ANNALES
POLONICI MATHEMATICI
XXXVIII (1980)

Grothendieck and Witt groups in the reduced theory of quadratic forms

by ANDRZEJ SŁADEK (Katowice)

Abstract. Let F be a formally real field. Denote by $G(F)$ and $G_t(F)$ the Grothendieck group of quadratic forms over F and its torsion subgroup, respectively. In this paper we study the structure of the factor group $G(F)/G_t(F)$. This reduced Grothendieck group is a free Abelian group. The main results of the paper describe some sets of generators for $G(F)/G_t(F)$, which in many cases allow us to find a basis for the group. Throughout the paper we use the language of the reduced theory of quadratic forms. In the final part of the paper we apply the results to determine completely the structure of the reduced Grothendieck group $G(F)/G_t(F)$ for all fields with $|g(F)| \leqslant 16$, where $g(F)$ is the factor group $F^*/T(F)$, $T(F)$ being the subgroup of all totally positive elements of F.

All the results concerning Grothendieck groups have their counter-parts for Witt groups and we also state and prove the results in that case.

Introduction. Let F be a field and let $G(F)$ denote the Grothendieck group of quadratic forms over F. In [10] it is proved that there exists a free Abelian group $N(F)$ such that $G(F) = G_t(F) \oplus N(F)$, where $G_t(F)$ denotes the torsion subgroup of $G(F)$.

In this paper we are mainly interested in determining the groups $N(F)$ in the above decomposition. If F is a non-real field, then it is well known that $N(F)$ is infinite cyclic. Thus we will investigate here exclusively the case of a formally real field F. In some special cases (e.g. of pythagorean fields satysfying SAP, superpythagorean fields, fields with at most 8 square classes) it is possible to find a basis for the group $N(F)$ but in general this has not been done yet. The main result of this paper describes some sets of generators for $N(F)$, which are smaller then those exhibited in [9] and in many cases allow us to find a basis for $N(F)$.

In discussing the structure of $N(F)$ we use the axiomatic approach to the reduced Grothendieck and Witt groups introduced by Marshall [5].

In the first section we collect the basic facts from the reduced theory of quadratic forms. In the second section we define a partial ordering in the group g of the set of quasi-orderings (X, g). The minimal elements of g are shown to supply some sets of generators for the Grothendieck and

Witt groups of (X, g). These are studied in Section 3. In the final section of the paper we apply the result of Section 3 to determine completely the structure of reduced Grothendieck and Witt groups for all fields with $|g(F)| \leqslant 16$, where $g(F)$ is the factor group $F^*/T(F)$, $T(F)$ being the subgroup of all totally positive elements of F (or, equivalently, the subgroup of all sums of squares).

1. Reduced theory of quadratic forms. In this section we recall the fundamental notions of the reduced theory of quadratic forms along the lines of Marshall [5].

Let g be an elementary 2-group (i.e., $a^2 = 1$ for each $a \in g$) with a distinguished element -1 and let X be any subset of the character group $\chi(g) = \mathrm{Hom}(g, \{1, -1\})$. A form over g of dimension n is a sequence $\varphi = (a_1, \ldots, a_n)$, where $a_1, \ldots, a_n \in g$. The integer $\sigma(\varphi) = \sum_{i=1}^{n} \sigma(a_i)$ will be called the *signature of* φ with respect to $\sigma \in X$, and $\det\varphi = a_1 \cdot \ldots \cdot a_n$ will be called the *determinant of* φ. In the set of forms over g we define the following equivalence relation; forms φ and ψ over g are said to be *equivalent modulo* X ($\varphi = \psi(\mathrm{mod}\, X)$) if and only if $\dim\varphi = \dim\psi$ and $\sigma(\varphi) = \sigma(\psi)$ for all $\sigma \in X$. Clearly, this is an equivalence relation; the equivalence class of the form $\varphi = (a_1, \ldots, a_n)$ will be denoted by $\langle\varphi\rangle = \langle a_1, \ldots, a_n\rangle$. We say that $b \in g$ is represented by the form $\varphi = (a_1, \ldots, a_n)$ (or by the class $\langle\varphi\rangle = \langle a_1, \ldots, a_n\rangle$) modulo X if there exist $b_2, \ldots, b_n$ such that $\varphi = (b, b_2, \ldots, b_n)(\mathrm{mod}\, X)$ $(\langle\varphi\rangle = \langle b, b_2, \ldots, b_n\rangle)$. Denote by $D_X(\langle\varphi\rangle)$ the set of all elements of g represented by $\langle\varphi\rangle$ modulo X.

The set $M(X, g)$ of equivalence classes of forms over g can be made into a commutative semi-ring by defining the addition and multiplication in the following way:

$$\langle a_1, \ldots, a_n\rangle + \langle b_1, \ldots, b_m\rangle = \langle a_1, \ldots, a_n, b_1, \ldots, b_m\rangle,$$

$$\langle a_1, \ldots, a_n\rangle \times \langle b_1, \ldots, b_m\rangle = \langle a_1 b_1, \ldots, a_1 b_m, \ldots, a_n b_1, \ldots, a_n b_m\rangle.$$

Using the family of sets $\Sigma(a, \varepsilon) = \{\sigma \in \chi(g); \sigma(a) = \varepsilon\}$, $a \in g$, $\varepsilon = \pm 1$ as a subbase, we may topologize the character group $\chi(g)$. The topological space $\chi(g)$ is Hausdorff, compact and totally disconnected. The sets $\Sigma(a, \varepsilon)$ are both open and closed. If g is finite, then this topology is discrete.

The pair (X, g) will be called a *set of quasi-orderings* iff it satisfies the following conditions:

O_1: X is a closed subset of $\chi(g)$,

O_2: $\sigma(-1) = -1$ for all $\sigma \in X$,

O_3: $\bigcap_{\sigma \in X} \ker\sigma = \{1\}$,

O_4: if $\langle\varphi_1\rangle, \langle\varphi_2\rangle \in M(X, g)$ and $a \in D_X(\langle\varphi_1\rangle + \langle\varphi_2\rangle)$, then there exist $a_i \in D_X(\langle\varphi_i\rangle)$, $i = 1, 2$, such that $a \in D_X(\langle a_1, a_2\rangle)$.

The main examples of sets of quasi-orderings are obtained in the following way. Let F^* be the multiplicative group of the field F and let $T(F)$ denote the sugbroup of F^* consisting of all totally positive elements of F. If we put $g(F) = F^*/T(F)$ and if $X(F)$ is the set of orderings of F, then for every ordering $P \in X(F)$ there exists exactly one character $\sigma \in \chi(g(F))$ such that $\ker\sigma = P/T(F)$. Thus, we may regard $X(F)$ as a subset of the character group $\chi(g(F))$ and then the pair $(X(F), g(F))$ is a set of quasi-orderings (cf. [5]). The distinguished element -1 in $g(F)$ is in that case the coset $(-1)\cdot T(F)$ and since the field is assumed to be formally real, we have $1 \neq -1$ in $g(F)$.

For any set of quasi-orderings (X, g) the following statements hold true:

(i) $a = b$ if and only if $\sigma(a) = \sigma(b)$ for all $\sigma \in X$.

(ii) If φ, ψ are forms over g and $\varphi = \psi$, then $\det\varphi = \det\psi$.

(iii) If $\langle\varphi\rangle \in M(X, g)$, then $D_X(\langle\varphi\rangle + \ldots + \langle\varphi\rangle) = D_X(\langle\varphi\rangle)$.

(iv) X is finite if and only if g is finite.

(v) If $|g| = 2^n < \infty$, then $n \leqslant |X| \leqslant 2^{n-1}$.

(vi) $D_X(\langle 1, a\rangle)$ is a subgroup of g for each $a \in g$.

The form $\langle 1, -1\rangle$ is called the *hyperbolic plane*, and a form $\langle\varphi\rangle \in M(X, g)$ which can be decomposed into the sum $\langle\varphi\rangle = \langle 1, -1\rangle + \langle\psi\rangle$, $\langle\psi\rangle \in M(X, g)$, is called *isotropic*. If $a \in g$ and $X(a) = \{\sigma \in X; \sigma(a) = 1\}$, then there exists exactly one $\bar\sigma \in \chi(g/D_X(\langle 1, a\rangle))$ such that $\sigma = \bar\sigma \circ c$, where $c\colon g \to g/D_X(\langle 1, a\rangle)$ is the canonical homomorphism. Denote $\bar X(a) = \{\bar\sigma \in \chi(g/D_X(\langle 1, a\rangle)); \sigma \in X(a)\}$. Clearly, $\bar X(a)$ and $X(a)$ are of the same cardinality. Marshall [5] has proved that $(\bar X(a), g/D_X(\langle 1, a\rangle))$ is a set of quasi-orderings.

We denote by $G(X, g)$ the Grothendieck ring of the semiring $M(X, g)$. Since in the additive semigroup $M(X, g)$ the cancellation law holds, $M(X, g)$ is injectively embedded into $G(X, g)$. The factor ring $W(X, g) = G(X, g)/H$, where H denotes the principal ideal generated by the hyperbolic plane, is called the *Witt ring* of (X, g).

The dimension semiring homomorphism $\dim\colon M(X, g) \to Z$ extends uniquely to a ring homomorphism $\dim\colon G(X, g) \to Z$ and the same holds for the signature homomorphism. The kernel of dim will be denoted by $G_0(X, g)$; we have the following direct sum decomposition of the Grothendieck group: $G(X, g) = Z\langle 1\rangle \oplus G_0(X, g)$.

Let $f\colon G(X, g) \to W(X, g)$ be the canonical homomorphism and let $W_0(X, g) = f(G_0(X, g))$. It is easy to see that restricting f to $G_0(X, g)$ we obtain an isomorphism of $G_0(X, g)$ onto $W_0(X, g)$. The ideals $G_0(X, g)$ and $W_0(X, g)$ are additively generated by the sets $\{\langle 1\rangle - \langle a\rangle; a \in g\}$ and $\{\langle 1, a\rangle; a \in g\}$ respectively.

Now we are going to compare the Grothendieck ring $G(F)$ of quadratic forms over the field F and the Grothendieck ring $G(X(F), g(F))$ of the set of quasi-orderings $(X(F), g(F))$, discussed above. Let $h\colon F^* \to g(F)$ be the canonical homomorphism of groups. We put $\bar{h}(\langle a_1, \ldots, a_n\rangle - \langle b_1, \ldots, b_m\rangle) = \langle h(a_1), \ldots, h(a_n)\rangle - \langle h(b_1), \ldots, h(b_m)\rangle$ and we check easily that $\bar{h}\colon G(F) \to G(X(F), g(F))$ is a well defined epimorphism. Pfister's Local-Global Principle asserts that $\ker \bar{h} = G_t(F)$ (see, for example, [10]). It is known that for any field F there exists a free abelian group $N(F)$ such that $G(F) = G_t(F) \oplus N(F)$ (cf. [9], p. 22). Hence $\bar{h}|_{N(F)}\colon N(F) \to G(X(F), g(F))$ is a group isomorphism. This fact motivates our interest in the reduced theory of quadratic forms. It enables us to study the Grothendieck and Witt groups modulo torsion subgroup in a natural way. In the case of a pythagorean field F, we have $G_t(F) = 0$ (cf. [8], Proposition 1.19), so that the reduced theory coincides with the classical theory of quadratic forms.

We shall say that (X, g) satisfies *Strong Approximation Property* (SAP) iff every open and closed subset of X is of the form $X(a) = \{\sigma \in X; \sigma(a) = 1\}$, $a \in g$. If $|g| = 2^n < \infty$, then (X, g) satisfies SAP if and only if $|X| = n$. For a field F, the set of quasi-orderings $(X(F), g(F))$ satisfies SAP if and only if the field F satisfies SAP in the meaning of [2]. If X consists of all σ in $\chi(g)$ such that $\sigma(-1) = -1$, then (X, g) is a set of quasi-orderings, and it will be called *full*. Clearly, if $|g| = 2^n$, then (X, g) is full $\Leftrightarrow |X| = 2^{n-1}$ $\Leftrightarrow D_X(\langle 1, a\rangle) = \{1, a\}$ for all $a \in g - \{1, -1\}$. For example, a set of quasi-orderings $(X(F), g(F))$, where F is a superpythagorean field, is full.

2. Minimal and maximal elements of g. Assume that (X, g) is a set of quasi-orderings. By O_2, the family $H(X, g)$ consisting of sets $X(a) = \{\sigma \in X; \sigma(a) = 1\}$, $a \in g$, is a subbase of a certain topological space which can be viewed as a subspace of the topological space $\chi(g)$.

First we restate some known properties of $H(X, g)$.

LEMMA 2.1 (Craven [1]). *The family $H(X, g)$ with the symmetrical difference is an elementary 2-group isomorphic with g. The mapping $a \mapsto X(-a)$ establishes an isomorphism between g and $H(X, g)$.*

This lemma follows easily from O_2 and O_3.

DEFINITION. For a, b in g, we say that $a \leqslant b$ iff $X(-a) \subset X(-b)$.

By Lemma 2.1, the relation $\leqslant$ is a partial ordering relation in g. Clearly, $1 \leqslant a \leqslant -1$ for all $a \in g$.

DEFINITION. An element $a \in g - \{1, -1\}$ will be called *minimal* (*maximal*) iff it is minimal (maximal) in the partially ordered set $g - \{1, -1\}$.

Denote: $\max(d) = \{a \in g;\ d \leqslant a,\ a \text{ maximal}\}$, $\min(d) = \{a \in g;\ a \leqslant d,\ a \text{ minimal}\}$, $\max(X, g) = \max(1)$, $\min(X, g) = \min(-1)$.

Remarks 2.2. The following observations are easy consequences of the axioms O_2–O_4.

(i) $a \leqslant b \Leftrightarrow D_X(\langle 1, a\rangle) \subset D_X(\langle 1, b\rangle)$,

(ii) $a \leqslant b \Leftrightarrow -b \leqslant -a \Leftrightarrow ab \leqslant b \Leftrightarrow a \leqslant -ab$,

(iii) if $a \leqslant b$ and $c \leqslant b$, then $ac \leqslant b$,

(iv) a is minimal $\Leftrightarrow -a$ is maximal,

(v) if $b \leqslant a$, then

$$\langle 1, -1\rangle + \langle 1, -a\rangle = \langle 1, -b\rangle + \langle 1, -ab\rangle,$$

$$\langle 1\rangle - \langle a\rangle = (\langle 1\rangle - \langle b\rangle) + (\langle 1\rangle - \langle ab\rangle).$$

If X is finite, then

(vi) $\max(b) \neq \emptyset$ and $\min(b) \neq \emptyset$ for every $b \in g - \{1, -1\}$,

(vii) a is minimal $\Leftrightarrow |\min(a)| = 1 \Leftrightarrow |\max(-a)| = 1 \Leftrightarrow |D_X(\langle 1, a\rangle)| = 2$.

Examples. (i) If $a \in g$ and $[g\colon D_X(\langle 1, -a\rangle)] = 2$, then a is minimal;

(ii) A set of quasi-orderings (X, g) is full $\Leftrightarrow \min(X, g) = \max(X, g) = g - \{1, -1\}$.

Proof. (i) $[g\colon D_X(\langle 1, -a\rangle)] = 2 \Leftrightarrow |X(-a)| = 1 \Rightarrow a$ is minimal.

Lemma 2.3. *If X is finite, then $A = \{a \in g;\ |X(-a)| \in 2Z\}$ is a subgroup of g and the index $[g\colon A] \leqslant 2$.*

Proof. For $a \in g$, let the symbol $u(a)$ denote 0 if $|X(-a)|$ is even and 1 if $|X(-a)|$ is odd. The map $u\colon g \to Z/2Z$ is group homomorphism and $\ker u = A$. This completes the proof.

3. Sets of generators for Grothendieck and Witt groups. In order to establish the connection between direct sum decompositions of Grothendieck and Witt groups it is necessary to select in the Grothendieck group a direct summand which contains the kernel of the canonical homomorphism $f\colon G \to W$. In the classical case this has been done in [9] for formally real fields and in [8] for non-real fields. We use here the generalized form of Lemma 1.10 cf. [9].

Lemma 3.1. *Let (X, g) be a set of quasi-orderings and let $\sigma \in X$. Then $Z\langle 1\rangle$, $Z(\langle 1\rangle - \langle -1\rangle)$ are infinite cyclic groups and*

$$G(X, g) = Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle -1\rangle) \oplus G_1,$$

where G_1 is the group additively generated by all elements $\langle 1\rangle - \langle a\rangle$, $a \in \ker\sigma$.

Proof. It suffices to show that $G_0(X, g) = Z(\langle 1\rangle - \langle -1\rangle) \oplus G_1$. By Remarks 2.2(v), $G_0(X, g) = Z(\langle 1\rangle - \langle -1\rangle) + G_1$. Now, let $n(\langle 1\rangle - \langle -1\rangle) = \sum n_i(\langle 1\rangle - \langle a_i\rangle) \in Z(\langle 1\rangle - \langle -1\rangle) \cap G_1$. Then $\varphi = n\langle 1\rangle + \sum n_i\langle a_i\rangle = (\sum n_i)\langle 1\rangle + n\langle -1\rangle = \psi$. Taking the value of the signature map σ on φ and ψ we obtain the equality $n + \sum n_i = \sum n_i - n$. Hence $n = 0$ and the proof is finished.

COROLLARY 3.2. *Let $G(X, g)$ be decomposed as in Lemma* 3.1. *Then* $W(X, g) = Z\langle 1\rangle \oplus f(G_1)$, *where f is the canonical homomorphism $G(X, g)$ onto $W(X, g)$. Moreover, G_1 and $f(G_1)$ are isomorphic.*

Proof. It suffices to notice that $Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle -1\rangle) = \ker f \oplus Z\langle 1\rangle$.

The following theorem contains the basic general information about the structure of the Grothendieck and Witt groups for the sets of quasi-orderings.

THEOREM 3.3. *Let (X, g) be a set of quasi-orderings. Then $G(X, g)$ and $W(X, g)$ are free abelian groups. If X is finite, then* $\operatorname{rank} G(X, g) = 1 + \operatorname{rank} W(X, g) = |X|+1$. *Otherwise,* $\operatorname{rank} G(X, g) = \operatorname{rank} W(X, g) = |g|$.

Proof. By Corollary 3.2 it suffices to consider the group $G(X, g)$. Let Y denote the subgroup of Z^X consisting of all bounded maps from X into Z. By the theorem of Nöbeling [6], Y is a free abelian group. Consider the signature homomorphism $\sigma\colon G(X, g) \to Z$. Putting $(F(A))(\sigma) = \sigma(A)$, $A \in G_0(X, g)$, we obtain an injection $F\colon G_0(X, g) \to Y$. Hence $G_0(X, g)$ and also $G(X, g)$ are free abelian groups.

At first, assume that X is finite. From the first part of the proof we obtain the inequality: $\operatorname{rank} G_0(X, g) \leqslant |X|$. Let $X = \{\sigma_1, \ldots, \sigma_r\}$ and $|g| = 2^{k+1}$. If $\ker\sigma_i = \{1, a_{i1}\} \times \ldots \times \{1, a_{ik}\}$ and $A_i = (\langle 1\rangle - \langle a_{i1}\rangle) \times \ldots \times (\langle 1\rangle - \langle a_{ik}\rangle)$, then $F(A_i)(\sigma_j) = \delta_{ij} 2^k$. Thus, the set $\{A_1, \ldots, A_r\}$ is independent, and $\operatorname{rank} G_0(X, g) \geqslant |X|$. Since $G(X, g) = Z\langle 1\rangle \oplus G_0(X, g)$, we have $\operatorname{rank} G(X, g) = |X|+1$.

Now, assume that X is infinite. In this case $G(X, g)$ is not finitely generated and $\operatorname{rank} G(X, g) = |G(X, g)|$. Since $G(X, g)$ consists of differences of finite sequences of elements of g, we have $|G(X, g)| = |g|$. Hence the result.

We have seen that the set $\{\langle 1\rangle - \langle a\rangle;\ a \in g\}$ generates the group $G_0(X, g)$ but its cardinality is always greater than rank $G_0(X, g)$. In subsequent theorems we shall find another set of generators for $G_0(X, g)$, which is much smaller and in some cases forms a free basis for the group. For this purpose we want each element $\langle 1\rangle - \langle a\rangle$, $a \in g$, to be a sum of the new generators.

LEMMA 3.4. *Let (X, g) be a finite set of quasi-orderings and let $d \in g - \{1\}$. Then*

(i) *in* $G(X, g)$

$$\langle 1\rangle - \langle d\rangle = \sum_{a \in \min(d)} \delta(a)(\langle 1\rangle - \langle a\rangle),$$

(ii) *in* $W(X, g)$

$$\langle 1, -d\rangle = \sum_{a \in \min(d)} \delta(a)\langle 1, -a\rangle,$$

where $\delta(a) = 0$ *or* $\delta(a) = 1$. *For any* $a \in \min(d)$ *there exists a representation of* $\langle 1\rangle - \langle d\rangle$ *and of* $\langle 1, -d\rangle$ *such that* $\delta(a) = 1$.

Proof. (i) We proceed by induction on $k = |\min(d)|$. First suppose $k = 1$. Since, by Remarks 2.2(vii), $\min(d) = \{d\}$, we get the result. Now assume $k > 1$ and $a \in \min(d)$. By Remarks 2.2 we have

$$\langle 1\rangle - \langle d\rangle = (\langle 1\rangle - \langle a\rangle) + (\langle 1\rangle - \langle ad\rangle)$$

and $\emptyset \neq \min(da) \subset \min(d) - \{a\}$.

To finish the proof, we apply the induction assumption to $\langle 1\rangle - \langle da\rangle$.

(ii) It follows from (i) because $f(\langle 1\rangle - \langle a\rangle) = \langle 1, -a\rangle$ ($f\colon G(X, g) \to W(X, g)$ is the canonical homomorphism). The lemma is proved.

COROLLARY 3.5. *If* X *is finite, then every element* $X(d)$ *of the family* $H(X, g)$ *is a disjoint union of minimal elements of* $H(X, g)$.

Proof. This follows from Lemma 3.4. Let $\langle 1\rangle - \langle -d\rangle = \sum(\langle 1\rangle - \langle -a_i\rangle)$, where $-a_i$ are some minimal elements of $\min(-d)$, i.e., $X(a_i)$ are minimal elements of $H(X, g)$. It suffices to notice that $X(d) = \{\sigma \in X;\ \sigma(\langle 1\rangle - \langle -d\rangle) = 2\}$. Hence, $X(d) = \bigcup X(a_i)$ and $X(a_i) \cap X(a_j) = \emptyset$ for $i \neq j$.

THEOREM 3.6. *Let* (X, g) *be a finite set of quasi-orderings and let us denote by* (A) *the group generated by the set* A. *If* $\min(X, g) \neq \emptyset$, *then*

$$\text{(i)}\quad G_0(X, g) = \big(\{\langle 1\rangle - \langle a\rangle;\ a \in \min(X, g)\}\big) = Z(\langle 1\rangle - \langle -1\rangle) \oplus \big(\{\langle 1\rangle - \langle a\rangle;\ a \in \min(X, g) \cap \ker\sigma\}\big),$$

$$\text{(ii)}\quad W_0(X, g) = \big(\{\langle 1, -a\rangle;\ a \in \min(X, g)\}\big) = Z\langle 1, 1\rangle \oplus \big(\{\langle 1, -a\rangle;\ a \in \min(X, g) \cap \ker\sigma\}\big),$$

where σ *is any element of* X.

Proof. It suffices to prove (i). The additive group $G_0(X, g)$ is generated by all elements $\langle 1\rangle - \langle d\rangle$, where $d \in g$. By Lemma 3.4 we obtain $G_0(X, g) = \big(\{\langle 1\rangle - \langle a\rangle;\ a \in \min(X, g)\}\big)$. Consider the group G_1 generated by all elements $\langle 1\rangle - \langle d\rangle$, where $d \in \ker\sigma$. If $d \in \ker\sigma$, then $\min(d) \subset \ker\sigma$. Hence, by Lemma 3.4(i), $G_1 = \big(\{\langle 1\rangle - \langle a\rangle;\ a \in \min(X, g) \cap \ker\sigma\}\big)$. Applying Lemma 3.1, we get the result.

It is worth while noticing that $\min(X, g) = \emptyset$ iff $|g| \leqslant 2$ and then $G_0(X, g) = Z(\langle 1\rangle - \langle -1\rangle)$.

An interesting question arises: when do the sets of generators occurring in Theorem 3.6 form free bases for $G_0(X, g)$ and $W_0(X, g)$? A partial answer is furnished by the next theorem.

THEOREM 3.7. *If* (X, g) *is a finite set of quasi-orderings with* $\min(X, g) \neq \emptyset$, *then the following statements are equivalent*:

(i) $A = \{\langle 1\rangle - \langle a\rangle\colon a \in \min(X, g)\}$ *is a free basis for the group* $G_0(X, g)$,

(ii) $Y = \{\langle 1\rangle - \langle a\rangle; [g\colon D_X(\langle 1, -a\rangle)] = 2\}$ *is a free basis for* $G_0(X, g)$,

(iii) (X, g) *satisfies SAP*,

(iv) $A = Y$.

Proof. (i) $\Rightarrow$ (iii). Let $X = \{\sigma_1, \ldots, \sigma_r\}$ and $A(\sigma) = A \cap \ker\sigma$, where σ denotes the signature map with respect to $\sigma \in X$. By Lemma 3.3 and Theorem 3.6, we see that $|A| = r$ and for every $\sigma_j \in X$ we have $|A(\sigma_j)| = r-1$. Hence for every $\sigma_i \in X$ there exists exactly one $a_i \in \min(X, g)$ such that $\sigma_j(a_i) = (-1)^{\delta_{ij}}$, i.e., $X(-a_i) = \{\sigma_i\}$. Since X is finite, the topology on X is discrete and every subset of X is open and closed. Clearly, $\{\sigma_{i_1}, \ldots, \sigma_{i_k}\} = X(-a_{i_1}) \cup \ldots \cup X(-a_{i_k}) = X(-a_{i_1} \cdot \ldots \cdot a_{i_k})$. Hence (X, g) satisfies SAP.

(iii) $\Rightarrow$ (ii), (iv). Assume that (X, g) satisfies SAP. Then for every $\sigma \in X$ there exists $a \in g$ such that $X(a) = \{\sigma\}$; moreover, a is minimal if and only if $|X(-a)| = 1$ (i.e., $[g\colon D_X(\langle 1, -a\rangle)] = 2$). Thus, $A = Y$, $|Y| = |X| = \operatorname{rank} G_0(X, g)$ and $G_0(X, g) = (Y)$. In this case Y is a free basis for $G_0(X, g)$.

(ii) $\Rightarrow$ (i), (iii). Let $|g| = 2^n$ and $|X| = r$. If $Y = \{\langle 1\rangle - \langle a_i\rangle\}_{1\leqslant i\leqslant k}$, then $a_1, \ldots, a_k$ are independent elements of g. Notice that $|A| \geqslant r \geqslant n \geqslant |Y|$. If Y is a free basis, then $|Y| = n = r$ (by Section 2 this is equivalent to (iii)). Since (iii) $\Rightarrow$ (iv), we get (i). At the same time (ii) $\Rightarrow$ (iv) is proved.

Now, (iv) implies that $r = n$ and this is equivalent to (iii). The theorem is proved.

The last theorem gives a characterization of (X, g) satisfying SAP. M. Kula (cf. [3]) has shown that for any pythagorean field F the sentences (ii), (iii) of Theorem 3.7 are equivalent.

Let $B(\sigma) = \{\langle 1\rangle - \langle -1\rangle\} \cup A(\sigma)$, $\sigma \in X$. By Theorem 3.6 we see that $G_0(X, g) = (B(\sigma))$. If (X, g) satisfies SAP or is full, then $|B(\sigma)| = |X|$ and therefore $B(\sigma)$ is a free basis for $G_0(X, g)$. In the next part of this paper we show an example of (X, g) such that $B(\sigma_1)$ is independent and $B(\sigma_2)$ is dependent for some $\sigma_1, \sigma_2 \in X$. There exists also (X, g) with the property that $B(\sigma)$ is dependent for all $\sigma \in X$. However, sometimes one can choose a basis for $G_0(X, g)$ from $B(\sigma)$.

COROLLARY 3.8. *Let X be finite.*

(i) *If* $m = |\min(X, g)|$, *then* $|X| \leqslant m \leqslant |g| - 2$.

The first inequality is an equality iff (X, g) satisfies SAP.

The second inequality is an equality iff (X, g) is full.

(ii) *If* $\sigma \in X$, *then* $|X| - 1 \leqslant |A(\sigma)| \leqslant \frac{1}{2}|g| - 1$.

Remarks.

(3.9) It is worth while noticing that $|\min(X(F), g(F))|$ is an invariant of the GR-equivalence in the meaning of [8], [10].

(3.10) There is an obvious analogue of Theorem 3.7 for the Witt group $W(X, g)$. One can just take $f(A)$, $f(Y)$ and $W_0(X, g)$ instead of A, Y and $G_0(X, g)$, where f is the canonical homomorphism f: $G(X, g) \to W(X, g)$.

4. Grothendieck and Witt groups for fields with $|g(F)| \leqslant 16$. In this section we show that the results of the previous section are precise enough to determine explicity the reduced Grothendieck and Witt groups for all fields with $|g(F)| \leqslant 16$. Of course, this class of fields contains all formally real fields with at most 16 square classes, but it also contains many fields with infinite group of square classes; for the example, the rationals.

First, we prepare a lemma which establishes the connection between $G(F)$ and $G(X(F), g(F))$.

LEMMA 4.1. *Let F be a formally real field and let the maps h, $\bar{h}$ be as in Section* 1. *Denote $A = \{A_1, \ldots, A_r\} \subset G_0(F)$.*

(i) *If $\bar{h}(A)$ generates $G_0(X(F), g(F))$, then*

$$G_0(F) = G_t(F) + (A).$$

(ii) *If $\bar{h}(A)$ is a free basis for $G_0(X(F), g(F))$, then*

$$G_0(F) \doteq G_t(F) \oplus ZA_1 \oplus \ldots \oplus ZA_r.$$

Proof. The map $\bar{h}|_{G_0(F)}$: $G_0(F) \to G_0(X(F), g(F))$ is surjective and $G_0(X(F), g(F))$ is a free Abelian group with $\ker \bar{h} = G_t(F)$. By a well-known theorem on Abelian groups, $\ker \bar{h}$ is a direct summand of $G_0(F)$ and we may take the complementary direct summand to satisfy the requirements of (ii) (cf. [4], p. 44). Hence the result.

We are now going to study the structure of Grothendieck and Witt groups of quadratic forms over fields F with $|g(F)| \leqslant 16$.

We shall use the sets of generators for $G(X(F), g(F))$ found in foregoing section to the construction of a free basis for the "free part" of $G(F)$. Let us first recall that $n \leqslant |X| \leqslant 2^{n-1}$ if $|g| = 2^n$ (cf. (v), Section 1). Moreover, in the case of $n = 4$, we have $|X| \neq 7$, as proved by Marshall [5]. The transition from the decomposition of the Grothendieck group $G(F)$ to the decomposition of the Witt group $W(F)$ will be accomplished along the same lines as this is done in Theorem 1.2 of [8].

We consider below all the possible cases.

Case I. $|g(F)| = 2$. Since $\min(X(F), g(F)) = \emptyset$, we see that

$$G(F) = Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle -1\rangle) \oplus G_t(F),$$

and

$$W(F) = Z\langle 1\rangle \oplus W_t(F).$$

Case II. $|g(F)| = 2^2$. The set of quasi-orderings satisfies SAP

Therefore $\min|(X(F), g(F))| = 2$. Let $\min(X(F), g(F)) = \{\bar{a}, \bar{b}\}$; here and throughout the remainder of the paper $\bar{a}$ denotes $h(a)$, for $a \in F^*$. Then

$$\begin{aligned} G(F) &= Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle a\rangle) \oplus Z(\langle 1\rangle - \langle b\rangle) \oplus G_t(F) \\ &= Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle -1\rangle) \oplus Z(\langle 1\rangle - \langle a\rangle) \oplus G_t(F), \\ W(F) &= Z\langle 1\rangle \oplus Z\langle 1, -a\rangle \oplus W_t(F), \end{aligned}$$

where a can be changed into b, by Theorem 3.6.

Case III. $|g(F)| = 2^3$.

(i) $|X(F)| = 3$. Then $(X(F), g(F))$ satisfies SAP, $|\min(X(F), g(F))|$, $= 3$ and, for every $\sigma \in X(F)$, $|\min(X(F), g(F)) \cap \ker\sigma| = 2$. Let $\min(X(F), g(F)) = (\min(X(F), g(F)) \cap \ker\sigma) \cup \{\bar{c}\} = \{\bar{a}, \bar{b}, \bar{c}\}$. In view of 3.1, 3.2, 3.7, 4.1 we may write

$$\begin{aligned} G(F) &= Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle a\rangle) \oplus Z(\langle 1\rangle - \langle b\rangle) \oplus Z(\langle 1\rangle - \langle c\rangle) \oplus G_t(F) \\ &= Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle -1\rangle) \oplus Z(\langle 1\rangle - \langle a\rangle) \oplus Z(\langle 1\rangle - \langle b\rangle) \oplus G_t(F), \\ W(F) &= Z\langle 1\rangle \oplus Z\langle 1, -a\rangle \oplus Z\langle 1, -b\rangle \oplus W_t(F). \end{aligned}$$

(ii) $|X(F)| = 4$. The set of quasi-orderings $(X(F), g(F))$ is full and therefore for each $\sigma \in X(F)$ we have $|\min(X(F), g(F)) \cap \ker\sigma| = 3$ (Corollary 3.8(iii)). If $\min(X(F), g(F)) \cap \ker\sigma = \{\bar{a}, \bar{b}, \bar{c}\}$, then we get the following decompositions:

$$\begin{aligned} G(F) &= Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle -1\rangle) \oplus Z(\langle 1\rangle - \langle a\rangle) \oplus Z(\langle 1\rangle - \langle b\rangle) \oplus \\ &\quad \oplus Z(\langle 1\rangle - \langle c\rangle) \oplus G_t(F), \\ W(F) &= Z\langle 1\rangle \oplus Z\langle 1, -a\rangle \oplus Z\langle 1, -b\rangle \oplus Z\langle 1, -c\rangle \oplus W_t(F). \end{aligned}$$

Case IV. $|g(F)| = 2^4$.

(i) $|X(F)| = 4$, i.e. $(X(F), g(F))$ satisfies SAP. Then we can write $\min(X(F), g(F)) = (\min(X(F), g(F)) \cap \ker\sigma) \cup \{\bar{d}\} = \{\bar{a}, \bar{b}, \bar{c}, \bar{d}\}$, where $\sigma \in X(F)$. In view of 3.2, 3.7 and 4.1 we have

$$\begin{aligned} G(F) &= Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle a\rangle) \oplus Z(\langle 1\rangle - \langle b\rangle) \oplus Z(\langle 1\rangle - \langle c\rangle) \oplus Z(\langle 1\rangle - \\ &\quad - \langle d\rangle) \oplus G_t(F) \\ &= Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle -1\rangle) \oplus Z(\langle 1\rangle - \langle a\rangle) \oplus Z(\langle 1\rangle - \langle b\rangle) \oplus Z(\langle 1\rangle - \\ &\quad - \langle c\rangle) \oplus G_t(F), \\ W(F) &= Z\langle 1\rangle \oplus Z\langle 1, -a\rangle \oplus Z\langle 1, -b\rangle \oplus Z\langle 1, -c\rangle \oplus W_t(F). \end{aligned}$$

(ii) $|X(F)| = 5$. We do not know any example of a field satisfying this condition(1), but there is known a construction of a set of quasi-orderings (X, g) for which $|X| = 5$ and $|g| = 2^4$. We shall find a basis for $G(X, g)$ in this case.

---

(1) For construction of such field see M. Kula, *Fields with prescribed quadratic form schemes*, Math. Z. 167 (1979), p. 201–212.

Arguing as in the proof of Lemma 4.2(i) we observe that $\bar{a} \in \min(X, g) \Leftrightarrow 3 \leqslant |X(\bar{a})| \leqslant 4 \Leftrightarrow 1 \leqslant |X(-\bar{a})| \leqslant 2$. By Corollary 3.5 we have $X = \bigcup X(-\bar{a}_i)$ for some $\bar{a}_i \in \min(X, g)$ such that $X(-\bar{a}_i) \cap X(-\bar{a}_j) = \emptyset$, $i \neq j$. There is only one possibility: $X = X(-\bar{a}_1) \cup X(-\bar{a}_2) \cup X(-\bar{a}_3)$ and $X(-\bar{a}_1) = \{\sigma_1\}$, $X(-\bar{a}_2) = \{\sigma_2, \sigma_3\}$, $X(-\bar{a}_3) = \{\sigma_4, \sigma_5\}$ (in any other case the first inequality in Corollary 3.8(i) does not hold). Since $X(-\bar{a}_1)$ contains only one element, then for $\bar{a} \in \min(X, g) - \{\bar{a}_1\}$ the sets $X(-\bar{a}_1)$ and $X(-\bar{a})$ are disjoint. Since the pair (X, g) does not satisfy SAP, by Corollary 3.8, $|\min(X, g)| \geqslant 6$. There is only one possibility, namely, that $\min(X, g) = \{\bar{a}_1, \ldots, \bar{a}_7\}$ and $X(-\bar{a}_1) = \{\sigma_1\}$, $X(-\bar{a}_2) = \{\sigma_2, \sigma_3\}$,

$$X(-\bar{a}_3) = \{\sigma_4, \sigma_5\}, \quad X(-\bar{a}_4) = \{\sigma_2, \sigma_4\}, \quad X(-\bar{a}_5) = \{\sigma_3, \sigma_5\},$$
$$X(-\bar{a}_6) = \{\sigma_2, \sigma_5\}, \quad X(-\bar{a}_7) = \{\sigma_3, \sigma_4\}.$$

Since the set $B(\sigma_1) = \{\langle 1\rangle - \langle -1\rangle\} \cup \{\langle 1\rangle - \langle \bar{a}\rangle;\ \bar{a} \in \min(X, g) \cap \ker\sigma_1\}$ contains 7 elements, it is dependent. For $i = 2, \ldots, 5$ the sets $B(\sigma_i)$ are free bases for $G_0(X, g)$. For example, $B(\sigma_2) = \{\langle 1\rangle - \langle -1\rangle, \langle 1\rangle - \langle \bar{a}_1\rangle, \langle 1\rangle - \langle \bar{a}_3\rangle, \langle 1\rangle - \langle \bar{a}_5\rangle, \langle 1\rangle - \langle \bar{a}_7\rangle\}$. If there exists a field F which might be the object of our present considerations, then

$$G(F) = Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle -1\rangle) \oplus Z(\langle 1\rangle - \langle a_1\rangle) \oplus Z(\langle 1\rangle - \langle a_3\rangle) \oplus$$
$$\oplus Z(\langle 1\rangle - \langle a_5\rangle) \oplus Z(\langle 1\rangle - \langle a_7\rangle) \oplus G_t(F),$$
$$W(F) = Z\langle 1\rangle \oplus Z\langle 1, -a_1\rangle \oplus Z\langle 1, -a_3\rangle \oplus Z\langle 1, -a_5\rangle \oplus Z\langle 1, -a_7\rangle \oplus$$
$$\oplus W(F).$$

(iii) $|X(F)| = 6$.

LEMMA 4.2. *Let (X, g) be a set of quasi-orderings such that $|g| = 2^4$ and $|X| = 6$. Then*

(i) $a \in \min(X, g) \Leftrightarrow 3 \leqslant |X(a)| \leqslant 4 \Leftrightarrow 2 \leqslant |X(-a)| \leqslant 3$,

(ii) *for $A = \{a \in g\colon |X(-a)| \in 2Z\}$ (it is a group), we have $[g\colon A] = 2$.*

Proof. (i) Assume $a \in \min(X, g)$. Then $|g/D_X(\langle 1, a\rangle)| = 2^3$. Since the pair $(\bar{X}(a), g/D_X(\langle 1, a\rangle))$ is a set of quasi-orderings and since $|\bar{X}(a)| = |X(a)|$, we get $3 \leqslant |X(a)| \leqslant 2^2$. Now, suppose $a \notin \min(X, g)$, i.e., $|g/D_X(\langle 1, a\rangle)| \leqslant 2^2$. Hence $|\bar{X}(a)| = |X(a)| \leqslant 2$, contradicting the second condition. Now it suffices to note that $|X(-a)| = |X| - |X(a)|$.

(ii) Assume $[g\colon A] \neq 2$, i.e., $[g\colon A] = 1$ (by Lemma 2.3). Then, by Remark 2.2 and Lemma 4.2(i), $\min(X, g) = \{a \in g\colon |X(-a)| = 2\}$, $\max(X, g) = \{a \in g\colon |X(-a)| = 4\}$ and $|\min(X, g)| = |\max(X, g)| = \frac{1}{2}|g - \{1, -1\}| = 7$.

Since $\max(X, g)$ and $\min(X, g)$ are disjoint and $\max(X, g) \cup \min(X, g) = g - \{1, -1\}$, by Corollary 3.8 we have for every $\sigma \in X$

$$|\max(X, g) \cap \ker\sigma| = |(g - \{1, -1\}) \cap \ker\sigma| - |\min(X, g) \cap \ker\sigma| \leqslant 7 - 5 = 2.$$

Now, the mapping $\max(X, g) \to 2^X$ defined by $a \mapsto X(a)$ is injectiv e and, as shown above, $|X(a)| = 2$ for every $a \in \max(X, g)$ and $X(a_1) \cap \cap X(a_2) \cap X(a_3) = \emptyset$ for every three different elements a_1, a_2, a_3 of $\max(X, g)$. Hence the number of elements of $\max(X, g)$ is not greater than the number of 2-element subsets of a 6-element set which have the property that the intersection of any three of them is empty. We get a contradiction: $7 = |\max(X, g)| \leqslant 6$. This finishes the proof.

Let $X(F) = \{\sigma_1, \ldots, \sigma_6\}$. By Lemma 4.2 we may decompose $g(F)$ in the following way:

$$g(F) = \{1, -1\} \times \{1, \bar{a}\} \times \{1, \bar{b}\} \times \{1, \bar{t}\}$$

and

$$X(\bar{a}) = \{\sigma_1, \sigma_2, \sigma_4, \sigma_5\}, \qquad X(\bar{b}) = \{\sigma_1, \sigma_3, \sigma_4, \sigma_6\}, \qquad X(\bar{t}) = \{\sigma_1, \sigma_2, a_3\}.$$

It is easy to see that $\left|\min\left(X(F), g(F)\right) \cap \ker \sigma\right| = 6$ for each $\sigma \in X(F)$. Then the set $B(\sigma)$ is dependent for each $\sigma \in X(F)$. Yet, we shall show that $B(\sigma)$ contains a basis set for $G_0\left(X(F), g(F)\right)$. Let, for example, $\sigma = \sigma_1$. Then $B(\sigma_1) = \{\langle 1\rangle - \langle -1\rangle, \langle 1\rangle - \langle \bar{a}\rangle, \langle 1\rangle - \langle \bar{b}\rangle, \langle 1\rangle - \langle \bar{t}\rangle, \langle 1\rangle - \langle \bar{a}\bar{t}\rangle, \langle 1\rangle - \langle \bar{b}\bar{t}\rangle, \langle 1\rangle - \langle \bar{a}\bar{b}\bar{t}\rangle\}$. Since

$$\langle 1\rangle - \langle \bar{a}\bar{b}\bar{t}\rangle = (\langle 1\rangle - \langle \bar{a}\bar{t}\rangle) + (\langle 1\rangle - \langle \bar{b}\bar{t}\rangle) - (\langle 1\rangle - \langle \bar{t}\rangle),$$

the set $B(\sigma_1) - \{\langle 1\rangle - \langle \bar{a}\bar{b}\bar{t}\rangle\}$ forms a free basis for $G_0\left(X(F), g(F)\right)$. Hence

$$\begin{aligned} G(F) &= Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle -1\rangle) \oplus Z(\langle 1\rangle - \langle a\rangle) \oplus Z(\langle 1\rangle - \langle b\rangle) \oplus Z(\langle 1\rangle - \\ &\quad - \langle t\rangle) \oplus Z(\langle 1\rangle - \langle at\rangle) \oplus Z(\langle 1\rangle - \langle bt\rangle) \oplus G_t(F), \end{aligned}$$

$$\begin{aligned} W(F) &= Z\langle 1\rangle \oplus Z\langle 1, -a\rangle \oplus Z\langle 1, -b\rangle \oplus Z\langle 1, -t\rangle \oplus Z\langle 1, -at\rangle \oplus \\ &\quad \oplus Z\langle 1, -bt\rangle \oplus W_t(F). \end{aligned}$$

This case takes place when F is the power series field $k((t))$ over a SAP pythagorean field k with three orderings (cf. [2]).

(iv) $|X(F)| = 8$, i.e. $\left(X(F), g(F)\right)$ is a full set of guasi-orderings. By Corollary 3.8,

$$G(F) = Z\langle 1\rangle \oplus Z(\langle 1\rangle - \langle -1\rangle) \oplus M \oplus G_t(F),$$

where

$$M = \bigoplus_{\dot{a} \in \ker\sigma - \{1\}} Z(\langle 1\rangle - \langle a\rangle), \qquad \sigma \in X(F)$$

and

$$W(F) = Z\langle 1\rangle \oplus N \oplus W_t(F),$$

where

$$N = \bigoplus_{\bar{a} \in \ker\sigma - \{1\}} Z\langle 1, -a\rangle, \qquad \sigma \in X(F).$$

References

[1] T. C. Craven, *The topological space of orderings of a rational function field*, Duke Math. J. 41 (1974), p. 339–347.

[2] R. Elman and T. Y. Lam, *Quadratic forms over formally real fields and pythagorean fields*, Amer. J. Math. 94 (1972), p. 1155–1194,

[3] M. Kula, *Ordered fields and quadratic forms over pythagorean fields*, Prace Naukowe Uniw. Śl., Katowice 158, Prace Mat. 7 (1977), p. 13–21.

[4] S. Lang, *Algebra*, 3rd printing, Reading (1971).

[5] M. Marshall, *A reduced theory of quadratic forms*, Preprint (1975).

[6] G. Nöbeling, *Verallgemeinerung eines Satzes von Herrn E. Specker*, Invent. Math. 6 (1968), p. 41–55.

[7] A. Sładek, *Grothendieck groups of quadratic forms over formally real fields*, Prace Naukowe Uniw. Śl., Katowice, Prace Mat. 5 (1974), p. 41–47.

[8] K. Szymiczek, *Quadratic forms over fields*, Diss. Math. 152 (1977).

[9] — *Quadratic forms over fields with finite square classes*, Acta Arith. 28 (1975), p. 195–221.

[10] — *Formy kwadratowe nad ciałami*, Prace Naukowe Uniw. Śl. Katowice 134 (1976).

Reçu par la Rédaction le 12. 10. 1976