PACIFIC JOURNAL OF MATHEMATICS
Vol. 76, No. 2, 1978

WHEN ARE WITT RINGS GROUP RINGS? II

ROGER WARE

It is known that if F is a superpythagorean field or a nonformally real field with (finite) u-invariant equal to the number of square classes then the Witt ring of quadratic forms over F is isomorphic to a group ring $Z/nZ[G]$ with $n = 0, 2$, or 4 and G a subgroup of the group of square classes of F. In this paper, we investigate those fields with Witt ring isomorphic to a group ring $Z/nZ[G]$ for some $n \geqq 0$ and some group G. It is shown that G is necessarily of exponent 2 and such a field is either superpythagorean or is not formally real with level (Stufe) $s(F) = 1$ or 2 (so $n = 0, 2$, or 4). Characterizations of these fields will be given both in terms of the behavior of their quadratic forms and the structure of their Galois 2-extensions.

1. Fields whose Witt rings are group rings. In notations and terminology we primarily follow [11]. All fields F will have characteristic different from two, $\dot{F}$ denotes the multiplicative group of F, $\dot{F}^2$ the subgroup of nonzero squares, and for a in $\dot{F}$, $[a]$ will denote the image of a in the group of square classes $Q(F) = \dot{F}/\dot{F}^2$. If ϕ is a quadratic form over F then the value set of ϕ is $D_F(\phi) = \{[a] \in Q(F) \mid a$ is represented by $\phi\}$. Isometries of quadratic forms will be written $\cong$ and $\phi \perp \psi$, $\phi \otimes \psi$ will denote, respectively, the orthogonal sum and tensor product of two forms ϕ and ψ. We will write $\phi = \langle a_1, a_2, \cdots, a_n\rangle$ to mean that ϕ has an orthogonal basis $e_1, e_2, \cdots, e_n$ with $\phi(e_i) = a_i \in \dot{F}$. In this case the determinant of ϕ is $\det \phi = [a_1 a_2 \cdots a_n] \in Q(F)$. The Witt ring of quadratic forms over F is denoted by $W(F)$.

The mapping $[a] \to \langle a\rangle$ identifies $Q(F)$ with a subgroup of units of $W(F)$ and induces a surjective ring homomorphism Ψ from the integral group ring $\boldsymbol{Z}[Q(F)]$ onto $W(F)$. Then $\Psi(\boldsymbol{Z}) = \boldsymbol{Z}/n\boldsymbol{Z}$ for some integer n and by a theorem of Pfister, F is not formally real if and only if $n > 0$. When this happens, $n = 2s$ where $s = s(F)$ is the least positive integer such that -1 is a sum of s squares in F. The integer $s(F)$ is called the level (Stufe) of F and is a power of 2. We will adopt the convention that $s(F) = 0$ for a formally real field F. Thus for any field F with level s, $W(F)$ is a $\boldsymbol{Z}/2s\boldsymbol{Z}$-algebra.

PROPOSITION 1.1 (*Compare* [11, *Exercise* 8, p. 335]). *Let F be a field and n a natural number. If $W(F)$ is a free $\boldsymbol{Z}/n\boldsymbol{Z}$-module then $n = 2s(F)$ and $s(F) = 0, 1$, or 2.*

Proof. Let $s = s(F)$. The equality $n = 2s$ follows immediately from the freeness assumption together with the fact that if $s > 0$ then the additive order of 1 in $W(F)$ is $2s$. Now assume $s > 0$. Then every odd dimensional form is a unit in $W(F)$. But any $\boldsymbol{Z}/n\boldsymbol{Z}$-basis for $W(F)$ necessarily contains an odd dimensional form so by multiplying the basis elements by its inverse we can find a basis $\{\phi_i\}_{i \in I}$ containing the form $\langle 1\rangle$. If $D_F(\langle 1, 1\rangle) \subset \{[1], [-1]\}$ then $s \leqq 2$ so we may suppose there exists $[a]$ in $D_F(\langle 1, 1\rangle)$ with $[a] \neq 1$, $[-1]$. There exist basis elements $\phi_1, \cdots, \phi_k$ and integers $n_1, \cdots, n_k$ such that $\langle -a\rangle = \sum_{i=1}^{k} n_i\phi_i$ in $W(F)$. By comparing determinants, we see that there exists an index j such that n_j is odd and $\det \phi_j \neq 1$, $[-1]$. Since $[a] \in D_F(\langle 1, 1\rangle)$, $2\langle 1\rangle + 2\langle -a\rangle = 0$ in $W(F)$ and hence $2\langle 1\rangle + \sum_{i=1}^{k} 2n_i\phi_i = 0$. Then the linear independence of the ϕ_i's forces $2n_j \equiv 0 \pmod{2s}$ which implies that the level s of F divides the odd integer n_j. Thus $s = 1$.

As a consequence of the foregoing proof we have

COROLLARY 1.2. *Let F be a field such that $W(F)$ is a free $\boldsymbol{Z}/n\boldsymbol{Z}$-module with $n \neq 2$. Then $D_F(\langle 1, 1\rangle) \subset \{1, [-1]\}$ with equality if and only if $n = 4$.*

PROPOSITION 1.3. *Let F be a field, G a group, and $n \geqq 0$. If $W(F) \cong \boldsymbol{Z}/n\boldsymbol{Z}[G]$ then G is a group of exponent 2.*

Proof. We may assume G is a subgroup of units of $W(F)$ which is also a $\boldsymbol{Z}/n\boldsymbol{Z}$-basis for $W(F)$. If $n = 0$ then for any $g \in G$ and any homomorphism $\sigma\colon W(F) \to \boldsymbol{Z}$, $\sigma(g^2) = 1$ so since $W(F) = \boldsymbol{Z}[G]$ is torsion free, $g^2 = 1$. If $n > 0$ then $n = 2s$ with $s = s(F) = 1$ or 2 and any element g in G can be written $g = 1 + \phi$ with $\dim \phi$ even. Then $g^2 = 1 + 2\phi + \phi^2$ and $\phi^2 = 2\phi'$ for some form ϕ'. Now 1 and g^2 are in the basis G, $s \neq 0$ in $\boldsymbol{Z}/n\boldsymbol{Z}$, and $s \cdot 1 + s \cdot g^2 = s \cdot 1 + s(1 + 2\phi + 2\phi') = 2s + 2s(\phi + \phi') = 0$ forcing $g^2 = 1$.

We now record a result which will be used several times throughout the paper.

Exact Sequence 1.4 [11, Th. 3.4, p. 202]. For a quadratic extension $K = F(\sqrt{d})$, the following sequence is exact

$$1 \longrightarrow \{1, [d]\} \longrightarrow Q(F) \xrightarrow{\varepsilon} Q(K) \xrightarrow{N} Q(F)\ .$$

Here, ε is the map induced by inclusion, and N is the homomorphism induced by the norm $N_{K/F}$.

THEOREM 1.5. *For a field F the following statements are equivalent.*

(1) $W(F) \cong Z/nZ[G]$ *for some integer* $n > 0$ *and some group* G.

(2) $W(F) = Z/nZ[H]$ *where either* $n = 2$ *and* $H = Q(F)$ *or* $n = 4$ *and* H *is a subgroup of index* 2 *in* $Q(F)$ *with* $[-1] \notin H$.

(3) *For every binary anisotropic form* β, $|D_F(\beta)| = 2$.

(4) *For every quadratic extension* K *of* F, *the image of* $\varepsilon\colon Q(F) \to Q(K)$ *has index* 2 *in* $Q(K)$.

(5) F *is not formally real and* $|D_F(\phi)| \leqq \dim \phi$ *for all anisotropic forms* ϕ.

(6) $|D_F(\phi)| = \dim \phi$ *for all anisotropic forms* ϕ.

(7) *For every finite subset* S *of* $Q(F)$ *there exists an anisotropic form* ϕ *such that* $D_F(\phi) = S$.

(8) *For every finite subgroup* H *of* $Q(F)$ *there exists an anisotropic form* ϕ *such that* $D_F(\phi) = H$.

(9) F *is not formally real and* $D_F(\langle 1, a\rangle) = \{1, [a]\}$ *for all* $[a] \neq 1, [-1]$.

(10) *The Kernel of the mapping* $\Psi\colon Z[Q(F)] \to W(F)$ *is the ideal generated by* $1 + [-1]$ *and* $2(1 - [-1])$. *Moreover,* $1 + [-1]$ *generates* $\operatorname{Ker}\Psi$ *if and only if* $s(F) = 1$.

REMARKS. 1. If $Q(F)$ is finite then we recover the $\bar{C}$ fields introduced in [5] and also studied in [16].

2. If F is a field satisfying statement (6), and hence statement (3), of Theorem 1.5 then $s(F) = 1$ or 2. In particular, F is not formally real. Moreover, if $s(F) \neq 1$ then $D_F(\langle a, a\rangle) = \{[a], [-a]\}$ for all a in $\dot{F}$. Indeed, if $\langle a, a\rangle$ is isotropic then $s(F) = 1$ and if $\langle a, a\rangle$ is anisotropic and $[b] \in D_F(\langle a, a\rangle)$ with $[b] \neq [a]$ then $\langle a, -b\rangle \cong \langle b, -a\rangle$ is anisotropic. If $[b] \neq [-a]$ then $|D_F(\langle b, -a\rangle)| = 2$ implies that $\{[a], [-b]\} = \{[b], [-a]\}$ which is impossible. Thus $D_F(\langle a, a\rangle) = \{[a], [-a]\}$ and $s(F) = 2$.[1]

Proof. We will prove the equivalence of the statements (2) through (10) and then, with the help of two lemmata, show that these are equivalent to (1).

(2) $\Rightarrow$ (3). If $n = 2$ and $H = Q(F)$, this is obvious. Thus suppose $n = 4$, $(Q(F)\colon H) = 2$, $[-1] \notin H$, and let $\beta = \langle a, b\rangle$ be anisotropic over F. If $[c] \in D_F(\langle a, b\rangle)$ then $\langle a\rangle + \langle b\rangle = \langle c\rangle + \langle cab\rangle$ in $W(F)$. If $\langle a\rangle = \langle b\rangle$ then $2\langle -a\rangle = 2\langle a\rangle = 2\langle c\rangle = 2\langle -c\rangle$ so $[c] \in \{[a], [-a]\}$ and $|D_F(\langle a, b\rangle)| = 2$. Next suppose $2\langle a, b\rangle = 0$ in $W(F)$. Then $2\langle \pm a\rangle + 2\langle \pm b\rangle = 0$ so, since $\langle a, b\rangle$ is anisotropic, $\langle a\rangle = \langle b\rangle$. Finally, using the relation $\langle x\rangle = -\langle -x\rangle$, we can rewrite $\langle a\rangle + \langle b\rangle = \langle c\rangle + \langle cab\rangle$

[1] I would like to express my thanks to the referee for pointing out an error in the original version of this remark.

as $n_1x + n_2y = n_3u + n_4v$ with $x = \langle \pm a \rangle$, $y = \langle \pm b \rangle$, $u = \langle \pm c \rangle$, $v = \langle \neq cab \rangle$, $n_i = \pm 1$, and $x, y, u, v \in H$. If $u = \pm v$ then $\langle c \rangle = \langle \pm cab \rangle$ so $\langle ab \rangle = \langle 1 \rangle$ and $\langle a \rangle = \langle b \rangle$. If $u = x$ or $u = y$ then $\langle c \rangle \in \{\langle a \rangle, \langle -a \rangle, \langle b \rangle, \langle -b \rangle\}$. If $\langle c \rangle = \langle -a \rangle$ or $\langle -b \rangle$ then $\langle a, b \rangle \cong \langle -a, -b \rangle$ whence $2\langle a, b \rangle = 0$ and $\langle a \rangle = \langle b \rangle$ as before. Thus, either $[a] = [b]$ and $D_F(\langle a, a \rangle) = \{[a], [-a]\}$ or $[a] \neq [b]$ and $D_F(\langle a, b \rangle) = \{[a], [b]\}$, proving (3).

The equivalence of (3) and (4) is a consequence of the exact sequence 1.4.

(3) $\Rightarrow$ (5). By Remark 2 above, F is not formally real and the proof that $|D_F(\phi)| \leqq \dim \phi$ is contained in the proof of Theorem 3.3 (iii) in [5].

(5) $\Rightarrow$ (6). If F is not formally real, a well known theorem of Kneser implies that $|D_F(\phi)| \geqq \dim \phi$ for any anisotropic form ϕ.

(6) $\Rightarrow$ (7). Let $S = \{[a_1], \cdots, [a_n]\}$ with $[a_1], \cdots, [a_n]$ distinct elements of $Q(F)$. Inductively, we can find an anisotropic form ψ with $D_F(\psi) = \{[a_1], \cdots, [a_{n-1}]\}$. By (6), $\dim \psi = n - 1$. Let $\rho = \psi \perp \langle a_n \rangle$. If ρ is anisotropic then (6) implies that $D_F(\rho) = S$ so we can take $\phi = \rho$. If ρ is isotropic then $[a_n] = [-a_i]$ for some $i \leqq n - 1$. Then $s(F) > 1$ and $\phi = \psi \perp \langle -a_n \rangle$ is anisotropic. Now $[a_1], \cdots, [a_{n-1}] \in D_F(\phi)$ so by (6) we need only show $[a_n] \in D_F(\phi)$. But $[-a_n] = [a_i]$ is in $D_F(\psi)$ so ϕ contains the subform $\langle -a_n, -a_n \rangle$ and Remark 2 above implies that $D_F(\langle -a_n, -a_n \rangle) = \{[-a_n], [a_n]\}$, proving (7).

The implication (7) $\Rightarrow$ (8) is obvious, and the proof of (8) $\Rightarrow$ (9) can be found in the proof of Proposition 5.10 of [5].

(9) $\Rightarrow$ (10). As is well known, the Kernel of Ψ is the ideal generated by $1 + [-1]$ and all elements of the form $g(a, x, y) = (1 + [a])(1 - [x^2 + ay^2])$ with $x, y \in F$ and $a, x^2 + ay^2 \in \dot{F}$. If $a \neq 1$, $[-1]$ then $[x^2 + ay^2] \in \{1, [a]\}$ which implies $g(a, x, y) = 0$. If $[a] = 1$ then $[x^2 + ay^2] \in D_F(\langle 1, 1 \rangle)$ so that $\langle 1, -(x^2 + ay^2) \rangle \cong \langle -1, x^2 + ay^2 \rangle$. Now if $[x^2 + ay^2] \neq 1, [-1]$ then $D_F(\langle 1, -(x^2 + ay^2) \rangle) = \{1, [-(x^2 + ay^2)]\}$ which forces $[-1] = 1$. Thus either $1 = [-1]$ and $1 + [-1]$ is the only generator of $\operatorname{Ker} \Psi$ or $1 \neq [-1]$ and $D_F(\langle 1, 1 \rangle) \subset \{1, [-1]\}$. Since F is not formally real we cannot have $D_F(\langle 1, 1 \rangle) = \{1\}$. Hence if $1 \neq [-1]$ then there exist x, y in F such that $g(1, x, y) = (1 + 1)(1 - [-1]) = 2(1 - [-1])$.

To prove the last statement of (10), suppose $1 + [-1]$ is the only generator of $\operatorname{Ker} \Psi$. Then there exists x in $\boldsymbol{Z}[Q(F)]$ such that $2(1 - [-1]) = (1 + [-1])x$. If $1 \neq [-1]$ then there exists a group homomorphism $\sigma \colon Q(F) \rightarrow \{1, -1\} \subset \boldsymbol{Z}$ such that $\sigma([-1]) = -1$. Then σ extends to a ring homomorphism $\bar{\sigma} \colon \boldsymbol{Z}[Q(F)] \rightarrow \boldsymbol{Z}$ and $\bar{\sigma}(2(1 - [-1])) = 4$, $\bar{\sigma}((1 + [-1])x) = 0$. Thus $1 = [-1]$, i.e., $s(F) = 1$.

(10) $\Rightarrow$ (2). If $1 + [-1]$ is the only generator, this is proved in [16, Proposition]. Thus assume $1 \neq [-1]$ and $1 + [-1]$ and $2(1 - [-1])$

generate the ideal Ker Ψ. Let $\Psi(Z) = Z/nZ$, $n \geqq 0$, and let H be any subgroup of $Q(F)$ with $[-1] \notin H$. Now $4=2(1+[-1])+2(1-[-1])$ so $4 = 0$ in $W(F)$. Since $1 \neq [-1]$ it follows that $n = 4$. Moreover, in $Z/4Z[Q(F)]$, $2(1 - [-1]) = 2(1 + [-1])$ so the Kernel of the induced map $\bar{\Psi}: Z/4Z[Q(F)] \rightarrow W(F)$ is generated by $1 + [-1]$. The remainder of the proof is the same (with Z replaced by Z/nZ) as the proof of the implication (v) $\Rightarrow$ (vi) in Theorem 1 of [15].

To complete the proof of Theorem 1.5 we need the following

LEMMA 1.6. *Let G be a group of exponent 2 and F_0 a field. Then there exists a field F containing F_0 and a $W(F_0)$-algebra isomorphism $W(F_0)[G] \rightarrow W(F)$ sending G onto a subgroup of $Q(F)$.*

Proof. Let I be a basis for G. Well order I with ordering $<$ and for each finite subset $J = \{i_1, \cdots, i_r\}$ of I with $i_1 < \cdots < i_r$, let F_J be the iterated formal power series field $F_0((t_{i_1})) \cdots ((t_{i_r}))$. If $J_1 \subset J_2$ are finite subsets of I then we have an inclusion $F_{J_1} \hookrightarrow F_{J_2}$ sending the indeterminate t_i to the corresponding indeterminate t_i' for $i \in J_1 \subset J_2$. These inclusion give rise to a directed system of fields. Let F be the direct limit of this system. We will regard F as the union of subfields $F_0((t_{i_1})) \cdots ((t_{i_n}))$, $i_1 < i_2 < \cdots < i_n$.

For each finite subset J of I, let G_J be the subgroup of G spanned by J. By a theorem of T. A. Springer, the correspondence $i \leftrightarrow \langle t_i \rangle$, $i \in J$, induces an isomorphism $W(F_0)[G_J] \cong W(F_J)$. If $J_1 \subset J_2$ are finite then any anisotropic form over F_{J_1} remains anisotropic over F_{J_2} and, since F is the union of the F_J's it follows that the map $W(F_J) \rightarrow W(F)$is injective for all finite subsets $J \subset I$. Hence the composite maps $W(F_0)[G_J] \overset{\cong}{\rightarrow} W(F_J) \hookrightarrow W(F)$ induce an isomorphism $W(F_0)[G] \overset{\cong}{\rightarrow} W(F)$, sending $g \in G$ to $\langle t_g \rangle \in Q(F)$.

LEMMA 1.7. *If $W(F) = Z/nZ[H]$ with $H \subset Q(F)$ then either $n = 2$ and $H = Q(F)$ or $n \in \{0, 4\}$ and $(Q(F): H) = 2$. Moreover, in the second case $[-1] \notin H$.*

Proof. By Proposition 1.1, $n = 0, 2$, or 4. By taking determinants we see that $n = 2$ if and only if $H = Q(F)$ while $n \in \{0, 4\}$ if and only if $(Q(F): H) = 2$. If $n = 0$ or 4 then the relation $\langle 1 \rangle + \langle -1 \rangle = 0$ implies that $\langle -1 \rangle \notin H$.

Now suppose statement (1) of Theorem 1.5 holds. By Propositions 1.1 and 1.3 we can write $W(F) = Z/nZ[G]$ where $n = 2s$ with $s = s(F) = 1$ or 2 and G is a group of exponent 2. Let $F_0 = C$ if $n = 2$ and $F_0 = F_3$ if $n = 4$. Then $W(F_0) = Z/nZ$ so by Lemma 1.6, there is a field K and an isomorphism $W(F) \rightarrow W(K)$ which maps G

onto a subgroup H of $Q(K)$. Then $W(K) = \boldsymbol{Z}/n\boldsymbol{Z}[H]$ and by Lemma 1.7, K satisfies statement (2) and hence statement (3) of Theorem 1.5. Since the implication $(2) \Rightarrow (1)$ is obvious, the proof will be complete if we can show that F also satisfies statement (3). By [10, Theorem, p. 21] or [11, Ex. 13, p. 294], there is an isomorphism $t: Q(F) \rightarrow Q(K)$ such that $t([-1]) = [-1]$ and $t(D_F(\langle a, b\rangle)) = D_K(\langle ta, tb\rangle)$. Thus if $\beta = \langle a, b\rangle$ is anisotropic over F then $\langle ta, tb\rangle$ is anisotropic over K so $|D_F(\beta)| = |t^{-1}(D_K(\langle ta, tb\rangle))| = |D_K(\langle ta, tb\rangle)| = 2$.

REMARKS. 1. If F satisfies the conditions of Theorem 1.5 with $n = 4$ then $W(F) = \boldsymbol{Z}/n\boldsymbol{Z}[H]$ for any subgroup H of $Q(F)$ with $(Q(F): H) = 2$ and $[-1] \notin H$.

2. It can happen that $WF = \boldsymbol{Z}/n\boldsymbol{Z}[H]$ with $H \not\subset Q(F)$. For example, let$F = \boldsymbol{F}_5((t))$. Then $W(F) = \boldsymbol{Z}/2\boldsymbol{Z}[H]$ with

$$H = \{1, \langle 1, 2, t\rangle, \langle 1, t, 2t\rangle, \langle 1, 2, 2t\rangle\} .$$

PROPOSITION 1.8. *For a formally real field the following statements are equivalent.*

(1) $W(F) \cong \boldsymbol{Z}[G]$ *for some group* G.

(2) $W(F) = \boldsymbol{Z}[H]$ *where* H *is a subgroup of index* 2 *in* $Q(F)$ *not containing* $[-1]$.

(3) *If* $\phi = \langle a_1, \cdots, a_n\rangle$ *is anisotropic with* $[a_1], \cdots, [a_n]$ *distinct in* $Q(F)$ *then* $D_F(\phi) = \{[a_1], \cdots, [a_n]\}$.

(4) *If* H *is a finite subgroup of* $Q(F)$ *not containing* $[-1]$ *then there exists an anisotropic form* ϕ *with* $D_F(\phi) = H$.

(5) *If* $[a[\neq 1, [-1]$ *then the image of* $\varepsilon: Q(F) \rightarrow Q(F(\sqrt{a}))$ *has index* 2.

(6) *For every formally real quadratic extension* K *of* F, $(Q(K): \operatorname{Im} \varepsilon) = 2$.

(7) *For every quadratic extension* K *of* F, $(Q(K): \operatorname{Im} \varepsilon) \leqq 2$.

(8) *For every anisotropic form* β, $|D_F(\beta)| \leqq 2$.

(9) *For every anisotropic form* ϕ, $|D(\phi)| \leqq \dim \phi$.

(10) *The Kernel of the mapping* $\Psi: \boldsymbol{Z}[Q(F)] \rightarrow W(F)$ *is the ideal generated by* $1 + [-1]$.

REMARKS. 1. Fields satisfying the equivalent conditions of Proposition 1.8 were introduced in [6] and have been studied in [1], [2], [3], [4], [7], [15], and [16]. Following Elman and Lam we will call them *superpythagorean*.

2. If K/F is a quadratic extension of fields then $\varepsilon: Q(F) \rightarrow Q(K)$ is surjective if and only if F is formally real, pythagorean, and $K = F(\sqrt{-1})$ [11, Ex. 5, p. 216].

Proof. By Proposition 1.3, the group G in (1) is necessarily of exponent 2, so the equivalence of (1), (2), and (10) can be found in [15]. The equivalence of (2) and (3) was observed in [16].

(3) $\Rightarrow$ (4). Let H be a finite subgroup of $Q(F)$ with $[-1] \notin H$. Write $H = \{[a_1], \cdots, [a_n]\}$ with $[a_1], \cdots, [a_n]$ distinct in $Q(F)$ and let $\phi = \langle a_1, \cdots, a_n \rangle$. Since (3) holds, so does (2) and hence by [15, Theorem 1] there is a signature $\sigma: W(F) \rightarrow \boldsymbol{Z}$ such that $\sigma(\langle a_i \rangle) = 1$, $i = 1, \cdots, n$. Then $\sigma(\phi) = n$ so ϕ is anisotropic. By (3), $D_F(\phi) = H$.

(4) $\Rightarrow$ (5). If $[a] \neq 1$, $[-1]$ then $[-1]$ is not in the subgroup $\{1, [-a]\}$ of $Q(F)$ so there exists an anisotropic form ϕ such that $D_F(\phi) = \{1, [-a]\}$. Write $\phi = \langle 1 \rangle \perp \phi'$. If ϕ' does not represent $-a$ then $\phi = \langle 1, 1, \cdots, 1 \rangle$ and since $D_F(\langle 1, 1 \rangle) = \{1\}$ implies that $D_F(\langle 1, \cdots, 1 \rangle) = \{1\}$ it follows that $D_F(\langle 1, 1 \rangle) = \{1, [-a]\}$. Hence $\langle 1, a \rangle \cong \langle -1, -a \rangle$, i.e., $[-1] \in D_F(\langle 1, a \rangle)$. Now choose an anisotropic form ψ such that $D_F(\psi) = \{1, [a]\}$ and write $\psi = \langle 1 \rangle \perp \psi'$. If ψ' does not represent a then, as above, we get $D_F(\langle 1, 1 \rangle) = \{1, [a]\}$ which implies that $[a] = 1$ or $[-1] = 1$. Thus $[a] \in D_F(\psi')$ so $D_F(\langle 1, a \rangle) \subset D(\psi) = \{1, [a]\}$. But then $[-1] \in D_F(\langle 1, a \rangle)$ implies that $[a] = 1$ or $[-1] = 1$. This contradiction forces $[-a] \in D_F(\phi')$ whence $D_F(\langle 1, -a \rangle) = \{1, [-a]\}$. Then the Exact Sequence 1.4 implies that the image of $\varepsilon: Q(F) \rightarrow Q(F(\sqrt{a}))$ has index 2.

(5) $\Rightarrow$ (6) is clear.

(6) $\Rightarrow$ (7). We first show F is pythagorean. Let $[a] \in D_F(\langle 1, 1 \rangle)$. Then $F(\sqrt{a})$ is formally real so if $[a] \neq 1$, the image of $\varepsilon: Q(F) \rightarrow Q(F(\sqrt{a}))$ has index 2. Thus $D_F(\langle 1, -a \rangle) = \{1, [-a]\}$. But $[a] \in D_F(\langle 1, 1 \rangle)$ so $\langle 1, -a \rangle \cong \langle -1, a \rangle$ whence $[-1] \in \{1, [-a]\}$. Since F is formally real, this forces $[a] = 1$ and F is pythagorean. Then $F(\sqrt{-1})$ is the only nonreal quadratic extension of F and by Remark 2 following the proposition, the map $Q(F) \rightarrow Q(F(\sqrt{-1}))$ is surjective. The implication (7) $\Rightarrow$ (8) follows from Exact Sequence 1.4, (8) $\Rightarrow$ (9) follows from the proof of [5, Th. 3.3] (or induction), and (9) $\Rightarrow$ (3) is obvious.

REMARK. If u is a unit in the Witt ring of a pythagorean field F then $u = \langle a \rangle$ for some $a \in \dot{F}$. Hence if $W(F) = \boldsymbol{Z}[H]$ with H a subgroup of units of $W(F)$ then $H \subset Q(F)$, $(Q(F): H) = 2$, and $[-1] \notin H$. Moreover, by [15, Th. 1], $W(F) = \boldsymbol{Z}[H']$ for any $H' \subset Q(F)$ with $[-1] \notin H'$ and $(Q(F): H') = 2$.

Combining Theorem 1.5 and Proposition 1.8 we obtain

THEOREM 1.9. *For a field F the following statements are equivalent.*

(1) $W(F) \cong \boldsymbol{Z}/n\boldsymbol{Z}[G]$ *for some integer* $n \geq 0$ *and some group* G.

(2) $W(F) = \boldsymbol{Z}/n\boldsymbol{Z}[H]$ *where either* $n = 2$ *and* $H = Q(F)$ *or*

$n \in \{0, 4\}$ and H is a subgroup of index 2 in $Q(F)$ with $[-1] \notin H$.

(3) *For every binary anisotropic form β, $|D_F(\beta)| \leqq 2$.*

(4) *For every anisotropic form ϕ, $|D_F(\phi)| \leqq \dim \phi$.*

(5) *For every finite subgroup H of $Q(F)$, with $[-1] \notin H$ if $s(F) \neq 1$, there exists an anisotropic form ϕ such that $D_F(\phi) = H$.*

(6) *For every quadratic extension K of F, the image of $\varepsilon: Q(F) \to Q(K)$ has index $\leqq 2$ in $Q(K)$.*

(7) *If $[a] \neq 1$, $[-1]$ then $D_F(\langle 1, a\rangle) = \{1, [a]\}$.*

(8) *If $\phi = \langle a_1, \cdots, a_n\rangle$ is anisotropic with $[a_1], \cdots, [a_n]$ distinct in $Q(F)$ then $D_F(\phi) = \{[a_1], \cdots, [a_n]\}$.*

(9) *The Kernel of the homomorphism $\Psi: \boldsymbol{Z}[Q(F)] \to W(F)$ is either the ideal generated by $1 + [-1]$ or the ideal generated by $1 + [-1]$ and $2(1 - [-1])$.*

DEFINITION 1.10. By a *field of class C* we will mean one which satisfies the equivalent conditions of Theorem 1.9.

EXAMPLES 1.11. (i) Any field with at most 2 square classes, e.g., a quadratically closed field, a Euclidean field, or a finite field, is a field of class C.

(ii) A formally real field is of class C if and only if it is superpythagorean.

(iii) If F is a nonformally real field with $|Q(F)| < \infty$ then F is a field of class C if and only if $|Q(F)| = u(F)$ where $u(F)$ is the u-invariant of F (see [5], [16]). In particular, nondyadic local fields are of class C.

(iv) If F is of class C and I is a totally ordered set then the field $F((t_i))_{i \in I}$ of iterated formal power series over F is a field of class C.

COROLLARY 1.12. *If $\{F_i\}_{i \in I}$ is a direct system of fields of class C then their direct limit $\varinjlim_i F_i$ is a field of class C.*

Proof. Let $F = \varinjlim_i F_i$ and let $f_i: F_i \to F$ be the natural inclusion, $i \in I$. Then $F = \bigcup_{i \in I} f_i(F_i)$ and each $f_i(F_i) \cong F_i$ is of class C so we may assume that $F = \bigcup_{i \in I} F_i$. Let $a \in F$ with $[a] \neq 1$, $[-1]$ in $Q(F)$ and let $[b] \in D_F(\langle 1, a\rangle)$. Then there exist $x, y \in F$ such that $b = x^2 + ay^2$. Choose $i \in I$ such that $a, b, x, y \in F_i$. Then $[a] \neq 1$, -1 in $Q(F_i)$ and $[b] \in D_{F_i}(\langle 1, a\rangle)$. Since F_i is of class C, $[b] = 1$ or $[a]$.

2. Going up and going down.

THEOREM 2.1 (*Going down*). *Let K/F be a finite extension of* *fields. If K is a field of class C then so is F.*

The following result of Elman and Lam will be crucial in the proof of Theorem 2.1.

Norm Principle [9, 2.11]. Let K/F be a quadratic extension and let $N: K \to F$ denote the norm. Let $x \in K$ and let ϕ be a form over F. If $\langle N(x)\rangle\phi \cong \phi$ over F then $\langle x\rangle\phi_K \cong \tau_K$ over K for some form τ over F.

Proof of Theorem 2.1. We proceed by induction on $[K: F]$. By the induction assumption we may assume that there is no field L with $F \subsetneqq L \subsetneqq K$. First suppose $[K: F] > 2$. Let $\langle 1, a\rangle$, $[a] \neq 1$, be an anisotropic form over F and let $[b] \in D_F(\langle 1, a\rangle)$. Since K contains no quadratic extension of F, $\langle 1, a\rangle$ remains anisotropic over K and $[a] \neq 1$ in K. Hence $D_K(\langle 1, a\rangle) = \{1, [a]\}$. Thus, in $Q(K)$, $[b] = 1$ or $[a]$, whence $[b] = 1$ or $[a]$ in $Q(F)$.

Thus we are left with the case $K = F(\sqrt{a})$ where $[a] \neq 1$. Let $\varepsilon: Q(F) \to Q(K)$ be the natural map. If ε is surjective then F is formally real, pythagorean, and $K = F(\sqrt{-1})$. If $b \in F$ with $[b] \neq 1$, $[-1]$ then $\langle 1, b\rangle$ is anisotropic over K so $D_K(\langle 1, b\rangle) = \{1, [b]\}$. Hence $D_F(\langle 1, b\rangle) \subset \{1, [-1], [b], [-b]\}$. If $[-1] \in D_F(\langle 1, b\rangle)$ then $\langle 1, b\rangle \cong \langle -1, -b\rangle$ over F which forces $2\langle 1, b\rangle = 0$ in $W(F)$. Since F is pythagorean, this implies $[b] = [-1]$. Hence $D_F(\langle 1, b\rangle) = \{1, [b]\}$ and F is superpythagorean.

Now suppose ε is not surjective and choose $[x] \in Q(K)$, $[x] \notin \operatorname{Im} \varepsilon$. Let $N: K \to F$ be the norm. Since $\langle N(x)\rangle\langle 1, N(x)\rangle \cong \langle 1, N(x)\rangle$ over F, it follows from the Norm Principle of Elman-Lam, that there are c, d in F such that $\langle x\rangle\langle 1, N(x)\rangle \cong \langle c, d\rangle$ over K. If $\langle c, d\rangle$ were anisotropic over K then either $D_K(\langle c, d\rangle) = \{[c], [d]\}$ if $[c] \neq [d]$ in $Q(K)$ or $D_K(\langle c, d\rangle) \subset \{[c], [-c]\}$ if $[c] = [d]$. Since $[x] \notin \operatorname{Im} \varepsilon$, $\langle c, d\rangle$ and hence $\langle 1, N(x)\rangle$ must be isotropic over K. Hence $[N(x)] = [-1]$ in $Q(K)$ and so $[N(x)] \in \{[-1], [-a]\}$ in $Q(F)$.

Case 1. $[N(x)] = [-1]$. Then $[N(x\sqrt{a})] = [a]$ in $Q(F)$, and since $\langle a\rangle\langle 1, a\rangle \cong \langle 1, a\rangle$, the Norm Principle applies to find c, d in F with $\langle x\sqrt{a}\rangle\langle 1, a\rangle \cong \langle c, d\rangle$ over K. If $\langle 1, a\rangle$ is anisotropic over K then $[x\sqrt{a}] \in \operatorname{Im} \varepsilon$, which implies, via Exact Sequence 1.4, that $[a] = 1$ in $Q(F)$. Thus $\langle 1, a\rangle$ is isotropic over K, i.e., $s(K) = 1$. Since $[x] \notin \operatorname{Im} \varepsilon$ and $[N(x)] = [-1]$ in $Q(F)$, $s(F) \neq 1$. Thus $K = F(\sqrt{-1})$. Now choose $b \in F$ with $[b] \neq 1$, $[-1]$. Then $[b] \neq 1$, $[-1]$ in K so $\langle 1, b\rangle$ is anisotropic over K and $D_K(\langle 1, b\rangle) = \{1, [b]\}$. Then $D_F(\langle 1, b\rangle) \subset \{1, [-1], [b], [-b]\}$ and if $[-1] \in D_F(\langle 1, b\rangle)$ then the Norm Principle yields c, d in F with $\langle x\rangle\langle 1, b\rangle \cong \langle c, d\rangle$ over K. This is impossible, because $\langle 1, b\rangle$ is anisotropic over K and $[x] \notin \operatorname{Im} \varepsilon$. Thus $D_F(\langle 1, b\rangle) = \{1, [b]\}$.

Case 2. $[N(x)] = [-a]$. If there exists $[y]$ in $Q(K)$ with $[y] \notin \operatorname{Im} \varepsilon$ and $[N(y)] = [-1]$ then we have returned to Case 1. Thus we can assume $[N(y)] = [-a]$ for all $y \notin \operatorname{Im} \varepsilon$. Thus $D_F(\langle 1, -a\rangle) = \{1, [-a]\}$. Now let $[b] \neq 1, [-1]$. If $\langle 1, b\rangle$ is isotropic over K then $[b] \in \{[-1], [-a]\} \subset Q(F)$ and so $[b] = [-a]$. Thus $D_F(\langle 1, b\rangle) = \{1, [b]\}$. If $\langle 1, b\rangle$ is anisotropic over K then $D_F(\langle 1, b\rangle) \subset \{1, [a], [b], [ab]\}$. If $[a] \in D_F(\langle 1, b\rangle)$ then $[-b] \in D_F(\langle 1, -a\rangle) = \{1, [-a]\}$. Hence $[b] = [a]$ and $D_F(\langle 1, b\rangle) \subset \{1, [a], [b], [ab]\} = \{1, [b]\}$.

COROLLARY 2.2. *If G is a finite group of automorphisms of a field K of class C then K^G is also of class C.*

Our next objective is to show that a quadratic extension of a field of class C is also of class C. For any extension K/F of fields, let $\varepsilon: Q(F) \to Q(K)$ and $i: W(F) \to W(K)$ be the natural maps and let $N: K \to F$ denote the norm.

PROPOSITION 2.3. *Let K/F be a quadratic extension of fields and let $R = \operatorname{Im} i$. If F is a field of class C then $W(K)$ is a free R-module of rank $\leqq 2$. If $[b]$ is any element in $Q(K)$ with $[b] \notin \operatorname{Im} \varepsilon$ then $\{1, \langle b\rangle\}$ is an R-basis for $W(K)$.*

The proof of Proposition 2.3 requires two lemmata.

LEMMA 2.4. *Let F be a field of class C and let ϕ be an anisotropic form over F.*

(1) *If $[a] \neq 1, [-1]$ and $\langle 1, a\rangle\phi = 0$ in $W(F)$ then there exists a form ψ such that $\phi \cong \langle 1, -a\rangle \otimes \psi$.*

(2) *If $s(F) \neq 1$ and $2\phi = 0$ then $\phi = 2\psi$ for some form ψ.*

Proof. (1) By [8, Cor. 2.3], we can write $\phi \cong \beta_1 \perp \cdots \perp \beta_r$ where each β_i is binary and $\langle 1, a\rangle\beta_i = 0$ in $W(F)$. If there exists an i such that $\beta_i = \langle b, b\rangle$ then $D_F(\beta_i) = \{[b], [-b]\}$ so $\langle -a\rangle\beta_i \cong \beta_i$ implies $[-a] \in \{1, [-1]\}$. Thus $\beta_i = \langle c_i, d_i\rangle$ with $[c_i] \neq [d_i]$. Then $D_F(\beta_i) = \{[c_i], [d_i]\}$ and $[-ac_i] \in \{[c_i], [d_i]\}$. Since $[a] \neq [-1]$, $[-ac_i] = [d_i]$. Thus $\langle c_i, d_i\rangle = \langle c_i\rangle\langle 1, -a\rangle$ and $\phi \cong \langle 1, -a\rangle \otimes \langle c_1, \cdots, c_r\rangle$.

(2) Write $\phi \cong \beta_1 \perp \cdots \perp \beta_r$ with $\beta_i = \langle c_i, d_i\rangle$ and $2\beta_i = 0$ in $W(F)$. Then $\langle c_i, d_i\rangle = \langle -c_i, -d_i\rangle$. Since β_i is anisotropic and $s(F) \neq 1$ it follows that $[c_i] = [d_i]$. Hence $\phi = 2\langle c_1, \cdots, c_r\rangle$.

LEMMA 2.5. *Let K/F be a quadratic extension of fields with F a field of class C and let $R = \operatorname{Im} i$. If $[b] \in Q(K) - \operatorname{Im} \varepsilon$ and $\phi \in R$ then $\langle b \rangle \phi = \phi$ in $W(K)$ implies $\phi = 0$.*

Proof. Write $K = F(\sqrt{a})$ with $a \in F$. Since $[b] \notin \operatorname{Im} \varepsilon$ and $[N(b)] \in D_F(\langle 1, -a \rangle)$ it follows that $[N(b)] = [-a]$ if $[a] \neq [-1]$ and $[N(b)] = [-1]$ if $[a] = [-1]$. Let ρ be an anisotropic form over F such that $\rho_K = \phi$ in $W(K)$. Then $\langle b \rangle \rho_K \cong \rho_K$ over K so by Scharlau's Norm Principle [11, Th. 4.3], $\langle N(b) \rangle \rho \cong \rho$ over F. Thus either $\langle 1, a \rangle \rho = 0$ if $[a] \neq [-1]$ or $2\rho = 0$ if $[a] = [-1]$. In the first case, Lemma 2.4(i) implies that $\rho \cong \langle 1, -a \rangle \otimes \psi$ for some form ψ so $\phi = \rho_K = 0$ in $W(K)$ and in the second case, $s(F) \neq 1$ so $\rho = 2\psi$ for some ψ which implies that $\phi = \rho_K = 0$ in $W(K)$, $K = F(\sqrt{-1})$.

To prove Proposition 2.3, we may suppose $\operatorname{Im} \varepsilon \neq Q(K)$. Choose $[b] \in Q(K) - \operatorname{Im} \varepsilon$ and suppose ϕ, ψ are elements of R such that $\phi + \psi \langle b \rangle = 0$ in $W(K)$. Let $\tau = \phi - \psi \in R$. Then $\langle b \rangle \tau = \langle b \rangle \phi - \langle b \rangle \psi = \langle b \rangle \phi + \phi = -\psi + \phi = \tau$ so by Lemma 2.5, $\phi = \psi$. But then $\langle -b \rangle \phi = \phi$ and $[-b] \notin \operatorname{Im} \varepsilon$ so $\phi = 0$, proving that 1, $\langle b \rangle$ are R-linearly independent. By Theorem 1.9, $(Q(K) : \operatorname{Im} \varepsilon) = 2$ so the set $\{1, \langle b \rangle\}$ generates $W(K)$ as an R-module.

PROPOSITION 2.6. *Let F be a field of class C, let $n = 2s(F)$, let $K = F(\sqrt{a})$ be a quadratic extension of F, and let $R = \operatorname{Im} i$.*

(1) *If $s(K) = 1$ then $R = \boldsymbol{Z}/2\boldsymbol{Z}[\operatorname{Im} \varepsilon]$. Moreover, if $K = F(\sqrt{-1})$ then $R \cong \boldsymbol{Z}/2\boldsymbol{Z}[H]$ where H is any subgroup of index 2 in $Q(F)$ with $[-1] \notin H$.*

(2) *If $s(K) \neq 1$ then $R = \boldsymbol{Z}/n\boldsymbol{Z}[\varepsilon(H)]$ where H is a subgroup of index 2 in $Q(F)$ with $[a] \in H$ and $[-1] \notin H$.*

(3) *i is surjective if and only if $W(K) = \boldsymbol{Z}/2\boldsymbol{Z}[\operatorname{Im} \varepsilon]$ if and only if $K = F(\sqrt{-1})$ with F superpythagorean.*

Proof. First assume $K = F(\sqrt{a})$ with $[a] \neq [-1]$. Then we can find a subgroup H of $Q(F)$ with $[a] \in H$ and $W(F) = \boldsymbol{Z}/n\boldsymbol{Z}[H]$. Then the exact sequence $1 \to \{1, [a]\} \to H \xrightarrow{\varepsilon} \varepsilon(H) \to 1$ induces an exact sequence

$$0 \longrightarrow (1 - \langle a \rangle)\boldsymbol{Z}/n\boldsymbol{Z}[H] \longrightarrow \boldsymbol{Z}/n\boldsymbol{Z}[H] \longrightarrow \boldsymbol{Z}/n\boldsymbol{Z}[\varepsilon(H)] \longrightarrow 0$$

which, together with the exact sequence

$$0 \longrightarrow (1 - \langle a \rangle) W(F) \longrightarrow W(F) \longrightarrow R \longrightarrow 0$$

shows that $R = \boldsymbol{Z}/n\boldsymbol{Z}[\varepsilon(H)]$.

Now $[a] \neq [-1]$ implies that $s(F) = s(K)$ by 1.9(2). Thus if $s(K) = 1$ then $n = 2$, $H = Q(F)$, and $\varepsilon(H) = \operatorname{Im} \varepsilon$ and if $s(K) \neq 1$ then $s(F) \neq 1$ so $[-1] \notin H$ and $(Q(F)\colon H) = 2$. This proves (2) and part of (1).

If $K = F(\sqrt{-1})$, let H be any subgroup of $Q(F)$ with $[-1] \notin H$. Then $W(F) = \boldsymbol{Z}/n\boldsymbol{Z}[H]$ and the restriction of ε to H induces an isomorphism $H \cong \varepsilon(H)$. Then from the exact sequences

$$0 \longrightarrow 2\boldsymbol{Z}/n\boldsymbol{Z}[H] \longrightarrow \boldsymbol{Z}/n\boldsymbol{Z}[H] \longrightarrow \boldsymbol{Z}/2\boldsymbol{Z}[H] \longrightarrow 0$$

$$0 \longrightarrow 2W(F) \longrightarrow W(F) \longrightarrow R \longrightarrow 0$$

we see that the natural surjection $\boldsymbol{Z}/2\boldsymbol{Z}[H] \to R$ induced by the isomorphism $H \cong \varepsilon(H)$, is an isomorphism $R = \boldsymbol{Z}/2\boldsymbol{Z}[\varepsilon(H)]$. Since $[-1] = 1$ in $Q(K)$, $\varepsilon([a]) = \varepsilon([-a])$ for any $[a] \in Q(F)$. Now either $[a]$ or $[-a]$ is in H so $\varepsilon(H) = \operatorname{Im} \varepsilon$.

Statement (3) follows from (1) and Remark 2 following the statement of Proposition 1.8.

Combining Propositions 2.3 and 2.6 we obtain

THEOREM 2.7. *Let K/F be a quadratic extension of fields with F a field of class C. Write $W(F) = \boldsymbol{Z}/n\boldsymbol{Z}[H]$ with $H \subset Q(F)$.*

(1) *If $K \neq F(\sqrt{-1})$ then $W(K) = \boldsymbol{Z}/n\boldsymbol{Z}[G]$ where G is the subgroup of $Q(K)$ generated by $\varepsilon(H)$and any element $[b]$ in $Q(K) - \operatorname{Im} \varepsilon$.*

(2) *If $K = F(\sqrt{-1})$ then $W(K) = \boldsymbol{Z}/2\boldsymbol{Z}[Q(K)]$.*

COROLLARY 2.8. *If K is a quadratic extension of a field of class C then K is also a field of class C.*

DEFINITION 2.9. By a 2-*extension of F* we mean a field K with $F \subset K \subset F(2)$ where $F(2)$ denotes the quadratic closure of F.

COROLLARY 2.10. *A 2-extension of a field of class C is again a field of class C.*

Proof. If $[K\colon F]$ is finite this follows from repeated applications of Corollary 2.8 and the general case then follows from Corollary 1.12.

COROLLARY 2.11. *Let K/F be a finite extension of fields with the same quadratic closure. Then F is a field of class C if and only if K is.*

PROPOSITION 2.12. *Let G be a finite group with no subgroup of* *index 2. Then there exists a Galois extension N/F with group G such that F is a field of class C and for all fields K with $F \subsetneqq K \subset N$, K is not a field of class C.*

Proof. As in [17, Example] or [18, Theorem 1.2] we can find a Galois extension N/F with N formally real, F Euclidean (uniquely ordered with 2 square classes), and $\mathrm{Gal}(N/F) = G$. Let K be any field with $F \subsetneqq K \subset N$. Since G has no subgroup of index 2, $[K: F] > 2$ and since the unique ordering on F has $[N: F]$ extensions to N, it must have $[K: F]$ extensions to K. Because F is uniquely ordered, a result of Prestel [12, 9.2, p. 146] states that K satisfies the Strong Approximation Property (SAP-see [7], [12]). By [7, Cors. 4.5 and 5.7] a field with more than 2 orderings which satisfies SAP cannot be superpythagorean and so K is not a field of class C.

COROLLARY 2.13. *For each integer $n \geqq 3$ there exists an extension K/F with F a field of class C, K not of class C, and $[K: F] = n$.*

We conclude this section with a result analogous to [6, Satz 4].

PROPOSITION 2.14. *For a field F with $s = s(F) \neq 1$ the following statements are equivalent.*

(1) *F is a field of class C.*

(2) *$W(K)$ is a free $\boldsymbol{Z}/2s\boldsymbol{Z}$-module for all quadratic extensions $K \neq F(\sqrt{-1})$ of F.*

(3) *$D_K(\langle 1, 1\rangle) \subset \{1, [-1]\}$ for all quadratic extensions $K \neq F(\sqrt{-1})$.*

Proof. $(1) \Rightarrow (2)$ follows from Theorem 2.7 and $(2) \Rightarrow (3)$ from Corollary 1.2.

$(3) \Rightarrow (1)$. If $[a] \neq 1$, $[-1]$ and $K = F(\sqrt{a})$ then $D_K(\langle 1, a\rangle) = D_K(\langle 1, 1\rangle) \subset \{1, [-1]\}$ so $D_F(\langle 1, a\rangle) \subset \{1, [-1], [a], [-a]\}$. If $[-a] \in D_F(\langle 1, a\rangle)$ then by Elman and Lam's Norm Principle, there exists $b \in F$ such that $\langle \sqrt{a}\rangle\langle 1, 1\rangle \cong \langle b, b\rangle$ over K. Then $[b\sqrt{a}] \in D_K(\langle 1, 1\rangle)$ so $[\sqrt{a}] \in \{[b], [-b]\} \subset \mathrm{Ker}\,(N_{K/F}: Q(K) \to Q(F))$. Since $[a] \neq [-1]$ it follows that $[-a] \notin D_F(\langle 1, a\rangle)$ and $D_F(\langle 1, a\rangle) = \{1, [a]\}$.

3. 2-extensions.

There is a close connection between the behavior of quadratic forms over a field F and the structure of the Galois group of its quadratic closure. In this section, we shall prove several results illustrating this principle in the case of fields of class C. As before, if K/F is an extension of fields then $\varepsilon = \varepsilon_{K/F}$

will denote the natural map $Q(F) \to Q(K)$ and $F(2)$ will denote the quadratic closure of F.

PROPOSITION 3.1. *F is a field of class C if and only if for every 2-extension K of F, $(Q(K): \operatorname{Im} \varepsilon) \leqq [K: F]$.*

Proof. ($\Rightarrow$) We may assume $[K: F] = 2^n$ is finite. We proceed by induction on n. If $n = 1$ this is Theorem 1.9. Thus suppose $n > 1$ and choose L with $F \subset L \subset K$ and $[L: F] = 2$. By Corollary 2.8, L is a field of class C so the induction assumption forces $(Q(K): \operatorname{Im} \varepsilon_{K/L}) \leqq 2^{n-1}$. Now $\varepsilon = \varepsilon_{K/L} \circ \varepsilon_{L/F}$ and the natural surjection $Q(L)/\operatorname{Im} \varepsilon_{L/F} \to \operatorname{Im} \varepsilon_{K/L}/\operatorname{Im} \varepsilon$ implies that $(\operatorname{Im} \varepsilon_{K/L}: \operatorname{Im} \varepsilon) \leqq (Q(L): \operatorname{Im} \varepsilon_{L/F}) \leqq 2$. Hence $(Q(K): \operatorname{Im} \varepsilon) = (Q(K): \operatorname{Im} \varepsilon_{K/L})(\operatorname{Im} \varepsilon_{K/L}: \operatorname{Im} \varepsilon) \leqq 2^n$.

($\Leftarrow$) follows from Theorem 1.9.

REMARK. For nonreal fields of class C we need not have equality. For example, if F is a finite field and K is any 2-extension of F, $K \neq F(2)$, then $(Q(K): \operatorname{Im} \varepsilon) = 2$. However, we do have the following

THEOREM 3.2. *For a field F with $-1 \notin F^2$ the following statements are equivalent.*

(1) *F is a field of class C.*

(2) *$[K: F] = [Q(K): \operatorname{Im} \varepsilon]$ for all finite Galois 2-extensions K with $-1 \notin K^2$.*

(3) *$\operatorname{Gal}(K/F)$ is a group of exponent 2 for all finite Galois 2-extensions K with $-1 \notin K^2$.*

Before proving Theorem 3.2, it will be convenient to record

LEMMA 3.3. *Let K/F be a finite Galois extension with group G. Then $[b] \in Q(K)^G$ if and only if $K(\sqrt{b})$ is Galois over F.*

Proof. Let $[b] \in Q(K)^G$. If σ is an F-homomorphism of $K(\sqrt{b})$ into the algebraic closure of F then $\sigma(K) = K$ so $\sigma(b) = bx^2$ for some x in K. Hence σ sends $\sqrt{b}$ to $\pm\sqrt{\sigma(b)} = \pm x\sqrt{b} \in K(\sqrt{b})$. Hence $K(\sqrt{b})$ is a normal extension of F. Since $K(\sqrt{b})/K$ and K/F are separable, it is a Galois extension.

Conversely, suppose $K(\sqrt{b})$ is Galois over F. Then for $\sigma \in G$, $K(\sqrt{b}) = K(\sqrt{\sigma(b)})$ so $[b] = [\sigma(b)]$ in $Q(K)$.

Proof of Theorem 3.2. (1) $\Rightarrow$ (3). Let K be a finite Galois 2-extension of F with $-1 \notin \dot{K}^2$. If $\operatorname{Gal}(K/F)$ is not of exponent 2, it contains a cyclic subgroup H of order 4. Let $L = K^H$. The unique quadratic extension of L in K has the form $L(\sqrt{x^2+y^2})$ where $x, y \in L$ and $[x^2+y^2] \neq 1$ in $Q(L)$ [11, Ex. 8(a), p. 217]. Since F is a field of class C, so is L, so $[x^2+y^2] = [-1]$. Thus $-1 \in K^2$, contrary to assumption.

$(3) \Rightarrow (1)$. Let $K = F(\sqrt{a})$ with $[a] \neq 1$, $[-1]$. We show that if $[b] \notin \mathrm{Im}\,\varepsilon$ then $[b\sqrt{a}] \in \mathrm{Im}\,\varepsilon$, whence $(Q(K) \colon \mathrm{Im}\,\varepsilon) = 2$. Consider the extension $K(\sqrt{b})$. If N is the closure of $K(\sqrt{b})$ over F then $|\mathrm{Gal}\,(N/F)| = 4$ or 8 and since $[b] \notin \mathrm{Im}\,\varepsilon$, $\mathrm{Gal}\,(N/F)$ is not a group of exponent 2. By (3), we must have $-1 \in N^2$, so $N = K(\sqrt{b}, \sqrt{\sigma(b)}) = K(\sqrt{b}, \sqrt{-1})$. Hence $[\sigma(b)] = [-1]$ in $Q(K(\sqrt{b}))$ which implies that $[\sigma(b)] = [-1]$ or $[-b]$ in $Q(K)$. If $[\sigma(b)] = [-1]$ then $[b] = [-1] \in \mathrm{Im}\,\varepsilon$. Hence $[\sigma(b)] = [-b]$ and so $[b\sqrt{a}] \in Q(K)^G$, $G = \mathrm{Gal}\,(K/F)$. By Lemma 3.3, $L = K(\sqrt{b\sqrt{a}})$ is a Galois extension of F. If $\sqrt{-1} \in L$ then $L = K(\sqrt{-1})$ and $[b\sqrt{a}] = [-1] \in \mathrm{Im}\,\varepsilon$. If $\sqrt{-1} \notin L$ then $\mathrm{Gal}\,(L/F)$ is a group of exponent 2, so again $[b\sqrt{a}] \in \mathrm{Im}\,\varepsilon$.

$(1) \Rightarrow (2)$. We proceed by induction on $[K \colon F]$. Since (1) holds, so does (3), so $\mathrm{Gal}\,(K/F)$ is of exponent 2. Hence we can find a Galois extension L/F with $K = L(\sqrt{b})$, $b \in F$, $[b] \neq 1$ in $Q(F)$. Consider the surjective map $Q(L)/\mathrm{Im}\,\varepsilon_{L/F} \xrightarrow{\varepsilon_{K/L}} \mathrm{Im}\,\varepsilon_{K/L}/\mathrm{Im}\,\varepsilon$. If $\bar{x} \in \mathrm{Ker}\,\bar{\varepsilon}_{K/L}$ then $\varepsilon_{K/L}(x) \in \mathrm{Im}\,\varepsilon$ so there exists y in $Q(F)$ such that $\varepsilon_{K/L}(x) = \varepsilon(y) = \varepsilon_{K/L}(\varepsilon_{L/F}(y))$. Hence $x\varepsilon_{L/F}(y) \in \mathrm{Ker}\,\varepsilon_{K/L} = \{1, [b]\} \subset \mathrm{Im}\,\varepsilon_{L/F}$. Hence $x \in \mathrm{Im}\,\varepsilon_{L/F}$ and $\bar{\varepsilon}_{K/L}$ is an isomorphism. Thus $(Q(K) \colon \mathrm{Im}\,\varepsilon) = (Q(K) \colon \mathrm{Im}\,\varepsilon_{K/L})(\mathrm{Im}\,\varepsilon_{K/L} \colon \mathrm{Im}\,\varepsilon) = (Q(K) \colon \mathrm{Im}\,\varepsilon_{K/L})(Q(L) \colon \mathrm{Im}\,\varepsilon_{L/F})$. Now $(Q(K) \colon \mathrm{Im}\,\varepsilon_{K/L}) = [K \colon L] = 2$ since L is a field of class C and $-1 \notin K^2$ and $(Q(L) \colon \mathrm{Im}\,\varepsilon_{L/F}) = [L \colon F]$ by the induction assumption.

$(2) \Rightarrow (1)$. This follows from Theorem 1.9(7) together with Exact Sequence 1.4.

REMARK. It can be shown that if F is any field of class C and K is a finite Galois extension with $[Q(K) \colon \mathrm{Im}\,\varepsilon] = [K \colon F]$ then $\mathrm{Gal}\,(K/F)$ is of exponent 2.

As a variation of Theorem 3.2 we have

THEOREM 3.2′. *For a formally real field F the following statements are equivalent.*

(1) *F is superpythagorean.*

(2) $[K \colon F] = [Q(K) \colon \mathrm{Im}\,\varepsilon]$ *for all finite formally real Galois 2-extensions K.*

(3) $\mathrm{Gal}\,(K/F)$ *is a group of exponent 2 for all finite formally real Galois 2-extensions K.*

Proof. The implications $(1) \Rightarrow (2)$ and $(1) \Rightarrow (3)$ follow from Theorem 3.2, while

(2) $\Rightarrow$ (1) is contained in Proposition 1.8.

(3) $\Rightarrow$ (1). As in the proof of (3) $\Rightarrow$ (1) in Theorem 3.2, we show that if $K = F(\sqrt{a})$ is a formally real quadratic extension and $[b] \notin \operatorname{Im} \varepsilon$ then $[b\sqrt{a}] \in \operatorname{Im} \varepsilon$.

Let $<$ be an ordering on F which extends to the formally real field K. Let $<_1$, $<_2$ be its extensions to K and suppose $0 <_1 \sqrt{a}$, $\sqrt{a} <_2 0$. We assert that if $c \in K$ is positive with respect to both $<_1$ and $<_2$ then $[c] \in \operatorname{Im} \varepsilon$. Indeed, if $0 <_i c$, $i = 1, 2$, then the ordering $<$ will have four extensions to the field $K(\sqrt{c})$ and hence if $R_<$ is a real closure of F with respect to the ordering $<$ then the minimal polynomial $f(x)$ of a primitive element for $K(\sqrt{c})$ over F will have 4 roots in $R_<$. Since $[K(\sqrt{c}) \colon F] = 4$ the splitting field N of $f(x)$ will be contained in $R_<$ and therefore will be formally real. The extension $K(\sqrt{c})/F$ consists of successive quadratic extensions so the Galois group $\operatorname{Gal}(N/F)$ is a 2-group (in fact, $\operatorname{Gal}(N/F) = 4$ or 8). By (3), $\operatorname{Gal}(N/F)$ is a group of exponent 2, so $K(\sqrt{c})$ is Galois over F and $\operatorname{Gal}(K(\sqrt{c})/F)$ is the Klein 4-group. Hence $[c] \in \operatorname{Im} \varepsilon$.

Now choose $[b] \notin \operatorname{Im} \varepsilon$. Then $[-b] \notin \operatorname{Im} \varepsilon$ so b must be positive with respect to one of the orderings on K and negative with respect to other. Replacing $[b]$ by $[-b]$, if necessary, we may suppose $0 <_1 b$ and $b <_2 0$. Then $b\sqrt{a}$ is positive with respect to both orderings, so $[b\sqrt{a}] \in \operatorname{Im} \varepsilon$.

The following rather technical lemma will be crucial in our investigation of fields of class C with $s(F) = 1$.

LEMMA 3.4. *Let F be a field of class C with $s(F) = 1$.*

(1) *If $L \subset F(\sqrt[2^{n_i}]{a_i} \mid i = 1, \cdots, r)$ with $a_i \in F$ and $n_i \geqq 0$ and if K is a quadratic extension of L then there exists c in F such that $K \subset F(\sqrt[2^{n_1+1}]{a_1}, \cdots, \sqrt[2^{n_r+1}]{a_r}, \sqrt{c})$.*

(2) *If K is a finite 2-extension of F then there exist $a_1, \cdots, a_s$ in F and nonnegative integers $m_1, \cdots, m_s$ such that*

$$K \subset F(\sqrt[2^{m_1}]{a_1}, \cdots, \sqrt[2^{m_s}]{a_s}) .$$

Proof. (2) follows from (1) by induction. To prove (1), let $K = L(\sqrt{x})$, $N = F(\sqrt[2^{n_1}]{a_1}, \cdots, \sqrt[2^{n_r}]{a_r})$, and write N as the union of a tower of fields $F = F_0 \subset F_1 \subset \cdots \subset F_t = N$ where $[F_{i+1} \colon F_i] = 2$ and $F_i = F_{i-1}(\sqrt{y_i})$ with $y_i = \sqrt[2^j]{a_k}$ for some $1 \leqq k \leqq r$ and $0 \leqq j < n_k$. Let $\varepsilon_i \colon Q(F_{i-1}) \to Q(F_i)$ be the natural map and let i_0 be then smallest index such that there exists x_0 in F_{i_0} with $[x_0[= [x]$ in $Q(N)$. If $i_0 = 0$ then $K = L(\sqrt{x}) \subset N(\sqrt{x_0})$ and we are done. If $i_0 > 0$ then $[x_0] \notin \operatorname{Im} \varepsilon_{i_0}$ so, since F is a field of class C and $-1 \in F^2$, $[x_0\sqrt{y_{i_0}}] \in$

$\operatorname{Im} \varepsilon_{i_0}$. Now choose $i_1 < i_0$ smallest such that there exists $x_1 \in F_{i_1}$ with $[x_1] = [x_0\sqrt{y_{i_0}}]$ in $Q(N)$. If $i_1 = 0$ we stop and if $i_1 > 0$ we continue in this way, obtaining a decreasing sequence $i_0 > i_1 > \cdots > i_t = 0$ and $x_j \in F_{i_j}$, $j = 0, \cdots, t$, such that $[x_{j+1}] = [x_j\sqrt{y_{i_j}}]$ in $Q(N)$. Then $x_t \in F$ and, in $Q(N)$, $[x_t] = [x_{t-1}\sqrt{y_{i_{t-1}}}] = \cdots = [x\sqrt{y_{i_0}} \cdots \sqrt{y_{i_{t-1}}}]$. Hence $\sqrt{x} \in F(b_1, \cdots, b_s, \sqrt{x_t})$, $b_i = \sqrt[2^{n_i+1}]{a_i}$, proving (1).

THEOREM 3.5. *For a field F with $|Q(F)| > 2$ the following statements are equivalent.*

(1) *F is a field of class C with $s(F) = 1$.*

(2) *If K is a quadratic extension of F and $G = \operatorname{Gal}(K/F)$ then $W(K)^G = W(K)$.*

(3) *Every 2-extension of degree 4 is a Galois extension.*

(4) *If K is a Galois extension with $\operatorname{Gal}(K/F)$ a 2-group then every subgroup of index 4 in $\operatorname{Gal}(K/F)$ is normal.*

(5) *The Dihedral group of order 8 does not occur as a Galois group over F.*

(6) *Every Galois extension of degree 8 is abelian.*

Proof. We first note that if $K = F(\sqrt{a})$ is a quadratic extension of F and if $G = \operatorname{Gal}(K/F)$ then $[u + v\sqrt{a}] \in Q(K)^G$ if and only if $[u^2 - v^2a] \in \{1, [a]\}$ in $Q(F)$. Thus if $[a] \neq 1, [-1]$ then $Q(K)^G = Q(K)$ if and only if $s(F) = 1$ and $D_F(\langle 1, a\rangle) = \{1, [a]\}$, proving the equivalence of (1) and (2). The equivalence of (2) and (3) follows from Lemma 3.3, the equivalence of (3) and (4) is elementary Galois theory, and the implications (4) $\Rightarrow$ (5) and (6) $\Rightarrow$ (5) are obvious.

(5) $\Rightarrow$ (3). If K is a nonGalois 2-extension of degree 4 over F then the Galois group of its Galois closure will be a subgroup of order 8 in the symmetric group of degree 4, i.e., the dihedral group of order 8. It remains to prove

(5) $\Rightarrow$ (6). We show that the quaternion group Q cannot occur as a group over F. If Q did occur there would exist fields L, K, and a, b in F such that $F \subset L \subset K$, $[K: L] = 2$, $L = F(\sqrt{a}, \sqrt{b})$, and $Q = \operatorname{Gal}(K/F)$. Since (5) holds, so do statements (1) and (3), so by Lemma 3.4 we could find c in F such that $K \subset F(\sqrt[4]{a}, \sqrt[4]{b}, \sqrt{c})$. By (3), the extensions $F(\sqrt[4]{a})$, $F(\sqrt[4]{b})$ are Galois and hence abelian over F. But then K would be contained in an abelian extension.

REMARKS. 1. Since there exist quadratically closed fields which admit the alternating group A_4 as Galois group, the hypothesis that K/F be a 2-extension is essential in statement (3).

2. If F is a field with $|Q(K)| = 2$ then F is a field of class C, F satisfies the conditions (2)-(6) (see Prop. 3.10), but we may have $s(F) \neq 1$.

3. The statement that $W(K)^G = W(K)$ for all Galois 2-extensions K of F, $G = \mathrm{Gal}\,(K/F)$, is not equivalent to the statements in Theorem 3.5. We will see that the field $\boldsymbol{Q}_5$ of 5-adic numbers provides an example of a field satisfying the statements of Theorem 3.5, but not the stronger condition. Indeed, we have

THEOREM 3.6. *For a field F with $|Q(F)| > 2$ the following statements are equivalent.*

(1) *F is a field of class C and for all $n \geqq 1$, all 2^nth roots of unity lie in F.*

(2) *Every 2-extension of F is abelian, i.e., $\mathrm{Gal}\,(F(2)/F)$ is an abelian group.*

(3) *Every finite 2-extension of F is Galois.*

(4) *If K/F is a finite Galois 2-extension with $G = \mathrm{Gal}\,(K/F)$ then $W(K)^G = W(K)$.*

Proof. (1) ⇒ (2). It suffices to show that every finite 2-extension K of F is abelian. By Lemma 3.4, K is contained in a composite of extensions of the form $F(\sqrt[2^n]{a})$, $a \in F$, $n \geqq 1$. Since all 2^nth roots of unity are in F, any such extension is cyclic, which proves that K/F is abelian. The implication (2) ⇒ (3) is immediate, while (3) ⇒ (4) follows from Lemma 3.3.

(4) ⇒ (3). We proceed by induction on $[K: F] > 1$ to show that the 2-extension K/F is Galois. Since K is a 2-extension there is a field L with $F \subset L \subset K$ and $[K: L] = 2$. By the induction assumption, L/F is Galois and so by (4), together with Lemma 3.3, K/F is Galois.

(3) ⇒ (2). By Theorem 3.5, the quaternion group Q does not occur as a Galois group over F. But by [13, 5.36, p. 92], any non abelian group all of whose subgroups are normal has Q as a homomorphic image. Hence all 2-extensions are abelian.

The proof that (2) implies (1) will use the following easy

LEMMA 3.7. *Let F be any field and let $[a] \neq 1$ in $Q(F)$. If there exists $n \geqq 1$ such that $F(\sqrt[2^n]{a}) = F(\sqrt[2^{n+1}]{a})$ then $[a] = [-1]$.*

Proof. Let $b_i = \sqrt[2^i]{a}$, $i = 0, \cdots, n+1$, let $F_0 = F$ and $F_{i+1} = F_i(\sqrt{b_i})$, $i = 0, \cdots, n$, let $\varepsilon_i\colon Q(F_{i-1}) \to Q(F_i)$, $i = 1, \cdots, n+1$ be the natural maps, and let $N_i\colon Q(F_i) \to Q(F_{i-1})$ be the norms. Now $b_n = \sqrt{b_{n-1}}$ is a square in F_n so $[b_n] \in \mathrm{Im}\,\varepsilon_n = \mathrm{Ker}\,N_n$ whence $[b_{n-1}] = [-1]$ in $Q(F_{n-1})$. But then $[b_{n-1}] \in \mathrm{Im}\,\varepsilon_{n-1}$ so $[b_{n-2}] = [-1]$ in $Q(F_{n-2})$. Continuing in this way, we get $[a] = [-1]$.

Now assume (2). By Theorem 3.5, F is a field of class C so we need only show that all 2^nth roots of 1 are in F for all $n \geqq 1$. If not, choose n smallest such that some 2^nth root ζ is not in F. Then $\zeta^2 \in F$ so $[F(\zeta): F] = 2$. Since $|Q(F)| > 2$, there exists a in F with $\sqrt{a} \notin F(\zeta)$. Since $\sqrt{-1} \in F(\zeta)$ it follows that $[a] \neq [-1]$ in $Q(F(\zeta))$. By Lemma 3.7, $[F(\zeta, \sqrt[2n]{a}): F(\zeta)] = 2^n$. Hence $\zeta \notin F(\sqrt[2n]{a})$ so we can find τ in $\mathrm{Gal}\,(F(\zeta, \sqrt[2n]{a})/F(\sqrt[2n]{a}))$ such that $\tau(\zeta) \neq \zeta$. Let σ be the $F(\zeta)$-automorphism of $F(\sqrt[2n]{a}, \zeta)$ sending $\sqrt[2n]{a}$ to $\zeta\sqrt[2n]{a}$. Then $\sigma\tau(\sqrt[2n]{a}) = \zeta\sqrt[2n]{a}$ while $\tau\sigma(\sqrt[2n]{a}) = \tau(\zeta)\sqrt[2n]{a}$. Hence $\sigma\tau \neq \tau\sigma$ and F has a nonabelian Galois 2-extension, completing the proof.

EXAMPLES 3.8. (i) The field $\boldsymbol{Q}_5$ satisfies the conditions of Theorem 3.5 but not Theorem 3.6. Given any field F of class C with $s(F) = 1$ there is a field K satisfying the conditions of Theorem 3.6 with $W(K) \cong W(F)$.

(ii) Becker [1] has shown that if F is superpythagorean then $F(\sqrt{-1})$ satisfies condition (2) of Theorem 3.6. In particular $F(\sqrt{-1})$ contains all 2^nth roots of unity.

(iii) If F_0 is quadratically closed and $F = F_0((t_1))_{i \in I}$ is a field of iterated formal power series over F then F is field of class C and F contains all 2^nth roots of unity. Hence all Galois 2-groups are abelian.

(iv) If K is a quadratically closed field and G is an abelian pro 2-group of automorphisms of K then K is the quadratic closure of K^G and $G = \mathrm{Gal}\,(K/K^G)$. Hence K^G is a field of class C.

COROLLARY 3.9. *Let F be a field of class C with $|Q(F)| > 2$. Let $\{[a_i]\}_{i \in I}$ be an $\boldsymbol{F}_2$-basis for $Q(F)$, let $F(2)$ be the quadratic closure of F, let $G_F(2) = \mathrm{Gal}\,(F(2)/F)$, and let $G_F(2)'$ denote the closure of the commutator subgroup of $G_F(2)$. Then*

(1) *If $s(F) = 1$ then $F(2) = F(\sqrt[2^{n_i}]{a_i} \mid i \in I, n_i \geqq 0)$.*

(2) *If all 2^nth roots of unity are in F then $G_F(2) \cong \boldsymbol{Z}_2^I$, where $\boldsymbol{Z}_2^I$ denotes the direct product of $|I|$ copies of the additive group of 2-adic integers.*

(3) *$G_F(2)$ is isomorphic to one of the following: $\boldsymbol{Z}_2^I$ for some set I or a nonabelian group which is either an extension of $\boldsymbol{Z}_2^I$ by $\boldsymbol{Z}/2\boldsymbol{Z}$, by $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}_2^J$, or by $\boldsymbol{Z}_2^J$ for some nonempty sets I, J.*

(4) *Every finite Galois 2-group of F is an extension of an abelian group by an abelian group.*

(5) *$G_F(2)'$ is an abelian group.*

Proof. (1) follows from Lemma 3.4.

(2) Consider the map $\pi: G_F(2) \rightarrow \boldsymbol{Z}_2^I$ induced by the natural maps $\pi_i\colon G_F(2) \to \mathrm{Gal}\,(F(\sqrt[2^n]{a_i})_{n\geqq 1}/F) \cong \boldsymbol{Z}_2$, $i \in I$. Since $\{[a_i] \mid i \in I\}$ is a basis and the finite extensions $F(\sqrt[2^{n_i}]{a_i})$ are cyclic, it follows that for fixed i in I, $F(\sqrt[2^{n_i}]{a_i} \mid n_i \geqq 0) \cap F(\sqrt[2^{n_j}]{a_j} \mid j \neq i, n_j \geqq 0) = F$. Hence π is surjective and, therefore, an isomorphism.

(3) If $G_F(2)$ is abelian all 2^2th roots of unity are in F so by (2), $G_F(2) \cong \boldsymbol{Z}_2^I$. If $G_F(2)$ is not abelian, let L be the extension of F obtained by adjoining all 2^nth roots of unity, $n \geqq 1$. Then L is a field of class C, $\mathrm{Gal}\,(L/F)$ is abelian, and by (2) $\mathrm{Gal}\,(F(2)/L) \cong \boldsymbol{Z}_2^I$ for some set I. If $\mathrm{Gal}\,(L/F)$ contains an automorphism $g \neq 1$ finite order with fixed field K then by applying Lemma 3.7 we see that $L = K(\sqrt{-1})$. Hence $\mathrm{Gal}\,(L/F) \cong \mathrm{Gal}\,(F(\sqrt{-1})/F) \times \mathrm{Gal}\,(L/F(\sqrt{-1}))$ and $\mathrm{Gal}\,(L/F(\sqrt{-1}))$ has no elements of finite order. Now if G is any abelian pro p-group with no elements of finite order, then by Pontryagin duality there exists a divisible abelian p-group M with $G \cong \mathrm{Hom}\,(M, \boldsymbol{Z}p^\infty)$, where $\boldsymbol{Z}p^\infty$ is the p-primary component of $\boldsymbol{Q}/\boldsymbol{Z}$. Since M is divisible, $M \cong \boldsymbol{Z}p^{\infty(J)}$ for some set J, whence $G \cong (\mathrm{Hom}\,(\boldsymbol{Z}p^\infty, \boldsymbol{Z}p^\infty))^J \cong \boldsymbol{Z}_2^J$. This proves (3).

(4) Let K be finite Galois 2-extension and again let L be the extension obtained from F by adjoining the 2^nth roots of 1 for all $n \geqq 1$. Then $K \cap L/F \subset L/F$ so $K \cap L/F$ is an abelian extension. By Theorem 3.6, KL/L is also an abelian extension and since $\mathrm{Gal}\,(KL/L) \cong \mathrm{Gal}\,(K/K \cap L)$, (4) is proved.

(5) Let L be as in (3) and (4). Since L/F is abelian, $G_F(2)' \subset \mathrm{Gal}\,(F(2)/L)$ and the latter is abelian.

For completeness, we include the following result concerning fields with exactly 2 square classes.

PROPOSITION 3.10. *For a field F the following statements are equivalent.*

(1) *$W(F) \in \{\boldsymbol{Z}, \boldsymbol{Z}/4\boldsymbol{Z}, \boldsymbol{Z}/2\boldsymbol{Z}[G]\}$ with $|G| = 2$.*

(2) $|Q(F)| = 2$.

(3) *Every finite 2-extension of F is cyclic.*

(4) *Either* $\mathrm{Gal}\,(F(2)/F) \cong \boldsymbol{Z}_2$ *or* $\mathrm{Gal}\,(F(2)/F) \cong \boldsymbol{Z}/2\boldsymbol{Z}$. *The second possibility occurs if and only if F is Euclidean.*

Proof. The equivalence of (1) and (2) is well known.

(2) $\Rightarrow$ (3). Let K/F be a finite Galois 2-extension with group G. Since $|Q(F)| = 2$, G has a unique subgroup of index 2. But, for any prime p, a p-group having a unique subgroup of index p is cyclic.

(3) $\Rightarrow$ (2). If $|Q(F)| > 2$ then F admits the Klein 4-group as a Galois group.

(3) $\Rightarrow$ (4). Assume (3). Then $|Q(F)| = 2$. If $s(F) = 0$ then F is

Euclidean so we may suppose $s(F) > 0$. We assert that for each integer $n \geqq 1$, F has a unique (cyclic) 2-extension of degree 2^n. Indeed, since F is not formally real it follows from Theorem 1.5 that the unique quadratic extension of F has exactly 2 squares classes and so also has a unique quadratic extension. Since a 2-extension consists of a tower of quadratic extensions, F has exactly one cyclic 2-extension of degree 2^n. Hence $\mathrm{Gal}\,(F(2)/F) \cong \boldsymbol{Z}_2$.

The implication $(4) \Rightarrow (3)$ is clear.

We next prove a result about fields of class C with $q(F) = |Q(F)| < \infty$. Recall that the *rank* of a pro p-group G, denoted rank G, is defined to be the cardinality of a minimal set of generators of the topological group G. We have rank $G = \dim_{F_p} H^1(G, \boldsymbol{Z}/p\boldsymbol{Z})$. Moreover, if G^* denotes the intersection of the Kernels of all homomorphisms $G \rightarrow \boldsymbol{Z}/p\boldsymbol{Z}$ then rank G is finite if and only if $\dim_{F_p} G/G^*$ is finite and when this happens, they are equal. For details see [14, 4.2, I-34-39].

THEOREM 3.11. *For a field F the following statements are equivalent.*

(1) *F is a field of class C with $q(F) < \infty$.*

(2) *There exists an integer m such that $q(K) \leqq m$ for all finite 2-extensions K of F.*

(3) *There exists an integer m such that $q(K) \leqq m$ for all 2-extensions K of F.*

(4) *There exists an integer n such that for all Galois extensions L/K with $F \subset K \subset L \subset F(2)$,* rank Gal $(L/K) \leqq n$.

(5) *There exists an integer n such that for every Galois 2-extension K/F, all closed subgroups of* Gal (K/F) *have* rank $\leqq n$.

(6) *There exists an integer n such that* rank $H \leqq n$ *for all closed subgroups H of* Gal $(F(2)/F)$.

Proof. $(1) \Rightarrow (2)$. Taking $m = q(F)$ this follows from Theorem 1.5 and Corollary 2.10.

$(2) \Rightarrow (1)$. If F is not a field of class C then we can find a quadratic extension of F_1 such that $q(F_1) > q(F)$. By Theorem 2.1, F_1 is not a field of class C so we can find a quadratic extension F_2 of F_1 such that $q(F_2) > q(F_1)$. Continuing in this way we can construct a tower $F_1 \subset F_2 \subset \cdots \subset F_m$ with F_m a 2-extension of F and $q(F_i) > q(F_{i-1})$. Thus $q(F_m) \geqq 2^m q(F) > m$ for all m.

$(2) \Rightarrow (3)$. Assume (2). Then there exists an integer m such that $q(K) \leqq m$ for all finite 2-extensions K/F. If there exists an infinite 2-extension L/F such that $Q(L)$ contains $m + 1$ distinct elements $[a_1], \cdots, [a_{m+1}]$ then $K = F(a_1, \cdots, a_{m+1})$ is a finite 2-extension with $q(K) \geqq m + 1$.

$(3) \Rightarrow (4)$. Choose m as in (3) and choose n with $m \leqq 2^n$. Let L/K be a Galois extension with $F \subset K \subset L \subset F(2)$ and let $G = \mathrm{Gal}(L/K)$. Then the elementary 2-group G/G^* corresponds to a Galois extension N/K and $|G/G^*| \leqq q(K) \leqq m$. Hence $\dim_{F_2} G/G^* \leqq n$, i.e., $\operatorname{rank} G \leqq n$.

$(4) \Rightarrow (5)$. Let K/F be a Galois 2-extension and let H be a closed subgroup of $\mathrm{Gal}(K/F)$. Then K/K^H is Galois with group H so by (4), $\operatorname{rank} H \leqq n$. The implication $(5) \rightarrow (6)$ is immediate.

$(6) \Rightarrow (2)$. Choose n as in (6) and let m be an integer with $2^n \leqq m$. Let K be a finite 2-extension of F. Then there is a closed subgroup H of $\mathrm{Gal}(F(2)/F)$ such that $K = F(2)^H$. Let $H_1 = \mathrm{Gal}(K(\sqrt{b} \mid b \in K)/K)$. Then H_1 is a factor group of H so $\operatorname{rank} H_1 \leqq \operatorname{rank} H \leqq n$. Hence $q(K)$ is finite and $q(K) = 2^{\operatorname{rank} H_1} \leqq 2^n \leqq m$.

COROLLARY 3.12 (cf. [1, Satz 19, p. 112]). *For a field F and an integer $n \geqq 0$ the following statements are equivalent.*

(1) *F is a field of class C with $q(F) = 2^n$.*

(2) *For all 2-extensions K of F, $q(K) \leqq 2^n$ and there exists a 2-extension with $q(K) = 2^n$.*

(3) *For all finite 2-extensions K of F*

$$q(K) = \begin{cases} 2^{n-1} & \text{if } F \text{ is real and } \sqrt{-1} \in K \\ 2^n & \text{otherwise.} \end{cases}$$

(4) $\operatorname{Rank} \mathrm{Gal}(F(2)/F) = n$ *and* $\operatorname{rank} G \leqq n$ *for all closed subgroups G of* $\mathrm{Gal}(F(2)/F)$.

(5) *For all closed subgroups G of finite index in* $\mathrm{Gal}(F(2)/F)$,

$$\dim_{F_2} H^1(G, Z/2Z) = \begin{cases} n - 1 & \text{if } F \text{ is real and } \sqrt{-1} \in F(2)^G \\ n & \text{otherwise.} \end{cases}$$

REMARK. If the conditions of Corollary 3.12 are satisfied for F and n then for all $m \leqq n$ there exists a field K (of class C) with $F \subset K \subset F(2)$ and $q(K) = 2^m$. Indeed, if $\mathrm{Gal}(F(2)/F)$ is of rank n then for any $m \leqq n$, $\mathrm{Gal}(F(2)/F)$ has a closed subgroup G of rank m so we can take $K = F(2)^G$.

For a field F, let $u(F)$ denote its u-invariant and $o(F)$ the number of orderings.

COROLLARY 3.13. *Let F be a field of class C. Then*

(1) *If F is not formally real then $u(K) = u(F)$ for all finite 2-extensions K of F and $u(K) \leqq u(F)$ for all 2-extensions K of F. Moreover, if K is a 2-extension with $u(K) < \infty$ then $u(K) = 2^m$ for*

some $m \geqq 0$ and for each integer $m \geqq 0$ with $2^m \leqq u(F)$, there exists a 2-extension K with $u(K) = 2^m$.

(2) (cf. [3, 3.9]) *If F is formally real then $o(K) = o(F)$ for all finite formally real 2-extensions K of F and $o(K) \leqq o(F)$ for all 2-extensions K. Moreover, if K is any formally real 2-extension with $o(K) < \infty$ then $o(K) = 2^m$ for some $m \geqq 0$ and for each integer $m \geqq 0$ with $2^m \leqq o(F)$ there exists a formally real 2-extension K with $o(K) = 2^m$.*

Proof. (1) follows from Corollary 3.12, the remark, and the fact that $u(K) = q(K)$ for any nonformally real field K class C (see [5], [16]).

(2) If K is a formally real field of class C then K is superpythagorean and by [7, Cor. 4.5], $o(K) = 1/2q(K)$. Hence we need only show that if $m \geqq 0$ and $2^m \leqq o(F)$ then there exists a 2-extension K with $o(K) = 2^m$. Let $F_1 = F(\sqrt{-1})$. Then F_1 is a field of class C and $q(F_1) = 1/2q(F) = o(F) \geqq 2^m$. Let K_1 be a 2-extension of F_1 with $q(K_1) = 2^m$ and let $K \subset K_1$ be a maximal formally real extension of F. Then K is of class C and if $[a] \neq 1$, $[-1]$ in $Q(K)$ then $K(\sqrt{a}) \not\subset K_1$. Hence Ker $(Q(K) \rightarrow Q(K_1)) = \{1, [-1]\}$ so $1/2q(K) \leqq q(K_1)$. On the other hand, $1/2q(K) = q(K(\sqrt{-1})) \geqq q(K_1)$ so $o(K) = 1/2q(K) = q(K_1) = 2^m$.

References

1. E. Becker, *Erblich-pythagoreische Körper und Ordnungen höherer Stufe*, Preprint, Köln, 1975.

2. L. Bröcker, *Über eine Klasse pythagoreischer Körper*, Arch. Math., **23** (1972), 405-407.

3. ———, *Characterization of fans and hereditarily pythagorean fields*, Math. Z., **151** (1976), 149-163.

4. R. Brown, *Superpythagorean fields*, J. Algebra, **42** (1976), 483-494.

5. C. Cordes, *The Witt group and the equivalence of fields with respect to quadratic forms*, J. Algebra, **26** (1973), 400-421.

6. J. Diller und A. Dress, *Zur Galoistheorie pythagoreische Körper*, Arch. Math., **16** (1965), 148-152.

7. R. Elman and T. Y. Lam, *Quadratic forms over formally real fields and pythagorean fields*, Amer. J. Math., **94** (1972), 1155-1194.

8. ———, *Quadratic forms and the u-invariant, I*, Math. Z., **131** (1973), 283-304.

9. ———, *Quadratic forms under algebraic extensions*, Math. Ann., **219** (1976), 21-42.

10. D. K. Harrison, *Witt Rings*, Lecture notes, Department of Mathematics, University of Kentucky, Lexington, Kentucky, 1970.

11. T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Reading, Massachusetts, 1973.

12. A. Prestel, *Lectures on Formally Real Fields*, Monografias de Matemática 22, Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1975.

13. J. J. Rotman, *The Theory of Groups*, Allyn and Bacon, Boston, Massachusetts, 1973.

14. J. P. Serre, *Cohomologie Galoisienne*, Springer Lecture Notes 5, 1965.

15. R. Ware, *When are Witt rings group rings?* Pacific J. Math., **49** (1973), 279-284.

16. ———, *A note on quadratic forms and the u-invariant,* Canad. J. Math., **26** (1974), 1242-1244.

17. ———, *A note on quadratic forms over pythagorean fields,* Pacific J. Math., **58** (1975), 651-654.

18. ———, *Some remarks on the map between Witt rings of an algebraic extension,* Conference on Quadratic Forms, Queen's papers in Pure and Applied Mathematics, No. 46, Queen's University, Kingston, Ontario, 1977.

Received July 27, 1977 and in revised form September 14, 1977. Support from NSF Grant MCS 76-06581 is gratefully acknowledged.

THE PENNSYLVANIA STATE UNIVERSITY
UNIVERSITY PARK, PA 16802