THE ALGEBRAIC THEORY OF QUADRATIC FORMS - AN INTRODUCTION

PAWEL GLADKI

Abstract. The following notes are based on a series of talks given at the Algebra and Logic Seminar at the University of Saskatchewan in the Summer 2004. They are entirely dependent on the cited bibliography. The main purpose of those notes is to provide some introductory knowledge required for understanding open questions in the theory of spaces of orderings that we are studying at the seminar. The material contained in those notes covers - more or less - the first chapter of the paper [6] and is intended to be as self-contained as possible.

1. Introduction

Recall that a **bilinear space** over a field K is a pair (V, β), where V is a finite dimensional vector space over the field K and $\beta : V \times V \to K$ is a bilinear functional on the space V. The **dimension** of a bilinear space is the dimension of the corresponding vector space V. A vector $v \in V$ is said to be **isotropic** if $v \neq 0$ and $\beta(v, v) = 0$. The space (V, β) is said to be **symmetric** when the bilinear functional β is symmetric and is said to be **alternating** if $\beta(v, v) = 0$ for every $v \in V$. If $\mathcal{B} = (v_1, \ldots, v_n)$ is a basis for the vector space V then the matrix $[\beta(v_i, v_j)]$ is called **the matrix of the bilinear space V relative to $\mathcal{B}$**. For two bases $\mathcal{B}$ and $\mathcal{C}$ and for two matrices A and B of β relative to $\mathcal{B}$ and $\mathcal{C}$, respectively, the following formula holds:

$$B = PAP^T,$$

where P denotes the transition matrix from $\mathcal{B}$ to $\mathcal{C}$ (for proof see [3], pages 95 - 100). The **determinant** of a bilinear space is defined to be the determinant of a matrix of β relative to any basis - it depends on the choice of the basis. According to the above formula we have:

$$\det B = (\det P)^2 \cdot \det A,$$

thus the determinant might be considered as an element of the **square class group** of the field K, that is the factor group $U(K)/U(K)^2$. In that sense the determinant is unique. We say that bilinear spaces (V, β) and (U, α) are **isometric** (written $V \cong U$) if there exists an isomorphism $i : V \to U$ such that:

$$\beta(u, v) = \alpha(i(u), i(v)),$$

for all $u, v \in V$. Since two bilinear spaces are isometric iff their matrices relative to any bases are congruent (for proof see [3], pages 95 - 100), we shall also use the notation $V \cong A$ to indicate that A is the matrix of V relative to some basis. Next, it can be shown (for proof see [3], pages 95 - 100) that the following five conditions for a given space (V, β) whose matrix relative to some basis is A are equivalent:

(1) $rad_1(V) = \{v \in V : \beta(v, u) = 0, u \in V\} = \{0\}$,

(2) $rad_2(V) = \{v \in V : \beta(u, v) = 0, u \in V\} = \{0\}$,
(3) $\det A \neq 0$,
(4) the mapping $\Lambda : V \to V^*$ given by:

$$\Lambda(v)(u) = \beta(v, u),$$

is an isomorphism of vector spaces,
(5) the mapping $\Psi : V \to V^*$ given by:

$$\Psi(v)(u) = \beta(u, v),$$

is an isomorphism of vector spaces.

If any (and hence all) of the above conditions are satisfied, we call (V, β) to be **non-singular**. Finally, we say that a space V is **diagonalizable** (or has an **orthogonal basis**) if there is a basis producing a diagonal matrix for V. The well-known Gramm-Schmidt theorem (for proof see [3], pages 109 - 112) states, that any bilinear symmetric space over a field of characteristic different from 2 is diagonalizable. In the case of characteristics 2 the theorem holds if we make an additional assumption that V is non-alternating. If A is a matrix with diagonal entries $a_1, \dots, a_n$ we shall simply write $(a_1, \dots, a_n)$ instead of A.

2. Hyperbolic planes, isotropic planes

Let K be any field, let (V, β) be a bilinear space over K. We say that vectors $u, v \in V$ form a **hyperbolic plane** if:

$$\beta(u, u) = \beta(v, v) = 0, \qquad \beta(u, v) = \beta(v, u) = 1.$$

The plane spanned on a hyperbolic pair is called the **hyperbolic plane**. We shall give some alternative definitions of hyperbolic planes.

Theorem 1. *Let (V, β) be a bilinear, symmetric, non-singular space of dimension 2 over a field K of characteristic different from 2. The following are equivalent:*

(1) *V is a hyperbolic plane,*
(2) *$V \cong \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$,*
(3) *$V \cong (1, -1)$,*
(4) *$\det V = (-1)U(K)^2$.*

Proof. (1)⇒(2) is trivial: just take the appropriate hyperbolic pair. To prove (2)⇒(3) suppose that u, v is the basis relative to which V has the matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Consider the vectors $x = \frac{1}{2}u + v$ and $y = \frac{1}{2}u - v$. Those vectors form a basis for V, since the transition matrix $\begin{bmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & -1 \end{bmatrix}$ is nonsingular. Moreover, by a direct computation:

$$\begin{bmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & -1 \end{bmatrix}^T = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

(3)⇒(4) is trivial, and for (4)⇒(1) assume that (a, b) is a diagonalization for V. Since $\det V = (-1)U(K)^2$, $abU(K)^2 = (-1)U(K)^2$, so $aU(K)^2 = -bU(K)^2$ and $V \cong (a, -a)$ is a certain basis $\{u, v\}$ of V. Then $u + v \neq 0$ and $\beta(u + v, u + v) = \beta(u, u) + 2\beta(u, v) + \beta(v, v) = \beta(u, u) + \beta(v, v) = a - a = 0$. Since V is nonsingular, there is a $w \in V$ such that $\beta(u + v, w) = c \neq 0$, so $\beta(u + v, \frac{1}{c}w) = 1$. The vectors

$u+v$ and $\frac{1}{c}w$ are linearly independent, since otherwise $\frac{1}{c}w = d(u+v)$, where $d \in K$, and then:

$$1 = \beta(u+v, \frac{1}{c}w) = \beta(u+v, d(u+v)) = d\beta(u+v, u+v) = d \cdot 0 = 0,$$

a contradiction. Thus $u+v$ and $\frac{1}{c}w$ form a basis for V such that the matrix of β relative to $(u+v, \frac{1}{c}w)$ is:

$$\begin{bmatrix} 0 & 1 \\ 1 & e \end{bmatrix}.$$

If $e = 0$ the proof is finished, so assume that $a \neq 0$. In this case take the vectors $u+v$ and $-\frac{1}{2}e(u+v) + \frac{1}{c}w$. Straightforward computation gives:

$$\beta(u+v, -\frac{1}{2}e(u+v) + \frac{1}{c}w) = \beta(u+v, \frac{1}{c}w) = 1$$

and

$$\beta(-\frac{1}{2}e(u+v)+\frac{1}{c}w, -\frac{1}{2}e(u+v)+\frac{1}{c}w) = -e\beta(u+v, \frac{1}{c}w)+\beta(\frac{1}{c}w, \frac{1}{c}w) = -e+e = 0.$$

□

A 2-dimensional bilinear space (V, β) over a field K is said to be an **isotropic plane** if there is an isotropic vector in V. Since singular planes are obviously isotropic, we will focus on nonsingular isotropic planes. Using similar tricks as in the previous proof we may show that the followin theorem holds.

Theorem 2. *Let (V, β) be a bilinear, symmetric, non-singular space of dimension 2 over a field K of characteristic different from 2. The following are equivalent:*

(1) *V is an isotropic plane,*
(2) $V \cong \begin{bmatrix} 0 & 1 \\ 1 & a \end{bmatrix}$ *for some $a \in K$,*
(4) $V \cong \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$,
(5) $V \cong (1, -1)$,
(6) $V \cong (a, -a)$ *for all $a \in U(K)$,*
(7) $\det V = (-1)U(K)^2$.

An arbitrary hyperbolic plane is always isotropic. The converse is true under the assumption that *charK* $\neq 2$. In the case when *charK* $= 2$ the following holds:

Theorem 3. *Let (V, β) be a bilinear, symmetric, non-singular space of dimension 2 over a field K of characteristic 2. The following are equivalent:*

(1) *V is isotropic but not hyperbolic,*
(2) *there is an $a \in U(K)$ such that* $V \cong \begin{bmatrix} 0 & 1 \\ 1 & a \end{bmatrix}$,
(3) *there is an $a \in U(K)$ such that* $V \cong (a, a)$.

The formal proof uses the same techniques as the previous and will be omitted.

3. Direct orthogonal sums. Metabolic and hyperbolic spaces.

Let (V, β) be a bilinear space over a field K, let $U_1, \ldots, U_k$ be subspaces of V. We say that V is the **internal direct orthogonal sum** of $U_1, \ldots, U_k$ if V is the direct sum of linear subspaces $U_1, \ldots, U_k$ (that is $V = U_1 + \ldots + U_k$ and for any $j \in \{1, \ldots, k\}$ $U_j \cap (U_1 + \ldots + U_{j-1} + U_{j+1} + \ldots + U_k) = \{0\}$) and for $u_i \in U_i$, $u_j \in U_j$, $i \neq j$, $\beta(u_i, u_j) = 0$. We will also need a more general concept of the **external direct orthogonal sum**. Let $(U_1, \beta_1), \ldots, (U_k, \beta_k)$ be a family of bilinear spaces over the same field K. We introduce a new vector space $V = U_1 \times \ldots \times U_k$ and make it into a bilinear space by defining a bilinear functional $\beta : V \times V \to K$ by the formula:

$$\beta((u_1, \ldots, u_k), (v_1, \ldots, v_k)) = \sum_{i=1}^{k} \beta_i(u_i, v_i).$$

If we identify the spaces U_i with subspaces $U_i' = \{0\} \times \ldots \times U_i \times \ldots \times \{0\}$, then the external direct orthogonal sum of U_i turns to be the internal direct orthogonal sum of U_i'. For both internal and external direct orthogonal sums we use notation $U_1 \perp \ldots \perp U_k$. The basic properties of direct orthogonal sums are gathered in the following theorem:

Theorem 4. *Let K be any field, let U, V, W, S, T be bilinear spaces over K.*

(1) $U \perp \{0\} \cong U$,
(2) $U \perp W \cong W \cong U$,
(3) $(U \perp W) \perp V \cong U \perp (W \perp V)$,
(4) $U \cong S \wedge W \cong T \Rightarrow U \perp W \cong S \perp T$,
(5) $\dim U \perp W = \dim U + \dim W$,
(6) $\det U \perp W = \det U \cdot \det W$,
(7) *if U and W are nonsingular, so is $U \perp W$.*

Proofs of the above identities are easy and left as an exercise - for example to prove (2) we shall consider the map $\Phi : U \times W \to W \times U$ given by $\Phi(u, w) = (w, u)$ and check, that Φ is an isometry.

The notion of direct orthogonal sums allows us to define metabolic and hyperbolic spaces. We say that (V, β) is **hyperbolic**, when there are hyperbolic planes H_i such that $V \cong H_1 \perp \ldots \perp H_k$. We say that V is **metabolic**, if there are nonsingular, symmetric isotropic planes P_i such tkat $V \cong P_1 \perp \ldots \perp P_k$. Obviously every hyperbolic space is metabolic, but over fields of characterictic not equal to 2 a metabolic space not necessarily is hyperbolic.

We will extensively use the following Witt decomposition theorem:

Theorem 5. *For every nonsingular symmetric space V over an arbitrary field K there exist uniquely determined subspaces M and N such that $V \cong M \perp N$, M is metabolic and N is anisotropic.*

Proof. First we will prove the existence of such decomposition. If N is anisotropic, there is nothing to prove. Asuume that V is isotropic and pick an isotropic vector $v \in V$. Since V is nonsingular, there is $w \in V$ such that $\beta(v, w) = b \neq 0$. The vectors v and w are linearly independent, since otherwise $w = cv$ and then:

$$0 \neq b = \beta(v, w) = \beta(v, cv) = c\beta(v, v) = 0,$$

a contradiction. Thus v, w span an isotropic plane, which is nonsingular; its matrix is:

$$\begin{bmatrix} 0 & b \\ b & a \end{bmatrix}.$$

Therefore V contains at least one metabolic subspace. From among all metabolic subspaces we choose one, which has the largest dimension and call it M. By the well-known orthogonal complement theorem (see [3] page 102) $V = M \perp M^{\perp}$, where $M^{\perp} = \{u \in V : \beta(v, u) = 0, v \in M\}$. It remains to show that $N = M^{\perp}$ is anisotropic. The orthogonal complement theorem implies, that N is nonsingular. If N were isotropic, we could choose an isotropic vector $v' \in N$ and build a nonsingular isotropic plane P contained in N. Then $M \perp P$ would be metabolic of the dimension greater than M - a contradiction.

The proof of uniqueness of such decomposition is based on some geometric arguments like the index of isotropy and could be found in [8], pages 150 - 159. □

4. Similarity of symmetric spaces

Let U and V be nonsingular symmetric spaces over an arbitrary field K. U and V are said to be **similar** (written $U \sim V$), if there are metabolic spaces M_1 and M_2 such that:

$$M_1 \perp U \cong M_2 \perp V.$$

Checking that $\sim$ is an equivalence relation that splits the set of all nonsingular symmetric bilinear spaces over the field K into disjoint classes of equivalence is left to the reader. Such classes are called **similarity classes** and denoted by $< U >$. The following lemma states the most basic properties of similarity relation.

Lemma 1. (1) *$< 0 >$ consists of all metabolic spaces,*
(2) *if $U \cong V$ then $U \sim V$, but the converse is not true in general,*
(3) *if U and V are anisotropic, then $U \sim V$ implies that $U \cong V$,*
(4) *if $V = M \perp N$ is the Witt decomposition of V, then $V \sim N$,*
(5) *every similarity class contains an anisotropic space unique up to isometry,*
(6) *every class contains a diagonalizable space and thus can be presented in the form:*

$$< V > = < a_1, \dots, a_n >,$$

(7) *dimensions of similar spaces differ by an even number.*

Proof. To prove (1) assume that $V \sim 0$, so there exist metabolic spaces M_1 and M_2 such that:

$$M_1 \perp V \cong M_2 \perp 0 \cong M_2.$$

Thus $M_1 \perp V$ and M_1 are both metabolic. Consider the Witt decomposition of the space V, $V = M \perp N$, where M is metabolic and N is nonsingular. We have:

$$M_1 \perp V \cong M_1 \perp M \perp N.$$

Both $M_1 \perp M$ and $M_1 \perp V$ are metabolic, so due to the uniqueness of the Witt decomposition of $M_1 \perp V$ $N \cong 0$ and thus V becomes metabolic.

In order to show (2) observe, that if $U \cong V$, then for any metabolic space M $M \perp U \cong M \perp V$, so $U \cong V$. To show (3) assume, that both U and V are anisotropic and $U \sim N$, that is $M_1 \perp U \cong M_2 \perp V$ for some metabolic M_1 and M_2. But uniqueness of the Witt decomposition guarantees that $U \cong V$.

Next, (4) follows from the fact that the zero space is metabolic and:

$$0 \perp V\ congV \cong M \perp N,$$

while (5) is implied by (3) and (4).

To prove (6) first assume that $< V >$ is the nonzero class. Then V is not metabolic, hence diagonalizable. It remains to point out a diagonalizable space in the zero class $< 0 >$ - but it is clear that $(-1, 1)$ is isotropic, hence metabolic and belonging to $< 0 >$. The statement (7) is obvious since metabolic spaces are of even dimension. □

5. Witt group of a field

Let K be an arbitrary field, let $W(K)$ denote the set of all silimarity classes of nonsingular symmetric spaces over K. We shall make $W(K)$ into a group by defining addition of similarity classes as follows:

$$< U > + < V > = < U \perp V > .$$

The sum $< U > + < V >$ does not depend on the choice of representatives U and V. For if $< U > \sim < S >$ and $< V > \sim < T >$, then let $M_1, \dots, M_4$ be metabolic spaces such that:

$$M_1 \perp U \cong M_2 \perp S, M_3 \perp V \cong M_4 \perp T.$$

Hence by theorem 4:

$$M_1 \perp M_3 \perp U \perp V \cong M_2 \perp M_4 \perp S \perp T,$$

so $< U > + < V > = < S > + < T >$. Neutrality of the zero class $< 0 >$, commutativity and associativity of addition follow similarly from theorem 4. It remains to show that each element $< u > \in W(K)$ has the opposite element $< V > \in W(K)$ satisfying $< U > + < V > = < 0 >$. If U is the bilinear space (U, α), our choice for V is the opposite bilinar space $(U, -\alpha)$, where:

$$(-\alpha)(u_1, u_2) = -\alpha(u_1, u_2),$$

denoted briefly $-U$. We claim that the space

$$(U, \alpha) \perp (U, -\alpha)$$

is metabolic. Observe that if u_1, u_2 are orthogonal in (U, α) then they are orthogonal in $(U, -\alpha)$. Hence if (U, α) is diagonalizable space and $(U, \alpha) \cong (a_1, \dots, a_n)$, then so is the opposite space and $(U, -\alpha) \cong (-a_1, \dots, -a_n)$. If $charK \neq 2$, then by 2 $(a, -a) \cong (1, -1)$ and by 4:

$$\begin{aligned}(U, \alpha) \perp (U, -\alpha) &\cong (a_1, \dots, a_n) \perp (-a_1, \dots, -a_n)\\ &\cong (a_1, -a_1) \perp \dots \perp (a_n, -a_n)\\ &\cong (1, -1) \perp \dots \perp (1, -1).\end{aligned}$$

Thus $(U, \alpha) \perp (U, -\alpha)$ is hyperbolic and hence metabolic. If $charK = 2$, we first assume that (U, α) is alternating. Let $u \in U$, $u \neq 0$. Then $\alpha(u, u) = 0$ and, by nonsingularity, there is a vector $v \in U$ such that $\alpha(u, v) = a \neq 0$. Then also $\alpha(u, \frac{1}{a}v) = 1$, and so we can say that for each nonzero $u \in U$ there is $v \in U$ such that $\alpha(u, v) = 1$. Notice, that u and v are linearly independent, since if $v = bu$, then:

$$1 = \alpha(u, v) = b\alpha(u, u) = 0,$$

a contradiction. The vectors u and v span a plane S. Since:

$$0 = \alpha(u+v, u+v) = \alpha(u,u) + \alpha(u,v) + \alpha(v,u) + \alpha(v,v) = \alpha(u,v) + \alpha(v,u),$$

it follows, that S has the matrix:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

But $charK = 2$, so $-1 = 1$ and thus the plane S is symmetric. Therefore U contains symmetric, nonsingular isotropic plane and - in particular - $\dim U \geq 2$. If $\dim U \geq 2$, we proceed by induction; by the orthogonal complement theorem we have:

$$U = S \perp S^{\perp}.$$

Here $S^{\perp}$ is nonsingular and has a dimension smaller than U. Hence by induction $S^{\perp} = P_1 \perp \ldots \perp P_k$, where P_i are pairwise orthogonal symmetric, nonsingular isotropic planes, so U is metabolic. Finally, if U is not alternating, then U is diagonalizable, $(U, \alpha) \cong (a_1, \ldots, a_n)$, so:

$$\begin{aligned} (U,\alpha) \perp (U, -\alpha) &\cong (a_1, \ldots, a_n) \perp (a_1, \ldots, a_n) \\ &\cong (a_1, a_1) \perp \ldots \perp (a_n, a_n), \end{aligned}$$

which is the direct orthogonal sum of nonsingular isotropic planes (see theorem 3).

The additive abelian group $W(K)$ of similarity classes of nonsingular symmetric spaces over a field K is said to be the **Witt group of the field K.**

Observe that when

$$< U > = < a_1, \ldots, a_n >, < V > = < b_1, \ldots, b_m >$$

are representations of the classes $< U >$ and $< V >$, then:

$$- < a_1, \ldots, a_n > = < -a_1, \ldots, -a_n >$$

and

$$< a_1, \ldots, a_n > + < b_1, \ldots, b_m > = < a_1, \ldots, a_n, b_1, \ldots, b_m > .$$

We shall give some examples of Witt groups.

Example 1. *Let K be a formally real field. Then the Witt group $W(K)$ contains elements of infinite order and hence is infinite abelian.*

As we know, K has characteristic zero, so metabolic spaces and hyperbolic spaces over K coincide and are direct orthogonal sums of hyperbolic planes $(-1, 1)$. Consider the odd-dimensional class $< 1 > \in W(K)$. Suppose that $n \cdot < 1 > = 0$ for a positive integer n. Then:

$$< 1, 1, \ldots, 1 > = < 1 > + < 1 > + \ldots < 1 > = n \cdot < 1 > = 0,$$

so the $n-$dimensional space $(1, \ldots, 1)$ is hyperbolic:

$$(1, \ldots, 1) \cong (1, -1, \ldots, 1, -1),$$

contrary to the fact that, over a formally real field, it does not represent -1. Thus $n \cdot < 1 > \neq 0$ for all positive integers n.

Recall that a field K is called **quadratically closed** if every element of K is a square of an element of K. Obviously the complex number field $\mathbb{C}$, as well as any algebraically closed field, is quadratically closed. It turns out that all finite fields of characteristic two are quadratically closed.

Example 2. *Let K be a quadratically closed field. Then the Witt group $W(K)$ is the 2-element group.*

Since K is quadratically closed, for all $a_1, \dots, a_n \in K$ $(a_1, \dots, a_n) \cong (1, \dots, 1)$. Thus each class $< U >$ in $W(K)$ can be written in the form:

$$< U >=< a_1, \dots, a_n >=< 1, \dots, 1 >= n\cdot < 1 > .$$

Since -1 is a square, for each nonsingular symmetric space U we have $U \cong -U$, so:

$$2\cdot < U >=< U > + < U >=< U > + < -U >= 0,$$

in particular $2\cdot < 1 >= 0$. Therefore $< U >= n\cdot < 1 >=< 0 >$ or $< 1 >$, depending on the parity of n and teh Witt group $W(K)$ consists of two elements 0 and $< 1 >$, where $< 1 >$ is of order 2.

Example 3. *The Witt group $W(\mathbb{R})$ of the field of real numbers is an infinite cyclic group, $W(\mathbb{R}) \cong \mathbb{Z}$.*

As we already know, $< 1 >$ is an element of infinite order. Let $< U >$ be a nonzero class and consider the presentation $< U >=< a_1, \dots, a_n >$, where $(a_1, \dots, a_n)$ is an anisotropic space. Using the same techniques as in the proof of the well-known inertia theorem (see [3] page 104) we conclude that either $(a_1, \dots, a_n) \cong (1, \dots, 1)$ or $(a_1, \dots, a_n) \cong (-1, \dots, -1)$. In the first case we have $< U >= n\cdot < 1 >$ and in the second case $< U >= n\cdot < -1 >$.

Now we shall introduce the notion of the dimension index. For an arbitrary field K define the map $e : W(K) \to \mathbb{Z}/2\mathbb{Z}$ by sending the class $< U >$ into $\dim U (mod 2)$. Observe, that e is a well defined group epimorphism. The well-definedness and surjectivity are obvious and it is a group homomorphism as the following computation shows:

$$\begin{aligned} e(< U > + < V >) &= e(< U \perp V >) = \dim(U \perp V) + 2\mathbb{Z} \\ &= (\dim U + \dim V) + 2\mathbb{Z} = (\dim U + 2\mathbb{Z}) + (\dim V + 2\mathbb{Z}) \\ &= e(< U >) + e(< V >). \end{aligned}$$

The homomorphism e is called the **dimension index** homomorphism. As an immediate consequence of the isomorphism theorem we kave the following statement:

$$W(K)/\ker e \cong \mathbb{Z}/2\mathbb{Z}.$$

6. Tensor products of bilinear spaces

We shall extend the notion of tensor products to bilinear spaces. For two bilinear spaces (U, α) and (V, β) over a field K their tensor product is to be a bilinear space $(U \otimes V, \gamma)$, where γ is a suitably chosen bilinear functional on the space $U \otimes V$. Consider the following diagram:

$$\begin{tikzcd}
U \times V \times U \times V \arrow[d, "\otimes"'] \arrow[rrd, "\alpha\cdot\beta"] & & \\
U \otimes V \otimes U \otimes V \arrow[rr, "h"'] & & K \\
U \otimes V \times U \otimes V \arrow[u, "\otimes"] \arrow[rru, "\gamma"'] & &
\end{tikzcd}$$

Here $\alpha \cdot \beta$ is the product of bilinear functionals α and β, that is the $4-$linear map $\alpha \cdot \beta : U \times V \times U \times V \to K$ defined by:

$$\alpha \cdot \beta(u, v, u', v') = \alpha(u, u') \cdot \beta(v, v').$$

By the universal property of tensor products there is a linear map $h : U \otimes V \otimes U \otimes V \to K$ such that:

$$h(u \otimes v \otimes u' \otimes v') = \alpha(u, u') \cdot \beta(v, v'),$$

so that the upper triangle in our diagra commutes. Now $\otimes$ in the vertical bottom line is the map that assigns to each pair of vectors $w_1, w_2 \in U \otimes V$ the simple tensor $w_1 \otimes w_2 \in (U \otimes V) \otimes (U \otimes V)$ and we define $\gamma : U \otimes V \times U \otimes V \to K$ to be the composition of the $\otimes$ and the map h. Thus $\gamma(w_1, w_2) = h(w_1 \otimes w_2)$ for all $w_1, w_2 \in U \otimes V$, in particular for the simple tensors $u \otimes v, u' \otimes v' \in U \otimes V$:

$$\gamma(u \times v, u' \otimes v') = h(u \otimes v \otimes u' \otimes v') = \alpha(u, u') \cdot \beta(v, v').$$

Since γ is the composition of the bilinear map $\otimes$ and the linear functional h, it is bilinear itself.

To show that γ is uniquely determined observe, that each bilinear functional γ on the space $U \otimes V$ satisfying:

$$\gamma(u \times v, u' \otimes v') = \alpha(u, u') \cdot \beta(v, v')$$

is uniquely determined on the set of all simple tensors $u \otimes v$ of the space $U \otimes V$, and these generate the space $U \otimes V$. Hence, by bilinearity of γ it is uniquely determined on the whole space $U \otimes V$.

The bilinear functional γ on the space $U \otimes V$ is said to be the **tensor product of bilinear functionals** α and β, written:

$$\gamma = \alpha \otimes \beta.$$

The bilinear space $(U \otimes V, \alpha \otimes \beta)$ is said to be the **tensor product of spaces** (U, α) and (V, β).

Now we shall investigate a matrix of the space $(U \otimes V, \alpha \otimes \beta)$. Suppose that $\{u_1, \dots, u_n\}$ and $\{v_1, \dots, v_m\}$ are bases for U and V and let $A = [a_{ij}]$, $B = [b_{ij}]$ be matrices for U and V with respect to the appropriate bases. We know that $\{u_i \otimes v_j : i \in \{1, \dots, n\}, j \in \{1, \dots, m\}\}$. We will find the matrix of $U \otimes V$ relative to this basis. First we choose the following order of basis vectors:

$$u_1 \otimes v_1, \dots, u_1 \otimes v_m, u_2 \otimes v_1, \dots, u_2 \otimes v_m, \dots, u_n \otimes v_1, \dots, u_n \otimes v_m.$$

If C denote the matrix of the space $U \otimes V$ relative to the above basis, then we have:

$$C = [(\alpha \otimes \beta)(u_i \otimes v_j, u_k \otimes v_l)] = [\alpha(u_i, u_k) \cdot \beta(v_j, v_l)] = [a_{ik} b_{jl}],$$

thus:

$$C = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n} \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \dots & a_{nn}B \end{bmatrix}.$$

The matrix C is called the **Kronecker product** of matrices A and B and is denoted by $A \otimes B$.

7. Witt ring and the fundamental ideal

Let K be any field and let $W(K)$ be the Witt group of the field K. We shall make it into a commutative ring by setting:

$$< U > \cdot < V >=< U \otimes V > .$$

Quite long and boring but straightforward computation shows that this multiplication is well defined and $(W(K), +, \cdot, < 0 >, < 1 >)$ is indeed a commutative ring with identity, which is said to be the **Witt ring of the field** K. Observe that each element of the Witt ring $W(K)$ can be written in the form $< a_1, \ldots, a_n >$ for some $a_1, \ldots, a_n \in U(K)$ and we have the following rules for computation in the ring $W(K)$:

$$< a_1, \ldots, a_n >=< b_1, \ldots, b_m > \Leftrightarrow (a_1, \ldots, a_n) \sim (b_1, \ldots, b_m),$$

$$< a_1, \ldots, a_n > + < b_1, \ldots, b_m >=< a_1, \ldots, a_n, b_1, \ldots, b_m >,$$

$$< a_1, \ldots, a_n > \cdot < b_1, \ldots, b_m >=< a_1b_1, \ldots, a_1b_m, \ldots, a_nb_1, \ldots, a_nb_m > .$$

Structure of the Witt ring can be completely described only when we have solved the classification problems for bilinear spaces over the field K. As was the case of the Witt group we can check, that the Witt ring of a quadratically closed field is isomorphic to the 2-element group and that the Witt ring of the field $\mathbb{R}$ is isomorphic to the ring $\mathbb{Z}$. We can also easily check that the dimension index map $e : W(K) \to \mathbb{Z}/2\mathbb{Z}$ sending the class $< U >$ into $\dim U(mod2)$ is a well defined ring epimorphism. The ideal $\ker e$ is said to be the **fundamental ideal** of the Witt ring $W(K)$ and is denoted by $I(K)$:

$$I(K) = \{< U >\in W(K) : \dim U \equiv 0(mod2)\}.$$

From the isomorphism theorem of ring theory follows immediately that:

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

We shall find a convenient set of generators of the fundamental ideal $I(K)$. For that purpose we introduce the notion of $n-$**ary classes**: we call the similarity class $< U >\in W(K)$ $n-$ary if it contains an $n-$dimensional space:

$$< U >=< a_1, \ldots, a_n >,$$

in particular for $n = 1, 2, 3, 4$ we speak of **unary, binary, ternary** and **quaternary** classes. We will carefully distinguish between generating $I(K)$ as an ideal in the Witt ring $W(K)$ and as an additive group, the subgroup of the additive Witt group $W(K)$. The following theorem exhibits a set of generators for the ideal $I(K)$ viewed as an additive group:

Theorem 6. *The fundamental ideal is additively generated by the following set of binary classes:*

$$\{< 1, a >: a \in U(K)\}.$$

Proof. The proof is rather trivial; given any element $< U >=< a_1, \ldots, a_n >$ of the Witt ring $W(K)$, we can write

$$< a_1, \ldots, a_n >=< 1, a_1 > + \ldots + < 1, a_n > -n\cdot < 1 > .$$

Now if $< a_1, \ldots, a_n >$ is an element of $I(K)$, then it is even-dimensional, so $n = 2m$ and hence:

$$< a_1, \ldots, a_n >=< 1, a_1 > + \ldots + < 1, a_n > -m\cdot < 1, 1 > .$$

□

8. Discriminant and the square of fundamental ideal

We know that a nonsingular isotropic plane P over a field K has the determinant $\det P = (-1)U(K)^2$, hence for a metabolic space $M = P_1 \perp \ldots \perp P_k$ we have $\det M = (-1)^k U(K)^2$. Any two metabolic spaces are similar, but when $-1 \notin U(K)^2$ the determinant assumes two distinct values. It follows that the determinant is not a similarity invariant. To modify the determinant function to make it well defined on similarity classes we introduce the notion of the discriminant. More precisely, let U be a nonsingular bilinear space over a field K. The **discriminant** of the space U is the element of the square class group $U(K)/U(K)^2$ defined as follows:

$$disc U = (-1)^{\frac{n(n-1)}{2}} \det U,$$

where $n = \dim U$.

Observe that if $U \sim V$ then $discU = discV$. Indeed, let $M_1 \perp U \cong M_2 \perp V$, where M_1, M_2 are metabolic and let $\dim M_1 = 2p$, $\dim M_2 = 2q$, $\dim U = n$ and $\dim V = m$. Therefore:

$$2p + n = \dim(M_1 \perp U) = \dim(M_2 \perp V) = 2q + m$$

and

$$(-1)^p \det U = \det(M_1 \perp U) = \det(M_2 \perp V) = (-1)^q \det V.$$

Thus $n - m$ is an even number, hence $n^2 - m^2$ is divisible by 4, and so:

$$2p + n(n-1) - (2q + m(m-1)) = 2(m-n) + n^2 - m^2 \equiv 0 (mod 4,)$$

hence also:

$$p + \frac{n(n-1)}{2} \equiv q + \frac{m(m-1)}{2} (mod 2)$$

and finally:

$$\begin{aligned} discU &= (-1)^{\frac{n(n-1)}{2}} \det U = (-1)^{p+\frac{n(n-1)}{2}} (-1)^p \det U \\ &= (-1)^{q+\frac{m(m-1)}{2}} (-1)^q \det V = (-1)^{\frac{m(m-1)}{2}} \det V \\ &= discV \end{aligned}$$

The above observation allows us to extend the notion of discriminant to the similarity classes: the **discriminant of the similarity class** $< U >$ is defined to be the common value $discU$ of discriminants of all spaces in the class $< U >$. The discriminant is thus a well defined map:

$$disc : W(K) \to U(K)/U(K)^2.$$

Unfortunately, this map is not a homomorphism: for take a field K with $-1 \notin U(K)^2$. Then we have $disc < 1 >= U(K)^2$, $disc < 1, 1 >= -U(K)^2$ and so:

$$disc(< 1 > + < 1 >) = -U(K)^2 \neq U(K)^2 = disc < 1 > \cdot disc < 1 > .$$

However, if we restrict ourselves to the fundamental ideal, the situation changes. Namely we have the following theorem:

Theorem 7. *The restriction disc* : $I(K) \to U(K)/U(K)^2$ *is an epimorphism of the additive group of the ideal* $I(K)$ *onto the square class group* $U(K)/U(K)^2$.

Proof. Let $< U >$ and $< V >$ be $n-$ary and $m-$ary classes. Since both numbers are even $n^2 + m^2 - (n+m)^2$ is divisible by 4, so:

$$n^2 - n + m^2 - m \equiv (n+m)^2 - (n+m)(mod 4)$$

and we have:

$$\frac{n(n-1)}{2} + \frac{m(m-1)}{2} \equiv \frac{1}{2}(n+m)(n+m-1)(mod 2).$$

Now the following computation proves our theorem:

$$\begin{aligned} disc(< U > + < V >) &= disc(< U \perp V >) \\ &= (-1)^{\frac{1}{2}(n+m)(n+m-1)} \det U \cdot \det V \\ &= (-1)^{\frac{n(n-1)}{2}} \det U (-1)^{\frac{m(m-1)}{2}} \det V \\ &= disc < U > \cdot disc < V > \end{aligned}$$

□

We proceed to the less obvious problem of determining the kernel of discriminant homomorphism. First observe, that if $0 \neq < U > \in \ker disc$ then $\dim U \geq 4$. It is clear that U is a nonzero space of even dimension, so it suffices to check that $\dim U \neq 2$. Assume *a contrario* that $U \cong (a,b)$. Then $U(K)^2 = disc < U > = disc < a, b > = -abU(K)^2$, so $bU(K)^2 = -aU(K)^2$ and thus $< U > = < a, b > = < a, -a > = 0$, which is impossible.

Next, all quaternary classes $< 1, a, b, ab >$ have discriminants equal to $U(K)^2$ and thus they belong to the $\ker disc$. In general the quaternary class $< a, b, c, d >$ belongs to the $\ker disc$ iff. there exist $x, y \in U(K)$ such that:

$$< a, b, c, d > = < a > \cdot < 1, x > \cdot < 1, y > .$$

Indeed, if $< a, b, c, d > \in \ker disc$ then $U(K)^2 = disc < a, b, c, d > = abcdU(K)^2$, so $dU(K)^2 = abcU(K)^2$ and hence:

$$\begin{aligned} < a, b, c, d > &= < a, b, c, abc > \\ &= < a >< 1, ab, ac, bc > \\ &= < a >< 1, ab >< 1, ac > \end{aligned}$$

as desired. Conversely, since $disc < a >< 1, x >< 1, y > = disc < a, ax, ay, axy > = U(K)^2$, every class of the form $< a >< 1, x >< 1, y >$ lies in the kernel of discriminant.

Now observe that since $< 1, x >$ and $< 1, y >$ belong to the fundamental ideal, their product $< 1, x, y, xy >$ belongs to the square of the ideal $I(K)$, denoted $I^2(K)$. In the fact more general proposition holds, namely the ideal $I^2(K)$ is additively generated by the following set:

$$\{< 1, a, b, ab >: a, b, \in U(K)\}$$

To show that recall that we already know that $I(K)$ is additively generated by the binary classes $< 1, a >$, $a \in U(K)$, so every element in $I(K)$ is the sum of products xy, x and y being finite sums of classes of the form $< 1, a >$. Multiplying out we get a finite sum of the classes $< 1, a, b, ab >$.

That means, that $I^2(K) \subset \ker disc$. It appears that the opposite inclusion holds: we have the following theorem due to Pfister:

Theorem 8. $I^2(K) = \ker disc$

Proof. Let $< U >$ be a nonzero even-dimensional class of discriminant $U(K)^2$, $n = \dim U$. We know that $n \geq 4$ and if $n = 4$ then $< U >=< a, b, c, d >=< a ><1, x >< 1, y >\in I^2(K)$. Hence we may assume that:

$$< U >=< a_1, \dots, a_n >$$

where $n \geq 6$ and $n \equiv 0 (mod 2)$. We proceed by induction on n. First observe that:

$$< a, b, c, d >=< 1, a, b, ab > + < 1, c, d, cd > - < 1, 1, ab, ab > + < ab, -cd >$$

and thus for each quaternary class we have:

$$< a, b, c, d > +I^2(K) =< ab, -cd > +I^2(K).$$

For now we can write:

$$\begin{aligned} < U > +I^2(K) &= < a_1, a_2, a_3, a_4 > + < a_5, \dots, a_n > +I^2(K) \\ &= < a_1a_2, -a_3a_4 > + < a_5, \dots, a_n > +I^2(K) \end{aligned}$$

and since $I^2(K) \subset \ker disc$:

$$< U > - < a_1a_2, -a_3a_4, a_5, \dots, a_n >\in I^2(K) \subset \ker disc,$$

but $< U >\in \ker disc$, hence it follows that:

$$< V >=< a_1a_2, -a_3a_4, a_5, \dots, a_n >\in \ker disc.$$

Now $< V >$ is an $(n-2)-$ary class, so by inductive hypothesis $< V >\in I^2(K)$. But $< U > - < V >$ also belongs to $I^2(K)$ and thus $< U >\in I^2(K)$. □

As an immediate consequence of the Pfister theorem and the isomorphism theorem we have the following isomorphism of groups:

$$I(K)/I^2(K) \cong U(K)/U(K)^2.$$

In the case when $W(K)$ is finite this gives another useful equality. Since $disc : I(K) \to U(K)/U(K)^2$ is an epimorphism, $U(K)/U(K)^2$ is also finite and since $W(K)/I(K) \cong \mathbb{Z}/2\mathbb{Z}$, $|W(K)| = 2 \cdot |I(K)|$. Now $|I(K)| = |U(K)/U(K)^2| \cdot |I^2(K)|$, which gives:

$$|W(K)| = 2 \cdot |I^2(K)| \cdot |U(K)/U(K)^2|.$$

9. Quadratic forms

A homogeneous polynomial of degree 2 in n indeterminates is said to be a **quadratic form** in n indeterminates. In other words a quadratic form f is an expression:

$$\begin{array}{rcccccccc} f = f(X_1, \dots, X_n) & = & c_{11}X_1^2 & + & c_{12}X_1X_2 & + & \dots & + & c_{1n}X_1X_n \\ & & & + & c_{22}X_2^2 & + & \dots & + & c_{2n}X_2X_n \\ & & & & & & & & \vdots \\ & & & & & & \dots & & \\ & & & & & & & + & c_{nn}X_n^2 \end{array}$$

The quadratic form f is completely determined by the upper triangular coefficient matrix $C = [c_{ij}]$ (where $c_{ij} = 0$ for $i > j$) and it is often convenient to use the matrix notation:

$$f = f(X) = XCX^T,$$

where $X = [X_1, \dots, X_n]$. We associate with f the following polynomial:

$$P = P(X, Y) = XCY^T$$

in $2n$ indeterminates, where $X = [X_1, \dots, X_n]$ and $Y = [Y_1, \dots, Y_n]$. Observe that:

$$P(Y,X) = YCX^T = (XCY^T)^T = XC^TY^T,$$

so $P(X,Y) = P(Y,X)$ only if C is diagonal. Furthermore:

$$\begin{aligned} f(X+Y) &= (X+Y)C(X+Y)^T \\ &= XCX^T + XCY^T + YCX^T + YCY^T \\ &= f(X) + P(X,Y) + P(Y,X) + f(Y). \end{aligned}$$

The polynomial F given by:

$$F(X,Y) = P(X,Y) + P(Y,X)$$

is called the symmetric bilinear form **corresponding** to the quadratic form f. The name "symmetric bilinear form" refers to the fact that the polynomial F satisfies the following identities:

$$F(X,Y) = F(Y,X), F(X+Y,Z) = F(X,Z) + F(Y,Z),$$

$$F(aX,Y) = aF(X,Y).$$

Now from the definition of F follows, that F is completely determined by f, namely:

$$F(X,Y) = f(X+Y) - f(X) - f(Y)$$

in particular we have:

$$F(X,X) = 2f(X).$$

Moreover, if $charK \neq 2$, then f is uniquely determined by F:

$$f(X) = \frac{1}{2}F(X,X).$$

Also the previous computations show that that the form F has the following matrix representation:

$$F(X,Y) = X(C+C^T)Y^T,$$

where $C + C^T$ is symmetric and if $chakK \neq 2$, then the quadratic form f has the following matrix representation:

$$f(X) = XSX^T,$$

where $S = \frac{1}{2}(C + C^T)$ is symmetric. The process of passing from the upper triangular matrix representation of the form to the symmetric matrix representation is known as the **symmetrization**. If the symmetric matrix S is diagonal, then the symmetric matrix representation is called **diagonal representation**. It is easy to verify that in the case of the field of the characteristics different from 2 the symmetric representation is unique and in the case of characteristics two the symmetric representation exists if and only if S is diagonal.

Two basic problems in quadratic form theory are the **representation problem** and the **classification problem**. We say that a nonzero element $a \in K$ is **represented by f over K** if there are $x_1, \dots, x_n \in K$ such that:

$$f(x_1, \dots, x_n) = a.$$

The set of all nonzero elements represented by f over K is said to be the **value set** of the form f and is denoted by $D_K(f)$. The form f is said to be **isotropic**, if zero is represented nontrivially - otherwise it is said to be **anisotropic**. If all nonzero elements of K are represented by f, then f is called **universal** over K.

The concept of classification of quadratic forms is based on the notion of equivalence of quadratic forms. Two quadratic forms f and g over the same field K are said to be **equivalent**, written $f \cong g$, provided there exists a substitution:

$$\begin{array}{ccccccc} X_1 & = & p_{11}Y_1 & + & p_{21}Y_2 & \dots & p_{n1}Y_n, \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ X_n & = & p_{1n}Y_1 & + & p_{2n}Y_2 & \dots & p_{nn}Y_n, \end{array}$$

of indeterminates with a nonsingular matrix $P = [p_{ij}]$ called the **transition matrix** with entries in K such that:

$$f(YP) = g(Y).$$

It is routine to check that equivalence of quadratic forms is indeed an equivalence relation.

10. Quadratic forms and bilinear spaces

We show how to associate symmetric bilinear spaces with quadratic forms over K. Let $f = XCX^T$ be the upper triangular representation, let $F(X,Y) = XAY^T$ be the corresponding bilinear form, where $A = C + C^T$. We know that the bilinear form F determines a bilinear space (V, ϕ) over K with $V \cong A$ in a basis $\{v_1, \dots, v_n\}$ of the space V. We say that the symmetric bilinear space (V, ϕ) **corresponds** to the quadratic form f. The **dimension** of the form is defined to be the dimension of V. The quadratic form f is said to be **nonsingular** when V is nonsingular.

From now on we will assume that $charK \neq 2$. We are going to modify the concept of the bilinear space V corresponding to the form f. Let $f = f(X) = XSX^T$ be the symmetric representation of f, where $S = \frac{1}{2}(C + C^T)$. The polynomial $B = B(X,Y) = XSY^T$ is said to be **associated** with the quadratic form f and the symmetric bilinear space (U, α) that it defines is said to be **associated** with the quadratic form f.

Observe that:

$$B(X,Y) = \frac{1}{2}F(X,Y), B(X,X) = \frac{1}{2}F(X,X) = f(X)$$

and that the norm of the vector x in the space (U, α) agrees with $f(x)$ - that was not the case of the space (V, ϕ). Moreover, since $\det A = (\frac{1}{2})^n \det S$, where $n = \dim f$, nonsingularity of f is equivalent to nonsingularity of (U, α). Similarly f is isotropic over K if and only if (U, α) is isotropic. Finally, it is easy to check that if f and g are two forms with symmetric representations $f = XAX^T$ and $g = XBX^T$ and associated symmetric bilinear spaces U and V, then the following three concepts are equivalent:

(1) isometry of bilinear spaces U and V,
(2) congruence of matrices A and B,
(3) equivalence of quadratic forms f and g.

Thus assigning to every quadratic form f over K the associated symmetric bilinear space (U, α) establishes a bijective correspondence between equivalence classes of quadratic forms and isometry classes of symmetric bilinear spaces. This correspondence preserves dimensions and determinants. The very natural question that arises is of diagonalization of quadratic forms.

Lemma 2. *Let $charK \neq 2$ and let $a, b, c \in U(K)$*

(1) $c \in D_K(a,b) \Leftrightarrow (a,b) \cong (c, abc)$,

(2) $1 \in D_K(a, b) \Leftrightarrow (a, b) \cong (1, ab)$,
(3) $a = b \neq 0 \Rightarrow (a, b) \cong (a + b, ab(a + b))$.

Proof. It suffices to show (1). By the previous theorem a field element c is represented by the quadratic form $f = (a, b)$ iff. it is the norm of an anisotropic vector of the associated space U with the diagonal matrix (a, b). Let $c = q(v)$. Since c is nonzero, the vector v is anisotropic. By the Gramm-Schmidt orthogonalization theorem there is an orthogonal basis $\{v, v_1\}$ containing v - and thus V has the diagonalization (c, d). Hence $(a, b) \cong (c, d)$ for some d, and since a, b are nonzero, we must have $d \in U(K)$. Comparing determinants gives $abU(K)^2 = cdU(K)^2$, whence $dU(K)^2 = abcU(K)^2$ and $d = abc \cdot e^2$, so:

$$(a, b) \cong (c, abce^2) \cong (c, abc).$$

This happens iff. the quadratic form (a, b) is equivalent to the form (c, abc). □

As a result we have the following theorem:

Theorem 9. *Let f be a quadratic form over a field K, $charK \neq 2$, let $c \in D_K(f)$. There are $a_2, \dots, a_n \in K$ such that:*

$$f \cong (c, a_2, \dots, a_n)$$

Proof. Let $f = XSX^T$ be the symmetric representation of the form f and let U be the symmetric representation of f, let U be the associated symmetric bilinear space. Then $U \cong S$ and c is the norm of an anisotropic vector. Using the same argument as in the proof of the previous lemma we find elements $a_2, \dots, a_n \in K$ such that $U \cong (c, a_2, \dots, a_n)$. Hence the matrices S and $(c, a_2, \dots, a_n)$ are congruent and thus f is equivalent to the form $g = X(c, a_2, \dots, a_n)X^T$. □

We can also introduce the concepts of direct orthogonal sum and of tensor product of quadratic forms. Let f and g be quadratic forms in n and m indeterminates $X = [X_1, \dots, X_n]$, $Y = [Y_1, \dots, Y_m]$ and let

$$f = XCX^T, g = YDY^T$$

be the upper triangular representations of f and g. The **direct orthogonal sum** of quadratic forms f and g is defined to be the quadratic form $f \perp g$ with the following upper triangular matrix representation:

$$f \perp g = Z(C \perp D)Z^T.$$

The **tensor product** of f and g is the form whose upper triangular form is of the following type:

$$f \otimes g = Z(C \otimes D)Z^T.$$

11. Witt ring of quadratic forms

We will copy the construction of the Witt ring of similarity classes of nonsingular symmetric bilinear spaces to the case of nonsingular quadratic forms. A quadratic form H over K is said to be **hyperbolic** if it is equivalent to a direct orthogonal sum of binary hyperbolic forms:

$$H \cong h_1 \perp \dots \perp h_k.$$

We define two quadratic forms f and g to be **similar**, written $f \sim g$, if there are hyperbolic forms H_1 and H_2 such that:

$$H_1 \perp f \cong H_2 \perp g.$$

It is easily checked that $\sim$ is an equivalence relation and that both $\cong$ and $\sim$ are compatible with direct orthogonal sum and tensor product of quadratic forms. The class of quadratic forms similar to f is denoted $< f >$ and said to be the **similarity class** of the form f. On the set $W_{qf}(K)$ of all similarity classes of nonsingular quadratic forms over K we define the sum:

$$< f > + < g >=< f \perp g >$$

and the product:

$$< f > \cdot < g >=< f \otimes g >,$$

which are well defined on similarity classes. We distinguish the similarity class $< 0 >$ of the zero form and the class $< 1 >$ of the 1-dimensional quadratic form $< 1 >= X_1^2$. Now it is easy to check that $(W_{qf}, +, \cdot, < 0 >, < 1 >)$ is a commutative ring with identity and that this ring is isomorphic to the Witt ring $W(K)$ of similarity classes of nonsingular symmetric bilinear spaces over K:

$$W_{qf}(K) \cong W(K).$$

The details of the proof are found in [8], pages 222 - 224.

12. Pfister forms

We shall prove the basic properties of Pfister forms following the simplified approach of Witt. Let f be a quadratic form over an arbitrary field F. A scalar $a \in U(K)$ is said to be a **similitude factor** of the quadratic form f, if f and its scalar multiple af are equivalent quadratic forms:

$$f \cong af$$

The set of all similitude factors will be denoted $G_K(f)$. Notice that $G_K(f) \neq 0$ since $1 \in G_K(f)$ and that $G_K(0) = U(K)$. Moreover, $G_K(f)$ forms a subgroup of the multiplicative group and

$$U(K)^2 \subset G_K(f).$$

Indeed, let $a \in U(K)$ and let $f = XCX^T$ be the upper trianglular representation. Then $a^2 f = aX \cdot C \cdot (aX)^T$, so substitution $Y = (aI)X$ takes the form f to $a^2 f$ and thus $f \cong a^2 f$ and, consequently, $a^2 \in G_K(f)$.

Now if $a, b \in G_K(f)$ then $f \cong af$ and $f \cong bf$, hence $abf = a(bf) \cong af \cong f$, so $ab \in G_K(f)$. Since $G_K(f)$ contains the squares, it follows that $G_K(f)$ is a subgroup of $U(K)$.

Now we will establish the connection between $D_K(f)$ and $G_K(f)$. We have the following useful relationship:

$$G_K(f) \subset D_K(f) \Leftrightarrow 1 \in D_K(f).$$

Clearly, $1 \in G_K(f)$, hence if $G_K(f) \subset D_K(f)$, then $1 \in D_K(f)$. Conversely, assume that $1 \in D_K(f)$ and $a \in G_K(f)$. Let $1 = f(x)$. Since $af \cong f$, there is a substitution $X = PY$ of variables such that $af(PY) = f(Y)$. Taking $Y = x$ we get $af(Px) = f(x) = 1$. It follows that $a^{-1} = f(y) \in D_K(f)$ for $y = Px$, hence also $a = a^2 f(y) = f(ay) \in D_K(f)$, as required.

We will now exhibit a special type of diagonal forms representing 1 with a much stronger relationship between the value set and the group of similitude factors. Let K be an arbitrary field. The $n-$**fold Pfister form** over K, written $((a_1, \dots, a_n))$, is the form of the type:

$$(1, a_1) \otimes \dots \otimes (1, a_n).$$

We call the form (1) to be the 0-fold Pfister form.

If $f = ((a_1, \dots, a_n))$ is an $n-$fold Pfister form and $i_1, \dots, i_n$ is a permutation of $1, \dots, n$, then it is easy to find a suitable substitution of variables showing that

$$f \cong ((a_{i_1}, \dots, a_{i_n})).$$

Obviously we have $\dim((a_1, \dots, a_n)) = 2^n$. Also if $charK \neq 2$, then

$$\det((a_1, \dots, a_n)) = U(K)^2.$$

If $charK \neq 2$, then the similarity classes $< 1, a >$ of 1-fold Pfister forms over K additively generate the fundamental ideal $I(K)$ and the similarity classes of 2-fold Pfister forms additively generate the square $I^2(K)$ of the fundamental ideal.

Over the field K of characteristic different from two $G_K(1, a) = D_K(1, a)$; indeed, it suffices to show that $D_K(1, a) \subset G_K(1, a)$. If $b \in D_K(1, a)$ then $(1, a) \cong (b, ab)$, hence $(1, a) \cong b(1, a)$ and $b \in G_K(1, a)$, as desired. This result generalizes as follows:

Theorem 10. *Let f be a Pfister form over a field K of characteristic different from two. Then:*

$$G_K(f) = D_K(f)$$

Proof. We proceed by induction. The form f can be written as:

$$f = (1, a) \otimes g = g \perp ag$$

where g is an $(n-1)-$fold Pfister form. It suffices to show that $D_K(f) \subset G_K(f)$. Let $b \in D_K(f)$. Then

$$b = x + ay$$

where $x, y \in D_K(g) \cup \{0\}$. If $y = 0$, then $b = x$ and by induction hypothesis $b \in G_K(g)$. Thus we have:

$$bf = bg \perp abg \cong g \perp ag = f.$$

If $x = 0$, then $b = ay$ and:

$$bf = bg \perp abg = ayg \perp a^2yg \cong ag \perp g \perp f.$$

Finally, if $x \neq 0$ and $y \neq 0$, then we have $x, y \in D_K(g) = G_K(g)$. Put $z = x^{-1}y$. Since $G_K(g)$ is a group, we have $z \in G_K(g)$. Write $b = x + ay = x(1 + az)$ and $f = g \perp ag \cong g \perp azg = (1, az) \otimes g$. We have:

$$bf = x(1 + az) \cdot (1, az) \otimes g \cong x \cdot (1, az) \otimes g$$

since $1 + az \in D_K(1, az) = G_K(1, az)$. Thus we have:

$$bf \cong x \cdot (1, az) \otimes g \cong (1, az) \otimes xg \cong (1, az) \otimes g \cong f.$$

□

We will end this section with three important consequences of the above result.

Theorem 11. *Let $charK \neq 2$ and let f be a Pfister form. Then $D_K(f)$ is a group under multiplication.*

The proof is obvious. In order to state the next theorem we define the **index** $indf$ of a quadratic form f over a field of characteristic not equal to two to be the number of hyperbolic planes in a Witt decomposition of the symmetric bilinear space U associated with the form f.

Theorem 12. *Let $charK \neq 2$ and let f be a Pfister form.*

1. *f is isotropic iff. f is hyperbolic.*
2. *Either $indf = 0$ or $indf = \frac{1}{2}\dim f$.*

Proof. Clearly $indf = 0$ iff. f is anisotropic and $indf = \frac{1}{2}\dim f$ iff. f is hyperbolic, so (1) and (2) are equivalent and it suffices to show (1). Assume that the n-fold Pfister form f is isotropic. Then $n > 0$. If $n = 1$ then $f = (1, a)$ and by theorem 2 f is isotropic iff. f is hyperbolic. Now we proceed with induction. Let:

$$f = (1, a) \otimes g = g \perp ag.$$

If g is isotropic, then by induction hypothesis g is hyperbolic and so is f. If g is anisotropic, then - since f is isotropic - there exist $x, y \in D_K(g)$ such that $x+ay = 0$. That means that also $\frac{x}{y} \in D_K(g)$ and thus:

$$f = g \perp ag = g \perp -\frac{x}{y}g \cong g \perp -g$$

and the latter is hyperbolic. □

The third result is known as the Pure Subform Theorem. For a given form $f = ((a_1, \dots, a_n))$ we write:

$$f = (1) \perp f'$$

where $f' = (a_1, \dots, a_n, a_1a_2, \dots, a_{n-1}a_n, \dots, a_1 \dots a_n)$ is a quadratic form of dimension $2^n - 1$. If $charK \neq 2$ then f' does not depend on the diagonalization of f: if $(1) \perp f' = (1) \perp f''$ then by the Witt cancellation theorem we get $f' = f''$. The form f' is said to be the **pure subform** of the Pfister form f.

It is often necessary to decide whether or not a given 1-fold Pfister form $(1, b)$ is a factor (in the sense of tensor product) of the given n-fold Pfister form f. If $f \cong (1, b) \otimes g = g \perp bg$, then $f' \cong g' \perp bg \cong g' \perp (b) \perp bg'$, so b is represented by the pure subform f'. The Pure Subform Theorem states that this necessary condition is also sufficient.

Theorem 13. *Let $charK \neq 2$ and let f be a n-fold Pfister form. If $b \in D_K(f')$ then there are $b_2, \dots, b_n$ such that:*

$$f\ cong((b, b_2, \dots, b_n))$$

Proof. We proceed with induction on n. If $n = 1$ then $f = (1, a)$ and $f' = (a)$, so $b \in D_K(f') = aU(K)^2$ and thus $f \cong ((a)) \cong ((b))$.

If $n = 2$ then $f = ((a, c))$ and $b \in D_K(f') = D_K(a, c, ac)$. There are b_2, b_3 such that $(a, c, ac) \cong (a, b_2, b_3)$. Comparing determinants gives $U(K)^2 = bb_2b_3U(K)^2$, so $b_3U(K)^2 = bb_2U(K)^2$ and hence:

$$f = (1, a, c, ac) \cong (1, b, b_2, bb_2) = ((b, b_2)).$$

If $n \geq 3$ then $f = (1, a) \otimes g = g \perp ag$. Thus $f' = g' \perp ag$ and $b \in D_K(f')$ implies that:

$$b = x + ay$$

where $x \in D_K(g') \cup \{0\}$ and $y \in D_K(g) \cup \{0\}$. If $y = 0$ then $b = x$ and by induction hypothesis there are $b_2, \dots, b_n \in U(K)$ such that $g \cong ((b, b_3, \dots, b_n))$. Hence:

$$f = (1, a) \otimes g \cong ((b, a, b_3, \dots, b_n)).$$

If $x = 0$ then $b = ay$, so $yg \cong g$ and so

$$f = g \perp ag \cong g \perp ayg = (1, ay) \otimes g = (1, b) \otimes g.$$

If $x \neq 0$ and $y \neq 0$ then by induction hypothesis there is a $(n-2)$-fold Pfister form m such that $g \cong (1, x) \otimes m$ and $g \cong yg$. Using these we have:

$$\begin{array}{rcl} f & = & g \perp ag \cong g \perp ayg \\ & \cong & (1, x) \otimes m \perp (ay, axy) \otimes m \\ & \cong & (1, x, ay, axy) \otimes m \\ & \cong & (1, b, axy, abxy) \otimes m \\ & = & (1, b) \otimes (1, axy) \otimes m \end{array}$$

where we also used $(x, ay) \cong (x + ay, (x + ay)axy)$. □

13. Prime ideals of the Witt ring and orderings

We shall determine minimal prime ideals of the Witt ring $W(K)$ and show that they are related to the orderings of the field K - this relationship becomes one of the most important features of the theory of Witt rings.

Theorem 14. *Let K be a field and let I be a prime ideal of $W(K)$.*

(1) *$W(K)/I$ is isomorphic either to the ring $\mathbb{Z}$ or to the finite field $\mathbb{F}_p$.*
(2) *If $W(K)/I \cong \mathbb{Z}$ then I is a minimal prime ideal.*
(3) *If $W(K)/I \cong \mathbb{F}_p$ then I is a maximal ideal.*

Proof. Let $h : \mathbb{Z} \to W(K)/I$ be the unique homomorphism given by

$$h(z) = z < 1 > + I.$$

Since every similarity class in $W(K)$ can be written as $< a_1, \dots, a_n >$, to show that h is surjective it suffices to prove that for every $< a_1, \dots, a_n > \in W(K)$ there is $z \in \mathbb{Z}$ such that:

$$< a_1, \dots, a_n > + I = z < 1 > + I.$$

If $n = 1$ then for each $a \in U(K)$:

$$(< a > - < 1 >)(< a > + < 1 >) = < a >^2 - < 1 > = 0 \in I,$$

so $< a > - < 1 > \in I$ or $< a > + < 1 > \in I$. In other words if I is a prime ideal and $a \in U(K)$, then:

$$< a > + I = < 1 > + I \quad \text{or} \quad < a > + I = - < 1 > + I.$$

Now we have for any $n \geq 1$:

$$\begin{array}{rcl} < a_1, \dots, a_n > + I & = & < a_1 > + \dots + < a_n > + I \\ & = & \pm < 1 > \pm \dots \pm < 1 > + I = z < 1 > + I, \end{array}$$

which proves surjectivity of h.

Now we will prove (1). Since I is an integral domain, $\ker h$ is a prime ideal in $\mathbb{Z}$, so $\ker h = 0$ or $\ker h = p\mathbb{Z}$ for a prime number p. Thus $W(K)/I \cong \mathbb{Z}$ or $W(K)/I \cong \mathbb{F}_p$.

(3) is obvious since $\mathbb{F}_p$ is a field and it remains to prove (2). Let $W(K)/I \cong \mathbb{Z}$ and let I_1 be a prime ideal in $W(K)$ such that $I_1 \subset I$. Thus the map $f : W(K)/I_1 \to W(K)/I$ given by:

$$f(< U > +I_1) =< U > +I$$

is a ring epimorphism and:

$$\ker f = \{< U > +I_1 :< U >\in I\} = I/I_1.$$

To show that $I_1 = I$ and therefore I is minimal it suffices to show that f is an isomorphism. To do that we will show that there is only one ring homomorphism $W(K)/I_1 \to W(K)/I$ and it is an isomorphism.

Notice that $W(K)/I_1 \cong \mathbb{Z}$. Indeed, I_1 is not maximal since $I_1 \subset I$ amd I is not maximal since $W(K)/I$ is not a field. According to (1) we have $W(K)/I_1 \cong \mathbb{Z}$. On the other hand $W(K)/I \cong \mathbb{Z}$, so that there exists an isomorphism $i : W(K)/I_1 \to W(K)/I$.

Now since $W(K)/I_1 \cong \mathbb{Z}$, every element in $W(K)/I_1$ is an integer multiple of the unit element $< 1 > +I_1$. Every ring homomorphism $W(K)/I_1 \to W(K)/I$ carries $< 1 > +I_1$ onto $< 1 > +I$ and so also $z < 1 > +I_1$ onto $z < 1 > +I$. Thus the homomorphism is uniquely determined on the ring $W(K)/P_1$ and it follows that there is at most one such homomorphism. □

The above theorem shows that the prime ideals of $W(K)$ split into two disjoint classes: the maximal ideals of finite index and the minimal prime ideals of infinite index. We also know that $W(K)$ has a maximal ideal of index 2, namely the fundamental ideal $I(K)$. We shall show that $I(K)$ is the only such ideal.

Lemma 3. *Let K be a field and let I be a prime ideal of $W(K)$.*

(1) *If $2 < 1 > +I = I$ then $I = I(K)$.*
(2) *If $W(K)/I \cong \mathbb{F}_2$ then $I = I(K)$.*

Proof. To say that $2 < 1 > +I = I$ is equivalent to say that $< 1 > +I = - < 1 > +I$. For each $a \in U(K)$:

$$(< a > - < 1 >)(< a > + < 1 >) =< a >^2 - < 1 >= 0 \in I,$$

so $< a > - < 1 >\in I$ or $< a > + < 1 >\in I$. In other words if I is a prime ideal and $a \in U(K)$, then:

$$< a > +I =< 1 > +I \quad \text{or} \quad < a > +I = - < 1 > +I.$$

Hence for each similarity class $< a_1, \dots , a_n >\in W(K)$ we have:

$$\begin{aligned} < a_1, \dots , a_n > +I &= < a_1 > + \dots + < a_n > +I \\ &= \pm < 1 > \pm \dots \pm < 1 > +I = n < 1 > +I \end{aligned}$$

But since $2 < 1 > +I = I$ it follows that:

$$\begin{aligned} < a_1, \dots , a_n >\in I &\Leftrightarrow n < 1 > +I = 0 + I \\ &\Leftrightarrow n \equiv 0(mod 2) \\ &\Leftrightarrow < a_1, \dots , a_n >\in I(K), \end{aligned}$$

so $I = I(K)$ as desired. This proves (1) and to show (2) observe that it $W(K)/I \cong \mathbb{F}_2$ then $2(< 1 > +I) = I$, hence $2 < 1 > +I = I$ and by (1) $I = I(K)$. □

This lemma says that the fundamental ideal is the uniue ideal of the Witt ring of index 2. Now we will exhibit an important relationship between prime ideals of the Witt ring $W(K)$ different from $I(K)$ and the orderings of the field K. The key results are the following two theorems. To prove them we need to introduce the notion of the signature. Let $f = (a_1, \ldots, a_n)$ be a nonsingular quadratic form over a formally real field. Let $s_P^+(a_1, \ldots, a_n)$ be the number of positive entries in the diagonal matrix $(a_1, \ldots, a_n)$ and $s_P^-(a_1, \ldots, a_n)$ - of negative entries. The integer:

$$sgn_P f = s_P^+(a_1, \ldots, a_n) - s_P^-(a_1, \ldots, a_n)$$

is said to be the **signature** of the form f at the ordering P of the field K. The inertia theorem asserts that the signature is well defined and it is easy to check that:

1. If $f \cong g$ then $sgn_P f = sgn_P g$.
2. $sgn_P(f \perp g) = sgn_P f + sgn_P g$.
3. $sgn_P(f \otimes g) = sgn_P f \cdot sgn_P g$.
4. If h is a hyperbolic form then $sgn_P h = 0$.
5. If $f \sim g$ then $sgn_P f = sgn_P g$.

The last properity allows us to extend the notion of signatures on the similarity classes and define:

$$sgn_P < f >= sgn_P f.$$

We will need the following lemma:

Lemma 4. *Let K be a formally real field and let P be an ordering of K.*

1. *$sgn_P : W(K) \to \mathbb{Z}$ is a ring epimorphism.*
2. *$\ker sgn_P$ is a prime ideal.*
3. *$\ker sgn_P$ is generated by the set:*

$$\{< 1, -a >: a \in P\}.$$

Proof. To prove (1) observe that:

$$\begin{aligned} sgn_P(< f > + < g >) &= sgn_P < f \perp g >= sgn_P(f \perp g) \\ &= sgn_P f + sgn_P g \\ &= sgn_P < f > + sgn_P < g > \end{aligned}$$

Similarly we can show that sgn_P preserves multiplication. Surjectivity follows from the fact that $sgn_P(n < 1 >) = n$ for all $n \in \mathbb{Z}$.

Now we have that $W(K)/\ker sgn_P \cong \mathbb{Z}$ and since $\mathbb{Z}$ is an integral domain $\ker sgn_P$ must be prime. To show (3) observe that if $a \in P$ then $sgn_P < 1, -a >= 0$ and so $\{< 1, -a >: a \in P\} \subset \ker sgn_P$. On the other hand if $< f >\in \ker sgn_P$ then $\dim f$ is even and we can write $f \cong (a_1, \ldots, a_{2k})$. Thus we must have:

$$s_P^+(a_1, \ldots, a_{2k}) = s_P^-(a_1, \ldots, a_{2k}) = k.$$

Eventually renumbering the entries we can assume that $a_1, \ldots, a_k$ are all in P and $a_{k+1}, \ldots, a_{2k}$ are in $-P$. Then:

$$\begin{aligned} < f > &= < a_1, a_{k+1} > + < a_2, a_{k+2} > + \ldots + < a_k, a_{2k} > \\ &= < a_1 >< 1, a_1 a_{k+1} > + < a_2 >< 1, a_2 a_{k+2} > + \ldots + \\ &+ < a_k >< 1, a_k a_{2k} > \end{aligned}$$

where $-a_i a_{i+k} \in P$ for $i \in \{1, \ldots, k\}$. □

Now we can state and prove the mentioned theorems:

Theorem 15. *Let K be any field.*

1. *If the Witt ring $W(K)$ has a prime ideal $I \neq I(K)$, then the field K is formally real and the set*
$$P = \{a \in U(K) :< 1, -a >\in I\}$$
is an ordering of the field K.
2. *Let K be a formally real field and let P be an ordering of K. Let I be the ideal of the ring $W(K)$ generated by the set:*
$$\{< 1, -a >\in W(K) : a \in P\}.$$
Then I is a minimal prime ideal of the Witt ring $W(K)$, $I \subset I(K)$ and $I \neq I(K)$.

Proof. In order to show that P is an ordering we first observe that for $a \in U(K)$:
$$a \in P \Leftrightarrow < a > +I =< 1 > +I.$$
Indeed, $a \in P$ iff. $< 1 > - < a >=< 1, -a >\in I$. This gives immediately $P \cdot P \subset P$. We also get easily that $P \cup -P = U(K)$: if $a \in U(K)$ is such that $a \notin P$, then $< a > +I \neq< 1 > +I$. For each $a \in U(K)$:
$$(< a > - < 1 >)(< a > + < 1 >) =< a >^2 - < 1 >= 0 \in I,$$
so $< a > - < 1 >\in I$ or $< a > + < 1 >\in I$. In other words if I is a prime ideal and $a \in U(K)$, then:
$$< a > +I =< 1 > +I \quad \text{or} \quad < a > +I = - < 1 > +I.$$
That means that in our case $< a > +I = - < 1 > +I$. Thus $< -a > +I =< 1 > +I$ showing that $-a \in P$.

It remains to show that $P + P \subset P$, so let $a, b \in P$ and $c = a + b$. Observe that $c = 0$, since otherwise $b = -a$ and from $< a > +I =< 1 > +I$ and $< b > +I =< 1 > +I$ we get:
$$2 < 1 > +I =< a, b > +I =< a, -a > +I = I$$
so, by the previous lemma, $I = I(K)$, contrary to the assumption. Thus $c \neq 0$ and we have:
$$< a, b >=< c, d >$$
where $d = abc$. Here $< d > +I =< a >< b >< c > +I =< c > +I$ and so:
$$< 1, 1 > +I =< a, b > +I =< c, d > +I =< c, c > +I.$$
We want $c \in P$ or in other words $< c > +I =< 1 > +I$. Suppose this is not the case, so that $< c > +I = - < 1 > +I$ and so we have
$$< 1, 1 > +I =< c, c > +I =< -1, -1 > +I.$$
Thus:
$$2 < 1 > \cdot 2 < 1 > +I = 4 < 1 > +I = I.$$
But I is prime, hence it follows that $2 < 1 > +I = I$ and this in turn gives $I = I(K)$ - a contradiction.

To show (2) recall that I is the kernel of the signature homomorphism and a prime ideal, so we have ring isomorphism $W(K)/ \ker sgn_P \cong \mathbb{Z}$. This implies that $\ker sgn_P$ is a minimal prime ideal of the Witt ring. Moreover, I is generated by a subset of the fundamental ideal, so $I \subset I(K)$ and $I \neq I(K)$ since the ideals have distinct indices in $W(K)$. □

Now we will slightly improve the described relationship between ideals and orderings. The set of all prime ideals of a ring R is said to be the **prime spectrum** of the ring R, denoted $SpecR$. We also define the **minimal prime spectrum** of R, denoted $MinSpecR$ as the set of all minimal prime ideals of R.

Theorem 16. *Let K be a formally real field. Then the map*

$$\sigma : X_K \to MinSpecW(K)$$

given by:

$$\sigma(P) = \ker sgn_P$$

is a bijective correspondence between the orderings of the field K and the minimal prime ideals of the Witt ring $W(K)$. The inverse map $\pi : MinSpecW(K) \to X_K$ is given by:

$$\pi(I) = \{a \in U(K) :< 1, -a >\in I\}.$$

Proof. To prove the theorem it is sufficient to show that $\pi \circ \sigma$ and $\sigma \circ \pi$ are identities on X_K and $MinSpecW(K)$. Fix a $P \in X_K$. We have:

$$\begin{aligned}\pi(\sigma(P)) &= \pi(\ker sgn_P) = \{a \in U(K) :< 1, -a >\in \ker sgn_P\} \\ &= \{a \in U(K) : sgn_P < 1, -a >= 0\} \\ &= \{a \in U(K) : a \in P\} = P.\end{aligned}$$

Next fix a $I \in MinSpecW(K)$. Then $\pi(I) = P = \{a \in U(K) :< 1, -a >\in I\}$ and $\sigma(P) = \ker sgn_P$, so we have to check that $I = \ker sgn_P$. Since I is a minimal prime ideal it suffices to show that:

$$\ker sgn_P \subset I.$$

But the ideal $\ker sgn_P$ is generated by the elements $< 1, -a >$, where $a \in P$, and from the definition of P follows that each such binary class belongs to I. □

14. Pfister's local-global principle

We shall describe the elements of special types of Witt ring in terms of information we gathered on the prime ideals and we shall formulate the famous local-global principle due to Pfister. Recall that for an arbitrary ring R $NilR$ denotes the set of all nilpotent elements of the ring R. This set is an ideal which is called the **nilradical** of the ring R. The classical result form the commutative algebra states that:

$$NilR = \bigcap \{I : I \in SpecR\}.$$

Thus in order to describe the nilpotent elements of the Witt ring W(K) we need to know the intersection of all prime ideals in $W(K)$. The results we have already proved describe only the behaviour of the minimal prime ideals. However, observe that every prime ideal of the Witt ring $W(K)$ contains a minimal prime ideal.

Indeed, let I be a prime ideal of $W(K)$. If K is not a real field, then the only prime ideal in $W(K)$ is the fundamental ideal $I(K)$, since any other prime ideal I would induce an ordering, according to the theorem 15. Thus $I(K)$ is the only prime ideal which therefore is minimal itself. If K is formally real with an ordering P and $I = I(K)$, then the ideal generated by the set

$$\{< 1, -a >\in W(K) : a \in P\}$$

is a minimal prime ideal contained in $I(K)$ by theorem 15. Finally, if K is formally real and $I \neq I(K)$, then the set:

$$P = \{a \in U(K) :< 1, -a >\in I\}$$

is an ordering of K and the subset:

$$S = \{< 1, -a >\in W(K) : a \in P\}$$

is contained in I, so that the ideal generated by S is contained in I. By theorem 15 this ideal is minimal and prime, which proves our assertion.

The above observation means, that:

$$\bigcap\{I : I \in MinSpecW(K)\} = \bigcap\{I : I \in SpecW(K)\}.$$

To be more precise we state this as a separate theorem:

Theorem 17. *Let K be an arbitrary field.*

1. $NilW(K) = \bigcap\{I : I \in MinSpecW(K)\}$.
2. *If K is nonreal, then $NilW(K) = I(K)$.*
3. *If K is formally real, then $NilW(K) = \bigcap\{\ker sgn_P : P \in X_K\}$*

For the latter considerations we will need the notion of the total signature. So far the signature sgn_P has been viewed as a function with variable similarity class $< f >$ and fixed ordering P. It is also possible to change this point of view. For each element $< f >$ of the Witt ring $W(K)$ we consider the function $Sgn < f >: X_K \to \mathbb{Z}$ given by:

$$Sgn < f > (P) = sgn_P < f >$$

and call it the **total signature** of the similarity class $< f >$.

We have observed that $sgn_P : W(K) \to \mathbb{Z}$ is a ring epimorphism - we also should view Sgn as a function on the Witt ring, that assigns to each $< f >\in W(K)$ a function $Sgn < f >$. So Sgn is a map from the Witt ring of a real field K into the set $\mathbb{Z}^{X_K}$ of function defined on the set X_K with values in $\mathbb{Z}$. We can give $\mathbb{Z}^{X_K}$ a structure of a ring setting:

$$(S_1 + S_2)(P) = S_1(P) + S_2(P), \qquad (S_1 \cdot S_2)(P) = S_1(P) \cdot S_2(P)$$

for $S_1, S_2 \in \mathbb{Z}^{X_K}$. It is not surprising that the total signature map $Sgn : W(K) \to \mathbb{Z}^{X_K}$ defined by:

$$Sgn(< f >) = Sgn < f >$$

is a ring homomorphism. Indeed, for all $< f >, < g >\in W(K)$ and for $P \in X_K$ we have:

$$\begin{aligned} Sgn(< f > + < g >)(P) &= (Sgn < f \perp g >)(P) = sgn_P < f \perp g > \\ &= sgn_P(f \perp g) = sgn_P f + sgn_P g \\ &= sgn_P < f > + sgn_P < g > \\ &= (Sgn < f >)(P) + (Sgn < g >)(P) \\ &= (Sgn < f > + Sgn < g >)(P) \end{aligned}$$

Similarly one shows that $Sgn(< f > \cdot < g >) = Sgn < f > \cdot Sgn < g >$. The total signature is not, in general, an epimorphism. Neither it is a monomorphism - the kernel $\ker Sgn$ is an ideal of the Witt ring $W(K)$ and it is a nontrivial question how to describe this ideal. The celebrated local-global principle provides a neccesary explanation. Now observe that in the view of the theorem 17 we can write:

$$NilW(K) = \ker Sgn$$

for every formally real field K.

We proceed to the study of the set $TorsW(K)$ of all torsion elements of the Witt ring $W(K)$. It is easy to check that they form an ideal. We will restrict ourselves to the case of formally real fields - it is possible to show that for nonreal fields we have $TorsW(K) = W(K)$. First observe that:

$$TorsW(K) \subset NilW(K).$$

Indeed, let $x \in TorsW(K)$. There is a positive integer n such that $nx = 0 \in W(K)$. Hence for every ordering P:

$$0 = sgn_P 0 = shn_P nx = n \cdot sgn_P x$$

and thus $sgn_P x = 0$, so $x \in \ker sgn_P$ for all P. Since $NilW(K) = \bigcap \{\ker sgn_P : P \in X_K\}$ it follows that $x \in NilW(K)$.

The main result to prove on torsion elements asserts that in the fact $TorsW(K) = NilW(K)$ for formally real fields. The proof of that fact requires a comparison of the Witt rings of a field K and of its extension field E. To begin with let K be a field of characteristic different from 2 and let E be any extension of K. Every nonsingular form f over K can be viewed as a quadratic form over E. If f and g are equivalent quadratic forms over K then there exists a nonsingular matrix P with entries in K such that:

$$f(YD) = g(Y)$$

and f and g are also equivalent as forms over E. Obviously converse is not true - so from now on we shall specify the ground field we have in mind and write $f \equiv_K g$ or $f \equiv_E g$. Hence we have:

$$f \equiv_K g \Rightarrow f \equiv_E g$$

and similarly:

$$f \sim_K g \Rightarrow f \sim_E g.$$

We may extend this "subscript notation" to the similarity classes and notice that the similarity class $< f >_K$ uniquely determines the similarity class $< f >_E$. In view of that we can speak of a map $i_* : W(K) \to W(E)$ given by:

$$i_*(< f >_K) =< f >_E .$$

This mapping turns out to be a ring homomorphism; for nonsingular quadratic forms f and g over K we have:

$$\begin{aligned} i_*(< f >_K + < g >_K) &= i_*(< f \perp g >_K) =< f \perp g >_E \\ &= < f >_E + < g >_E \\ &= i_*(< f >_K) + i_*(< g >_K) \end{aligned}$$

A similar computation for multiplication is left to the reader. This homomorphism is said to be **induced** by the inclusion map $i : K \hookrightarrow E$. This mapping is, in general, neither surjective nor injective. We will focus on determining the kernel of the homomorphism i_* induced by the quadratic extension.

Let $E = K(\sqrt{a})$ where $a \in U(K) \setminus U(K)^2$. Since a is not a square in K but is a square in E, the form $(1, -a)$ is anisotropic over K and hyperbolic over E. Hence:

$$0 \neq < 1, -a >_K \in \ker i_*$$

More generally, for any quadratic form g over K and $b \in U(K)$ the form $(b, -ab) \perp g$ is isotropic over E and $(1, -a) \otimes g$ is hyperbolic over E. We shall show that the converse statements are true.

Theorem 18. *Let $E = K(\sqrt{a})$ where $a \in U(K) \setminus U(K)^2$.*

(1) *Let f be an anisotropic quadratic form over K. Then f is isotropic over E iff. there is an element $b \in U(K)$ such that:*

$$f \equiv_K (b, -ab) \perp g$$

for a quadratic form g over K.

(2) *Let f be an anisotropic quadratic form over K. Then f is hyperbolic over E iff.*

$$f \equiv_K (1, -a) \otimes g$$

for a quadratic form g over K.

(3) *The kernel* $\ker i_*$ *is the principal ideal:*

$$\ker i_* =< 1, -a > \cdot W(K)$$

Proof. (1) Let $f = (a_1, \dots, a_n)$ be anisotropic over K and isotropic over E. Let $x_1, \dots, x_n, y_1, \dots, y_n \in K$ not all equal to zero be such that:

$$a_1(x_1 + y_1\sqrt{a})^2 + \dots + a_n(x_n + y_n\sqrt{a})^2 = 0.$$

Since $a \notin U(K)^2$ it follows that:

$$\sum a_i x_i^2 + a \sum a_i y_i^2 = 0 \text{ and } \sum a_i x_i y_i = 0.$$

Let (U, β) be the $n-$dimensional bilinear space associated with f. It follows that:

$$f(x) + af(y) = 0 \text{ and } \beta(x, y) = 0.$$

As not all x_i, y_i are zero, $x \neq 0$ or $y \neq 0$. But since f is anisotropic over K, $f(x) + af(y) = 0$ implies that $x \neq 0$ and $y \neq 0$.

That means that x and y are anisotropic orthogonal vectors in U. By the Gramm-Schmidt theorem we may pick an orthogonal basis for U starting with vectors x and y, so that a diagonalization of U has the shape:

$$(f(x), f(y), b_3, \dots, b_n).$$

Setting $b = f(y)$ we obtain that $f(x) = -ab$ and:

$$f = (a_1, \dots, a_n) \equiv_K (-ab, b, b_3, \dots, b_n) \equiv (b, -ab) \perp g.$$

(2) Let $f = (a_1, \dots, a_n)$ be anisotropic over K and hyperbolic over E. If $n = 2$ then the result follows from (1), since:

$$f \cong_K (b, -ab) \cong_K (1, -a) \otimes (b).$$

We proceed by induction on n. If f is hyperbolic over E then it is also isotropic over E and by (1):

$$f \cong_K (b, -ab) \perp g$$

where g is anisotropic over K (since f is). Here both f and $(b, -ab)$ are hyperbolic, so from the Witt decomposition it might be inferred that g is also hyperbolic over E. By induction hypothesis $g \cong_K (1, -a) \otimes g'$ and hence:

$$f \cong_K (b, -ab) \perp (1, -a) \otimes g' \cong_K (1, -a) \otimes ((b) \perp g').$$

(3) follows immediately from (2). □

Before we proceed to the main results on torsion elements in Witt rings, we shall prove one more lemma:

Lemma 5. *Let K be a formally real field. For each $x \in NilW(K)$ there exists an integer n such that:*

$$2^n x = 0 \in W(K)$$

Proof. Let $x \in NilW(K)$ and suppose that for all positive integers $2^n x \neq 0$. Let f be such anisotropic form that $x =< f >$. Consider the family:

$$\mathcal{F} = \{E \supset K : 2^n < f >_E \neq 0 \text{ for all positive integers } n\}.$$

Since $K \in \mathcal{F}$, $\mathcal{F} \neq \emptyset$. Let $\mathcal{C} = \{E_j : j \in J\}$ be a chain and let $E = \bigcup\{E_j : j \in J\}$. As a sum of a family of fields, E is a field and it belongs to $\mathcal{F}$. Indeed, suppose that for some n $2^n < f >_E = 0 \in W(K)$. Denote:

$$2^n \times f = \underbrace{f \perp \ldots \perp f}_{2^n}$$

Thus the quadratic form $2^n \times f$ is hyperbolic over the field E, so we have the equivalence $2^n \times f \cong_E h$, where $h = (1, -1) \perp \ldots \perp (1, -1)$ is the hyperbolic form of appropriate dimension. Hence for some nonsingular matrix D with entries in E we have $(2^n \times f)(YD) = h(Y)$. Every entry of D belongs to some field E_j and since $\mathcal{C}$ is a chain, we may pick an i such that all entries are contained in the field E_i. That means that $2^n \times f$ is hyperbolic over E_i, contrary to $E_i \in \mathcal{F}$.

We have checked that all hypotheses of Zorn Lemma are satisfied, so we may pick a maximal element F of the family $\mathcal{F}$. Observe that F is formally real. Indeed, suppose that F is nonreal and denote by $s(F)$ the smallest number n such that -1 is a sum on n squares in F. Notice that there exists an integer m such that $s(K) = 2^m$. For if suppose that $s(F) > 1$ and $s(F)$ is not a power of 2. Then there is a positive integer m such that:

$$2^m < s(K) < 2^{m+1}.$$

Thus we can write $1 + A + B = 0$, where A is the sum of less than 2^m squares and B is the sum of 2^m squares. Multiplying by $1 + A$ yields:

$$(1 + A)^2 + (1 + A)B = 0.$$

Since $s(F) > 2^m$ here $1 + A \neq 0$, hence also $B \neq 0$ and it follows that $1 + A \in D_F(2^m \times (1))$ and $B \in D_F(2^m \times (1))$. But $2^m \times (1)$ is a Pfister form, so $D_F(2^m \times (1))$ is a group and therefore $(1 + A)B \in D_F(2^m \times (1))$. Now since

$$-1 = \frac{(1 + A)B}{(1 + A)^2}$$

which means that -1 is the sum of 2^m squares in F, contrary to $2^m < s(F)$. Thus we proved that $s(F) = 2^m$.

Now observe that the order of the unit element $< 1 >$ in the additive group of $W(K)$ equals $2s(F)$. Indeed, since $s(F) = 2^m$ the form $s(F) \times (1) = 2^m \times (1)$ is a Pfister form and thus $D_F(s(F) \times (1)) = G_F(s(F) \times (1))$. By definition of $s(F)$, $-1 \in D_F(s(F) \times (1))$ and hence:

$$2^m \times (1) \cong (-1)(2^m \times (1)) = 2^m \times (-1)$$

and thus:

$$2^m \times (1) \perp 2^m \times (1) \cong 2^m \times (1) \perp 2^m \times (-1).$$

Since $2^m \times (1) \perp 2^m \times (1)$ is the $(m+1)$-fold Pfister form $2^{m+1} \times (1)$ and $2^m \times (1) \perp 2^m \times (-1)$ is equivalent to the direct orthogonal sum of 2^m binary hyperbolic forms $(1, -1)$, we have the following equality in the Witt ring:

$$2^{m+1} \times < 1 >= 0.$$

Therefore the additive order of $< 1 >$ is a divisor of $2^{m+1} = 2s(F)$ and it remains to show that $s(F) \times < 1 > \neq 0$ in $W(F)$. Contrary to this, assume $s(F) \times < 1 >= 0$. Thus we may pick some $x_1, \ldots, x_s \in K$ not all equal to zero such that:

$$x_1^2 + \ldots + x_s^2 = 0.$$

We may assume that $x_s \neq 0$. Then we get:

$$(x_1/x_s)^2 + \ldots + (x_{s-1}/x_s)^2 = -1$$

which is a contradiction. Therefore the order of $< 1 >$ is $2s(F)$.

That means that every element of the Witt ring $W(F)$ is torsion and has a order dividing $2s(F)$, hence a power of two - contrary to the property defining the field F. Thus we proved that F is formally real.

Now we shall show that F has at least four square classes. Notice that

$$(aU(F)^2)^2 = a^2 U(F)^2 = U(F)^2,$$

so the order of every element in $U(F)/U(F)^2$ is 1 or 2 and in the case when $U(F)/U(F)^2$ is finite that means that the order of $U(F)/U(F)^2$ is even. On the other hand since F is formally real, $U(F)/U(F)^2$ is nontrivial. Hence it suffices to show that $U(F)/U(F)^2$ has order different from 2. Otherwise F has two square classes. Then $P = U(F)^2$ is the unique ordering of F and $\ker sgn_P$ is the zero ideal, since for each $a \in P = U(F)^2$ we have $< 1, -a >= 0$. Thus the epimorphism $sgn_P : W(F) \to \mathbb{Z}$ becomes an isomorphism and it follows that $W(F)$ has no nonzero nilpotent elements contradicting the fact that $x =< f >$ is a nilpotent in $W(K)$, hence also in $W(F)$.

Since $|U(F)/U(F)^2| \geq 4$ we may choose an element $a \in U(F)$ which is neither square nor negative sqare. Then also -1 is not a square and

$$F_1 = F(\sqrt{a}) \text{ and } F_2 = F(\sqrt{-a})$$

are quadratic extensions of F. By the maximality of F, $F_1, F_2 \notin \mathcal{F}$ and there exist positive integers n_1, n_2 such that:

$$2^{n_1} < f >_{F_1} = 0 \text{ and } 2^{n_2} < f >_{F_2} = 0.$$

Taking $n = n_1 + n_2$ we get:

$$2^n < f >_{F_1} = 0 \text{ and } 2^n < f >_{F_2} = 0.$$

By theorem 18 there are forms g_1 and g_2 over F such that:

$$2^n < f >_F =< 1, -a >_F < g_1 >_F \; 2^n < f >_F < g_2 >_F$$

Multiplying the above equalities by $< -a >_F$ and $< a >_F$, respectively, and using the fact that $< -a > \cdot < 1, -a >=< 1, -a >$ and $< a > \cdot < 1, a >=< 1, a >$ we get:

$$< -a >_F 2^n < f >_F = 2^n < f >_F \text{ and } < a >_F 2^n < f >_F = 2^n < f >_F$$

and thus:

$$< -a >_F 2^n < f >_F =< a >_F 2^n < f >_F$$

hence multiplying by $< a >_F$:

$$< -1 > 2^n < f >_F = 2^n < f >_F$$

and finally:

$$2^{n+1} < f >_F = 0$$

which contradicts the defining property of the field F. □

We have already observed that $TorsW(K) \subset NilW(K)$. The above lemma shows that also $TorsW(K) \supset NilW(K)$ - in the fact we have proved something more, namely every element has a 2-power order. Anyway, the following important equality holds:

$$TorsW(K) = NilW(K)$$

Combining with the previous remarks we get:

$$TorsW(K) = \bigcap\{\ker sgn_P : P \in X_K\}$$

Now let K be a formally real field with fixed ordering P, let f be an anisotropic quadratic form over K. Let K_P denote a real closure inducing the ordering P on K. Then $U(K_P)^2$ is the unique ordering of K_P and $\ker sgn_P$ is the zero ideal, since for each $a \in U(K_P)^2$ we have $< 1, -a >= 0$. Thus the epimorphism $sgn_{U(K_P)^2} : W(K_P) \to \mathbb{Z}$ becomes an isomorphism. Hence:

$$< f >_{K_P} = 0 \Leftrightarrow sgn_{U(K_P)^2} f = 0.$$

But since P is induced from the unique ordering $U(K_P)^2$ in K_P and f is the form over K:

$$sgn_{U(K_P)^2} f = sgn_P f$$

hence:

$$< f >_{K_P} = 0 \Leftrightarrow sgn_P f = 0.$$

Now since we can change P arbitrary, in view of the equality

$$TorsW(K) = \bigcap\{\ker sgn_P : P \in X_K\}$$

we have:

$$< f >_{K_P} = 0, P \in X_K \Leftrightarrow < f > \in TorsW(K).$$

This result is known as the famous **Pfister's Local - Global Principle**, first proved in 1966. Since $NilW(K) = \ker Sgn$ and $TorsW(K) = NilW(K)$ we have another version of this principle, which describes all torsion elements of $W(K)$ in terms of total signature:

$$TorsW(K) = \ker Sgn.$$

15. T-forms and Pfister T-forms

From now on our main goal is to set up a theory of quadratic forms "relative" to a preordering T (or "reduced" modulo T). We will restrict ourselves only to the case of field whose characteristic is different from two. This theory will lead to a relative Witt ring denoted $W_T(K)$, which shares many of the properties of the ordinary Witt ring $W(K)$. Actually, $W_T(K)$ turns out to be isomorphic to a certain quotient ring of $W(K)$, namely:

$$W(K)/I$$

where I is the ideal generated by the set:

$$\{<1,-a>\in W(K) : a\in T\}.$$

In the case when K is formally real and T is the sum of squares, this ideal clearly corresponds with intersection of all minimal prime ideals (since each minimal prime ideal is generated by the set $\{<1,-a>\in W(K) : a\in P\}$, where P is some ordering of K) and - as $NilW(K)=\bigcap\{I : I\in MinSpecW(K)\}$ - we have the following alternative description of the reduced Witt ring of a formally real field:

$$W(K)/NilW(K).$$

Therefore one could take this to be the definition of $W_T(K)$. However, such definition appears in some kind of "magic" way and obscures the fact that there is a reasonable quadratic form theory associated with $W_T(K)$. For better motivation we shall first develop the relevant "reduced" quadratic form theory relative to T and then construct the Witt ring $W_T(K)$ from it.

Let T be a fixed preordering in K, that is such a set that $K^2\subset T$, $T+T\subset T$, $T\cdot T\subset T$ and $T\subsetneq K$. By a **T-form** of dimension n we mean a formal expression

$$f=(a_1,\ldots,a_n)_T$$

where $a_1,\ldots,a)n\in U(K)$. For such a $T-$form f and any ordering X_T we define the **P-signature** of f in the following way. Let $s_P^+(a_1,\ldots,a_n)$ be the number of those entries in the sequence $a_1,\ldots,a_n$ that belong to P and $s_P^-(a_1,\ldots,a_n)$ be the number of those entries in the sequence $a_1,\ldots,a_n$ that belong to $-P$ The integer:

$$sgn_P f=s_P^+(a_1,\ldots,a_n)-s_P^-(a_1,\ldots,a_n)$$

is said to be the $P-$signature of the form f. Clearly $sgn_P f\equiv\dim f(mod 2)$.

We can define the **direct orthogonal sum** and the **tensor product** of T-forms as we did for ordinary forms, namely:

$$(a_1,\ldots,a_n)_T\perp(b_1,\ldots,b_m)_T=(a_1,\ldots,a_n,b_1,\ldots,b_m)_T$$

and

$$(a_1,\ldots,a_n)_T\otimes(b_1,\ldots,b_m)_T=(a_1b_1,\ldots,a_1b_m,\ldots,a_nb_1,\ldots,a_nb_m)_T.$$

A straightforward calculation gives:

$$sgn_P(f\perp g)=sgn_P f+sgn_P g$$

and

$$sgn_P(f\otimes g)=sgn_P f\cdot sgn_P g.$$

Next, we say that two T-forms f and g are **T-isometric** (in symbols $f\cong_T g$) if f and g have the same dimensions and the same signatures with respect to any $P\in X_T$. Notice that this definiton also agrees with the definition of equivalence of quadratic forms or - equivalently - isometry of bilinear spaces: it can be proved (see [3] pages 104-105) that two bilinear spaces over the field of real numbers $\mathbb{R}$ are isometric iff. they have the same dimensions and signatures. This result remains true if we replace the field $\mathbb{R}$ with any field with two square classes (see [8] pages 108-109).

As was the case with ordinary quadratic forms, we can easily check that:

$$(a_1, \ldots, a_n)_T \cong_T (a_1t_1, ldots, a_nt_n)$$

for $t_1, \ldots, t_n \in U(T)$ and

$$(a, b)_T \cong_T (a + b, ab(a + b))_T$$

provided $a + b \neq 0$. Next, the binary hyperbolic T-form $(1, -1)_T$ is called **T-hyperbolic plane** and the direct orthogonal sum of n T-hyperbolic planes is called the **hyperbolic space**. Clearly a T-form is hyperbolic iff. its signature with respect to any $P \in X_T$ is equal to zero. A T-form is said to be **T-isotropic** if there exist $t_1, \ldots, t_n \in T$ not all zero such that:

$$a_1t_1 + \ldots + a_nt_n = 0.$$

To illustrate this notion consider the case of a formally real field with preordering $T = \sum K^2$ being the set of sums of quares. To say that $(a_1, \ldots, a_n)_{\sum K^2}$ is $\sum K^2$-isotropic means that there are some x_{ij} not all zero such that:

$$a_1(x_{11}^2 + \ldots + x_{1r_1}^2) + \ldots + a_n(x_{n1}^2 + \ldots + x_{nr_n}^2) = 0.$$

Taking $r = \max\{r_1, \ldots, r_n\}$ and eventually substituting $x_{ij} = 0$ for some i, j we get:

$$(a_1x_{11} + \ldots, a_nx_{n1}) + \ldots + (a_1x_{1r} + \ldots + a_nx_{nr}) = 0$$

which means that the quadratic form

$$r(a_1, \ldots, a_n) = (a_1, \ldots, a_n) \perp \ldots \perp (a_1, \ldots, a_n) = (a_1, \ldots, a_n, \ldots, a_1, \ldots, a_n)$$

is isotropic. It this is the case we say that the quadratic form $(a_1, \ldots, a_n)$ is **weakly isotropic**. Obviously if K is pythagorean, that is $\sum K^2 = K^2$, this will imply that $(a_1, \ldots, a_n)$ is isotropic.

We define the **set of values** of the T-form $f = (a_1, \ldots, a_n)_T$ to be:

$$D_T(f) = \{a_1t_1 + \ldots + a_nt_n \neq 0 : t_1, \ldots, t_n \in T\}.$$

If an element $b \in U(K)$ belongs to $D_T(f)$ we say that b is **represented** by f. Observe that, since $T + T \subset T$, $T \cdot T \subset T$ and $K^2 \subset T$:

$$D_T((t_1, \ldots, t_r) \otimes f) = D_T(f) = D_T(rf)$$

for any $t_1, \ldots, t_r \in T$. This follows that for any natural number r:

$$f \text{ is } T\text{-isotropic } \Leftrightarrow rf \text{ is } T\text{-isotropic .}$$

We can also relate the notion of T-isotropy to the usual notion of isotropy as follows:

$$f \text{ is } T\text{-isotropic } \Leftrightarrow \bigvee_{t_1,\ldots,t_r \in U(T)} < t_1, \ldots, t_r > \otimes f \text{ is isotropic.}$$

The next result, which is considerably deeper, gives the analog of this for the notion of hyperbolocity:

Theorem 19. *For any T-form f the following three conditions are equivalent:*

1. *f is T-hyperbolic;*

(2) $<< t_1, \dots, t_r >> \cdot < f >= 0$ *in* $W(K)$ *for some* $t_1, \dots, t_r \in U(T)$;
(3) $< t_1, \dots, t_r > \cdot < f >= 0$ *in* $W(K)$ *for some* $t_1, \dots, t_r \in U(T)$.

Proof. (2) ⇒ (3) and (3) ⇒ (1) are obvious. In order to prove (1) ⇒ (2) observe that:

$$2^n < a_1, \dots, a_n >= \sum_e < e_1, \dots, e_n ><< e_1a_1, \dots, e_na_n >>\in W(K)$$

where $e = (e_1, \dots, e_n)$ ranges over all such n-tuples that $e_i = \pm 1$. To prove the above identity we use induction by n. Notice that $e_i << e_ia_i >>= a_i << e_ia_i >>$, so $< e_1, \dots, e_n ><< e_1a_1, \dots, e_na_n >>=< a_1, \dots, a_n ><< e_1a_1, \dots, e_na_n >>$ and therefore it suffices to show that:

$$\sum_e << e_1a_1, \dots, e_na_n >>= 2^n < 1 >\in W(K).$$

For $n = 1$ we have $<< a_1 >> + << -a_1 >>= 2 < 1 >\in W(K)$. For $n > 1$ denote $e' = (e_1, \dots, e_{n-1})$ and write:

$$\begin{aligned}\sum_e << e_1a_1, \dots, e_na_n >>=& \sum_{e'} << e_1a_1, \dots, e_{n-1}a_{n-1}, a_n >>\\ + & \sum_{e'} << e_1a_1, \dots, e_{n-1}a_{n-1}, -a_n >>\\ = & \sum_{e'} << e_1a_1, \dots, e_{n-1}a_{n-1} >> (<< a_n >> + << -a_n >>)\\ = & 2\sum_{e'} << e_1a_1, \dots, e_{n-1}a_{n-1} >>= 2^n < 1 >\in W(K)\end{aligned}$$

Now assume that $f = (a_1, \dots, a_n)_T$ is T-hyperbolic. We shall try to apply the above formula. Fix an n-tuple e and consider two cases. First, assume that the preordering $T[e_1a_1, \dots, e_na_n]$ generated over T by $\{e_1a_1, \dots, e_na_n\}$ is different from K. Then there exists an ordering $P \supset T[e_1a_1, \dots, e_na_n]$. For this P we have:

$$e_i \in P \Leftrightarrow a_i \in P$$

and so:

$$sgn_P < e_1, \dots, e_n >= sgn_P f = 0.$$

Thus half of the $e_i's$ are 1's and the other half are -1's, which gives $(e_1, \dots, e_n) = 0 \in W(K)$ so we can drop the corresponding term on the right side of the above formula.

If $T[e_1a_1, \dots, e_na_n] = K$ then note that

$$T[e_1a_1, \dots, e_na_n] \setminus \{0\} = D_T(((e_1a_1, \dots, e_na_n))_T).$$

In particular $-1 \in D_T(((e_1a_1, \dots, e_na_n))_T)$ which implies that $2((e_1a_1, \dots, e_na_n))_T$ is T-isotropic. By the previous remarks there exist $t'_1, \dots, t'_m \in U(T)$ such that

$$(t'_1, \dots, t'_m)((e_1a_1, \dots, e_na_n))$$

is isotropic and so is:

$$((t'_1, \dots, t'_m, e_1a_1, \dots, e_na_n))$$

which as a Pfister form is also hyperbolic. Therefore, multiplying both sides of our main equality by a suitable Pfister form $<< t_1, \dots, t_r >>$ we get:

$$<< t_1, \dots, t_r >> \cdot < f >= 0 \in W(K)$$

□

Observe that hyperbolicity implies isotropy, so if a T-form f is T-hyperbolic, then it is also T-isotropic. Converse is true for Pfister forms; let a T-form $f = ((b_1, \ldots, b_n))_T$ be T-isotropic. Thus for some $t_i, t_{ij} \in T$ not all zero:

$$t_0 + t_1 b_1 + \ldots + t_n b_n + t_{12} b_1 b_2 + \ldots = 0.$$

Let $P \in X_T$. The equation above implies that the $b_j's$ cannot all be in P, say $b_1 \in -P$. Then

$$agn_P f = sgn_P(1, b_1)_T sgn_P((b_2, \ldots, b_n))_T = 0$$

so f is T-hyperbolic.

16. Witt ring of T-forms

We start our construction of the Witt ring of T-forms with the following "representation" criterion, analogous to the theorem 9:

Theorem 20. *Let $f = (a_1, \ldots, a_n)_T$ be a T-form. Then $c \in D_T(f)$ iff. there are $b_2, \ldots, b_n \in U(K)$ such that:*

$$f \cong_T (c, b_2, \ldots, b_n)$$

Proof. Let $c \in D_T(f)$, say $c = a_1 t_1 + \ldots + a_n t_n$. Without loss of generality we may assume that $a_1 t_1 + \ldots + a_r t_r \neq 0$ for all r (otherwise we can work with $(a_{r+1} t_{r+1} + \ldots + a_n t_n)_T$). We have:

$$\begin{aligned}
(a_1, \ldots, a_n)_T &\cong_T (a_1, a_2)_T \perp (a_3, \ldots, a_n)_T \\
&\cong_T (t_1 a_1, t_2 a_2)_T \perp (a_3, \ldots, a_n)_T \\
&\cong_T (t_1 a_1 + t_2 a_2, t_1 a_1 t_2 a_2 (t_1 a_1 + t_2 a_2))_T \perp (a_3, \ldots, a_n)_T \\
&\cong_T (t_1 a_1 + t_2 a_2, a_3, \ldots, a_n, t_1 a_1 t_2 a_2 (t_1 a_1 + t_2 a_2))_T \\
&\cong_T \ldots \cong_T (a_1 t_1 + \ldots + a_n t_n, b_2, \ldots, b_n)_T
\end{aligned}$$

Conversely, let $t \cong_T (c, b_2, \ldots, b_n)_T$. Then $(a_1, \ldots, a_n, -c, -b_2, \ldots, -b_n)_T$ is T-hyperbolic and by theorem 19:

$$< t_1, \ldots, t_r >< a_1, \ldots, a_n >=< t_1, \ldots, t_r >< c, b_2, \ldots, b_n >\in W(K)$$

for some $t_1, \ldots, t_r \in T$. Since the left- and right hand sides above are forms of equal dimensions, they must be equivalent as ordinary forms. In particular $t_1 c \in D_T((t_1, \ldots, t_r)_T f) = D_T(f)$, so $c \in t_1^{-1} D_T(f) = D_T(f)$. □

As a corollary we have the following:

Theorem 21. *For any T-form f the following statements are equivalent:*

(1) *f is T-isotropic,*
(2) *$f \cong_T (1, -1)_T \perp g$ for some T-form g,*
(3) *$D_T(f) = U(K)$,*
(5) *there exists an element $b \in U(K)$ such that both $\pm b \in D_T(f)$.*

Proof. (2) $\Rightarrow$ (3) $\Rightarrow$ (4) are clear, we shall show (4) $\Rightarrow$ (1). Let $\pm b \in D_T(f)$. This follows that $2f$ is T-isotropic and since $D_T(f) = D_T(rf)$ we have that f is isotropic itself.

(1) $\Rightarrow$ (2). Let $f = (a_1, \ldots, a_n)_T$ be T-isotropic, that is $a_1t_1 + \ldots + a_nt_n = 0$ where not all $t_i \in T$ are zero, say $t_1 \neq 0$. Then:

$$-a_1t_1 = a_2t_2 + \ldots + a_nt_n \in D_T(a_2, \ldots, a_n)$$

and by the representation criterion

$$(a_2, \ldots, a_n)_T \cong_T (-a_1t_1) \perp g$$

for some T-form g and therefore $f \cong_T (a_1t_1, -a_1t_1)_T \perp g \cong_T (1, -1)_T \perp g$. □

Observe that conditions (1) and (2) are analogous to those for quadratic forms, but (3) and (4) are special features in the "mod T" theory. Another important corollary is the following "Witt decomposition" theorem:

Theorem 22. *For any T-form f there exist uniquely (up to isometry) determined T-forms g and h such that $f \cong_T g \perp h$, where g is T-anisotropic and h is hyperbolic.*

Proof. Existence: if f is T-anisotropic, there is nothing to prove. Assume that $f = (a_1, \ldots, a_n)_T$ is isotropic. By the previous theorem $f \cong_T (1, -1)_T \perp g$ for some T-form g'. Now we proceed by induction - if g' is T-anisotropic, then we are done - otherwise we decompose g' as $g' \cong_T (1, -1)_T \perp g''$ and finally we end up with the decomposition $f \cong_T h \perp g$, where g is T-anisotropic and h is T-hyperbolic.

Uniqueness: as was the case with the existence part, we "copy" the proof from the "normal" theory. Note that the Witt cancellation theorem, which was the key result used in the proof in "normal" theory, now is an immediate consequence of the definitions we are using. □

Now we can translate the whole theory of the Witt ring in the "normal" case into the language of T-forms. We say that two T-forms f and g are T-**similar**, denoted $f \sim_T g$, if there exist T-hyperbolic T-forms h_1 and h_2 such that:

$$h_1 \perp f \cong_T h_2 \perp g.$$

It is easy to verify, that the similarity relation is indeed an equivalence relation. Clearly the zero class $< 0 >_T$ consists of all hyperbolic T-forms and if $f \cong_T g$ then $f \sim_T g$, but the converse is not true unless f and g are T-anisotropic (that follows from the Witt decomposition theorem). If $f \cong_T h \perp g$ is the Witt decomposition, then $f \sim_T g$, and thus every similarity class of T-forms contains an anisotropic form. On the set $W_T(K)$ of all T-similarity classes we define addition:

$$< f >_T + < g >_T = < f \perp g >_T$$

and multiplication:

$$< f >_T \cdot < g >_T = < f \otimes g >_T$$

and therefore we make $W_T(K)$ into a ring, which is said to be the **Witt ring of** T-**forms** over the field K. In order to verify that $(W_T(K), +, \cdot, < 0 >_T, < 1 >_T)$ is indeed a commutative ring with identity, we proceed in the similar manner as was the case with "normal" theory, extensively using the Witt decomposition theorem.

There are, however, a few differences that distinguish $W(K)$ from $W_T(K)$. First of all, for any T-form f and an integer $r \geq 1$ f is T-hyperbolic iff. rf is T-hyperbolic. The implication ($\Rightarrow$) is clear, to prove the converse assume that rf is hyperbolic for some $r \geq 1$. From theorem 19 we conclude that $< t_1, \dots, t_s >< rf >= 0 \in W(K)$. But:

$$\begin{aligned} < t_1, \dots, t_s >< rf > &= < t_1, \dots, t_s > (\underbrace{< f > + \dots + < f >}_{r}) = \\ &= < t_1, \dots, t_s > (< \underbrace{1, \dots, 1}_{r} >< f >) = \\ &= (< t_1, \dots, t_s >< \underbrace{1, \dots, 1}_{r} >) < f > \end{aligned}$$

and since $1 = 1^2$, $U(K)^2 \subset T$ and $T \cdot T \subset T$ that follows that $< t'_1, \dots, t'_{s'} >< f >= 0 \in W(K)$, so that f is hyperbolic. That means, in particular, that $W_T(K)$ is always torson-free as an Abelian group. However, we know that $W(K)$ is never torsion-free, unless K is formally real and pythagorean.

Now consider the mapping $\Phi : W(K) \to W_T(K)$ given by:

$$\Phi(< a_1, \dots, a_n >) =< a_1, \dots, a_n >_T .$$

It is easy to check that Φ is a ring epimorphism. We define the **fundamental ideal** $I_T(K)$ as an image $\Phi(I(K))$ of the fundamental ideal of similarity classes of even-dimensional forms. Thus $I_T(K)$ becomes the ideal of T-similarity classes of even-dimensional T-forms. Again, the $n-$th power $I^n_T(K)$ is additively generated by the T-smilarity classes of the n-fold T-Pfister forms $<< a_1, \dots, a_n >>_T$:

$$I^n_T(K) =< \{<< a_1, \dots, a_n >>_T : a_i \in U(K)\} > .$$

In the same way as in the absolute theory the isomorphism:

$$W_T(K)/I_T(K) \cong \mathbb{Z}/2/Z$$

can be checked. We can also introduce the notion of the **determinant** of the T-form class f:

$$\det f = a_1 \cdot \dots \cdot a_n \cdot U(T) \in U(K)/U(T)$$

where $f = (a_1, \dots, a_n)_T$. This determinant is defined uniquely up to the isometry of T-forms. Indeed, let $f = (a_1, \dots, a_n)_T \cong_T (b_1, \dots, b_n)_T = g$ and let $c = a_1 \dots a_n$, $d = b_1 \dots b_n$. It suffices to show that $cd \in U(T)$. Since the preordering T is the intersection of all orderings P extending T, it suffices to show that $sgn_P c = sgn_P d$ for every $P \in X_T$. Fix $P \in X_T$ and let $a_1, \dots, a_r \in -U(P)$, $a_{r+1}, \dots, a_n \in U(P)$, $b_1, \dots, b_s \in -U(P)$, $b_{s+1}, \dots, b_n \in U(P)$. Since

$$n - 2r = sgn_P f = sgn_P g = n - 2s$$

we have that $r = s$ and hence $sgn_P c = (-1)^r = (-1)^s = sgn_P d$.

Having well defined determinant, we can define the **discriminant** of T-form and therefore we are able to prove the second important isomorphism:

$$I_T(K)/I^2_T(K) \cong U(K)/U(T)$$

using the same techniques as in the absolute thoery.

17. Pfister's local-global principle for T-forms

In the set X_K of all orderings of the field K we define the **Harrison sets**:

$$H(a) = \{P \in X_K : a \in P\}.$$

We introduce the topology in X_K by using Harrison sets as a subbasis. It is relatively easy to show that X_K is a Boolean space, that is compact, Hausdorff and totally disconnected. It turns out that for every Boolean space it is possible to pick a field K such that the given space is homeomorphic to X_K. For proof see [7] pages 62 - 69.

Observe that the set X_T of all orderings extending the given preordering T is closed in X_K. Indeed, let $P \in X_K \setminus X_T$ and fix an element $a \in T \setminus P$. Then $-a \in P$ and $H(-a)$ is a neighbourhood of P disjoint from X_T. Thus $X_K \setminus X_T$ is open and so X_T is closed. In particular, X_T is Boolean itself, i.e. Hausdorff, compact and totally disconnected. A subbasis for the topology on X_T is given by the relative Harrison sets:

$$H_T(a) = \{P \in X_T : a \in P\}.$$

Now consider the set of integers $\mathbb{Z}$ with the discrete topology. Denote by $C(X_T, \mathbb{Z})$ the ring of continuous functions from X_T to $\mathbb{Z}$ with addition and multiplication defined pointwise:

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

and

$$(\phi \cdot \psi)(P) = \phi(P) \cdot \psi(P).$$

Since X_T is compact, the image of any continuous function $\phi \in C(X_T, \mathbb{Z})$ is a finite set and the family:

$$\{\phi^{-1}(\{r\}) : r \in \phi(X_T)\}$$

forms a finite partition of X_T into clopen sets. Conversely, let $C_1, \ldots, C_k$ be a finite partition of X_T. We can define continuous function $\phi \in C(X_T, \mathbb{Z})$ by:

$$\phi(P) = n_1 \cdot \chi_{C_1} + \ldots + n_k \cdot \chi_{C_k}$$

for arbitrary integers $n_1, \ldots, n_k$. Therefore, as an Abelian group $C(X_T, \mathbb{Z})$ is additively generated by the characteristic function χ_A of the clopen sets $A \in X_T$.

Now let $< f >_T \in W_T(K)$ be a T-similarity class. As was the case with absolute theory, we can define the **total signature** $Sgn_T < f >_T$: $X_T \to \mathbb{Z}$ by:

$$Sgn_T < f >_T (P) = sgn_P f.$$

Observe that if f is a unary form $f = (a)$, then $Sgn_T < f >_T (X_T) \subset \{1, -1\}$. Moreover:

$$Sgn_T < f >_T^{-1} (\{1\}) = \{P \in X_T : a \in P\} = H_T(a)$$

and

$$Sgn_T < f >_T^{-1} (\{-1\}) = \{P \in X_T : a \in -P\} = H_T(-a)$$

so $Sgn_T < f >_T$ is continuous. It is easy to check that:

$$Sgn_T < f \perp g >_T = Sgn_T < f >_T + Sgn_T < g >_T$$

and

$$Sgn_T < f \otimes g >_T = Sgn_T < f >_T \cdot Sgn_T < g >_T,$$

so that the mapping $Sgn_T : W_T(K) \to C(X_T, \mathbb{Z})$ given by:

$$Sgn_T(< f >_T) = Sgn_T < f >_T$$

is well-defined ring homomorphism. We know that in the absolute theory the mapping Sgn was - in general - neither an epimorphism nor a monomorphism and that question of describing the kernel of Sgn was far from trivial. We proved that $\ker Sgn$ was equal to the set of nilpotent elements of $W(K)$ and the celebrated Pfister theorem stated that $\ker Sgn = NilW(K) = TorsW(K)$. However, this is not the case in the "modulo T" theory. We already know that $W_T(K)$ is always torsion-free, so that the question of describing torsion elements is out of our interest. Not surprisingly, Sgn_T tuns out to be a monomorphism. Indeed, if $Sgn_T(< f >_T) = 0$, then $sgn_P f = 0$ for all $P \in X_T$, so that f is hyperbolic and therefore $< f >_T = 0 \in W_T(K)$.

We shall slightly modify the "local-global problem" for the "modulo T" theory. Consider the diagram:

$$\begin{tikzcd}
 & W(K) \arrow[dl, "\Phi"'] \arrow[dr, "\widehat{Sgn_T}"] & \\
W_T(X) \arrow[rr, "Sgn_T"] & & C(X_T, \mathbb{Z})
\end{tikzcd}$$

where $\Phi : W(K) \to W_T(K)$ is given by:

$$\Phi(< a_1, \ldots, a_n >) = < a_1, \ldots, a_n >_T$$

and $\widehat{Sgn_T} = Sgn_T \circ \Phi$. The local-global principle "modulo T" by Pfister, Becker, Köpping, Bröcker and Scharlau states as follows:

Theorem 23. $\ker \Phi = \ker \widehat{Sgn_T} = < \{< 1, -t >: t \in T\} > \subset W(K)$

Proof. Since Sgn_T is injective, $\ker \Phi = \ker \widehat{Sgn_T}$. Clearly $sgn_P < 1, -t > = 0$ for all $P \in X_T$, so $\ker \widehat{Sgn_T} \supset < \{< 1, -t >: t \in T\} >$. Conversely, let $< f > = < a_1, \ldots, a_n > \in \ker \widehat{Sgn_T}$. Denote $I = < \{< 1, -t >: t \in T\} >$. If $n = 0$ there is nothing to prove. It $n > 0$, we proceed by induction. f viewed as a T-form is T-hyperbolic and hence T-isotropic. Thus for some $t_i \in T$ not all zero:

$$t_1 a_1 + \ldots + t_n a_n = 0.$$

Let:

$$a_i' = \begin{cases} a_i, & \text{if } t_i = 0 \\ t_i a_i, & \text{if } t_i \neq 0 \end{cases}$$

and consider $f' = (a_1', \ldots, a_n')$. In $W(K)$ we have:

$$< f > - < f' > = \sum_{t_i \neq 0} a_i < 1, -t_i > \in I]$$

so it suffices to show that $< f' > \in I$. But since f' is isotropic, we have $f' \equiv (1, -1) \perp f''$ for some $(n-2)$-dimensional form f''. Clearly $\widehat{Sgn_T}(< f'' >) = \widehat{Sgn_T}(< f' >) = \widehat{Sgn_T}(f) = 0$, so by the inductive hypothesis we have $f'' \in I$ and hence $f \in I$. □

Consider the case when $T = \sum K^2$ in a formally real field K. Then $X_T = X_K$ and the theorem above gives:

$$\begin{aligned}\ker Sgn &= <\{<1,-a>: a \in \sum K^2\}> \\ &= \bigcap_{P \in X_K} <\{<1,-a>: a \in P\}> \\ &= \bigcap\{kersgn_P : P \in X_K\}\end{aligned}$$

and we get back the classical Pfister local-global principle. But we also know that $\bigcap\{kersgn_P : P \in X_K\} = TorsW(K)$ and that Φ is an epimorphism, so we have:

$$W_{\sum K^2}(K) \cong W(K)/\ker\Phi = W(K)/\ker\widehat{Sgn_{\sum K^2}} = W(K)/TorsW(K).$$

This ring, usually denoted $W_{red}(K)$, is called the **reduced Witt ring** of K.

18. Spaces of orderings

We fix a proper preordering $T \subset K$ and denote $G_T = U(K)/U(T)$. This group is naturally isomorphic with a subgroup of $\{-1,1\}^{X_T}$. Indeed, each $a \in U(K)$ defines a function $\overline{a} : X_T \to \{-1,1\}$ given by:

$$\overline{a}(P) = \begin{cases} 1, & \text{if } a \in P \\ -1, & \text{if } a \in -P \end{cases}$$

Clearly $\overline{ab} = \overline{a} \cdot \overline{b}$, so the mapping:

$$a \mapsto \overline{a}$$

defines a group homomorphism from $U(K)$ into $\{-1,1\}^{X_T}$. Clearly $U(T)$ is contained in the kernel of this homomorphism. Conversely, if $a \notin U(T)$, then there exists $P \in X_T$ such that $a \in -P$, so that $\overline{a}(P) = -1$. Thus the above function is injective and by the isomorphism theorem $G_T = U(K)/U(T)$ is isomorphic to a certain subgroup of $\{-1,1\}^{X_T}$. The elements of G_T would be therefore denoted often as $\overline{a}$.

Later we will introduce the notion of quadratic forms over spaces of orderings. For use of this paragraph, we shall speak of so called **forms** with entries in G_T as of n-tuples $f = (\overline{a_1}, \dots, \overline{a_n})$. The number n here is called the **dimension** of the form f. The product $\overline{a_1} \cdot \ldots \cdot \overline{a_n} \in G_T$ is called the **determinant** of f and for each $P \in X_T$ the sum $sgn_P f = \sum_{i=1}^n \overline{a_i}(P) \in \mathbb{Z}$ is said to be the **signature** of the form f. We say that $\overline{b} \in G_T$ is **represented** by f if for some $t_1, \dots, t_n \in T$ we have $b = \sum_{i=1}^n a_i t_i$. The set of all elements $\overline{b} \in G_T$ represented by f is called the **value set** of f and is denoted by $D(f)$. Observe that $D((\overline{a})) = \{\overline{b}\}$ and for $n \geq 3$:

$$\overline{b} \in D((\overline{a_1}, \dots, \overline{a_n})) \Leftrightarrow \overline{b} \in D((\overline{a_1}, \overline{c}))$$

for some $\overline{c} \in D((\overline{a_2}, \dots, \overline{a_n}))$. Indeed, suppose that $b = a_1t_1 + \ldots + a_nt_n$. If $a_2t_2 + \ldots + a_nt_n \neq 0$, take $c = a_2t_2 + \ldots + a_nt_n$. If $a_2t_2 + \ldots + a_nt_n = 0$ then $b = a_1t_1 = a_1t_1 + c0$, so we can choose arbitrary $\overline{c}$.

Therefore the study of value sets reduces (by induction) to the 2-dimensional case. The following lemma gives a complete description of the case of value sets of 2-dimensional forms:

Lemma 6. $D(\overline{a_1}, \overline{a_2}) = \{\overline{b} : \bigwedge_{P \in X_T} \overline{b}(P) = \overline{a_1}(P) \vee \overline{b}(P) = \overline{a_2}(P)\}$.

Proof. Let $\overline{b} \in D(\overline{a_1}, \overline{a_2})$ and let $P \in X_T$. Then $b = a_1t_1 + a_2t_2$. If $\overline{a_1}(P) = -\overline{a_2}(P)$ then clearly $\overline{b}(P) = \overline{a_1}(P)$ or $\overline{b}(P) = \overline{a_2}(P)\}$. If $\overline{a_1}(P) = \overline{a_2}(P) = 1$ then - since $b = a_1t_1 + a_2t_2$ - $\overline{b}(P) = 1$. Similarly, if $\overline{a_1}(P) = \overline{a_2}(P) = -1$ then - since $b = a_1t_1 + a_2t_2$ - $\overline{b}(P) = -1$.

Assume that for all $P \in X_T$ $\overline{b}(P) = \overline{a_1}(P)$ or $\overline{b}(P) = \overline{a_2}(P)$. Suppose that $b \notin Ta_1 + Ta_2$, that is $b/a_1 \notin T + Ta_2/a_1$. Consider the preordering $T' = T[\frac{a_2}{a_1}] = T + T\frac{a_2}{a_1}$ and let P be such ordering extending T' that $\frac{b}{a_2} \notin P$. Obviously $P \in X_T$. Furthermore, $\overline{\frac{a_2}{a_1}}(P) = 1$ and $\overline{\frac{a_2}{a_1}}(P) = -1$. Thus $\overline{a_1}(P) = \overline{a_2}(P)$ and $\overline{b}(P) = -\overline{a_1}(P)$ - a contradiction. □

The next result shows that every represented element has a "transversal" representation:

Lemma 7. *Let $a_1, \ldots, a_n, b \in U(K)$. TFAE:*

(1) $\overline{b} \in D((\overline{a_1}, \ldots, \overline{a_n}))$

(2) $b = a'_1 + \ldots + a'_n$ *for some* $a'_i \in U(K)$ *such that* $\overline{a'_i} = \overline{a_i}$.

Proof. (2) $\Rightarrow$ (1) is clear, so let's prove the converse. Let $b = a_1t_1 + \ldots + a_nt_n$. Since $p = (\frac{p+1}{2})^2 - (\frac{p-1}{2})^2$ we get $\frac{a_1+\ldots+a_n}{b} = r^2 - s^2 = (1 + r^2) - (1 + s^2)$ for some $r, s \in K$. Thus

$$(1 + r^2)b = a_1 + \ldots + a_n + (1 + s^2)b = \sum_{i=1}^{n}(1 + (1 + s^2)t_i)a_i$$

and we may set $a'_i = \frac{1+(1+s^2)t_i}{1+r^2}a_i$. □

Now we can proceed to the definition of a **space of orderings**. Recall that a character on a group G is a group homomorphism $x : G \to \{-1, 1\}$. The group of all characters is denoted by $\chi(G)$. The space of orderings is a pair (X, G) satisfying the following axions:

(1) $X \neq \emptyset$, $G < \{-1, 1\}^X$, $const. - 1 \in G$ and:

$$\bigwedge_{x,y\in X} x \neq y \Rightarrow (\bigvee_{a\in G} a(x) = a(y))$$

Observe that we can construct a natural embedding of X into $\chi(G)$ by identifying:

$$x \mapsto (G \ni a \mapsto a(x) \in \{-1, 1\}).$$

The set of all such $c \in G$ that either $c(x) = a(x)$ or $c(x) = b(x)$ for each $x \in X$ will be called the **value set** and denoted by $D(a, b)$.

(2) If $x \in \chi(G)$ satisfies $x(const. - 1) = -1$ and:

$$\bigwedge_{a,b\in\ker(x)} D(a, b) \subset \ker(x)$$

then x is in the image of the natural embedding $X \hookrightarrow \chi(G)$.

(3) $\bigwedge_{a_1,a)2,a_3\in G}(\bigvee_{c\in D(a_2,a_3)} b \in D(a_1, c)) \Rightarrow (\bigvee_{d\in D(a_1,a_2)})$

Notice that if $x \in X$ is viewed as a character $x \in \chi(G)$ then we clearly have:

$$x(-1) = (-1)(x) = -1$$

and thus if $a, b \in \ker(x)$ then $D(a, b) \subset \ker(x)$. Thus the axion (2) is just saying that every character on G having these properties is in X. Elements of X are often referred to as orderings and $\ker(x)$ is sometimes called the positive cone of x. The following theorem explains this notation:

Theorem 24. *If T is a proper preordering in a formally real field K, then the pair (X_T, G_T) is a space of orderings.*

Proof. Since T is proper, $X_T \neq \emptyset$. By one of the previous lemmas G_T can be viewed as a subgroup of $\{-1,1\}^{X_T}$ and - clearly - $\overline{-1} \in G_T$ plays the role of the *const.* -1 function. Fix $P, Q \in X_T$ such that $P \neq Q$ and let $a \in P$ be an element such that $a \notin Q$. Thus $\overline{a}(P) = 1$ and $\overline{a}(Q) = -1$, so G_T separates points in X_T and axion (1) is satisfied.

Let $x \in \chi(G_T)$ be such a character that $x(\overline{-1}) = -1$ and suppose that:

$$\bigwedge_{\overline{a},\overline{b} \in \ker(x)} D(\overline{a}, \overline{b}) \subset \ker(x).$$

Let $P = \{a \in U(K) : \overline{a} \in \ker(x)\} \cup \{0\}$. Clearly $T \subset P$ (if $a \in T$ then $\overline{a} = 0 \in G_T = U(K)/U(T)$), $P \cup -P = K$ (let $a \in U(K)$ be such that $\overline{a} \notin \ker(x)$; then $x(\overline{a}) = -1$, so $x(-\overline{a}) = 1$ and $-\overline{b} \in \ker(x)$), $P \cap -P = \{0\}$ (let $a \in U(K)$ be such that $\overline{a} \in \ker(x)$ and $-\overline{a} \in \ker(x)$; then $x(\overline{a}) = 1$ and $x(-\overline{a}) = 1$ which implies that $\overline{a} = 0$), $P \cdot P \subset P$ (let $a, b \in U(K)$ be such that $x(\overline{a}) = 1$ and $x(\overline{b}) = 1$; then clearly $x(\overline{a} \cdot \overline{b} = 1)$ and $P + P \subset P$ (let $a, b \in U(K)$ be such that $\overline{a} \in \ker(x)$ and $\overline{b} \in \ker(x)$; if $a + b = 0$, we are done; if $a + b \neq 0$then $D(\overline{a}, \overline{b}) \subset \ker(x)$ and $\overline{a+b} \in D(\overline{a}, \overline{b})$ - indeed $a + b = 1^2 a + 1^2 b$; hence $\overline{a+b} \in D(\overline{a}, \overline{b})$ and it follows that $x(\overline{a+b}) = 1$). Thus $P \in X_T$ and x is the character on G_T corresponding to P.

Let $\overline{a_1}, \overline{a_2}, \overline{a_3} \in G_T$ and suppose that for some $\overline{c} \in D(\overline{a_2}, \overline{a_3})$ we have $\overline{b} \in D(\overline{a_1}, \overline{c})$. Using the recently proved characterization of $D(\overline{a_2}, \overline{a_3})$ we have $c = t_2' a_2 + t_3' a_3$ and then - using the same characterization for $D(\overline{a_1}, \overline{c})$ - we have $b = t_1 a_1 + t_2 a_2 + t_3 a_3$. If $t_1 a_1 + t_2 a_2 \neq 0$ then we may take $d = t_1 a_1 + t_2 a_2$ so that $\overline{b} \in D(\overline{d}, \overline{a_3})$. Otherwise $b = t_3 a_3$ and we may choose an arbitrary $\overline{d} \in D(\overline{a_1}, \overline{a_2})$. □

We shall give a natural topology to the space (X, G) - namely the weakest topology such that functions:

$$a : X \to \{-1, -1\}, \qquad a \in G$$

are continuous (with discrete topology on $\{-1, 1\}$). It is easy to observe that if we give to the group $\chi(G)$ the natural topology, that is the weakest topology such that multiplication in $\chi(G)$ is continuous, then the topology induced by the embedding:

$$X \hookrightarrow \chi(G)$$

on the set X is the same as the topology defined above and that the sets:

$$U(a) = \{x \in X : a(x) = 1\}$$

for a subbasis for this topology. Using the same methods as for the set X_F we can prove that (X, G) is a Boolean space (see [5] page 23). Spaces of orderings form a category, that is we can speak of morphisms of spaces of orderings. Namely a **morphism** from a space of orderings (X, G) to a space of orderings (Y, H) is a mapping $\alpha : X \to Y$ such that:

$$\bigwedge_{a \in H} a \circ \alpha \in G.$$

In particular every morphism α induces a group homomorphism:

$$a \mapsto a \circ \alpha$$

from G to H. Clearly α is continuous, since $\alpha^{-1}(U(a)) = U(a \circ \alpha)$. An **isomorphism** from (X, G) to (Y, H) is a morphism $\alpha : X \to Y$ which is bijective and such that the induced group homomorphism:

$$a \mapsto a \circ \alpha$$

is also bijective. Next, we say that a space of orderings (X, G) is **realized** by the preordering T in the field K if $(X, G) \cong (X_T, G_T)$. Notice that the question whether a given space (X, G) is realized by the preordering $\sum K^2$ for some field is - in general - very hard.

19. Quadratic forms over spaces of orderings and the Witt Ring

Fix a space of orderings (X, G). A **form** over a space of orderings (X, G) is a formal $n-$tuple $f = (a_1, \dots, a_n)$ with entries in G. The number n is called the **dimension** of the form f, the product $a_1 \cdot \ldots \cdot a_n \in G$ is called the **determinant** pf f and denoted by $\det f$. For each $x \in X$ the **signature** of f at x is $sgn_x f = \sum_{i=1}^n a_i(x) \in \mathbb{Z}$.

We can also define the **value set** $D(f)$ of a form $f = (a_1, \dots, a_n)$, often written as $D(a_1, \dots, a_n)$. We proceed by induction - if $f = (a)$, then:

$$D(f) = a,$$

if $f = (a, b)$ then, not surprisingly:

$$D(f) = D(a, b) = \{c \in G : \bigwedge_{x \in X} c(x) = a(x) \vee c(x) = b(x)\},$$

and, finally, if $f = (a_1, \dots, a_n)$, then:

$$D(f) = \bigcup_{b \in D(a_2, \dots, a_n)} D(a_1, b).$$

We say b is **represented** by a form f if $b \in D(f)$.

We use standard notation from quadratic form theory. If $f = (a_1, \dots, a_n)$ and $g = (b_1, \dots, b_m)$ then we define the **direct orthogonal sum**:

$$f \perp g = (a_1, \dots, a_n, b_1, \dots, b_m)$$

and the **tensor product**:

$$f \otimes g = (a_1 b_1, \dots, a_1 b_m, \dots, a_n b_1, \dots, a_n b_m).$$

We shall also write cf to denote the form $(ca_1, \dots, ca_n)$, $c \in G$, and $k \times f$ instead of $\underbrace{f \perp \ldots \perp f}_{k}$, $k \in \mathbb{N}$. As was the case in the classical theory, the forms of the shape:

$$(1, a_1) \otimes \ldots \otimes (1, a_n)$$

are called **Pfister forms** and denoted by $((a_1, \dots, a_n))$.

Now we shall study some basic properities of value sets of quadratic forms over spaces of orderings. First of all, observe that our inductive definition makes $D(f)$ independent on the order of the entries of f. Indeed, let $f = (a_1, \dots, a_n)$. The result is clear if $n = 1$ or $n = 2$, so suppose that $n \geq 3$. It suffices to show that the value set does not change if we permute two adjacent elements a_i and

a_j. If $i, j \geq 2$, then the statement is clear by induction. If $i = 1$ and $j = 2$, suppose that $b \in D(a_2, a_1, a_3, \ldots, a_n)$. Thus $b \in D(a_2, c)$ and $c \in D(a_1, d)$, $d \in D(a_3, \ldots, a_n)$. By the associativity axiom (3) $b \in D(a_1, e)$ for some $e \in D(a_2, d)$, so $b \in D(a_1, a_2, \ldots, a_n)$.

Clearly, $D(cf) = cD(f)$ for any $c \in G$, since $c^2 = 1$. Next, observe that:

$$c \in D(f \perp g) \Leftrightarrow \bigvee_{a \in D(f)} \bigvee_{b \in D(g)} c \in D(a, b).$$

Indeed, assume that $f = (a_1, \ldots, a_k)$, $g = (a_{k+1}, \ldots, a_n)$. First, we shall prove the implication ($\Rightarrow$). If $k = 1$, then $c \in D(a_1, b)$, $b \in D(a_2, \ldots, a_n)$, so we can take $a = a_1$. If $k \geq 2$ then $c \in D(a_1, d)$, $d \in D(f' \perp g)$, where $g' = (a_2, \ldots, a_k)$. By induction $d \in D(e, p)$, $e \in D(f')$, $p \in D(r)$ and hence by the associativity axiom (3) $c \in D(r, p)$ for some $r \in D(a_1, e)$. Thus $r \in D(f)$, so we can take $a = r$, $b = p$.

To prove ($\Leftarrow$), assume that $k = 1$. Then, since $a \in D(a_1)$ and thus $a = a_1$, we have $c \in D(a_1, b)$. If $k \geq 2$ then $a \in D(a_1, d)$, $d \in D(f')$, where $f' = (a_2, \ldots, a_n)$. Again, by the associativity axiom (3), $c \in D(a_1, e)$ where $e \in D(d, b)$. By induction on k, $e \in D(f' \perp g)$. This proves $c \in D(f \perp g)$.

Moreover, using induction we can show that:

$$c \in D(f_1 \perp \ldots \perp f_k) \Leftrightarrow \bigvee_{a_i \in D(f_i)} c \in D(a_1, \ldots, a_k).$$

Next, we say that a set $M \subset G$ is **additively closed** if for any $a, b \in M$ we have $D(a, b) \subset M$. Observe, that $D(f)$ is the smallest additively closed set containing the entries of f. Indeed, say $f = (a_1, \ldots, a_n)$. Using $D(a_1, \ldots, a_n) = \bigcup_{b \in D(a_2, \ldots, a_n)} D(a_1, b)$ and induction on n we see that any additively closed set containing $a_1, \ldots, a_n$ must contain $D(f)$. It remains to check, that $D(f)$ is itself additively closed. Let $a, b \in D(f)$ and let $c \in D(a, b)$. Then $c \in D(f \perp f) = D((a_1, a_1) \perp \ldots \perp (a_n, a_n))$, so $c \in D(d_1, \ldots, d_n)$ for some $d_i \in D(a_i, a_i)$, $i \in \{1, \ldots, n\}$. Thus $d_i(x) = a_i(x)$ for all $x \in X$, so $d_i = a_i$, do $c \in D(f)$.

As an immediate consequence we get that also:

$$D(k \times f) = D(f).$$

Now we shall introduce the notion of the **isometry** of quadratic forms over spaces of orderings. We also proceed by induction; if $f = (a)$ and $g = (b)$, then

$$f \cong g \Leftrightarrow a = b,$$

if $f = (a_1, a_2)$ and $g = (b_1, b_2)$ then:

$$f \cong g \Leftrightarrow \bigwedge_{x \in X} sgn_x f = a_1(x) + a_2(x) = b_1(x) + b_2(x) = sgn_x g,$$

finally, if $f = (a_1, \ldots, a_n)$, $g = (b_1, \ldots, b_n)$ then:

$$f \cong g \Leftrightarrow$$
$$\bigvee_{a, b, c_3, \ldots, c_n \in G} \begin{array}{l} (a_2, \ldots, a_n) \cong (a, c_3, \ldots, c_n) \wedge (a_1, a) \cong (b_1, b) \wedge \\ \wedge (b_2, \ldots, b_n) \cong (b, c_3, \ldots, c_n) \end{array}.$$

This definition allows us to give an alternative description of the set of values of f, analogous to the representation theorem in the classical sense. Namely, if

$f = (a_1, \dots, a_n)$:

$$b_1 \in D(f) \Leftrightarrow \bigvee_{b_2,\dots,b_n} f \cong (b_1, \dots, b_n)$$

We proceed by induction on n. If $n = 1$, the result is clear, if $n = 2$ it suffices to compare signatures: if $(a_1, a_2) \cong (b_1, b_2)$ then $b_1 \in D(a_1, a_2)$ and $a_1a_2 = b_1b_2$, so $b_2 = a_1a_2b_1$. Conversely, if $b_1 \in D(a_1, a_2)$ then $(a_1, a_2) \cong (b_1, b_2)$ where $b_2 = a_1a_2b_1$. Suppose that $n \geq 3$. If $(a_1, \dots, a_n) \cong (b_1, \dots, b_n)$ then we may pick $a, b, c_3, \dots, c_n$ such that:

$$(a_2, \dots, a_n) \cong (a, c_3, \dots, c_n) \wedge (a_1, a) \cong (b_1, b) \wedge (b_2, \dots, b_n) \cong (b, c_3, \dots, c_n).$$

Thus $b_1 \in D(a_1, a)$ and, by inductive hypothesis, $a \in D(a_2, \dots, a_n)$, so $b_1 \in D(a_1, \dots, a_n)$. Conversely, if $b_1 \in D(a_1, \dots, a_n)$ then $b_1 \in D(a_1, a)$ for some $a \in D(a_2, \dots, a_n)$. Thus $(a_1, a) \cong (b_1, b)$ where $b = a_1ab_1$ and, by induction, $(a_2, \dots, a_n) \cong (a, c_3, \dots, c_n)$ for some $c_3, \dots, c_n$. Thus $(a_1, \dots, a_n) \cong (b_1, \dots, b_n)$ where $b_2 = b$, $b_i = c_i$, $i \in \{3, \dots, n\}$.

Next, observe that if $b_i = a_{\pi(i)}$ for some permutation π of $\{1, \dots, n\}$ then:

$$(a_1, \dots, a_n) \cong (b_1, \dots, b_n).$$

In order to prove that we may assume $n \geq 3$. If $\pi(1) = i \geq 2$, take $a = a_i$, $b = a_1$ and $c_3, \dots, c_n$ to be the elements left after a_1 and a_i are deleted from the list $a_1, \dots, a_n$. Since $a, c_3, \dots, c_n$ is a permutation of $a_2, \dots, a_n$, $b, c_3, \dots, c_n$ is a permutation of $b_2, \dots, b_n$ and b_1, b is a permutation of a_1, a, the result follows by induction. If $\pi(1) = 1$ take $a = b = a_2$ and $c_i = a_i$.

Observe that if $f \cong g$, then $\dim f = \dim g$. It is easy to prove by induction that also $\det f = \det g$, $sgn_x f = sgn_x g$ for all $x \in X$, $D(f) = D(g)$ and $cf \cong cg$ for all $c \in G$. As was the case with "normal" quadratic forms, the relation $\cong$ is an equivalence relation; indeed, it is clearly symmetric and reflexive, so we have to show that it is transitive. We shall state this as a separate result.

Lemma 8. *The relation $\cong$ is transitive.*

Proof. Let f, g and h be such n-dimensional forms over (X, G) that $f \cong g$ and $g \cong h$. Using induction we shall show that $f \cong h$. If $n = 1$ or $n = 2$, the result is clear. Let $n = 3$, $f = (a_1, a_2, a_3)$, $h = (b_1, b_2, b_3)$. Since $D(f) = D(g) = D(h)$ we have that $b_1 \in D(f)$, so $b_1 \in D(a_1, a)$ for some $a \in D(a_2, a_3)$. Thus $(a_1, a) \cong (b_1, b)$ and $(a_2, a_3) \cong (a, c_3)$ for some $b, c_3 \in G$. Thus:

$$(b_1, b_2, b_3) = h \cong g \cong f = (a_1, a_2, a_3) \cong (b_1, b, c_3).$$

Comparing signatures gives $b_2(x) + b_3(x) = b(x) + c_3(x)$ for all $x \in X$, so $(b_2, b_3) \cong (b, c_3)$.

Let $n \geq 4$. Pick elements $a, b, c \in G$ and $(n-1)-$dimensional forms f', g', h' so that

$$f = (a) \perp f' \text{ , } g = (b) \perp g' \text{ and } h = (c) \perp h'.$$

Since $f \cong g$ and $g \cong h$, there exist $a', b', b'', c' \in G$ and $(n-2)-$dimensional forms α, β such that:

$$f' \cong (a') \perp \alpha, g' \cong (b') \perp \alpha, g' \cong (b'') \perp \beta, h' \cong (c') \perp \beta, (a, a') \cong (b, b').$$

and $(b, b'') \cong (c, c')$. By induction $(b') \perp \alpha \cong (b'') \perp \beta$, so there exist $b_1, b_2 \in G$ and an $(n-3)-$dimensional form γ such that:

$$\alpha \cong (b_1) \perp \gamma, \beta \cong (b_2) \perp \gamma, (b', b_1) \cong (b'', b_2).$$

Hence:

$$(a, a', b_1) \cong (b, b', b_1) \cong (b, b'', b_2) \cong (c, c', b_2)$$

so there exist $a_1, c_1, d \in G$ satisfying:

$$(a', b_1) \cong (a_1, d), (c', b_2) \cong (c_1, d), (a, a_1) \cong (c, c_1).$$

Let $\delta = (d) \perp \gamma$. Then:

$$f' = (a') \perp \alpha \cong (a', b_1) \perp \gamma \cong (a_1, d) \perp \gamma \cong (a_1) \perp \delta$$

and

$$h' = (c') \perp \beta \cong (c', b_2) \perp \gamma \cong (c_1, d) \perp \gamma \cong (c_1) \perp \delta.$$

By induction $f' \cong (a_1) \perp \delta$ and $h' \cong (c_1) \perp \delta$. Since $(a, a_1) \cong (c, c_1)$ this proves $f \cong h$. □

Now observe that - as in the classical case - for any forms f, f', g, g' $f \cong f'$ and $g \cong g'$ implies:

$$f \perp g \cong f' \perp g' \text{ and } f \otimes g \cong f' \otimes g'.$$

Indeed, since isometry of forms is independent on order of entries of form, $f \perp g \cong g \perp f$ and $f \otimes g \cong g \otimes f$, so we may assume that $f = f'$. If $g \cong g'$ then $cg \cong cg'$, so it suffices to show the result for $\perp$. By induction on dimension of f we are reduced to the case when $\dim(f) = 1$, say $f = (a_1)$. Let $a, c_3, \dots, c_n$ be such that $g = (a, c_3, \dots, c_n)$ and let $b = a$. Then

$$g \cong (a, c_3, \dots, c_n), g' \cong (b, c_3, \dots, c_n), (a_1, a) \cong (a_1, b)$$

so $(a_1) \perp g \cong (a_1) \perp g'$ by definition of $\cong$.

We can also state the following result, being an analogon to the Witt cancellation theorem: for any forms f, f', g, g' $f \cong f'$ and $f \perp g \cong f' \perp g'$ implies $g \cong g'$. Indeed, using independence on permutations and induction on the dimension of f we can reduce to the case $f = f'$ and $\dim f = 1$, say $f = (a_1)$. Let $a, b, c_3, \dots, c_n$ be such that

$$g \cong (a, c_3, \dots, c_n), g' \cong (b, c_3, \dots, c_n), (a_1, a) \cong (a_1, b).$$

Comparing determinants yields $a = b$, so $g \cong (a, c_3, \dots, c_n) = (b, c_3, \dots, c_n) \cong g'$, so that $g \cong g'$.

Now we are in a good point to define the Witt ring of quadratic forms over a space of orderings. A form $(a, -a)$, $a \in G$, is called a **hyperbolic plane.** Note that $(a, -a) \cong (1, -1)$ for any $a \in G$. A form h is called a **hyperbolic form** if:

$$h = \underbrace{(1, -1) \perp \ldots \perp (1, -1)}_{k}$$

and we say that two forms f and g are **similar,** denoted $f \sim g$, if there exist hyperbolic forms h_1 and h_2 such that:

$$f \perp h_1 \cong g \perp h_2.$$

This is easily seen to be an equivalence relation. On the set $W(X, G)$ of all similarity classes we define addition:

$$< f > + < g > = < f \perp g >$$

and multiplication:

$$< f > \cdot < g > = < f \otimes g >$$

and therefore we make $W(X, G)$ into a commutative ring with identity, which will be called the **Witt ring of a space of orderings**.

At the end of this section we shall introduce the notion of isotropy. A form f will be called **isotropic** if there is a form g such that $f \cong (1, -1) \perp g$. Otherwise f will be called **anisotropic**. As we remember, in the "classical" theory there was a useful relationship between isometry and similarity - in the case of the Witt ring of a space of orderings we have the following criterion:

$$f \cong g \Leftrightarrow f \sim g \wedge \dim f = \dim g.$$

Implication ($\Rightarrow$) is clear and to prove the converse suppose that $f \perp k \times (1, -1) \cong g \perp k \times (1, -1)$. Comparing dimensions and using $\dim f = \dim g$ we get $k = l$, so $f \cong g$ by the Witt cancellation theorem.

Next, observe that:

$$f \text{ is isotropic } \Leftrightarrow \bigvee_{g} f \sim g \wedge \dim f > \dim g.$$

Implication ($\Rightarrow$) is clear and to prove the converse suppose that $f \perp k \times (1, -1) \cong g \perp k \times (1, -1)$. Comparing dimensions and using $\dim f > \dim g$ we get $k < l$, so $f \cong g \perp (l - k) \times (1, -1)$ by the Witt cancellation theorem.

Another useful characterization of isotropy is as follows:

$$f \text{ is isotropic } \Leftrightarrow D(f) = G \Leftrightarrow D(f) \cap -D(f) \neq \emptyset.$$

We shall prove that f is isotropic $\Rightarrow D(f) = G$; suppose that $f \cong (1, -1) \perp g$. Since $(1, -1) \cong (a, -a)$, this yields $f \cong (a, -a) \perp g$, so $a \in D(f)$ and therefore $D(f) = g$. The implication $D(f) = G \Leftrightarrow D(f) \cap -D(f) \neq \emptyset$ is clear, so let us prove $D(f) \cap -D(f) \neq \emptyset \Rightarrow f$ is isotropic. Say $f \cong (a_1, \ldots, a_n)$ and $-a_1 \in D(f)$. Since $D(a_1) = \{a_1\}$ and $-a_1 \neq a_1$, $n \geq 2$. Next, since $-a_1 \in D(f)$, $-a_1 \in D(a_1, a)$ for some $a \in D(a_2, \ldots, a_n)$. Comparing signatures we get that $-a_1 = a$ and hence $-a_1 \in D(a_2, \ldots, a_n)$. Thus $(a_2, \ldots, a_n) \cong (-a_1, c_3, \ldots, c_n)$ for some $c_3, \ldots, c_n \in G$. Therefore:

$$f \cong (a_1, \ldots, a_n) \cong (a_1, -a_1, c_3, \ldots, c_n) \cong (1, -1, c_3, \ldots, c_n)$$

and f is isotropic.

As an immediate corollary we see that if f is anisotropic then so is $n \times f$ for any $n \geq 1$ (since $D(f) = D(nf)$).

Observe that if $f \perp g$ is isotropic then there exists $b \in D(f)$ such that $-b \in D(g)$. Indeed, say $f = (a) \perp f'$ and suppose that $f \perp g \cong (1, -1) \perp h \cong (a, -a) \perp h$. By the Witt cancellation theorem $f' \perp g \cong (-a) \perp h$, that is $-a \in D(f' \perp g)$. If g is one-dimensional then $f' \perp g = g$ and we take $b = a$. Otherwise we may choose $c \in D(f')$ and $d \in D(g)$ such that $-a \in D(c, d)$. Then $(c, d) \perp (-a, -acd)$, that is $(a, c) \cong (-d, -acd)$, so that $-d \in D(a, c) \subset D(f)$ and we can take $b = -d$.

20. Pfister's local-global principle for spaces of orderings

The following is an abstract version of Pfister's local-global principle for quadratic forms over spaces of orderings:

Theorem 25. *For any forms f, g:*

$$f \sim g \Leftrightarrow \bigwedge_{x \in X} sgn_x f = sgn_x g$$

Proof. ($\Rightarrow$) If $f \sim g$ then for some hyperbolic forms h_1, h_2 $f \perp h_1 \equiv g \perp h_2$. Since signatures of hyperbolic forms are equal to zero it follows that $sgn_x f = sgn_x g$ for all $x \in X$.

($\Leftarrow$) By considering the form $f \perp -g$ it suffices to show that if $sgn_x f = 0$ for all $x \in X$ then $f \sim 0$. Suppose that $f \nsim 0$. Since for every isotropic form f there exists a form g such that $\sim g$ and $\dim f > \dim g$, we may assume that f is anisotropic. If f is anisotropic then so is $n \times f$ for any $n \geq 1$, so we may assume that $2^n \times f \nsim 0$ for all $n \geq 0$. By the Zorn's lemma we may choose a multiplicative set S in the Witt ring $W(X, G)$ with $2 \in S$ maximal subject to the condition that $g \otimes f \nsim 0$ for all $< g > \in S$.

We shall show that:

$$\bigwedge_{a \in G} < 1, a > \in S \vee < 1, -a > \in S$$

but both possibilities cannot occur. Suppose that $< 1, a > \notin S$. Since $(1, a) \otimes (1, a) \sim 2 \times (1ma)$ and $2 \in S$, the multiplicative set generated by S and $< 1, a >$ is $S \cup < 1, a > \otimes S$. By the maximality of S, $(1, a) \otimes g_1 \otimes f \sim 0$ for some $g_1 \in S$. Similarly, if $< 1, -a > \notin S$ then $< 1, -a > \otimes g_2 \otimes f \sim 0$ for some $g_2 \in S$. Since $2 \sim (1, 1) \sim (1, a) \perp (1, -a)$, this implies:

$$\begin{aligned} 2 \times g_1 \otimes g_2 \otimes f &\sim g_1 \otimes g_2 \otimes f \perp g_1 \otimes g_2 \otimes f \\ &\sim (1, 1) \otimes g_1 \otimes g_2 \otimes f \\ &\sim [(1, a) \perp (1, -a)] \otimes g_1 \otimes g_2 \otimes f \\ &\sim (1, a) \otimes g_1 \otimes g_2 \otimes f \perp (1, -a) \otimes g_1 \otimes g_2 \otimes f \\ &\sim 0 \end{aligned}$$

so that $2 \times g \times f \sim 0$ where $g = g_1 \otimes g_2$. Since $2 \times g \in S$, this is a contradiction. If both $< 1, a >$ and $< 1, -a >$ are in S, then $(1, a) \otimes (1, -a) \sim 0 \in S$, a contradiction.

Therefore we have a well-defined function $x : G \to \{-1, 1\}$ given by:

$$x(a) = \begin{cases} 1 & \text{if } < 1, a > \in S \\ -1 & \text{if } < 1, -a > \in S \end{cases}$$

Note that $< 1, a > \in S \Leftrightarrow < 1, -a > \notin S \Leftrightarrow (1, -a) \otimes g \otimes f \sim 0$ that means $ar \otimes f \sim g \otimes f$ for some $< g > \in S$. It follows easily that x is a character on G.

Now we shall show that $x \in X$. Suppose that $a, b \in \ker x$, $c \in D(a, b)$ and $c \notin \ker x$. Then $(a, b) \cong (c, cab)$. Also $ag \otimes f \sim g \otimes f$, $bg \otimes f \sim g \otimes f$ and $cg \otimes f \sim -g \otimes f$ for some $g \in S$. Then $(a, b) \otimes g \otimes f \sim 2 \times g \otimes f$, $(c, cab) \otimes g \otimes f \sim -2 \otimes g \otimes f$ so $4 \times g \otimes f \sim 0$ contradicting $4 \times < g > \in S$. Thus $a, b \in \ker x$, $c \in D(a, b)$ implies that $c \in \ker x$, so by the second axiom $x \in X$.

To complete the proof we need to show that $sgn_x f \neq 0$. Let $f = (a_1, \ldots, a_n)$ and suppose that $e_i = a_i(x)$ so that $sgn_x f = \sum_{i=1}^n a_i(x) = \sum_{i=1}^n e_i$. By the definition of x, $< 1, a(x)a > \in S$ holds for any $a \in G$, hence $< 1, e_i a_i > \in S$, so $f \otimes \prod_{i=1}^n (1, e_i a_i) \nsim 0$. On the other hand $a_i(1, e_i a_i) \cong e_i(1, e_i a_i)$ so:

$$f \otimes \prod_{i=1}^n (1, e_i a_i) = (a_1, \ldots, a_n) \otimes \prod_{i=1}^n (1, e_i a_i) \cong (e_1, \ldots, e_n) \otimes \prod_{i=1}^n (1, e_i a_i).$$

It follows that $(e_1, \ldots, e_n) \nsim 0$ and since each e_i is 1 or -1 this means $\sum_{i=1}^n e_i \neq 0$. □

As an immediate consequence of the above theorem we have the following fact:

$$f \cong g \Leftrightarrow \dim f = \dim g \wedge \bigwedge_{x \in X} sgn_x f = sgn_x g.$$

This is clear for dimensions 1 and 2. Also for dimension ≥ 3 the implication $(\Rightarrow)$ is easily checked by induction. In order to prove the converse suppose that $\dim f = \dim g$ and for all $x \in X$ we have $sgn_x f = sgn_x g$. This implies $f \sim g$ which - since the dimensions of f and g are equal - means that $f \cong g$.

The above characterization agrees with the intuition for "normal" quadratic forms over reals. It also allows us to give an alternate definition of a space of orderings. Namely, a space of orderings is said to be a pair (X, G) satisfying the following axioms:

(1) $X \neq \emptyset$, $G < \{-1,1\}^X$, $const. -1 \in X$ and
$$\bigwedge_{x,y \in X} x \neq y \Rightarrow (\bigvee_{a \in G} a(x) = a(y)).$$

(2) The image of the natural embedding of X into $\chi(G)$:
$$x \mapsto (G \ni a \mapsto a(x) \in \{-1,1\})$$
is closed in $\chi(G)$.

(3) For any forms f and g with entries in G:
$$\bigwedge_{c \in D(f \perp g)} \bigvee_{a \in D(f)} \bigvee_{b \in D(g)} c \in D(a,b).$$

The proof of equivalence of those two definitions of a space of orderings is given in details in [5] on page 27.

21. Subspaces and preorderings

Assume that (X, G) is a space of orderings. Recall that for any $a \in G$ the set:

$$U(a) = \{x \in X : a(x) = 1\}$$

is clopen. Such sets form a subbasis for topology on X and the sets:

$$U(a_1, \ldots, a_n) = \bigcap_{i=1}^{n} U(a_i)$$

are a basis for the topology. A subset $Y \subset X$ is called a **subspace** of X if Y is expressible as

$$Y = \bigcap_{a \in S} U(a)$$

for some, not necessarily finite, subset $S \subsetneq G$. The **subspace generated** by a subset Y in X is just the smallest subspace of (X, G) containing Y. For any subspace Y of X let $G|_Y$ denote the group of all restrictions $a|_Y$, $a \in G$, and for any form $f = (a_1, \ldots, a_n)$ with entries in G let $f|_Y$ denote the form $(a_1|_Y, \ldots, a_n|_Y)$. Speaking of a subspace Y of (X, G) we shall refer to the pair $(Y, G|_Y)$.

Let K be a formally real field and consider the full space of orderings

$$(X_{\sum K^2}, G_{\sum K^2}).$$

Subspaces of such space have the form (X_T, G_T) where T is a preordering in K. Indeed, let $Y \subset X_{\sum K^2}$ be a subspace, say $Y = \bigcap_{\overline{a} \in S} U(\overline{a})$. Then $Y = X_T$ where T is the preordering in K generated by the elements a, $\overline{a} \in S$, and $G|_Y =$

G_T. Conversely, it T is a preordering of K, then $X_T = \bigcap_{a \in T \setminus \{0\}} U(\overline{a})$. Such correspondence is one-to-one and inclusion-reversing: if T and T' are preorderings in K then $X_{T'}$ is a subspace of X_T iff $T' \supset T$.

We shall try to establish a similar result for abstract spaces of orderings. A **preordering** in G is a subgroup T of G which is additively closed in the following sense:

$$\bigwedge_{a,b \in T} D(a,b) \subset T.$$

Theorem 26. (1) *Let $Y = U(c_1, \ldots, c_k)$. Denote $g = (1, c_1) \otimes \ldots \otimes (1, c_k)$. Then the preordering generated by $\{c_1, \ldots, c_k\}$ is:*

$$D(g) = \{b \in G : bg \cong g\} = \{b \in G : b = 1 \textit{ on } Y\}.$$

(2) *Let $Y = \bigcap_{a \in S} U(a)$ for any set $S \subset G$. Then the preordering generated by S is:*

$$\{b \in G : b = 1 \textit{ on } Y\}.$$

Proof. Let T denote the preordering generated by $c_1, \ldots, c_k$. Clearly g is the sum of the 1-dimensional forms $(c_{i_1} \cdot \ldots \cdot c_{i_s})$, $1 \leq i_1 < \ldots < i_s \leq k$, $0 \leq s \leq k$, so - since $D(g)$ is the smallest additively closed set containing the entries of g - $D(g)$ is the smallest additively closed set containing the products $c_{i_1} \cdot \ldots \cdot c_{i_s}$. These products are obviously in T, so $D(g) \subset T$. The set:

$$\{b \in G : b = 1 \text{ on } Y\}$$

is a preordering containing $c_1, \ldots, c_k$, so $T \subset \{b \in G : b = 1 \text{ on } Y\}$. Now fix an element $b \in G$ such that $b = 1$ on Y. Comparing signatures and dimensions and using the alternative definition of isometry we see that $g \cong bg$ (the signature of each side at x is 2^n if $x \in Y$ and 0 otherwise). Finally, since $1 \in D(g)$, $g \cong bg$ implies $b \in D(g)$.

In order to prove (2) - again, one inclusion is clear. For the other suppose $b = 1$ on Y. Since b is continuous and X is compact, this implies that $b = 1$ on some set $U(c_1, \ldots, c_k)$, $\{c_1, \ldots, c_k\} \subset S$. Thus b lies in the preordering generated by $\{c_1, \ldots, c_k\}$. □

As an immediate corollary we see that there is a natural one-to-one inclusion-reversing correspondence between subspaces of X and preorderings in G. Indeed, if Y is any subspace, then $T = \{b \in G : b = 1 \text{ on } Y\}$ is a preordering. If $T \subset G$ is any preordering, then $Y = \bigcup_{c \in T} U(c)$ is a subspace and $T = \{b \in G : b = 1 \text{ on } Y\}$.

Now we want to prove that every subspace of a space of orderings is actually a space of orderings. In order to do that we need the following lemma:

Lemma 9. (1) *Let $Y = U(c_1, \ldots, c_k)$. Denote $g = (1, c_1) \otimes \ldots \otimes (1, c_k)$. Let $f = (a_1, \ldots, a_n)$ and let $f|_Y = (a_1|_Y, \ldots, a_n|_Y)$. Then:*

$$\begin{aligned} b|_Y \in D(f|_Y) \quad &\Leftrightarrow \quad b \in D(f \otimes g) \\ &\Leftrightarrow \quad b \in D(a_1 s_1, \ldots, a_n s_n) \textit{ for some } s_1, \ldots, s_n \in D(g) \end{aligned}$$

(2) *Let $Y = \bigcap_{a \in S} U(a)$ for any set $S \subset G$. Let $f = (a_1, \ldots, a_n)$ and let $f|_Y = (a_1|_Y, \ldots, a_n|_Y)$. Then:*

$$b|_Y \in D(f|_Y) \Leftrightarrow b \in D(a_1 s_1, \ldots, a_n s_n) \textit{ for some } s_1, \ldots, s_n \in G \textit{ s.t. } s_i = 1 \textit{ on } Y.$$

Proof. We shall use the alternate definition of value sets and isometry. Suppose $b|_Y \in D(f|_Y)$ so $f \cong (b_1, \dots, b_n)$ on Y for some $b_1, \dots, b_n \in G$ with $b_1 = b$. Comparing signatures $f \otimes g \cong (b_1, \dots, b_n) \otimes g$ on X. Since $1 \in D(g)$ this proves $b = b_1 \in D(f \otimes g)$. In turn, using $f \otimes g \cong a_1 g \perp \dots \perp a_n g$ and the third alternate axiom, $b \in f \otimes g$ implies that $b \in D(a_1 s_1, \dots, a_n s_n)$ for some $s_1, \dots, s_n \in D(g)$. In turn, since $s_i = 1$ on Y, this implies $b_Y \in D(f|_Y)$.

In (2) the implication ($\Leftarrow$) is clear. To prove ($\Rightarrow$) assume that $b|_Y \in D(f|_Y)$, that is $(a_1, \dots, a_n) \cong (b_1, \dots, b_n)$ on Y for some $b_1, \dots, b_n \in G$ with $b_1 = b$. Y is the intersection of the sets $U(c_1, \dots, c_k)$, $c_1, \dots, c_k \in S$ and the function:

$$x \mapsto \sum_{i=1}^{n} a_i(x) - \sum_{i=1}^{n} b_i(x)$$

is continuous. By compactness of X $(a_1, \dots, a_n) \cong (b_1, \dots, b_n)$ on $U(c_1, \dots, c_k)$ for some $c_1, \dots, c_k \in S$. By the previous part of the theorem $b \in D(a_1 s_1, \dots, a_n s_n)$ where $s_i \in D((1, c_1) \perp \dots \perp (1, c_k))$. Since $Y \subset U(c_1, \dots, c_k)$ and $s_i = 1$ on $U(c_1, \dots, c_k)$ we see that $s_i = 1$ on Y. □

Now we are able to finish our proof. We proceed with checking the alternate axioms of a space of orderings. (1) and (2) are clear, so let us consider (3). Suppose $a|_Y \in D(f|_Y \perp g|_Y)$, $f = (b_1, \dots, b_k)$, $g = (c_1, \dots, c_l)$. By the previous lemma $a \in D(b_1 s_1, \dots, b_k s_k, c_1 t_1, \dots, c_l t_l)$ with $s_i = t_j = 1$ on Y. By the third alternate axiom for (X, G) we have $b \in D(b_1 s_1, \dots, b_k s_k)$, $c \in D(c_1 t_1, \dots, c_l t_l)$ with $a \in D(b, c$. Then $a|_Y \in D(b|_Y, c|_Y)$, $b|_Y \in D(f|_Y)$, $c|_Y \in D(g|_Y)$.

22. Fans

Let G be a multiplicative group with exponent 2. Fix an element $e \in G$, $e \neq 1$ (to play the role of the constant function -1) and set

$$X = \{x \in \chi(G) : x(e) = -1\}.$$

Elements of G may be viewed as functions on X by defining

$$a(x) = x(a) \text{ for all } a \in G, x \in X.$$

The pair (X, G) constructed this way is called a **fan**. Not surprisingly we shall prove the following theorem:

Theorem 27. *Any fan (X, G) is a space of orderings.*

Proof. We shall use the standard axioms of a space of orderings. First, observe that if H is any subgroup of G maximal subject to the condition $e \notin H$, then $H = \ker x$ for some $x \in X$. Indeed, suppose that $b \notin H$. Then $H \cup bH$ is a subgroup of G containing H, so $e \in H \cup bH$. Since $e \notin H$, this means that $e \in bH$, or $b \in eH$. Thus $H \cup eH = G$, so we have a character $x : G \to \{-1, 1\}$ with $\ker x = H$. Then $e \notin \ker x$, so $x(e) = -1$, that is $x \in X$.

We can identify G with a subgroup of $\{-1, 1\}^X$ by viewing $a \in G$ as the function $a : X \to \{-1, 1\}$ given by:

$$a(x) = x(1).$$

This is correct: if $a \neq b$ then $ab \neq 1$, so $e \notin \{1, eab\}$. Hence, by the Zorn's lemma, we get a subgroup H of G with $\{1, eab\} \subset H$ maximal subject to the condition $e \notin H$. By the previuos observation, $H = \ker x$ for some $x \in X$ and hence $x(eab) = 1$, that is $x(a) = -x(b)$ or $a(x) = -b(x)$ and therefore a and b define distinct functions on X.

Now the axiom (1) is clearly satisfied and so is (2). Before we prove (3) observe, that if $a, b \in G$, $ab \neq -1$, then $D(a,b) = \{a, b\}$. Indeed, suppose $c \notin \{a, b\}$. Then $-1 \notin \{1, ab, -ac, -bc\}$ so, by the Zorn's lemma, we have a subgroup H of G with $\{1, ab, -ac, -bc\} \subset H$ maximal to the condition $-1 \notin H$. By the previous observation we have $x \in X$ with $\ker x = H$. Thus $(ab)(x) = 1$, that is $a(x) = b(x)$ and $(-ac)(x) = 1$, that is $c(x) = -a(x) \neq a(x)$. Thus $a(x) + b(x) \neq c(x) + a(x)b(x)c(x)$, so $(a, b) \ncong (c, abc)$ which means that $c \notin D(a, b)$.

To finish the proof suppose $b \in D(a_1, c)$ for some $c \in D(a_2, a_3)$. We want to show $b \in D(d, a_3)$ for some $d \in D(a_1, a_2)$. If $a_1a_2 \neq -1$, $a_1a_3 \neq -1$ and $a_2a_3 \neq -1$, then by the above note $c = a_2$ or a_3 and $b = a_1, a_2$ or a_3. Thus we can take $d = a_1$ or a_2 in this case. If $a_1a_2 = -1$, then $D(a_1, a_2) = G$ so we can take $d = b$. If $a_1a_3 = -1$ or $a_2a_3 = -1$ then $D(a_1, a_3) = G$ or $D(a_2, a_3) = G$, so we can take $d = a_1$ or $d = a_2$. □

The motivation for considering fans comes from the following example. Let K be a field. Recall that a subring $B \subset K$ is called the **valuation ring** if for any unit $a \in U(K)$ we have $a \in B$ or $a^{-1} \in B$. It is easily checked that valuation rings are local rings with the only maximal ideal:

$$\mathfrak{M} = \{a \in U(K) : a^{-1} \notin B\} \cup \{0\}$$

and the group of units:

$$U = \{a \in U(K) : a, a^{-1} \in B\} = B \setminus \mathfrak{M}.$$

The field $\overline{K} = B/\mathfrak{M}$ is called the residue field. A ring homomorphism $\alpha : B \to K'$, where K' is any field, is called a **place**, when $\ker \alpha = \mathfrak{M}$. We can extend any place α to a function $\alpha : K \to K' \cup \{\infty\}$ by setting $\alpha(a) = \infty$ if $a \in K \setminus B$. A place is called **real valued** if $K' = \mathbb{R}$. Next, the set:

$$U_\alpha^+ = \{a \in K : \alpha(a) \neq \infty, \alpha(a) > 0\}$$

happens to be a subgroup of $U(K)$. It can be checked that $-1 \notin U(K)^2 U_\alpha^+$ and that $K^2 U_\alpha^+ = U(K)^2 U_\alpha^+ \cup \{0\}$ is a preordering. Furthermore, if P^* is a subgroup of $U(K)$ such that $U(K)^2 U_\alpha^+ \subset P^*$ and $[U(K) : P^*] = 2$ and $-1 \notin P^*$ then $P = P^* \cup \{0\}$ is an ordering. It can be shown that every ordering on K is obtained by this process starting with some real place α. Proofs of all the facts mentioned above can be found in [2].

Now $(X_{K^2 U_\alpha^+}, G_{K^2 U_\alpha^+})$ is a fan. The proof is clear from the above remarks. Some authors (e.g. T. Y. Lam in [4], see page 39) give another definition of fan: a fan is a preordering T of a formally real field K such that for any set $P^* \supset T$ such that $-1 \notin P^*$ and $[U(K) : P^*] = 2$ the set $P = P^* \cup \{0\}$ is an ordering. We see that those two definitions are somehow "isomorphic".

Fans can be characterized in variuos ways:

Theorem 28. *Let (X, G) be a space of orderings. The following are equivalent:*

(1) *(X, G) is a fan.*
(2) *$D(1, a) = \{1, a\}$ for all $a \in G \setminus \{-1\}$.*
(3) *For all $a_1, \ldots, a_n \in G$ if $a_ia_j \neq -1$ for $i \neq j$, then $D(a_1, \ldots, a_n) = \{a_1, \ldots, a_n\}$.*
(4) *If $x \in \chi(G)$ satisfies $x(-1) = -1$ then $x \in X$.*

Proof. (1) $\Rightarrow$ (2) follows from the proof of the previous theorem, (2) $\Rightarrow$ (3) can be proved by induction; $D(a) = \{a\}$ is true in general. Also $D(a,b) = aD(1,ab)$, so if (2) holds then $D(a,b) = a\{1,ab\} = \{a,b\}$ if $ab \neq -1$. Now suppose that $b \in D(a_1,\dots,a_n)$ for $n \geq 3$ and $a_ia_j \neq -1$ for $i \neq j$. Thus $b \in D(a_1,c)$ for some $c \in D(a_2,\dots,a_n)$. By induction $c = a_j$ for some $j \geq 2$. Thus $b \in D(a_1,a_j)$, so $b = a_1$ or $b = a_j$ - anyway, $b \in \{a_1,\dots,a_n\}$.

To prove (3) $\Rightarrow$ (4) it suffices to show that if $a,b \in \ker x$ then $D(a,b) \subset \ker x$, so that $x \in X$ by the axiom (2). Since $-1 \notin \ker x$, $ab \neq -1$, so, by our assumption, $D(a,b) = \{a,b\}$. The implication (4) $\Rightarrow$ (1) is obvious. □

We also need to know when a finite space of orderings is a fan. Suppose that (X,G) is a space of ordering with X finite (so G is also finite). Viewing elements of X as characters we have:

$$\bigcap_{x\in X} \ker x = \{1\}$$

so we can find some smallest subset $\{x_1,\dots,x_n\}$ of X with

$$\bigcap_{i=1}^{n} \ker x_i = \{1\}.$$

Any such subset will be called a **minimal generating set** for X.

Theorem 29. *Let (X,G) be a space of orderings with a minimal generating set $\{x_1,\dots,x_n\}$. Then:*

1. $|G| = 2^n$
2. *$\{x_1,\dots,x_n\}$ is a basis over a field $\mathbb{F}_2$ for the character group $\chi(G)$. In particular each $x \in X$ is expressible uniquely as*
$$x = \prod_{i=1}^{n} x_i^{e_i}, e_i \in \{0,1\}.$$
3. *A necessary condition for a character $x = \prod_{i=1}^{n} x_i^{e_i}$, $e_i \in \{0,1\}$, to be in X is that*
$$\sum_{i=1}^{n} e_i \equiv 1 mod 2.$$
In particular, $n \geq |X| \geq 2^{n-1}$.
4. *(X,G) is a fan iff $|X| = 2^{n-1}$.*

Proof. Let $\{x_1,\dots,x_n\}$ be a minimal generating set for (X,G), so that

$$\bigcap_{i=1}^{n} \ker x_i = \{1\}.$$

Consider the chain of subgroups:

$$G \subset \ker x_1 \supset \ker x_1 \cap \ker x_2 \supset \ldots \supset \bigcap_{i=1}^{n} \ker x_i = \{1\}.$$

For $j \in \{1,\dots,n\}$ $\ker x_j$ has index 2 in G and $\bigcap_{i=1}^{j-1} \ker x_i \not\subseteq \ker x_j$ by the minimal choice of the subset $\{x_1,\dots,x_n\}$. Thus $(\bigcap_{i=1}^{j-1} \ker x_i) \cdot \ker x_j = G$ and

$$\frac{\bigcap_{i=1}^{j-1} \ker x_i}{\bigcap_{i=1}^{j} \ker x_i} \cong \frac{(\bigcap_{i=1}^{j-1} \ker x_i) \cdot \ker x_j}{\ker x_j} = \frac{G}{\ker x_j}.$$

This means $\bigcap_{i=1}^{j} \ker x_i$ has index 2 in $\bigcap_{i=1}^{j-1} \ker x_i$, $j \in \{1, \dots, n\}$, so $\{1\} = \bigcap_{i=1}^{n} \ker x_i$ has index 2^n in G, that is $|G| = 2^n$ and (1) is proved.

By counting we see that the natural injection $G \hookrightarrow \prod_{i=1}^{n} G/\ker x_i$ is surjective , so we get elements $a_1, \dots, a_n$ in G such that $x_i(a_j) = -1$ if $i = j$ and 1 otherwise. Clearly $a_1, \dots, a_n$ becomes a $\mathbb{F}_2$-basis of G, that is every element $a \in G$ is expressible uniquely as $a = \prod_{i=1}^{n} a_i^{e_i}$, $e_i \in \{0, 1\}$. Also it is clear that $x_1, \dots, x_n$ is just the dual basis of $\chi(G)$. This proves (2).

Since each $x \in X$ must satisfy $x(-1) = (-1)(x) = -1$, (3) and (4) are also clear. □

The above argument also shows that if (X, G) has a finite generating set, then it is finite. If $a_1, \dots, a_n$ is the dual basis of G corresponding to $x_1, \dots, x_n$ then, in terms of this basis, $-1 = a_1 \dots a_n$, which can be easily checked by evaluating each side at x_j, $j \in \{1, \dots, n\}$.

Observe that if $n = 1$ or $n = 2$ then $n = 2^{n-1}$, so $x_1, \dots, x_n$ are the only elements in X. This is not the case when $n \geq 3$: for example if $n = 3$ then $|X| = 3$ or $|X| = 4$ - if the second possibility holds, the character $x_1x_2x_3$ belongs to X.

If (X, G) is any space of orderings then by a **fan** in (X, G) we mean subspace Y of X such that the space of orderings $(Y, G|_Y)$ is a fan. In the case of the space of orderings $(X_{\sum K^2}, G_{\sum K^2})$, K a real field, the fans are $(X_{K^2 U_\alpha^+}, G_{K^2 U_\alpha^+})$, where $\alpha : K \to \mathbb{R} \cup \{\infty\}$ are the real valued places. Clearly any subspace of a fan is a fan. Fans containing only 1 or 2 elements are said to be **trivial**.

23. Representation theorem

Let (X, G) be any space of orderings. The representation theorem describes the image of the Witt ring $W(X, G)$ in the ring of continuous functions $C(X, \mathbb{Z})$. We start with the following lemma:

Lemma 10. *Let $f : X \to \mathbb{Z}$ be a continuous function. Then for some integer $n \geq 0$ $2^n f$ is represented by a form, that is there exists a form ϕ with entries in G such that:*

$$\bigwedge_{x \in X} 2^n f(x) = sgn_x \phi.$$

Proof. Since f is continuous and $\mathbb{Z}$ is endowed with a discrete topology, we see that:

$$\bigwedge_{x \in X} \bigvee_{U(a_1, \dots, a_v)} x \in U(a_1, \dots, a_v) \wedge f \text{ is constant on } U(a_1, \dots, a_v).$$

Now, since X is compact, there exist elements $a_{ij} \in G$, $i \in \{1, \dots, k\}$, $j \in \{1, \dots, v_i\}$ such that:

$$X = \bigcup_{i=1}^{k} U(a_{i1}, \dots, a_{iv_i})$$

and f is constant on each $U(a_{i1}, \dots, a_{iv_i})$. Let $\overline{G} < G$ be a subgroup generated by -1 and the elements a_{ij}. For $x \in X$ let:

$$\overline{x} = \{y \in X : a(y) = a(x) \text{ for all } a \in \overline{G}\}$$

and

$$\overline{X} = \{\overline{x} : x \in X\}.$$

If we view elements of X as characters on G, then elements of $\overline{X}$ are just restrictions of elements of X to $\overline{G}$. Elements of $\overline{X}$ can be viewed as characters on the finite group $\overline{G}$, so $\overline{X}$ is finite. If $\overline{x} = \overline{y}$ then $a_{ij}(x) = a_{ij}(y)$ for all i, j, so x, y lie in the same $U(a_{i1}, \dots, a_{iv_i})$, so $f(x) = f(y)$. Thus we get well-defined function $\overline{f} : \overline{X} \to \mathbb{Z}$ given by:

$$\overline{f}(\overline{x}) = f(x) \text{ for all } x \in X.$$

$\overline{G}$ may be viewed as a vector space over the field $\mathbb{F}_2$, so we may pick a basis $-1, a_1, \dots, a_n$ for $\overline{G}$. Define:

$$p_{\overline{x}} =< 1, a_1(x)a_1 > \otimes \dots \otimes < 1, a_n(x)a_n >$$

for every $\overline{x} \in \overline{X}$. Then

$$p_{\overline{x}}(y) = \begin{cases} 2^n & \text{if } \overline{y} = \overline{x} \\ 0 & \text{if } \overline{y} \neq \overline{x} \end{cases}$$

Thus:

$$sgn_y \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) p_{\overline{x}} = 2^n \overline{f}(\overline{y}) = 2^n f(y)$$

for each $y \in Y$. Since $p_{\overline{x}} \in W(X, G)$ and $\overline{f}(\overline{x}) \in \mathbb{Z}$, we may take $\phi = \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) p_{\overline{x}}$. □

Now we proceed to the main representation theorem:

Theorem 30. *Let $f : X \to \mathbb{Z}$ be a continuous function. Then the following statements are equivalent:*

(1) *f is represented by a form, that is there exists a form ϕ with entries in G such that:*
$$\bigwedge_{x \in X} f(x) = sgn_x \phi.$$
(2) *For all finite fans $Y \subset X$:*
$$\sum_{x \in Y} f(x) \equiv 0 mod |Y|.$$
(3) *For all finite fans $Y \subset X$ and for all $a \in G$:*
$$\sum_{x \in Y} a(x) f(x) \equiv 0 mod |Y|.$$

Proof. (1) $\Rightarrow$ (2). Suppose that f is represented by $\phi = (a_1, \dots, a_n)$ and that $Y \subset X$ is a finite fan. Then $f(y) = \sum_{i=1}^n a_i(y)$ and so:

$$\sum_{y \in Y} f(y) = \sum_{i=1}^n (\sum_{y \in Y} a_i(y)).$$

Thus we are reduced to showing that for any $a \in G$ we have:

$$\sum_{y \in Y} a(y) \equiv 0 mod |Y|.$$

If $a = \pm 1$ on Y then $\sum_{y \in Y} a(y) = \pm |Y|$. If $a \neq \pm 1$ on Y then $Y = U(a|_Y) \cup U(-a|_Y)$ and, since Y is a fan, $U(a|_Y)$ and $U(-a|_Y)$ have each half as many elements as Y, so:

$$\sum_{y \in Y} a(y) = |U(a|_Y)| - |U(-a|_Y)| = 0.$$

(2) ⇒ (3) Suppose that for all finite fans $Y \subset X$ $\sum_{x\in Y} f(x) \equiv 0 mod|Y|$. Fix an element $a \in G$ and a fan $Y \subset X$ - we want to show that:

$$\sum_{x\in Y} a(x)f(x) \equiv 0 mod|Y|.$$

If $a = \pm 1$ on Y the result is clear. Otherwise, since $Y = U(a|_Y) \cup U(-a|_Y)$ and $U(a|_Y)$ is a fan with $\frac{1}{2}|Y|$ elements which implies $\sum_{x\in U(a|_Y)} f(x) \equiv mod\frac{1}{2}|Y|$, we have:

$$\begin{aligned}\sum_{x\in Y} a(x)f(x) &= \sum_{x\in U(a|_Y)} f(x) - \sum_{x\in U(-a|_Y)} f(x)\\ &= 2(\sum_{x\in U(a|_Y)} f(x)) - (\sum_{x\in Y} f(x)) \equiv 0 mod|Y|.\end{aligned}$$

(3) ⇒ (1). Suppose that f is not represented by a form. Let

$$\mathcal{F} = \{Y : Y \subset X \text{ is a subspace, } f|_Y \text{ is not represented by a form }\}.$$

Such family is nonempty. For an arbitrary chain $\mathcal{C} = \{Y_i : i \in I\} \subset \mathcal{F}$ consider the set $Y = \bigcap_{i\in I} Y_i$. Y is a subspace and if $f|_Y$ is represented by a form, say $(a_1|_Y, \ldots, a_n|_Y)$ then, by continuity, the set:

$$U = \{x \in X : f(x) = \sum_{i=1}^{n} a_i(x)\}$$

is open in X and contains Y. Thus by compactness of X it contains Y_i, so $f|_{Y_i}$ is represented by $(a_1|_{Y_i}, \ldots, a_n|_{Y_i})$. Therefore the Zorn's lemma applies and we have the subspace Y with $f|_Y$ not represented and Y is minimal with this property.

Now observe, that every fan in Y is also a fan in X, so our assumption that:

$$\sum_{x\in Z} a(x)f(x) \equiv 0 mod|Z|$$

for all $a \in G$ still holds for all finite fans $Z \subset Y$. Thus we may replace X with Y. So now f is not represented and $f|_Y$ is represented for each proper subspace $Y \subset X$.

We shall show that (X, G) is not a fan. Suppose that the opposite is true. Since f is continuous and $\mathbb{Z}$ is endowed with a discrete topology, we see that:

$$\bigwedge_{x\in X} \bigvee_{U(a_1,\ldots,a_v)} x \in U(a_1, \ldots, a_v) \wedge f \text{ is constant on } U(a_1, \ldots, a_v).$$

Now, since X is compact, there exist elements $a_{ij} \in G$, $i \in \{1, \ldots, k\}$, $j \in \{1, \ldots, v_i\}$ such that:

$$X = \bigcup_{i=1}^{k} U(a_{i1}, \ldots, a_{iv_i})$$

and f is constant on each $U(a_{i1}, \ldots, a_{iv_i})$. Let $\overline{G} < G$ be a subgroup generated by -1 and the elements a_{ij}. Pick any subgroup $H \subset G$ so that $G = \overline{G} \times H$, that is G is the direct product of $\overline{G}$ and H. Let:

$$Y = \{x \in \chi(G) : x|_H = 1 \wedge x(-1) = -1\}.$$

Since X is a fan, $Y \subset X$, and clearly Y is a fan. Again, $\overline{G}$ may be viewed as a vector space over the field $\mathbb{F}_2$, so we may pick a basis $-1, a_1, \dots, a_n$ for $\overline{G}$. We see that $|Y| = 2^n$. As before, define:

$$\overline{x} = \{y \in X : a(y) = a(x) \text{ for all } a \in \overline{G}\}$$

and

$$\overline{X} = \{\overline{x} : x \in X\}.$$

If we view elements of X as characters on G, then elements of $\overline{X}$ are just restrictions of elements of X to $\overline{G}$. Elements of $\overline{X}$ can be viewed as characters on the finite group $\overline{G}$, so $\overline{X}$ is finite. If $\overline{x} = \overline{y}$ then $a_{ij}(x) = a_{ij}(y)$ for all i, j, so x, y lie in the same $U(a_{i1}, \dots, a_{iv_i})$, so $f(x) = f(y)$. Thus we get well-defined function $\overline{f} : \overline{X} \to \mathbb{Z}$ given by:

$$\overline{f}(\overline{x}) = f(x) \text{ for all } x \in X.$$

Define:

$$p_{\overline{x}} =< 1, a_1(x)a_1 > \otimes \dots \otimes < 1, a_n(x)a_n >$$

for every $\overline{x} \in \overline{X}$. Then

$$p_{\overline{x}}(y) = \begin{cases} 2^n & \text{if } \overline{y} = \overline{x} \\ 0 & \text{if } \overline{y} \neq \overline{x} \end{cases}$$

Thus:

$$sgn_y \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) p_{\overline{x}} = 2^n \overline{f}(\overline{y}) = 2^n f(y)$$

for each $y \in Y$. Since $p_{\overline{x}} \in W(X, G)$ and $\overline{f}(\overline{x}) \in \mathbb{Z}$, we see that - as in the previous lemma - f is represented by the form $\phi = \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) p_{\overline{x}}$. Now for every S running through subsets of $\{1, \dots, n\}$ define:

$$a_S = \prod_{i \in S} a_i.$$

Thus we may expand $p_{\overline{x}}$ as $p_{\overline{x}} = \sum_S a_S(x) < a_S >$ and write:

$$\phi = \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) p_{\overline{x}} = \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) \sum_S a_S(x) < a_S >= \sum_S m_S < a_S >$$

where $m_S = \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) a_S(x)$. Now:

$$m_S = \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) a_S(x) = \sum_{y \in Y} f(y) a_S(y) = 0 mod 2^n$$

for each subset S of $\{1, \dots, n\}$. That means, that each of the integers m_S is divisible by 2^n, so f is represented by the form:

$$\sum_S \frac{m_S}{2^n} < a_S >\in W(X, G)$$

which is a contradiction. So (X, G) must not be a fan.

By one of the cited characterizations of fans, there exists $a \in G$ such that $a \neq -1$ and $D(1, a) \neq \{1, a\}$. Thus there exists $b \in D(1, a)$, $b \notin \{1, a\}$. Thus $(1, a) \cong (b, ab)$, that is $(-a, b, ab) \sim (1)$. Take $a_1 = -a$, $a_2 = b$ and $a_3 = ab$. Observe that $a_i \neq 1$, so $U(a_i)$ is a proper subspace of X. By the minimal choice of X, $f|_{U(a_i)}$ is represented. also $(a_1, a_2, a_3) \sim (1)$, so - by comparison of signatures - we get:

For each $x \in X$ exactly one of $a_1(x), a_2(x), a_3(x)$ is -1.

In particular $U(a_i) \cup U(a_j) = X$ for $i \neq j$. Thus we can assume $U(a_i) \neq \emptyset$ (otherwise $U(a_j) = X$). Let ϕ_i be a form with entries in G such that $\phi_i|_{U(a_i)}$ represents $f|_{U(a_i)}$. We can assume $\phi_3 \sim 0$, replacing f by $f - \phi_3$ if necessary, where ϕ_3 is viewed as a function $sgn.\phi_3$. We can also assume that $\phi_i|_{U(a_i)}$ is anisotropic. Next, by the lemma used in proof that every subspace is a space of orderings, we see that $D(\phi_i|_{U(a_i)}) = D(\phi_i \otimes (1, a_i))|_{U(a_i)}$ which means that $\phi_i \otimes (1, a_i)$ is anisotropic for $i \in \{1, 2\}$.

Let $x \in X$. If $a_1(x) = a_2(x) = 1$, then $sgn_x \phi_i = f(x)$ for $i \in \{1, 2\}$, so:

$$sgn_x \phi_1 \otimes (1, a_1) = 2f(x) = sgn_x \phi_2 \otimes (1, a_2).$$

If $a_1(x) = 1$, $a_2(x) = -1$, then $a_3(x) = 1$, so $sgn_x \phi_1 = f(x) = sgn_x \phi_3 = 0$ and $sgn_x (1, a_2) = 0$ so:

$$sgn_x \phi_1 \otimes (1, a_1) = 0 = sgn_x \phi_2 \otimes (1, a_2).$$

Similarly, if $a_1(x) = -1$, $a_2(x) = 1$ then $sgn_x \phi_1 \otimes (1, a_1) = 0 = sgn_x \phi_2 \otimes (1, a_2)$. Thus $\phi_1 \otimes (1, a_1)$ and $\phi_2 \otimes (1, a_2)$ have the same signatures at all $x \in X$ and both are anisotropic, so:

$$\phi_1 \otimes (1, a_1) \cong \phi_2 \otimes (1, a_2).$$

To finish the proof if suffices to show that there exists a form ϕ such that $\phi|_{U(a_i)} \cong \phi_i|_{U(a_i)}$. Let $S = D(\phi_1 \otimes (1, a_1)) = D(\phi_2 \otimes (1, a_2))$. Again using the mentioned lemma for the proof that every subspace is a space of orderings we get:

$$S|_{U(a_i)} = D(\phi_i \otimes (1, a_i))|_{U(a_i)} = D(\phi_i|_{U(a_i)})$$

for $i \in \{1, 2\}$. Pick $p \in S$ and decompose $\phi_i \cong (p) \perp \phi_i'$ on $U(a_i)$, so:

$$\phi_i \otimes (1, a_i) \cong (p, pa_i) \perp \phi_i' \otimes (1, a_i)$$

on X for $i \in \{1, 2\}$. Rewriting $\phi_1 \otimes (1, a_1) \cong \phi_2 \otimes (1, a_2)$ using this and cancelling form (p) we obtain:

$$(pa_1) \perp \phi_1' \otimes (1, a_1) \cong (pa_2) \perp \phi_2' \otimes (1, a_2).$$

Multiplying by a_2 and adding $(-pa_1a_2)$ to both sides yields:

$$(pa_1a_2) \perp a_2\phi_1' \otimes (1, a_1) \cong (p) \perp \phi_2' \otimes (1, a_2)$$

and

$$(1, -1) \perp a_2\phi_1' \otimes (1, a_1) \cong p(1, -a_1a_2) \perp \phi_2' \otimes (1, a_2).$$

It follows that the right side of the above equation is isotropic so, using one of the properties of isotropic direct orthogonal sums, there exists $s \in D(1, -a_1a_2)$ such that $-ps \in D(\phi_2' \otimes (1, a_2))$. Thus $-ps|_{U(a_2)} \in D(\phi_2'|_{U(a_2)})$, so $\phi_2' \cong (-ps) \perp \phi_2''$ on $U(a_2)$, so:

$$\phi_2' \otimes (1, a_2) \cong (-ps, -psa_2) \perp \phi_2'' \otimes (1, a_2)$$

on X. Also, $(1, -a_1a_2) \cong (s, -sa_1a_2)$. Rewriting the previous equation using these last two relations gives:

$$(1, -1) \perp a_2\phi_1' \otimes (1, a_1) \cong (ps, -psa_1a_2, -ps, -psa_2) \perp \phi_2'' \otimes (1, a_2).$$

Cancelling the hyperbolic planes $(1, -1) \cong (ps, -ps)$ and multiplying by a_2 this yields:

$$\phi_1' \otimes (1, a_1) \cong (-psa_1, -ps) \perp \phi_2'' \otimes (1, a_2).$$

It follows that $-ps \in D(\phi_1' \otimes (1, a_1))$, so $\phi_1' \cong (-ps) \perp \phi_1''$ on $U(a_1)$, that is $\phi_1' \otimes (1, a_1) \cong (-ps, -psa_1) \perp \phi_1'' \otimes (1, a_1)$ on X. Rewriting the above equality using this and cancelling we obtain:

$$\phi_1'' \otimes (1, a_1) \cong \phi_2'' \otimes (1, a_2)$$

on X. Since

$$\phi_i \cong (p) \perp \phi_i' \cong (p, -ps) \perp \phi_i''$$

on $U(a_i)$, $i \in \{1, 2\}$, we are done by induction on the dimension. □

The structure of the space of orderings (X, G) is determined by just two things: the topology on X and the fans in X. The following corollary makes this clear:

Theorem 31. *Let $f : X \to \{-1, 1\}$ be any continuous function. Then the following are equivalent:*

1. $f \in G$.
2. $\prod_{i=1}^4 f(x_i) = 1$ *for all 4-element fans* $\{x_1, x_2, x_3, x_4\}$ *in* X.
3. $\sum_{i=1}^4 f(x_i) \equiv 0 mod 4$ *for all 4-element fans* $\{x_1, x_2, x_3, x_4\}$ *in* X.

Proof. (1) ⇒ (2) is clear: if $f \in G$ then the condition $\prod_{i=1}^4 f(x_i) = 1$ just follows from the fact that, as characters, $\prod_{i=1}^4 x_i = 1$. (2) ⇔ (3) is obvious since $f(x_i) = \pm 1$. Therefore we have to prove that (3) ⇒ (1).

Suppose that $\sum_Z f(x_i) \equiv 0 mod 4$ for all 4-element fans Z in X. We shall show that f is represented by a form $\phi = (a_1, \ldots, a_n)$. Suppose that f is not repretented by a form - then, by the representation theorem, there exists a finite fan $V \subset X$ such that:

$$\sum_{x \in V} f(x) \not\equiv 0 mod |V|.$$

Take a minimal such V. Clearly $V \notin \{1, 2\}$ and, by hypothesis, $|V| \neq 4$, so $|V| \geq 8$. To simplify notation we replace X by V, so $X = V$ is a fan. Thus, by the characterization of finite spaces of orderings as fans, $|G| = 2^{n+1}$. Pick $b_1 \in G$, $b_1 \neq \pm 1$, and let $b_2 = -b_1$. By minimality of V:

$$\sum_{x \in U(b_i)} f(x) \equiv 0 mod 2^{n-1}, i \in \{1, 2\}.$$

Moreover, since $f(x) = \pm 1$:

$$\sum_{x \in U(b_i)} f(x) \in \{0, 2^{n-1}, -2^{n-1}\}, i \in \{1, 2\}.$$

Note also that, since $b_2 = -b_1$:

$$\sum_{x \in X} f(x) = \sum_{x \in U(b_1)} f(x) + \sum_{x \in U(b_2)} f(x).$$

Thus, for $\sum_{x \in X} f(x) \neq 0 mod |V|$ to hold, one of the above sums must be zero and the other $\pm 2^{n-1}$. Replacing f by $-f$ and interchanging the roles of b_1 and b_2 if necessary, we may assume:

$$\sum_{x \in U(b_1)} f(x) = 0 \text{ and } \sum_{x \in U(b_2)} f(x) = 2^{n-1}.$$

Since $\sum_{x\in U(b_1)} f(x) = 0$, there exist $x_1, x_2 \in U(b_1)$ such that $f(x_1) = 1$ and $f(x_2) = -1$. Pick $x_3 \in U(b_2)$. Then $x_4 = x_1x_2x_3 \in U(b_2)$ since:

$$b_2(x_4) = b_2(x_1)b_2(x_2)b_2(x_3) = (-1)(-1)(1) = 1.$$

Next, $f(x) = 1$ for all $x \in U(b_2)$, since $\sum_{x\in U(b_2)} f(x) = 2^{n-1}$. In particular, $f(x_i) = 1$ for $i \in \{3, 4\}$. Thus:

$$\sum_{i=1}^{4} f(x_i) = 2 \neq 0 mod 4.$$

But $\{x_1, x_2, x_3, x_4\}$ forms a 4-element fan, which yields a contradiction.

Therefore f is represented by $\phi = (a_1, \ldots, a_n)$. For fixed $x \in X$ let k be the number of positive entries of ϕ and l the number of negative entries. Then $k+l = n$ and $k - l = sgn_x\phi = \pm 1$. This forces n to be odd, say $n = 2m + 1$ and

$$sgn_x\phi = 1 \Leftrightarrow k = m + 1 \wedge l = m$$

and

$$sgn_x\phi = -1 \Leftrightarrow k = m \wedge l = m + 1.$$

It follows that $sgn_x\phi = a(x)$ where $a = (-1)^m \prod_{i=1}^{n} a_i$. Applying the Pfister's local-global principle we get

$$\phi \sim (a)$$

so f can be viewed as an element of G. □

24. Stability index

The **stability index** of a space of orderings (X, G), denoted $stab(X, G)$, is defined to be the maximum n such that there exists a fan $Y \subset X$ with $|Y| = 2^n$ or ∞ if no such finite n exists. Observe that if $x, y \in X$, $x \neq y$, then $\{x, y\}$ is a fan, so the stability index of (X, G) is greater or equal than 1. Thus stability index zero just means X is a singleton set. We shall obtain other characterizations of the stability index, but first we need some terminology and a lemma.

The **derived form** f' of a Pfister form $f = (1, a_1) \otimes \ldots \otimes (1, a_n)$ is defined by:

$$f = (1) \perp f'.$$

Lemma 11. *Let* $Y = U(a_1, \ldots, a_n)$, $f = (1, a_1)\otimes\ldots\otimes(1, a_n)$, *with* $a_1, \ldots, a_n \in G$. *Let* $b \in D(f')$. *Then there exist* $b_1, \ldots, b_n \in G$ *such that* $Y = U(b, b_2, \ldots, b_n)$.

Proof. If $n = 1$ the hypothesis on b forces $b = a_1$ so the result is clear. Assume $n \geq 2$ and let $f \equiv g \perp a_1g$, where $g = (1, a_2) \otimes \ldots \otimes (1, a_n)$. Then $f' \equiv g' \perp a_1g$ where g' is the derived form of g. By the characterization of the value set of the form f' we have $b \in D(c, a_1d)$ with $c \in D(g')$ and $d \in D(g)$. By induction on:

$$U(a_2, \ldots, a_n) = U(c, b_3, \ldots, b_n).$$

We shall show that this implies that $Y = U(a_1, \ldots, a_n) = U(b, a_1cd, b_3, \ldots, b_n)$. Let $x \in X$. Suppose first that $a_i(x) > 0$, $i \in \{1, \ldots, n\}$. Then b, c, d are positive at x (since $b, c, d \in D(f)$) and $b_3, \ldots, b_n$ are positive at x using $U(a_2, \ldots, a_n) = U(c, b_3, \ldots, b_n)$, which proves $x \in U(b, a_1cd, b_3, \ldots, b_n)$. Now suppose that

$$b, a_1cd, b_3, \ldots, b_n$$

are positive at x. Since $b \in D(c, a_1d)$ and $bc \in D(1, a_1cd)$ we get $bc > 0$ at x and hence $c > 0$ at x. Thus, using $U(a_2, \ldots, a_n) = U(c, b_3, \ldots, b_n)$, $a_2, \ldots, a_n$ are positive at x and $d > 0$ at x (since $d \in D(g)$). Finally, as $a_1cd > 0$ at x it follows $a_1 > 0$ at x.

Now since $Y = U(a_1, \dots, a_n) = U(b, a_1cd, b_3, \dots, b_n)$ we are done taking $b_2 = a_1cd$. □

Theorem 32. *For $k \geq 1$ the following are equivalent:*

1. *$stab(X, G) \leq k$.*
2. *$f \in Cont(X, \mathbb{Z}) \Rightarrow 2^k f \in W(X, G)$.*
3. *Every basic set $Y \subset X$ is expressible as $Y = U(a_1, \dots, a_k)$ for some $a_1, \dots, a_k \in G$.*

Proof. (1) ⇒ (2). Suppose $f \in Cont(X, \mathbb{Z})$. Then, for any finite fan $Z \subset X$, $|Z|$ divides 2^k. Thus $\sum_{x \in Z} 2^k f(x) \equiv 0 mod |Z|$ holds for all finite fans $Z \subset X$, so $2^k f \in W(X, G)$ by the representation theorem.

(2) ⇒ (3). Y is basic so $Y = U(a_1, \dots, a_n)$ for some $n \geq 0$. Choose n as small as possible. If $n \leq k$ we are done, so suppose $n > k$. Define $f : X \to \mathbb{Z}$ by:

$$f(x) = \begin{cases} 1 & \text{if } x \in Y \\ 0 & \text{if } x \notin Y \end{cases}$$

Then $2^k f$ is represented by some form ϕ with entries in G. We may assume that ϕ is anisotropic. Let $g = (1, a_1) \otimes \dots \otimes (1, a_n)$. If $Y = \emptyset$ then $Y = U(-1)$ contradicting $n > k$. Thus $Y \neq \emptyset$, so - since $sgn_x g = 2^n$ for all $x \in Y$ - g is anisotropic. Also $g \sim 2^{n-k} \times \phi$, hence $g \cong 2^{n-k} \times \phi$. It follows that $1 \in D(2^{n-k} \times \phi) = D(\phi)$, so for some form h we have:

$$\phi \cong (1) \perp h.$$

Substituting and cancelling (1) this yields:

$$g' \cong (2^{n-k} - 1) \times (1) \perp 2^{n-k} \times h.$$

Since $n > k$, this implies $1 \in D(g')$ so by the previuos lemma:

$$Y = U(1, c_1, \dots, c_n) = U(c_2, \dots, c_n)$$

for some $c_2, \dots, c_n \in G$. This contradicts the choice of n.

(3) ⇒ (1). Let $Z \subset X$ be a finite fan. We want to show $|Z| \leq 2^k$. Replacing X by Z we can assume X itself is a finite fan, $|X| = 2^m$. Let $x \in X$. The singleton set $\{x\}$ is basic and m inequalities are needed to describe this set. This proves $m \leq k$; if $U(a) \neq \emptyset$ then $a \neq -1$ so either $U(a) = X$ (if $a = 1$) or $|U(a)| = \frac{1}{2}|X|$ (if $a \neq 1$). This means that always $|U(a)| \geq \frac{1}{2}|X|$ - using this and induction we see that

$$U(a_1, \dots, a_k) \neq \emptyset \Rightarrow |U(a_1, \dots, a_k)| \geq \frac{1}{2^k}|X|.$$

In particular, when $U(a_1, \dots, a_k) = \{x\}$, then $1 \geq \frac{1}{2^k}|X|$ so $2^k \geq |X| = 2^m$ - so $k \geq m$ as claimed. □

25. Direct sums and group extensions of spaces of orderings

We say that (X, G) is a **singleton space** if $X = \{x\}$, so $G = \{-1, 1\}$. We say that (X, G) is the **direct sum** of the spaces of orderings (X_i, G_i), $i \in \{1, \dots, n\}$, denoted $(X, G) = (X_1, G_1) \oplus \dots \oplus (X_n, G_n)$, if X is the disjoint union of the sets X_i and G consists of all functions $a : X \to \{-1, 1\}$ such that $a|_{X_i} \in G_i$, $i \in \{1, \dots, n\}$. Finally, we say that (X, G) is a **group extension** of $(\overline{X}, \overline{G})$ if G has exponent 2,

$\overline{G}$ is a subgroup of G and X, viewed as a set of characters on G, consists of all characters x on G such that $x|_{\overline{G}} \in \overline{X}$.

Observe that any direct sum of spaces of orderings is a space of orderings. Indeed, from the definition of direct sum it is clear that the natural homomorphism $a \mapsto (a|_{X_1}, \dots, a|_{X_n})$ from G to the product group $G_1 \times \dots \times G_n$ is an isomorphism. We shall check the alternate axioms: (1) is clear. The topology on X is the direct sum topology and X is compact in this topology. Since the natural embedding $u : X \hookrightarrow \chi(G)$ is continuous, $u(X)$ is compact and hence closed in $\chi(G)$ - this proves (2). Next, for any forms f, g with entries in G it is clear that:

$$f \cong g \Leftrightarrow f|_{X_i} \cong g|_{X_i}, i \in \{1, \dots, n\}$$

and, consequently:

$$D(f) = \{b \in G : b|_{X_i} \in D(f|_{X_i}), i \in \{1, \dots, n\}\}.$$

This proves (3).

We can also prove that any group extension of a space of orderings is a space of orderings - this is a bit more complicated, though. Since G has exponent 2, G decomposes as a direct product $G = \overline{G} \times H$. Such decomposition is not unique. Thus, a a set of characters on G, $X = \overline{X} \times \chi(G)$, where $\chi(H)$ denotes the character group of H. We shall chceck the alternate axioms of a space of orderigs: (1) and (2) are clear, so we shall focus on proving (3).

First note that if ϕ is any form with entries in G, then we get forms ϕ_i with entries in $\overline{G}$ and distinct elements $h_1, \dots, h_s$ in H such that the entries of ϕ are just some permutation of the entries of $h_1\phi_1 \perp \dots \perp h_s\phi_s$. The forms ϕ_i will be called the **residue forms** of ϕ.

Now we shall show that:

$$\bigwedge_{x \in X} \phi(x) = 0 \Leftrightarrow \bigwedge_{\overline{x} \in \overline{X}} \bigwedge_{i \in \{1, \dots, s\}} \phi_i(\overline{x}) = 0.$$

In order to prove this observe that $\phi(x) = \sum_{i=1}^{s} h_i(s)\phi_i(x)$ for each $x \in X$. Now x decomposes as $x = \overline{x}y$ with $\overline{x} \in \overline{X}$ and $y \in \chi(H)$ and $h_i(x) = x(h_i) = y(h_i)$ and $\phi_i(x) = \phi_i(\overline{x})$. Thus

$$\bigwedge_{x \in X} \phi(x) = 0 \Leftrightarrow \bigwedge_{\overline{x} \in \overline{X}} \bigwedge_{y \in \chi(H)} \sum_{i=1}^{s} y(h_i)\phi_i(\overline{x}) = 0.$$

By linear independence of characters the above is equivalent to

$$\bigwedge_{\overline{x} \in \overline{X}} \bigwedge_{i \in \{1, \dots, s\}} \phi_i(\overline{x}) = 0.$$

In the next step we shall prove that if $\phi_1, \dots, \phi_s$ are anisotropic then $D(\phi) = \bigcup_{i=1}^{s} h_i D(\phi_i)$ - otherwise $D(\phi) = G$. For, if some ϕ_i is isotropic, then $\phi_i \cong (1, -1, \dots)$, so $\phi \cong (\dots, h_i, -h_i, \dots)$ so $D(\phi) = G$. Assume that $\phi_1, \dots, \phi_s$ are anisotropic. One inclusion is clear and to prove the other suppose that $b \in D(\phi)$. Thus we have a form ψ with $\phi \cong \psi$ with b appearing as an entry of ψ. We can assume $\psi = h_1\psi_1 \perp \dots \perp h_t\psi_t$ with $t \geq s$ and $\psi_1, \dots, \psi_t$ forms with entries in $\overline{G}$, $h_1, \dots, h_t \in H$ distinct. Take ϕ_i to be the zero dimensional form if $i > s$. Thus, by the previous claim applied to the difference $\phi \perp -\psi$ we see that $\phi_i \sim \psi_i$ for $i \in \{1, \dots, t\}$. Since the ϕ_i for $i \in \{1, \dots, s\}$ are anisotropic, we must have $\dim \phi_i \leq \dim \psi_i$, $i \in \{1, \dots, s\}$. Since ϕ and ψ have the same dimension, this forces

$t = s$ and $\phi_i \cong \psi_i$ for $i \in \{1, \dots, s\}$. Finally, since b is an entry of some $h_i\psi_i$, bh_i is an entry of ψ_i, so $bh_i \in D(\phi_i)$, that is $b \in h_i D(\phi_i)$.

Finally we are ready to prove the axiom (3). Suppose that $a \in D(\phi \perp \psi)$. We want $b \in D(\phi)$, $c \in D(\psi)$ such that $a \in D(b, c)$. We can assume that ϕ and ψ have residue form decompositions $h_1\phi_1 \perp \dots \perp h_t\phi_t$ and $h_1\psi_1 \perp \dots \perp h_t\psi_t$ as above. If all $\phi_i \perp \psi_i$ are anisotropic, then $a \in h_i D(\phi_i \perp \psi_i)$ for some i. If ϕ_i and ψ_i have both dimensions ≥ 1, we can apply (3) for $(\overline{X}, \overline{G})$ to get $ah_i \in D(b', c')$ for some $b' \in D(\phi_i)$, $c' \in D(\psi_i)$. In this case we can take $b = h_i b'$, $c = h_i c'$. The other cases are even simpler: if ψ_i say, is zero dimensional, then $a \in h_i D(\phi_i)$, so we may take $b = a$, c arbitrary in $D(\psi)$ in this case. When one of the $\phi_i \perp \psi_i$ is isotropic, we shall first consider the case when ϕ_i and ψ_i have both dimensions ≥ 1. Then $b' \in D(\phi_i)$ with $-b' \in D(\psi_i)$ and we take $b = h_i b'$, $c = -h_i b'$. If ψ_i say, is zero dimensional, then ϕ_i is isotropic, so $D(\phi) = G$ so take $b = a$, c arbitrary in $D(\psi)$.

Thus we proved that any group extension (X, G) of a space of orderings $(\overline{X}, \overline{G})$ is a space of orderings. Suppose that $a \in G$. What is $D(1, a)$? If $a \notin \overline{G}$, then $D(1, a) = \{1, a\}$. If $a = -1$, then $D(1, a) = G$. If $a \in \overline{G} \setminus \{-1\}$, then the value stet of the form $(1, a)$ is the same as the value set of $(1, a)$ for the space of orderings $(\overline{X}, \overline{G})$.

Next, the Witt ring $W(X, G)$ is isometric to the group ring $W(\overline{X}, \overline{G})[H]$, where H is any group chosen as in the previous proof.

Finally, the ring $W(X, G)$, where (X, G) is the direct sum of spaces

$$(X_1, G_1), \dots, (X_n, G_n),$$

may be identified with the subring of the direct product ring $\prod_{i=1}^n W(X_i, G_i)$ consisting of all $(f_1, \dots, f_n)$ with $\dim f_i \equiv \dim f_j mod2$ if $i \neq j$.

26. Spaces of orderings of finite chain length and the structural theorem

The **chain length** of a space of orderings (X, G), denoted $cl(X, G)$, is the maximum integer d such that there exist $a_0, \dots, a_d \in G$ with $U(a_0) \subsetneq \dots \subsetneq U(a_d)$ or ∞ if no such finite d exists. Clearly:

$$U(a) \subset U(b) \Leftrightarrow b \in D(1, a) \Leftrightarrow D(1, b) \subset D(1, a).$$

It is easy to observe, that the singleton space has chain length 1 and that fans have chain length ≤ 2. If (X, G) is the direct sum of (X_i, G_i), $i \in \{1, \dots, n\}$, the chain length of (X, G) is the sum of the chain lengths of the (X_i, G_i). Similarly, if (X, G) is a group extension of $(\overline{X}, \overline{G})$ and $(\overline{X}, \overline{G})$ is not the singleton space, then the chain length of (X, G) is equal to the chain length of $(\overline{X}, \overline{G})$.

The following theorem describes the nature of spaces of finite chain length:

Theorem 33. *Every space of orderings of finite chain length is built up, recursively, in an essentially unique way, from singleton spaces, using the direct sum and the group extension constructions.*

The proof of this theorem is quite long and will be omitted - it can be found in [5] on pages 65-82.

27. Isotropy theorem

The importance of spaces of orderings of finite chain length becomes clear from the isotropy theorem:

Theorem 34. *Let (X, G) be a space of orderings and f a form with entries in G. Suppose that f is anisotropic. Then there exists a subspace Y of X of finite chain length such that $f|_Y$ is anisotropic.*

Proof. By Zorn's lemma we have a subspace $Y \subset X$ minimal subject to the condition that $f|_Y$ is anisotropic: if $\{Y_i : i \in I\}$ is a chain of subspaces of X such that $f|_{Y_i}$ is anisotropic and $Y = \bigcap_{i \in I} Y_i$, then $f|_Y$ is anisotropic - otherwise we would have some form g with entries in G with $f \cong (-1, 1) \perp g$ on Y and then, by continuity, $f \cong (-1, 1) \perp g$ on Y_i for some i. Thus $f|_Y$ is anisotropic but $f|_Z$ is isotropic for each proper subspace Z of Y and we want to show that $(Y, G|_Y)$ has finite chain length; to simplify notation we may replace (X, G) by $(Y, G|_Y)$ and and having f anisotropic but $f|_Z$ isotropic for each proper subspace Z of X we want to chow that (X, G) has finite chain length.

Let $n = \dim f$ and suppose that we have a chain $U(a_d) \subsetneq \ldots \subsetneq U(a_0)$ in X. Without loss of generality we may assume that $a_0 = 1$ and $a_d = -1$. Since $U(a_i) \neq U(a_{i+1})$, $a_i \neq a_{i+1}$, that is $a_i a_{i+1} \neq 1$, so $U(a_i a_{i+1})$ is a proper subspace of X. Thus we have a form g_i of dimension $n - 2$ with entries in G such that $f \sim g_i$ on $U(a_i a_{i+1})$, so:

$$f \otimes (1, a_i a_{i+1}) \sim g_i \otimes (1, a_i a_{i+1}), i \in \{0, \ldots, d-1\}.$$

Since $U(a_{i+1}) \subset U(a_i)$, $(1, a_{i+1}) \cong (a_i, a_i a_{i+1})$, so we get:

$$\begin{aligned} (a_0 a_1, a_1 a_2, \ldots, a_{d-1} a_d) &\cong (a_1, a_1 a_2, \ldots, a_{d-1} a_d) \\ &\cong (1, a_2, a_2 a_3, \ldots, a_{d-1} a_d) \\ &\cong (1, 1, a_3, \ldots, a_{d-1} a_d) \\ &\vdots \quad \vdots \\ &\cong (1, 1, \ldots, 1, -1). \end{aligned}$$

Here we use $a_0 = 1$ and $a_d = -1$. Thus by adding the d previous equations and using the above result we get:

$$(2d - 2) \times f \sim \sum_{i=0}^{d-1} g_i \otimes (1, a_i a_{i+1}).$$

But $(2d - 2) \times f$ is anisotropic so, comparing dimensions, we see that $(2d - 2)n \leq 2(n - 2)d$, so $d \leq \frac{n}{2}$. □

There is also an extended version of the isotropy theorem, which should be mentioned:

Theorem 35. *Let (X, G) be a space of orderings and let $f_1, \ldots, f_n$ be forms with entries in G. Then:*

1. *If $\bigcap_{i=1}^{n} D(f_i) = \emptyset$ then there exists a subspace Y of (X, G) of finite chain length such that $\bigcap_{i=1}^{n} D(f_i|_Y) = \emptyset$.*
2. *If $\bigcap_{i=1}^{n} D(f_i) \subset \ker x$ for some $x \in X$, then there exists a subspace Y of (X, G) of finite chain length such that $x \in Y$ and $\bigcap_{i=1}^{n} D(f_i|_Y) \subset \ker x|_Y$.*

The proof is also quite long and will be omitted - it can be found in [1] on pages 111-114.

References

[1] C. Andradas, L. Brocker, J. Ruiz, *Constructible sets in real geometry*, Springer, New York 1996

[2] O. Endler, *Valuation theory*, Springer, New York 1972

[3] A. I. Kostrikin, Yu. I. Manin, *Linear algebra and geometry*, Gordon and Breach, New York 1989

[4] T. Y. Lam, *Orderings, valuations and quadratic forms*, Regional Conference Series in Mathematics 52, AMS, Providence 1983

[5] M. Marshall, *Spaces of orderings and abstract real spectra*, LNM 1636, Springer, New York 1996

[6] M. Marshall, *Open questions in the theory of spaces of orderings*, J. Symb. Logic 67 (2001), 341-352

[7] A. Prestel, *Lectures on formally real fields*, LNM 1093, Springer, New York 1984

[8] K. Szymiczek, *Bilinear algebra: an introduction to the algebraic theory of quadratic forms*, Gordon and Breach, New York 1997