ACTA ARITHMETICA
XXVIII (1975)

Quadratic forms over fields with finite square class number

by

K. Szymiczek (Katowice)

Introduction. Throughout the paper, k denotes a field of characteristic other than 2 and $g(k) = k^*/k^{*2}$. We denote by q the square class number of k, that is, $q = |g(k)|$.

In this paper we investigate the behaviour of the set of equivalence classes of quadratic forms over k with respect to orthogonal sum of quadratic forms. This behaviour is characterized by the structure of Grothendieck group $G(k)$ of quadratic forms over k.

In Section 2 we describe completely the groups $G(k)$ for all fields with $q \leqslant 8$, by giving a decomposition of $G(k)$ into direct sum of cyclic groups and determining generators for the direct summands. It turns out that in the case of fields with $q = 8$ there are at most 13 non-isomorphic groups $G(k)$, 7 for non-real fields and 6 for real fields. A satisfactory feature of the classification is that the type of $G(k)$ is completely determined by the behaviour of binary quadratic forms over the field k and by the reality of k.

Another classification of Grothendieck groups has been supplied by W. Scharlau [12]. He classifies the groups $G(k)$ for fields with the property that the subgroup $B_2(k)$ of the Brauer group $B(k)$ consisting of elements of order $\leqslant 2$ has at most 4 elements. This class of fields contains even some fields with infinite square class number but it does not contain all the fields with $q = 8$. In fact, if $Q(k)$ denotes the number of non-isomorphic quaternion algebras over k, then clearly $Q(k) \leqslant |B_2(k)|$, so Scharlau's classification covers at most the fields with $Q \leqslant 4$. Now, as proved by L. Szczepanik [15], in 5 of the 13 cases of fields with $q = 8$ we have $Q > 4$, hence those 5 cases do not fall under Scharlau's assumption (these are the cases IV and VII of Theorem 2.4 and IV, V, VI of Theorem 2.5 below). Moreover, Scharlau gives details only in the case $|B_2(k)| = 2$ and for fields k with $|B_2(k)| = 4$ he gives only possible types of $G(k)$ modulo a subgroup of exponent 2, without specifying the properties of fields determining the type of $G(k)$.

In Section 3 we obtain easily a parallel classification of Witt groups $W(k)$ of anisotropic quadratic forms over fields k with $q \leqslant 8$. In the case of non-real fields with $q \leqslant 8$ a classification of Witt groups has been given in a recent paper of C. M. Cordes [1]. While the type of $W(k)$ in the present paper depends only on the behaviour of binary forms over k, Cordes uses the u-invariant and the number Q of quaternion algebras to differentiate between the cases.

Let us describe briefly the contents of the two remaining sections. Section 1 contains a general study of sets of generators for the group $G(k)$, mostly without assuming that q is finite. In particular, in the case of a real field, we relate the structure of $G(k)$ to the number of orderings of k and investigate the influence of some extremal behaviour of binary forms over k on the number of orderings of the field (Proposition 1.22) and on the structure of $G(k)$ (Propositions 1.11 and 1.23).

In Section 4 we collect a number of examples of fields with $q = 8$ showing that all the cases, with the possible exception of two, of the classification theorems for Grothendieck groups actually do occur.

Notation. A diagonalized quadratic form $f = a_1x_1^2+\ldots+a_nx_n^2$, where $a_i \in k^*$, will be denoted by $f = (a_1, \ldots, a_n)$ and its equivalence class by $\langle f\rangle = \langle a_1, \ldots, a_n\rangle$. For $a \in k^*$ we shall use the bold-faced $\boldsymbol{a}$ to denote the canonical image of a in $g(k)$, i.e., $\boldsymbol{a} = ak^{*2}$. If a quadratic form f represents an element a in k^*, we write $f \approx a$. If $f \approx a$, then f represents all the elements of $\boldsymbol{a}$; so we can speak of the representability of elements of $g(k)$ by a quadratic form. The subset of $g(k)$ represented by a form f will be denoted $D(f)$. The number of elements of $g(k)$ represented by the form $(1, 1)$ will be denoted by q_2. Thus $q_2 = |D(1, 1)|$. If $q_2 = 1$, the field is said to be pythagorean. A form f is said to be universal if it represents all the elements of k^* (or equivalently, if $D(f) = g(k)$).

If k is non-real, we write $s = s(k)$ for the stufe of k. Thus s is the minimal number of summands in a representation of -1 as a sum of squares. The stufe is always a power of two, as proved by A. Pfister in 1965 (cf. [11]).

Infinite cyclic group will be denoted by $\boldsymbol{Z}$ (the group of rational integers) and a cyclic group of order n by $\boldsymbol{Z}/n\boldsymbol{Z}$. A direct sum of n copies of a group G will be denoted by $G^{(n)}$. If G is a group and S is a subset of G, then we denote by $[S]$ the subgroup generated by S.

To avoid repetitions, let it be agreed that "field" will always mean "field of characteristic other than 2" and "form" will mean "a non-singular quadratic form".

1. Sets of generators for the Grothendieck group. We refer to [7], [10] and [13] for basic facts from the theory of quadratic forms over fields. Let k be a field and $G(k)$ its Grothendieck group of quadratic forms.

In this section we do not assume that the square class number of k is finite, unless otherwise stated. The following lemma is well known.

Lemma 1.1. *$G(k) = \boldsymbol{Z}\oplus G_0(k)$, where the infinite cyclic summand is generated by $\langle 1\rangle$ and $G_0(k)$, the subgroup of 0-dimensional elements of $G(k)$, is generated by all the elements of the form $\langle 1\rangle - \langle c\rangle$, where c runs through k^*.*

Let us remark that in the case when $g(k)$ is finite, the group $G(k)$ is a finitely generated abelian group and so, by a classical theorem, a direct sum of cyclic groups. It is also well known that the only possible torsion in $G(k)$ is a 2-power torsion.

Lemma 1.2. *If a is not a square in k and the form $(1, a)$ is universal and $g(k) = \{\boldsymbol{1}, \boldsymbol{a}\}\times h$ (a direct product), then $G_0(k)$ is generated by $\langle 1\rangle - \langle a\rangle$ and all elements $\langle 1\rangle - \langle b\rangle$, where $\boldsymbol{b}$ runs through h.*

Proof. G_0 is generated by all elements $\langle 1\rangle - \langle c\rangle$, $c \in k^*$. Take an element $\boldsymbol{ab}$ in $\boldsymbol{a}h$, then $\langle 1, a\rangle = \langle b, ab\rangle$. Hence $\langle 1\rangle - \langle ab\rangle = \langle 1\rangle - \langle a\rangle - (\langle 1\rangle - \langle b\rangle)$ and so $\langle 1\rangle - \langle ab\rangle$ may be omitted in the set of generators for G_0.

Corollary 1.3. *If -1 is not a square in k and $g(k) = \{\boldsymbol{1}, \boldsymbol{-1}\}\times h$, then G_0 is generated by $\langle 1\rangle - \langle -1\rangle$ and all elements $\langle 1\rangle - \langle b\rangle$, where $\boldsymbol{b}$ runs through h.*

Lemma 1.4. *Let $g(k) = \prod_{i\in I}\{\boldsymbol{1}, \boldsymbol{a}_i\}\times h$, where a_i are chosen in such a way that all the binary forms $(1, a_i)$, $i \in I$, are universal. Then $G_0(k)$ is generated by all the elements $\langle 1\rangle - \langle a_i\rangle$, $i \in I$, and $\langle 1\rangle - \langle b\rangle$, where $\boldsymbol{b}$ runs through h.*

Proof. We shall prove that every element $\langle 1\rangle - \langle ab\rangle$, where $\boldsymbol{a} \in \prod_{i\in I}\{\boldsymbol{1}, \boldsymbol{a}_i\}$ and $\boldsymbol{b} \in h$, can be represented as a linear combination with integer coefficients of a finite set of elements $\langle 1\rangle - \langle a_i\rangle$ and of $\langle 1\rangle - \langle b\rangle$. This follows from the following identity:

$$\langle 1\rangle - \langle ab\rangle = \sum_{j=1}^{n}(-1)^{j+1}(\langle 1\rangle - \langle a_j\rangle) + (-1)^n(\langle 1\rangle - \langle b\rangle),$$

where $a = a_1 \ldots a_n$. If $n = 0$, then $a = 1$ and the identity holds; if $n = 1$, then $a = a_1$ and the result has been proved in Lemma 1.2. Assume the identity holds for some $n \geqslant 1$ and $a' = a_1 \ldots a_{n+1} = a_1 a$, where $a = a_2 \ldots \ldots a_{n+1}$. Then

$$\begin{aligned}\langle 1\rangle - \langle a'b\rangle &= \langle 1\rangle - \langle a_1(ab)\rangle = \langle 1\rangle - \langle a_1\rangle - (\langle 1\rangle - \langle ab\rangle)\\ &= \langle 1\rangle - \langle a_1\rangle - \Big(\sum_{j=1}^{n}(-1)^{j+1}(\langle 1\rangle - \langle a_{j+1}\rangle) + (-1)^n(\langle 1\rangle - \langle b\rangle)\Big)\\ &= \sum_{j=1}^{n+1}(-1)^{j+1}(\langle 1\rangle - \langle a_j\rangle) + (-1)^{n+1}(\langle 1\rangle - \langle b\rangle),\end{aligned}$$

as required.

COROLLARY 1.5. *If the forms $(1, a_i)$, $i = 1, \ldots, n$, are universal and $a = a_1 \ldots a_n$, then*

$$\langle 1\rangle - \langle a\rangle = \sum_{j=1}^{n} (-1)^{j+1}(\langle 1\rangle - \langle a_j\rangle).$$

LEMMA 1.6. *Assume $g(k) = \prod_{i\in I} \{\mathbf{1}, \boldsymbol{a}_i\} \times h$, where a_i is a sum of two squares, for all $i \in I$. Then the set of elements $\langle 1\rangle - \langle a_i\rangle$, $i \in I$, is linearly independent (over $\boldsymbol{Z}$).*

Proof. First observe that all the elements $\langle 1\rangle - \langle a_i\rangle$, $i \in I$, are of order two since $\langle 1, 1\rangle = \langle a_i, a_i\rangle$ for each $i \in I$. Assume now that

$$\sum_{j=1}^{n} (\langle 1\rangle - \langle a_{i_j}\rangle) = 0,$$

where $\{i_1, \ldots, i_n\}$ is a finite subset of I. Taking determinants on both sides we get

$$\prod_{j=1}^{n} \boldsymbol{a}_{i_j} = \mathbf{1},$$

a contradiction.

Now we are ready to determine the Grothendieck group in a case when the behaviour of binary forms makes the situation as simple as possible. But we assume nothing about the square class number of the field.

PROPOSITION 1.7 ([13], Theorem 4.1.1). *Let k be a field such that every binary form over k is universal. Then*

$$\det\colon G_0(k) \to g(k)$$

is an isomorphism, and so $G(k) \cong \boldsymbol{Z} \oplus g(k)$.

Hence, if $\{\boldsymbol{a}_i\colon i \in I\}$ is any basis for $g(k)$, then $\{\langle 1\rangle - \langle a_i\rangle\colon i \in I\}$ is a basis for $G_0(k)$.

Proof. $G_0(k)$ is generated by all elements $\langle 1\rangle - \langle c\rangle$, $\boldsymbol{c} \in g(k)$. An application of Corollary 1.5 and Lemma 1.6 gives the result.

LEMMA 1.8. *Let k be a field with square class number 2^n. The number u_2 of universal binary classes over k is a power of 2 and $u_2 \leqslant 2^n$. If k is non-real and $u_2 < 2^n$, then $u_2 \leqslant 2^{n-2}$.*

Proof. First observe that if the forms $(1, a)$ and $(1, b)$ are both universal, then so is $(1, -ab)$. This enables us to introduce the following law of composition in the set $U_2(k)$ of equivalence classes of binary universal forms:

$$\langle 1, a\rangle \times \langle 1, b\rangle = \langle 1, -ab\rangle.$$

This is clearly well defined on equivalence classes and makes $U_2(k)$ into an abelian group of exponent 2 with the identity $\langle 1, -1\rangle$. Hence $u_2 = |U_2(k)|$, is a power of two and $u_2 \leqslant 2^n$ (for details, see [18]). On the other hand, we denote by R Kaplansky's radical of the field k, i.e. the set of those elements $\boldsymbol{a}$ in $g(k)$ which make any quaternion algebra $(a, b/k)$ split (cf. [6]). R can be easily identified as the set of $\boldsymbol{a}$ in $g(k)$ such that the class $\langle 1, -a\rangle$ is universal, and in fact the mapping sending $\boldsymbol{a}$ in R into $\langle 1, -a\rangle$ in $U_2(k)$ is an isomorphism. Hence $|R| = u_2$. Assume now that $u_2 = 2^{n-1}$. Then the index $[g(k){:}R] = 2^n/2^{n-1} = 2$ and, by Lemma 2 of [6], k is a real field with a unique ordering. Hence if k is non-real, $u_2 \neq 2^{n-1}$ and the lemma is proved.

COROLLARY 1.9. *If k is a non-real field and $q = 4$, then either all binary forms over k are universal or there exists exactly one binary universal class over k (the hyperbolic plane). If k is a non-real field and $q = 8$, then either all binary forms over k are universal or there are at most 2 universal binary classes over k.*

We shall now turn to formally real fields and derive various structure theorems for Grothendieck groups of such fields. First we prove the following general lemma:

LEMMA 1.10. *Let k be a real field and $g(k) = \{\mathbf{1}, -\mathbf{1}\} \times h$, where all the elements of h are positive in a fixed ordering of k. Then*

$$G(k) \cong \boldsymbol{Z} \oplus \boldsymbol{Z} \oplus G_1,$$

where the two infinite cyclic summands are generated by $\langle 1\rangle$ and $\langle 1\rangle - \langle -1\rangle$, respectively, and G_1 is generated by all elements $\langle 1\rangle - \langle a\rangle$, $\boldsymbol{a} \in h$.

Proof. In view of Lemma 1.1 it suffices to show that

$$G_0(k) = [\langle 1\rangle - \langle -1\rangle] \oplus G_1.$$

By Corollary 1.3 the group $G_0(k)$ is generated by $\langle 1\rangle - \langle -1\rangle$ and all $\langle 1\rangle - \langle a\rangle$, $\boldsymbol{a} \in h$. Hence it is sufficient to prove that from

$$x_0(\langle 1\rangle - \langle -1\rangle) + \sum_{i=1}^{n} x_i(\langle 1\rangle - \langle a_i\rangle) = 0,$$

where $\boldsymbol{a}_i \in h$, it follows $x_0 = 0$.

The above relation can be rewritten as

$$\langle b_1, \ldots, b_m\rangle = \langle c_1, \ldots, c_m\rangle,$$

where $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_m\} \subset \{\mathbf{1}, -\mathbf{1}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\}$ and $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\} \cap \cap \{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_m\} = \emptyset$.

If $x_0 \neq 0$, then $-\mathbf{1}$ belongs to one of the sets $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ or $\{\boldsymbol{c}_1, \ldots \ldots, \boldsymbol{c}_m\}$; assume that $\boldsymbol{b}_1 = -\mathbf{1}$. Then $\langle c_1, \ldots, c_m\rangle \approx -1$, a contradiction, since $c_1, \ldots, c_m$ are positive in the given ordering of the field. Hence $x_0 = 0$ and the lemma is proved.

We have already considered the case when every binary form over a field is universal. If k is real, this cannot happen, but it is possible that "a half" of binary forms are universal (see the example 2.5. I in § 4 below). We determine the group $G(k)$ for such a field k.

PROPOSITION 1.11. *Let k be a real field, $g(k) = \{\mathbf{1}, -\mathbf{1}\} \times \prod_{i\in I} \{\mathbf{1}, \boldsymbol{a}_i\}$ and assume that all the binary forms $(1, a_i)$, $i \in I$, are universal. Then*

$$G(k) \cong \mathbf{Z} \oplus \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^{|I|},$$

where the two infinite cyclic summands are generated by $\langle 1\rangle$ and $\langle 1\rangle - \langle -1\rangle$ and the remaining summands are generated by the elements $\langle 1\rangle - \langle -a_i\rangle$, $i \in I$.

Proof. By Lemma 1.4, $G_0(k)$ is generated by $\langle 1\rangle - \langle -1\rangle$ and all elements $\langle 1\rangle - \langle a_i\rangle$, $i \in I$. Using the identity

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

we can replace the above set of generators by $\{\langle 1\rangle - \langle -1\rangle, \langle 1\rangle - \langle -a_i\rangle : i \in I\}$. Now observe that $\langle 1\rangle - \langle -1\rangle$ is of infinite order and $2(\langle 1\rangle - \langle -a_i\rangle) = 0$, for all $i \in I$. Hence

$$G_0 = [\langle 1\rangle - \langle -1\rangle] \oplus G_1,$$

where G_1 is generated by the set $S = \{\langle 1\rangle - \langle -a_i\rangle : i \in I\}$. Since $(1, a_i)$ is universal, $-a_i$ is a sum of two squares; also $g(k) = \{\mathbf{1}, -\mathbf{1}\} \times \prod_{i\in I} \{\mathbf{1}, -\boldsymbol{a}_i\}$, hence Lemma 1.6 applies and gives the result.

Our next goal is to relate the structure of the groups $g(k)$ and $G(k)$ to the number of orderings on the field k. If $a \in k$ is totally positive, then so is every element of $\boldsymbol{a} = ak^{*2}$. Hence we shall speak of totally positive elements of the group $g(k)$. Obviously, they constitute a subgroup of $g(k)$. We have the following general result:

PROPOSITION 1.12. *Let k be a real field and*

$$g(k) = \{\mathbf{1}, -\mathbf{1}\} \times T \times \prod_{i\in I} \{\mathbf{1}, \boldsymbol{a}_i\},$$

where T denotes the subgroup of totally positive elements of $g(k)$. The number $r = r(k)$ of orderings of the field k is finite if and only if I is finite. If $|I| = p < \infty$, then

$$p+1 \leqslant r(k) \leqslant 2^p.$$

Proof. We assume first that $|I| = p < \infty$. In the case $p = 0$, the set of totally positive elements defines an ordering of k and hence the unique ordering. Thus $r = 1$ and the theorem holds. Assume now $p \geqslant 1$. If

$$P_1 = T \times \{\mathbf{1}, \boldsymbol{a}_1\} \times \ldots \times \{\mathbf{1}, \boldsymbol{a}_p\}$$

is an ordering of k (we think here of P_1 as a subset of k^* rather than of $g(k)$), then any other ordering of the field can be represented as

$$P = T \times \{\mathbf{1}, \varepsilon_1 \boldsymbol{a}_1\} \times \ldots \times \{\mathbf{1}, \varepsilon_p \boldsymbol{a}_p\},$$

where $\varepsilon_j = \pm 1$. Hence the number of orderings cannot exceed 2^p. To prove the inequality $p+1 \leqslant r$, we represent all the r orderings in the form

$$P_i = T \times \{\mathbf{1}, \varepsilon_{i1} \boldsymbol{a}_1\} \times \ldots \times \{\mathbf{1}, \varepsilon_{ip} \boldsymbol{a}_p\}, \quad i = 1, \ldots, r,$$

where $\varepsilon_{ij} = \pm 1$ and $\varepsilon_{1j} = 1$, $j = 1, \ldots, p$.

Consider the matrix $M = [\varepsilon_{ij}]$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant p$. The first row of M consists of 1's and any two rows are different. If a column, jth say, consisted exclusively of 1's, then a_j would be positive at every ordering of k, hence $a_j \in T$, a contradiction. We denote by E_j the jth column of M and define the componentwise multiplication of the columns. Observe that if a product $E_{j_1} \ldots E_{j_t}$ is equal to the unit vector (whose all components are 1), then

$$a_{j_1} \ldots a_{j_t} \in P_1 \cap \ldots \cap P_r = T,$$

a contradiction. Consider the matrix M. The number of all possible products of columns one, two, etc. at a time, is at most

$$\binom{p}{1} + \binom{p}{2} + \ldots + \binom{p}{p} = 2^p - 1.$$

If the number of distinct products was less than $2^p - 1$, then we would have at least one equality of the type

$$E_{j_1} \ldots E_{j_t} = E_{i_1} \ldots E_{i_s}, \quad \{j_1, \ldots, j_t\} \neq \{i_1, \ldots, i_s\}$$

and this clearly produces a non-trivial product of the vectors equal to the unit vector. Hence the number of distinct vectors obtained by multiplying columns of the matrix M is exactly $2^p - 1$ and it cannot exceed 2^{r-1} (the total number of vectors with components $1, \pm 1, \ldots, \pm 1$). Hence $2^p - 1 \leqslant 2^{r-1}$, and so $p \leqslant r-1$, if $p > 1$. If $p = 1$, then a_1 is not totally positive, hence $r \geqslant 2 = p+1$.

To complete the proof, assume now that $r(k) < \infty$ and $|I| = \infty$. Let p be any integer and $P_i = T \times \prod_{j\in I} \{\mathbf{1}, \varepsilon_{ij} \boldsymbol{a}_j\}$, $i = 1, \ldots, r$ be the r orderings. Consider the first p columns of the matrix $[\varepsilon_{ij}]$. As above, any product of any number of these columns is different from the unit vector, hence $2^p - 1 \leqslant 2^{r-1}$ for any integer p, a contradiction. Hence if r is finite so is I, and the proposition is proved.

We recall that a field k is said to be pythagorean if every sum of squares of elements of k is a square itself. In a pythagorean field the subgroup T of totally positive elements of $g(k)$ is trivial and we get the following result.

COROLLARY 1.13 (Elman and Lam [2], 4.5 and 5.7). *Let k be a pythagorean field with $q = 2^n$. Then $n \leqslant r \leqslant 2^{n-1}$.*

A pythagorean field with $q = 2^n$ and $r = 2^{n-1}$ is said to be superpythagorean. The pythagorean fields with $q = 2^n$ and $r = n$ can be shown to satisfy a certain strong approximation property (SAP, cf. [2]). In the case $q = 4$ both classes coincide; in the case $q = 8$ the two classes of pythagorean fields are different.

COROLLARY 1.14. *Let k be a real field with a unique ordering. Then* rank $G(k) = 2$.

Proof. If $r = 1$, then $g(k) = \{\mathbf{1}, -\mathbf{1}\}\times T$, where T is the subgroup of totally positive elements. By Lemma 1.10 we have $G(k) \cong \mathbf{Z}\oplus \mathbf{Z}\oplus G_1$, where G_1 is generated by all elements $\langle 1\rangle - \langle a\rangle$, $\boldsymbol{a}\,\epsilon\, T$. By Artin–Schreier theorem, any such a is a sum of squares, hence a sum of 2^m squares, for an integer m, hence $2^m(\langle 1\rangle - \langle a\rangle) = 0$. Thus G_1 is a torsion group and rank $G(k) = 2$.

Now we want to establish that in the case $r = 2$ we have rank $G(k) = 3$. First we reformulate some well known Pfister's results concerning the Witt ring $W(k)$ for the case of Grothendieck ring $G(k)$. Let k be a real field and P an ordering of k. The map

$$\sigma_P\colon\; M(k)\to\mathbf{Z},\qquad \sigma_P\langle a_1, \ldots, a_n\rangle = \sum_{i=1}^{n}\operatorname{sgn}_P a_i$$

is a semiring homomorphism ($M(k)$ is the semiring of equivalence classes of non-singular quadratic forms over k), hence by the universal property of Grothendieck ring, σ_P factors uniquely through a ring homomorphism $G(k)\to\mathbf{Z}$, which will also be denoted by σ_P. Hence

$$\sigma_P(\langle f\rangle - \langle g\rangle) = \sigma_P\langle f\rangle - \sigma_P\langle g\rangle.$$

Now using standard arguments one can easily deduce from the results of [11] the following Pfister's Local-Global Principle:

(1.15) *$A\,\epsilon\, G(k)$ is torsion if and only if* $\dim A = 0$ *and* $\sigma_P(A) = 0$ *at every ordering P of the field k.*

We denote by k_P the real closure of k which induces the ordering P on k. Further, let $j_P\colon G(k)\to G(k_P)$ be the canonical mapping and $G^t(k)$ the torsion subgroup of $G(k)$. Then an equivalent formulation of (1.15) is the following.

(1.16) *The sequence*

$$0\to G^t(k)\to G_0(k)\xrightarrow{\Pi j_P}\prod G_0(k_P)$$

is exact.

Now we can prove the following assertion.

PROPOSITION 1.17. *Let k be a real field and $g(k) = \{\mathbf{1}, -\mathbf{1}\}\times\{\mathbf{1}, \boldsymbol{a}\}\times T$, where T is the subgroup of totally positive elements of $g(k)$. Then*

$$G(k) = \mathbf{Z}^{(3)}\oplus G^t(k),$$

where the three infinite cyclic summands are generated by $\langle 1\rangle$, $\langle 1\rangle - \langle -1\rangle$, $\langle 1\rangle - \langle a\rangle$, respectively.

Proof. From Proposition 1.12 we obtain $r = 2$. Let P_1 and P_2 be the two orderings of k and k_1 and k_2 the two corresponding real closures of k. Consider the mapping

$$(j_1, j_2)\colon\; G_0(k)\to G_0(k_1)\times G_0(k_2).$$

We have

$$(j_1, j_2)(\langle 1\rangle - \langle a\rangle) = (\langle 1\rangle - \langle -1\rangle, 0)$$

and

$$(j_1, j_2)(\langle 1\rangle - \langle -a\rangle) = (0, \langle 1\rangle - \langle -1\rangle),$$

where we have assumed that $a\,\epsilon\, P_2$ and $-a\,\epsilon\, P_1$. This shows that the homomorphism (j_1, j_2) is surjective. Since the group $G_0(k_1)\times G_0(k_2)$ is free, we have

$$G_0(k) = [\langle 1\rangle - \langle a\rangle]\oplus[\langle 1\rangle - \langle -a\rangle]\oplus \operatorname{Ker}(j_1, j_2)$$

by a standard lemma on abelian groups (cf. [8], p. 44).

From (1.16) we obtain

$$\operatorname{Ker}(j_1, j_2) = G^t(k),$$

and the identity

$$\langle 1\rangle - \langle a\rangle + \langle 1\rangle - \langle -a\rangle = \langle 1\rangle - \langle -1\rangle$$

shows that

$$[\langle 1\rangle - \langle a\rangle]\oplus[\langle 1\rangle - \langle -a\rangle] = [\langle 1\rangle - \langle -1\rangle]\oplus[\langle 1\rangle - \langle a\rangle],$$

which proves the proposition.

Remark 1.18. Using Elman and Lam's Normality Theorem [2] one can prove that for any field with finite number r of orderings one has rank $G(k) = r+1$. This has been noticed by A. Sladek (for details and an independent elementary proof, see [14]). However, the proof in the general case does not point out any basis for the group $G(k)$.

Now we will prove two results concerning pythagorean fields.

PROPOSITION 1.19. *A field k is pythagorean if and only if the Grothendieck group $G(k)$ is torsion free.*

Proof. If k is not pythagorean, then $(1, 1)$ represents a non-square a, say, and then $\langle 1, 1\rangle = \langle a, a\rangle$ and $2(\langle 1\rangle - \langle a\rangle) = 0$, i.e. $\langle 1\rangle - \langle a\rangle \neq 0$ is a torsion element in $G(k)$.

To prove the converse we need a lemma.

LEMMA 1.20. *Let k be a pythagorean field and n a positive integer. Then for any positive integer m,*

$$n\langle a_1, \ldots, a_m\rangle = n\langle b_1, \ldots, b_m\rangle \Rightarrow \langle a_1, \ldots, a_m\rangle = \langle b_1, \ldots, b_m\rangle.$$

Proof by induction on m. Consider first the case $m = 1$. If $n\langle a\rangle = n\langle b\rangle$, then $n\langle a\rangle \approx b$. But k is pythagorean, hence $\langle a\rangle \approx b$, and $\langle a\rangle = \langle b\rangle$.

Assume the lemma holds for forms of dimension m.

If $n\langle a_1, \ldots, a_{m+1}\rangle = n\langle b_1, \ldots, b_{m+1}\rangle$, then $n\langle a_1, \ldots, a_{m+1}\rangle \approx b_{m+1}$ and by pythagoreanity, $\langle a_1, \ldots, a_{m+1}\rangle \approx b_{m+1}$.

Consequently $\langle a_1, \ldots, a_{m+1}\rangle = \langle c_1, \ldots, c_m, b_{m+1}\rangle$ for some $c_1, \ldots, c_m$. Now $n\langle c_1, \ldots, c_m, b_{m+1}\rangle = n\langle b_1, \ldots, b_{m+1}\rangle$ and by Witt's cancellation theorem ([19], Satz 4) we get $n\langle c_1, \ldots, c_m\rangle = n\langle b_1, \ldots, b_m\rangle$. Applying the induction hypothesis we obtain $\langle c_1, \ldots, c_m\rangle = \langle b_1, \ldots, b_m\rangle$ and finally

$$\langle a_1, \ldots, a_{m+1}\rangle = \langle c_1, \ldots, c_m, b_{m+1}\rangle = \langle b_1, \ldots, b_{m+1}\rangle,$$

as required.

Now we may complete the proof of Proposition 1.19. Assume k is pythagorean. If there is a torsion element A in $G(k)$ we write $A = \langle f_1\rangle - \langle f_2\rangle$ and assume $nA = 0$, $n > 0$. Then $n\langle f_1\rangle = n\langle f_2\rangle$ and so $\dim f_1 = \dim f_2$ and Lemma 1.20 applies: $\langle f_1\rangle = \langle f_2\rangle$, i.e. $A = 0$. Thus there is no non-trivial torsion in $G(k)$.

PROPOSITION 1.21. *Let k be a pythagorean field and*

$$g(k) = \{\mathbf{1}, -\mathbf{1}\} \times \prod_{i\in I} \{\mathbf{1}, \boldsymbol{a}_i\}.$$

Then the set $\mathscr{B} = \{\langle 1\rangle - \langle -1\rangle, \langle 1\rangle - \langle a_i\rangle : i \in I\}$ is linearly independent.

In particular, if $q = |g(k)| = 2^n$, then rank $G(k) \geqslant n+1$.

Proof. In this proof the symbol (a, b) denotes the quaternion algebra corresponding to $a, b \in k^*$. We shall use the Hasse algebra and apart from its standard properties ([10], § 58) we shall make use of the following straightforward consequence of the definition:

For positive integers x_i one has

$$S\Big(\sum_{i=1}^{n} x_i\langle a_i\rangle\Big) \sim \bigotimes_{i=1}^{n} \big(a_i, (a_1^{x_1} \ldots a_{i-1}^{x_{i-1}})^{x_i} a_i^{x_i(x_i+1)/2}\big).$$

Assume now that a finite subset of $\mathscr{B}$ is linearly dependent. Then

$$x_1(\langle 1\rangle - \langle b_1\rangle) + \ldots + x_r(\langle 1\rangle - \langle b_r\rangle) = y_1(\langle 1\rangle - \langle c_1\rangle) + \ldots + y_s(\langle 1\rangle - \langle c_s\rangle),$$

where all the coefficients are positive integers. Moreover, Proposition 1.19 makes it clear that we can assume the coefficients x_i, y_j not to be all even. Multiplying by 2 and rearranging the summands we obtain

$$\begin{aligned} A &= 2(x_1 + \ldots + x_r)\langle 1\rangle + 2y_1\langle c_1\rangle + \ldots + 2y_s\langle c_s\rangle \\ &= 2(y_1 + \ldots + y_s)\langle 1\rangle + 2x_1\langle b_1\rangle + \ldots + 2x_r\langle b_r\rangle = B. \end{aligned}$$

These two quadratic forms have isomorphic Hasse algebras. But

$$\begin{aligned} SA &\sim S(2y_1\langle c_1\rangle + \ldots + 2y_s\langle c_s\rangle) \\ &\sim \bigotimes_{i=1}^{s} \big(c_i, (c_1^{2y_1} \ldots c_{i-1}^{2y_{i-1}})^{2y_i} c_i^{y_i(2y_i+1)}\big) \\ &\sim \bigotimes_{i=1}^{s} (c_i, c_i^{y_i}) \sim (c_{i_1}, -1) \otimes \ldots \otimes (c_{i_l}, -1) \\ &\sim (-1, c_{i_1} \ldots c_{i_l}), \end{aligned}$$

where $i_1, \ldots, i_l$ are those indices i for which y_i is odd. Similarly, $SB \sim \sim(-1, b_{j_1}, \ldots, b_{j_m})$, where $j_1, \ldots, j_m$ are those indices j for which x_j is odd. Thus $SA \sim SB$ implies $(-1, c_{i_1} \ldots c_{i_l}) \cong (-1, b_{j_1} \ldots b_{j_m})$, hence $c_{i_1} \ldots c_{i_l} b_{j_1} \ldots b_{j_m}$ is a sum of two squares, hence a square, since the field is pythagorean.

But $\boldsymbol{c}_i$, $\boldsymbol{b}_j$ are elements of a basis for $g(k)$, hence their product cannot be a square. This shows that the set $\mathscr{B}$ is linearly independent.

We end this section with some observations relating the number of orderings of a pythagorean field to the behaviour of binary forms over the field.

PROPOSITION 1.22. *Let k be a real field with square class number $q = 2^n \geqslant 4$ and r orderings.*

(i) *k is superpythagorean (i.e. $r = 2^{n-1}$) if and only if k is pythagorean and every anisotropic binary form represents at most 2 elements of $g(k)$.*

(ii) *If k is pythagorean and there exists an anisotropic binary form representing more than 2 elements of $g(k)$ and $n \geqslant 3$, then $r \leqslant 3\cdot 2^{n-3}$.*

Proof. Let $\{-\mathbf{1}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{n-1}\}$ be a basis for the group $g(k)$. As observed by Elman and Lam ([2], p. 1181) two orderings on k are the same if and only if each a_i has the same sign under both orderings. If $r = 2^{n-1}$, then all possible combinations of signs do occur and so every element of $g(k)$ different from $\mathbf{1}$ is negative at a certain ordering. Hence $D(1, 1) = \mathbf{1}$ and k is pythagorean. If $q = 4$ we check at once $|D(1, a_1)| = |D(1, -a_1)| = 2$ and this proves the assertion. Assume $q \geqslant 8$. Let (a, b) be an anisotropic form, i.e. $\boldsymbol{ab} \neq -\mathbf{1}$. If $\boldsymbol{ab} = \mathbf{1}$, then $D(a, b) = \boldsymbol{a}D(1, 1) = \boldsymbol{a}$, i.e. $|D(a, b)| \leqslant 2$, as required. If $\boldsymbol{ab} \neq \mathbf{1}$, then $|D(a, b)| = |D(1, ab)|$ and so we can consider the form $(1, c)$, where $\boldsymbol{c} \neq \pm\mathbf{1}$. Fix an ordering P

at which c is positive (this is possible for any pythagorean field by [2], Prop. 4.1). Assume $(1, c) \approx d$, where $\boldsymbol{d} \neq \mathbf{1}$ and $\boldsymbol{d} \neq \boldsymbol{c}$. Then also $\boldsymbol{d} \neq -\mathbf{1}$ and $\boldsymbol{d} \neq -\boldsymbol{c}$ since every element represented by $(1, c)$ is positive at P. Thus $\boldsymbol{d}$ does not belong to the subgroup of $g(k)$ generated by $-\mathbf{1}, \boldsymbol{c}$ and we can choose a basis for $g(k)$ of the form $\{-\mathbf{1}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{b}_3, \ldots, \boldsymbol{b}_{n-1}\}$. Since d is positive whenever c is, we obtain $r \leqslant 3\cdot 2^{n-3}$, which proves (ii). But if $r = 2^{n-1}$ this is impossible, hence $|D(a, b)| = |D(1, c)| = 2$ and the first part of (i) is proved. Conversely, assume that k is pythagorean and $|D(a, b)| \leqslant 2$ for $\boldsymbol{ab} \neq -\mathbf{1}$. Let $\{-\mathbf{1}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{n-1}\}$ be any basis for $g(k)$. We prove that the subgroup P of $g(k)$ generated by $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{n-1}\}$ defines an ordering of the field. Clearly, $P \cup -P = g(k)$ and P is closed under multiplication. Take arbitrary α in $\boldsymbol{a}$ and β in $\boldsymbol{b}$, where $\boldsymbol{a}, \boldsymbol{b} \in P$. Then $\boldsymbol{ab} \neq -\mathbf{1}$ and $(a, b) \approx \alpha+\beta$, hence $\alpha+\beta \in \boldsymbol{a}$ or $\alpha+\beta \in \boldsymbol{b}$. This shows that P (as a subset of k^*) is closed under addition, hence P defines an ordering of k. But if $\{-\mathbf{1}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{n-1}\}$ is a basis for $g(k)$ then so is $\{-\mathbf{1}, \pm\boldsymbol{a}_1, \ldots, \pm\boldsymbol{a}_{n-1}\}$ for any choice of the signs; hence there are 2^{n-1} distinct orderings and the proposition is proved.

PROPOSITION 1.23. *If k is a superpythagorean field with square class number $q = 2^n$, then*

$$G(k) \cong \mathbf{Z}^{(2^{n-1}+1)}.$$

If $g(k) = \{\mathbf{1}, -\mathbf{1}\} \times h$, then the direct summands are generated by $\langle 1\rangle$, $\langle 1\rangle - \langle -1\rangle$, and all the elements $\langle 1\rangle - \langle a\rangle$, $\boldsymbol{a} \in h$.

Proof. Propositions 1.22 and 1.19 show that the homomorphism $\prod j_P$ in (1.16) is in fact an injection. We shall show that the image of $\prod j_P$ contains 2^{n-1} linearly independent elements which will prove all the assertions of Proposition 1.23. Let $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{n-1}\}$ be any basis for h. The 2^{n-1} orderings of the field are completely determined by the signs of a_i. Let P be any ordering and assume that $\varepsilon_1 a_1, \ldots, \varepsilon_{n-1}a_{n-1} \in P$, where $\varepsilon_i = \pm 1$. Put

$$A_P = (\langle 1\rangle - \langle -\varepsilon_1 a_1\rangle) \ldots (\langle 1\rangle - \langle -\varepsilon_{n-1}a_{n-1}\rangle)$$

(we use here the ring structure of $G(k)$).

Observe that $j_P(\langle 1\rangle - \langle a\rangle) = 0$ if $a \in P$ and $j_P(\langle 1\rangle - \langle a\rangle) = \langle 1\rangle - \langle -1\rangle$ if $-a \in P$.

Hence

$$j_P(A_P) = (\langle 1\rangle - \langle -1\rangle)^{n-1} = 2^{n-2}(\langle 1\rangle - \langle -1\rangle) \neq 0$$

and

$$j_{P'}(A_P) = 0 \quad \text{for any ordering } P' \neq P.$$

Thus the images under the map $\prod j_P$ of 2^{n-1} elements A_P, where P runs through all the orderings of k, form a linearly independent subset of $\prod G_0(k_P)$, and by the remark above, we are finished.

2. Classification of Grothendieck groups for fields with $q \leqslant 8$.

The main results in this section are Theorems 2.4 and 2.5 which classify the groups $G(k)$ for fields with $q = 8$. For the sake of completeness we include the cases $q = 1, 2, 4$. Theorem 2.1 follows directly from Lemma 1.1 and Theorem 2.2 follows from Proposition 1.7 (the non-real case) and Lemma 1.10 (the real case). Theorem 2.3 has been proved first in [17] by another method and we give here a brief and easy proof for it by using the results of § 1.

THEOREM 2.1. *Let k be a field of characteristic other than 2 and $q(k) = 1$. Then $G(k) \cong \mathbf{Z}$ and the group is generated by the class $\langle 1\rangle$.*

THEOREM 2.2. *Let k be a field of characteristic other than 2 and $q(k) = 2$. If k is non-real, then*

$$G(k) \cong \mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}.$$

If k is real, then

$$G(k) \cong \mathbf{Z} \oplus \mathbf{Z}.$$

In both cases the cyclic summands are generated by $\langle 1\rangle$ and $\langle 1\rangle - \langle a\rangle$, where a is a non-square in k.

THEOREM 2.3. *Let k be a field of characteristic not 2 and $q(k) = 4$.*

A. *Let k be a non-real field.*

(I) *If every binary quadratic form over k is universal, then*

$$G(k) \cong \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^{(2)}.$$

(II) *If $(1, 1)$ is universal but there are non-universal binary forms over k, then*

$$G(k) \cong \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^{(3)}.$$

(III) *If $(1, 1)$ is not universal, then*

$$G(k) \cong \mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}.$$

B. *Let k be a real field.*

(IV) *If k is non-pythagorean, then*

$$G(k) \cong \mathbf{Z}^{(2)} \oplus \mathbf{Z}/2\mathbf{Z}.$$

(V) *If k is pythagorean, then*

$$G(k) \cong \mathbf{Z}^{(3)}.$$

Proof. We put $g(k) = \{\mathbf{1}, \boldsymbol{e}\} \times \{\mathbf{1}, \boldsymbol{a}\}$, where $e = -1$ unless -1 is a square in k. We also use the notation: $E = \langle 1\rangle - \langle e\rangle$, $A = \langle 1\rangle - \langle a\rangle$, $D = \langle 1\rangle - \langle ea\rangle$. If $q = 4$, then $s = 1, 2$ or infinity, as proved by Kaplansky ([5], Theorem 4).

Case (I). Proposition 1.7 yields all the information needed:

$$G_0 = [E]\oplus[A] \cong (\boldsymbol{Z}/2\boldsymbol{Z})^{(2)}.$$

Case (II). By Lemma 1.1, we have $G_0 = [E, A, D]$. Now E and A are linearly independent (Lemma 1.6) and D does not belong to $[E, A]$, for otherwise $D = E+A$, i.e. $\langle 1, ea\rangle = \langle e, a\rangle$ and $\langle 1, ea\rangle$ would be a second universal binary class, contrary to Corollary 1.9. Hence

$$G_0 = [E]\oplus[A]\oplus[D] \cong (\boldsymbol{Z}/2\boldsymbol{Z})^{(3)}.$$

Case (III). By Corollary 1.3, the group G_0 is generated by E and A. Here $2E = 0$ and $2A \neq 0$ (otherwise $\langle 1, 1\rangle = \langle a, a\rangle$ would be a universal class). Moreover, $\langle 1, 1\rangle = \langle -1, -1\rangle$ and $\langle a, a\rangle = \langle -a, -a\rangle$, hence $\langle 1, 1, 1, 1\rangle = \langle -1, -1, 1, 1\rangle = \langle a, -a, a, -a\rangle = \langle a, a, a, a\rangle$, and so $4A = 0$. Now E does not belong to $[A]$ since none of the elements of $[A]$ has determinant -1. Thus

$$G_0 = [A, E] = [A]\oplus[E] \cong \boldsymbol{Z}/4\boldsymbol{Z}\oplus\boldsymbol{Z}/2\boldsymbol{Z}.$$

Case (IV). Now $(1, 1)$ represents a non-square in k, so assume that $(1, 1) \approx a$. Then $(1, -a)$ is universal and Proposition 1.11 applies:

$$G(k) = [\langle 1\rangle]\oplus[E]\oplus[A] \cong \boldsymbol{Z}\oplus\boldsymbol{Z}\oplus\boldsymbol{Z}/2\boldsymbol{Z}.$$

Case (V). Now Proposition 1.17 shows that

$$G(k) = [\langle 1\rangle]\oplus[E]\oplus[A] \cong \boldsymbol{Z}^{(3)}.$$

We come now to the main theorems of this section. We recall our notation: $q = q(k) = |g(k)|$, $q_2 = |D(1, 1)|$, $u_2 = |U_2(k)|$, the number of binary universal classes over k. Both q_2 and u_2 are powers of two, $q_2 \leqslant q$, $u_2 \leqslant q$ and $q_2 > 1$ if k is non-real and $q > 1$. It will be also convenient to have the inequality $s \leqslant q_2$ at hand ([11], p. 126).

Theorem 2.4 (Classification Theorem for Grothendieck groups of non-real fields with $q = 8$). *Let k be a non-real field of characteristic not 2 and $q(k) = 8$. Then the Grothendieck group $G(k)$ is determined as follows.*

(i) *The case $q_2 = 8$.*

(I) *If $u_2 = 8$ (i.e. every binary quadratic form over k is universal), then*

$$G(k) \cong \boldsymbol{Z}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{(3)}.$$

(II) *If $2 \leqslant u_2 < 8$, then*

$$G(k) \cong \boldsymbol{Z}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{(4)}.$$

(III) *If $u_2 = 1$ and there exists a non-universal binary form representing more than 2 elements of $g(k)$, then*

$$G(k) \cong \boldsymbol{Z}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{(5)}.$$

(IV) *If $u_2 = 1$ and every non-universal binary form represents at most 2 elements of $g(k)$, then*

$$G(k) \cong \boldsymbol{Z}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{(7)}.$$

(ii) *The case $q_2 = 4$.*

(V) *If $s = 4$, or if $s \leqslant 2$ and $u_2 \geqslant 2$, then*

$$G(k) \cong \boldsymbol{Z}\oplus\boldsymbol{Z}/4\boldsymbol{Z}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{(2)}.$$

(VI) *If $s \leqslant 2$ and $u_2 = 1$, then*

$$G(k) \cong \boldsymbol{Z}\oplus\boldsymbol{Z}/4\boldsymbol{Z}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{(3)}.$$

(iii) *The case $q_2 = 2$.*

(VII) *If $q_2 = 2$, then every anisotropic binary form represents exactly 2 elements of $g(k)$ and*

$$G(k) \cong \boldsymbol{Z}\oplus(\boldsymbol{Z}/4\boldsymbol{Z})^{(3)}\oplus\boldsymbol{Z}/2\boldsymbol{Z}.$$

Remark. In Section 4 we produce examples of fields which show that all the cases of Theorem 2.4 do occur, except possibly (II).

Theorem 2.5 (Classification Theorem for Grothendieck groups of real fields with $q = 8$). *Let k be a real field with square class number $q = 8$. Then the Grothendieck group $G(k)$ is determined as follows.*

(i) *The case $q_2 = 4$.*

(I) *If $u_2 \geqslant 2$, then*

$$G(k) \cong \boldsymbol{Z}^{(2)}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{(2)}.$$

(II) *If $u_2 = 1$, then*

$$G(k) \cong \boldsymbol{Z}^{(2)}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{(3)}.$$

(ii) *The case $q_2 = 2$.*

(III) *If $u_2 \geqslant 2$, then*

$$G(k) \cong \boldsymbol{Z}^{(3)}\oplus\boldsymbol{Z}/2\boldsymbol{Z}.$$

(IV) *If $u_2 = 1$, then*

$$G(k) \cong \boldsymbol{Z}^{(3)}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{(2)}.$$

(iii) *The case $q_2 = 1$ (i.e., k is a pythagorean field).*

(V) *If there is an anisotropic binary form representing more than 2 elements of $g(k)$, then*

$$G(k) \cong \boldsymbol{Z}^{(4)}.$$

(VI) *If every anisotropic binary form represents at most 2 elements of $g(k)$, then*

$$G(k) \cong \boldsymbol{Z}^{(5)}.$$

Remark. We shall prove in Section 4 that each of the six cases of Theorem 2.5 actually occurs, except possibly (II).

Proof of Theorem 2.4. In each of the seven cases we fix a decomposition of $g(k)$ into direct product of subgroups of order two: $g(k) = \{\mathbf{1}, \boldsymbol{e}\} \times \{\mathbf{1}, \boldsymbol{a}\} \times \{\mathbf{1}, \boldsymbol{b}\}$, where we assume that $e = -1$ whenever -1 is not a square in k, and a and b are chosen to satisfy certain conditions. We use the following notation for the generators of $G_0(k)$: $E = \langle 1\rangle - \langle e\rangle$, $A = \langle 1\rangle - \langle a\rangle$, $B = \langle 1\rangle - \langle b\rangle$, $C = \langle 1\rangle - \langle ab\rangle$, $D = \langle 1\rangle - \langle ea\rangle$, $F = \langle 1\rangle - \langle eb\rangle$, $H = \langle 1\rangle - \langle eab\rangle$.

Case (i). $q_2 = 8$. Here the form $(1, 1)$ is universal and so the stufe $s \leqslant 2$. Also $\langle 1, 1\rangle = \langle c, c\rangle$ for every $\boldsymbol{c}$ in $g(k)$, so that $2(\langle 1\rangle - \langle c\rangle) = 0$.

Subcase (I). Proposition 1.7 proves that

$$G_0 = [E] \oplus [A] \oplus [B] \cong (\boldsymbol{Z}/2\boldsymbol{Z})^{(3)}.$$

Subcase (II). Choose a non-square e such that $(1, e)$ be universal. Then by Lemma 1.2, we have $G_0 = [E, A, B, C]$. Assume that $C \in [E, A, B]$; then necessarily $C = A + B$ (determinants), and this implies $\langle 1, ab\rangle = \langle a, b\rangle$. We show that also $(1, ab) \approx e$. In fact, if $s = 1$, then from $(1, e) \approx ab$ we get $(1, ab) \approx e$. If $s = 2$, then $e = -1$, $(1, 1) \approx -ab$ and so $(1, ab) \approx -1 = e$. Thus in either case $(1, ab) \approx e, a, b$ and so $\langle 1, ab\rangle$ is a third universal class, contrary to Corollary 1.9. (An alternative proof: if $C = A + B$, then $G_0 \cong (\boldsymbol{Z}/2\boldsymbol{Z})^{(3)} \cong g(k)$, and by Theorem 2.2 of [18] all binary forms over k have to be universal). Hence using Lemma 1.6 we get

$$G_0 = [E, A, B, C] = [E] \oplus [A] \oplus [B] \oplus [C] \cong (\boldsymbol{Z}/2\boldsymbol{Z})^{(4)}.$$

Subcase (III). $(1, 1)$ is the only universal form, so $\langle 1, 1\rangle = \langle 1, -1\rangle$ and consequently $s = 1$. Now $D(1, c)$ is a subgroup of $g(k)$ and $|D(c, d)| = |D(1, cd)|$. Hence if $2 < |D(c, d)| < 8$, then $|D(c, d)| = 4$, and so there exists a form $(1, e)$ representing exactly 4 elements of $g(k)$. If $D(1, e) = \{\mathbf{1}, \boldsymbol{e}, \boldsymbol{a}, \boldsymbol{ea}\}$, then we choose an element $\boldsymbol{b}$ in $g(k)$ which is not represented by $(1, e)$ and write $g(k) = \{\mathbf{1}, \boldsymbol{e}\} \times \{\mathbf{1}, \boldsymbol{a}\} \times \{\mathbf{1}, \boldsymbol{b}\}$. We know that $\langle 1, e\rangle = \langle a, ea\rangle$, and this implies $\langle b, eb\rangle = \langle ab, eab\rangle$ and $\langle 1, a\rangle = \langle e, ea\rangle$. Thus $E = A + D$ and $B + F = C + H$. The group G_0 is generated by the elements E, A, B, C, D, F, H (Lemma 1.1) and the above relations show that D and H are superfluous in the set of generators. By Lemma 1.6, the elements E, A, B are independent; put $G_1 = [E, A, B]$. Then C does not belong to G_1, for otherwise $C = A + B$ and $\langle 1, a\rangle = \langle b, ab\rangle$. We observe that $(1, e) \approx a$ implies $(1, a) \approx e$ (since $s = 1$), and so $(1, a)$ would be a universal form which is not the case. Thus $C \notin G_1$.

Write $G_2 = [E, A, B, C]$ and observe that $F \notin G_2$. Otherwise, comparing determinants we get either $F = E + B$ or $F = E + A + C$. Now the first possibility gives $\langle 1, e\rangle = \langle b, eb\rangle$ which implies the universality of $(1, e)$, a contradiction. The second possibility implies $\langle 1, b\rangle = \langle ea, eab\rangle$. But this is also impossible: if $(1, b) \approx ea$, then $(1, ea) \approx b$ and from $(1, e) \approx ea$, $(1, a) \approx ea$ we get $(1, ea) \approx a, e$. Thus $(1, ea)$ would be a second universal binary form. Summarizing we get:

$$\begin{aligned} G_0 &= G_2 \oplus [F] = G_1 \oplus [C] \oplus [F] \\ &= [E] \oplus [A] \oplus [B] \oplus [C] \oplus [F] \cong (\boldsymbol{Z}/2\boldsymbol{Z})^{(5)}. \end{aligned}$$

Subcase (IV). Here again $s = 1$ and G_0 is generated by the seven elements E, A, B, C, D, F, H. We prove that they are independent. Let us prove first that any four of them are independent. Suppose, for instance, $A + B + D + F = 0$. Then $A + B = D + F$, hence $\langle a, b\rangle = \langle ea, eb\rangle$ and (a, b) represents at least 4 elements of $g(k)$, contrary to (IV). Similarly, any sum of three or two of them is not 0. Put $G_1 = [E, A, B, C]$ and $G_2 = [D, F, H]$. To get the result it suffices to show that $G_1 \cap G_2 = 0$. First note that none of D, F, H belongs to G_1, for $\det(E + A + B + C) = \boldsymbol{e}$ and so this sum is not equal to D, F, H, and as remarked above, D, F, H cannot be expressed as a sum of 3 or less generators of G_1. Similarly, $D + F$, $D + H$, $F + H$ do not belong to G_1. To see this observe that the determinants of the sums of any three of E, A, B, C are $\boldsymbol{eab}$, $\boldsymbol{ea}$, $\boldsymbol{eb}$, $\mathbf{1}$. Thus none of $D + F$, $D + H$, $F + H$ can be a sum of three or four generators of G_1 because of unequal determinants, and also none of them can be a sum of less than 3 generators of G_1. It remains to prove that $D + F + H \notin G_1$. First observe that $\det(D + F + H) = \boldsymbol{e}$ and none of the sums of two or three generators of G_1 has determinant $\boldsymbol{e}$. Thus the only possibility is $E + A + B + C = D + F + H$, or equivalently, $H = E + A + B + C + D + F$, or else $\langle 1, 1, 1, 1, 1, eab\rangle = \langle e, a, b, ab, ea, eb\rangle$. That this cannot happen is easily seen on using Witt's theorem on piecewise equivalence ([19], Satz 7; compare [7], p. 25). In view of the hypothesis (IV) every dyadic change of the form (e, a, b, ab, ea, eb) reduces merely to a permutation of the diagonal entries and so we never pass from this form by dyadic changes to $(1, 1, 1, 1, 1, eab)$. Thus we have proved that $G_1 \cap G_2 = 0$, and so we get

$$G_0 = G_1 \oplus G_2 = [E] \oplus [A] \oplus [B] \oplus [C] \oplus [D] \oplus [F] \oplus [H] \cong (\boldsymbol{Z}/2\boldsymbol{Z})^{(7)}.$$

Case (ii). $q_2 = 4$. We know that $s \leqslant q_2$, so we have now $s \leqslant 4$ and $s > 1$ (otherwise $q_2 = q = 8$). Note also that in the case (ii) the class $4\langle 1\rangle$ is universal. This is obvious if $s = 2$, and if $s = 4$, then $(1, 1)$ is anisotropic and represents 4 elements of $g(k)$, hence $(1, 1, 1)$ represents at least 5 elements of $g(k)$ (cf. [9], p. 13). Consequently, the multiplicative class $4\langle 1\rangle$ represents all $g(k)$. Hence $4(\langle 1\rangle - \langle c\rangle) = 0$, for every c in k^*.

Subcase (V). Consider first the case $s = 4$. Assume $-1 = a + b$, where $a, b \in D(1, 1)$. These lie in different cosets of k^* modulo k^{*2} and so we may write $D(1, 1) = \{\mathbf{1}, \boldsymbol{a}\} \times \{\mathbf{1}, \boldsymbol{b}\}$ and $g(k) = \{\mathbf{1}, \mathbf{-1}\} \times D(1, 1)$.

Here $\langle a, b\rangle = \langle -1, -ab\rangle$, hence $\langle 1, a, b, ab\rangle = \langle 1, -1, 1, -1\rangle$ which is equivalent to $A+B+C = 2E$. By Lemma 1.2, $G_0 = [E, A, B, C]$ and the above relation shows that

$$G_0 = [E, A, B] = [E]\oplus[A]\oplus[B] \cong \boldsymbol{Z}/4\boldsymbol{Z}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{(2)}.$$

Assume that $s = 2$. Now $D(1, 1) = \{\boldsymbol{1}, -\boldsymbol{1}\}\times\{\boldsymbol{1}, \boldsymbol{a}\}$ and $g(k) = D(1, 1)\times\times\{\boldsymbol{1}, \boldsymbol{b}\}$. Consider (V). Since $u_2 \geqslant 2$, either $(1, a)$ or $(1, -a)$ is universal and we choose $\boldsymbol{a}$ so that $(1, a)$ be universal. By Lemma 1.4 we obtain $G_0 = [E, A, B]$. Here $2E = 2A = 4B = 0$, $2B \neq 0$ and $E\notin[A, B]$, $A\notin[B]$ (by comparison of determinants). Hence

$$G_0 = [B]\oplus[E]\oplus[A] \cong \boldsymbol{Z}/4\boldsymbol{Z}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{(2)}.$$

Subcase (VI). Now $\langle 1, -1\rangle$ is the only universal class and $G_0 = [E, A, B, C]$ (Corollary 1.3). From $\langle 1, 1\rangle = \langle a, a\rangle$ we obtain $2B = 2C$. Hence $G_0 = [E, A, B, B-C]$, where $2E = 2A = 2(B-C) = 0$ and $4B = 0$, $2B\neq 0$. Certainly $E\notin G_1 = [A, B, B-C]$ (determinants), so we may write $G_0 = [E]\oplus G_1$. Now $[B]\cap[A, B-C] = 0$, otherwise we would get $2B = A+B-C$ (determinants), and $\langle 1, a\rangle = \langle b, ab\rangle$, contrary to the non-universality of $(1, a)$. Thus

$$G_1 = [B]\oplus[A, B-C] = [B]\oplus[A]\oplus[B-C],$$

since $A\neq B-C$ (otherwise $(1, -a)$ would be universal). Hence

$$G_0 = [B]\oplus[E]\oplus[A]\oplus[B-C] \cong \boldsymbol{Z}/4\boldsymbol{Z}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{(3)}.$$

Case (iii). $q_2 = 2$. Now obviously $s > 1$ and from $s\leqslant q_2$ we get $s = 2$. Thus $D(1, 1) = \{\boldsymbol{1}, -\boldsymbol{1}\}$. None of anisotropic binary forms can be universal, since if $(1, a)$ is universal, then $-\boldsymbol{a}\in D(1, 1)$. But, in fact, more is true. Using an argument due to L. Szczepanik, we prove that $|D(c, d)|\leqslant 2$ for any anisotropic form (c, d). If this is not the case, we may assume that $|D(1, a)| = 4$ and $D(1, a) = \{\boldsymbol{1}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{ab}\}$. Then from $\langle 1, 1\rangle = \langle -1, -1\rangle$ we get $\langle 1, b, b\rangle = \langle 1, -b, -b\rangle$. We have $\langle 1, -b\rangle\approx -a$ and so $\langle 1, -b, -b\rangle\approx -a$, while we shall prove that $\langle 1, b, b\rangle$ does not represent $-a$. To this end we must determine $D(1, b, b) = \bigcup D(c, b)$, where $\boldsymbol{c}$ runs through $D(1, b)$. We shall show that $D(1, b) = \{\boldsymbol{1}, \boldsymbol{b}\}$ and so $D(1, b, b) = D(1, b)\cup D(b, b) = \{\boldsymbol{1}, \boldsymbol{b}, -\boldsymbol{b}\}$ does not contain $-\boldsymbol{a}$, as required.

Now we determine $D(1, b)$. Knowing $D(1, 1)$ and $D(1, a)$ we see at once that $-\boldsymbol{1}$ and $-\boldsymbol{a}$ do not belong to $D(1, b)$, hence also $-\boldsymbol{b}$ and $-\boldsymbol{ab}$ do not. If $\boldsymbol{ab}\in D(1, b)$, then $(1, -ab)\approx -a, -b, -ab$, hence also $(1, -ab)\approx(-a)(-ab) = a^2b$. Thus $(1, -ab)\approx a^2b(-b)$, and so $\boldsymbol{ab}\in D(1, 1)$, a contradiction. Hence $\boldsymbol{ab}\notin D(1, b)$, $|D(1, b)| < 4$, and so $D(1, b) = \{\boldsymbol{1}, \boldsymbol{b}\}$ as required.

Now we determine $G(k)$. Write $g(k) = \{\boldsymbol{1}, -\boldsymbol{1}\}\times\{\boldsymbol{1}, \boldsymbol{a}\}\times\{\boldsymbol{1}, \boldsymbol{b}\}$; then $2E = 4A = 4B = 4C = 0$ and $2A\neq 0$, $2B\neq 0$, $2C\neq 0$. By Lemma 1.2,

$$G_0 = [E, A, B, C] = [E]\oplus[A, B, C]$$

(since $E\notin[A, B, C]$). Here $[A]\cap[B] = 0$, since otherwise $2A = 2B$ which gives $\boldsymbol{ab}\in D(1, 1)$, and we want to prove that $[C]\cap[A, B] = 0$. Indeed, if not, then eliminating the cases, where determinants are not equal, one gets the following possibilities: either

(1) $2C = 2A+2B$,

or

(2) C or $3C = A+B$ or $3A+B$ or $A+3B$ or $3A+3B$.

Consider (1). We obtain $\langle 1, 1, ab, ab\rangle = \langle a, a, b, b\rangle$ and we show that this is impossible by applying piecewise equivalence. Observe that (a, a) can be changed dyadically only into $(-a, -a)$ and similarly (b, b) only into $(-b, -b)$. Now (a, b), $(-a, b)$ etc. represent only 2 elements of $g(k)$ and so cannot be changed dyadically in a non-trivial manner. Hence there is no way of getting either 1 or ab by applying dyadic changes to (a, a, b, b) and consequently (1) cannot hold.

As to (2), we observe that the possibilities are $\pm C = \pm A\pm B$. Here the only one non-obvious possibility is $A+B+C = 0$ (all the others are ruled out by $|D(c, d)|\leqslant 2$, $\boldsymbol{cd}\neq -\boldsymbol{1}$). But this implies $\langle 1, 1, 1\rangle = \langle a, b, ab\rangle$ which again contradicts piecewise equivalence. Hence

$$G_0 = [A]\oplus[B]\oplus[C]\oplus[E] \cong (\boldsymbol{Z}/4\boldsymbol{Z})^{(3)}\oplus\boldsymbol{Z}/2\boldsymbol{Z}.$$

This completes the proof of Theorem 2.4.

Proof of Theorem 2.5. Let k be a real field with $q = 8$. In each of the six cases of the theorem we fix an ordering of k and write $g(k) = \{\boldsymbol{1}, -\boldsymbol{1}\}\times\{\boldsymbol{1}, \boldsymbol{a}\}\times\{\boldsymbol{1}, \boldsymbol{b}\}$, where a and b are assumed to be positive in the given ordering of k. We denote the generators of G_0 by $E = \langle 1\rangle - -\langle -1\rangle$, $A = \langle 1\rangle - \langle a\rangle$, etc., as in the proof of the preceding theorem. Note that now E is of infinite order and by Lemma 1.10, we have

$$G_0 = [E]\oplus G_1,$$

where $G_1 = [A, B, C]$ is to be determined.

Case (i). $q_2 = 4$.

Assume (I). In this case $\boldsymbol{a}, \boldsymbol{b}\in D(1, 1)$ and $\langle 1, -a\rangle$, $\langle 1, -b\rangle$ are easily shown to be universal. Hence by Proposition 1.11,

$$G_1 = [A, B] = [A]\oplus[B] \cong (\boldsymbol{Z}/2\boldsymbol{Z})^{(2)}.$$

If there is only one universal binary class, then $A+B+C \neq 0$ and we obtain

$$G_1 = [A, B, C] = [A] \oplus [B] \oplus [C] \cong (\boldsymbol{Z}/2\boldsymbol{Z})^{(3)},$$

which proves (II).

Case (ii). $q_2 = 2$.

Assume a is a sum of two squares and b is not. If an element c is a sum of squares in k, then it is already a sum of two squares. Indeed, let t be the minimal number such that any sum of squares in k is a sum of t squares and $2^\tau \leqslant t < 2^{\tau+1}$. Then $q \geqslant 2 \cdot 2^{\tau(\tau+1)/2} \geqslant 2t$ ([11], Satz 25), and it follows easily that in case $q = 8$ we have $t = 2$. A consequence of this fact is that $2A = 0$ and B and C are of infinite order.

Assume now (III). We may assume that $(1, -a)$ is universal. Hence $(1, -a) \approx -b$ and $\langle 1, b\rangle = \langle a, ab\rangle$, i.e. $B = A+C$. Hence

$$G_1 = [A, B] = [B] \oplus [A] \cong \boldsymbol{Z} \oplus \boldsymbol{Z}/2\boldsymbol{Z}.$$

Subcase (IV). We have $\langle 1, 1\rangle = \langle a, a\rangle$, hence $\langle b, b\rangle = \langle ab, ab\rangle$ and $2B = 2C$. Now $G_1 = [B, A, B-C]$, where B is of infinite order and $2A = 2(B-C) = 0$. Hence $G_1 = [B] \oplus [A, B-C]$. Now $A \neq B-C$, since otherwise $\langle 1, b\rangle = \langle a, ab\rangle$, $(1, -a) \approx -b$ and so $(1, -a)$ would be a second universal form, contrary to (IV). Thus

$$G_1 = [B] \oplus [A] \oplus [B-C] \cong \boldsymbol{Z} \oplus (\boldsymbol{Z}/2\boldsymbol{Z})^{(2)}.$$

Case (iii). $q_2 = 1$.

Proposition 1.19 asserts that $G(k)$ is a torsion free group and so A, B, C are all of infinite order.

Assume (V). Without loss of generality let $(1, a)$ represent more than 2 elements of $g(k)$, i.e. $(1, a) \approx b$. Hence $\langle 1, a\rangle = \langle b, ab\rangle$ and $A = B+C$ and $G_1 = [A, B]$. Now Proposition 1.21 proves that

$$G_1 = [A] \oplus [B] \cong \boldsymbol{Z}^{(2)}.$$

Subcase (VI). By Proposition 1.22, the field is superpythagorean and now Proposition 1.23 proves that

$$G_1 = [A] \oplus [B] \oplus [C] \cong \boldsymbol{Z}^{(3)}.$$

This completes the proof of Theorem 2.5.

3. Classification of Witt groups for fields with $q \leqslant 8$.

The Witt group $W(k)$ of a field k can be defined as the factor group $G(k)/H$, where H is the subgroup of $G(k)$ generated by the hyperbolic plane $\langle 1, -1\rangle$. The canonical surjection $f\colon G(k) \to W(k)$ can be easily shown to act in the following manner:

$$f(\langle a_1, \ldots, a_n\rangle - \langle b_1, \ldots, b_m\rangle) = \langle a_1, \ldots, a_n, -b_1, \ldots, -b_m\rangle \bmod H.$$

Hence all the results of Section 1 concerning sets of generators for $G(k)$ can be reformulated for the case of Witt groups. If $G(k) = X_1 \oplus \ldots \oplus X_n$, then $W(k) = f(X_1) + \ldots + f(X_n)$ and if $H \subset X_1$, then $W(k) = f(X_1) \oplus \ldots \oplus f(X_n)$, where $f(X_1) \cong X_1/H$ and $f(X_i) \cong X_i$ for $i > 1$.

Hence, to obtain a classification for Witt groups of fields with $q \leqslant 8$ we shall use the classification of Grothendieck groups carried out in Section 2. In each of the cases we find a direct summand X of $G(k)$ such that $H \subset X$, and we determine a direct sum decomposition for X/H (Proposition 3.1) and then write automatically a direct sum decomposition for $W(k)$. Observe that for X we can take $[\langle 1\rangle] \oplus [\langle 1\rangle - \langle -1\rangle]$, whenever $\langle 1\rangle - \langle -1\rangle$ generates a direct summand of $G(k)$, since $\langle 1, -1\rangle = 2\langle 1\rangle - (\langle 1\rangle - \langle -1\rangle)$. It turns out that $\langle 1\rangle - \langle -1\rangle$ generates a direct summand for all fields k with $q \leqslant 8$, as can be seen immediately from the decompositions of $G(k)$ given in Section 2. By Lemma 1.10, this happens for all real fields and for non-real fields one can easily prove that $\langle 1\rangle - \langle -1\rangle$ generates a direct summand of $G_0(k)$ in each of the following cases (independently on the value of q): (i) $s = 1$ or 2, (ii) $s > 2$ and the class $s\langle 1\rangle$ is universal (then $\langle 1\rangle - \langle -1\rangle$ is an element of maximal order in $G_0(k)$ and generates a direct summand by [16], Corollary 2)[1].

PROPOSITION 3.1. *Suppose $\langle 1\rangle - \langle -1\rangle$ generates a direct summand of $G_0(k)$, $X = [\langle 1\rangle] \oplus [\langle 1\rangle - \langle -1\rangle]$ and $H = [\langle 1, -1\rangle]$.*

If k is a non-real field and s is the stufe of k, then $X/H \cong \boldsymbol{Z}/2s\boldsymbol{Z}$ and the group is generated by $\langle 1\rangle \bmod H$.

If k is a real field, then $X = [\langle 1\rangle] \oplus H$, and so $X/H \cong \boldsymbol{Z}$, where the group is generated by $\langle 1\rangle \bmod H$.

Proof. In the real case there is nothing to prove and so we assume that k is non-real. We define $h\colon X \to \boldsymbol{Z}/2s\boldsymbol{Z}$ by putting

$$h\big(x\langle 1\rangle + m(\langle 1\rangle - \langle -1\rangle)\big) = (x+2m) \pmod{2s}.$$

Clearly h is a surjective homomorphism and $\operatorname{Ker} h$ can be easily shown to coincide with H. Hence the result.

THEOREM 3.2 (Classification Theorem for Witt groups of fields with $q \leqslant 8$). *Let k be a field of characteristic other than 2 and with square class number $q \leqslant 8$. Then the Witt group $W(k)$ is determined as follows.*

1. $q = 1$: $W(k) \simeq \boldsymbol{Z}/2\boldsymbol{Z}$.

2. $q = 2$, *k non-real:*

(2.1) $\quad W(k) \simeq (\boldsymbol{Z}/2\boldsymbol{Z})^{(2)}$, *if* $s = 1$,

(2.2) $\quad \simeq \boldsymbol{Z}/4\boldsymbol{Z}$, *if* $s = 2$.

[1] Added in proof. It can be proved that $\langle 1\rangle - \langle -1\rangle$ always generates a direct summand in $G_0(k)$. The proof will appear in the Proc. of J. Bolyai Math. Soc. Colloquium on Number Theory held at Debrecen in October 1974.

$q = 2$, k *real*:

(2.3) $W(k) \cong \mathbf{Z}$.

3. $q = 4$, k *non-real*:

(3.1) $W(k) \cong (\mathbf{Z}/2\mathbf{Z})^{(3)}$, *if* (I) *of Theorem* 2.3 *holds and* $s = 1$,

(3.2) $\cong \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, *if* (I) *holds and* $s = 2$,

(3.3) $\cong (\mathbf{Z}/2\mathbf{Z})^{(4)}$, *if* (II) *holds*,

(3.4) $\cong (\mathbf{Z}/4\mathbf{Z})^{(2)}$, *if* (III) *holds*.

$q = 4$, k *real*:

(3.5) $W(k) \cong \mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, *if k is non-pythagorean*,

(3.6) $\cong \mathbf{Z} \oplus \mathbf{Z}$, *if k is pythagorean.*

4. $q = 8$, k *non-real*:

(4.1) $W(k) \cong (\mathbf{Z}/2\mathbf{Z})^{(4)}$, *if* $q_2 = u_2 = 8$ *and* $s = 1$,

(4.2) $\cong \mathbf{Z}/4\mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^{(2)}$, *if* $q_2 = u_2 = 8$ *and* $s = 2$,

(4.3) $\cong (\mathbf{Z}/2\mathbf{Z})^{(5)}$, *if* $q_2 = 8$, $2 \leqslant u_2 < 8$ *and* $s = 1$,

(4.4) $\cong \mathbf{Z}/4\mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^{(3)}$, *if* $q_2 = 8$, $2 \leqslant u_2 < 8$ *and* $s = 2$,

(4.5) $\cong (\mathbf{Z}/2\mathbf{Z})^{(6)}$, *if* $q_2 = 8$, $u_2 = 1$ *and there exists* $a \in k^*$ *such that* $|D(1, a)| = 4$,

(4.6) $\cong (\mathbf{Z}/2\mathbf{Z})^{(8)}$, *if* $q_2 = 8$, $u_2 = 1$ *and* $|D(1, a)| \leqslant 2$ *for every non-universal form* $(1, a)$,

(4.7) $\cong (\mathbf{Z}/4\mathbf{Z})^{(2)} \oplus \mathbf{Z}/2\mathbf{Z}$, *if* $q_2 = 4$, $u_2 \geqslant 2$ *and* $s = 2$,

(4.8) $\cong \mathbf{Z}/8\mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^{(2)}$, *if* $q_2 = 4$ *and* $s = 4$,

(4.9) $\cong (\mathbf{Z}/4\mathbf{Z})^{(2)} \oplus (\mathbf{Z}/2\mathbf{Z})^{(2)}$, *if* $q_2 = 4$, $u_2 = 1$ *and* $s = 2$,

(4.10) $\cong (\mathbf{Z}/4\mathbf{Z})^{(4)}$, *if* $q_2 = 2$.

5. $q = 8$, k *real*:

(5.1) $W(k) \cong \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^{(2)}$, *if* $q_2 = 4$ *and* $u_2 \geqslant 2$,

(5.2) $\cong \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^{(3)}$, *if* $q_2 = 4$ *and* $u_2 = 1$,

(5.3) $\cong \mathbf{Z}^{(2)} \oplus \mathbf{Z}/2\mathbf{Z}$, *if* $q_2 = 2$ *and* $u_2 \geqslant 2$,

(5.4) $\cong \mathbf{Z}^{(2)} \oplus (\mathbf{Z}/2\mathbf{Z})^{(2)}$, *if* $q_2 = 2$ *and* $u_2 = 1$,

(5.5) $\cong \mathbf{Z}^{(3)}$, *if k is pythagorean but not superpythagorean*,

(5.6) $\cong \mathbf{Z}^{(4)}$, *if k is superpythagorean.*

Remark. The fields in all the cases are known to exist except in (4.3), (4.4), (4.7) and (5.2).

4. Examples. In this section we give examples of fields corresponding to the Classification Theorems 2.4 and 2.5. For each case, except 2.4. II and 2.5. II, we point out a field which satisfies the conditions imposed in Classification Theorems. Let us remark that in [17] there have been given examples of fields showing that all the cases of Theorems 2.1, 2.2 and 2.3 actually occur.

We shall use four different constructions of fields with finite square class number: Gross and Fischer's, formal power series fields over a field with finite square class number, quadratic extensions of fields with finite square class number and a construction of Elman and Lam. First we tate the result of Gross and Fischer ([4], pp. 301–302).

Lemma 4.1. *Let k be any field of characteristic other than two and let $\{a_i \in k^*: i \in I\}$ be any set of representatives for a subgroup S of the group $g(k) = k^*/k^{*2}$. Then there exists an algebraic extension K of k such that $\{a_i: i \in I\}$ is a set of representatives for elements of the group $g(K)$. K can always be chosen non-real and if k is real and $-1 \in S$, then K can be chosen real, too.*

This lemma enables us to construct fields of the type 2.4.I and 2.5.I. In fact, using Lemma 4.1, one can prove that for any integer $n \geqslant 0$ there exists a field k such that $q = u_2 = 2^n$ (i.e. every binary form over k is universal; see [1], p. 407; [3], (3.8); [18], Theorem 2.3). This comprises 2.4.I.

The case 2.5.I. We shall prove that *for any integer $n > 0$ there exists a real field k such that $q = 2^n$, $q_2 = u_2 = 2^{n-1}$.*

For $n = 3$ we shall obtain a field satisfying 2.5.I. In the case $n = 1$ we can put $k = \mathbf{R}$, so assume $n > 1$. We choose n prime numbers $p_1, \ldots, p_n$ such that $p_i \equiv 1 \pmod 4$, $i = 1, \ldots, n$ and the g.c.d. $(p_i + p_j, p_1 \ldots p_n) = 1$ for all i, j, $1 \leqslant j < i \leqslant n$. Here $p_1 \equiv 1 \pmod 4$ can be chosen arbitrarily and if $p_1, \ldots, p_m$ have already been chosen in such a way that $p_i \equiv 1 \pmod 4$, $i = 1, \ldots, m$, the g.c.d. $(p_i + p_j, p_1 \ldots p_m) = 1$ for $1 \leqslant j < i \leqslant m$ and $p_i \equiv 1 \pmod{p_j}$, then we pick up a prime p_{m+1} such that $p_{m+1} \equiv 1 \pmod{4p_j}$, $j = 1, \ldots, m$. Then it is easy to check that $p_1, \ldots, p_{m+1}$ have the required property (cf. [18]).

Now, according to Lemma 4.1, there exists a real algebraic extension k of the rationals such that

$$g(k) = \{1, -1\} \times \{1, p_1\} \times \ldots \times \{1, p_{n-1}\}.$$

Here $q = 2^n$ and $q_2 = 2^{n-1}$, since every p_i is a sum of two squares. Since $p_i + p_j$ is coprime with $p_1 \ldots p_{n-1}$, it is a square in k, that is, for every pair of indices i, j we have $\langle 1, -p_i \rangle \approx p_j$. Also $\langle 1, -p_i \rangle \approx -1$, i.e. the forms $\langle 1, -p_i \rangle$ represent all the basis elements of $g(k)$, hence each of them is universal. Multiplying these universal forms according to the rule introduced in the proof of Lemma 1.8, we obtain 2^{n-1} universal classes. But $u_2 < 2^n$ (since $\langle 1, 1\rangle$ is not universal), hence $u_2 = 2^{n-1}$ and the statement is proved.

We remark here that the same method gives also an example of a field k with $q = q_2 = u_2 = 2^n$. We choose k to be non-real with $g(k) = \{\mathbf{1}, \boldsymbol{p}_1\} \times \ldots \times \{\mathbf{1}, \boldsymbol{p}_n\}$. Then as above all the forms $\langle 1, -p_i\rangle = \langle 1, p_i\rangle$ are universal and they generate 2^n universal forms. Hence we have a field satisfying 2.4.I.

The cases 2.4.II and 2.5.II will be left without examples. I do not know at the moment if the cases actually do occur [2].

In most of the following examples we shall use the fields of formal power series. We state here without proof a lemma giving some known properties of quadratic forms over those fields.

LEMMA 4.2. *Let k be a field of characteristic not 2 and $K = k((t))$ be the field of formal power series over k. Then the following statements hold true.*

(4.2.1) $g(K) = g(k) \times \{\mathbf{1}, \boldsymbol{t}\}$, *in particular, if $q(k)$ is finite, then* $q(K) = 2q(k)$.

(4.2.2) *If $a, b \in k^*$ and (a, b) is not the hyperbolic plane, then it represents over K only those square classes of $g(K)$ which are of the form cK^{*2}, where $c \in k^*$ is represented by (a, b) over k.*

(4.2.3) *If $a, b \in k^*$, then (a, bt) represents only 2 elements of $g(K)$ over K (that is, $\boldsymbol{a}$ and $\boldsymbol{bt}$).*

(4.2.4) *The hyperbolic plane is the only universal class over K, that is,* $u_2(K) = 1$.

(4.2.5) *If k is non-real, then so is K and $s(K) = s(k)$.*

The cases 2.4.III and 2.4.IV. *For any integer $n \geqslant 3$ and any m, $1 \leqslant m \leqslant n$, there exists a field K such that $q = q_2 = 2^n$, $u_2 = 1$, every anisotropic binary form represents at most 2^m elements of $g(K)$ and there is an anisotropic binary form representing exactly 2^m elements of $g(K)$.* For take any field k such that $q(k) = 2^m$, $s(k) = 1$ and every binary form over k is universal. Put $K = k((t_1)) \ldots ((t_{n-m}))$ and apply Lemma 4.2 to check that K has the required properties. The cases $n = 3$, $m = 2$ and $n = 3$, $m = 1$ comprise 2.4.III and 2.4.IV, respectively.

The case 2.4.V. *For any integer $n \geqslant 3$ there exists a non-real field K such that $q = 2^n$, $q_2 = 4$ and $s = 4$.* Here the field $K = \boldsymbol{Q}_2((t_1)) \ldots ((t_{n-3}))$, where $\boldsymbol{Q}_2$ denotes the field of 2-adic numbers, satisfies the requirements (for $n = 3$ we have $K = \boldsymbol{Q}_2$ which falls under 2.4.V). It would be desirable to find out whether or not the second possibility (i.e. $s = 2$ and $u_2 = 2$) appearing in 2.4.V actually occurs.

The case 2.4.VI. *For any integer $n \geqslant 3$ there exists a non-real field K such that $q = 2^n$, $q_2 = 4$, $s = 2$ and $u_2 = 1$* (put $n = 3$ to obtain 2.4.VI). Let k be an algebraic extension of $\boldsymbol{Q}(\sqrt{-2})$ with $g(k) = \{\mathbf{1}, -\mathbf{1}\} \times \{\mathbf{1}, \boldsymbol{a}\}$, where $a^2 = -2$. Here $s = 2$ and every binary form is universal (see [17], p. 35), in particular, $q_2(k) = 4$. Put $K = k((t_1)) \ldots ((t_{n-2}))$ and apply Lemma 4.2 to obtain the result.

The case 2.4.VII. *For any integer $n \geqslant 2$ there exists a non-real field K such that $q = 2^n$, $q_2 = 2$, $u_2 = 1$ and $s = 2$* ($n = 3$ gives 2.4.VII). Indeed, let p be a prime number congruent to $3 \pmod 4$ and put $K = F_p((t_1)) \ldots ((t_{n-1}))$ or $\boldsymbol{Q}_p((t_1)) \ldots ((t_{n-2}))$ where F_p denotes a prime field of characteristic p and $\boldsymbol{Q}_p$ is the field of p-adic numbers. Well known behaviour of binary forms over F_p and $\boldsymbol{Q}_p$ and Lemma 4.2 yield the result.

Now we shall discuss the four remainig cases of Theorem 2.5. First we quote some results of Gross and Fischer concerning the behaviour of the group $g(k)$ under quadratic extensions of k. Let $K = k(\sqrt{a})$ be a quadratic extension of the field k ($\operatorname{char} k \neq 2$). Define $i\colon g(k) \to g(K)$ by putting $i(bk^{*2}) = bK^{*2}$ and $N\colon g(K) \to g(k)$ by $N(aK^{*2}) = N_{K/k}(a)k^{*2}$. These are group homomorphisms and *the sequence*

$$1 \to \{k^{*2}, ak^{*2}\} \to g(k) \xrightarrow{i} g(K) \xrightarrow{N} g(k)$$

is exact (cf. [4], p. 298). From this we get easily the following result.

LEMMA 4.3. *Let k be a field with* $\operatorname{char} k \neq 2$ *and $g(k) = \{\mathbf{1}, \boldsymbol{a}\} \times h$, $K = k(\sqrt{a})$. Assume further that $D(1, -a) = \prod_{i \in I} \{\mathbf{1}, \boldsymbol{b}_i\}$ and $c_i \in K$ are chosen to satisfy $N_{K/k}(c_i) = b_i$, $i \in I$. Then*

$$g(K) = h \times \prod_{i \in I} \{\mathbf{1}, \boldsymbol{c}_i\}$$

(here h is meant to be the subgroup of $g(K)$ with the same coset representatives as in $g(k)$).

The case 2.5.III. Let k be a real algebraic extension of the rationals such that $g(k) = \{\mathbf{1}, -\mathbf{1}\} \times \{\mathbf{1}, \mathbf{2}\}$ (Lemma 4.1). We consider $K = k(\sqrt{2})$ and prove that K satisfies 2.5. III. The form $(1, -2)$ is universal over k, hence $D(1, -2) = \{\mathbf{1}, -\mathbf{1}\} \times \{\mathbf{1}, \mathbf{2}\}$.

We have $N_{K/k}(1 + \sqrt{2}) = -1$ and $N_{K/k}(2 + \sqrt{2}) = 2$, hence, by Lemma 4.3, -1, $1 + \sqrt{2}$, $2 + \sqrt{2}$ are the representatives of a basis for the group $g(K)$. Observe that K is a real field and $q = 8$. Moreover, $2 + \sqrt{2}$ is a sum of two squares,

$$2 + \sqrt{2} = (1 + \tfrac{1}{2}\sqrt{2})^2 + (\tfrac{1}{2}\sqrt{2})^2,$$

[2] Added in proof. I can only prove the following. If there exists a real field satisfying 2.5.II, then a suitable quadratic extension of it is a non-real field satisfying 2.4.II.

while $1+\sqrt{2}$ is not, since its conjugate is negative in the ordering of K induced by that of $\boldsymbol{R}$. It follows that $D_K(1, 1) = \{K^{*2}, (2+\sqrt{2})K^{*2}\}$, i.e. $q_2 = 2$. Further, $u_2 \leqslant q_2 = 2$ (since the universality of $(1, a)$ implies that $-a$ is a sum of two squares) and we prove $u_2 = 2$ by establishing that $\left(1, -(2+\sqrt{2})\right)$ is universal. In fact, the equality above implies that $\left(1, -(2+\sqrt{2})\right) \approx -1$, and we have also $1-(2+\sqrt{2}) = (-1)(1+\sqrt{2})$, that is $\left(1, -(2+\sqrt{2})\right) \approx -(1+\sqrt{2})$. Hence the form represents all the basis elements of $g(K)$ and so is universal. Summing up: *K is real*, $q = 8$, $q_2 = u_2 = 2$, that is, K falls under 2.5.III.

The case 2.5.IV. *For any integer $n \geqslant 3$ there exists a real field K such that $q = 2^n$, $q_2 = 2$ and $u_2 = 1$.* Take k as in the preceding example and put $K = k\left((t_1)\right) \ldots \left((t_{n-2})\right)$. Lemma 4.2 gives the result. When $n = 3$ we obtain a field satisfying 2.5.IV.

The case 2.5.V. If k falls under 2.5.V, then, by Proposition 1.22(ii), the number r of orderings is $\leqslant 3$. On the other hand, the field is pythagorean, so $r \geqslant 3$, by Corollary 1.13. Hence $r = 3$ and the field satisfies SAP ([2], Corollary 5.7). Conversely, if $q(k) = 8$, k is pythagorean and satisfies SAP, then $r = 3$ and there must be an anisotropic binary form representing more than 2 elements of $g(k)$, since otherwise, by Proposition 1.22(i), k is superpythagorean, i.e. $r = 4$.

Hence 2.5.V characterizes pythagorean fields with $q = 8$ satisfying SAP. The existence of such a field for any q has been proved by Elman and Lam ([2], p. 1187).

The case 2.5.VI. By Proposition 1.22(i), the field is superpythagorean. Clearly, for any $n \geqslant 1$ there exists a superpythagorean field with square class number $q = 2^n$, for example $\boldsymbol{R}\left((t_1)\right) \ldots \left((t_{n-1})\right)$, as follows directly from Lemma 4.2.

Remark. The above examples of fields provide at the same time examples for the Classification Theorem 3.2 for Witt groups of fields with $q \leqslant 8$. However, here the number of cases where the existence of fields is not known, increases to 4. In fact, the case 2.4.II splits into two cases 3.2(4.3) and 3.2(4.4), the case 2.4.V also splits into two cases one of which (3.2(4.7)) is not covered with any example, and finally, the case 2.5.II goes into 3.2(5.2).

References

[1] C. M. Cordes, *The Witt group and the equivalence of fields with respect to quadratic forms*, J. Algebra 26 (1973), pp. 400–421.

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

[3] — — *Quadratic forms and the u-invariant. II*, Invent. Math. 21 (1973), pp. 125–137.

[4] H. Gross and H. R. Fischer, *Non real fields k and infinite dimensional k-vector-spaces*, Math. Ann. 159 (1965), pp. 285–308.

[5] I. Kaplansky, *Quadratic forms*, J. Math. Soc. Japan 5 (1953), pp. 200–207.

[6] — *Fröhlich's local quadratic forms*, J. Reine Angew. Math. 239/240 (1969), pp. 74–77.

[7] — *Linear Algebra and Geometry — A second course*, Boston 1969.

[8] S. Lang, *Algebra*, Reading 1971.

[9] F. Lorenz, *Quadratische Formen über Körpern*, Lecture Notes in Mathematics No. 130, Berlin 1970.

[10] O. T. O'Meara, *Introduction to Quadratic Forms*, Berlin 1963.

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

[12] W. Scharlau, *Quadratische Formen und Galois-Cohomologie*, Invent. Math. 4 (1967), pp. 238–264.

[13] — *Quadratic forms*, Queen's Papers on Pure and Applied Mathematics No. 22, Kingston, Ont., 1969.

[14] A. Sładek, *Grothendieck groups of quadratic forms over formally real fields*, Uniw. Śląski w Katowicach — Prace Mat. 5 (1974), pp. 41–47.

[15] L. Szczepanik, *Quaternion algebras and binary quadratic forms*, Uniw. Śląski w Katowicach — Prace Mat. 6 (1975).

[16] T. Szele, *On direct decompositions of abelian groups*, J. London Math. Soc. 28 (1953), pp. 247–250.

[17] K. Szymiczek, *Grothendieck groups of quadratic forms and G-equivalence of fields*, Proc. Cambridge Philos. Soc. 73 (1973), pp. 29–36. Corrigendum, ibid. 74 (1973), p. 199.

[18] — *Universal binary quadratic forms*, Uniw. Śląski w Katowicach — Prace Mat. 5 (1974), pp. 49–57.

[19] E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. 176 (1937), pp. 31–44.

INSTITUTE OF MATHEMATICS
SILESIAN UNIVERSITY
Katowice

Received on 8.4.1974 (561)

ACTA ARITHMETICA
XXVIII (1975)