Canad. J. Math. Vol. **52** (4), 2000 pp. 833–848

W-Groups under Quadratic Extensions of Fields

Dedicated to Paulo Ribenboim on his Seventieth Birthday

Ján Mináč and Tara L. Smith

Abstract. To each field F of characteristic not 2, one can associate a certain Galois group $\mathcal{G}_F$, the so-called W-group of F, which carries essentially the same information as the Witt ring $W(F)$ of F. In this paper we investigate the connection between $\mathcal{G}_F$ and $\mathcal{G}_{F(\sqrt{a})}$, where $F(\sqrt{a})$ is a proper quadratic extension of F. We obtain a precise description in the case when F is a pythagorean formally real field and $a = -1$, and show that the W-group of a proper field extension K/F is a subgroup of the W-group of F if and only if F is a formally real pythagorean field and $K = F(\sqrt{-1})$. This theorem can be viewed as an analogue of the classical Artin-Schreier's theorem describing fields fixed by finite subgroups of absolute Galois groups. We also obtain precise results in the case when a is a double-rigid element in F. Some of these results carry over to the general setting.

1 Introduction

Throughout the entire paper, we assume that the characteristic of all considered fields is not 2. To each field F, one can associate a certain Galois group $\mathcal{G}_F$, the W-group of F, which carries essentially the same information as the Witt ring $W(F)$ of F. To be precise, the following is true.

Theorem *Let F and L be fields. Then $W(F) \cong W(L)$ implies $\mathcal{G}_F \cong \mathcal{G}_L$. The converse is also true under the further assumption that $s(F) = s(L)$ whenever $\langle 1, 1\rangle_F$ is universal.*

(See [MiSp3, Theorem 3.8]. We denote $s(F)$ to mean the level of F. It is the smallest positive integer n such that -1 can be written as a sum of n squares. If no such expression exists, we say that $s(F) = \infty$.)

The W-groups $\mathcal{G}_F$ and their properties have been studied in [AKM], [MiSp2], [MiSp3], [MiSm1], [MiSm2]. In this article we examine the connections between $\mathcal{G}_F$ and $\mathcal{G}_{F(\sqrt{a})}$ for $a \in \dot{F} - \dot{F}^2$. This is an important open problem as in general any classification of possible $W\big(F(\sqrt{a})\big)$ for given $W(F)$ is not known. In the case of algebraic number fields, some interesting results have been obtained; see, for example, [PSCL] and the references contained therein. For the basic theory of quadratic forms and quaternion algebras, we refer the reader to [L1] and [Sc]. For the basic theory of profinite groups and Galois cohomology, see [Ser]. For the basic notions on Pontrjagin duality, see [Mor]. In addition to the connection with quadratic form theory, our other motivation is the investigation of the

Received by the editors February 15, 1999; revised December 11, 1999.
The first author was supported by the Natural Sciences and Engineering Research Council of Canada and the special Dean of Science fund at UWO.
AMS subject classification: 11E81, 12D15.

cohomology rings of W-groups. In particular, Theorem 3.2 below is used in [AKM, Theorems 5.12 and 5.13]. In this paper we concentrate on the Galois-theoretic aspects of the problems outlined above.

The W-group $\mathcal{G}_F$ of a field F is the Galois group over F of the field $F^{(3)}$, which is the compositum over F of all extensions which are cyclic of order 2, cyclic of order 4, and dihedral of order 8. The field $F^{(3)}$ can also be constructed as follows: Let $F^{(2)}$ denote the compositum over F of all quadratic extensions of F. Then $F^{(3)}$ is the compositum over $F^{(2)}$ of all quadratic extensions of $F^{(2)}$ which are Galois over F.

These groups all lie in the category $\mathcal{C}at$, whose objects are those pro-2-groups G satisfying $g^4 = 1$ and $g^2 \in Z(G)$ for all $g \in G$. The Frattini subgroup of such a group G, denoted $\Phi(G)$, is (topologically) generated by squares [MiSm2, Proposition 1.3]. For G in $\mathcal{C}at$, $\Phi(G) = [G, G]G^2 = G^2$. Let G be a group in $\mathcal{C}at$. Given a set of elements $g_i \in G$, i in some index set I, we write $\langle g_i \mid i \in I\rangle$ for the subgroup of G topologically generated by the set $\{g_i \mid i \in I\}$, that is, the closed subgroup of G generated by the set of elements g_i. From now on we shall always assume that all our subgroups are closed subgroups of our pro-2-groups.

We will need to understand precisely how the relations on $W(F)$ determine $\mathcal{G}_F$ and conversely. This is explained in detail in [MiSm1], [MiSm2], [MiSp3], but we give a brief description below.

Let $G = \dot{F}/\dot{F}^2$ be the group of square classes of F. Then G has a natural structure as a vector space over the field $\mathbb{Z}/2\mathbb{Z}$, and we can choose a basis $B = \{b_i : i \in I\}$ for G as a $\mathbb{Z}/2\mathbb{Z}$-vector space, where I is some linearly ordered index set. Let Q be the subgroup of the Brauer group $\mathrm{Br}(F)$ of F generated by the classes of quaternion algebras over F. (See [L1, Chapter III], or [Ma, Chapter 2].) Let $\mathcal{F}$ be the free group in the category $\mathcal{C}at$ on the symbols $\{z_i : i \in I\}$. Then $\Phi(\mathcal{F})$, the Frattini subgroup of $\mathcal{F}$, is generated by $\langle z_i^2, [z_i, z_j] : i, j \in I, j > i\rangle$. It is a topological product of copies of $\mathbb{Z}/2\mathbb{Z}$ on the generators described above. Let P be the set of homogeneous polynomials of degree 2 in the variables t_i, $i \in I$, with coefficients in $\mathbb{Z}/2\mathbb{Z}$. Thus P is a $\mathbb{Z}/2\mathbb{Z}$-vector space. There is a natural pairing $\langle\ ,\ \rangle : \Phi(\mathcal{F}) \times P \to \mathbb{Z}/2\mathbb{Z}$, obtained by letting $\{z_i^2, [z_i, z_j] : i, j \in I,\ j > i\}$ and $\{t_i^2, t_i t_j; i, j \in I,\ j > i\}$ be dual bases. We have a group homomorphism $\theta\colon P \to Q$ given by $\theta(t_i^2) = (b_i, b_i)$, $\theta(t_i t_j) = (b_i, b_j)$. Let $\mathcal{R} = (\ker\theta)^{\perp} = \{s \in \Phi(\mathcal{F}) : \langle s, p\rangle = 0\ \forall p \in \ker\theta\}$. Then $\mathcal{R}$ can be viewed as the dual Q^* of Q. It can then be shown that the W-group $\mathcal{G}_F$ and the group $\mathcal{F}/\mathcal{R}$ are isomorphic pro-2-groups. (For any abelian topological group T, we denote as T^* its Pontrjagin dual.)

We now consider what happens when we take a proper quadratic extension $K = F(\sqrt{a})$ of the field F. Letting $H = \mathrm{Gal}(F^{(3)}/K)$, we see that H sits as a subgroup of index 2 in $\mathcal{G}_F$, and is a quotient of $\mathcal{G}_K$ (see Lemma 2.1). Thus it is natural to ask just how H sits in $\mathcal{G}_F$, and how $\mathcal{G}_K$ projects onto H. In other words, we want to understand the short exact sequences

$$1 \to H \to \mathcal{G}_F \to \mathrm{Gal}(K/F) \to 1$$

and

$$1 \to \mathrm{Gal}(K^{(3)}/F^{(3)}) \to \mathcal{G}_K \to H \to 1.$$

In particular, when are these sequences split? Just what can be said in each case?

To assist us in analyzing what is happening, we recall the Square-Class Exact Sequence for quadratic extensions [L1, Theorem 3.4]:

Theorem **(Square-Class Exact Sequence)** *Let $K = F(\sqrt{a})$ be a quadratic extension of the field F. Let $\epsilon\colon \dot{F}/\dot{F}^2 \to \dot{K}/\dot{K}^2$ be the map induced by the inclusion of F in K, and let $N\colon \dot{K}/\dot{K}^2 \to \dot{F}/\dot{F}^2$ be the homomorphism induced by the norm from K to F. Then the following sequence is exact:*

$$1 \longrightarrow \{\dot{F}^2, a\dot{F}^2\} \longrightarrow \dot{F}/\dot{F}^2 \xrightarrow{\epsilon} \dot{K}/\dot{K}^2 \xrightarrow{N} \dot{F}/\dot{F}^2.$$

2 The General Case

We now consider what can be said in general regarding the relationship between the W-group of a field F and the W-group of some quadratic extension of F. If K is any field extension of F we see immediately that $F^{(2)} \subseteq K^{(2)}$. But also we have the following.

Lemma 2.1 *Let K/F be any field extension. Then $F^{(3)} \subseteq K^{(3)}$. In particular, if $K = F(\sqrt{a})$ is a quadratic extension of F, then $F^{(3)} \subseteq K^{(3)}$.*

Proof Because $F^{(3)}$ is the compositum of all quadratic, cyclic of order 4, and dihedral of order 8 extensions L of F, it is enough to show that for each such L we have that the compositum KL is itself a compositum of quadratic, cyclic of order 4 and dihedral of order 8 extensions over K. But it is well known that for any field extension K/F, if L/F is a finite Galois extension and $H = \mathrm{Gal}(L/F)$, then the compositum KL/K is a finite Galois extension and $\mathrm{Gal}(KL/K)$ is a subgroup of H (see [Art, pp. 67–68]). This gives the desired result. ∎

Lemma 2.2 *Let $K = F(\sqrt{a})$ be any proper quadratic extension of F. Then $K^{(2)} \subseteq F^{(3)}$.*

Proof Since $K^{(2)}$ is the compositum of all quadratic extensions of K it is enough to show that each quadratic extension $K(\sqrt{k})$ is contained in $F^{(3)}$. However the Galois closure of $K(\sqrt{k})$ over F is of the form $F(\sqrt{a}, \sqrt{b}, \sqrt{k})$ for some $b \in \dot{F}$ (see the proof of Cor. 2.19 in [MiSp3]), so $K(\sqrt{k}) \subseteq F(\sqrt{a}, \sqrt{b}, \sqrt{k}) \subseteq F^{(3)}$. ∎

These two lemmas combined show that we have the tower of fields

$$F \subseteq K \subseteq F^{(2)} \subseteq K^{(2)} \subseteq F^{(3)} \subseteq K^{(3)}.$$

Corollary 2.3 *Let $K = F(\sqrt{a})$ be any proper quadratic extension of F. Then we have the short exact sequence*

$$1 \to \mathrm{Gal}(K^{(3)}/F^{(3)}) \to \mathcal{G}_K \to \mathrm{Gal}(F^{(3)}/K) \to 1.$$

Moreover, $\mathrm{Gal}(K^{(3)}/F^{(3)})$ is elementary 2-abelian (possibly infinite), and the extension given by the short exact sequence is central. Finally, $\mathrm{Gal}(F^{(3)}/K)$ is a subgroup of index 2 in $\mathcal{G}_F$.

Proof The short exact sequence follows immediately from our tower of field extensions and Galois theory. That $\mathrm{Gal}(K^{(3)}/F^{(3)})$ is elementary 2-abelian follows from the fact that it is a subgroup of $\mathrm{Gal}(K^{(3)}/K^{(2)})$, which has exponent at most 2. Since also $\mathrm{Gal}(K^{(3)}/K^{(2)}) \subseteq$

$Z(\mathcal{G}_K)$ this shows that the extension is central. From Pontrjagin duality theory between compact and discrete groups it follows that $\mathrm{Gal}(K^{(3)}/F^{(3)}) = \prod_J(\mathbb{Z}/2\mathbb{Z})$ for some index set J. (See, *e.g.* [Ko, p. 39].) The fact that $\mathrm{Gal}(F^{(3)}/K)$ is of index 2 in $\mathcal{G}_F$ follows from the fact that $K = F(\sqrt{a})$ is a proper quadratic extension of F. ■

Assume now that $K = F(\sqrt{a})$ as above and let $\mathcal{B} = \{[a], [a_i] \mid i \in I\}$ be a basis for $\dot{F}/\dot{F}^2$ and $\{\sigma, \sigma_i \mid i \in I\}$ be a minimal set of generators for $\mathcal{G}_F$ which is dual to $\mathcal{B}$. (That is, σ fixes $\sqrt{a_i}$ for all $i \in I$, $\sigma(\sqrt{a}) = -\sqrt{a}$, σ_i fixes $\sqrt{a}$ for all $i \in I$, and $\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$ for all $i, j \in I$.) Let B be the smallest closed subgroup of $\mathcal{G}_F$ containing the set $\{\sigma_i \mid i \in I\}$. Recall that in Section 1 we asked under what circumstances does the exact sequence

$$1 \to H \to \mathcal{G}_F \to \mathbb{Z}/2\mathbb{Z} \to 1$$

split. The answer turns out to be quite simple.

Proposition 2.4 *Let $H = \mathrm{Gal}\big(F^{(3)}/F(\sqrt{a})\big)$. Then $\mathcal{G}_F \cong H \rtimes \mathbb{Z}/2\mathbb{Z}$ (i.e., the short exact sequence above is split) if and only if F is formally real and a is not a sum of squares in F.*

Proof Keeping the notation as above, we have that $\mathcal{G}_F/H$ is generated by the image of σ, so that the given sequence is split if and only if we can find such a σ with $\sigma^2 = 1$. But this can happen if and only if F is formally real (so that there exist an involution in $\mathcal{G}_F$), and a is such that $\sqrt{a}$ is not fixed by some involution $\sigma \in \mathcal{G}_F$ which does not belong to $\Phi(\mathcal{G}_F)$. (See [MiSp2, Theorem 2.7 and Corollary 2.10].) But this in turn happens if and only if there is some ordering $P = P_\sigma$ such that $a \notin P$. This can be found if and only if a is not a sum of squares in F. (See [L2, Theorem 1.6].) ■

Suppose still that $K = F(\sqrt{a})$ and that $\mathcal{B} = \{[a], [a_i] \mid i \in I\}$ is a basis for $\dot{F}/\dot{F}^2$, and again let $\{\sigma, \sigma_i \mid i \in I\}$ be a minimal set of generators for $\mathcal{G}_F$ which is dual to $\mathcal{B}$. Let B be the smallest closed subgroup of $\mathcal{G}_F$ containing the set $\{\sigma_i \mid i \in I\}$. Then $B \subseteq H := \mathrm{Gal}(F^{(3)}/K)$. Clearly H is generated by B and all commutators $[\sigma, \sigma_i]$ and σ^2, that is, $H = B\Phi(\mathcal{G}_F)$. Then $\Phi(B) = B \cap \Phi(\mathcal{G}_F)$ and B is the essential subgroup of $\mathcal{G}_F$ associated with H. (In general, a subgroup U of $\mathcal{G}_F$ is called an *essential* subgroup of $\mathcal{G}_F$ iff $\Phi(\mathcal{G}_F) \cap U = \Phi(U)$.) Then, as in [CSm1], we see that $H \cong B \times \prod_J(\mathbb{Z}/2\mathbb{Z})$ where $\Phi(\mathcal{G}_F) = \Phi(B) \times \prod_J(\mathbb{Z}/2\mathbb{Z})$. Thus we have shown the following.

Proposition 2.5 *Let K/F be any proper quadratic extension of fields, and let B be the essential subgroup of* $\mathrm{Gal}(F^{(3)}/K)$ *described above. Then there exists an index set J such that $H = B \times \prod_J(\mathbb{Z}/2\mathbb{Z})$.*

We can further determine $|J|$ as follows. Let $D\langle 1, -a\rangle$ denote the set of all non-zero values assumed by the quadratic form $x^2 - ay^2$ over F. Let $\mathcal{A}$ be any $\mathbb{Z}/2\mathbb{Z}$-basis for $D\langle 1, -a\rangle/\dot{F}^2$.

Proposition 2.6 $|J| = |\mathcal{A}|$.

Proof Once again we apply the Square-Class Exact Sequence to our particular quadratic extension. Then $\dot{K}/\dot{K}^2 \cong \frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2, a\dot{F}^2\}} \oplus N(\dot{K})/\dot{F}^2$. On the other hand from Kummer theory

https://doi.org/10.4153/CJM-2000-036-0 Published online by Cambridge University Press

we know that $\dot{K}/\dot{K}^2$ is dual to $\mathcal{G}_K/\big(\Phi(\mathcal{G}_K)\big)$. We already observed that $\mathrm{Gal}(K^{(3)}/F^{(3)}) \subseteq \Phi(\mathcal{G}_K)$. Hence

$$\text{(A)}\qquad \begin{aligned} \frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2, a\dot{F}^2\}} \oplus N(\dot{K})/\dot{F}^2 \cong \dot{K}/\dot{K}^2 &\cong \big(\mathcal{G}_K/\Phi(\mathcal{G}_K)\big)^* \cong \big(H/\Phi(H)\big)^* \\ &= \big(B/\Phi(B)\big)^* \oplus \Big(\bigoplus_J \mathbb{Z}/2\mathbb{Z}\Big). \end{aligned}$$

This decomposes into two isomorphisms: $\frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2,a\dot{F}^2\}} \cong \big(B/\Phi(B)\big)^*$ and $D\langle 1,-a\rangle/\dot{F}^2 \cong N(\dot{K})/\dot{F}^2 \cong \bigoplus_J \mathbb{Z}/2\mathbb{Z}$.

For the reader's convenience we shall justify the statements above with more details. We have

$$\begin{aligned} \frac{\mathcal{G}_K}{\Phi(\mathcal{G}_K)} &\cong \frac{\frac{\mathcal{G}_K}{\mathrm{Gal}(K^{(3)}/F^{(3)})}}{\frac{\Phi(\mathcal{G}_K)}{\mathrm{Gal}(K^{(3)}/F^{(3)})}} \\ &\cong \frac{H}{\mathrm{Gal}(\frac{F^{(3)}}{K^{(2)}})} \\ &\cong \frac{H}{\Phi(H)}. \end{aligned}$$

We indeed have $\mathrm{Gal}(F^{(3)}/K^{(2)}) \cong \Phi(H)$ because $K^{(2)}$ is the maximal multiquadratic subextension of $F^{(3)}/K$. Hence $\frac{\mathcal{G}_K}{\Phi(\mathcal{G}_K)} \cong \frac{H}{\Phi(H)}$. All other isomorphisms in (A) follow immediately from the discussion preceeding Proposition 2.5. The isomorphism $\frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2,a\dot{F}^2\}} \cong (\frac{B}{\Phi(B)})^*$ follows from the Kummer theory applied to the subgroup $\dot{K}^2\dot{F}$ of $\dot{K}$ and its corresponding multiquadratic extension of $\dot{K}$. (See [AT, p. 21, Theorem 3].)

Now we shall prove the key isomorphism $\frac{N(\dot{K})}{\dot{F}^2} \cong (T)^* \cong \bigoplus_J \frac{\mathbb{Z}}{2\mathbb{Z}}$ where $T \cong \prod_J \frac{\mathbb{Z}}{2\mathbb{Z}}$ is the right factor in the decomposition $H = B \times \prod_J (\mathbb{Z}/2\mathbb{Z})$. (We assume that this decomposition is fixed.)

Let us think about $\frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2,a\dot{F}^2\}} \oplus \frac{N(\dot{K})}{\dot{F}^2}$ as the Pontrjagin dual of $\frac{H}{\Phi(H)}$. Observe that by Kummer theory $\frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2,a\dot{F}^2\}}$ can be considered as a subspace of $(\frac{H}{\Phi(H)})^*$ in a natural way, but an embedding of $\frac{N(\dot{K})}{\dot{F}^2}$ into $(\frac{H}{\Phi(H)})^*$ depends on the choice of representatives of the cosets of $\dot{K}/\dot{F}\dot{K}^2 \cong \frac{N(\dot{K})}{\dot{F}^2}$. We assume that we have some fixed set of representatives of the cosets of $\dot{K}/\dot{F}\dot{K}^2$. Because $T \subset \Phi(\mathcal{G}_F)$ we see that when we consider $\frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2,a\dot{F}^2\}}$ as a group of continuous functions $\frac{H}{\Phi(H)} \to \{\pm 1\}$, then $\frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2,a\dot{F}^2\}}$ restricted to T consists of just the trivial function which sends all of T to 1. Consider restrictions of $\frac{N(\dot{K})}{\dot{F}^2} \subset (\frac{H}{\Phi(H)})^*$ to T. In this way we obtain a homomorphism $\phi\colon \frac{N(K)}{\dot{F}} \to T^*$. We claim that ϕ is the promised isomorphism. First we shall show that ϕ is surjective. Let s be any element of $T^* \subset (\frac{H}{\Phi(H)})^*$. Then there exist elements $[f] \in \frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2,a\dot{f}^2\}}$ and $[k] \in \frac{N(\dot{K})}{\dot{F}^2}$ such that $s = [f] + [k] \in \frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2,a\dot{F}^2\}} \oplus \frac{N(\dot{K})}{\dot{F}^2}$. However $[f]$ is trivial on T. Hence $\phi(k) = s$.

Now we shall show that ϕ is injective. Suppose that $[k] \in \frac{N(\dot{K})}{\dot{F}^2}$ such that $\phi(k) = 1$. Then we can find an element $[f] \in \frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2, a\dot{F}^2\}}$ such that the map $\frac{H}{\Phi(H)} \to \{\pm 1\}$ associated with $[k]$ restricted to $\frac{B}{\Phi(B)}$ coincides with the map $\frac{B}{\Phi(B)} \to \{\pm 1\}$ associated with $[f]$. Then $s = [f] + [k] \in \frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2, a\dot{F}^2\}} \oplus \frac{N(K)}{\dot{F}^2}$ is the trivial map $\frac{H}{\Phi(H)} \to \{1\}$. Hence we see that both $[k]$ and $[h]$ are unit elements in $\frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2, a\dot{F}^2\}}$ and $\frac{N(K)}{\dot{F}^2}$ respectively and ϕ is injective.

Therefore we proved that $\frac{N(\dot{K})}{\dot{F}^2}$ is the Pontrjagin dual to $T = \prod_J \mathbb{Z}/2\mathbb{Z}$. Thus we see that

$$\frac{N(\dot{K})}{\dot{F}^2} \cong \frac{D\langle 1, -a\rangle}{\dot{F}^2} \cong \bigoplus_J \mathbb{Z}/2\mathbb{Z} = \Big(\prod_J \mathbb{Z}/2\mathbb{Z}\Big)^*.$$

Hence indeed $|\mathcal{A}| = |J|$ as claimed. ■

Note that $\operatorname{im}(N)$ is the subgroup of $\dot{F}/\dot{F}^2$ consisting of elements represented by the form $\langle 1, -a\rangle$. In particular, if $a = -1$ and F is pythagorean, then ϵ is surjective. In this case, $F^{(2)} = K^{(2)}$. Also, if $-a$ is rigid, then a minimal set of generators for $\mathcal{G}_K$ has the same cardinality as a minimal set of generators for $\mathcal{G}_F$.

3 Adjoining $\sqrt{-1}$ to a Real Pythagorean Field

Recall that a formally real field F is *Euclidean* if $|\dot{F}/\dot{F}^2| = 2$. Such a field has a unique ordering in which $\dot{F}^2$ consists of the positive elements and $-\dot{F}^2$ consists of the negative elements. Aside from real closed fields, the most natural example of a Euclidean field is the field of all constructible real numbers. (See [L3, p. 89].)

Recall also that for any field, F_q denotes the quadratic closure of F, *i.e.*, the smallest quadratically closed field containing F (hence $\dot{F}_q = \dot{F}_q^2$). The most basic example is $\mathbb{Q}_q$ which is the field of all constructible numbers.

In analogue with the classical results of Artin-Schreier, Becker proved the following.

Theorem 3.1 **(Becker)** *Let F be a formally real field and E/F be an algebraic extension. Then the following are equivalent.*

(1) E is Euclidean and $E \subset F_q$.
(2) E is a subfield in F_q of finite codimension $\neq 1$.

One can also think about $F^{(3)}$ as an analogue of the quadratic closure F_q despite the fact that in general we do not have $(F^{(3)})^{(3)} = F^{(3)}$. We are able to characterize all field extensions K/F such that $F^{(3)} = K^{(3)}$. We show that the only case when $F^{(3)} = K^{(3)}$ and $F \neq K$ occurs when $K = F(\sqrt{-1})$, and F is a formally real pythagorean field. (See

Theorems 3.2 and 3.6 below.) This statement can be thought of as an analogue of classical results of Artin-Schreier and Becker.

Recall that the following conditions are equivalent: (See [MiSp2, Theorem 2.1].)

(1) F is pythagorean.
(2) $\mathcal{G}_F$ is generated by involutions.
(3) $\Phi(\mathcal{G}_F) = [\mathcal{G}_F, \mathcal{G}_F]$.

We have the following result.

Theorem 3.2 *Let F be any pythagorean field. Then* $F^{(3)} = F(\sqrt{-1})^{(3)}$.

Proof Let F be any pythagorean field. As noted at the end of Section 2, from using the Square-Class Exact Sequence we see that the map N is trivial and the map ϵ is surjective, so $F^{(2)} = F(\sqrt{-1})^{(2)}$. We set $F_1 := F$ and $F_2 := F(\sqrt{-1})$. We have $\dot{F}_1/\dot{F}_1^2 \cong \dot{F}_2/\dot{F}_2^2 \cup -\dot{F}_2/\dot{F}_2^2$. We then have the exact sequences

$$1 \longrightarrow V_i \longrightarrow S_i \longrightarrow \mathcal{G}_{F_i} \longrightarrow 1$$

where S_i is the free group in $\mathcal{C}at$ on $\dim_{\mathbb{F}_2}(\dot{F}_i/\dot{F}_i^2)$ generators, $i = 1, 2$.

From [MiSp3, Corollary 2.21] we know that V_i and $\operatorname{Quat}(F_i)$ are dual to each other. (Recall that the groups V_i are compact topological groups and the groups $\operatorname{Quat}(F_i)$ are discrete groups generated by the classes of quaternion algebras sitting inside of the Brauer groups $\operatorname{Br}(F_i)$ of F_i, $i = 1, 2$.) Let $\operatorname{Br}_2(F_i)$ denote the subgroup of $\operatorname{Br}(F_i)$ consisting of elements of order at most 2. Then we know $\operatorname{Br}_2(F_i) = \operatorname{Quat} F_i$ [Me]. Furthermore, by Merkurjev [Me] we have the exact sequence of groups

$$\dot{F}/\dot{F}^2 \xrightarrow{\alpha} \operatorname{Br}_2(F) \xrightarrow{\tau} \operatorname{Br}_2\big(F(\sqrt{-1})\big) \xrightarrow{\delta} \operatorname{Br}_2(F)$$

where δ is the corestriction map, τ is induced by the inclusion $F \hookrightarrow F(\sqrt{-1})$, and $\alpha([f]) = [(\frac{-1,f}{F})]$ for each $[f] \in \dot{F}/\dot{F}^2$. Because F is a pythagorean field, α is injective and δ is the trivial map. Namely, the injectivity of α is equivalent to the fact that each sum of two squares is a square. The surjectivity of τ can be seen as follows: From Merkurjev's theorem on the second cohomology of absolute Galois groups with $\mathbb{Z}/2\mathbb{Z}$-coefficients and [Wd, Lemma 1.7] as well as the projection formula [Wd, 1.4] we see that the corestriction map is determined by its restrictions on the classes of quaternion algebras defined over $F(\sqrt{-1})$ with one 'slot' in F. Applying the projection formula and using the fact that the image of the norm map is the squares in F, we obtain the desired result. Hence $\operatorname{Br}_2(F) \cong \dot{F}/\dot{F}^2 \oplus \operatorname{Br}_2\big(F(\sqrt{-1})\big)$. On the other hand, since $F(\sqrt{-1})^{(3)} \supseteq F^{(3)}$, we see that we have the following commutative diagram:

$$\begin{array}{ccccccccc}
 & & & & & & 1 & & \\
 & & & & & & \downarrow & & \\
 & & 1 & & 1 & & \mathrm{Gal}(F_2^{(3)}/F_1^{(3)}) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & V_2 & \longrightarrow & S_2 & \longrightarrow & \mathcal{G}_{F_2} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & V_1 & \longrightarrow & S_1 & \longrightarrow & \mathcal{G}_{F_1} & \longrightarrow & 1 \\
 & & & & & & \downarrow & & \\
 & & & & & & \mathrm{Gal}(F_2/F_1) & & \\
 & & & & & & \downarrow & & \\
 & & & & & & 1 & &
\end{array} .$$

Our goal is to show that $F_2^{(3)} = F_1^{(3)}$, which is equivalent to showing that the map $\mathcal{G}_{F_2} \to \mathcal{G}_{F_1}$ is injective. From the commutative diagram above we see that it is enough to show that $V_2 = V_1 \cap S_2$. Dualizing our isomorphism $\mathrm{Br}_2(F_1) \cong \dot{F}_1/\dot{F}_1^2 \oplus \mathrm{Br}_2(F_2)$ we obtain $V_1 \cong (\dot{F}_1/\dot{F}_1^2)^* \times V_2$. We shall consider this isomorphism from a slightly different point of view. Choose a basis $\{[-1]\} \cup \{[a_i] \mid i \in I_2\}$ of $\dot{F}_1/\dot{F}_1^2$ such that $\{[a_i] \mid i \in I_2\}$ is also a basis for $\dot{F}_2/\dot{F}_2^2$. Then we have the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Q_1 & \xrightarrow{i_1} & H^2(G_{F_1}^{[2]}) & \xrightarrow{\mathrm{infl}_1} & \mathrm{Br}_2(F_1) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\
0 & \longrightarrow & Q_2 & \xrightarrow{i_2} & H^2(G_{F_2}^{[2]}) & \xrightarrow{\mathrm{infl}_2} & \mathrm{Br}_2(F_2) & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array} .$$

(We employ the same notation for the kernels of inflations as in [MiSp3, Theorem 2.20].) We can identify $H^1(G_{F_i}^{[2]})$ with $\dot{F}_i/\dot{F}_i^2$, $i = 1, 2$. Then β is defined via $[-1] \mapsto 0$ and $[a_i] \mapsto [a_i]$. In other words, it is the restriction map. Then α and γ are induced via β. We see that α is well-defined, that is $\alpha(Q_1) \subseteq Q_2$, because γ is well-defined: it is again the restriction map. We claim that in fact $\alpha(Q_1) = Q_2$. Indeed, suppose $q_2 \in Q_2$. Let $s \in H^2(G_{F_1}^{[2]})$ such that $\beta(s) = i_2(q_2)$. Then $\gamma\big(\mathrm{infl}_1(s)\big) = 0$; therefore $\mathrm{infl}_1(s) = [(\frac{-1, f}{F_1})]$ for some $f \in \dot{F}_1$. Hence $s = [-1](\sum_{j \in J}[a_j]) + q_1$, where $[f] = \prod_{j \in J}[a_j]$ and q_1 is a suitable element of Q_1. Thus $\beta(s) = \beta(q_1) = i_2(q_2)$, and $\alpha(q_1) = q_2$ as desired.

Using the condition $\alpha(Q_1) = Q_2$ and the pairings $\Phi(S_i) \times H^2(G_{F_i}^{[2]}) \to \mathbb{Z}/2\mathbb{Z}$ described in [MiSp3] (see also Section 1), we see (where $V_i = \mathrm{Ann}\, Q_i$ is the annihilator of Q_i with respect to the pairings above) that $V_1 \cap S_2 = V_2$. Our proof is now complete. ■

Remark 3.3 A further explanation of the equality $V_1 \cap S_2 = V_2$ is as follows: Suppose that $r \in V_1 \cap S_2 = V_1 \cap \Phi(S_2)$. Then $\langle r, q_1\rangle_1 = 0$ for all $q_1 \in Q_1$. Let $q_2 \in Q_2$. Then there exists $q_1 \in Q_1$ such that $\alpha(q_1) = q_2$. We have $\langle r, q_2\rangle_2 = \langle r, q_1\rangle_1 = 0$. Hence $r \in V_2$.

Remark 3.4 One can also obtain the results above from the approach taken in [CSm1], [CSm2]. (In [CSm2], subgroups of W-groups and their relationships with homomorphic images of Witt rings are investigated.)

Corollary 3.5 *Let F be a formally real pythagorean field. Then $\mathcal{G}_F \cong \mathcal{G}_{F(\sqrt{-1})} \rtimes \langle\sigma_{-1}\rangle$, where σ_{-1} is an involution and the action of σ_{-1} on $\mathcal{G}_{F(\sqrt{-1})}$ is given by $\sigma_{-1}\tau_i\sigma_{-1} = \tau_i^{-1}$ for a suitable generating set $\{\tau_i \mid i \in I\}$ of $\mathcal{G}_{F(\sqrt{-1})}$.*

Proof Since $F^{(3)} = F(\sqrt{-1})^{(3)}$, we see that $\mathcal{G}_{F(\sqrt{-1})}$ is a subgroup of index 2 in $\mathcal{G}_F$. The fact that $\mathcal{G}_F \cong \mathcal{G}_{F(\sqrt{-1})} \rtimes \langle\sigma_{-1}\rangle$, where σ_{-1} is an involution, follows from the short exact sequence

$$1 \to \mathcal{G}_{F(\sqrt{-1})} \to \mathcal{G}_F \xrightarrow{\pi} \mathrm{Gal}\left(\frac{F(\sqrt{-1})}{F}\right) \to 1$$

and the fact that for any involution $\sigma_{-1} \in \mathcal{G}_F - \Phi(\mathcal{G}_F)$, π restricted to $\{1, \sigma_{-1}\}$ is an isomorphism. The existence of such σ_{-1} follows from [MiSp2, Theorem 2.7 and Corollary 2.10]. (Alternatively, one can apply Proposition 2.4 above.)

Finally we shall show that we can choose a suitable generating set $\{\tau_i \mid i \in I\}$ of $\mathcal{G}_{F(\sqrt{-1})}$ such that $\sigma_{-1}\tau_i\sigma_{-1} = \tau_i^{-1}$ for each $i \in I$.

Because $\mathcal{G}_F$ is generated by involutions $\sigma \in \mathcal{G}_F - \Phi(\mathcal{G}_F)$ and since for each such involution σ we have $\sigma(\sqrt{-1}) = -\sqrt{-1}$ we see that $\mathcal{G}_{F(\sqrt{-1})}$ is generated by products of an even number of involutions $\sigma \in \mathcal{G}_F - \Phi(\mathcal{G}_F)$. Since we can rewrite any product $\sigma_1\sigma_2$ as $(\sigma_1\sigma_{-1})(\sigma_{-1}\sigma_2)$ we see that $\tau_i = \sigma_i\sigma_{-1}$, $\sigma_i \in \mathcal{G}_F - \Phi(\mathcal{G}_F)$, generate $\mathcal{G}_{F(\sqrt{-1})}$ as a topological group. Because $\sigma_{-1}\tau_i\sigma_{-1} = \tau_i^{-1}$ for each τ_i as above we see that the set $\{\tau_i \mid i \in I\}$ is the desired generating set of $\mathcal{G}_{F(\sqrt{-1})}$. ∎

Now we shall prove the converse of Theorem 3.2.

Theorem 3.6 *Let K/F be any proper extension of fields such that $F^{(3)} = K^{(3)}$. Then F is pythagorean and $K = F(\sqrt{-1})$.*

Proof Let K/F be a proper field extension such that $F^{(3)} = K^{(3)}$. Then $K \subseteq F^{(3)}$. We begin by showing the existence of a subfield L of K of index 2. If $K \subseteq F^{(2)}$, choose $1 \neq \sigma \in \mathrm{Gal}(K/F)$ and let L be the fixed field of σ. Otherwise, let $KF^{(2)}$ denote the compositum of K and $F^{(2)}$ inside $F^{(3)}$. Choose $1 \neq \sigma \in \mathrm{Gal}(KF^{(2)}/F^{(2)})$. Consider $\bar\sigma = \sigma|_K$. The fixed field of $\bar\sigma$ cannot be K or else σ fixes $KF^{(2)}$. Then let L be the fixed field of $\bar\sigma$ in K. Since $\bar\sigma^2 = 1$, we see $[K : L] = 2$ as desired.

Since $F^{(3)} = K^{(3)}$, we see that $\mathcal{G}_K \subsetneq \mathcal{G}_F$. From [CSm1, Theorem 2.1], we see that $\mathcal{G}_K \cong H \times \prod_I \mathbb{Z}/2\mathbb{Z}$ where $H \cap \Phi(\mathcal{G}_F) = \Phi(H)$ and $\prod_I \mathbb{Z}/2\mathbb{Z} \subseteq \Phi(\mathcal{G}_F)$. On the other hand, no W-group other than $\mathbb{Z}/2\mathbb{Z}$ can have a direct factor isomorphic to $\mathbb{Z}/2\mathbb{Z}$ [CSm1, Proposition 2.3]. Therefore either $\mathcal{G}_K \cong \mathbb{Z}/2\mathbb{Z} \subseteq \Phi(\mathcal{G}_F)$ or $\Phi(\mathcal{G}_K) = \mathcal{G}_K \cap \Phi(\mathcal{G}_F)$. If $\mathcal{G}_K \cong \mathbb{Z}/2\mathbb{Z}$, then K is a Euclidean field (see [MiSp2]), and $K^{(3)} = K(\sqrt{-1})$. Because

$\Phi(\mathcal{G}_F) \supseteq \mathcal{G}_K$ we see that $K \supseteq F^{(2)} \subseteq F(\sqrt{-1})$. This is a contradiction to the assumption that $[K(\sqrt{-1}) : K] = 2$. Thus the case $\mathbb{Z}/2\mathbb{Z} \cong \mathcal{G}_K \subseteq \Phi(\mathcal{G}_F)$ cannot happen. (Alternatively one could use the well-known fact that real closed fields do not have subfields of finite codimension.) Thus we see that $\Phi(\mathcal{G}_K) = \mathcal{G}_K \cap \Phi(\mathcal{G}_F)$.

Observe that the natural map $\dot{F}/\dot{F}^2 \to \dot{K}/\dot{K}^2$ can be identified with the restriction map $\big(\mathcal{G}_F/\Phi(\mathcal{G}_F)\big)^* \to \big(\mathcal{G}_K/\Phi(\mathcal{G}_K)\big)^* = \Big(\mathcal{G}_K/\big(\mathcal{G}_K \cap \Phi(\mathcal{G}_F)\big)\Big)^*$, where * denotes the Pontrjagin dual of the group described in the corresponding bracket. Since the canonical map $\mathcal{G}_K/\Phi(\mathcal{G}_K) \to \mathcal{G}_F/\Phi(\mathcal{G}_F)$ is injective and since both $\mathcal{G}_K/\Phi(\mathcal{G}_K)$ and $\mathcal{G}_F/\Phi(\mathcal{G}_F)$ are products of copies of $\mathbb{Z}/2\mathbb{Z}$, we see that the natural map $\dot{F}/\dot{F}^2 \to \dot{K}/\dot{K}^2$ is a surjective map. Since the map $\dot{F}/\dot{F}^2 \to \dot{K}/\dot{K}^2$ factors through $\dot{L}/\dot{L}^2$, we see that $\dot{L}/\dot{L}^2$ maps surjectively onto $\dot{K}/\dot{K}^2$ as well. Letting $K = L(\sqrt{a})$ and applying the Square-Class Exact Sequence to this quadratic extension, we see that the norm map N must be trivial, in which case necessarily $[-a] \in \dot{L}^2$ so that $K = L(\sqrt{-1})$ and L is pythagorean. Then we see by Theorem 3.2 that $F^{(3)} = K^{(3)} = L^{(3)}$. If $L = F$ we are done. If $L \neq F$ we can repeat the argument above where K is replaced by L. We thus obtain a pythagorean field M, with $F \subseteq M \subseteq L$ and $L = M(\sqrt{-1})$. Since L is also pythagorean, we see $L = L^2 + L^2 = L^2$. But then $[K : L] = 1$, a contradiction. Then in fact $L = F$, F is pythagorean, and $K = F(\sqrt{-1})$ as desired. ■

Corollary 3.7 *Let K/F be any extension of fields. Then $F^{(2)} = K^{(2)}$ if and only if $F^{(3)} = K^{(3)}$.*

Proof By the preceding theorem, if $F^{(3)} = K^{(3)}$ then F is pythagorean and $K = F(\sqrt{-1})$ so by the square class exact sequence we see that $F^{(2)} = K^{(2)}$. Conversely, if $F^{(2)} = K^{(2)}$, then $K \subseteq F^{(2)}$, and by Kummer theory we see that $\dot{K} = \dot{F}\dot{K}^2$, and therefore again the map $\dot{F}/\dot{F}^2 \to \dot{K}/\dot{K}^2$ is surjective. Proceeding as in the previous proof, we see that F is pythagorean and $K = F(\sqrt{-1})$. Then by Theorem 3.2, we have that $F^{(3)} = K^{(3)}$.

Remark 3.8 In the introduction to this section, we pointed out that in general $(F^{(3)})^{(3)} \neq F^{(3)}$. It is not a surprising fact that $(F^{(3)})^{(3)} = F^{(3)}$ happens only in a "very few cases". To be precise we have

Proposition 3.9 *Let F be any field. Then $(F^{(3)})^{(3)} = F^{(3)}$ if and only if*

(1) F is quadratically closed, or
(2) F is Euclidean.

Proof If F is quadratically closed then $F^{(3)} = F$ and $(F^{(3)})^{(3)} = F^{(3)} = F$. If F is Euclidean, then $F^{(3)} = F(\sqrt{-1})$, (see Theorem 3.2 above), and $(F^{(3)})^{(3)} = F(\sqrt{-1}) = F^{(3)}$. On the other hand if $(F^{(3)})^{(3)} = F^{(3)}$ then from Theorem 3.6 above, we can immediately conclude that either F is quadratically closed or F is pythagorean and $F^{(3)} = F(\sqrt{-1})$. However, in the latter case we see that $|\dot{F}/\dot{F}^2| = 2$, $-1 \notin \dot{F}^2$ and F is pythagorean. Hence F is Euclidean as desired. ■

There is a quite nice method we can employ here to construct WF from WK, since we are working with a formally real pythagorean field. We know from [L2] that we have an embedding $WF \hookrightarrow \mathcal{C}(X, \mathbb{Z})$, where $\mathcal{C}(X, \mathbb{Z})$ denotes the ring of continuous functions from the space of F-orderings X to $\mathbb{Z}$ and the embedding is given by $\varphi \mapsto \hat{\varphi}$ with $\hat{\varphi}(P) := \operatorname{sgn}_P \varphi$

for each form $\varphi \in WF$ and each ordering $P \in X$. Further, we know that the image of WF in $\mathcal{C}(X, \mathbb{Z})$ is completely and constructively determined by the following Representation Theorem [L2, Theorem 7.2], provided that we know all fans T of finite index in $\dot{F}/\dot{F}^2$.

Representation Theorem *Let $f \in \mathcal{C}(X, \mathbb{Z})$. Then there exists $\varphi \in WF$ such that $f = \hat{\varphi}$ if and only if for each fan $T \subseteq \dot{F}$ of finite index in $\dot{F}$ we have a congruence*

$$\sum_{P \in X/T} f(P) \equiv 0 (\text{mod } |X/T|).$$

(Here X/T denotes the set of those orderings $P \in X$ which contain T.) ■

Then given $\mathcal{G}_K$, we know $\mathcal{G}_F \cong \mathcal{G}_K \rtimes \langle \sigma_{-1} \rangle$ and therefore we know the space of orderings X_F of F, including the structure of all fans of finite index in F. Hence via the Representation Theorem we know WF as well. One recovers X_F from $\mathcal{G}_F$ as follows: There is a one-to-one correspondence between the cosets $\sigma\Phi(\mathcal{G}_F)$ with $\sigma^2 = 1$, $\sigma \notin \Phi(\mathcal{G}_F)$ and orderings P_σ on F, as explained in [MiSp2]. We can then identify X_F with the folowing set of subsets of $H^1(\mathcal{G}_F)$ (the set of all continuous homomorphisms $\mathcal{G}_F \to \mathbb{Z}/2\mathbb{Z}$):

$$\tilde{P}_\sigma := \text{Ann}(\sigma) := \{\psi \in H^1(\mathcal{G}_F) \mid \psi(\sigma) = 0\}.$$

Thus

$$X_F = \{\tilde{P}_\sigma \mid \sigma \in \mathcal{G}_F, \sigma^2 = 1, \sigma \notin \Phi(\mathcal{G}_F)\}.$$

Moreover, recalling that $\dot{F}/\dot{F}^2 \cong H^1(\mathcal{G}_F)$, we see that we can represent elements $[\varphi] \in WF$ as $[\langle \psi_1, \psi_2, \ldots, \psi_n \rangle] \in WF$, where $\psi_1, \ldots, \psi_n \in H^1(\mathcal{G}_F)$. Then X_F is the topological space with subbasis the family of Harrison sets $H(\psi) := \{\tilde{P} \in X_F \mid \psi \in \tilde{P}\}$. Further we see that a set $S \subseteq X_F$ is a fan if and only if $S = \{\tilde{P}_\sigma \mid \sigma \in H_S \subseteq \mathcal{G}_F, \sigma^2 = 1, \sigma \notin \Phi(H_S)\}$ where H_S is any essential subgroup of $\mathcal{G}_F$ generated by involutions which have the property that for any three involutions $\sigma_1, \sigma_2, \sigma_3 \in H_S - \Phi(\mathcal{G}_F)$, the element $\sigma_1\sigma_2\sigma_3$ is again an involution. (See also [CSm1, Section 4] for more details on fan subgroups of $\mathcal{G}_F$.)

4 Adjoining the Square Root of a Double-Rigid Element

Recall that an element $b \in \dot{F} - (\dot{F}^2 \cup -\dot{F}^2)$ is called a *rigid* element of F if and only if the set of values $D_F\langle 1, b \rangle$ of the quadratic form $x^2 + by^2$ over the field F is the smallest possible, namely $D_F\langle 1, b \rangle = \{[1], [b]\}$.

In the case when both elements $[b]$ and $[-b]$ are rigid we call b a *double-rigid* element of F. Double-rigid elements play an important role in the theory of quadratic forms. (See *e.g.* [Be1], [Be2], [BCW], [MiSp1].) In particular, one can define the following interesting subset $A(F) := \{x \in \dot{F} \mid x \text{ or } -x \text{ is nonrigid.}\}$ Remarkably enough, one can show that $A(F)$ is a subgroup of $\dot{F}$. (See [Be1] and [Be2].) In this section we shall assume that $K = F(\sqrt{a})$ and a is a double rigid element. Then $D_F\langle 1, -a \rangle = \{\dot{F}^2, -a\dot{F}^2\}$.

In the Square-Class Exact Sequence we have $\text{im}\, N = \dot{F}^2 \cup -a\dot{F}^2$ and $\dim_{\mathbb{Z}/2\mathbb{Z}} \dot{K}/\dot{K}^2 = \dim_{\mathbb{Z}/2\mathbb{Z}} \dot{F}/\dot{F}^2$. Since $\ker \epsilon = \{\dot{F}^2, a\dot{F}^2\}$, we see that we can choose a basis $\{\sqrt{a}, b_j \mid j \in J\}$ for $\dot{K}/\dot{K}^2$ such that $\{a, b_j \mid j \in J\}$ is a basis for $\dot{F}/\dot{F}^2$. (For if $\sqrt{a} \equiv b \ (\text{mod } \dot{K}^2)$ for some $b \in \dot{F}$ then $\sqrt{a} = b(x^2 + ay^2 + 2xy\sqrt{a})$ for some nonzero $x, y \in F$, so that $x^2 + ay^2 = 0$, forcing $a \equiv -1 \ (\text{mod } \dot{F}/\dot{F}^2)$, a contradiction.)

https://doi.org/10.4153/CJM-2000-036-0 Published online by Cambridge University Press

Suppose that $\mathcal{B} = \{[a], [a_i] \mid i \in I\}$ is a basis for $\dot{F}/\dot{F}^2$. Let $\{\sigma, \sigma_i \mid i \in I\}$ be a minimal set of generators for $\mathcal{G}_F$ which are dual to $\mathcal{B}$. (That is, σ fixes $\sqrt{a_i}$ for all $i \in I$, $\sigma(\sqrt{a}) = -\sqrt{a}$, σ_i fixes $\sqrt{a}$ for all $i \in I$, and $\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$ for all $i, j \in I$.)

Recall that B is the smallest closed subgroup of $\mathcal{G}_F$ containing the set $\{\sigma_i \mid i \in I\}$. (See Section 2.) Then $B \subseteq H := \mathrm{Gal}(F^{(3)}/K)$. Then from Propositions 2.5 and 2.6, we obtain the following result:

Proposition 4.1 *Let $K = F(\sqrt{a})$ where $-a$ is rigid. Then $H \cong B \times \mathbb{Z}/2\mathbb{Z}$.*

Proof In this case $[-a]$ is a $\mathbb{Z}/2\mathbb{Z}$-basis for $D\langle 1, -a\rangle$. ■

In the case when a is a double-rigid element, it was shown by Berman [Be2, Corollary 2.6] that $WF \cong WF(\sqrt{a})$, though not canonically. This was also proved, under the assumption that F was not formally real, in [MiSp1]. (Note that when F is not formally real, the notions of rigid and double-rigid coincide [Be1].) Here the authors would like to point out two minor inaccuracies in [MiSp1]. First, in Remark 1.7 on p. 837, one should still assume that the field L is not formally real and that L has at least four square classes. Second, in Remark 1.8 on p. 838, one should observe that in the case when L is a C-field, both L and $L(\sqrt{a})$ are fields of the same level and with square-class groups of the same size, so they must have isomorphic Witt rings by [Wa].

Now we can say a good deal more about $\mathcal{G}_K$ and $\mathcal{G}_F$ in the case where $K = F(\sqrt{a})$ and a is a double-rigid element.

Proposition 4.2 *Let $K = F(\sqrt{a})$ where $a \in \dot{F}$ is a double-rigid element. Then $K^{(2)} = F^{(2)}(\sqrt[4]{a})$, $K^{(2)} \subseteq F^{(3)}$, and $K^{(3)} = F^{(3)}(\sqrt[8]{a})$.*

Proof Because a is a double rigid element in F we see from the Square-Class Exact Sequence that

$$\frac{\dot{K}}{\dot{K}^2} \cong \frac{\dot{F}}{\{\dot{F}^2, a\dot{F}^2\}} \oplus \frac{\sqrt{a}\dot{F}}{\{\dot{F}, a\dot{F}^2\}}.$$

Therefore $K^{(2)} = F^{(2)}(\sqrt[4]{a})$.

Because $K^{(3)}$ is the compositum of all quadratic, cyclic of order 4 and dihedral of order 8 extensions of K, we shall investigate which Galois extensions of K of the types above occur. It is well known that this is essentially equivalent to the characterization of the splitting quaternion algebras over K. (See *e.g.* [MiSp3, Propositions 2.3 and 2.4, p. 41].) Each such quaternion algebra has one of the following shapes:

(1) $A_K = (\frac{f_1, f_2}{K})$, $f_1, f_2 \in \dot{F}$,
(2) $A = (\frac{f_1, \sqrt{a} f_2}{K})$, $f_1, f_2 \in \dot{F}$,
(3) $A = (\frac{\sqrt{a} f_1, \sqrt{a} f_2}{K})$, $f_1, f_2 \in \dot{F}$.

Case 1 Set $A = (\frac{f_1, f_2}{F})$, $f_1, f_2 \in \dot{F}$ and $[A_K] = [A \otimes_F K] = 0$ in $\mathrm{Br}(K)$. Using once again the exact sequence of groups

$$\frac{\dot{F}}{\dot{F}^2} \xrightarrow{\alpha} \mathrm{Br}_2(F) \xrightarrow{\tau} \mathrm{Br}(K),$$

https://doi.org/10.4153/CJM-2000-036-0 Published online by Cambridge University Press

where $\alpha([f]) = [(\frac{a,f}{F})]$ for each $[f] \in \frac{\dot F}{\dot F^2}$ and τ is induced by the inclusion $F \hookrightarrow F(\sqrt{a}) = K$, we see that there exists an element $f \in \dot F$ such that $[(\frac{f_1,f_2}{F}) \otimes (\frac{a,f}{F})] = 0$ in $Br_2 F$.

Consider now the group extension

$$1 \to \Phi(\mathcal{G}_F) \to \mathcal{G}_F \to E_F \to 1$$

where E_F is the Galois group of the maximal multiquadratic extension of F (*i.e.*, $E_F = \mathrm{Gal}(F^{(2)}/F)$).

Applying the 5-term short exact sequence we obtain (see [E, p. 77]):

$$0 \longrightarrow H^1(E_F) \xrightarrow{\text{inf}} H^1(\mathcal{G}_F) \xrightarrow{\text{Res}} H^1\big(\Phi(\mathcal{G}_F)\big) \xrightarrow{\text{tra}} H^2(E_F) \xrightarrow{\text{inf}} H^2(G_F).$$

Here inf = inflation, Res = restriction and tra = transgression are well-known maps in the cohomology of groups.

Because inf: $H^1(E_F) \to H^1(\mathcal{G}_F)$ is an isomorphism we see that our sequence can be replaced by $0 \to H^1\big(\Phi(\mathcal{G}_F)\big) \xrightarrow{\text{tra}} H^2(E_F) \xrightarrow{\text{inf}} H^2(\mathcal{G}_F)$. Thus we can think of $H^1\big(\Phi(\mathcal{G}_F)\big) \cong (\frac{\dot F^{(2)}}{(\dot F^{(2)})^2})^{E_F}$ (see [GMi, p. 100]) as elements of $H^2(E_F)$ which die in $H^2(\mathcal{G}_F)$. In particular we see that the element $(f_1) \cup (f_2) + (a) \cup (f) \in H^2(E_F)$ can be identified with a certain element, say z, of the square-class group $(\frac{\dot F^{(2)}}{(\dot F^{(2)})^2})^{E_F}$. Here (f_1), (f_2), (a), (f) correspond to elements of $H^1(E_F)$ associated with $[f_1]$, $[f_2]$, $[a]$, $[f]$ respectively.

Observe that we have the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Phi(\mathcal{G}_K) & \longrightarrow & \mathcal{G}_K & \longrightarrow & E_K & \longrightarrow & 1 \\ & & \big\downarrow u & & \big\downarrow v & & \big\downarrow w & & \\ 1 & \longrightarrow & \Phi(\mathcal{G}_F) & \longrightarrow & \mathcal{G}_F & \longrightarrow & E_F & \longrightarrow & 1 \end{array}$$

where all vertical maps are induced by inclusions

$$F \subseteq K \subseteq F^{(2)} \subseteq K^{(2)} \subseteq F^{(3)} \subseteq K^{(3)}$$

observed earlier and the restrictions of Galois actions.

Therefore one can compare our short exact sequences of cohomology groups attached to the horizontal rows of our diagram above.

We obtain

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1\big(\Phi(\mathcal{G}_K)\big) & \xrightarrow{\text{tra}} & H^2(E_K) & \xrightarrow{\text{inf}} & H^2(\mathcal{G}_K) \\ & & \big\uparrow u_* & & \big\uparrow v_* & & \big\uparrow w_* \\ 0 & \longrightarrow & H^1\big(\Phi(\mathcal{G}_F)\big) & \xrightarrow{\text{tra}} & H^2(E_F) & \xrightarrow{\text{inf}} & H^2(\mathcal{G}_F) \end{array}.$$

Since $(a)_K$ vanishes in $H^1(E_K)$ we see that $\text{tra}\big(u_*(z)\big) = (f_1)_K \cup (f_2)_K$. But this means that the element of $(\frac{\dot K^{(2)}}{(\dot K^{(2)})^2})^{E_K}$ associated with $u_*(z)$ (and $(f_1)_K \cup (f_2)_K$), is the image of the element in $(\frac{\dot F^{(2)}}{(\dot F^{(2)})^2})^{E_F}$ associated with z. Therefore if L/K is the Galois extension "associated

https://doi.org/10.4153/CJM-2000-036-0 Published online by Cambridge University Press

with the splitting quaternion algebra $(\frac{f_1, f_2}{K}) = 0 \in \mathrm{Br}(K)$," (*i.e.*, $L = K^{(2)}(\sqrt{b})$, where b is any element in $F(\sqrt{f_1})$ whose norm in F is f_2), then $L \subset F^{(3)} \cdot K^{(2)} = F^{(3)}$.

Case 2 $A = (\frac{f_1\sqrt{a}, f_2}{K})$, $f_1, f_2 \in \dot{F}$, $[A] = 0$ in $\mathrm{Br}_2(K)$.

Here the key observation is that $-\sqrt{a}f_2$ is a rigid element of K. (See [Be2, Theorem 2.3].) Then $[(\frac{f_1, \sqrt{a}f_2}{K})] = 0$ in $\mathrm{Br}_2 K$ forces $[f_1] \in D_K\langle 1, -\sqrt{a}f_2\rangle$ (see [L1, p. 58, Theorem 2.7]), and $[f_1] = [1]$ or $[-\sqrt{a}f_2] = [f_1]$. In the first case, we do not obtain any associated Galois extension L/K so there is nothing to worry about. The second case is impossible as $\sqrt{a} \notin \dot{F}\dot{K}^2$.

Case 3 $A = (\frac{\sqrt{a}f_1, \sqrt{a}f_2}{K})$, $f_1, f_2 \in \dot{F}$, $[A] = 0$ in $\mathrm{Br}_2(K)$.

We pointed out in our discussion that $-\sqrt{a}f_1$, $-\sqrt{a}f_2$ are both rigid elements of $\dot{K}$. Hence $[A] = 0$ forces $[f_1]_K = [-f_2]_K$. (Thus $[f_1]_F = [-f_2]_F$ or $[f_1]_F = [-af_2]_F$.) In any case, using arguments as in Case 1, we see that if L/K is any Galois extension (either a cyclic of order 4 or a dihedral of order 8 extension) associated with A, then $LK^{(2)} = K^{(2)}(\sqrt[4]{\sqrt{a}f_2})$. However $K^{(2)}(\sqrt[4]{f_2}) \subset F^{(3)}$ and therefore we see that each Galois extension L/K as above is contained in $F^{(3)}(\sqrt[8]{a})$.

Observing that $\sqrt[8]{a} \in K^{(3)}$, we see that we can combine the three cases above to a single statement $K^{(3)} = F^{(3)}(\sqrt[8]{a})$. ■

Remark 4.3 Observe that although $\sqrt[8]{a}$ is not uniquely determined by the field extension K/F, the field extension $F^{(3)}(\sqrt[8]{a})$ is determined by K/F. This can be seen directly as follows. For each element $c \in \dot{F}$ such that $K = F(\sqrt{c})$ we have $c = ab^2$ for some $b \in \dot{F}$. Hence $F^{(3)}(\sqrt[8]{c}) = F^{(3)}(\sqrt[8]{a}\sqrt[4]{b}) = F^{(3)}(\sqrt[8]{a})$. The last equality is true because $\sqrt[4]{b} \in F^{(3)}$.

Proposition 4.4 *Let $K = F(\sqrt{a})$ where $a \in \dot{F}$ is a double-rigid element. Then $K^{(3)} = F^{(3)}(\sqrt[8]{a})$ is a nontrivial quadratic extension of $F^{(3)}$ which is Galois over F.*

Proof Because $\sqrt[4]{a} \in F^{(3)}$ and $K^{(3)} = F^{(3)}(\sqrt[8]{a})$ we see that $K^{(3)}/F^{(3)}$ is a quadratic extension. From Theorem 3.6, we see that $K^{(3)} \neq F^{(3)}$. Hence we see that $K^{(3)}/F^{(3)}$ is a nontrivial quadratic extension.

Set $L = F(\zeta_8, \sqrt[8]{a})$, where ζ_8 is a primitive 8-th root of unity. We may set $\zeta_8 = \frac{\sqrt{2}+i\sqrt{2}}{2} \in F^{(2)}$. Then L/F is a Galois extension of F. Because $K^{(3)}$ is the compositum of $F^{(3)}$ with L, we see that $K^{(3)}/F$ is Galois as well. ■

Theorem 4.5 *Let $K = F(\sqrt{a})$ where a is a double-rigid element in $\dot{F}$. Then $\mathcal{G}_F \cong \mathbb{Z}/4\mathbb{Z} \rtimes B$, where B is an essential subgroup of $\mathcal{G}_F$ associated to the subgroup $H = \mathrm{Gal}(F^{(3)}/K)$. Furthermore if $\widetilde{B}$ is an essential subgroup of $\mathcal{G}_K$ associated to the subgroup $\widetilde{H} = \mathrm{Gal}\big(K^{(3)}/K(\sqrt[4]{a})\big)$, then $\widetilde{B} \cong B$ and $\mathcal{G}_K \cong \mathbb{Z}/4\mathbb{Z} \rtimes \widetilde{B}$. Moreover, one can find a subgroup C of index 2 in $\widetilde{B}$ such that $\widetilde{B} = C \cup \sigma C$ for some element $\sigma \in \widetilde{B}$ and the action of C is trivial on the first factor $\mathbb{Z}/4\mathbb{Z} = \langle\tau\rangle$ in the isomorphism $\mathcal{G}_K \cong \mathbb{Z}/4\mathbb{Z} \rtimes \widetilde{B}$ and the action of σ is either also trivial or $\sigma^{-1}\tau\sigma = \tau^3$. The choice of action of σ on $\mathbb{Z}/4\mathbb{Z}$ depends on the presence of $\sqrt{-1} \in \dot{F}$.*

Proof That $\mathcal{G}_F \cong \frac{\mathbb{Z}}{4\mathbb{Z}} \rtimes B$ follows directly from Theorem 3.5 in [MiSm2] and its proof. There it is further shown that the action of B on $\tau \in \mathbb{Z}/4\mathbb{Z}$ is trivial if $-1 \in \dot{F}^2$. If $-1 \notin \dot{F}^2$, then choosing $[-1] = [a_1] \in \{[a_i], i \in I\}$, the action of all σ_i on τ is trivial, except $\sigma_1^{-1}\tau\sigma_1 = \tau^3$.

We claim that we can choose our generators σ_i, $i \in I$, of B such that $\sigma_i(\sqrt[4]{a}) = \sqrt[4]{a}$ for all $i \in I$. Indeed we have for $H = \mathrm{Gal}(\frac{F^{(3)}}{K})$,

$$\left(\frac{H}{\Phi(H)}\right)^* \cong \frac{\dot{K}^{(2)}}{(\dot{K}^{(2)})^2} \cong \frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2, a\dot{F}^2\}} \oplus \sqrt{a}\frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2, a\dot{F}^2\}}.$$

Therefore we can choose a minimal set of generators $\{\sigma_i, i \in I\}$ of B such that they act trivially on $\sqrt[4]{a}$ and such that $(\frac{B}{\Phi(B)})^* = \frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2, a\dot{F}^2\}}$. (Recall that $\frac{H}{\Phi(H)} \cong \big((\frac{H}{\Phi(H)})^*\big)^* \cong (\frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2, a\dot{F}^2\}} \oplus \sqrt{a}\frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2, a\dot{F}^2\}})^*$.) Then $H \cong B \times \frac{\mathbb{Z}}{2\mathbb{Z}} = B \times \langle\tau\rangle$ where τ acts trivially on $F^{(2)}$ and $\tau(\sqrt[4]{a}) = -\sqrt[4]{a}$. (See Proposition 2.6 and its proof.)

Now we consider the natural projection $\Theta\colon \mathcal{G}_K \to H$. We claim that there exists a subgroup $\widetilde{B}$ of $\mathcal{G}_K$ which is mapped isomorphically onto B under the map Θ.

Because $\sigma_i(\sqrt[4]{a}) = \sqrt[4]{a}$ for each $i \in I$ we may choose $\tilde{\sigma}_i = \mathcal{G}_K$, $i \in I$, such that $\Theta(\widetilde{\sigma}_i) = \sigma_i$ and $\widetilde{\sigma}_i(\sqrt[8]{a}) = \sqrt[8]{a}$. We set $\widetilde{B}$ to be the subgroup of $\mathcal{G}_K$ topologically generated by $\{\tilde{\sigma}_i, i \in I\}$. Then $\Theta(\widetilde{B}) = B$. In order to show that Θ restricted to $\widetilde{B}$ induces an isomorphism, it is enough to show that for each $\gamma \in \Phi(\widetilde{B})$ such that $\Theta(\gamma) = 1$, we have $\gamma = 1 \in \mathcal{G}_K$. To show that $\gamma = 1$ (when assuming $\Theta(\gamma) = 1$, which is equivalent to assuming that $\gamma|F^{(3)}$ is the identity), it is enough to show that $\gamma(\sqrt[8]{a}) = \sqrt[8]{a}$. Since γ is a product of some commutators of the form $[\tilde{\sigma}_i, \widetilde{\sigma}_j]$, $i, j \in I$ and squares $\tilde{\sigma}_i^2$, $i \in I$, it is enough to observe that $[\tilde{\sigma}_i, \tilde{\sigma}_j](\sqrt[8]{a}) = \sqrt[8]{a}$ for each $i, j \in I$ and $\tilde{\sigma}_i^2(\sqrt[8]{a}) = \sqrt[8]{a}$ for each $i \in I$. To see this consider restrictions of $[\tilde{\sigma}_i, \tilde{\sigma}_j]$ and $\tilde{\sigma}_i^2$ onto $K(\sqrt[8]{a}, \sqrt{-1})$, which is a Galois extension of K. Because all $\tilde{\sigma}_i$ act trivially on $\sqrt[4]{a}$ we see that for each $i, j \in I$, $i \neq j$, both $\tilde{\sigma}_i$ and $\tilde{\sigma}_j$ restrict to an abelian subgroup of $G := \mathrm{Gal}\big(K(\sqrt[8]{a}, \sqrt{-1})/K\big)$, hence $[\tilde{\sigma}_i, \tilde{\sigma}_j]|K(\sqrt[8]{a}, \sqrt{-1})$ is the identity. Similarly for all $\tilde{\sigma}_i$, we see that $\tilde{\sigma}_i^2|K(\sqrt[8]{a}, \sqrt{-1})$ is the identity. Hence B is indeed an isomorphic image of $\tilde{B}$ under the map Θ.

On the other hand, because $\tau(\sqrt[4]{a}) = -\sqrt[4]{a}$ and $\tau(\sqrt{-1}) = \sqrt{-1}$, we see that for any lift $\tilde{\tau} \in \mathcal{G}_K$ (*i.e.*, $\Theta(\tilde{\tau}) = \tau$), we have the restriction of $\tilde{\tau}$ to $\mathrm{Gal}\big(K(\sqrt[8]{a}, \sqrt{-1})/K(\sqrt{-1})\big) \cong \mathbb{Z}/4\mathbb{Z}$ is a generator of this cyclic group. In particular the order of $\tilde{\tau}$ is 4. Moreover, since $\tilde{\tau}^2(\sqrt[8]{a}) = -\sqrt[8]{a}$ and for each $\gamma \in \Phi(\tilde{B})$ we have $\gamma(\sqrt[8]{a}) = \sqrt[8]{a}$, we see that $\tilde{B} \cap \langle\tilde{\tau}\rangle = \{1\}$.

On the other hand from our observations $(\frac{H}{\Phi(H)})^* = (\frac{B}{\Phi(B)})^* \times (\langle\tau\rangle)^* \cong \frac{\dot{K}^{(2)}}{(\dot{K}^{(2)})^2}$ we see that $\{\widetilde{B} \cup \tilde{\tau}\}$ generates the group $\mathcal{G}_K$. Thus we see that indeed $\mathcal{G}_K \cong \langle\tilde{\tau}\rangle \rtimes \widetilde{B} \cong \frac{\mathbb{Z}}{4\mathbb{Z}} \rtimes \widetilde{B}$. Finally using once again [Be2, Theorem 2.3], we see that $\sqrt{a}$ is a double-rigid element of K. Therefore we can again refer the reader to Theorem 3.5 and its proof in [MiSm2] to conclude that the action of all σ_i on τ is trivial, except $\tilde{\sigma}_1\tilde{\tau}\tilde{\sigma}_1 = \tilde{\tau}^3$ in the case when $\sqrt{-1} \notin \dot{F}(\Rightarrow \sqrt{-1} \notin \dot{K})$. Our proof is now complete. ■

Remark The authors would like to take this opportunity to correct a misprint in the table of W-groups in [MiSm2]. The group 16.43 in the table on p. 1287 should be $\mathbb{Z}/4\mathbb{Z} \rtimes \big(\mathbb{Z}/4\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z})\big)$, of order 2^7, and not the group of order 2^8 as indicated.

https://doi.org/10.4153/CJM-2000-036-0 Published online by Cambridge University Press

References

[AKM] A. Adem, D. Karagueuzian and J. Mináč, *On the cohomology of Galois groups determined by Witt rings.* Max Planck Institute Preprint **30**, 1998; Adv. Math., to appear.

[Art] E. Artin, *Galois theory.* Dover Publications, 1998.

[AT] E. Artin and J. Tate, *Class Field Theory.* Addison-Wesley, Redwood City, California, 1990.

[Be1] L. Berman, *The Kaplansky Radical and Values of Binary Quadratic Forms.* PhD thesis, University of California, Berkeley, California, 1978.

[Be2] ———, *Quadratic forms and power series fields.* Pacific J. Math. **89**(1980), 257–267.

[BCW] L. Berman, C. Cordes and R. Ware, *Quadratic forms, rigid elements and formal power series fields.* J. Algebra **66**(1980), 123–133.

[CSm1] T. Craven and T. L. Smith, *Formally real fields from a Galois theoretic perspective.* J. Pure Appl. Algebra **145**(2000), 19–36.

[CSm2] ———, *Witt ring quotients associated to subgroups of $\dot{F}/\dot{F}^2$.* Unpublished manuscript, 1997.

[E] L. Evens, *The Cohomology of Groups.* Oxford Mathematical Monographs, Oxford University Press, New York, 1991.

[GMi] W. Gao and J. Mináč, *Milnor Conjecture and Galois theory I.* Fields Institute Communications **16**(1997), 95–110.

[Jac] N. Jacobson, *Lectures in Abstract Algebra, Vol. III.* Van Nostrand Company, Inc., 1964.

[Ko] H. Koch, *Galoissche Theorie der p-Erweiterungen.* Springer-Verlag, Berlin, 1970.

[L1] T. Y. Lam, *The Algebraic Theory of Quadratic Forms.* Benjamin/Cummings Publishing Co., Reading, Mass., 1980.

[L2] ———, *Orderings, Valuations and Quadratic Forms.* Conference Board of the Mathematical Sciences **52**, Amer. Math. Soc., Providence, RI, 1983.

[L3] ———, *The theory of ordered fields.* In: Ring Theory and Algebra III (ed. B. R. McDonald), Amer. Math. Soc. **55**(1980), 1–152.

[MMS] L. Mahé, J. Mináč and T. Smith, *Additive structure of subgroups of $\dot{F}/\dot{F}^2$ and Galois theory.* In preparation.

[Ma] M. Marshall, *Abstract Witt Rings.* Queen's Papers in Pure and Appl. Math. **57**, Queen's University, Kingston, Ontario, 1980.

[Me] A. Merkurjev, *On the norm residue symbol of degree 2.* Dokl. Akad. Nauk. SSSR **261**(1981), 542–547; English transl. in Soviet Mat. Dokl. **24**(1981), 546–551.

[MiSm1] J. Mináč and T. Smith, *W-groups and values of binary forms.* J. Pure Appl. Algebra **87**(1993), 61–78.

[MiSm2] ———, *Decomposition of Witt rings and Galois groups.* Canad. J. Math **47**(1995), 1274–1289.

[MiSp1] J. Mináč and M. Spira, *$u = 4$ and quadratic extensions.* Rocky Mountain J. Math. **19**(1989), 833–845.

[MiSp2] ———, *Formally real fields, pythagorean fields, C-fields and W-groups.* Math. Z. **205**(1990), 519–530.

[MiSp3] ———, *Witt rings and Galois groups.* Ann. of Math. **144**(1996), 35–60.

[Mor] S. A. Morris, *Pontrjagin duality and the structure of locally compact abelian groups.* London Math. Soc. Lecture Note Ser. **29**, Cambridge University Press, 1977.

[PSCL] R. Perlis, K. Szymiczek, P. E. Conner and R. Litherland, *Matching Witts with global fields.* In: Recent Advances in Real Algebraic Geometry and Quadratic Forms (eds. W. Jacob, T. Y. Lam and R. O. Robson), Contemp. Math. **155**(1994), 365–387.

[Ser] J.-P. Serre, *Galois cohomology.* Springer-Verlag, 1997.

[Sc] W. Scharlau, *Quadratic and Hermitian Forms.* Grundlehren Math. Wiss. **270**, Springer-Verlag, Berlin, 1985.

[Wd] A. Wadsworth, *Merkurjev's elementary proof of Merkurjev's theorem.* Contemp. Math. **55**(1986), 741–776.

[Wa] R. Ware, *When are Witt rings group rings? II.* Pacific J. Math **76**(1978), 541–564.

Department of Mathematics
University of Western Ontario
London, Ontario
N6A 5B7
email: minac@uwo.ca

Department of Mathematical Sciences
University of Cincinnati
Cincinnati, Ohio 45221-0025
USA
email: tara.smith@math.uc.edu

https://doi.org/10.4153/CJM-2000-036-0 Published online by Cambridge University Press