of* F *over* S *is* $d = 2^k < \infty$, *then the ideal* $\mathfrak{J}^k$ *is non-zero, but* $\mathfrak{J}^{k+1} = 0$.

Remark. This integer k, which measures the "imperfection" of F, is invariant under finite extensions of F, and increases by 1 under a simple transcendental extension.

The following definition will be convenient. Elements $a_1, \ldots, a_n$ of F are *"independent"* over S if the field $S(a_1, \ldots, a_n)$ has degree 2^n over S.

LEMMA 5. *Suppose that the elements* $a_1, \ldots, a_n$ *of* F *are "independent" over* S, *and that* $b \neq 0$ *is an element of* $S(a_1, \ldots, a_n)$. *Then the inner product module*

$$X = (\langle a_1\rangle \oplus \langle 1\rangle) \otimes \ldots \otimes (\langle a_n\rangle \oplus \langle 1\rangle)$$

is isomorphic to $X \otimes \langle b\rangle$.

Proof. For each subset $I = \{i_1, \ldots, i_r\}$ of $\{1, \ldots, n\}$ let

$$a_I = a_{i_1} \ldots a_{i_r} \in F .$$

Thus X is isomorphic to an orthogonal direct sum:

$$X \cong \bigoplus \langle a_I\rangle .$$

In other words X has an orthogonal basis consisting of vectors x_I with $q(x_I) = a_I$.

Since the elements a_I form a basis for $S(a_1, \ldots, a_n)$ over S, we can write b uniquely as a sum

$$b = \sum f_I^2 a_I .$$

Let J+I again denote the symmetric difference $(J \cup I) - (J \cap I)$, and let J–I stand for $J-(J \cap I)$. Consider the vectors

$$y_J = \sum_I f_{J+I}\, a_{J-I}\, x_I$$

in X. Evidently

$$y_J \cdot y_K = \sum_I f_{J+I}\, f_{K+I}\, a_{J-I}\, a_{K-I}\, a_I .$$

If $J \neq K$, then the I-th term cancels the $(I + J + K)$-th term, so that $y_J \cdot y_K = 0$. If $J = K$, then

$$y_J \cdot y_J = \sum_I f_{J+I}^2\, a_{J-I}^2\, a_I = \sum_I f_{J+I}^2\, a_{J+I}\, a_J = b a_J$$

This proves that

$$X \cong \bigoplus \langle b a_J\rangle \cong X \otimes \langle b\rangle ,$$

which proves Lemma 5.

Proof of Theorem 5. To show that $\mathfrak{J}^{k+1} = 0$, it suffices to show that every product of the form

$$(\langle a_1\rangle + \langle 1\rangle)\ldots(\langle a_{k+1}\rangle + \langle 1\rangle)$$

is zero in W(F). Given $a_1,\ldots,a_{k+1}$ in F, let $n \geq 0$ be the largest integer such that $a_1,\ldots,a_n$ are "independent" over S. Then $n \leq k$, since F has degree 2^k over S. But Lemma 5 implies that

$$(\langle a_1\rangle + \langle 1\rangle)\ldots(\langle a_n\rangle + \langle 1\rangle)\langle 1\rangle$$

$$= (\langle a_1\rangle + \langle 1\rangle)\ldots(\langle a_n\rangle + \langle 1\rangle)\langle a_{n+1}\rangle,$$

from which the conclusion follows.

Conversely, choosing "independent" elements $a_1,\ldots,a_k$, it is clear that

$$(\langle a_1\rangle + \langle 1\rangle)\ldots(\langle a_k\rangle + \langle 1\rangle) \neq 0$$

in W(F). This completes the proof.

Concluding Remarks. It would be interesting to have further information about this chain of ideals

$$W(F) \supset \mathcal{J} \supset \mathcal{J}^2 \supset\ldots\supset \mathcal{J}^k \supset 0 .$$

Presumably the homomorphism Δ carries each $\mathcal{J}^n$ to a subvariety of $\Delta(W)$? The dimension of this subvariety should depend only on n and k.

Note that $\Delta(\mathcal{J})$ is the intersection of $\Delta(W)$ and $P(C_0)$. Similarly it can be shown that $\Delta(\mathcal{J}^2) = \Delta(W) \cap P(S+\mathfrak{M}_0)$, where $\mathfrak{M}_0 = \mathfrak{M} \cap C_0$. Perhaps each $\Delta(\mathcal{J}^n)$ is the intersection of $\Delta(W)$ with a suitable projective space?

It would also be interesting to study the quotient groups $\mathcal{J}^n/\mathcal{J}^{n+1}$. For $n = 1$ this quotient is canonically isomorphic to $F^\bullet/S^\bullet$. (Compare Pfister [6].) As in [5], one can define groups K_nF which generalize the usual groups of algebraic K-theory. There is a canonical surjection

$$K_nF/2K_nF \to \mathcal{J}^n/\mathcal{J}^{n+1}.$$

For $n = 0,1,2$ this surjection is actually bijective, but the corresponding question for higher values of n remains open.

Institute for Advanced Study
Princeton, New Jersey

REFERENCES

[1] N. Bourbaki, Éléments de Math. XXIV – Algèbre – Ch. 9, Formes sesquilinéaires et formes quadratiques.

[2] I. Kaplansky, Linear Algebra and Geometry – A Second Course, Allyn and Bacon, 1969.

[3] M. Knebusch, *Grothendieck-und Wittringe von nichtausgearteten symmetrischen Bilinearformen*, Sitzungsb. Heidelb. Akad. Wiss., Math.-nat. Kl. 1969/70, 3. Abh.

[4] J. Milnor, *On simply connected 4-manifolds*, pp. 122-128 of "Symposium Internat. de Topologia Alg.", Mexico, 1958.

[5] ____________, *Algebraic K-theory and quadratic forms*, Invent. math. 9 (1970), 318-344.

[6] A. Pfister, *Quadratische Formen in beliebigen Körpern*, Invent. Math. 1, (1966), 116-132.

[7] J. P. Serre, *Formes bilinéaires symétriques entières a discriminant* ±1, Sem. Cartan 1961/62, Exp. 14-15.

[8] E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. reine angew. Math. 176, (1937), 31-44.