Can. J. Math., Vol. XXXI, No. 5, 1979, pp. 1047–1058

QUADRATIC FORMS OVER QUADRATIC EXTENSIONS OF FIELDS WITH TWO QUATERNION ALGEBRAS

CRAIG M. CORDES AND JOHN R. RAMSEY, JR.

1. Introduction. In this paper, we analyze what happens with respect to quadratic forms when a square root is adjoined to a field F which has exactly two quaternion algebras. There are many such fields—the real numbers and finite extensions of the p-adic numbers being two familiar examples. For general quadratic extensions, there are many unanswered questions concerning the quadratic form structure, but for these special fields we can clear up most of them.

It is assumed char $F \neq 2$ and $K = F\ (\sqrt{a})$ where $a \in \dot{F} - \dot{F}^2$. $\dot{F}$ denotes the non-zero elements of F. Generally the letters $a, b, c, \ldots$ and $\alpha, \beta, \ldots$ refer to elements from $\dot{F}$ and $x, y, z, \ldots$ come from $\dot{K}$. Diagonalized quadratic forms are denoted by $\varphi = (x_1, \ldots, x_n)$ and $D_K(\varphi) = \{y \in \dot{K} \mid \varphi \text{ represents } y \text{ over } K\}$. The number of quaternion algebras over K is $m(K)$, $q(K) = |\dot{K}/\dot{K}^2|$, and $u(K)$ is the u-invariant. If $A \subseteq \dot{K}$, then $\langle A \rangle$ is the subgroup in $\dot{K}$ generated by A. This symbol will also refer to $\dot{F}$, but the context will always make clear which is meant.

A subgroup of central importance throughout will be the radical, $R(K) = \{x \mid D_K(1, -x) = \dot{K}\}$. Another formulation for $R(K)$ is $\{x \mid [x, y] \cong [1, -1]$ for all $y \in \dot{K}\}$ where $[x, y]$ is the quaternion algebra over K with structure constants x, y. For more on $R(K)$, see [**1**], [**2**], and [**6**]. In [**2**], it was shown the role $R(F)$ plays when $q(F) < \infty$, $m(F) = 2$, and F is non-formally real. The Witt ring (and hence the quadratic form structure) is determined by the level (Stufe), $q(F)$, $|{}^{D(1,1)}/\dot{F}^2|$, and $|{}^{R(F)}/\dot{F}^2|$. When F is formally real and $m(F) = 2$, then it follows from the proof of Proposition 2.3 in [**10**] that $R(F)$ has index 2 in $\dot{F}$. The quadratic form structure is now given by Theorem 1 of [**6**] and is rather uncomplicated. In fact from the above, it is easy to see that for real F, $m(F) = 2$ if and only if $R(F)$ has index 2. Moreover, $D_F(1, 1) = R(F)$.

The main results of this paper are the following two theorems.

THEOREM (3.8, 4.8). *Let F be a field with $m(F) = 2$ and let $K = F(\sqrt{a})$ where $a \in \dot{F} - \dot{F}^2$. Then $m(K) = 4$ when $a \in R(F)$ and $m(K) \leqq 2$ when $a \notin R(F)$. Moreover, for $a \notin R(F)$, $m(K) = 1$ if and only if F is formally real.*

THEOREM (3.10, 4.14). *If $m(F) = 2$, $q(F) < \infty$, and $K = F\ (\sqrt{a})$ where $a \in \dot{F} - \dot{F}^2$, then $N_{K/F}(x) \in R(F)$ if and only if there is an $f \in \dot{F}$ such that $fx \in R(K)$. Moreover, $|{}^{R(K)}/\dot{K}^2| = |{}^{R(F)}/\dot{F}^2|^2$ when $a \notin R(F)$ and $|{}^{R(K)}/\dot{K}^2| = \frac{1}{2}|{}^{R(F)}/\dot{F}^2|^2$ when $a \in R(F)$.*

Received May 10, 1978.

https://doi.org/10.4153/CJM-1979-096-x Published online by Cambridge University Press

2. Some preliminaries. If $m(F) = 2$, then it is well known that $D_F(1, -b)$ has index 1 or 2 for all $b \in \dot{F}$. From Theorem 1, 2 in [**6**], it follows that if $D_F(1, -b)$ has index 1 or 2 for all $b \in \dot{F}$ (and is 2 for at least one b), then $m(F) = 2$. This is how we will show $m(K) \leqq 2$ when $a \notin R(F)$ and $m(K) \geqq 4$ when $a \in R(F)$. Another result that will be used frequently is Lemma 1 of [**2**]. Namely, for $m(F) = 2$ and $b, c \in \dot{F}$, $D_F(1, b) = D_F(1, c)$ if and only if $bc \in R(F)$. Actually one direction of this is true more generally for any field; i.e., $D_F(a_1, \ldots, a_n) = D_F(r_1a_1, \ldots, r_na_n)$ for all $n \geqq 2$ and $r_i \in R(F)$. See [**1**].

A helpful lemma which we apply is given below. We will use this often with no further mention. An easy but interesting corollary of the lemma and $R(F) = \bigcap_{b \in F} D_F(1, b)$ (see [**2**]) is also given.

LEMMA. *Let $b, c \in \dot{F}$. Then $D_F(1, -b) \cap D_F(1, -c) \subseteq D_F(1, -bc)$.*

COROLLARY. $R(F) = \bigcap_{b \in B} D_F(1, -b)$ *where $B \subseteq \dot{F}$ and $\langle R(F), B\rangle = \dot{F}$.*

We are now ready to obtain results which are needed to analyze K when $m(F) = 2$.

PROPOSITION 2.1. *If $m(F) = 2$ and if $d \in \dot{F} - R(F)$, then every quaternary form over F of determinant d is isotropic.*

Proof. Let φ be any (non-singular) quaternary form over F. Since φ is isotropic if and only if $b\varphi$ is, we may assume $1 \in D_F(\varphi)$. So $\varphi \cong (1, -a, -b, abd)$. Since $d \notin R(F)$, $[-abc, d]$ takes on both possible values as c runs through $\dot{F}$. In particular, there is a $c \in \dot{F}$ such that $[-abc, d] = [a, b]$. It follows from [**7**, Theorem 3.21, p. 124] that $(-1, c, -cd) \cong (-a, -b, abd)$. Thus $\varphi \cong (1, -1, c, -cd)$ is isotropic.

The norm $N_{K/F}$ will play an important role in everything that follows. We abbreviate $N_{K/F}$ to N; and K, F are always related for the remainder of the paper as stated in the introduction; i.e., $K = F(\sqrt{a})$ where $a \in \dot{F} - \dot{F}^2$. An immediate consequence of Elman's and Lam's Norm Principle [**4**, Theorem 2.11] with $\varphi = (1)$ is the next proposition.

PROPOSITION 2.2. *If $x \in \dot{K}$ and $N(x) \in \dot{F}^2$, then there is a $\beta \in \dot{F}$ and a $y \in \dot{K}$ such that $x = \beta y^2$.*

Theorem 2.13 in [**4**] is also called the Norm Principle. It states for K, F as above that given a quadratic form φ over F and $x \in \dot{K}$, then $N(x) \in D_F(\varphi) \cdot D_F(\varphi)$ if and only if $x \in \dot{F} \cdot D_K(\varphi)$. We will have frequent occasion to apply this result and will refer to it as the Norm Principle.

PROPOSITION 2.3. *If $m(F) = 2$, then $\dot{F} \cap R(K) = R(F) \cup aR(F)$.*

Proof. $R(F) \cup aR(F) \subseteq \dot{F} \cap R(K)$ follows from the Corollary to Proposition 3 in [**1**]. On the other hand, if $c \in \dot{F} \cap R(K)$, then $x \in D_K(1, -c)$ for all $x \in \dot{K}$. Hence the Norm Principle implies $N(x) \in D_F(1, -c)$ and so $D_F(1, -a) \subseteq D_F(1, -c)$. Thus $c \in R(F) \cup aR(F)$ by the first paragraph of this section.

https://doi.org/10.4153/CJM-1979-096-x Published online by Cambridge University Press

COROLLARY 2.4. *If $m(F) = 2$ and $R(F) = \dot{F}^2$, then $R(K) = \dot{K}^2$.*

Proof. If $x \in R(K)$, then the Norm Principle gives $N(x) \in R(F) = \dot{F}^2$. So by Proposition 2.2, $x \equiv \beta \pmod{\dot{K}^2}$ for some $\beta \in \dot{F}$. But $\beta \in \dot{F} \cap R(K) = R(F) \cup aR(F) \subseteq \dot{K}^2$.

Much of the later work depends heavily on Scharlau's method of transfer [**9**]. For $y = b + c\sqrt{a} \in \dot{K}$, let S_y be the linear functional on K defined by $S_y(\alpha + \beta\sqrt{a}) = \alpha c - \beta b$ for all $\alpha, \beta \in F$. Then $\ker S_y = Fy$. If S_y^* denotes the transfer with respect to S_y and φ is any K-form, then $S_y^*(\varphi)$ is isotropic if and only if $D_K(\varphi)$ contains fy for some $f \in \dot{F}$.

PROPOSITION 2.5. *If $x, y \in \dot{K}$, then $S_y^*(x) = \alpha(1, -N(xy))$ where α is any member of $D_F[S_y^*(x)]$.*

Proof. Let $x = \alpha + \beta\sqrt{a}$, $y = b + c\sqrt{a}$. Then with respect to the basis $\{1, \sqrt{a}\}$ for K over F, the bilinear form associated with $S_y^*(x)$ has the matrix

$$\begin{pmatrix} \alpha c - \beta b & a\beta c - \alpha b \\ a\beta c - \alpha b & a(\alpha c - \beta b) \end{pmatrix}.$$

The determinant of this matrix is $-N(x)N(y)$ and the result follows.

PROPOSITION 2.6. *Let $m(F) = 2$ and suppose $x, y \in \dot{K}$. If $N(x) \notin R(F)$, then there exists an $f \in \dot{F}$ such that $fy \in D_K(1, -x)$.*

Proof. Such an f exists if and only if $S_y^*(1, -x)$ is isotropic. By Proposition 2.5

$$S_y^*(1, -x) = \alpha(1, -N(y)) - \beta(1, -N(xy))$$

for particular $\alpha, \beta \in \dot{F}$. So the determinant of $S_y^*(1, -x)$ is $N(x)$, and by Proposition 2.1, $S_y^*(1, -x)$ is isotropic.

We conclude this section by recalling from [**5**, pp. 298–299] how to find basis representatives for $\dot{K}/\dot{K}^2$. Let $B \cup \{a\}$ be a set of representatives for a basis of $\dot{F}/\dot{F}^2$ and let C be a set of representatives for a basis of $D_F(1, -a)$. For each $\alpha = e^2 - af^2 \in C$, let $\bar{\alpha} = e + f\sqrt{a}$. Then a set of representatives for a basis of $\dot{K}/\dot{K}^2$ is given by $\{b\} \cup \{\bar{\alpha}\}$ where $b \in B, \alpha \in C$.

3. The case $a \notin R(F)$. Throughout this section, we assume $a \notin R(F)$ and $m(F) = 2$. These assumptions will not be stated in the propositions but will be in the main results.

PROPOSITION 3.1. *For every $c \in \dot{F}$, $\dot{F} \subseteq D_K(1, -c)$.*

Proof. Suppose $b, c \in \dot{F}$. Since $a \notin R(F)$, $[a, \alpha]$ takes on both possible values as α runs through $\dot{F}$. Choose α such that $[b, c] \cong [a, \alpha]$. Then over F,

$$(1, -b) \otimes (1, -c) = (1, -b, -c, bc) \cong (1, -a) \otimes (1, -\alpha).$$

https://doi.org/10.4153/CJM-1979-096-x Published online by Cambridge University Press

Hence, $(1, -b) \otimes (1, -c)$ is hyperbolic over K and $b \in D_K(1, -c)$. Thus $\dot{F} \subseteq D_K(1, -c)$.

The next corollary now follows immediately from the Norm Principle.

COROLLARY 3.2. *For $x \in \dot{K}$ and $c \in \dot{F}$, $x \in D_K(1, -c)$ if and only if $N(x) \in D_F(1, -c)$.*

COROLLARY 3.3. *If $c \in \dot{F}$, then $D_K(1, -c)$ has index 1 or 2 in $\dot{K}$.*

Proof. Suppose $x, y \notin D_K(1, -c)$. By the above, $N(x), N(y) \notin D_F(1, -c)$. But $m(F) = 2$ then implies $N(xy) \in D_F(1, -c)$ and so $xy \in D_K(1, -c)$.

The next two results are immediate consequences of Corollary 3.2.

COROLLARY 3.4. *If $x \in \dot{K}$, then $\dot{F} \cap D_K(1, -x) = D_F(1, -N(x))$.*

COROLLARY 3.5. *For $x \in \dot{K}$, $\dot{F} \subseteq D_K(1, -x)$ if and only if $N(x) \in R(F)$.*

PROPOSITION 3.6. *If $x \in \dot{K}$ and $N(x) \notin R(F)$, then $D_K(1, -x)$ has index 2 in $\dot{K}$.*

Proof. By Corollary 3.4, $\dot{F} \cap D_K(1, -x)$ has index 2 in $\dot{F}$. So there is a $c \in \dot{F}$ such that exactly one of f or fc is in $D_K(1, -x)$ for $f \in \dot{F}$. Consider $y \in \dot{K}$. By Proposition 2.6, there is an $f \in \dot{F}$ such that $fy \in D_K(1, -x)$. Hence either y or cy must be in $D_K(1, -x)$.

PROPOSITION 3.7. *If $x \in \dot{K}$ and $N(x) \in R(F)$, then $D_K(1, -x)$ has index 1 or 2 in $\dot{K}$.*

Proof. Suppose $D_K(1, -x) \neq \dot{K}$ and let $y_1, y_2 \notin D_K(1, -x)$. It suffices to show $y_1y_2 \in D_K(1, -x)$. If $N(y_1) \in R(F)$, then $S_{y_1}{}^*(1, -x) = \alpha(1, -N(y_1)) - \beta(1, -N(xy_1))$ is clearly isotropic. Therefore there is an $f \in \dot{F}$ such that $fy_1 \in D_K(1, -x)$. But then by Corollary 3.5, $y_1 \in D_K(1, -x)$. This contradiction shows $N(y_1), N(y_2) \notin R(F)$, and so $D_K(1, -y_i)$, $i = 1, 2$, have index 2 in $\dot{K}$. If $N(y_1y_2) \in R(F)$, then as above $y_1y_2 \in D_K(1, -x)$. If $N(y_1y_2) \notin R(F)$, then $D_F(1, -N(y_1)) \neq D_F(1, -N(y_2))$ by Lemma 1 of [**2**]. So there is a $\beta \in \dot{F} - [D_F(1, -N(y_1) \cup D_F(1, -N(y_2))]$ and Corollary 3.4 now gives

$$\beta \notin D_K(1, -y_1) \cup D_K(1, -y_2).$$

But x does not belong to the union either means we must have $\beta x \in D_K(1, -y_i)$, $i = 1, 2$. Therefore $y_i \in D_K(1, -\beta x)$ for each $i = 1, 2$ and so $y_1y_2 \in D_K(1, -\beta x)$. Moreover, $\beta \notin D_K(1, -y_i)$, $i = 1, 2$ implies $y_1, y_2 \notin D_K(1, -\beta)$. So $y_1y_2 \in D_K(1, -\beta)$ by Corollary 3.3. Finally $y_1y_2 \in D_K(1, -\beta) \cap D_K(1, -\beta x) \subseteq D_K(1, -x)$.

Since $D_K(1, -x)$ has index 1 or 2 for every $x \in \dot{K}$, we now have $m(K) \leqq 2$ (see the first paragraph of Section 2). If $m(K) = 1$, then $R(K) = \dot{K}$ and by Proposition 2.3, $\dot{F} = R(F) \cup aR(F)$. Thus $R(F)$ has index 2 in $\dot{F}$ and so F

https://doi.org/10.4153/CJM-1979-096-x Published online by Cambridge University Press

must be a formally real field [**6**, Lemma 2]. Conversely, if F is a real field with $m(F) = 2$, then $R(F)$ has index 2 in $\dot{F}$. Consequently $-a \in R(F)$ and $D_F(1, -a) = D_F(1, 1) = R(F)$. In particular, $N(x) \in R(F)$ for all $x \in \dot{K}$. Fix $x, y \in \dot{K}$. Then

$$S_y^*(1, -x) = \alpha(1, -N(y)) - \beta(1, -N(xy))$$

is clearly isotropic over F, and there must be an $f \in \dot{F}$ satisfying $fy \in D_K(1, -x)$. But $\dot{F} \subseteq D_K(1, -x)$ by Corollary 3.5 then gives $y \in D_K(1, -x)$. It now follows that $x \in R(K)$. So $R(K) = \dot{K}$ and therefore $m(K) = 1$.

THEOREM 3.8. *Let F be a field with $m(F) = 2$ and $K = F(\sqrt{a})$ where $a \in \dot{F} - \dot{F}^2$. If $a \notin R(F)$, then $m(K) \leqq 2$. Moreover $m(K) = 1$ if and only if F is formally real.*

Recall that quadratic forms over fields with exactly one quaternion algebra are determined up to equivalence by just their determinant and dimension. Quadratic form structure over non-formally real fields with exactly two quaternion algebras depends heavily on the radical. Under certain finiteness conditions, we can say a lot more about $R(K)$.

PROPOSITION 3.9. *Let $|\dot{F}/R(F)| < \infty$ and suppose $x \in \dot{K}$. If $N(x) \in R(F)$, then there is an $f \in \dot{F}$ such that $fx \in R(K)$.*

Proof. If $R(F) = \dot{F}^2$, then the proposition follows immediately from Proposition 2.2. So we may assume $|R(F)/\dot{F}^2| > 1$. Suppose $N(x) \in R(F)$ but $\dot{F}x \cap R(K) = \emptyset$. By the above we must also have $N(x) \notin \dot{F}^2$.

Using the remarks at the end of Section 2, we will now construct a set of representatives for a basis of $\dot{K}/\dot{K}^2$. Let $\{\alpha_i\}_{i \in I}$ be a basis for $R(F)$ over $\dot{F}$ (mod $\dot{F}^2$) and adjoin $\{\beta_j\}_{j=1}^k$ to get a basis for $D_F(1, -a)$. If there are no such β_i, then F is formally real [**6**, Lemma 2] and $m(K) = 1$. Hence $R(K) = \dot{K}$ and the proposition follows. So we assume $1 \leqq k < \infty$ and we may also take one of the α_i to be $N(x)$. Now $D_F(1, -a)$ has index 2 in $\dot{F}$ so there is a $\beta \in \dot{F} - D_F(1, -a)$ so that

$$\{\alpha_i\}_{i \in I} \cup \{\beta_j\}_{j=1}^k \cup \{\beta\}$$

forms a basis for $\dot{F}$. Moreover, we choose $\beta = a$ if $a \notin D_F(1, -a)$ and $\beta_k = a$ if $a \in D_F(1, -a)$. For each α_i and β_j, choose x_i and y_j such that $N(x_i) = \alpha_i$ and $N(y_j) = \beta_j$. For $\alpha_i = \alpha$, select $x_i = x$. Finally let $\gamma = \beta$ if $a \in D_F(1, -a)$ and let $\gamma = \beta_k$ otherwise. Then

$$\{\alpha_i\}_{i \in I} \cup \{\beta_j\}_{j=1}^{k-1} \cup \{\gamma\} \cup \{x_i\}_{i \in I} \cup \{y_j\}_{j=1}^k$$

is a set of representatives for a basis of $\dot{K}/\dot{K}^2$.

We are working under the assumptions F is non-real (so $m(K) = 2$) and $\dot{F}x \cap R(K) = \emptyset$. By Lemma 1 of [**2**] and Proposition 2.3, the set of $D_K(1, -fx)$ as f runs through distinct square classes of $\langle \beta_1, \ldots \beta_{k-1}, \gamma \rangle$ are distinct subgroups in $\dot{K}$ of index 2. By Corollary 3.5, $\dot{F} \subseteq D_K(1, -fx)$ for all $f \in \dot{F}$; and it

https://doi.org/10.4153/CJM-1979-096-x Published online by Cambridge University Press

follows just as in the discussion prior to Theorem 3.8 that $x_i \in D_K(1, -fx)$ for $i \in I$. So if we denote $\langle y_1, \ldots, y_k \rangle \dot{K}^2$ by V, then the set of $D_K(1, -fx) \cap V$ form 2^k distinct subspaces of V of dimension $k - 1$. But there are only $2^k - 1$ distinct hyperplanes in a vector space over $GF(2)$ of dimension k. This is a contradiction and so it was false to assume $\dot{F}x \cap R(K) = \emptyset$.

THEOREM 3.10. *Suppose $m(F) = 2$, $q(F) < \infty$, and $K = F(\sqrt{a})$ where $a \in \dot{F} - R(F)$. Then for $x \in \dot{K}$, $N(x) \in R(F)$ if and only if there is an $f \in \dot{F}$ so that $fx \in R(K)$. Moreover, $|{}^{R(K)}/\dot{K}^2| = |{}^{R(F)}/\dot{F}^2|^2$.*

Proof. The sufficiency follows from the Norm Principle, and the necessity comes from Proposition 3.9.

If $|{}^{R(F)}/\dot{F}^2| = 1$, then $|{}^{R(K)}/\dot{K}^2| = 1$ by Corollary 2.4. If $|{}^{R(F)}/\dot{F}^2| > 1$, let $\{\alpha_i\}_{i=1}^n$ be a set of representatives for a basis of ${}^{R(F)}/\dot{F}^2$. Choose $x_i \in \dot{K}$ satisfying $N(x_i) = \alpha_i$. By the above there exist $f_i \in \dot{F}$ such that $f_i x_i \in R(K)$; and moreover, $\{\alpha_i\} \cup \{f_i x_i\}_{i=1}^n$ form an independent set modulo $\dot{K}^2$. Since $R(F) \subseteq R(K)$ [**1**, Proposition 3], we have

$$V = \langle \alpha_1, \ldots, \alpha_n, f_1 x_1, \ldots, f_n x_n \rangle \dot{K}^2 \bmod \dot{K}^2$$

is a $2n$-dimension subspace of ${}^{R(K)}/\dot{K}^2$. Now suppose $x \in R(K)$. Then $N(x) \in R(F)$ implies there must be $y \in \langle f_1 x_1, \ldots, f_n x_n \rangle \dot{K}^2$ so that $N(x) \equiv N(y) \pmod{\dot{F}^2}$. By Proposition 2.2, $xy = \beta z^2$ where $\beta \in \dot{F}$, $z \in \dot{K}$. But $x, y \in R(K)$ give $\beta \in R(K) \cap \dot{F} = R(F)$. So $x \equiv \beta y \pmod{\dot{K}^2}$ and $x \in V$. Consequently $V = R(K)$ and $|{}^{R(K)}/\dot{K}^2| = |{}^{R(F)}/\dot{F}^2|^2$ follows.

It would seem as if some result similar to Proposition 3.9 would hold without any finiteness conditions. Then the same proof as for Theorem 3.10 would enable us to write a basis for $R(K)$. But as yet we have been unable to find such a result or to discover a counterexample.

4. The case $a \in R(F)$. Throughout this section it is assumed $m(F) = 2$ and $a \in R(F)$. The results when $a \in R(F)$ are not as simple as for $a \notin R(F)$. The primary reason for this is that $\dot{F} \subseteq D_K(1, -c)$ is no longer true for all $c \in \dot{F}$. The next proposition, which does not depend on $m(F) = 2$, shows what can be said.

PROPOSITION 4.1. *For every $c \in \dot{F}$, $\dot{F} \cap D_K(1, -c) = D_F(1, -c)$.*

Proof. Clearly $D_F(1, -c) \subseteq \dot{F} \cap D_K(1, -c)$. So suppose $b \in \dot{F} \cap D_K(1, -c)$. Then $(1, -c) \otimes (1, -b)$ is isotropic over K and hence hyperbolic [**8**, Theorem 2]. Therefore, by [**9**, Remark 2.29] there are $e, f \in \dot{F}$ such that $(1, -c) \otimes (1, -b) \cong (1, -a) \otimes (e, f)$ over F. But $a \in R(F)$ implies $(1, -a) \otimes (e, f)$ is isotropic and so $b \in D_F(1, -c)$.

COROLLARY 4.2. *Let $c \in \dot{F}$. Then $\dot{F} \subseteq D_K(1, -c)$ if and only if $c \in R(F)$. Moreover, $c \in R(F)$ if and only if $c \in R(K)$.*

PROPOSITION 4.3. *If $c \in \dot{F} - R(F)$, then $D_K(1, -c)$ has index 4 in $\dot{K}$.*

https://doi.org/10.4153/CJM-1979-096-x Published online by Cambridge University Press

Proof. $\dot{F} \cap D_K(1, -c) = D_F(1, -c)$ has index 2 in $\dot{F}$. Choose $b \in \dot{F} - D_F(1, -c)$ and select $y \in \dot{K}$ satisfying $N(y) = b$. By the Norm Principle y, $by \notin D_K(1, -c)$. Hence $D_K(1, -c)$ has index at least 4 in $\dot{K}$. But for $x \in \dot{K}$, either $N(x)$ or $N(xy) \in D_F(1, -c)$. Thus again by the Norm Principle, either x or $xy \in \dot{F} \cdot D_K(1, -c) = D_K(1, -c) \cup b\, D_K(1, -c)$. So x is in one of the cosets of $D_K(1, -c)$ represented by 1, b, y, or by.

So we see already that $m(K) \geqq 4$ since $(x, y) \cong (u, v)$ if and only if $xy \equiv uv \pmod{\dot{K}^2}$ and $[x, y] = [u, v]$. We will show equality holds here.

PROPOSITION 4.4. *If $x \in \dot{K}$, then $\dot{F} \cap D_K(1, -x)$ has index either* 1 *or* 2 *in* $D_F(1, -N(x))$.

Proof. By the Norm Principle, $\dot{F} \cap D_K(1, -x) \subseteq D_F(1, -N(x))$. So it suffices to show that $\alpha\beta \in D_K(1, -x)$ whenever $\alpha, \beta \in D_F(1, -N(x)) - D_K(1, -x)$. Now $\alpha, \beta \in D_F(1, -N(x))$ implies

$$N(x) \in D_F(1, -\alpha) \cap D_F(1, -\beta);$$

and so by the Norm Principle,

$$x \in \dot{F} \cdot D_K(1, -\alpha) \cap \dot{F} \cdot D_K(1, -\beta).$$

Also $\alpha, \beta \notin D_K(1, -x)$ means $\alpha, \beta \notin R(K)$ and therefore $\alpha, \beta \notin R(F)$ as well. Hence $D_F(1, -\alpha)$ and $D_F(1, -\beta)$ have index 2 in $\dot{F}$, and b can be chosen so that $b \in \dot{F} - (D_F(1, -\alpha) \cup D_F(1, -\beta))$. Using the above and $x \notin D_K(1, -\alpha) \cup D_K(1, -\beta)$, we obtain $x \in bD_K(1, -\alpha) \cap bD_K(1, -\beta)$. That is, $bx \in D_K(1, -\alpha) \cap D_K(1, -\beta)$ which is contained in $D_K(1, -\alpha\beta)$. But $b \notin D_F(1, -\alpha) \cup D_F(1, -\beta)$ yields $\alpha, \beta \notin D_F(1, -b)$ which means $\alpha\beta \in D_F(1, -b)$. Consequently $b \in D_K(1, -\alpha\beta)$ and this combined with $bx \in D_K(1, -\alpha\beta)$ gives $x \in D_K(1, -\alpha\beta)$. Thus $\alpha\beta \in D_K(1, -x)$.

COROLLARY 4.5. *Let $x \in \dot{K}$ with $N(x) \notin R(F)$. Then $D_K(1, -x)$ has index* 2 *or* 4 *in $\dot{K}$ depending on whether $\dot{F} \cap D_K(1, -x)$ has index* 1 *or* 2 *respectively in* $D_F(1, -N(x))$.

The proof of the corollary follows exactly the same steps as the proof for Proposition 3.6. We see that the coset representatives for $D_K(1, -x)$ in $\dot{K}$ can be chosen to be any set of coset representatives for $\dot{F} \cap D_K(1, -x)$ in $\dot{F}$.

COROLLARY 4.6. *If $\dot{F} \subseteq D_K(1, -x)$, then*

$$\dot{F} \cap D_K(1, -bx) = D_F(1, -b) \text{ for all } b \in \dot{F}.$$

Proof. By Proposition 4.4, $N(x) \in R(F)$. Thus $\dot{F} \cap D_K(1, -bx)$ has index 1 or 2 in $\dot{F}$. But

$$\dot{F} \cap D_K(1, -bx) = \dot{F} \cap D_K(1, -bx) \cap D_K(1, -x) \subseteq \dot{F} \cap D_K(1, -b) = D_F(1, -b).$$

So we are done if $b \notin R(F)$. If $b \in R(F)$, then $D_K(1, -bx) = D_K(1, -x)$ and this, too, yields our claim.

https://doi.org/10.4153/CJM-1979-096-x Published online by Cambridge University Press

Suppose $b \in \dot{F} - R(F)$. Then by Proposition 4.3, $D_K(1, -b)$ has index 4 in $\dot{K}$. In particular there are (up to isomorphism) exactly 4 quaternion algebras, $[b, y]$, as y runs through $\dot{K}$. The next proposition says this set of quaternion algebras is independent of b.

PROPOSITION 4.7. *If $b, c \in \dot{F} - R(F)$, then the four quaternion algebras over K of the form $[b, y]$, $y \in \dot{K}$ are the same as those of the form $[c, z]$, $z \in \dot{K}$.*

Proof. If $bc \in R(F)$, then $[bc, x]$ is split for all $x \in \dot{K}$ and $[b, x] = [c, x]$. So we assume $bc \notin R(F)$, and by Lemma 1 of [**2**], $D_F(1, -b) \not\subseteq D_F(1, -bc)$. We may choose an $\alpha \in \dot{F} - [D_F(1, -b) \cup D_F(1, -c)]$. Pick $x \in \dot{K}$ such that $N(x) \equiv \alpha (\mathrm{mod}\ \dot{F}^2)$. Since $\dot{F} \cap D_K(1, -bc) = D_F(1, -bc)$ has index 2 in $\dot{F}$, we may choose x (by adjusting with an $\dot{F}$-scalar if necessary) so that $x \notin D_K(1, -bc)$. Since $N(x) \notin D_F(1, -b) \cup D_F(1, -c)$, the Norm Principle implies $x, \alpha x \notin D_K(1, -b) \cup D_K(1, -c)$. Hence $1, \alpha, x, \alpha x$ are representatives for all four cosets of both $D_K(1, -b)$ and $D_K(1, -c)$. The four quaternion algebras then of the form $[b, y]$ are $[b, 1]$, $[b, \alpha]$, $[b, x]$, and $[b, \alpha x]$; similarly for $[c, z]$. Clearly $[b, 1] = [c, 1]$. Also $\alpha \notin D_F(1, -b) \cup D_F(1, -c)$ yields $b, c \notin D_F(1, -\alpha)$ which means $bc \in D_F(1, -\alpha)$. Hence $[b, \alpha] = [c, \alpha]$.

Claim. $[b, x] = [c, \alpha x]$.

This will be true if and only if

$$(1, -b, -x, bx) \cong (1, -c, -\alpha x, c\alpha x)$$

[**7**, Proposition 2.5, p. 57]. Consider $D_K(-x, bx) \cap D_K(-\alpha x, c\alpha x)$. This set will be non-empty if and only if

$$V = D_K(1, -b) \cap \alpha D_K(1, -c) \neq \emptyset.$$

Now $\alpha \notin D_F(1, -c)$, and so

$$D_F(1, -b) = [D_F(1, -b) \cap D_F(1, -c)] \cup V.$$

But $D_F(1, -b) \cap D_F(1, -c) \subseteq D_F(1, -bc)$ and the initial fact that $D_F(1, -b) \not\subseteq D_F(1, -bc)$ imply there is $\beta \in V - D_F(1, -bc)$.

So $V \neq \emptyset$ and in fact $-\beta x \in D_K(-x, bx) \cap D_K(-\alpha x, c\alpha x)$. Hence

$$(1, -b, -x, bx) \cong (1, -b, -\beta x, b\beta x) \quad \text{and}$$

$$(1, -c, -\alpha x, c\alpha x) \cong (1, -c, -\beta x, c\beta x).$$

All four of these are equivalent if and only if $(-b, b\beta x) \cong (-c, c\beta x)$ which is true if and only if $\beta x \in D_K(1, -bc)$.

From Proposition 4.3 and its proof, the coset representatives of $D_K(1, -bc)$ are $1, \beta, y, \beta y$ where y is chosen with $N(y) = \beta$. Since $N(x) = \alpha \notin D_F(1, -b) \cup D_F(1, -c)$, $N(x) \in D_F(1, -bc)$. Thus from the Norm Principle,

$$x \in \dot{F} \cdot D_K(1, -bc) = D_K(1, -bc) \cup \beta D_K(1, -bc).$$

https://doi.org/10.4153/CJM-1979-096-x Published online by Cambridge University Press

But x was chosen not to be in $D_K(1, -bc)$. So $\beta x \in D_K(1, -bc)$ and the claim is established.

The proof will be complete if we show $[b, \alpha x] = [c, x]$. Viewing the following products in the Brauer group of K, we have $[b, x] = [c, \alpha x] = [c, \alpha][c, x] = [b, \alpha][c, x]$ implies $[b, \alpha x] = [b, \alpha][b, x] = [c, x]$.

THEOREM 4.8. *Let F be a field with $m(F) = 2$ and $K = F(\sqrt{a})$ where $a \in \dot{F} - \dot{F}^2$. If $a \in R(F)$, then $m(K) = 4$.*

Proof. From Proposition 4.7 it follows that the set of quaternion algebras over K of the form $[b, x]$, $b \in \dot{F}$, $x \in \dot{K}$ comprise a subgroup (of the Brauer group) of order 4. Call this subgroup H. Next we will show that if $N(y) \notin R(F)$, then all $[x, y]$, $x \in \dot{K}$, lie in H. By the remarks after Corollary 4.5, $D_K(1, -y)$ has coset representatives $\{1, \alpha\}$ or $\{1, \alpha, \beta, \alpha\beta\}$ where $\alpha, \beta \in \dot{F}$. Thus $[x, y]$ is isomorphic to one of $[1, y]$, $[\alpha, y]$, $[\beta, y]$, or $[\alpha\beta, y]$. In any case, $[x, y] \in H$.

To complete the proof, we must show $[x, y] \in H$ whenever $N(x), N(y) \in R(F)$. For such x, y we pick any $z \in \dot{K}$ with $N(z) \notin R(F)$. This is possible since $R(F) \subsetneqq D_F(1, -a) = \dot{F}$. Then $N(xz) \notin R(F)$ and by Proposition 2.6, there exists $f \in \dot{F}$ satisfying $-fxy \in D_K(1, -xz)$. Therefore, $xz \in D_K(1, fxy)$ and

$$(1, fxy) \cong (xz, fyz).$$

So $(x, fy) \cong (z, fxyz)$, and this yields $[x, fy] = [z, fxyz]$ which implies

$$[x, y] = [x, f] \cdot [z, fxyz].$$

But the factors on the right hand side have been shown to lie in H.

COROLLARY 4.8. *If $N(x) \in R(F)$, then $D_K(1, -x)$ has index* 1, 2, *or* 4 *in $\dot{K}$.*

Knowing $m(K) = 4$ is useful. For example by [**7**, Corollary 4.12, P. 323], if K is non-real, then $m(K) = 4$ implies $u(K) = 4$. Thus, quadratic forms are determined up to equivalence by dimension, determinant, and Hasse invariant.

Our last goal is to find a statement akin to Theorem 3.10. Some of the tools that are needed hold under no finiteness conditions, but once again we have been unable to free the major result of this hypothesis.

PROPOSITION 4.9. *Let $x \in \dot{K}$ and $f, g \in \dot{F}$. Then*

$$\dot{F} \cap D_K(1, -fx) = \dot{F} \cap D_K(1, -gx)$$

if and only if $fg \in R(F) \cdot \langle N(x) \rangle$.

Proof. It follows from the Norm Principle that both $\dot{F} \cap D_K(1, -fx)$ and $\dot{F} \cap D_K(1, -gx)$ are contained in $D_F(1, -N(x))$. So

$$\dot{F} \cap D_K(1, -fx) = \dot{F} \cap D_K(1, -gx)$$

https://doi.org/10.4153/CJM-1979-096-x Published online by Cambridge University Press

is equivalent to showing $\alpha \in D_K(1, -fx)$ if and only if $\alpha \in D_K(1, -gx)$ for all $\alpha \in D_F(1, -N(x))$. And this is equivalent to

(*) fx and gx are simultaneously in or out of $D_K(1, -\alpha)$ for all

$$\alpha \in D_F(1, -N(x)).$$

Suppose $fg \in R(F) \cdot \langle N(x) \rangle$. Then either $fg \in R(F)$ or $fg \in N(x) \cdot R(F)$ and in either case $D_F(1, -N(x)) \subseteq D_F(1, -fg)$. Thus $\alpha \in D_F(1, -fg)$ and $fg \in D_K(1, -\alpha)$ for all $\alpha \in D_F(1, -N(x))$. Hence (*) holds.

Conversely, now suppose (*) holds. We will be done if we can show $fg \in D_K(1, -\alpha)$ for all $\alpha \in D_F(1, -N(x))$. This is true since then $fg \in D_F(1, -\alpha)$ by Proposition 4.1, and so $\alpha \in D_F(1, -fg)$ would yield $D_F(1, -N(x)) \subseteq D_F(1, -fg)$. $fg \in R(F) \cdot \langle N(x) \rangle$ now follows from Lemma 1 of [**2**]. If fx, gx are both in $D_K(1, -\alpha)$, then clearly so is fg. Consider the case then where neither fx nor gx is in $D_K(1, -\alpha)$ for some $\alpha \in D_F(1, -N(x))$. Suppose $fg \notin D_K(1, -\alpha)$. Then $1, fx, gx, fg$ are the 4 coset representatives for $D_K(1, -\alpha)$ in $\dot{K}$. Choose $y \in \dot{K} - D_K(1, -\alpha)$ such that $N(y) \equiv fg \pmod{\dot{F}^2}$. This can always be done by multiplying some y satisfying $N(y) = fg$ by an appropriate element of $\dot{F}$. The Norm Principle implies $fgy \notin D_K(1, -\alpha)$, and so $1, y, fg, fgy$ are also representatives for the 4 cosets of $D_K(1, -\alpha)$. Therefore y must be in the same coset as either fx or gx. The Norm Principle then says $N(fxy)$ or $N(gxy) \in D_F(1, -\alpha)$. But $N(x) \in D_F(1, -\alpha)$ by assumption on α and the above now gives $N(y) \in D_F(1, -\alpha)$. This contradiction shows it was false to suppose $fg \notin D_K(1, -\alpha)$.

COROLLARY 4.10. *If* $|\dot{F}/R(F)| < \infty$ *and* $x \in \dot{K}$, *then there is an* $f \in \dot{F}$ *such that* $\dot{F} \cap D_K(1, -fx) = D_F(1, -N(x))$.

Proof. There exist $b_i \in \dot{F}$, $1 \leqq i \leqq n$, which form an independent set modulo $\dot{F}^2$, such that for $V = \langle b_1, \ldots, b_n \rangle \dot{F}^2$ the following hold: 1) $\dot{F}$ is generated by $R(F)$, $N(x)$, and V and 2) $\langle R(F), N(x) \rangle \dot{F}^2 \cap V = \dot{F}^2$. That is, $\{b_1, \ldots, b_n\}$ is a set of representatives for a basis of $\dot{F}/R(F)$ when $N(x) \in R(F)$ and $\{b_1, \ldots, b_n, N(x)\}$ suffices when $N(x) \notin R(F)$. Suppose there is no $f \in \dot{F}$ satisfying

$$\dot{F} \cap D_K(1, -fx) = D_F(1, -N(x)).$$

Then by Propositions 4.4 and 4.9, $\{\dot{F} \cap D_K(1, -fx) \pmod{\dot{F}^2} | f \in V\}$ is a set of 2^n subspaces of index 2 in $D_F(1, -N(x)) \bmod \dot{F}^2$. But there exist only $2^n - 1$ hyperplanes in any vector space of dimension n over $GF(2)$. This is a contradiction and so we must have a desired $f \in \dot{F}$.

PROPOSITION 4.11. *Let* $x \in \dot{K}$ *satisfy* $N(x) \notin R(F)$ *and* $\dot{F} \cap D_K(1, -x) = D_F(1, -N(x))$. *Then* $D_K(1, -N(x)) \subseteq D_K(1, -x)$.

Proof. By Proposition 4.9, $\dot{F} \cap D_K(1, -xN(x)) = D_F(1, -N(x))$. So from Corollary 4.5, $D_K(1, -xN(x))$ and $D_K(1, -x)$ both have index 2 in $\dot{K}$. Consesequently $D_K(1, -xN(x)) \cap D_K(1, -x)$ has index at most 4. But this inter-

https://doi.org/10.4153/CJM-1979-096-x Published online by Cambridge University Press

section is contained in $D_K(1, -N(x))$ which has index 4 by Proposition 4.3. Thus

$$D_K(1, -xN(x)) \cap D_K(1, -x) = D_K(1, -N(x))$$

and the result follows.

COROLLARY 4.12. *Suppose* $|\dot{F}/R(F)| < \infty$ *and* $x \in \dot{K}$. *If* $N(x) \in R(F)$, *then there is an* $f \in \dot{F}$ *so that* $fx \in R(K)$.

Proof. Corollary 4.10 says there exists an $f \in \dot{F}$ satisfying

$$\dot{F} \cap D_K(1, -fx) = D_F(1, -N(x));$$

i.e., $\dot{F} \subseteq D_K(1, -fx)$. We will show $fx \in R(K)$. If $y \in \dot{K}$ and $N(y) \in R(F)$, then as we have seen before (e.g. in the proof of 3.7), $y \in D_K(1, -fx)$. Consider then $N(y) \notin R(F)$. Again by 4.10, there is a $g \in \dot{F}$ with

$$\dot{F} \cap D_K(1, -gy) = D_F(1, -N(y)) = D_F(1, -N(gy)).$$

Proposition 4.11 yields $D_K(1, -N(y)) \subseteq D_K(1, -gy)$. If we can show $gy \in D_K(1, -fx)$, we will be done. Suppose $gy \notin D_K(1, -fx)$. Then $fx \notin D_K(1, -gy)$ and the above gives $fx \notin D_K(1, -N(y))$. So $N(y) \notin D_K(1, -fx)$. But this contradicts $\dot{F} \subseteq D_K(1, -fx)$.

From this corollary we can improve the statement in 4.8. For if $fx \in R(K)$, then $D_K(1, -x) = D_K(1, -f)$; and Proposition 4.3 now yields the next result.

COROLLARY 4.13. *If* $|\dot{F}/R(F)| < \infty$, $x \in \dot{K}$, *and* $N(x) \in R(F)$, *then* $D_K(1, -x)$ *has index* 1 *or* 4 *in* $\dot{K}$. *Moreover, its index is* 1 *if and only if* $\dot{F} \subseteq D_K(1, -x)$.

The proof of Theorem 3.10 now applies to the case where $a \in R(F)$. The only adjustment required is that the square class of a in F is lost when we move up to K. So when $q(F) < \infty$, $R(K)$ is only half the size it is when $a \notin R(K)$. We record these remarks and previous ones in the following theorem.

THEOREM 4.14. *Suppose* $m(F) = 2$, $q(F) < \infty$, *and* $K = F(\sqrt{a})$ *where* $a \in R(F) - \dot{F}^2$. *Then for* $x \in \dot{K}$, $N(x) \in R(F)$ *if and only if there is an* $f \in \dot{F}$ *so that* $fx \in R(K)$. *Moreover*, $|R(K)/\dot{K}| = \frac{1}{2}|R(F)/\dot{F}^2|^2$.

5. Remarks. The important statement in Theorems 3.10 and 4.14 is that $N(x) \in R(F)$ if and only if there is an $f \in \dot{F}$ satisfying $fx \in R(K)$. It only depends on $|\dot{F}/R(F)| < \infty$—as Proposition 3.9 and Corollary 4.12 show—and not on $q(F) < \infty$. Unfortunately the arguments used to prove these relied on the finiteness conditions, and we have been unable to avoid this requirement. The major problem in finding a possible counterexample is that there are so few fields known having a radical which has the property $\dot{F}^2 \subsetneq R(F) \subsetneq \dot{F}$.

Both real and non-real fields with "non-trivial" radical have been discovered (see [**1**], [**11**]), and further investigation is merited. The real significance of $R(F)$ is yet to be found. When $m(F) = 2$, it has been shown what role $R(F)$

https://doi.org/10.4153/CJM-1979-096-x Published online by Cambridge University Press

plays; and in fact, it was the missing link that supplied the complete answer to the quadratic form structure. This paper has shown that there is quite a difference for quadratic extensions, $F(\sqrt{a})$, depending on whether $a \in R(F)$. And even though $m(K) \leqq 4$ when $m(F) = 2$, the case $m(K) = 4$ is still not fully understood.

References

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

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

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

4. R. Elman and T. Y. Lam, *Quadratic forms under algebraic extensions*, Math. Ann. *219* (1976), 21–42.

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

6. I. Kaplansky, *Frohlich's local quadratic forms*, J. Reine Angew, Math. *239* (1969), 74–77.

7. T. Y. Lam, *The algebraic theory of quadratic forms* (W. A. Benjamin, Reading, Massachusetts, 1973).

8. A. Pfister, *Multaplikative quadratische Formen*, Arch. Math. *16* (1965), 363–370.

9. W. Scharlau, *Quadratic forms*, Queen's papers on pure and applied mathematics No. *22* (Kingston, Ontario, 1969).

10. L. Szczepanik, *Quaternion algebras and binary quadratic forms*, Univ. Ślaski W. Katowicach Prace Naukowe No. *87* Prace Mat. No. *6* (1975), 17–27.

11. K. Szymiczek, *Quadratic forms over fields with finite square class number*, Acta. Arith. *28* (1975), 195–221.

Louisiana State University,
Baton Rouge, Louisiana

https://doi.org/10.4153/CJM-1979-096-x Published online by Cambridge University Press