ACTA ARITHMETICA
XLI (1982)

Quadratic forms over fields with four quaternion algebras

by

CRAIG M. CORDES (Baton Rouge, La.)

1. Introduction. Let F be a field of characteristic different from two. The quadratic form structure of F is reflected exactly by the Witt ring $W(F)$. The group structure of $W(F)$ appears to be easier to analyze than the multiplicative aspect, and a primary reason for this is the present lack of knowledge about the Kaplansky radical, $R(F)$, of F. Here we determine $W(F)$ for all fields which have at most four quaternion algebras and for which $R(F)$ has finite index in $F^{\cdot} = F - \{0\}$.

Diagonalized quadratic forms over F will be denoted as $\langle a_1, \ldots, a_n\rangle$ and their value sets in $F^{\cdot}$ as $D(\langle a_1, \ldots, a_n\rangle)$. The number of quaternion algebras over F is $m = m(F)$ and $q = q(F) = |F^{\cdot}/F^{\cdot 2}|$. The quaternion algebra with structure constants $a, b \in F^{\cdot}$ will appear as $[a, b]$. The notation $\langle a_1, \ldots, a_n\rangle G$ with $a_i \in F^{\cdot}$ and G a subgroup of $F^{\cdot}$ will denote the subgroup in $F^{\cdot}$ generated by G and the a_i where the a_i are independent modulo G. Usually G will be either $F^{\cdot 2}$ or $R = R(F)$. Other notation and terminology will follow what is used in [9].

Attempts have been successful in classifying Witt rings with small q (and small $|F^{\cdot}/R|$). Almost all of these fields, however, have at most four quaternion algebras. The key to finding $W(F)$ when $m \leqslant 2$ was the fact that $D(\langle 1, -a\rangle) = D(\langle 1, -b\rangle)$ if and only if $ab \in R$. In general this very powerful result (whose proof is easy when $m \leqslant 2$) fails when $m = 4$. We will show here that it does hold when $m = 4$ and $8 < |F^{\cdot}/R| < \infty$.

The proof will depend on a collection of $D(\langle 1, -a\rangle)$'s. It is well-known that $|Q(a)| = |F^{\cdot}/D(\langle 1, -a\rangle)|$ where $Q(a) = \{[a, b] \mid b \in F^{\cdot}\}$. Thus all $D(\langle 1, -a\rangle)$ must have index at most m in $F^{\cdot}$. The first part of this paper explores what kind of collections can exist when $m = 4$ for which the $D(\langle 1, -a\rangle)$ all have the same index. The second part introduces two new subgroups of $F^{\cdot}$ when $8 < |F^{\cdot}/R| < \infty$ and $m = 4$, and these are used to find $W(F)$.

2. Existing results. Call $u = u(F)$ the u-invariant of F. Then $m = 1$ if and only if F is non-formally real and $u \leqslant 2$. $W(F)$ then depends on whether the level $s = s(F)$ is 1 or 2 and the result is given by Theorem 3.5 of [9] (p. 44). For completeness, we will state it here as Theorem A. As with our other structure results, we write $W(F)$ as a direct sum of cyclic subgroups and state the multiplication in terms of a set of generators for these subgroups. The generators will be given as anisotropic forms, but it is understood that these are just representatives for their Witt classes.

THEOREM A. *Let F be a field with $m = 1$ and suppose $F^{\cdot} = \langle\{a_i\}_{i\in I}\rangle F^{\cdot 2}$. If $s = 2$, assume $1 \in I$ and set $a_1 = -1$. If $s = 1$, assume $1 \notin I$. Then $W(F)$ is a direct sum of $\langle 1\rangle$ and $\{\langle 1, -a_i\rangle\}_{i\in I-\{1\}}$. The order of $\langle 1\rangle$ is $2s$, the order of every $\langle 1, -a_i\rangle$ is 2, and the product of any $\langle 1, -a_i\rangle$'s is 0.*

Kaplansky [7] showed that when $|F^{\cdot}/R| = 2$, then F is real and $R = D(\langle 1, 1\rangle)$. In fact it is easy to see for real fields that $|F^{\cdot}/R| = 2$ if and only if $m = 2$. $W(F)$ now can be written as the same direct sum as in Theorem A if $D(\langle 1, 1\rangle) = \langle\{a_i\}_{i\in I}\rangle F^{\cdot 2}$. The non-real case for $m = 2$ is not known in general yet but is given in the proof of Theorem 1 of [3] when $|F^{\cdot}/R| < \infty$. Note that if $m = 2$, then $s \leqslant 4$.

THEOREM B. *Let F be a field with $m = 2$ and suppose $R = \langle\{a_i\}_{i\in I}\rangle F^{\cdot 2}$. If $-1 \in R - F^{\cdot 2}$, assume $1 \in I$ and set $a_1 = -1$. Otherwise assume $1 \notin I$.*

(i) *If F is real, then $|F^{\cdot}/R| = 2$ and $W(F)$ is the direct sum of $\langle 1\rangle$ and $\{\langle 1, -a_i\rangle\}_{i\in I}$. $\langle 1\rangle$ has infinite order, each $\langle 1, -a_i\rangle$ has order 2, and the product of any $\langle 1, -a_i\rangle$'s is 0.*

(ii) *If F is non-real, $|F^{\cdot}/R| < \infty$, and $s = 2$ with $-1 \in R$ or $s = 1$, then there exist $\{b_1, \ldots, b_{2n}, c, d\}$ where $|F^{\cdot}/R| = 2^{2n}$, such that $W(F)$ is the direct sum of $\langle 1\rangle$, $\{\langle 1, -a_i\rangle\}_{i\in 1-\{1\}}$, $\{\langle 1, -b_j\rangle\}_{j=1}^{2n}$, and $\langle 1, -c, -d, cd\rangle$. The order of $\langle 1\rangle$ is $2s$ and is 2 for all other generators. The product of any two non-$\langle 1\rangle$ generators is 0 except $\langle 1, -b_j\rangle\cdot\langle 1, -b_k\rangle = \langle 1, -c, -d, cd\rangle$ which holds if and only if $\{j, k\} = \{2e-1, 2e\}$ for every $1 \leqslant e \leqslant n$.*

(iii) *If F is non-real, $|F^{\cdot}/R| < \infty$, and $s = 2$ with $-1 \notin R$, then there exist $\{b_0, \ldots, b_{2n-2}\}$, where $|F^{\cdot}/R| = 2^{2n}$, such that $W(F)$ is the direct sum of $\langle 1\rangle$, $\{\langle 1, -a_i\rangle\}_{i\in I}$, $\{\langle 1, -b_j\rangle\}_{j=0}^{2n-2}$. The orders of $\langle 1\rangle$ and $\langle 1, -b_0\rangle$ are 4, the orders of all other generators are 2, and the same product rule in* (ii) *holds (where $\langle 1, -c, -d, cd\rangle$ is the unique, anisotropic, quaternion form over F).*

(iv) *If F is non-real, $|F^{\cdot}/R| < \infty$, and $s = 4$, then there exist $\{b_1, \ldots, b_{2n-2}\}$, where $|F^{\cdot}/R| = 2^{2n-1}$, such that $W(F)$ is the direct sum of $\langle 1\rangle$, $\{\langle 1, -a_i\rangle\}_{i\in I}$, and $\{\langle 1, -b_j\rangle\}_{j=1}^{2n-2}$. The order of $\langle 1\rangle$ is 8 and is 2 for the other generators. The product rule in* (iii) *holds.*

It should be noted that for non-real fields $m = 2$ and $m = 4$ both imply $u = 4$. The group structure of $W(F)$ is then given for any $|F^{\cdot}/R|$ by Theorem 4.5 of [1].

3. Fields with $m < \infty$. This section contains some results for fields with $m < \infty$. Included is a weak form of $D(\langle 1, -a\rangle) = D(\langle 1, -b\rangle)$ iff $ab \in R$.

PROPOSITION 1. *If F is a field with $m < \infty$ and $d \in F^{\cdot}$, then there are exactly $m - |F^{\cdot}/D(\langle 1, -d\rangle)|$ anisotropic forms of determinant d and dimension 4 which represent 1.*

Proof. Let φ be a 4-dimensional form of determinant d which represents 1. Then $\varphi \cong \langle 1, -xd, -yd, xyd\rangle$. The Hasse invariant of φ (as defined in [10]) is $[-1, -1]\cdot[x, y]$. Thus there are exactly m such forms. And φ is isotropic if $\varphi \cong \langle 1, -1, a, -ad\rangle$. Clearly there are $|F^{\cdot}/D(\langle 1, -d\rangle)|$ of these. ∎

COROLLARY 1. *If F is non-real, $m < \infty$, and $u \leqslant 4$, then there are $m - |F^{\cdot}/D(\langle 1, -d\rangle)|$ anisotropic 4-dimensional forms of determinant d.*

COROLLARY 2. *If $m < \infty$ and $D(\langle 1, -a\rangle)$ has index m in $F^{\cdot}$, then $D(\langle 1, -x\rangle) \cap yD(\langle 1, -ax\rangle) \neq \emptyset$ for all $x, y \in F^{\cdot}$.*

Proof. By Proposition 1, $\langle 1, -x, -y, axy\rangle$ must be isotropic. ∎

THEOREM 1. *Let F be a field with $m < \infty$, and suppose $D(\langle 1, -a\rangle)$, $D(\langle 1, -b\rangle)$ both have index m in $F^{\cdot}$. Then $D(\langle 1, -a\rangle) = D(\langle 1, -b\rangle)$ if and only if $ab \in R$.*

Proof. One direction follows from Proposition 1 of [2]. So assume $D(\langle 1, -a\rangle) = D(\langle 1, -b\rangle)$, and let $1, x_2, \ldots, x_m$ be a set of coset representatives for $D(\langle 1, -a\rangle)$. Then $\{\langle 1, -a, -x_i, x_i b\rangle\}_{i=2}^{m}$ is a set of $m-1$ inequivalent, anisotropic forms of determinant ab. By Proposition 1, $|F^{\cdot}/D(\langle 1, -ab\rangle)| \leqslant 1$. Hence $ab \in R$.

4. Binary form value sets when $m = 4$. Throughout this section, we will assume F is a field with $m = 4$, $|F^{\cdot}/R| > 8$, and H is a subgroup of index 2 in $F^{\cdot}$ which contains R. We will be interested in the collection $\{D(\langle 1, -zx\rangle) \mid x \in H\}$ for some fixed z. In particular for $z = 1$, can this collection of value sets all have index at most 2? Can they all have index 1 or 4? The same questions will also be asked if $z \notin H$. One of the answers will allow us to strengthen Theorem 1 when $m = 4$.

PROPOSITION 2. *Suppose $D\langle 1, -x\rangle$ has index 2 for all $x \in H - R$. If $a, b \in F^{\cdot}$, $ab \notin R$ and $D(\langle 1, -a\rangle)$, $D(\langle 1, -b\rangle)$ both have index 2, then $D(\langle 1, -a\rangle) \neq D(\langle 1, -b\rangle)$.*

Proof. Suppose $D(\langle 1, -a\rangle) = D(\langle 1, -b\rangle)$. Then the Lemma of [4] implies these sets equal $D(\langle 1, -ab\rangle)$. Consequently, $D(\langle 1, -d\rangle) \cap \langle a, b\rangle R$

$= R$ for all $d \notin D(\langle 1, -a\rangle)$. In particular $D(\langle 1, -d\rangle)$ must have index 4 and so $H = D(\langle 1, -a\rangle)$. Notice $-a, -b, -ab \in H$ then yields $-1, a, b \in H$.

Claim 1. If $c \notin \langle a, b\rangle R$, then there is no $d \notin cR$ such that $D(\langle 1, -c\rangle) = D(\langle 1, -d\rangle)$ and such that these subgroups have index 2 in $\dot{F}$.

Otherwise, by the above, $D(\langle 1, -e\rangle) = H$ for all $e \in \langle a, b, c\rangle R - R$. Thus for any $y \notin H$, $D(\langle 1, -y\rangle) \cap \langle a, b, c\rangle R$ contains some $e \notin R$; and so $y \in D(\langle 1, -e\rangle) = H$. Contradiction.

Claim 2. If $E = \{[c, x] \mid c \in H - \langle a, b\rangle R,\ x \in \dot{F}\}$, then $|E| = 2$. In particular E is a subgroup (of the Brauer group).

First note that $|\dot{F}/R| > 8$ implies $E \neq \emptyset$. Secondly since $D(\langle 1, -c\rangle)$ has index 2 for all $c \in H - R$, there are only two quaternion algebras of the form $[c, x]$ for a fixed c. Suppose $c, d \in H - \langle a, b\rangle R$ and $c \notin dR$. By Claim 1, $D(\langle 1, -c\rangle)$, $D(\langle 1, -d\rangle)$, and $D(\langle 1, -cd\rangle)$ are distinct subgroups (of index 2 all of which contain the index 4 subgroup $D(\langle 1, -c\rangle) \cap \cap D(\langle 1, -d\rangle)$). Hence $\dot{F} = D(\langle 1, -c\rangle) \cup D(\langle 1, -d\rangle) \cup D(\langle 1, -cd\rangle)$. Select some $y \notin D(\langle 1, -c\rangle) \cup D(\langle 1, -d\rangle)$. Then $y \in D(\langle 1, -cd\rangle)$ and so $[cd, y] = 1$. This means $[c, y] = [d, y]$, and we see every pair of non-split members of E are equal. The claim is established.

Consider some $c \in H - \langle a, b\rangle R$. Since $a \in H$, $[c, x]\cdot[ac, x] = [a, x] \in E$ for every $x \in \dot{F}$. Similarly $[b, x]$, $[ab, x] \in E$. Let $x \notin D(\langle 1, -a\rangle) = D(\langle 1, -b\rangle)$. Then $|E| = 2$ yields $[a, x] = [b, x]$ which in turn gives $[ab, x] = 1$. But this contradicts $x \notin D(\langle 1, -ab\rangle)$, and the proof of Proposition 2 is finished. ■

PROPOSITION 3. *If* $E = \{[a, x] \mid a \in H,\ x \in \dot{F}\}$, *then* $|E| = 2$.

Proof. This follows by using Proposition 2 and applying the same argument as in Claim 2 above. ■

THEOREM 2. *If F is a non-real field with $m = 4$, $|\dot{F}/R| > 8$, and if $H \supseteq R$ is a subgroup of index 2 in $\dot{F}$, then there is an $a \in H$ such that $D(\langle 1, -a\rangle)$ has index 4.*

Proof. Suppose not. Then there are two cases to consider.

I. There exists $b \in \dot{F} - H$ satisfying $bD(\langle 1, -b\rangle) \cap H \neq \emptyset$. Here we have $\dot{F} = \langle b\rangle H$, and all the quaternion algebras over F are of the forms $[\alpha, \beta]$, $[\alpha, \beta b]$, or $[ab, \beta b]$ where $a, \beta \in H$. If $[b, b] \in E$, then this would show all quaternion algebras over F belonged to E. But $|E| = 2$ then contradicts $m = 4$. Now $bD(\langle 1, -b\rangle) \cap H \neq \emptyset$ implies there is an $a \in H$ such that $ab \in D(\langle 1, -b\rangle)$. Thus $[ab, b] = 1$ and so $[a, b] = [b, b] \in E$.

II. $bD(\langle 1, -b\rangle) \cap H = \emptyset$ for all $b \notin H$. Hence $D(\langle 1, -b\rangle) \subseteq H$ for $b \notin H$. In particular $-1 \notin H$, and so $D(\langle 1, a\rangle) \subseteq H$ for all $a \in H$. It now follows that $D(\langle a_1, \ldots, a_n\rangle) \subseteq H$ for $a_i \in H$. But using $n = s+1$ and $a_i = 1$ for all i shows $\dot{F} \subseteq H$. Contradiction. ■

Both of the hypotheses $|\dot{F}/R| > 8$ and F non-real are necessary for the conclusion of Theorem 2 to hold. If K is a field with $u = 2$, $q = 4$, then for $F = K((x))$, $R(F) = \dot{F}^2$, $q(F) = 8$, and $m(F) = 4$. Moreover, $D(\langle 1, -x\rangle) = \dot{K}\dot{F}^2$ for all $x \in H = \dot{K}\dot{F}^2 - \dot{F}^2$. A real field not satisfying Theorem 2's conclusion may be obtained by applying Kula's Theorem 3.3 of [8] to $F_1 = R$ and $F_2 = Q_2$ (the 2-adics). This will give a field F with $m = 4$, $R = \dot{F}^2$, $q = 16$ that even satisfies $D(\langle 1, -a\rangle) = D(\langle 1, -b\rangle)$ iff $ab \in R$. But $H = \{\text{positive elements}\}$ gives the counterexample.

Next we consider the case of the $D(\langle 1, -a\rangle)$ where the a's do not belong to H. Here we can make a much stronger statement than Theorem 2. The restriction $|\dot{F}/R| > 8$ can be halved and the result applies to real fields as well. In fact the only exception will be the unique, real, "Pythagorean-type" fields with $|\dot{F}/R| = m = 4$.

THEOREM 3. *If F is a field with $m = 4$, $|\dot{F}/R| > 4$, and if $H \supseteq R$ is a subgroup of index 2 in $\dot{F}$, then there is an $a \in \dot{F} - H$ such that $D(\langle 1, -a\rangle)$ has index 4.*

Proof. Suppose not. Note then that Proposition 2's conclusion still holds. To see this, proceed just as in that proof up to Claim 1. It shows that $\dot{F} - D(\langle 1, -a\rangle) \subseteq H$.

This is impossible since $D(\langle 1, -a\rangle)$ has index 2.

Kaplansky ([7], Theorem 2) showed that if every $D(\langle 1, x\rangle)$ has index at most 2, then $m \leqslant 2$. Thus there is an $x \in H$ such that $D(\langle 1, -x\rangle)$ has index 4. By Proposition 2, $D(\langle 1, -a\rangle)$ and $D(\langle 1, -ax\rangle)$ are distinct subgroups of index 2 for all $a \notin H$. Thus by the Lemma of [4], $D(\langle 1, -a\rangle) \cap \cap D(\langle 1, -ax\rangle) = D(\langle 1, -x\rangle)$, and so $D(\langle 1, -x\rangle) \subseteq D(\langle 1, -a\rangle)$. In particular $a \in D(\langle 1, x\rangle)$ for all $a \notin H$ shows $D(\langle 1, x\rangle) = \dot{F}$. The above also demonstrates that the only $x \in \dot{F}$ for which $D(\langle 1, -x\rangle)$ has index 4 are those $x \in -R$. So if $y \notin \pm R$, then $D(\langle 1, \pm y\rangle)$ are distinct subgroups of index 2 whose intersection is $D(\langle 1, 1\rangle)$. Thus $D(\langle 1, 1\rangle) \subseteq D(\langle 1, y\rangle)$ for all $y \notin \pm R$. But there can exist only 3 distinct subgroups of index 2 containing a given subgroup of index 4. Hence $|\dot{F}/R| \leqslant 5$. Contradiction. ■

COROLLARY. *Let F be a non-real field with $m = 4$ and $|\dot{F}/R| = 2^r$ where $3 < r < \infty$. Then there are at least $r+1$ distinct elements $a_i \in \dot{F}$ modulo R for which $D(\langle 1, -a_i\rangle)$ has index 4.*

Proof. Let $H \supseteq R$ be any subgroup of index 2 in $\dot{F}$. Then by Theorem 3, there is an $a_1 \notin H$ such that $D(\langle 1, -a_1\rangle)$ has index 4. Now let $H_1 \supseteq R$ be any subgroup of $\dot{F}$ of index 2 with $a_1 \in H_1$. Again by Theorem 3, there is an $a_2 \notin H_1$ so that $D(\langle 1, -a_2\rangle)$ has index 4. We can continue in this way to get $a_1, \ldots, a_r$. Finally by Theorem 2, there is an element $a_{r+1} \in \langle a_1 a_2, \ldots, a_1 a_r\rangle R$ with $D(\langle 1, -a_{r+1}\rangle)$ having index 4. ■

The last corollary could be stated for arbitrary fields too. The proof showed that if $2 < r < \infty$, then $a_1, \ldots, a_r$ can always be obtained.

Remark. All the results in this section thus far actually hold when $m = 4$ is replaced by the (apparently) weaker condition of $D(\langle 1, -x\rangle)$ having index at most 4 for all $x \in \dot F$ and having index 4 for at least one such x. When F is non-real and $|\dot F/R| < \infty$, this new condition implies $m = 4$ or 8. The case $m = 8$ can occur if $u = q = 8$ as well. Of course the requirement of $|\dot F/R| > 8$ is not met here; and we know of no example where this is met and the new condition and $m = 4$ are not equivalent.

We now want to investigate the same type of question but switch the roles of the index 2 and index 4 value sets. Here it has been necessary to rely heavily on counting arguments, and so the restriction $|\dot F/R| < \infty$ is seen almost throughout. We have no evidence to suggest the results do not hold in the infinite case but have been unable to extend virtually any of what follows in this paper beyond the above finite limitation.

PROPOSITION 4. *Let F be a field with $m = 4$. If $D(\langle 1, -a\rangle)$, $D(\langle 1, -b\rangle)$, and $D(\langle 1, -ab\rangle)$ all have index 4 in $\dot F$, then for any $x, y \in \dot F$, $\langle x\rangle D(\langle 1, -a\rangle) \neq \langle y\rangle D(\langle 1, -b\rangle)$.*

Proof. If we have $\langle x\rangle D(\langle 1, -a\rangle) = \langle y\rangle D(\langle 1, -b\rangle)$, then for any $z \notin \langle y\rangle D(\langle 1, -b\rangle)$ it must be the case that $D(\langle 1, -a\rangle) \cap zD(\langle 1, -b\rangle) = \emptyset$. But this contradicts Corollary 2 of Proposition 1. ■

THEOREM 4. *Let F be a field with $m = 4$, $4 < |\dot F/R| < \infty$, and suppose $H \supseteq R$ is a subgroup of index 2 in $\dot F$. Then there is an $a \in H$ such that $D(\langle 1, -a\rangle)$ has index 2.*

Proof. Suppose not. Then $D(\langle 1, -a\rangle)$ has index 4 for all $a \in H - R$. Consider the collection $\{\langle x\rangle D(\langle 1, -a\rangle)\}$ where $a \in H - R$ and $x \notin D(\langle 1, -a\rangle)$. By Proposition 4, this collection contains $3(t/2 - 1)$ distinct subgroups of index 2 in $\dot F$ where $t = |\dot F/R|$. This number still holds if we regard everything modulo R. But $\dot F/R$ only has $t - 1$ distinct subgroups of index 2. Thus $3(t/2 - 1) \leqslant t - 1$ or $t \leqslant 4$. Contradiction. ■

Remark. Using results in Section 3 of [3], it is easy to see Theorem 4 holds for all non-real fields with $|\dot F/R| < \infty$ and $m = 4$. This generalization fails in the real case only in the essentially unique situation where $|\dot F/R| = 4$ and $H = \langle -1\rangle R$.

The problem seems very much more complicated when we try to obtain a result in this setting analogous to Theorem 3. But it is this last case which will prove to be so useful in finding $W(F)$.

5. Some involved counting. We are interested in showing that if $m = 4$, then there is an $a \notin H$ such that $D(\langle 1, -a\rangle)$ has index 2. This fails to be true for all non-real fields satisfying $m = 4$ and $|\dot F/R| = 8$. When $|\dot F/R| < 8$, there is essentially only one type of field which has $m = 4$. This is a real field with $|\dot F/R| = 4$, but it is not a counterexample. So obviously we will need $|\dot F/R| > 8$ if we are to get anywhere. But first we prove a useful proposition and a technical lemma.

PROPOSITION 5. *Let F be a field with $m = 4$ and suppose $D(\langle 1, -x\rangle)$ and $D(\langle 1, -y\rangle)$ both have index 4 in $\dot F$. Then $D(\langle 1, -x\rangle) \cap D(\langle 1, -y\rangle)$ has index equal to 4 times the index of $D(\langle 1, -xy\rangle)$.*

Proof. If index $D(\langle 1, -xy\rangle)$ is 1, then $xy \in R$ and the result is clear.

Suppose index $D(\langle 1, -xy\rangle) = 2$. Now $D(\langle 1, -x\rangle) \nsubseteq D(\langle 1, -xy\rangle)$ for otherwise $D(\langle 1, -x\rangle) = D(\langle 1, -x\rangle) \cap D(\langle 1, -xy\rangle) \subseteq D(\langle 1, -y\rangle)$ implies $xy \in R$ by Theorem 1. Contradiction to index $D(\langle 1, -xy\rangle) = 2$. Thus $D(\langle 1, -x\rangle) \cap D(\langle 1, -y\rangle) = D(\langle 1, -x\rangle) \cap D(\langle 1, -y\rangle) \cap D(\langle 1, -xy\rangle) = D(\langle 1, -x\rangle) \cap D(\langle 1, -xy\rangle)$ has index 8.

Finally assume $D(\langle 1, -xy\rangle)$ has index 4. Clearly $A = D(\langle 1, -x\rangle) \cap D(\langle 1, -y\rangle)$ has index 8 or 16. If it is 8, then there are $a, b, c \in \dot F$ such that $D(\langle 1, -x\rangle) = \langle a\rangle A$, $D(\langle 1, -y\rangle) = \langle b\rangle A$, and $\dot F = \langle a, b, c\rangle A$. But then $D(\langle 1, -x\rangle) \cap cD(\langle 1, -y\rangle) = \emptyset$ is a contradiction to Corollary 2 of Proposition 1. ■

LEMMA. *Let F be a field with $m = 4$ and $|\dot F/R| < \infty$. If $D(\langle 1, -x\rangle)$ has index 2 in $\dot F$ for x in exactly 3 cosets of R, then $|\dot F/R| \leqslant 8$.*

Proof. Let a, b, c be representatives for the 3 cosets. If a, b, c are independent modulo R, then $\dot F = \langle a, b, c, x, \ldots\rangle R$ and $H = \langle ab, ac, x, \ldots\rangle R$ is a subgroup of index 2 in $\dot F$. Moreover, $D(\langle 1, -y\rangle)$ has index 4 for all $y \in H - R$. This contradicts Theorem 4 if $|\dot F/R| \geqslant 8$. The case $|\dot F/R| = 4$ is clear. So we may now assume $c = ab$.

Let $x \in \dot F - \langle a, b\rangle R$, and consider $D(\langle 1, -x\rangle)$ and $D(\langle 1, -ax\rangle)$. Both of the subgroups have index 4 and by Proposition 5, $A = D(\langle 1, -x\rangle) \cap D(\langle 1, -ax\rangle)$ has index 8. Thus there are α, β, γ such that $D(\langle 1, -x\rangle) = \langle \alpha\rangle A$, $D(\langle 1, -ax\rangle) = \langle \beta\rangle A$, and $\dot F = \langle \alpha, \beta, \gamma\rangle A$. It is now easy to see that there is exactly one common subgroup of index 2 of the sets $\langle y\rangle D(\langle 1, -x\rangle)$ and $\langle z\rangle D(\langle 1, -ax\rangle)$.

Now let $H \supseteq R$ be any subgroup of index 4 in $\dot F$ satisfying $\dot F = \langle a, b\rangle H$. Just as in the proof of Theorem 4, there are $3(t/4 - 1)$ distinct subgroups of index 2 of the form $\langle y\rangle D(\langle 1, -x\rangle)$ where $x \in H - R$. But those of the form $\langle y\rangle D(\langle 1, -ax\rangle)$ add at least $2(t/4 - 1)$ additional ones, and the $\langle y\rangle D(\langle 1, -abx\rangle)$ add $t/4 - 1$ more. Thus $t - 1 \geqslant 6(t/4 - 1)$ or $t \leqslant 10$. ■

THEOREM 5. *Let F be a field with $m = 4$ and $|\dot F/R| < \infty$. If F contains a subgroup $H \supseteq R$ of index 2 such that $D(\langle 1, -a\rangle)$ has index 4 for all $a \in \dot F - H$, then $|\dot F/R| \leqslant 8$.*

Proof. Let $t = |\dot F/R|$. The idea of the first part of the proof is to count the total number of appearances in $X = \bigcup_{a \notin H} D(\langle 1, -a\rangle)$ of cosets of R as a runs through a set of representation for $\dot F - H$ modulo R. This count will be done in two different ways.

Step 1. Each $D(\langle 1, -a\rangle)$ contains $t/4$ cosets of R, and so there is a total of $t^2/8$ such appearances.

Now for $y \in H$, how many $D(\langle 1, -a\rangle)$, $a \notin H$, does yR appear in? Since $y \in D(\langle 1, -a\rangle)$ iff $a \in D(\langle 1, -y\rangle)$, the answer is the number of R-cosets in $D(\langle 1, -y\rangle) \cap (F^{\cdot} - H)$. Consider $z \notin H$. Similarly zR appears in $\big|\big(D(\langle 1, -z\rangle) \cap zH\big)/R\big|$ $D(\langle 1, -a\rangle)$'s.

Suppose $D(\langle 1, -a\rangle) \subseteq H$ for some $a \notin H$. Then $-a \in H$ implies $-1 \notin H$. On the other hand, if $D(\langle 1, -y\rangle) \subseteq H$ for some $y \in H$, then clearly $-1 \in H$. In particular, these two possibilities cannot happen simultaneously. We will consider each separately.

Step 2. $-1 \in H$. Then $D(\langle 1, -a\rangle) \cap H$ has index 8 for all $a \notin H$, and so there are $t/8$ R-cosets in $D(\langle 1, -z\rangle) \cap zH$ for all $z \notin H$. This means that the number of appearances in X of R-cosets which do not lie in H is $t^2/16$.

Let: p = the number of R-coset representatives, $y \in H$, such that $D(\langle 1, -y\rangle)$ has index 2 in $F^{\cdot}$ but is not H.
q = the number of such y for which $D(\langle 1, -y\rangle) \subsetneqq H$.
r = the number of such y for which $D(\langle 1, -y\rangle) = H$.

Then $t/2 - p - q - r - 1$ is the number of such y for which $D(\langle 1, -y\rangle)$ has index 4 in $F^{\cdot}$ but is not contained in H.

Using the observations stated in Step 1, we are now ready to count the appearances in X of R-cosets, yR, which do lie in H. This total will be $t/2$ (corresponds to $y \in R$) plus $p \cdot (t/4) + q \cdot 0 + r \cdot 0 + (t/2 - p - q - r - 1) \cdot (t/8)$. So by Step 1, $t^2/8 = t^2/16 + t/2 + pt/4 + (t/2 - p - q - r - 1)\,t/8$ which simplifies to $q + r - p = 3$.

Step 3. Claim: $p \geqslant q - 1$. This is clear if $q = 0$ or 1. Suppose $q \geqslant 2$ and let $x_1, \ldots, x_q$ be an appropriate set of representatives with $D(\langle 1, -x_i\rangle) \subsetneqq H$. By Theorem 1, $D(\langle 1, -x_i\rangle) \cap D(\langle 1, -x_j\rangle)$ has index 4 in H and hence 8 in $F^{\cdot}$ for $i \neq j$. Thus Proposition 5 shows $D(\langle 1, -x_1x_i\rangle)$, $2 \leqslant i \leqslant q$, has index 2 in $F^{\cdot}$. The claim will be established if we can show $D(\langle 1, -x_1x_i\rangle) \neq H$. But if equality did hold here, then $D(\langle 1, -x_1\rangle) = D(\langle 1, -x_1\rangle) \cap D(\langle 1, -x_1x_i\rangle) \subseteq D(\langle 1, -x_i\rangle)$. Thus $D(\langle 1, -x_1\rangle) = D(\langle 1, -x_i\rangle)$ which contradicts Theorem 1.

Combining the claim with the equality in Step 2 gives $r \geqslant 2$. But if $D(\langle 1, -x\rangle) = D(\langle 1, -y\rangle) = H$ for $xy \notin R$, then $D(\langle 1, -xy\rangle) = H$. Hence $r \geqslant 3$.

Step 4. Set $T = \{y \in H \mid D(\langle 1, -y\rangle) = H\} \cup R$. Then it is easy to see T is a subgroup of H.

Claim: $|T/R| \leqslant 4$. If this is not the case, then $T \supseteq \langle x, y, z\rangle R$ for some $x, y, z \in H$. Fix $a \in F^{\cdot} - H$. Clearly $\langle x, y, z\rangle R \cap D(\langle 1, -ax\rangle) \neq R$; let $a \notin R$ be in this intersection. Thus $ax \in D(\langle 1, -a\rangle) = H$. But $x \in H$ implies $a \in H$. Contradiction and so $|T/R| \leqslant 4$.

But clearly $|T/R| = r + 1$, so the above shows that $r = 3$. From Step 2 then, $p = q$.

Step 5. We want to show $p = q = 0$. Suppose not, and let $W = \{x_1, \ldots, x_q\}$ be a set of distinct elements modulo R which satisfy $D(\langle 1, -x_i\rangle) \subsetneqq H$. Also let x, y, xy be representatives for the 3 cosets of R for which $D(\langle 1, -\alpha\rangle) = H$. Now for $\alpha \in \langle x, y\rangle R - R$, $x_1\alpha \notin W$ because otherwise $D(\langle 1, -x_1\rangle) = D(\langle 1, -x_1\rangle) \cap D(\langle 1, -\alpha\rangle) = D(\langle 1, -x_1\alpha\rangle)$ would contradict Theorem 1. For the same reason $D(\langle 1, -x_1\alpha\rangle)$ has index 2 and $x_1 \notin \langle x, y\rangle R$ implies $D(\langle 1, -x_1\alpha\rangle) \neq H$. Thus x_1x, x_1y, x_1xy are 3 of the p elements satisfying $D(\langle 1, -y\rangle) \neq H$ of index 2. From Step 3, we know $q-1$ of these elements are of the form $x_1x_2, \ldots, x_1x_q$. Hence at least 2 of x_1x, x_1y, x_1xy are of this form. But if $x_1\alpha = x_1x_i$, then $\alpha = x_i$ yields a contradiction. So $p = q = 0$.

We have now, in the case where $-1 \in H$, shown that F satisfies the hypothesis of the last lemma. Thus $|F^{\cdot}/R| \leqslant 8$.

Step 6. $-1 \notin H$. Again let p be as above, but now let q = the number of $a \notin H$ modulo R such that $D(\langle 1, -a\rangle) \subsetneqq H$. Note that by Step 1, for $y \in H$, the number of $D(\langle 1, -a\rangle)$, $a \notin H$, that yR appears in is $\frac{1}{2}|D(\langle 1, -y\rangle)/R|$.

So the number of appearances in X of elements $yR \subseteq H$ is the sum of $t/2$ (corresponding to $y = 1$), $p \cdot (t/4)$ ($D(\langle 1, -y\rangle)$ has index 2), and $(t/2 - p - 1)t/8$ ($D(\langle 1, -y\rangle)$ has index 4). The number for $zR \nsubseteq H$ is $q \cdot 0$ ($D(\langle 1, -z\rangle) \subsetneqq H$) plus $(t/2 - q)t/8$ ($D(\langle 1, -z\rangle) \nsubseteq H$). By Step 1 $t^2/8 = t/2 + pt/4 + (t/2 - p - 1)t/8 + (t/2 - q)t/8$. Simplifying yields $q - p$, $= 3$. But even though q is different here than in Step 3, the same result and proof holds. Clearly $p \geqslant q - 1$ contradicts $q - p = 3$. Thus the case $-1 \notin H$ cannot occur. ■

Actually the remarks prior to Proposition 5 allow us to conclude more. If F is a field with $m = 4$, $|F^{\cdot}/R|$ finite and different from 8, then for every subgroup $H \supseteq R$ of index 2 in $F^{\cdot}$, there is an $a \notin H$ with $D(\langle 1, -a\rangle)$ having index 2. There is also a corollary analogous to the one following Theorem 3. The proof is the same.

Corollary. *Let F be a field with $m = 4$ and $|F^{\cdot}/R| = 2^r$ with $r < \infty$, $r \neq 3$. Then there are at least $r+1$ distinct elements $a_i \in F^{\cdot}$ modulo R for which $D(\langle 1, -a_i\rangle)$ has index 2.*

6. Preliminaries for finding $W(F)$.

Theorem 5 and the remarks immediately following its proof give the key to finding the structure of $W(F)$. It is the same powerful result which holds where $m \leqslant 2$, but we must make some restrictions on $|F^{\cdot}/R|$.

Theorem 6. *Let F be a field with $m = 4$ and $|F^{\cdot}/R|$ finite but not 8. Then for $a, b \in F^{\cdot}$, $D(\langle 1, -a\rangle) = D(\langle 1, -b\rangle)$ if and only if $ab \in R$.*

Proof. If $a \in R$, this is clear. Theorem 1 yields the result when $D(\langle 1, -a\rangle)$ has index 4. So suppose that $D(\langle 1, -a\rangle)$ has index 2 and that $ab \notin R$. Then as we have seen several times before, $D(\langle 1, -a\rangle) = D(\langle 1, -b\rangle) = D(\langle 1, -ab\rangle)$. Consider $x \notin D(\langle 1, -a\rangle)$. Clearly $D(\langle 1, -x\rangle) \cap \langle a, b\rangle R = R$, and consequently $D(\langle 1, -x\rangle)$ must have index 4. But this being the case for all $y \in xD(\langle 1, -a\rangle)$ is a contradiction to Theorem 5. ■

Finding the structure of $W(F)$ when $m = 2$ involved the discovery of a set $\{b_j\}_{j\in J}$ for which $D(\langle 1, -b\rangle)$, $b \in \langle\{b_j\}\rangle R$, had index 2. In particular the non-split quaternion algebras of the form $[b, c]$, $b \in \langle\{b_j\}\rangle R$ were all equal. We will use this concept when $m = 4$, but the situation is complicated by the fact that not all the non-split algebras are the same.

Proposition 6. *Let F be a field with $m = 4$ and $8 \neq |F^{\cdot}/R| < \infty$. Suppose $D(\langle 1, -a\rangle)$, $D(\langle 1, -b\rangle)$ have index 2 and $ab \notin R$. Then $D(\langle 1, -ab\rangle)$ has index 2 if and only if the non-split quaternion algebras of the forms $[a, \alpha]$ and $[b, \beta]$ are equal.*

Proof. Set $A = D(\langle 1, -a\rangle) \cap D(\langle 1, -b\rangle)$. Then A has index 4 by Theorem 6.

Suppose $D(\langle 1, -ab\rangle)$ has index 2. Then by Theorem 6, $D(\langle 1, -a\rangle)$, $D(\langle 1, -b\rangle)$, and $D(\langle 1, -ab\rangle)$ are all distinct; and clearly they all contain A. Thus the union of these 3 subgroups must be $F^{\cdot}$ since an elementary 2-group has exactly 3 subgroups of index 2 which contain a given subgroup of index 4. Let $c \in F^{\cdot} - \big(D(\langle 1, -a\rangle) \cup D(\langle 1, -b\rangle)\big)$. Then $c \in D(\langle 1, -ab\rangle)$ and $[ab, c] = 1$. Thus $[a, c] = [b, c] \neq 1$.

Conversely suppose $D(\langle 1, -ab\rangle)$ has index 4. Then $A = D(\langle 1, -ab\rangle)$. Pick $c \in F^{\cdot} - \big(D(\langle 1, -a\rangle) \cup D(\langle 1, -b\rangle)\big)$. Hence $[ab, c] \neq 1$ implies $[a, c] \neq [b, c]$. Contradiction. ■

Proposition 7. *Let F be a field with $m = 4$ and $8 \neq |F^{\cdot}/R| < \infty$. If Q is a fixed non-split quaternion algebra over F, set $A_Q = \{a \in F^{\cdot} \mid D(\langle 1, -a\rangle)$ has index 2 and $[a, b] = Q$ for $b \notin D(\langle 1, -a\rangle)\}$. Then $B_Q = A_Q \cup R$ is a subgroup of $F^{\cdot}$.*

Proof. Since A_Q contains cosets of R, it suffices to show that $ab \in A_Q$ whenever $a, b \in A_Q$ and $ab \notin R$. By Proposition 6, $D(\langle 1, -ab\rangle)$ has index 2. Let $c \notin D(\langle 1, -ab\rangle)$. Then as in the proof of Proposition 6, $c \in D(\langle 1, -a\rangle) \cup D(\langle 1, -b\rangle)$, but $c \notin D(\langle 1, -a\rangle) \cap D(\langle 1, -b\rangle)$. If $c \in D(\langle 1, -a\rangle) - D(\langle 1, -b\rangle)$, then $[ab, c] = [a, c]\,[b, c] = [b, c] = Q$. ■

In order to simplify the notation, whenever we are dealing with more than one non-split quaternion algebra, we will write A_i and B_i instead of A_{Q_i} and B_{Q_i}. The next proposition is a collection of facts easily proved by Propositions 6 and 7.

Proposition 8. *Let F be a field with $m = 4$ and $8 \neq |F^{\cdot}/R| < \infty$. The following hold:*

(i) $B_1 \cap B_2 = R$, $A_1 \cap A_2 = \emptyset$.

(ii) *If $a, a' \in A_1$, $b, b' \in A_2$, and $ab = a'b' \pmod R$, then $a \equiv a'$, $b \equiv b' \pmod R$.*

(iii) *If $a \in A_1$ and $b \in A_2$, then $D(\langle 1, -a\rangle) \cap D(\langle 1, -b\rangle) = D(\langle 1, -ab\rangle)$ has index 4 in $F^{\cdot}$.*

One might think that it should be possible for $A_Q \neq \emptyset$ for all non-split Q over F. Surprisingly this is not the case when $8 \neq |F^{\cdot}/R| < \infty$, but it can happen when $|F^{\cdot}/R| = 8$.

Proposition 9. *Let F be a field with $m = 4$ and $8 \neq |F^{\cdot}/R| < \infty$. If Q_1, Q_2, Q_3 are the non-split quaternion algebras over F, then exactly one of A_1, A_2, A_3 is empty.*

Proof. Suppose first that none of $A_1, A_2, A_3 = \emptyset$, and let $a \in A_1$, $b \in A_2$, and $c \in A_3$. Set $A = D(\langle 1, -a\rangle)$, $B = D(\langle 1, -b\rangle)$, and $C = D(\langle 1, -c\rangle)$. By Proposition 8(iii), $A \cap B = D(\langle 1, -ab\rangle)$, $A \cap C = D(\langle 1, -ac\rangle)$, and $B \cap C = D(\langle 1, -bc\rangle)$ all have index 4. Thus $(A \cap B) \cap C$ has index either 4 or 8. But $A \cap B \cap C = D(\langle 1, -ab\rangle) \cap D(\langle 1, -ac\rangle)$ which has index 16 by Proposition 5. Contradiction and so at least one of A_1, A_2, A_3 is empty.

Suppose in fact that $A_2 = A_3 = \emptyset$. If $B_1 = F^{\cdot}$, then $m = 2$ by Kaplansky ([7], Theorem 2). Thus $B_1 \neq F^{\cdot}$ and there is a subgroup $H \supseteq B_1$ of index 2 in $F^{\cdot}$. Moreover, $D(\langle 1, -x\rangle)$ has index 4 for all $x \in F^{\cdot} - H$. This contradicts Theorem 5. So no two of A_1, A_2, A_3 can be empty. ■

For the remainder of the paper, we assume $A_1, A_2 \neq \emptyset$ and $A_3 = \emptyset$. Also denote $|B_1/R| = 2^p$ and $|B_2/R| = 2^q$. If $B_1B_2 \neq F^{\cdot}$, then just as above, there is an $H \supseteq B_1B_2$ of index 2 which contradicts Theorem 5. So by this and Proposition 8 (i), we see $F^{\cdot}/R$ is the direct sum of B_1/R and B_2/R. Hence $r = p + q$ where $|F^{\cdot}/R| = 2^r$. Another way of stating the above is the following proposition.

Proposition 10. *Let F be a field with $m = 4$ and $8 \neq |F^{\cdot}/R| < \infty$. If $B_1 = \langle b_1, \ldots, b_p\rangle R$ and $B_2 = \langle c_1, \ldots, c_q\rangle R$, then $F^{\cdot} = \langle b_1, \ldots, b_p, c_1, \ldots \ldots, c_q\rangle R$.*

Corollary. *If $D(\langle 1, -x\rangle)$ has index 4 in $F^{\cdot}$, there are $a \in A_1$, $b \in A_2$, unique modulo R, such that $x = ab$. Moreover, $D(\langle 1, -x\rangle) = D(\langle 1, -a\rangle) \cap D(\langle 1, -b\rangle)$.*

Proposition 11. *Let $a \in B_i$, $b \in B_j$ where $i \neq j$. Then $b \in D(\langle 1, -a\rangle)$.*

Proof. If either a or $b \in R$, then clearly $b \in D(\langle 1, -a\rangle)$. So suppose $a, b \notin R$. If $b \notin D(\langle 1, -a\rangle)$, then $[a, b] = Q_i$. But then also $a \notin D(\langle 1, -b\rangle)$ implies $[b, a] = Q_j$. Contradiction. ■

7. The structure of $W(F)$. The notation of the previous sections will still be in force. In fact they will be further restricted to the following: $R = \langle\{a_i\}_{i\in I}\rangle F^{\cdot 2}$ where if $-1 \in R - F^{\cdot 2}$, then $1 \in I$ and $a_1 = -1$; otherwise $1 \notin I$. In any event, setting $I' = I - \{1\}$ means $I' = I$ except when

$-1 \in R - F^{\cdot 2}$. $B_1 = \langle b_1, \ldots, b_p\rangle R$ and $B_2 = \langle c_1, \ldots, c_q\rangle R$ where $b_1 = -1$ if $D(\langle 1, 1\rangle)$ has index 2. By the Corollary to Proposition 10, if $D(\langle 1, 1\rangle)$ has index 4, then there is a unique (modulo R) $b \in B_1$ such that $-b \in B_2$ and $D(\langle 1, 1\rangle) = D(\langle 1, -b\rangle) \cap D(\langle 1, b\rangle)$. If $s \geqslant 4$, then not both b, $-b \in D(\langle 1, 1\rangle)$. If one of them belongs to $D(\langle 1, 1\rangle)$, we assume it is $b = b_1 \in B_1$. If neither belong, then exactly one of b or $-b$ is totally positive. Assume it is $b = b_1$. Finally pick d_l, e_l, $1 \leqslant l \leqslant 3$ so that $[d_l, e_l] = Q_l$; and Q_i is associated with the B_i above for $i = 1, 2$.

The structure of $W(F)$ will be given as a direct sum of cyclic subgroups generated by some of $\langle 1\rangle$, $\{\langle 1, -a_i\rangle\}_{i \in I}$, $\{\langle 1, -b_j\rangle\}_{j=1}^{p}$, $\{\langle 1, -c_k\rangle\}_{k=1}^{q}$, and $\{\langle 1, -d_l, -e_l, d_l e_l\rangle\}_{l \in L}$. There are 10 cases, and they depend on s and what happens to $D(\langle 1, 1\rangle)$. The b_j, c_k, d_l, e_l may be different from case to case, but they will always satisfy the conditions in the last paragraph. Proposition 11 shows that most of these generators have a 0 product in $W(F)$. In fact we will select them so that there are essentially only 2 ways the products are not 0. The only possible non-zero product of $\langle 1, -b_j\rangle$ with another generator is if this other element is either $\langle 1\rangle$ or another $\langle 1, -b_i\rangle$. This is easy to see unless $s = \infty$ and the other element is of the form $\langle 1, -d, -e, de\rangle$, but we will select the d_l, e_l, so this will work too. A similar statement can be made for the $\langle 1, -c_k\rangle$. If the b_j can be selected so that $\langle 1, -b_i\rangle \cdot \langle 1, -b_j\rangle \neq 0$ iff $\{i, j\} = \{2f-1, 2f\}$, $1 \leqslant f \leqslant p/2$, then we say condition $B(M)$ holds. We say condition $B(N)$ holds if the above product is non-zero if and only if $\{i, j\} = \{2f, 2f+1\}$, $1 \leqslant f \leqslant (p-1)/2$. $C(M)$ and $C(N)$ denote analogous situations for the $\langle 1, -c_k\rangle$. Notice that $\langle 1, -b_i\rangle \cdot \langle 1, -b_j\rangle \neq 0$ means this product must be $\langle 1, -d_1, -e_1, d_1 e_1\rangle$.

We are now ready to state the structure theorem for $W(F)$. The proof techniques are similar for each case so only one will be done in detail.

THEOREM 7. *Let F be a field with $m = 4$ and $8 < |F^{\cdot}/R| < \infty$. Then there are elements as described above so that $W(F)$ is the direct sum of the subgroups generated by $\langle 1\rangle$, $\{\langle 1, -a_i\rangle\}_{i \in I'}$, $\{\langle 1, -b_j\rangle\}_{j=m}^{p}$, $\{\langle 1, -c_k\rangle\}_{k=n}^{q}$, and $\{\langle 1, -d_l, -e_l, d_l e_l\rangle\}_{l \in L}$. These subgroups all have order 2 unless specifically stated otherwise. There exist 10 cases.*

I. $s = 1$. *Then p, q are even; $(m, n) = (1, 1)$; $L = \{1, 2\}$; $B(M)$ and $C(M)$ hold.*

II. $s = 2$, $-1 \in R$. *Then p, q are even; $(m, n) = (1, 1)$; $L = \{1, 2\}$; $B(M)$ and $C(M)$ hold; $\langle 1\rangle$ has order 4.*

III. $s = 2$, $-1 \in B_1 - R$. *Then p, q are even; $(m, n) = (2, 1)$; $L = \{3\}$; $B(M)$ (for $f \geqslant 2$) and $C(M)$ hold; $\langle 1\rangle$ and $\langle 1, -b_2\rangle$ have order 4.*

IV. $s = 2$, $-1 \notin B_1$. *Then p, q are even; $(m, n) = (1, 2)$; $L = \emptyset$; $B(M)$ and $C(M)$ hold; $\langle 1\rangle$, $\langle 1, -b_2\rangle$, and $\langle 1, -c_2\rangle$ have order 4.*

V. $s = 4$, $-1 \in B_1$. *Then p is odd, q is even; $(m, n) = (2, 1)$; $L = \{2\}$; $B(N)$ and $C(M)$ hold; $\langle 1\rangle$ has order 8.*

VI. $s = 4$, $b_1 \in D(\langle 1, 1\rangle)$. *Then p is even, q is odd; $(m, n) = (1, 2)$; $L = \emptyset$; $B(M)$ and $C(N)$ hold; $\langle 1\rangle$ has order 8, $\langle 1, -b_2\rangle$ has order 4.*

VII. $s = 4$, $b_1 \notin D(\langle 1, 1\rangle)$. *Then p, q are odd; $(m, n) = (1, 2)$; $L = \emptyset$; $B(N)$ and $C(N)$ hold; $\langle 1\rangle$ has order 8, $\langle 1, -b_1\rangle$ has order 4.*

VIII, IX, *and* X *are exactly the same as* V, VI, *and* VII *respectively except "$s = 4$, $\langle 1\rangle$ has order 8" is replaced by "$s = \infty$, $\langle 1\rangle$ has infinite order".*

Proof. We prove only V where $s = 4$, $-1 = b_1 \in B_1$. The methods are similar to those used for Theorem 1 in [3]. Now $s = 4$ implies $D(\langle 1, 1\rangle) \nsupseteq B_1$ and so $G_1 = B_1 \cap D(\langle 1, 1\rangle)$ has index 2 in B_1. In fact $B_1 = \langle -1\rangle G_1$. By Proposition 11, $B_2 \subseteq D(\langle 1, -b\rangle)$ for all $b \in B_1$. Clearly $R \subseteq D(\langle 1, -b\rangle)$. Consequently $B_1 \nsubseteq D(\langle 1, -b\rangle)$ for $b \in B_1 - R$ by Proposition 10, and so $B_1 \cap D(\langle 1, -b\rangle)$ has index 2 in B_1. Theorem 6 shows that $\{B_1 \cap D(\langle 1, -b\rangle) \mid b \in B_1 - R\}$ forms a set of $2^p - 1$ distinct subgroups of index 2 in B_1, and since this is all there can be modulo R, for any $R \subseteq G \subseteq B_1$ of index 2, there must be a $b \in B_1$ satisfying $G = B_1 \cap D(\langle 1, -b\rangle)$.

Let $b_2 \in G_1 - R$ and write $G_1 = \langle b_2\rangle G_2$. Then there is a $b_3 \in B_1$ such that $B_1 \cap D\langle 1, -b_3\rangle = \langle -1\rangle G_2$. Moreover, $b_3 \in B_1 \cap D(\langle 1, 1\rangle) = G_1$. Notice that $-1 \in D(\langle 1, -a\rangle)$ (and hence $\langle 1, -a\rangle$ has order 2 in $W(F)$) for all $a \in G_1 - R$. We have $b_i \notin D(\langle 1, -b_j\rangle)$ for $\{i, j\} = \{2, 3\}$ and so $\langle 1, -b_2\rangle \cdot \langle 1, -b_3\rangle \neq 0$ in $W(F)$. Also $B_1 = \langle -1, b_2, b_3\rangle G_3$ where $G_1 \cap \cap D(\langle 1, -b_2\rangle) \cap D(\langle 1, -b_3\rangle) = G_3$. If $G_3 \neq R$, then select $b_4 \in G_3 - R$ and set $G_3 = \langle b_4\rangle G_4$. There exists $b_5 \in B_1$ satisfying $B_1 \cap D(\langle 1, -b_5\rangle) = \langle -1, b_2, b_3\rangle G_4$. And $b_5 \in B_1 \cap D(\langle 1, 1\rangle) \cap D(\langle 1, -b_2\rangle) \cap D(\langle 1, -b_3\rangle) = G_3$. So $\langle 1, -b_4\rangle \cdot \langle 1, -b_5\rangle \neq 0$ and $B_1 = \langle -1, b_2, b_3, b_4, b_5\rangle G_5$ where $G_3 \cap D(\langle 1, -b_4\rangle) \cap D(\langle 1, -b_5\rangle) = G_5$. Continuing in this fashion, we see p is odd and $B(N)$ holds.

To construct the c_j, we employ the same technique. Recall $-1 \in D(\langle 1, -c\rangle)$ for all $c \in B_2$. Pick any $c_1 \in B_2 - R$ and a $c_2 \in B_2 - D(\langle 1, -c_1\rangle)$. Then $\langle 1, -c_1\rangle \cdot \langle 1, -c_2\rangle \neq 0$ and $B_2 = \langle c_1, c_2\rangle G_2$ where $G_2 = B_2 \cap \cap D(\langle 1, -c_1\rangle) \cap D(\langle 1, -c_2\rangle)$. Proceeding as above, we see q is even and $C(M)$ holds.

We have found the desired multiplicative properties and subgroup orders. Showing the sum is direct and that $W(F)$ is all of this sum follows from the proof of Theorem 4.5 in [1]. ■

Theorem 4.5 in [1] is used to finish off all the non-real fields (I–VII), and the main idea behind finding the multiplicative structure is the same as above. Namely every subgroup (containing R) of index 2 in B_i is obtained as $B_i \cap D(\langle 1, -b\rangle)$ for some $b \in B_i$, $i = 1$ or 2. Getting started is the only problem. We briefly describe this process below.

Finding the b's in I, II and the c's in I, II, III is done exactly the same way as finding the c's for V. To find the b's in III, let $b_2 \in B_1 - -D(\langle 1, 1\rangle)$ and build B_1 from $\langle -1, b_2\rangle F^{\cdot 2}$. Finding the b's in IV is more complicated. By the Corollary of Proposition 10, there are $b_1 \in B_1$, $-b_1 \in B_2$ so that $D(\langle 1, 1\rangle) = D(\langle 1, -b_1\rangle) \cap D(\langle 1, b_1\rangle)$. Then $G_1 = B_1 \cap D(\langle 1, 1\rangle) = B_1 \cap D(\langle 1, -b_1\rangle)$ has index 2 in B_1, and $B_1 = \langle a\rangle G_1$, $G_1 = \langle b_1\rangle G_2$. Now there is a $b_2 \in B_1$ satisfying $B_1 \cap D(\langle 1, -b_2\rangle) = \langle a\rangle G_2$. It turns out a can be changed to this b_2 and the other b's are built from $\langle b_1, b_2\rangle G_2$. The same procedure, starting with $c_1 = -b_1$ gives the c's in IV and the b's in VI. If $b_1 \notin D(\langle 1, 1\rangle)$ (where $D(\langle 1, 1\rangle) \subseteq D(\langle 1, -b_1\rangle)$), set $B_1 = \langle b_1\rangle G_1$; and for $b_2 \in G_1 - R$, set $G_1 = \langle b_2\rangle G_2$. Then there is a $b_3 \in B_1$ so that $D(\langle 1, -b_3\rangle) = \langle b_1\rangle G_2$. B_1 is now built from $\langle b_1, b_2, b_3\rangle$. This method gives the b's in VII and, by starting with $c_1 = -b_1$, the c's in VI, VII.

Finding the b's and c's in VIII, IX, and X is done in exactly the way it is for V, VI, VII. That the orders also work out comes from the construction and Proposition 1.3 of [9], p. 298.

Theorem 4.5 of [1] applies only to non-real fields and thus does not help with the direct sum in VIII–X. However, since $m = 4$, we have that I^3F is torsion-free from Theorems 3.1 and 3.4 of [5]. So the dimension, determinant, Hasse invariant, and total signature classify quadratic forms over F (Theorem 3 of [6]). Actually the total signature is easy because by the following proposition, F has only one ordering when $|F^{\cdot}/R| > 4$.

PROPOSITION 12. *Let F be a real field with $m = 4$ and $|F^{\cdot}/R| > 4$. Then F has a unique ordering.*

Proof. F has a unique ordering if and only if $\sigma(F) = \bigcup_{n=1}^{\infty} D(n\langle 1\rangle)$ has index 2 in $F^{\cdot}$. Since $m = 4$, $D(\langle 1, 1\rangle)$ has index 2 or 4. If it is 2, we are done. Suppose it is 4. If $D(\langle 1, 1, 1, 1\rangle)$ has index 2, we are done; and if not, then $\sigma(F) = D(\langle 1, 1\rangle)$. Thus for every $a \in \sigma(F)$, $D(\langle 1, a\rangle) = \sigma(F)$. By Theorem 1, $a \in R$ and so $|F^{\cdot}/R| \leqslant 4$. ∎

When $|F^{\cdot}/R| \leqslant 4$ and $m = 4$, then $|F^{\cdot}/R|$ must be 4 and there are exactly 2 orderings on F.

Using the same principle as in the proof of Theorem 4.5 of [1] along with the signature, it is easy to see the sum in VIII–X is direct.

LEMMA. *Let F be a real field with an ordering P. If f, g are quadratic forms over F which have the same signature with respect to P and the same determinants and Hasse invariants, then* $\dim f \equiv \dim g \pmod 8$.

Proof. It suffices to consider f, g in a real closure K of F at P. So let $n = \dim f$, $n^+ =$ the number of 1's in a diagonalization of f over K, and $n^- =$ the number of -1's. Similarly for g, m, m^+, m^-. Then $d(f) = d(g)$ implies $n^- \equiv m^- \pmod 2$. That is, $n^- = 2k + l$ and $m^- = 2k' + l$ where l is 0 or 1. Now the Hasse invariant of f in K is $[-1, -1]^{k+l}$. Since this must also be $[-1, -1]^{k'+l}$, we have $k \equiv k' \pmod 2$. Finally since the signatures $\sigma(f) = \sigma(g)$, we have

$$n - m = \sigma(f) - \sigma(g) + 2(2k + l - 2k' - l) \equiv 0 \pmod 8. \ ∎$$

The lemma enables us to show the direct sum in VIII–X is in fact all of $W(F)$. Let f be an anisotropic form over F (where $8 < |F^{\cdot}/R| < \infty$). We build a form by first taking $\sigma(f)\langle 1\rangle$ (to get the desired signature) and adding appropriate $\langle 1, -a_i\rangle$, $\langle 1, -b_j\rangle$, $\langle 1, -c_k\rangle$, and $\langle 1, -1\rangle$ to make the determinant right. Then add appropriate $\langle 1, -1, 1, -1\rangle$, $\langle 1, -b_j, 1, -b_j\rangle$, and $\langle 1, -d, -e, de\rangle$ to make the Hasse invariant right. This new form, by the lemma, has the same dimension mod 8 as f. Adding the necessary multiple of $\langle 1, -1\rangle\langle 1, 1\rangle\langle 1, 1\rangle$ to the proper side gives equivalent forms by Theorem 3 of [6].

Possibly obscured by writing down a decomposition of $W(F)$ when $8 < |F^{\cdot}/R| < \infty$ and $m = 4$ was what actually determined it. We summarize the answer in the following corollary to Theorem 7.

COROLLARY. *If F is a field with $m = 4$ and $8 < |F^{\cdot}/R| < \infty$, then $W(F)$ is determined by $|F^{\cdot}/R|$, p, q, and the behavior of $D(\langle 1, 1\rangle)$.*

8. Value sets of ternary forms. When $m = 2$, it is well-known that every anisotropic ternary form $\langle a, b, c\rangle$ represents everything except $-abcR$. For $m = 4$, they usually miss more. We will keep the notation developed previously and note that it is sufficient to calculate $D(\langle 1, a, b\rangle)$. The answer depends on which of Q_1, Q_2, or Q_3 that $[-a, -b]$ is.

THEOREM 8. *Let F be a field with $m = 4$ and $8 \neq |F^{\cdot}/R| < \infty$. Suppose $\langle 1, a, b\rangle$ is anisotropic over F.*

(i) *If $[-a, -b] = Q_i$ where $\{i, j\} = \{1, 2\}$, then $D(\langle 1, a, b\rangle) = F^{\cdot} - (-abB_j)$.*

(ii) *If $[-a, -b] = Q_3$, then $D(\langle 1, a, b\rangle) = F^{\cdot} - (-abB_1 \cup -abB_2)$.*

Proof. $D(\langle 1, a, b\rangle)$ represents $c \in F^{\cdot}$ if and only if $\langle 1, a, b, -c\rangle$ is isotropic which is true if and only if there exists an $x \in F^{\cdot}$ satisfying $\langle 1, a, b, -c\rangle \cong \langle 1, -1, x, abcx\rangle$. So $c \in D(\langle 1, a, b\rangle)$ is equivalent to finding an x such that the Hasse invariants of the two above 4-dimensional forms are the same. That is, $[-1, -1][x, -abc] = [-abc, -1][a, b][-c, ab]$. This equation simplifies to $[-abc, -cx] = [-a, -b]$. So when is there a $y \in F^{\cdot}$ such that $[-abc, y] = [-a, -b]$? If $[-a, -b] = Q_i$, $i = 1, 2$, then the only ways are when $D(\langle 1, abc\rangle)$ has index 4 or when $-abc \in B_i$. Thus by the Corollary of Proposition 10 $-abc \notin B_1 \cup B_2$ or $-abc \in B_i$. Now (i) follows. If $[-a, -b] = Q_3$, then there is such a y if and only if $-abc \notin B_1 \cup B_2$; and (ii) follows. ∎

Corollary. *Let F be a field with $m = 4$, $R = F^2$, and $8 \neq q < \infty$. Then anisotropic ternary forms over F are determined by their value sets.*

Proof. It suffices to show that $D(\langle 1, a, b\rangle) = D(\langle 1, c, d\rangle)$ implies $\langle a, b\rangle \cong \langle c, d\rangle$ for anisotropic $\langle 1, a, b\rangle$, $\langle 1, c, d\rangle$. By a cardinality argument on the value sets mod F^2 and by Theorem 8, it is clear that it is impossible for exactly one of $[-a, -b]$, $[-c, -d]$ to be Q_3.

If $[-a, -b] = [-c, -d] = Q_3$, then by Theorem 8, $-abB_1 \cup -abB_2 = -cdB_1 \cup -cdB_2$. Thus $abcd \in B_1 \cap B_2 = F^2$. But then Corollary 2.9 [9, P. 60] shows $\langle -a, -b\rangle \cong \langle -c, -d\rangle$. If $[-a, -b] = [-c, -d] = Q_i$, $i = 1$ or 2, then Theorem 8 yields $abB_j = cdB_j$, $\{i, j\} = \{1, 2\}$. But the quaternion algebra equality also implies $-a, -b, -c, -d \in B_i$. Thus $abcd \in B_1 \cap B_2 = F^2$ and again $\langle -a, -b\rangle \cong \langle -c, -d\rangle$. Finally assume, $[-a, -b] = Q_1$ and $[-c, -d] = Q_2$. Then from Theorem 8, $abB_2 = cdB_1$. But this cannot happen since $B_1 \neq B_2$. ■

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] — *Kaplansky's radical and quadratic forms over non-real fields*, Acta Arith. 28 (1975), pp. 253–261.

[3] — *Quadratic forms over non-formally real fields with a finite number of quaternion algebras*, Pacific J. Math. 63 (1976), pp. 357–365.

[4] C. M. Cordes and J. R. Ramsey, *Quadratic forms over fields with $u = q/2 < \infty$*, Fund. Math. 99 (1978), pp. 1–10.

[5] R. Elman and T. Y. Lam, *Quadratic forms and the u-invariant. II*, Invent. Math. 21 (1973), pp. 125–137.

[6] — — *Classification theorems for quadratic forms over fields*, Comment. Math. Helvetici 49 (1974), pp. 373–381.

[7] I. Kaplansky, *Fröhlich's local quadratic forms*, J. Reine Angew. Math. 239 (1969), pp. 74–77.

[8] M. Kula, *Fields with prescribed quadratic form schemes*, preprint.

[9] T. Y. Lam, *The algebraic theory of quadratic forms*, W. A. Benjamin, Reading, Mass., 1973.

[10] O. T. O'Meara, *Introduction to quadratic forms*, Springer-Verlag, New York 1963.

MATHEMATICS DEPARTMENT
LOUISIANA STATE UNIVERSITY
Baton Rouge, Louisiana 70803

Received on 19. 11. 1979 (1184)

ACTA ARITHMETICA
XLI (1982)

Partitions into distinct small primes

by

J. Riddell* (Victoria, B. C., Canada)

Introduction. Throughout, p_n will denote the nth prime. In Theorem 1 we find estimates for $\sum_{k=1}^{n} p_k$ (see (3)), but because of the application of Theorem 3 later, it will be more convenient to work with the sum $y(n) = 3 + \sum_{k=4}^{n} p_k$ instead.

Theorem 1.

$$y(n) < \tfrac{1}{2}n^2(\log n + \log\log n) \qquad \textit{for } n \geqslant 4. \tag{1}$$

Given $0 \leqslant a < 1$, there exists an integer $N(a)$ such that

$$\tfrac{1}{2}n^2(\log n + a\log\log n) < y(n) \tag{2}$$

for $n \geqslant N(a)$, and $N(0) = 5$. Moreover, (2) is true if

$$a < 1 - \frac{2 - \log\left[1 - \dfrac{\log 2}{\log n}\right]}{\log\log n},$$

so that given $0 < \varepsilon \leqslant 1$, we can take $a = 1 - \varepsilon$ in (2), provided $n \geqslant n_0(\varepsilon) = N(1-\varepsilon)$.

$$\sum_{k=1}^{n} p_k < \tfrac{1}{2}n^2(\log n + \log\log n) \qquad \textit{for } n \geqslant 6, \tag{3}$$

and lower bounds for this sum are given by those for $y(n)$.

Corollary. $\sum_{k=1}^{n} p_k \sim \frac{1}{2}n^2(\log n + \log\log n)$.

We shall see later that $N(.1) = 5$ and $N(.156) = 140$ (see Remark 1, following the proof of (2)). The inequalities (1) and (2) are used in proving

Theorem 2. *Let $\varepsilon > 0$ and write $y(n) = y$. Then*

$$\sqrt{2y}\sqrt{\log\sqrt{2y} + (\tfrac{1}{2}-\varepsilon)\log\log\sqrt{2y}} < p_n < \sqrt{2y}\sqrt{\log\sqrt{2y} + (\tfrac{1}{2}+\varepsilon)\log\log\sqrt{2y}}$$

* Research partially supported by NSERC Grant A-5208.