5. PFISTER FORMS

§5.1. Pfister Forms

The **tensor product** of two diagonal quadratic forms is defined by:

$$\langle a_1, \ldots, a_m\rangle \otimes \langle b_1, \ldots, b_m\rangle$$
$$= \langle a_1b_1, \ldots, a_1b_m, a_2b_1, \ldots, a_2b_m, \ldots, a_mb_n\rangle.$$

NOTES:

(1) $\otimes$ is well-defined, commutative, associative and distributive over $\oplus$.

(2) In W(F) we have ab = core ($a \otimes b$).

(3) $a \otimes$ H is hyperbolic for any quadratic form a.

A Pfister plane is a 2-dimensional quadratic form of the form $\langle 1, a\rangle$.

Notation: $\langle\langle a\rangle\rangle$.

Example 1: H = $\langle\langle -1\rangle\rangle$ is a Pfister plane.

A **Pfister form** is a quadratic form of the form:

$$\langle\langle a_1\rangle\rangle \otimes \ldots \otimes \langle\langle a_n\rangle\rangle.$$

Notation: $\langle\langle a_1, \ldots, a_n\rangle\rangle$.

Example 2:

(1) 2^nH = $\langle\langle -1, -1, \ldots, -1\rangle\rangle$ (with $n + 1$ terms).

(2) The quadratic form $\langle 1, -a, -b, ab\rangle$ associated with the quaternion algebra $[a, b]_F$ is $\langle\langle -a, -b\rangle\rangle$.

(3) $2^n\langle 1\rangle = \langle\langle 1, 1, \ldots, 1\rangle\rangle$ (with n terms).

NOTE: $\langle\langle -1, a_1, \ldots, a_n\rangle\rangle = H \otimes \langle\langle a_1, \ldots, a_n\rangle\rangle$ and so is hyperbolic.

If φ is a quadratic form then $\varphi = \langle 1\rangle \oplus \varphi'$ for some quadratic form φ'. Call **φ'** the **pure subform** of φ. This generalises the pure part of a quaternion algebra.

If φ is a quadratic form:
$D_F(\varphi)$ is defined to be $\{a \in F \mid \varphi(x_1, \ldots, x_n) = a$ for some n and some $x_1, \ldots, x_n \in F\}$.

$D_F^{\#}(\varphi)$ denotes the non-zero elements of $D_F(\varphi)$.

Example 3: $\frac{1}{2} \in D_{\mathbb{Q}}(\langle 1, 1\rangle)$ since $\frac{1}{2} = (\frac{1}{2})^2 + (\frac{1}{2})^2$.

Theorem 1:
(1) $\langle\langle a, b\rangle\rangle = \langle\langle a, ab\rangle\rangle$;
(2) If $a + bk^2 \neq 0$ then $\langle\langle a, b\rangle\rangle = \langle\langle a + bk^2, ab\rangle\rangle$.
Proof:
(1) $\langle\langle a, ab\rangle\rangle = \langle 1, a, ab, a^2b\rangle$
$= \langle 1, a, ab, b\rangle$
$= \langle\langle a, b\rangle\rangle$.
(2) Suppose that $a + bk^2 \neq 0$.
Then $\langle a, b\rangle \cong a(x - kby)^2 + b(kx + ay)^2$
$= \langle a + bk^2, (a + bk^2)ab\rangle$.

(Note that the determinant of the transformation is $a + bk^2 \neq 0$.)

Hence $\langle\langle a, b\rangle\rangle = \langle 1, a, b, ab\rangle$

$$= \langle 1, a + bk^2, (a + bk^2)ab, ab\rangle$$

$$= \langle\langle a + bk^2, ab\rangle\rangle.$$ ✋☺

Corollary: If $a + b \neq 0$ then $\langle\langle a, b\rangle\rangle = \langle\langle a + b, ab\rangle\rangle$.

§5.2. Isotropic Pfister Forms

Theorem 2: If $\varphi = \langle\langle a_1, \ldots, a_n\rangle\rangle$ and $b_1 \in D_F(\varphi)^\#$ then

$$\varphi \cong \langle\langle b_1, \ldots, b_n\rangle\rangle \text{ for some } b_2, \ldots, b_n \in F.$$

Proof: Induction on n.

If $n = 1$, $\varphi = \langle\langle a_1\rangle\rangle$ and $\varphi' = \langle a_1\rangle$.

Hence $b_1 = a_1x^2$ for some $x \in F^\#$ and so

$$\varphi = \langle 1, a_1\rangle = \langle 1, b_1\rangle = \langle\langle b_1\rangle\rangle.$$

Suppose it is true for $n - 1$.

Let $\tau = \langle\langle a_2, \ldots, ba_n\rangle\rangle$.

Now $\varphi = \langle\langle a_1\rangle\rangle \otimes \tau$

$$= \langle 1, a_1\rangle \otimes \tau$$

$$= (\langle 1\rangle \oplus \langle a_1\rangle) \otimes \tau$$

$$= \tau \oplus a_1\tau$$

$$= \langle 1\rangle \oplus \tau' \oplus a_1(\langle 1\rangle \oplus \tau').$$

Hence $\varphi' = \tau' \oplus a_1(\langle 1\rangle \oplus \tau')$.

Hence $b_1 = x + a_1(k^2 + y)$ for some $x, y \in D_F(\tau')$ and $k \in F$.

Case I: $k^2 + y = 0$:

Then $b_1 \in D_F{}^\#(\tau')$ and so by induction,

$\tau = \langle\langle b_1, \ldots, b_{n-1}\rangle\rangle$ for some $b_2, \ldots, b_{n-1}$.

Putting $b_n = a_1$, $\varphi = \langle\langle b_1, \ldots, b_n\rangle\rangle$.

Case II: $k^2 + y \neq 0$:
In this case we show first that $\varphi = \langle\langle a_1(k^2 + y)\rangle\rangle \otimes \tau$.
If $y = 0$, this is obvious, so suppose $y \neq 0$.
Then $y \in D_F^{\#}(\tau')$.
By induction, $\tau = \langle\langle x, b_3, \ldots, b_n\rangle\rangle$ for some $b_3, \ldots, b_n$.
Thus $\varphi = \langle\langle a_1(k^2 + y), x, b_3, \ldots, b_n\rangle\rangle$.
Now $\langle\langle a_1(k^2 + y), x\rangle\rangle = \langle\langle a_1(k^2 + y) + x, a_1(k^2 + y)x\rangle\rangle$
by the corollary to Theorem 1.
$= \langle\langle b_1, b_2\rangle\rangle$ if we choose
$b_2 = a_1(k^2 + y)$.
Hence $\varphi = \langle\langle b_1, b_2, b_3, \ldots, b_n\rangle\rangle$. ✋☺

Theorem 3: An isotropic Pfister form is hyperbolic.
Proof: If φ is an isotropic Pfister form, $\varphi = H \oplus \theta$ for some θ.
Therefore $\varphi' = \langle -1\rangle \oplus \theta$.
Hence $-1 \in D_F^{\#}(\varphi)$ and so by Theorem 2,
$\varphi = \langle\langle -1, b_2, \ldots, b_n\rangle\rangle$ for some $b_2, \ldots, b_n$ which is hyperbolic. ✋☺

§5.3. The Characteristic of a Witt Ring

The **characteristic** of a ring R with 1 is:

$$\begin{cases} \text{the additive order of 1 if this is finite} \\ 0 \text{ if 1 has infinite order} \end{cases}.$$

We denote it by **char R**.

NOTE: If R has characteristic n then the additive order of every element divides n because $nr = (n1)r = 0$. The characteristic of a field is 0 or prime, but for general rings it may be composite.

Theorem 4:
If W(F) has finite characteristic it is a power of 2.
Proof: Let char W(F) = n where $2^{k+1} < n \le 2^k$.
Then $n\langle 1\rangle$ is hyperbolic and so 2^k is isotropic.
Hence by Theorem 3, it is hyperbolic and so
in W(F), $2^k\langle 1\rangle = 0$.
Hence n divides 2^k and so is a power of 2. ✋☺

Theorem 5: If -1 can be expressed as a sum of n squares in F, but no fewer, then n is a power of 2.
Proof: Let $2^k \le n < 2^{k+1}$.
Then $-1 = x_1^2 + \ldots + x_n^2$ for some x_i's $\in F^\#$.
Therefore $(n + 1)\langle 1\rangle$ is isotropic and so $2^{k+1}\langle 1\rangle$ is hyperbolic.
Thus in W(F) $2^{k+1}\langle 1\rangle = 0$.
Hence char F divides 2^{k+1}.

Let char(F) = 2^{t+1} where $0 \le t \le k$.
Then $2^{t+1}\langle 1\rangle$ is hyperbolic and so $2^{t+1}\langle 1\rangle \cong 2^t\langle 1, -1\rangle$.
By Witt's Cancellation Theorem $2^t\langle 1\rangle \cong 2^t\langle -1\rangle$.
Hence -1 can be expressed as a sum of 2^t squares and so:

$$2^k \le n \le 2^t \le 2^k.$$

Thus $n = 2^t = 2^k$. ✋☺

§5.4. The Level of a Field

The **level** of a field is:

$$\begin{cases} \text{the smallest } n \text{ such that } -1 \text{ is a sum of } n \text{ squares} \\ \infty \text{ if no such } n \text{ exists} \end{cases}.$$

Theorem 6: If F has finite level n, char W(F) = $2n$. ✋

Examples 3:

(1) level $\mathbb{C} = 1$;

(2) level $\mathbb{R}$ = level $\mathbb{Q} = \infty$;

(3) the level of a finite field F = $\begin{cases} 1 \text{ if } |F| \equiv 1 \pmod 4 \\ 2 \text{ if } |F| \equiv 3 \pmod 4 \end{cases}$.

Theorem 7: If n is a positive square-free integer the level of $\mathbb{Q}[i\sqrt{n}] \leq 4$.

Proof: $-1 = (i\sqrt{n})^2 + n - 1$. ✋☺

By a theorem of Lagrange, every positive integer is the sum of at most 4 squares. Hence level $\mathbb{Q}[i\sqrt{n}] \leq 5$. By Theorem 5, level $\mathbb{Q}[i\sqrt{n}] \leq 4$.

In fact, level $\mathbb{Q}[i\sqrt{n}] = \begin{cases} 1 \text{ if } n = 1 \\ 4 \text{ if } n \equiv -1 \pmod 8 \\ 2 \text{ otherwise} \end{cases}$.

Example 4: Express -1 as a sum of 4 squares in $\mathbb{Q}[i\sqrt{7}]$.

Solution: $-1 = (i\sqrt{7})^2 + 2^2 + 1^2 + 1^2$.

Example 5: Express –1 as a sum of 2 squares in $\mathbb{Q}[i\sqrt{3}] = \mathbb{Q}[\omega]$.
Solution: $-1 = \omega + \omega^2$.

Example 6: Express –1 as a sum of 2 squares in $\mathbb{Q}[i\sqrt{13}]$.
Solution: $-1 = \left(\frac{3}{2}\right)^2 + \left(\frac{i\sqrt{13}}{2}\right)^2$.

NOTE: If $n = a^2 + b^2$, $-1 = \left(\frac{i\sqrt{n}}{a}\right)^2 + \left(\frac{b}{a}\right)^2$.
If $n - 1 = a^2 + b^2$ then:

$$-1 = \left(\frac{a}{n-1} + \frac{bi\sqrt{n}}{n-1}\right)^2 + \left(\frac{b}{n-1} - \frac{ai\sqrt{n}}{n-1}\right)^2 .$$

coopersnotes.net
LIST OF TITLES

GENERAL

- The Mathematics At The Edge Of The Rational Universe

ELEMENTARY

- Basic Mathematics
- Concepts of Algebra
- Concepts of Calculus
- Elementary Algebra
- Elementary Calculus

1st YEAR UNI

- Techniques of Algebra
- Techniques of Calculus
- Matrices

2nd YEAR UNI

- Linear Algebra
- Languages & Machines
- Discrete Mathematics

3rd YEAR UNI

- Group Theory volume 1
- Group Theory volume 2
- Galois Theory
- Graph Theory
- Number Theory
- Geometry
- Topology
- Set Theory

POSTGRADUATE

- Ring Theory
- Representation Theory
- Quadratic Forms
- Group Tables vol 1
- Group Tables vol 2