

## QUADRATIC FORMS OVER NONFORMALLY REAL FIELDS WITH A FINITE NUMBER OF QUATERNION ALGEBRAS

CRAIG M. CORDES

**This paper is concerned with quadratic forms over a nonformally real field,  $F$ , of characteristic not two, which has only a finite number,  $m$ , of quaternion algebras. The number  $q = |\dot{F}/\dot{F}^2|$  is always assumed to be finite. Of central importance will be the radical,  $R$ , which can be defined by  $R = \{a \in \dot{F} \mid G(1, -)a = \dot{F}\}$  where  $\dot{F} = F - \{0\}$  and  $G(1, -a)$  is the set of nonzero elements represented by the form  $x^2 - ay^2$  over  $F$ . The main result here is that a finite Witt ring (and hence the complete quadratic form structure) is determined when  $m = 2$  by the Witt group and the order of  $\dot{F}/R$ .**

Other results include analyzing the quadratic form structure for fields which satisfy  $|\dot{F}/R| \leq 8$  and discovering an upper bound for  $m$  in terms of  $q$  and the largest index in  $\dot{F}$  of all  $G(1, a)$ . Finally, the concept of a quadratic form scheme is introduced. This idea comes from an attempt to abstract value sets of binary quadratic forms in order to eliminate the immediate necessity of a field in their study.

Kaplansky [4] showed that if  $m = 2$ , the  $u$ -invariant of a nonformally real field is four. Lam and Elman [3] demonstrated that the quaternion algebras form a subgroup of the Brauer group only when  $u = 1, 2, 4$ , or  $8$ . As a consequence of their proof of this, it follows that if  $m = 4$ ,  $u = 4$  also. Moreover, it is well known that when  $u = 4$ , the quaternion algebras do form a subgroup; and this was the key needed in [1] to discover the Witt group structure for fields with  $u = 4$ . These group structure theorems are used here to prove the main result. In [2] it was shown that many results concerning  $\dot{F}^2$  remain valid for  $R$ . This is the case in the analysis of fields with  $|\dot{F}/R| \leq 8$ . The structure answers are virtually the same as those found in [1] for fields with  $|\dot{F}/\dot{F}^2| \leq 8$ . Since the value sets of binary forms completely determine quadratic forms over a field, quadratic form schemes may be of value. Here some elementary questions are answered; and an interesting example is given of a scheme for a field which would have  $q = 16$ ,  $u = m = 4$ , and level (Stufe)  $s = 2$  if the field existed.

2. Throughout this section  $F$  will be a nonformally real field with  $m = 2$  and  $q < \infty$ . Before the main result of this section,

some preliminaries are needed.

LEMMA 1. *Let  $F$  be a nonreal field with  $m=2, q < \infty$ , and radical  $R$ . For  $a, b \in \dot{F}$ ,  $G(1, a) = G(1, b)$  if and only if  $ab \in R$ .*

*Proof.* The sufficiency follows from Proposition 1 in [2]. Suppose then that  $G(1, a) = G(1, b)$ . Now  $c \in G(1, a)$  if and only if  $\{c, -a\} = 1$  where  $\{c, -a\}$  is the Hilbert symbol for  $c, -a$ . So it follows that  $\{c, -a\} = \{c, -b\}$  for all  $c \in \dot{F}$ . For  $m = 2$  the Hilbert symbol is a multiplicative function while one variable is fixed. Hence,  $\{c, ab\} = 1$  for all  $c \in \dot{F}$  and  $G(1, -ab) = \dot{F}$ .

LEMMA 2. *Let  $V$  be an  $n$ -dimensional vector space over  $GF(q)$ . If  $W$  is a  $k$ -dimensional subspace of  $W$ , then there are  $(q^{n-k} - 1)/(q - 1)$   $(n - 1)$ -dimensional subspaces of  $V$  containing  $W$ .*

The proof is elementary and will be omitted. However, from Lemma 2 comes an important corollary.

COROLLARY. *Let  $F$  be a nonreal field with  $m = 2, q = 2^r < \infty$ , and radical  $R$ . If  $A \supseteq R$  is a subgroup of index 2 in  $\dot{F}$ , then there is an  $a \in \dot{F}$  such that  $G(1, a) = A$ .*

*Proof.* By Proposition 1 of [2],  $R \subset G(1, b)$  for all  $b \in \dot{F}$ . Since  $m = 2$ ,  $G(1, b)$  is a subgroup of index 1 or 2 (depending on whether  $-b \in R$  or  $-b \notin R$ ). Now let  $a_1, \dots, a_{2^t}$  be representatives for the cosets of  $R$  in  $\dot{F}$ . Then the  $G(1, a_i), 1 \leq i \leq 2^t$ , by Lemma 1, are all distinct, and all but one of them is a subgroup, containing  $R$ , of index two.  $\dot{F}/\dot{F}^2$  can be considered as a vector space over  $GF(2)$  of dimension  $r$ , and  $R/\dot{F}^2$  is a subspace of dimension  $r - t$ . So by Lemma 2, there are  $2^t - 1$  subgroups of  $\dot{F}$  containing  $R$  which have index 2. Since  $A$  is one of them,  $A = G(1, a_i)$  for some  $1 \leq i \leq 2^t$ .

At this time the structure for the Witt group  $W$  of  $F$  needs to be recalled. When  $m = 2$  (and hence  $u = 4$ ), this structure is obtained from Theorem 4.5 [1]. Let  $[c, d]$  denote the quaternion algebra with structure constants  $c, d \in \dot{F}$ ,  $G$  denote  $G(1, 1)$ ,  $H$  denote the group of quaternion algebras (in the Brauer group of  $F$ ), and  $\bar{H}$  denote the subgroup of  $H$  whose members have the form  $[a, a]$ . In addition, let the groups  $G/\dot{F}^2, \dot{F}/G$ , and  $H/\bar{H}$  be freely generated by  $\{a_i \dot{F}^2\}_{i \in I}, \{b_j G\}_{j \in J}$ , and  $\{[c_l, d_l] \bar{H}\}_{l \in L}$  respectively. Also assume that if  $s = 2$ , then  $0 \in I$  and  $a_0 = -1$ . If  $\varphi$  is a quadratic form over  $F$ , let  $\bar{\varphi}$  denote the element in  $W$  which represents the

class of forms having anisotropic parts equivalent to that of  $\varphi$ . Write  $\langle \bar{\varphi} \rangle$  to mean the subgroup of  $W$  generated by  $\bar{\varphi}$ . As a group,  $W$  is given by the following direct sums of cyclic groups:

$$\begin{aligned}
 s = 1: W &= \langle (\bar{1}) \rangle \bigoplus_{i \in I} \langle (\bar{1}, a_i) \rangle \bigoplus \langle \bar{1}, c_1, d_1, c_1 d_1 \rangle, \\
 s = 2: W &= \langle (\bar{1}) \rangle \bigoplus_{i \in I - \{0\}} \langle (\bar{1}, -a_i) \rangle \bigoplus_{j \in J} \langle (\bar{1}, b_j) \rangle \bigoplus_{l \in L} \langle \bar{1}, -c_l, -d_l, c_l d_l \rangle, \\
 s = 4: W &= \langle (\bar{1}) \rangle \bigoplus_{i \in I} \langle \bar{1}, -a_i \rangle.
 \end{aligned}$$

In order to determine the ring structure of  $W$ , it is necessary to find out how the group generators multiply.  $(\bar{1})$  is the multiplicative identity, and any  $(\bar{1}, x)$  times a quaternary form of determinant 1 is 0 in  $W$  (since  $u = 4$ ). So the remaining cases are where binary forms comprise the product. Since  $m = 2$ , the product  $(\bar{1}, x) \otimes (\bar{1}, y)$  in  $W$  is either 0 or  $\bar{\psi}$  where  $\psi$  is the unique quaternary form of determinant 1. Also  $(\bar{1}, x) \otimes (\bar{1}, y) = 0$  if and only if  $-y \in G(1, x)$ . The goal will be to show that under correct hypotheses, a map between sets of these group generators can be constructed which preserves multiplication and addition. So the rings will be isomorphic. The following theorem formalizes the result.

**THEOREM 1.** *Let  $F$  be a nonformally real field with  $m = 2$ ,  $q = 2^r < \infty$ , and  $|R/\dot{F}^2| = 2^k$ . Then  $r \equiv k \pmod{2}$  if  $s = 1, 2$ , and  $r \not\equiv k \pmod{2}$  if  $s = 4$ . Moreover, the structure of the Witt ring is determined by its group structure and  $k$ .*

Before the proof, note that  $\dot{F}/\dot{F}^2$  is a group with exponent two and thus can be considered as a vector space over  $GF(2)$ . Hence, if  $\dot{F}^2 \subseteq B \subseteq C$  for multiplicative subgroups  $B, C$  of  $\dot{F}$ , then there is a subgroup  $A$  of  $\dot{F}$  with  $\dot{F}^2 \subseteq A$  such that  $C/\dot{F}^2$  is the direct sum (in the vector space) of  $A/\dot{F}^2$  and  $B/\dot{F}^2$ . In the forthcoming proof, this is denoted by  $C = A \otimes B$  because the above implies  $C$  is the direct product of  $A$  and  $B$  as well.

*Proof.* There are four different cases:  $s = 1, s = 4, s = 2$  with  $-1 \notin R$ , and  $s = 2$  with  $-1 \in R$ . The proofs are similar so only the case  $s = 2$  with  $-1 \notin R$  will be done in detail.

From Proposition 1 of [2],  $R \subset G(1, a)$  for all  $a \in \dot{F}$ . So for  $b \notin G(1, 1), G(1, 1) \cap G(1, b) = R \otimes A_1$  where  $|A_1/\dot{F}^2| = 2^{r-k-2}$  and  $\dot{F} = \langle -1, b \rangle \dot{F}^2 \otimes R \otimes A_1$ , ( $\langle -1, b \rangle \dot{F}^2$  is the subgroup in  $\dot{F}$  generated by  $-\dot{F}^2$  and  $b\dot{F}^2$ ). Now, if possible, choose  $a_1 \in A_1 - \dot{F}^2$ . Then  $A_1 = \langle a_1 \rangle \dot{F}^2 \otimes A_2$ ; and by the corollary to Lemma 2, there is an  $x$  such that  $G(1, -x) = \langle -1, b \rangle \dot{F}^2 \otimes R \otimes A_2$ . It is clear also from this that

$x \in G(1, 1) \cap G(1, b) \cap G(1, -x) = R \otimes A_2$ . Since  $G(1, -x) \neq \dot{F}$ , there is an  $a_2 \in A_2 - \dot{F}^2$  such that  $x = \alpha a_2$  for some  $\alpha \in R$ . By Lemma 1,  $G(1, -a_2) = G(1, -x)$ ; and so in particular,  $a_1 \notin G(1, -a_2)$ , or equivalently,  $a_2 \notin G(1, -a_1)$ . Also note  $G(1, -a_1) = \langle -1, b, a_1 \rangle \otimes R \otimes A_3$  where  $A_3 = G(1, -a_1) \cap A_2$ . In fact, by the preceding,  $A_2 = \langle a_2 \rangle \dot{F}^2 \otimes A_3$ . Summarizing,  $\dot{F} = \langle -1, b, a_1, a_2 \rangle \dot{F}^2 \otimes R \otimes A_3$  with  $G(1, 1) = \langle -1, a_1, a_2 \rangle \dot{F}^2 \otimes R \otimes A_3$ ,  $G(1, -a_1) = \langle -1, b, a_1 \rangle \dot{F}^2 \otimes R \otimes A_3$ , and  $G(1, -a_2) = \langle -1, b, a_2 \rangle \dot{F}^2 \otimes R \otimes A_3$ . If  $A_3 \neq \dot{F}^2$ , then exactly the same procedure can be used on it. That is, if  $A_3 = \langle a_3 \rangle \dot{F}^2 \otimes A_4$ , then there is an  $x$  such that  $G(1, -x) = \langle -1, b, a_1, a_2 \rangle \dot{F}^2 \otimes R \otimes A_4$ . Similarly  $a_3, a_4, A_5$  are obtained so that  $G(1, 1) = \langle -1, a_1, a_2, a_3, a_4 \rangle \dot{F}^2 \otimes R \otimes A_5$ ,  $G(1, -a_1) = \langle -1, b, a_1, a_3, a_4 \rangle \dot{F}^2 \otimes R \otimes A_5$ ,  $G(1, -a_2) = \langle -1, b, a_2, a_3, a_4 \rangle \dot{F}^2 \otimes R \otimes A_5$ ,  $G(1, -a_3) = \langle -1, b, a_1, a_2, a_3 \rangle \dot{F}^2 \otimes R \otimes A_5$ , and  $G(1, -a_4) = \langle -1, b, a_1, a_2, a_4 \rangle \dot{F}^2 \otimes R \otimes A_5$ . The process will continue to yield pairs  $a_n, a_{n+1}$  as long as  $|A_{n+1}/\dot{F}^2| \geq 2^2$ . Notice that at no point can  $A_n = \langle x \rangle \dot{F}^2$  because, if so,  $G(1, -x) = \dot{F}$ . But this contradicts  $x \notin R$ . Hence, the process stops after  $(r - k - 2)/2$  pairs of  $a_i$ 's have been selected. This shows  $r \equiv k \pmod{2}$ .

Since  $-1 \notin R$ , the group structure for  $W$  is  $W = \langle \bar{1} \rangle \bigoplus_{i=1}^{r-k-2} \langle \overline{(1, a_i)} \rangle \oplus \langle \overline{(1, b)} \rangle \langle \bigoplus \langle \overline{(1, -c, -d, cd)} \rangle$  where  $a_i, 1 \leq i \leq r - k - 2$ , can be selected as above and  $R = \langle a_{r-k-1}, \dots, a_{r-2} \rangle \dot{F}^2$ . Suppose  $F'$  is another field with  $m = 2$  and Witt ring  $W'$  such that  $W \cong W'$  (as groups) and  $k = k'$ . By Proposition 4.4 [1],  $q = q'$ ; and  $s = s'$  follows from the fact that the Witt group has exponent  $2s$ , (see [7]). So  $a'_i, 1 \leq i \leq r - k - 2$ , and  $b'$  can be obtained similarly to those for  $F$ . By the remarks preceding the theorem,  $\overline{(1, -a_i)} \otimes \overline{(1, b)} = 0$  and  $\overline{(1, -a_i)} \otimes \overline{(1, -a_j)} \neq 0$  if and only if  $\{i, j\} = \{2e - 1, 2e\}$  for some  $e, 1 \leq e \leq (r - k - 2)/2$ . Moreover, if  $\overline{(1, -a_i)} \otimes \overline{(1, -a_j)} \neq 0$ , it must be  $\overline{(1, -c, -d, cd)}$ . Similar statements hold for  $F'$ . Thus the map which takes  $\overline{(1)} \rightarrow \overline{(1)}$ ,  $\overline{(1, -a_i)} \rightarrow \overline{(1, -a'_i)}$  for  $1 \leq i \leq r - k - 2$ ,  $\overline{(1, b)} \rightarrow \overline{(1, b')}$ , and  $\overline{(1, -c, -d, cd)} \rightarrow \overline{(1, -c', -d', c'd')}$  extends to a ring isomorphism from  $W$  onto  $W'$ . This completes the proof for the case  $s = 2$  with  $-1 \notin R$ .

The case  $s = 1$  is done in exactly the same fashion except  $-1, b$  in the first step are replaced by  $a_1, a_2$  with  $a_1, a_2$ , and  $a_1 a_2 \notin R$ . This also works for  $s = 2$  with  $-1 \in R$ . When  $s = 4$ ,  $-1, b$  are replaced by  $-1$ ; and this accounts for the change in parity of  $r - k$ . The proof of Theorem 1 is now finished.

The theorem shows that when  $|W| = 4q < \infty$ , the Witt ring is determined by  $(W, +)$  and  $|R/\dot{F}^2|$ . However, no examples are known with  $q < \infty$  and  $R \neq \dot{F}$  or  $\dot{F}^2$ . If no fields with  $m = 2, q < \infty$ , and  $R \neq \dot{F}^2$  existed (which is unlikely), the above would imply the stronger theorem that the Witt ring for fields with  $|W| = 4q$  was determined

by the Witt group.

3. In this section, the analysis in [1] on fields with  $q \leq 8$  is generalized to fields whose radical has index  $t$  in  $\dot{F}$  of at most eight. If  $t = |\dot{F}/R| = 1$ , then  $u = 2$  and such fields are well-known. For example, see [1, p. 406]. Kaplansky [5] has shown that  $t \neq 2$  for nonreal fields. By Theorem 3.8 [1] and Theorem 3 [2],  $m \leq (1/t)\binom{t}{3} + 1$ . So if  $t = 4$ , then  $m = 2$  and the possible structures can be obtained from Theorem 1. There are three possibilities (for a fixed  $q$ ), and they correspond to  $s = 2$  with  $-1 \in R$  and  $-1 \notin R$  and to  $s = 1$ . If  $t = 8$ , then  $m \leq 8$  from the above and  $u \leq 8$  from the corollary to Theorem 1 [2]. By the discussion preceding Theorem 4 in [2] and by the same techniques used for Proposition 5.15 in [1], it is easily seen that for fields with fixed  $u = t$  and  $q$ , there are only three possible Witt rings (again corresponding to  $s = 2$  with  $-1 \in R$  and  $-1 \notin R$  and to  $s = 1$ ). The case  $t = 8, u = 8, m = 8$  falls into one of these three types. If  $t = 8$  and  $u < 8$ , then Theorem 6 [2] yields  $u = 4$  and Theorems 3, 4 [2] imply  $m \leq 4$ . The cases left to consider then, are  $t = 8, u = 4, m = 2$  or  $4$ , and  $s = 1, 2$  or  $4$ .

PROPOSITION 1. *There are no fields with  $u = 4, m = 4, s = 4$ , and  $t = 8$ .*

*Proof.* Suppose  $F$  were such a field. By Theorem 2 [2],  $G(1,1) = \langle c, d \rangle R$  where  $cd \notin R$ . (Note difference of meanings of  $G(1, 1)$  in [2] and here.) Also  $F = \langle -1, c, d \rangle R$ . A basis for the group of quaternion algebras is then  $[-1, -1]$  and  $[c, d]$ . Consequently,  $\pm 1 \notin G(c, d)$  and  $G(1, -c) = \langle -1, c \rangle R, G(1, -d) = \langle -1, d \rangle R, G(1, -cd) = \langle -1, cd \rangle R, G(1, cd) = \langle cd \rangle R, G(1, c) = \langle c \rangle R,$  and  $G(1, d) = \langle d \rangle R$ . Hence  $G(1, c, d, c) = \bigcup_{\alpha \in G(1, c), \beta \in G(1, d, c)} G(\alpha, \beta) = G(1, c) \cup G(1, d) \cup G(c, c) \cup G(c, d) = \langle c, d \rangle R$ . But this contradicts  $u = 4$ . So  $F$  does not exist.

LEMMA 3. *There are no fields with  $u = 4$  and  $G(1, 1) = R \cup -R$ .*

The proof of this is virtually identical to the one of Lemma 6.5 [1]. Just replace  $\dot{K}^2$  in 6.5 by  $R$  here. By continuing as in [1], it can be shown that fields with  $m = 4$  and  $s = 1, 2$  comprise three types and are unique up to equivalence (i.e., they have isomorphic Witt rings, see [1]).

PROPOSITION 2. *All fields with fixed  $q, t = 8, u = 4, s = 2, -1 \in R$ , and  $m = 4$  are equivalent.*

*Proof.* By Theorem 4 [2], there is an  $a \in \dot{F} - R$  such that

$|G(1, a)/R| > 2$ . So  $G(1, a) = \langle a, b \rangle R$ , and from this, it follows that  $G(1, ab) = G(1, b) = \langle a, b \rangle R$ . Hence, if  $\hat{F} = \langle a, b, c \rangle R$ , then  $G(1, xc) = \langle xc \rangle R$  for all  $x \in \langle a, b \rangle R$ . By using Proposition 2.2 [1], it is easy to see now that any two such fields must be equivalent.

The next two propositions are proved in the same manner. Note that by Lemma 3, Proposition 3 can be proved by replacing  $a$  in the proof of Proposition 2 with  $-1$ .

**PROPOSITION 3.** *All fields with fixed  $q, t = 8, u = 4, s = 2, -1 \notin R$ , and  $m = 4$  are equivalent.*

**PROPOSITION 4.** *All fields with fixed  $q, t = 8, u = 4, s = 1$ , and  $m = 4$  are equivalent.*

Actually the hypothesis of  $m = 4$  in the last 3 propositions is superfluous because by Theorem 1, it is impossible to have a field with  $s = 1$  or  $2, m = 2$ , and  $t = 8$ . Theorem 1 also implies the next result.

**PROPOSITION 5.** *All fields with fixed  $q, t = 8, u = 4, s = 4$ , and  $m = 2$  are equivalent.*

This completes all possibilities with  $t = 8$ . The existence of such fields is only known to the extent of the knowledge dealing with  $q = 8$  and  $R = \hat{F}^2$  (see §6 of [1]). Since  $m = 2$  or  $4$  implies  $u = 4$  for nonreal fields, the specification of  $u$  is unnecessary in all of the above cases. In fact, the parameters  $q, t, m, s$ , and whether or not  $-1 \in R$  determine the field with respect to quadratic forms (i.e., Witt ring). The question of  $-1 \in R$  is only relevant, of course, when  $s = 2$ . Theorem 2 is a summary of the results of this section.

**THEOREM 2.** *Let  $F$  be a nonreal field, with  $q < \infty$ , whose radical,  $R$ , has index  $t \leq 8$  in  $\hat{F}$ . Then the parameters  $q, t, m, s$ , and whether or not  $-1 \in R$  determine the Witt ring of  $F$ . The only possible sets of these parameters for a fixed  $q$  are*

- (1)  $t = 1, m = 1, s = 2$  or  $1$
- (2)  $t = 4, m = 2, s = 2$  (with  $-1 \in R$  or  $-1 \notin R$ ) or  $1$
- (3)  $t = 8, m = 4, s = 2$  (with  $-1 \in R$  or  $-1 \notin R$ ) or  $1$
- (4)  $t = 8, m = 2, s = 4$
- (5)  $t = 8, m = 8, s = 2$  (with  $-1 \in R$  or  $-1 \notin R$ ) or  $1$ .

4. If  $F$  is a field and  $|\hat{F}/G(1, a)| = p$ , then it is clear that the field has at least  $p$  quaternion algebras. Thus a (probably) crude estimate, in terms of the indices of the  $G(1, a)$  in  $\hat{F}$ , for the greatest

lower bound for the number  $m$  of quaternion algebras which a field has is the largest such index. In [1], best possible upper bounds for  $m$  in terms of  $q$  were obtained. In this section upper bounds for  $m$  for nonreal fields with  $q < \infty$  will be found in terms of  $q$  and the maximum index  $p$  of the  $G(1, a)$  in  $\dot{F}$ . When  $p = q/2$ , this result will yield the same answer as was found in [1].

By Theorem 3.8 [1] and its proof,  $m - 1$  is the number of anisotropic ternary forms of determinant 1 over  $F$ ; and an estimate for the number of such forms is what will be sought. Let  $d \notin -\dot{F}^2$ . Since  $|\dot{F}/G(1, d)| \leq p$ , there are at most  $p - 1$  binary forms  $\varphi_d$  of determinant  $d$  such that the ternary form  $\varphi_d \oplus (d)$  is anisotropic. This can be done for all  $d \notin -\dot{F}^2$ , and thus there are at most  $(q - 1)(p - 1)$  anisotropic ternary forms of determinant 1 counted in this way. But, of course, there is some overlap in this count. Every ternary form  $\varphi$  of determinant 1 represents  $|G(\varphi)/\dot{F}^2| d$ 's.

*Claim.* If  $\varphi = (a, b, ab)$  is anisotropic, then  $|G(\varphi)/\dot{F}^2| \geq 3q/2p$ .

*Proof.* There is a  $c \in G(a, b, ab) - G(a, b)$ . Suppose  $c = ax^2 + by^2 + abz^2$ . Let  $e = by^2 + abz^2$ . Then  $G(a, e) \not\subseteq G(a, b)$ . Consider  $G(a, e) - G(a, b) = a[G(1, ae) - G(1, ab)] = a[G(1, ae) - G(1, ab) \cap G(1, ae)]$ . Since  $G(a, e) \not\subseteq G(a, b)$ ,  $|[G(1, ab) \cap G(1, ae)]/\dot{F}^2| \leq 1/2 |G(1, ae)/\dot{F}^2|$ . Therefore, there are at least  $1/2 |G(1, ae)/\dot{F}^2|$  square classes represented by  $G(a, e)$  that are not represented by  $G(a, b)$ . But every binary form represents at least  $q/p$  square classes so  $|G(\varphi)/\dot{F}^2| \geq 3q/2p$  and the claim is proved.

By the claim and the preceding discussion, it now follows that the number of anisotropic ternary forms of determinant 1 is at most  $(2p(p - 1)(q - 1))/3q$ .

**THEOREM 3.** *Let  $F$  be a nonreal field with  $q < \infty$ . If  $p$  is the maximum index of all  $G(1, a)$  in  $F$ , then the number of nonsplit quaternion algebras over  $F$  is at most  $(2p(p - 1)(q - 1))/3q$ .*

This upper bound turns out to be best possible for extreme values of  $p$ . For example, if  $p = 1$ , then  $u \leq 2$  and there are no nonsplit quaternion algebras. If  $p = 2$ , then Theorem 3 implies  $m - 1 \leq 4(q - 1)/3q < 2$ . So  $m \leq 2$ . But  $p > 1$  means  $m > 1$  and hence  $m = 2$ . This was first shown by Kaplansky in [4]. The other extreme is when  $p = q/2$ . Here the theorem yields  $m - 1 \leq ((q - 1)(q - 2))/6$ , and this agrees with the findings of Proposition 4.3 [1]. However, it is not known whether the upper bound in Theorem 3 is best possible for other values of  $p$  between 2 and  $q/2$ .

5. The existence of fields with prescribed properties relating to quadratic forms can frequently be determined by observing what must happen to the value sets of binary forms. For this reason the concept of a quadratic form scheme is introduced here. The idea is to abstract value sets and eliminate the immediate necessity of a field.

DEFINITION. A *quadratic form scheme* consists of a (multiplicative) group  $A$  of exponent two and a set of subgroups  $\{X_a\}_{a \in A}$  which satisfy the following:

- (1)  $a \in X_a$  for all  $a \in A$
- (2) there is a  $-1 \in A$  and  $-a \equiv (-1)a$
- (3) for  $a, b \in A$ ,  $b \in X_a$  if and only if  $-a \in X_{-b}$ .

The group  $A$  then corresponds to  $\hat{F}/\hat{F}^2$  for fields and the  $X_a$  can be thought of as value sets for the quadratic forms  $(1, a)$ . Condition (3) then merely states the fundamental property that  $b \in G(1, a)$  if and only if  $-a \in G(1, -b)$ . The element  $-1 \in A$  corresponds to  $-\hat{F}^2$ . Notice that  $-1$  could be 1 in  $A$ . In order to determine the quadratic form structure over any field, it is sufficient to compute the value sets for all of the forms. To do this one only needs to know the  $G(1, a)$ ; and so knowing the  $X_a$  might be enough to construct a possible value set configuration for some field. Although this might be the case in general, it is not true if the field is specified to be nonreal. For example, let  $A$  be the group of exponent two with basis  $\{-1, a, b\}$  and consider the quadratic form scheme with  $X_1 = \langle a, b \rangle$ ,  $X_{-1} = \langle -1, a, b \rangle$ ,  $X_a = \langle a \rangle$ ,  $X_{-a} = \langle -1, a \rangle$ ,  $X_b = \langle b \rangle$ ,  $X_{-b} = \langle -1, b \rangle$ ,  $X_{ab} = \langle ab \rangle$ , and  $X_{-ab} = \langle -1, ab \rangle$ . Then  $G(1, 1, 1) = \bigcup_{\alpha \in G(1, 1)} G(1, \alpha) = G(1, 1) \cup G(1, a) \cup G(1, b) \cup G(1, ab) = \langle a, b \rangle = G(1, 1)$ . This is obviously a contradiction for nonreal fields. Two natural questions to ask, then, are (1) given a quadratic form scheme, when does there exist a field corresponding to it and (2) when is there a nonreal field for the scheme.

In an attempt to analyze nonreal fields with  $m = 4$  by dealing with value sets, some possible schemes with  $q = 16$  were discovered. The goal was to show something akin to Theorem 1. However, the attempt was not successful; and in fact, the following scheme makes the existence of an analogous result doubtful. Let  $A$  be a group of exponent two with basis  $\{-1, a, b, c\}$ . The table lists a possible scheme associated with  $A$ .

This scheme is internally consistent with respect to quadratic forms. If there is a field corresponding to it, then  $q = 16$ ,  $m = 4$ ,  $u = 4$ ,  $s = 2$ , and  $R = \hat{F}^2$ . It can also be shown that this scheme is unique (up to the equivalence of the possible associated fields) with respect to  $m = 4$  and the indicated Witt group structure. For  $m = 2$ ,

this situation did not arise. Even more interesting is that this scheme cannot be obtained from the quadratic form structure of a power series field,  $F((x))$ , where  $q(F) = 8$ . It turns out that this is the only such scheme with  $q = 16$ ,  $m > 2$ , and trivial radical (i.e.,  $R = \dot{K}^2$ ) that cannot be so obtained. This will be covered in more detail in a future paper.

elements $y \in A$	associated subgroups $X_y$
1	$\langle -1, a, b \rangle$
-1	$\langle -1, a, b, c \rangle$
$a$	$\langle -1, a \rangle$
$-a$	$\langle -1, a, bc \rangle$
$b$	$\langle -1, b \rangle$
$-b$	$\langle -1, b, c \rangle$
$c$	$\langle b, c \rangle$
$-c$	$\langle b, -c \rangle$
$ac$	$\langle ac, bc \rangle$
$-ac$	$\langle -ac, -bc \rangle$
$bc$	$\langle a, b, c \rangle$
$-bc$	$\langle a, b, -c \rangle$
$ab$	$\langle -1, ab \rangle$
$-ab$	$\langle -1, ab, ac \rangle$
$abc$	$\langle a, bc \rangle$
$-abc$	$\langle a, -bc \rangle$

REFERENCES

1. C. Cordes, *The Witt group and the equivalence of fields with respect to quadratic forms*, J. Algebra, **26** (1973), 400-421.
2. ———, *Kaplansky's radical and quadratic forms over nonreal fields*, Acta Arith., **82** (1975), 253-261.
3. R. Elman and T. Y. Lam, *Quadratic forms and the u-invariant. II*, Inventiones Math., **21** (1973), 125-137.
4. I. Kaplansky, *Quadratic forms*, J. Math. Soc. Japan, **5** (1953), 200-207.
5. ———, *Frohlich's local quadratic forms*, J. Reine Angew. Math., **239** (1969), 74-77.
6. T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Reading, Massachusetts, 1973.
7. A. Pfister, *Multiplikative quadratische Formen*, Arch. Math., **16** (1965), 363-370.
8. T. A. Springer, *Quadratic forms over fields with a discrete valuation*, Indag. Math., **17** (1955), 352-362.

Received October 23, 1975 and in revised form February 18, 1976.

LOUISIANA STATE UNIVERSITY, BATON ROUGE

