Math. Z. 205, 519–530 (1990)

Mathematische Zeitschrift

Formally real fields, pythagorean fields, C-fields and W-groups

Ján Mináč [1,*] **and Michel Spira** [2,**]

[1] Department of Mathematics, University of Western Ontario, Middlesex College, London, Ontario N6A 5B7, Canada
[2] Departamento de Matemática, Universidade Federal de Minas Gerais, Caixa Postal 702, 30161 Belo Horizonte MG, Brasil

Received February 2, 1989; in final form August 27, 1989

1 Introduction

This paper is a continuation of [MS], where W-groups were introduced. For the reader's convenience we recall in this section some of the concepts and notations used in this latter paper. If F is a field (always assumed to have characteristic not equal to 2) we define:

$F^{(2)}:=$compositum of all quadratic extensions of F.

$F^{(3)}:=$compositum of all quadratic extensions K of $F^{(2)}$ such that K/F is Galois.

$\mathcal{G}_F:=\mathrm{Gal}(F^{(3)}/F)$.

$[\sigma]:=$the conjugacy class of $\sigma\in\mathcal{G}_F$.

$\Phi_F:=$the subgroup of $\mathcal{G}_F$ topologically generated by the squares of elements of $\mathcal{G}_F$.

$F(2):=$the quadratic closure of F.

$G_F:=\mathrm{Gal}(F(2)/F)$.

$s(F):=$the level of F.

$u(F):=$the u-invariant of F.

$[a]:=$the class of $a\in\dot{F}$ in $\dot{F}/\dot{F}^2$.

$X_F:=$the set of orderings of F.

The group $\mathcal{G}_F$ will be seen as a topological group with the usual pro-2-group topology. This group has very pleasant properties, among which we list $g^4=1$ for all $g\in\mathcal{G}_F$ and the fact that commutators are in the center. We take the commutator subgroup $[\mathcal{G}_F, \mathcal{G}_F]$ to be the topological closure of the abstract commutator subgroup of $\mathcal{G}_F$. Note that since $[x, y]=x^{-2}(xy^{-1})^2y^2$ for x, y in any group, it follows that $[\mathcal{G}_F\ \mathcal{G}_F]\subset\Phi_F$.

* Supported in part by the National Science Foundation and the Natural Sciences and Engineering Research Council of Canada

** This article is a modified version of part of the second author's Ph.D. thesis, U.C. Berkeley, 1987

Note that $\Phi_F = \mathrm{Gal}(F^{(3)}/F^{(2)})$, and that $\mathcal{G}_F/\Phi_F \cong \mathrm{Gal}(F^{(2)}/F)$. A simple remark is that $\mathcal{G}_F/\Phi_F \cong \prod_{i\in I} \mathbb{Z}/2\mathbb{Z}$ if and only if $\dot{F}/\dot{F}^2 \cong \bigoplus_{i\in I} \mathbb{Z}/2\mathbb{Z}$; this follows from the fact that $F^{(2)}$ is the composition of the quadratic extensions $F(\sqrt{a})$ where $[a]$ ranges over a basis of $\dot{F}/\dot{F}^2$.

All other notations and concepts used in this paper can be found in standard works in quadratic forms, e.g., [L 1], [L 2].

The importance of W-groups can be seen from the following theorem:

Theorem 1.1 ([MS]). *Let F, L be fields; then*

1. $WF \cong WL \Rightarrow \mathcal{G}_F \cong \mathcal{G}_L$.
2. *If $\langle 1, 1\rangle_F$ is universal assume also that $s(F) = s(L)$. Then $\mathcal{G}_F \cong \mathcal{G}_L \Rightarrow WF \cong WL$.*

This theorem shows that Witt ring invariants can be translated into group theoretic information and conversely; the aim of this paper is to present a few examples to illustrate this. We choose formally real fields and pythagorean fields (Sect. 2) and C-fields (Sect. 3) because in these cases it is particularly easy to translate field properties into Witt ring information (see [L 1], [L 2], [War]). We remark that the results in Sect. 2, which parallel the classical Artin-Schreier-Becker theory (see [Bec]), have led to the notion of a generalized ordering which is studied in [MM].

In [MS] it was shown that $F^{(3)}$ is the compositum of all extensions K of F such that $\mathrm{Gal}(K/F)$ is one of $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{D}_4$ (here $\mathbb{D}_4$ denotes the usual dihedral group of order 8). The importance of $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{D}_4$ can easily be seen by theorems 1.3 and 1.6 below, which show that the splitting of quaternion algebras over F is precisely reflected in the Galois theory of F.

Definition 1.2. *A Galois extension L of F is called a $\mathbb{Z}/4\mathbb{Z}$-extension of F if $\mathrm{Gal}(L/F) \cong \mathbb{Z}/4\mathbb{Z}$. If $a \in \dot{F} \setminus \dot{F}^2$ then by a $\mathbb{Z}/4\mathbb{Z}^a$-extension of F we mean a $\mathbb{Z}/4\mathbb{Z}$-extension K of F such that $K \supset F(\sqrt{a})$.*

Theorem 1.3 ([L 1] exercise VII.8). *Let $a \in \dot{F} \setminus \dot{F}^2$. Then there exists a $\mathbb{Z}/4\mathbb{Z}^a$-extension of F if and only if $\left(\frac{a, a}{F}\right) = 1$.*

Definition 1.4. *Two elements a, $b \in \dot{F}$ are called independent modulo squares if $[a]$ and $[b]$ are linearly independent in $\dot{F}/\dot{F}^2$.*

Definition 1.5. *A Galois extension L of F is called a $\mathbb{D}_4$-extension of F if $\mathrm{Gal}(L/F) \cong \mathbb{D}_4$. If a, $b \in \dot{F}$ are independent modulo squares then by a $\mathbb{D}_4^{a,b}$-extension of F we mean a $\mathbb{D}_4$-extension K of F such that $K \supset F(\sqrt{a}, \sqrt{b})$ and $\mathrm{Gal}(K/F(\sqrt{ab})) \cong \mathbb{Z}/4\mathbb{Z}$.*

Theorem 1.6. ([F] (7.7)). *Let a, $b \in \dot{F}$ be independent modulo squares. Then there exists a $\mathbb{D}_4^{a,b}$-extension of F if and only if $\left(\frac{a, b}{F}\right) = 1$.*

2 Formally real fields and pythagorean fields

In this section we characterize formally real fields in terms of the existence of special involutions in their W-groups. We also explain how orderings arise from the W-group and introduce the concept of relative real closure. We finish by characterizing pythagorean fields via their W-groups.

We will be working constantly with involutions of $\mathcal{G}_F$. To simplify notation, we will say that such an involution σ is

simple if $\sigma\in\Phi_F$ (note that every nonidentity element of Φ_F is a central involution);

real if σ is not simple and if the fixed field $F_\sigma^{(3)}$ of σ is formally real;

nonreal if σ is not simple and not real.

Notice that if $\sigma\in\mathcal{G}_F$ and $\sigma\Phi_F$ contains an involution then every nonidentity element of $\sigma\Phi_F$ is an involution.

Theorem 2.7. *Let F be a field. Then*

1. *If F is formally real then $\mathcal{G}_F$ contains a real involution.*
2. *If $\mathcal{G}_F$ contains a nonsimple involution then F is formally real.*

Proof. (1) Suppose that F is formally real and let $P\in X_F$. By [Bec] there exists an involution $\tilde{\sigma}\in G_F$ such that $\sqrt{-1}^{\tilde{\sigma}}=-\sqrt{-1}$ and $P=F(2)_{\tilde{\sigma}}^2\cap\dot{F}$. Let $\sigma:=\tilde{\sigma}|_{F^{(3)}}$. Then $\sigma^2=1$ and $\sqrt{-1}^{\sigma}=-\sqrt{-1}$, so $\sigma\notin\Phi_F$ and $F_\sigma^{(3)}=F(2)_{\tilde{\sigma}}\cap F^{(3)}$ is formally real. Therefore σ is a real involution. Note that $P=(F_\sigma^{(3)})^2\cap\dot{F}$.

(2) Let σ be a nonsimple involution in $\mathcal{G}_F$, and let b be any element of $\dot{F}$ such that $(\sqrt{b})^{\sigma}=-\sqrt{b}$. Note that such b exists because $\sigma\notin\Phi_F$.

Claim 1. b is not a sum of two squares.

Proof of claim. Suppose b is a sum of two squares. By Theorem 1.3 there exists a $\mathbb{Z}/4\mathbb{Z}^b$-extension L of F. Let $\bar{\sigma}:=\sigma|_L$; note that since L/F is Galois we have $\bar{\sigma}\in\mathrm{Gal}(L/F)$. Write $\mathrm{Gal}(L/F)=\langle\tau\colon\tau^4=1\rangle$. Since $\sigma^2=1$ we have $\bar{\sigma}=1$ or $\bar{\sigma}=\tau^2$. In either case we get $\sqrt{b}=(\sqrt{b})^{\bar{\sigma}}$, a contradiction.

Claim 2. If $\left(\frac{b,c}{F}\right)=1$ then $(\sqrt{c})^{\sigma}=\sqrt{c}$.

Proof of claim. If $c\in\dot{F}^2$ the claim is clear, so we assume $c\notin\dot{F}^2$. If b and c are dependent modulo squares we get $1=\left(\frac{b,c}{F}\right)\sim\left(\frac{b,b}{F}\right)$ and therefore b is a sum of two squares, a contradiction. Hence b and c are independent modulo squares and by Theorem 1.6 there exists a $\mathbb{D}_4^{b,c}$-extension L of F. Let $\bar{\sigma}:=\sigma|_L$. Because $[F^{(3)}:F_\sigma^{(3)}]=2$ and $(\sqrt{b})^{\sigma}=-\sqrt{b}$ it follows that $[L:L_{\bar{\sigma}}]=2$. In such an extension only an element of order 4 can move both $\sqrt{b}$ and $\sqrt{c}$, and hence $\sqrt{c}=(\sqrt{c})^{\bar{\sigma}}=(\sqrt{c})^{\sigma}$.

Claim 3. $(\sqrt{-1})^{\sigma}=-\sqrt{-1}$. In particular $\sqrt{-1}\notin F$.

Proof of claim. Since $\left(\frac{b,-b}{F}\right)=1$ it follows by claim 2 that $(\sqrt{-b})^{\sigma}=\sqrt{-b}$. But then $(\sqrt{-b})^{\sigma}=(\sqrt{-1})^{\sigma}(\sqrt{b})^{\sigma}$ implies that $-\sqrt{-1}^{\sigma}\sqrt{b}=\sqrt{-b}$ and therefore $\sqrt{-1}^{\sigma}=-\sqrt{-1}$.

Now let $P := \{p \in \dot{F} : (\sqrt{p})^\sigma = \sqrt{p}\}$. Note that $P = (F_\sigma^{(3)})^2 \cap \dot{F}$. It is clear that

1. $-1 \notin P$ (by claim 3);
2. $\dot{F}^2 \subset P$ and $P.\,P \subset P$;
3. $P \cap -P = \emptyset$, and
4. $P \cup -P = \dot{F}$.

So all we need for P to be an ordering is $P + P \subset P$. Let $p \in P$. Then $(\sqrt{p})^\sigma = \sqrt{p}$ and since $(\sqrt{-1})^\sigma = -\sqrt{-1}$ we get $(\sqrt{-p})^\sigma = -\sqrt{-p}$. Now $\left(\frac{1+p,\,-p}{F}\right) = 1$ and by claim 2 we get $(\sqrt{1+p})^\sigma = \sqrt{1+p}$, i.e., $1 + p \in P$. Therefore P is additively closed and we are done. □

Remarks. (1) As it is clear from the proof above, if $L \subset F(2)$ is any Galois extension of F such that $F^{(3)} \subset L$ then Theorem 2.7 holds for $\mathrm{Gal}(L/F)$ instead of $\mathscr{G}_F$. As a matter of fact, this remark is valid for all the results in this section. What one really needs is to have all quadratic, $\mathbb{Z}/4\mathbb{Z}$- and $\mathbb{D}_4$-extensions of F available. $F^{(3)}$ is simply the smallest Galois extension of F inside $F(2)$ for which our results hold.

(2) We showed above that if F is formally real then $\mathscr{G}_F$ contains a real involution. In the next section we will show that nonreal involutions fail to exist if and only if F is superpythagorean.

Definition 2.8. *The fixed field $F_\sigma^{(3)}$ of a nonsimple involution $\sigma \in \mathscr{G}_F$ will be called a relative real closure of F.*

In the course of the proof of Theorem 2.7 we established the following correspondence between X_F and the set of nonsimple involutions of $\mathscr{G}_F$:

1. For each $P \in X_F$ there exists a real involution $\sigma \in \mathscr{G}_F$ such that $P = (F_\sigma^{(3)})^2 \cap \dot{F}$. Here we set $\sigma = \sigma_P$; this entails a slight abuse of notation since in general such σ is not uniquely determined (see Proposition 2.9).

2. Each nonsimple involution $\sigma \in \mathscr{G}_F$ determines $P \in X_F$ given by $P = (F_\sigma^{(3)})^2 \cap \dot{F}$. In this case we set $P = P_\sigma$; this is no abuse of notation since P_σ is uniquely determined by σ.

Note that if $P \in X_F$ then $P = P_{\sigma_P}$ and therefore the map {nonsimple involutions of $\mathscr{G}_F\} \to X_F$ described in (2) above is surjective. We now describe this map in more detail.

Proposition 2.9. 1. *Let σ and τ be nonsimple involutions in $\mathscr{G}_F$. Then $P_\sigma = P_\tau \Leftrightarrow \sigma\Phi_F = \tau\Phi_F$.*

2. *Let σ, τ be nonsimple conjugate involutions in $\mathscr{G}_F$. Then $P_\sigma = P_\tau$.*

3. *Let σ and τ be real involutions in $\mathscr{G}_F$. Then $P_\sigma = P_\tau \Leftrightarrow \sigma$ and τ are conjugate in $\mathscr{G}_F$.*

Proof. (1) From the explicit description of P_σ and P_τ we see that $P_\sigma = P_\tau \Leftrightarrow (\sqrt{a})^\sigma = (\sqrt{a})^\tau$ for all $a \in \dot{F}$. This happens if and only if $\sigma|_{F(2)} = \tau|_{F(2)}$, i.e., $\sigma\tau^{-1} \in \mathrm{Gal}(F^{(3)}/F^{(2)}) = \Phi_F$.

(2) Write $\sigma = \gamma^{-1}\tau\gamma$. Then $\sigma = \tau\tau^{-1}\gamma^{-1}\tau\gamma = \tau[\tau, \gamma] \in \tau\Phi_F$, and therefore $P_\sigma = P_\tau$ by (1).

(3) If σ and τ are conjugate we have $P_\sigma = P_\tau$ by (2). Assume now that $P_\sigma = P_\tau =: P$. Let $\tilde{\sigma}$ and $\tilde{\tau}$ be involutions in G_F such that $F(2)_{\tilde{\sigma}}$ and $F(2)_{\tilde{\tau}}$ are euclidean closures of $F_\sigma^{(3)}$ and $F_\tau^{(3)}$, respectively. Note that $F(2)_{\tilde{\sigma}}$ and $F(2)_{\tilde{\tau}}$ are

both euclidean closures of F with respect to P. We have $\sigma=\tilde{\sigma}|_{F(3)}$ and $\tau=\tilde{\tau}|_{F(3)}$. It follows from [L1], Theorem VIII.2.8 that there is an order preserving F-isomorphism $\gamma'\colon F(2)_{\tilde{\sigma}}\to F(2)_{\tilde{\tau}}$, which extends to an F-automorphism $\tilde{\gamma}\in G_F$. Then an easy computations shows that $\tilde{\gamma}\tilde{\tau}\tilde{\gamma}^{-1}=\tilde{\sigma}$. Setting $\gamma:=\tilde{\gamma}|_{F(3)}$ we get $\gamma\tau\gamma^{-1}=\sigma$. □

Corollary 2.10. *Let F be a field. Then there exists a bijection between the set of orderings of F and the nontrivial cosets $\sigma\Phi_F$ where σ is an involution. This bijection is given by $P\mapsto\sigma_P\,\Phi_F$ and $\sigma\Phi_F\mapsto P_\sigma$.*

Proof. This is a restatement of Proposition 2.9(1) and of previous remarks. □

We finish this section with a characterization of pythagorean fields via their W-groups.

Theorem 2.11. *The following conditions are equivalent:*
1. *F is pythagorean.*
2. *$\mathcal{G}_F$ is generated by involutions.*
3. *$\Phi_F=[\mathcal{G}_F,\mathcal{G}_F]$.*

Proof. (1)⇒(2) Suppose F is pythagorean. If F is not formally real then F is quadratically closed and hence $\mathcal{G}_F=\{1\}$ is generated by the empty set of involutions. If F is formally real then F is the intersection of the family of its euclidean closures $\{F_i\colon i\in I\}$ ([Bec] Corollary 2 of Satz 10). Let $\tilde{\sigma}_i$ be the involution of G_F corresponding to F_i. Then G_F is generated by the $\tilde{\sigma}_i$'s and therefore $\mathcal{G}_F$ is generated by the (real) involutions $\sigma_i:=\tilde{\sigma}_i|_{F(3)}$.

(2)⇒(3) Let $\tau=\sigma_1\sigma_2\ldots\sigma_n$ where the σ_i's are involutions in $\mathcal{G}_F$. Then

$$\tau^2=(\sigma_1\sigma_2\ldots\sigma_n)(\sigma_1\sigma_2\ldots\sigma_n).$$

In this expression we can move the rightmost σ_1 past all the σ_i's to its left until it cancels out with the other σ_1, at the price of introducing commutators. Since the commutators are in the center of $\mathcal{G}_F$ we can move all of them to the right side of the expression and repeat the procedure with σ_2, etc. In the end we are left with an expression for τ^2 as a product of commutators. This shows that the abstract subgroup generated by the squares is contained in the abstract commutator subgroup; since the reverse inclusion is always true we get equality. Taking closures finishes the argument.

(3)⇒(1) Suppose $\Phi_F=[\mathcal{G}_F,\mathcal{G}_F]$ and let $\Psi\colon\mathcal{G}_F\to\mathbb{Z}/4\mathbb{Z}$ be a homomorphism. Then Ψ factors through $\mathcal{G}_F/[\mathcal{G}_F,\mathcal{G}_F]=\mathcal{G}_F/\Phi_F$ which is elementary 2-abelian, and therefore Ψ cannot be onto. In other words F has no $\mathbb{Z}/4\mathbb{Z}$-extensions and therefore F is pythagorean by Theorem 1.3.

3 C-fields and abelian W-groups

In this section we will characterize C-fields via their W-groups, and obtain all the abelian W-groups in the process. Recall that F is a C-field if $D_F\langle 1,a\rangle=\{[1],[a]\}$ for all $a\in\dot{F}\setminus(\pm\dot{F}^2)$. It is well known that the possible values of the level of a C-field are 1, 2 and ∞ ([War] Proposition 1.1); our characterization distinguishes between these possibilities.

We will also characterize superpythagorean fields (i.e., C-fields of level ∞) as fields having the largest possible "number" of relative real closures (see Definition 2.8); these closures will be described at the end of the section. We recall that a field F is euclidean if F is formally real and $\dot{F}/\dot{F}^2=\{[1],[-1]\}$; note that F is euclidean if and only if F is superpythagorean and $|\dot{F}/\dot{F}^2|=2$.

Throughout this section we will let I denote an arbitrary set of indices with $|I|\geqq 1$. If $a\in\dot{F}$, by $\sqrt[4]{a}$ we will always mean a fixed choice of fourth root of a inside some algebraic closure of F. We give $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ the discrete topology and $\prod_{i\in I}\mathbb{Z}/2\mathbb{Z}$ and $\prod_{i\in I}\mathbb{Z}/4\mathbb{Z}$ the product topology.

We begin by classifying the abelian W-groups; we look at the small ones in the next theorem, and finish with Theorem 3.13.

Theorem 3.12. *Let F be a field. Then*

1. $\mathcal{G}_F=\{1\}\Leftrightarrow F$ *is quadratically closed* $\Leftrightarrow WF\cong\mathbb{Z}/2\mathbb{Z}$.
2. $\mathcal{G}_F=\mathbb{Z}/2\mathbb{Z}$ *or* $\mathbb{Z}/4\mathbb{Z}\Leftrightarrow|\dot{F}/\dot{F}^2|=2$.
3. $\mathcal{G}_F\cong\mathbb{Z}/2\mathbb{Z}\Leftrightarrow F$ *is euclidean* $\Leftrightarrow WF\cong Z$.
4. $\mathcal{G}_F\cong\mathbb{Z}/4\mathbb{Z}\Leftrightarrow F$ *is not formally real*, $|\dot{F}/\dot{F}^2|=2$; *and* $u(F)=2\Leftrightarrow WF\cong\mathbb{Z}/2\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ *or* $WF\cong\mathbb{Z}/4\mathbb{Z}$.

Proof. (1) $\mathcal{G}_F=\{1\}\Leftrightarrow F$ has no proper quadratic extensions, and the result follows.

(2) If $\mathcal{G}_F=\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$ then F has a unique quadratic extension, i.e., $|\dot{F}/\dot{F}^2|=2$. Conversely, if $|\dot{F}/\dot{F}^2|=2$ then $[F^{(2)}:F]=2$; the square class exact sequence ([L1] Theorem VII.3.4) shows that $[\dot{F}^{(2)}/(\dot{F}^{(2)})^2|\leqq 2$ and therefore $[F^{(3)}:F^{(2)}]\leqq 2$. Hence $[F^{(3)}:F]\leqq 4$, i.e., $|\mathcal{G}_F|\leqq 4$. Since F has a unique quadratic extension we cannot have $\mathcal{G}_F\cong\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ and the result follows since $\mathcal{G}_F\neq\{1\}$ by (1).

(3) Suppose that F is euclidean. Then $\dot{F}/\dot{F}^2=\{[1],[-1]\}$ and $F(2)=F(\sqrt{-1})$ ([L1] exercise VII.5). In particular $G_F\cong\mathbb{Z}/2\mathbb{Z}$ and therefore $\mathcal{G}_F\cong\mathbb{Z}/2\mathbb{Z}$.

Conversely, assume $\mathcal{G}_F\cong\mathbb{Z}/2\mathbb{Z}$. Then $|\dot{F}/\dot{F}^2|=2$, and F is pythagorean because F has no $\mathbb{Z}/4\mathbb{Z}$-extensions. Since F is not quadratically closed it follows that F is formally real, and therefore F is euclidean.

Finally, the fact that F is euclidean if and only if $WF\cong Z$ is well known ([L3], Example 1.12).

(4) If $\mathcal{G}_F=\mathbb{Z}/4\mathbb{Z}$ then $|\dot{F}/\dot{F}^2|=2$ by (2) above. If $F(\sqrt{a})$ is the unique quadratic extension of F then a is a sum of two squares and if follows immediately that F is not formally real and $u(F)=2$. These conditions in turn imply that $WF\cong\mathbb{Z}/2\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ or $\mathbb{Z}/4\mathbb{Z}$ by [L1] Theorem II.3.5. Finally, if WF is of one of those forms, we compute $IF\cong\mathbb{Z}/2\mathbb{Z}$ and $I^2F=\{0\}$, so $|\dot{F}/\dot{F}^2|=2$. Then $\mathcal{G}_F=\mathbb{Z}/4\mathbb{Z}$ follows by (2) and (3). $\square$

Theorem 3.13. *Assume $\dot{F}/\dot{F}^2\cong\bigoplus_{i\in I}\mathbb{Z}/2\mathbb{Z}$ and $|I|\geqq 2$. Then the following conditions are equivalent:*

1. $\mathcal{G}_F\cong\prod_{i\in I}\mathbb{Z}/4\mathbb{Z}$.
2. $\mathcal{G}_F$ *is abelian.*
3. F *is a C-field and* $s(F)=1$.

Proof. (1)$\Rightarrow$(2). Trivial.

(2)$\Rightarrow$(3) Since $\mathcal{G}_F$ is abelian we see that F has no $\mathbb{D}_4$-extensions. In particular, F has no $\mathbb{D}_4^{a,-a}$-extensions and therefore $s(F)=1$. Moreover by Theorem 1.6 we see that F is a C-field.

(3)$\Rightarrow$(1) Let $\{[a_i]: i \in I\}$ be a basis of $\dot{F}/\dot{F}^2$.

Claim 1. A basis of $\dot{F}^{(2)}/(\dot{F}^{(2)})^2$ is $\{[\sqrt{a_i}]: i \in I\}$.

Proof of claim. It is enough to show that given a finite family $\{[a_1], \ldots, [a_n]\}$ of $[a_i]$'s, a basis of $\dot{K}_n/\dot{K}_n^2$ is $\{[\sqrt{a_i}]: 1 \leqq i \leqq n\} \cup \{[a_j]: j \neq 1, \ldots, n\}$ where $K_n := F(\sqrt{a_1}, \ldots, \sqrt{a_n})$.

So let $K_i := F(\sqrt{a_1}, \ldots, \sqrt{a_i})$ and consider the tower of quadratic extensions $F \subset K_1 \subset \ldots \subset K_n$. Since F is a C-field it follows by the square class exact sequence ([L 1] Theorem VII.3.4; see also [Ber], Corollary 1.12) that a basis for $\dot{K}_1/\dot{K}_1^2$ is $\{[\sqrt{a_1}], [a_i]: i \neq 1\}$. Now all K_i's are C-fields ([War] Corollary 2.8). In particular K_1 is a C-field and the same reasoning as above shows that a basis of $\dot{K}_2/\dot{K}_2^2$ is $\{[\sqrt{a_1}], [\sqrt{a_2}], [a_i]: i \neq 1, 2\}$. Iteration of this procedure yields the required basis of $\dot{K}_n/\dot{K}_n^2$.

Claim 2. $F^{(3)} = F(\sqrt[4]{a_i}: i \in I)$.

Proof of claim. By the definition of $F^{(3)}$ we know that $F(\sqrt[4]{a_i}) \subset F^{(3)}$ for all $i \in I$. On the other hand $F^{(3)}$ is a compositum of some quadratic extensions of $F^{(2)}$ which by claim 1 are of the form $F(\sqrt[4]{a_{i_1} \ldots a_{i_n}})$ for some $i_1, \ldots, i_n \in I$. The claim follows.

This explicit description of $F^{(3)}$ allows us to use abelian Kummer theory ([AT], Sect. 1) to conclude that $\mathscr{G}_F \cong \prod_{i \in I} \mathbb{Z}/4\mathbb{Z}$. More precisely, $\mathscr{G}_F$ is generated by the set $\{\tau_i: i \in I\}$ where

$$\sqrt[4]{a_i}^{\tau_j} = \begin{cases} \sqrt{-1}\sqrt[4]{a_i} & \text{if } i = j, \\ \sqrt[4]{a_i} & \text{if } i \neq j. \end{cases} \quad \square$$

Corollary 3.14. *Let F be a formally real field. Then F has a unique relative real closure $\Leftrightarrow F$ is euclidean. In this case F is its own unique real closure.*

Proof. Suppose first that F is euclidean. Then $F(2) = F(\sqrt{-1}) = F^{(3)}$ and it follows immediately that F is its own unique relative real closure. Conversely, suppose F has a unique relative real closure, and let σ be a real involution in $\mathscr{G}_F$. Since distinct elements of $\sigma\Phi_F$ give rise to distinct relative real closures of F we see that $\Phi_F = \{1\}$. Therefore $\mathscr{G}_F$ is a group of exponent 2; in particular $\mathscr{G}_F$ is abelian. Perusing our list of abelian W-groups and noticing that $\mathscr{G}_F \neq \{1\}$ because $|\dot{F}/\dot{F}^2| \geqq 2$, we see that we must have $\mathscr{G}_F = \mathbb{Z}/2\mathbb{Z}$, and therefore F is euclidean. $\square$

We now make a comment which will be used in the next two theorems. Let F be a field and M a (possibly infinite) Galois extension of F. Suppose K and L are two subfields of M, linearly disjoint over F and such that L is Galois over F and $M = KL$. Then $\mathrm{Gal}(M/L) \lhd \mathrm{Gal}(M/F)$ and we can write $\mathrm{Gal}(M/F) = \mathrm{Gal}(M/L) \rtimes \mathrm{Gal}(M/K)$. It follows that the Krull topology of $\mathrm{Gal}(M/F)$ is exactly the product of the Krull topologies of $\mathrm{Gal}(M/L)$ and $\mathrm{Gal}(M/K)$ ([A] Theorem 4 Chap. 6).

Theorem 3.15. *A field F is a C-field with $\dot{F}/\dot{F}^2 \cong (\bigoplus_{i\in I} \mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}/2\mathbb{Z}$ and $s(F)=2$ if and only if $\mathcal{G}_F \cong (\prod_{i\in I} \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/4\mathbb{Z}$ where the action of a generator σ of the outer $\mathbb{Z}/4\mathbb{Z}$ on $\tau \in \prod_{i\in I} \mathbb{Z}/4\mathbb{Z}$ is given by $\sigma^{-1}\tau\sigma = \tau^3$.*

Proof. Suppose first that $\mathcal{G}_F$ is as given in the hypothesis. For simplicity, write $A := \prod_{i\in I} \mathbb{Z}/4\mathbb{Z}$ and $B := \mathbb{Z}/4\mathbb{Z} = \langle \sigma \rangle$; we may then assume that $\mathcal{G}_F = A \rtimes B$.

Claim 1. F is not formally real.

Proof of claim. By Theorem 2.7 it is enough to show that all involutions of $\mathcal{G}_F$ are simple. So let $\tau \in A$ and $\sigma^i\tau$, $0 \leqq i \leqq 3$, be an involution. Then

$$1 = (\sigma^i\tau)^2 = \sigma^{2i}(\sigma^{-i}\tau\sigma^i)\tau = \sigma^{2i}\tau^{1+3^i}$$

so

$$1 = \sigma^{2i} = \tau^{1+3^i}$$

and therefore $i \in \{0, 2\}$. Both possibilities imply $\tau^2 = 1$; since all elements of order 2 in A are squares it follows that $\sigma^i\tau \in \Phi_F$ and we are done with the claim.

Claim 2. $[\mathcal{G}_F, \mathcal{G}_F] = A^2$.

Proof of claim. Since $\mathcal{G}_F/A^2 \cong (\prod_{i\in I} \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z}$ is abelian we see that $[\mathcal{G}_F, \mathcal{G}_F] \subset A^2$. For the reverse inclusion, notice that for $\tau \in A$ we have $\sigma^{-1}\tau\sigma = \tau^3$ and hence $\tau^2 = [\tau, \sigma]$.

Claim 3. Every $\mathbb{Z}/4\mathbb{Z}$-extension of F contains $\sqrt{-1}$. In particular, $D_F\langle 1, 1\rangle = \{[1], [-1]\}$.

Proof of claim. First notice that $\mathbb{Z}/4\mathbb{Z}$-extensions of F do exist, e.g., take the fixed field of A. Now let L be a $\mathbb{Z}/4\mathbb{Z}$-extension of F, and let $^-$ denote the restriction homomorphism $\mathcal{G}_F \to \mathbb{Z}/4\mathbb{Z} \cong \mathrm{Gal}(L/F)$. Since $\mathbb{Z}/4\mathbb{Z}$ is abelian, $^-$ factors through $\mathcal{G}_F/[\mathcal{G}_F, \mathcal{G}_F] \cong (\prod_{i\in I} \mathbb{Z}/2\mathbb{Z}) \times B$. It follows that $\bar{B} = \mathbb{Z}/4\mathbb{Z}$ and that $\bar{A} \in \{0, 2\} \subset \mathbb{Z}/4\mathbb{Z}$. Hence the intermediate quadratic extension $F(\sqrt{a})$ of L is uniquely determined as the fixed field of $A \times B^2$, and therefore $D_F\langle 1, 1\rangle = \{[1], [a]\}$ by Theorem 1.3.

It remains to show that $[a] = [-1]$; for that it is enough to show that $s(F) = 2$, since then $[-1] \neq [1]$ and $-1 \in D_F\langle 1, 1\rangle$. First note that we cannot have $s(F) = 1$. Indeed, if so, then $\langle 1, 1\rangle$ is universal and therefore $\dot{F}/\dot{F}^2 = D_F\langle 1, 1\rangle = \{[1], [a]\}$. Hence $|\dot{F}/\dot{F}^2| = 2$ and therefore $\mathcal{G}_F$ is abelian by Theorem 3.12(2), a contradiction.

Now let $b \in D_F\langle 1, 1, 1, 1\rangle$. Since $D_F\langle 1, 1\rangle = \{[1], [a]\}$ we see that we have either $b \in D_F\langle 1, 1\rangle$ or $b \in D_F\langle 1, a\rangle$ or $b \in D_F\langle a, a\rangle = aD_F\langle 1, 1\rangle = D_F\langle 1, 1\rangle$. In any case we have $b \in D_F\langle 1, 1, 1\rangle$, which shows that $s(F) < 4$. Since $s(F)$ cannot be 3 and we already know that $s(F) \neq 1$, we must have $s(F) = 2$. We then get $[a] = [-1]$ and we are done with the claim.

Claim 4. F is a C-field.

Proof of claim. Let $a\in\dot F\setminus(\pm\dot F^2)$ and let $b\in D_F\langle 1,\ -a\rangle$; we want to show that $[b]\in\{[1],\ [-a]\}$. Assume $[b]\neq[1]$. We have $[b]\neq[a]$, since $a\in D_F\langle 1,\ -a\rangle$ would imply that a is a sum of two squares, i.e., $[a]=[\pm 1]$, a contradiction by the choice of a. Hence a and b are independent modulo squares, and since $\left(\frac{a,b}{F}\right)=1$ there exists a $\mathbb{D}_4^{a,b}$-extension K of F by Theorem 1.6.

Let $^{-}: \mathscr{G}_F\to \mathrm{Gal}(K/F)\cong\mathbb{D}_4$ denote the restriction homomorphism. Since $\mathbb{D}_4$ is nonabelian $\bar A$ and $\bar B$ cannot commute elementwise, and therefore there must exist $\tau\in A$ such that $[\bar\sigma,\ \bar\tau]\neq 1$. Because $\mathbb{D}_4$ is generated by any noncommuting pair of its elements, we have $\mathbb{D}_4=\langle\bar\sigma,\ \bar\tau\rangle$. The relation in $\mathscr{G}_F$ gives $\bar\sigma^{-1}\bar\tau\bar\sigma=\bar\tau^3$; in particular the order of $\bar\tau$ is 4 because $[\bar\sigma,\ \bar\tau]\neq 1$, and so $\bar\sigma$ is a noncentral involution in $\mathbb{D}_4$. Now let ε be any element of A; from $[\tau,\ \varepsilon]=1$ we get $[\bar\tau,\ \bar\varepsilon]=1$ and therefore we must have $\bar\varepsilon\in\langle\bar\tau\rangle$, i.e., $\bar A\subset\langle\bar\tau\rangle$.

Carrying this information back to K we see that $(\sqrt{ab})^\sigma=-\sqrt{ab}$ and that $(\sqrt{ab})^\tau=\sqrt{ab}$ for all $\tau\in A$. Since $(\sqrt{ab})^{\sigma^2}=\sqrt{ab}$ it follows that $\sqrt{ab}$ is fixed by $A\times B^2$ and therefore $[ab]=[-1]$ by claim 3, implying that $[b]=[-a]$. This finishes the proof of the "if" part of the theorem.

We now prove the "only if" part. Suppose that F is a C-field with $s(F)=2$ and $\dot F/\dot F^2\cong(\bigoplus_{i\in I}\mathbb{Z}/2\mathbb{Z})\oplus\mathbb{Z}/2\mathbb{Z}$. Let $\{[-1],\ [a_i]\colon i\in I\}$ be a basis of $\dot F/\dot F^2$. Since $s(F)=2$ there exists a $\mathbb{Z}/4\mathbb{Z}^{-1}$-extension L of F. We have $L=F(\sqrt{y})$ where $y\in F(\sqrt{-1})$ is such that $[N_{F(\sqrt{-1})/F}(y)]=[-1]$ by Theorem 1.3. It then follows as in the proof of Theorem 3.13 that

1. $\{[y],\ [a_i]\colon i\in I\}$ is a basis of $F(\sqrt{-1})^{\cdot}/(F(\sqrt{-1})^{\cdot})^2$;
2. $\{[\sqrt{y}],\ [a_i]\colon i\in I\}$ is a basis of $\dot L/\dot L^2$;
3. $\{[y],\ [\sqrt{a_i}]\colon i\in I\}$ is a basis of $\dot F^{(2)}/(\dot F^{(2)})^2$

and therefore $F^{(3)}=F(\sqrt{y},\ \sqrt[4]{a_i}\colon i\in I)=L(\sqrt[4]{a_i})\colon i\in I)$. From (2) above and abelian Kummer theory it follows that $A:=\mathrm{Gal}(F^{(3)}/L)=\langle\tau_i\colon i\in I\rangle\cong\prod_{i\in I}\mathbb{Z}/4\mathbb{Z}$ where

$$(\sqrt[4]{a_i})^{\tau_j}=\begin{cases}\sqrt{-1}\sqrt[4]{a_i} & \text{if } i=j\\ \sqrt[4]{a_i} & \text{if } i\neq j\end{cases}$$

and the τ_j's act trivially on $\sqrt{-1}$ and $\sqrt{y}$ for all $j\in I$.

Now write $B:=\mathrm{Gal}(F^{(3)}/F(\sqrt[4]{a_i}\colon i\in I))=\langle\sigma\rangle\cong\mathbb{Z}/4\mathbb{Z}$. We then have

$$(\sqrt{-1})^\sigma=-\sqrt{-1},$$
$$(\sqrt[4]{a_i})^\sigma=\sqrt[4]{a_i},$$
$$(\sqrt{y})^\sigma=\sqrt{y^\sigma}.$$

Finally, notice that for each $i\in I$ the extension $F_i:=F(\sqrt{-1},\ \sqrt[4]{a_i})$ is a $\mathbb{D}_4$-extension of F, and that $F^{(3)}$ is the compositum of L and all the F_i's. The descriptions of σ and of the τ_i's show that the equation $\sigma^{-1}\tau_i\sigma=\tau_i^3$ holds when restricted to L and the F_j's, and hence $\sigma^{-1}\tau_i\sigma=\tau_i^3$ in $\mathscr{G}_F$. Since L and

$F(\sqrt[4]{a_i}\colon\ i\in I)$ are linearly disjoint over F we see that $\mathcal{G}_F = A \rtimes B \cong (\prod_{i\in I} \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/4\mathbb{Z}$; the comments preceding this theorem show that this isomorphism is indeed a homeomorphism. $\square$

Theorem 3.16. *For a field F the following statements are equivalent:*

1. *F is superpythagorean and $\dot{F}/\dot{F}^2 \cong (\bigoplus_{i\in I} \mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}/2\mathbb{Z}$.*
2. *$\mathcal{G}_F \cong (\prod_{i\in I} \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$ where the action of a generator $\sigma\in\mathbb{Z}/2\mathbb{Z}$ on $\tau\in\prod_{i\in I}\mathbb{Z}/4\mathbb{Z}$ is given by $\sigma^{-1}\tau\sigma=\tau^3$.*
3. *$\mathcal{G}_F$ contains a nonsimple involution, $\mathcal{G}_F/\Phi_F \cong (\prod_{i\in I} \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$ and every nonsimple involution of $\mathcal{G}_F$ is real.*

Proof. (1)⇒(2) Same as in the proof of the corresponding fact in Theorem 3.15. Here we get $F^{(3)} = F(\sqrt{-1}, \sqrt[4]{a_i}\colon i\in I)$ where $\{[-1], [a_i]\colon i\in I\}$ is a basis of $\dot{F}/\dot{F}^2$. Also $\mathcal{G}_F = \langle \sigma, \tau_i\colon i\in I\rangle$, where $\sigma^{-1}\tau_i\sigma=\tau_i^3$, $\tau_i\tau_j=\tau_j\tau_i$ for all $i, j\in I$ and

$$(1)\qquad \begin{aligned} (\sqrt{-1})^{\sigma} &= -\sqrt{-1} \\ (\sqrt[4]{a_i})^{\sigma} &= \sqrt[4]{a_i} \\ (\sqrt{-1})^{\tau_i} &= \sqrt{-1} \\ (\sqrt[4]{a_i})^{\tau_j} &= \begin{cases} \sqrt{-1}\sqrt[4]{a_i} & \text{if } i=j \\ \sqrt[4]{a_i} & \text{if } i\neq j. \end{cases} \end{aligned}$$

(2)⇒(3) Let $A := \prod_{i\in I} \mathbb{Z}/4\mathbb{Z}$ and $B := \mathbb{Z}/2\mathbb{Z} = \langle\sigma\rangle$; we can then assume $\mathcal{G}_F = A \rtimes B$. Since $\sigma^{-1}\tau\sigma=\tau^3$ and Φ_F is contained in the center of $\mathcal{G}_F$ we see that σ is a nonsimple involution. Since $\mathcal{G}_F/A^2 \cong (\prod_{i\in I}\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$ is elementary 2-abelian we see that $\Phi_F \subset A^2$. The reverse inclusion is obvious, so we get $\Phi_F = A^2$. This gives us the required expression for $\mathcal{G}_F/\Phi_F$; in order to finish the proof we only have to show that all nonsimple involutions of $\mathcal{G}_F$ are real.

So let δ be a nonsimple involution. Any element in $\delta\Phi_F$ can be written as $\delta\tau^2$ for some $\tau\in A$; since $\delta\notin A$ we have $\delta^{-1}\tau\delta=\tau^3$ and therefore $\delta\tau^2 = \tau\delta\tau^{-1}\in[\delta]$. This shows that $\delta\Phi_F\subset[\delta]$ and therefore $\delta\Phi_F=[\delta]$, and hence δ is real. We remark that the set of nonsimple involutions of $\mathcal{G}_F$ is precisely σA.

(3)⇒(1) The existence of a nonsimple involution means that F is formally real (Theorem 2.7), and the expression for $\mathcal{G}_F/\Phi_F$ gives $\dot{F}/\dot{F}^2 \cong (\bigoplus_{i\in I}\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}/2\mathbb{Z}$. So all we have to show is that F is a C-field.

Let $\delta_0\in\mathcal{G}_F$ be any nonsimple involution. Since every nonsimple involution is real, $\delta_0\Phi_F = [\delta_0]$.* This shows that $\Phi_F = [\delta_0, \mathcal{G}_F]$; in particular $\Phi_F = [\mathcal{G}_F, \mathcal{G}_F]$ and therefore F is pythagorean by Theorem 2.11.

* (See Prop. 2.9.)

Now let $a \notin (\pm \dot{F}^2)$ and let $b \in D_F\langle 1, -a\rangle \setminus \dot{F}^2$; we want to show that $[b] = [-a]$. We have $[b] \neq [a]$, for otherwise $a \in D_F\langle 1, -a\rangle$ and this would imply that $a \in D_F\langle 1, 1\rangle = \dot{F}^2$, a contradiction. So a and b are independent modulo squares and hence there exists a $\mathbb{D}_4^{a,b}$-extension L of F. Suppose now $[b] \neq [-a]$. Since F is pythagorean it follows that ab is not a totally negative element of F and therefore there exists an ordering $P \in X_F$ such that $ab \in P$. Using the results in Sect. 5 we can write $P = P_\delta$ for some nonsimple involution $\delta \in \mathscr{G}_F$.

Let $^-: \mathscr{G}_F \to \mathrm{Gal}(L/F) \cong \mathbb{D}_4$ denote the restriction map. Then $\bar{\delta}$ fixes $\sqrt{ab}$; since $\bar{\delta}$ has order $\leqq 2$ we see that $\bar{\delta}$ is in the center of $\mathbb{D}_4$. Reading the equation $\Phi_F = [\delta, \mathscr{G}_F]$ in $\mathbb{D}_4$ we conclude that $\mathbb{D}_4$ is a group of exponent 2, a contradiction. Therefore $[b] = [-a]$ and we are done.

Corollary 3.17. *Let F be a field. Then every relative real closure of F is formally real $\Leftrightarrow F$ is superpythagorean.*

Proof. The case $|\dot{F}/\dot{F}^2| \geqq 4$ is simply a restatement of (1)$\Leftrightarrow$(3) in Theorem 3.16, and the case $|\dot{F}/\dot{F}^2| = 2$ is Corollary 3.14. □

Let P be an ordering of a superpythagorean field F; we will now describe the set of relative real closures of F with respect to P. If $|\dot{F}/\dot{F}^2| = 2$ then F is euclidean, P is the unique ordering of F and F is its own unique relative real closure, as we have already seen. Suppose now $|\dot{F}/\dot{F}^2| \geqq 4$ and let σ be a real involution of $\mathscr{G}_F$ such that $P = P_\sigma$. Fix a basis $\{[-1], [a_i]: i \in I\}$ of $\dot{F}/\dot{F}^2$ with $a_i \in P$. We can then construct $\mathscr{G}_F = \langle \sigma, \tau_i: i \in I\rangle = A \rtimes B$ as in Theorem 3.16. We saw that here $\Phi_F = A^2$, and it follows that the set of relative real closures of F with respect to P is exactly $\{F^{(3)}_{\sigma\tau^2}: \tau \in A\}$. Fix $\tau \in A$ and let $S \subset I$ be defined by

$$(2) \qquad (\sqrt[4]{a_i})^{\tau^2} = \begin{cases} \sqrt[4]{a_i} & \text{if } i \in S \\ -\sqrt[4]{a_i} & \text{if } i \notin S. \end{cases}$$

Then it is easily seen, using (1), that

$$(3) \qquad F^{(3)}_{\sigma\tau^2} = F(\sqrt[4]{a_i}, \sqrt{-1}\sqrt[4]{a_j})$$

where $i \in S$ and $j \in I \setminus S$. Conversely, given a subset $S \subset I$ we define $\tau \in A$ by

$$(\sqrt{-1})^\tau = \sqrt{-1}$$

$$(\sqrt[4]{a_i})^\tau = \begin{cases} \sqrt[4]{a_i} & \text{if } i \in S \\ \sqrt{-1}\sqrt[4]{a_i} & \text{if } i \notin S. \end{cases}$$

It is then clear that (2) holds, and that $F^{(3)}_{\sigma\tau^2}$ is given by (3). We have then proved the following result:

Corollary 3.18. *Let F be a superpythagorean field, $\{[-1], [a_i]: i \in I\}$ a basis of $\dot{F}/\dot{F}^2$ (where this time we allow $I = \emptyset$) and σ a nonsimple involution in $\mathscr{G}_F$. Then* *the set of real closures of F with respect to* P_σ *is in a* $1-1$ *correspondence with the subsets* $S \subset I$. *This correspondence is given by*

$$S \mapsto F(\sqrt[4]{a_i}, \sqrt{-1}\sqrt[4]{a_j})$$

for $i \in S, j \in I \setminus S$.

The computation of the relative real closures in the last corollary can be carried on in a more general way, as follows. We let $\mathscr{G}_F = \langle \sigma, \tau_i \colon i \in I \rangle = A \rtimes B$ be as above but now choose an arbitrary basis $\{[-1], [b_i] \colon i \in I\}$ of $\dot{F}/\dot{F}^2$. Fix $\tau \in A$, and write $I = \mathscr{A} \cup \mathscr{B} \cup \mathscr{C} \cup \mathscr{D}$ where

$$(\sqrt[4]{b_i})^\sigma = \begin{cases} \sqrt[4]{b_i} & \text{if } i \in \mathscr{A} \\ -\sqrt[4]{b_i} & \text{if } i \in \mathscr{B} \\ \sqrt{-1}\sqrt[4]{b_i} & \text{if } i \in \mathscr{C} \\ -\sqrt{-1}\sqrt[4]{b_i} & \text{if } i \in \mathscr{D} \end{cases}$$

Now write $\mathscr{A} = \mathscr{A}_1 \cup \mathscr{A}_2$, $\mathscr{B} = \mathscr{B}_1 \cup \mathscr{B}_2$, $\mathscr{C} = \mathscr{C}_1 \cup \mathscr{C}_2$ and $\mathscr{D} = \mathscr{D}_1 \cup \mathscr{D}_2$ where

$$(\sqrt[4]{b_i})^{\tau^2} = \begin{cases} \sqrt[4]{b_i} & \text{if } i \in \mathscr{A}_1 \cup \mathscr{B}_1 \cup \mathscr{C}_1 \cup \mathscr{D}_1 \\ -\sqrt[4]{b_i} & \text{if } i \in \mathscr{A}_2 \cup \mathscr{B}_2 \cup \mathscr{C}_2 \cup \mathscr{D}_2. \end{cases}$$

We leave it to the reader to check that

$$F^{(3)}_{\sigma\tau^2} = F(\sqrt[4]{b_i}, \sqrt{-1}\sqrt[4]{b_j}, (1+\sqrt{-1})\sqrt[4]{b_k}, (1-\sqrt{-1})\sqrt[4]{b_l})$$

where $i \in \mathscr{A}_1 \cup \mathscr{B}_2$, $j \in \mathscr{A}_2 \cup \mathscr{B}_1$, $k \in \mathscr{C}_1 \cup \mathscr{D}_2$ and $l \in \mathscr{C}_2 \cup \mathscr{D}_1$.

Acknowledgements. Professor T.Y. Lam made a large number of comments which improved the exposition beyond what the authors could possibly do by themselves. We are very indebted to him.

References

[A] Artin, E.: Algebraic numbers and algebraic functions. New York: Gordon and Breach 1967

[AT] Artin, E., Tate, J.: Class field theory. New York: Benjamin 1967

[Bec] Becker, E.: Euklidische Körper und euklidische Hüllen von Körpern. J. Reine Angew. Math. **268/269**, 41–52 (1974)

[Ber] Berman, L.: The Kaplansky radical and values of binary quadratic forms. Ph.D. thesis, Berkeley 1979

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

[F] Fröhlich, A.: Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants. J. Reine Angew. Math. **360**, 84–123 (1985)

[L1] Lam, T.Y.: The algebraic theory of quadratic forms. Reading, Mass.: Benjamin/Addison-Wesley 1973

[L2] Lam, T.Y.: Orderings, valuations and quadratic forms. Conf. Board of the Mathematical Sciences. Am. Math. Soc., vol. 52, 1983

[L3] Lam, T.Y.: Ten lectures in quadratic forms over fields. Queen's Pap. Pure Appl. Math. **46**, 1–102 (1977)

[MM] Mináč, J., Mahé, L.: Generalized orderings and *W*-groups (in preparation)

[MS] Mináč, J., Spira, M.: Witt rings and Galois groups (in preparation)

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