BULL. AUSTRAL. MATH. SOC. 12D15,12F10, 11E81
VOL. 67 (2003) [329–341]

SEMIORDERINGS AND WITT RINGS

THOMAS C. CRAVEN AND TARA L. SMITH

For a pythagorean field F with semiordering Q and associated preordering T, it is shown that the Witt ring $W_T(F)$ is isomorphic to the Witt ring $W(K)$ where K is a closure of F with respect to Q. For an arbitrary preordering T, it is shown how the covering number of T relates to the construction of $W_T(F)$.

1. INTRODUCTION AND NOTATION

In [**5**], the first author introduced the concept of an *order closed field*, a field which has no proper algebraic extension to which all of its orderings extend uniquely. These were studied much more deeply in [**7**] in which a second concept was introduced, that of a *strongly order closed field*, a field with the property that it has no proper algebraic extension to which all of its orderings extend. Among other things, it is shown that for large classes of fields, the two concepts coincide. It is still an open question whether every order closed field is strongly order closed. In [**7**], although the spaces of orderings are homeomorphic in going to an order closure, no attempt is made to keep the reduced Witt ring from becoming larger. Indeed, [**7**, Section 5] explores the reasons that this is impossible when one deals with the entire set of orderings of a field. In the present paper we are able to obtain control over the growth of the reduced Witt ring by restricting attention to the orderings over certain types of preordering.

The work here depends strongly on the use of semiorderings of a field.

DEFINITION: A *semiordering* on a field F is a subset Q of F satisfying $1 \in Q$, $Q \cup -Q = F$, $Q \cap -Q = \{0\}$, $Q + Q \subseteq Q$, and $F^2Q = Q$.

Thus a semiordering is more general than an ordering in that it need not be closed under multiplication. A semiordering which is not an ordering is called a *proper semiordering.* The concept of a semiordering first occurs in work of Baer [**1**]. Semiorderings have had a major place in the theory of formally real fields since their use in quadratic form theory by Prestel [**20**] and subsequent work by Becker and Köpping [**3**]. An excellent source of general information on semiorderings can be found in a survey by Lam [**15**]. More recent uses are found in [**21**] and [**14**]. They also show up in applications to division algebras, where a Baer ordering is just a generalisation of semiordering

Received 6th November, 2002
The second author was upported in part by the Taft Memorial Fund of the University of Cincinnati.

to the situation of a division ring with a nontrivial involution (see [8]). Following [20] and [15], we write Y_F for the topological space of all semiorderings and X_F for the subspace of orderings, where the topology is given by the Harrison subbasis. This is defined as the collection of all subsets of the form

$$H(a) = \{\, Q \in Y_F \mid a \in Q \,\} \qquad \bigl(a \in \dot{F}\bigr). \tag{1}$$

We allow our orderings, semiorderings, *et cetera* to contain zero, but sometimes we need to eliminate zero from a set. In general, for any subset $S \subseteq F$, we write $\dot{S}$ for $S \setminus \{0\}$.

We follow Efrat and Haran [11] in defining a field F with semiordering Q to be *semireal closed* if Q does not extend to any algebraic extension of F and to be *quadratically semireal closed* if Q does not extend to any quadratic extension of F. We extend this to say that, given an arbitrary semiordered field (F, Q), an extension $(K, \widetilde{Q})$ is a *semireal closure* (respectively *quadratic semireal closure*) of F if K is contained in the algebraic (respectively quadratic) closure of F, $\widetilde{Q} \cap F = Q$ and Q does not extend to any algebraic (respectively quadratic) extension of K. There is a subtlety here that is not readily apparent. This is not the same as saying that $(K, \widetilde{Q})$ is semireal closed (respectively, quadratically semireal closed) with $\widetilde{Q} \cap F = Q$. As an example, take $F = \mathbb{Q}((x))$, the field of Laurent series over the rationals, and let Q be its ordering in which x is positive. Then a semireal closure of F will be the real closed field L equal to the compositum $\widetilde{\mathbb{Q}} \cdot \mathbb{Q}((x))\bigl(x^{1/n}, n = 2, 3, 4, \dots\bigr)$, where $\widetilde{\mathbb{Q}}$ is a real closure of $\mathbb{Q}$. Inside this field, we have $F' = \mathbb{Q}\bigl(\sqrt{2}\bigr)((x))$ which has four orderings and four proper semiorderings. (For the construction, see [20, Theorems 7.8, 7.9].) Let Q' be one of the proper semiorderings of F' that restricts to Q. Then (F', Q') has a semireal closure $(K, \widetilde{Q})$ inside L which has four orderings and is a semireal closed field extending (F, Q), but is not a semireal closure of (F, Q) since Q will extend further even though $\widetilde{Q}$ will not.

For any field F, we denote the algebraic closure by $\overline{F}$ and the quadratic closure by F_q. We shall begin by proving the existence of semireal closures, but first we state one of the few theorems in the literature on extending semiorderings.

Theorem 1.1. ([20, Theorems 1.24, 1.26], [4, 2.16–2.18].) *Let F be a field and let K be an extension of F. A semiordering Q of F extends to K if and only if for every $a_1, \dots, a_n \in \dot{Q}$, the quadratic form $\sum_1^n a_i x_i^2$ has no nontrivial zeros in K. If $[K : F]$ is odd, then Q always extends to K. If $K = F(\sqrt{a})$, then Q extends to K if and only if $aQ \subseteq Q$.*

Theorem 1.2. *Let (F, Q) be a semiordered field. Then there exist a semireal closure and a quadratic semireal closure of (F, Q).*

PROOF: We do the semireal closure case. The quadratic case is done by replacing the algebraic closure $\overline{F}$ by the quadratic closure. Consider the collection of all subfields of $\overline{F}$ to which Q extends. For any chain F_α of such subfields, the union is again a field to which Q extends by Theorem 1.1 since any equation $\sum_1^n a_i x_i^2 = 0$ depends on only finitely many of the subfields. Thus Zorn's Lemma guarantees a maximal element of our class of subfields, which is a semireal closure by definition. ∎

PREORDERINGS ASSOCIATED WITH SEMIORDERINGS

A *preordering* of a field F is a proper subset $T \subseteq F$ satisfying $F^2 \subseteq T$, $T+T \subseteq T$ and $T \cdot T \subseteq T$. A preordering is always equal to the intersection of the set of orderings containing it [**15**, Theorem 1.6]. We write

$$Y_T = \{\, Q \in Y_F \mid T \cdot Q \subseteq Q \,\} \tag{2}$$

for the space of all semiorderings associated with a given preordering T and X_T for the subspace of all orderings in Y_T, the topology being inherited from Y_F (see (1)). Because of the multiplicative structure of orderings, the set X_T can be written as $X_T = \{\, P \in X_F \mid T \subseteq P \,\}$. Note that the spaces Y_F and X_F occur by taking T as the preordering of all sums of squares in F. We think of the reduced Witt ring $W_{\text{red}}(F)$ as a subring of the ring of continuous functions $\mathcal{C}(X_F, \mathbb{Z})$, where $\mathbb{Z}$ has the discrete topology. To develop a local version of the work in [**7**], we work only with the set X_T for a preordering T associated with a given semiordering. By restricting functions from X_F to X_T, we obtain a quotient ring $W_T(F)$ of the reduced Witt ring $W_{\text{red}}(F)$ [**15**, Section 1]. One of our major goals is to find an extension field K of F such that the canonical homomorphism $W_{\text{red}}(F) \to W(K)$ induces an isomorphism $W_T(F) \cong W(K)$. In the next section we are able to do this for certain preorderings by using quadratic semireal closures.

DEFINITION: Let S be any subset of Y_F, that is, any collection of semiorderings of the field F. Following [**11**], we say that the semiorderings in S form a *cover* of the preordering

$$T = \{\, a \in F \mid aQ \subseteq Q \text{ for all } Q \in S \,\}.$$

Efrat and Haran note that for any preordering T, the set of all $P \in X_T$ form a cover of T and define the *covering number* $\operatorname{cn}(T)$ to be the minimum size of a cover for T. We shall use the notation T_S for the preordering above associated with S, writing T_Q if $S = \{Q\}$. Other than in exceptional cases, such as a SAP preordering or an archimedean ordering, a minimal cover uses proper semiorderings.

https://doi.org/10.1017/S0004972700033797 Published online by Cambridge University Press

2. Quadratic semireal closures for pythagorean fields

For an inclusion of fields $F \subseteq K$, the image of the induced ring homomorphism $W(F) \to W(K)$ is generally of great interest, but also often difficult to compute. Given a formally real field F, constructing a pythagorean algebraic extension to which a given set of orderings extends uniquely is quite complicated, and it is also very difficult to control what happens to the Witt ring (see, for example, [**7,** Section 5]). We now investigate the role of quadratic semireal closures in this endeavor.

It turns out that we can actually construct quadratic semireal closures of a pythagorean semiordered field (F, Q) by using valuation theory. Let T be the preordering $T_Q = \{ a \in F \mid aQ \subseteq Q \}$. We follow Lam [**15,** Chapter 3] in writing $A^T = \prod\{ A(P) \mid P \in X_F,\ P \supseteq T \}$, where $A(P)$ is the canonical valuation ring associated with the ordering P determined by archimedean classes [**15,** Theorem 2.6]. The ring A^T is a valuation ring associated to some valuation v on F and v is fully compatible with T (that is, $1 + \mathfrak{m}_v \subseteq T$, where $\mathfrak{m}_v$ is the maximal ideal of A^T).

Theorem 2.1. *Let (F, Q) be a semiordered pythagorean field and let T, v, A^T, $\mathfrak{m}_v$ be as above. The 2-henselisation $\widetilde{F}$ of F with respect to v is a quadratic semireal closure of (F, Q). Furthermore, $W_T(F) \cong W(\widetilde{F})$.*

Proof: First note that the space of orderings is the proper one: Restriction of orderings (or semiorderings) from $\widetilde{F}$ to F is a homeomorphism [**20,** Lemma 8.2], [**15,** Proposition 3.17]. The semiordering Q is compatible with v in the strong sense that $a \in Q, v(a) < v(b)$ implies that $a - b \in Q$: Indeed, we have $a - b = a(1 - a^{-1}b)$ where $a \in Q,\ 1 - a^{-1}b \in 1 + \mathfrak{m}_v \subseteq T$, whence $a - b \in Q$. Let $\widetilde{Q}$ be the extension of Q to $\widetilde{F}$. By [**11,** Lemma 4.2], we shall be finished if we can show that the preordering covered by $\widetilde{Q}$ is $\widetilde{F}^2$. Let $x \in \widetilde{F}$ be such that $x\widetilde{Q} = \widetilde{Q}$. Since a 2-henselian extension is immediate, the value groups and residue fields are the same for v on F and its unique extension to $\widetilde{F}$. Thus we can find an element $z \in F$ with $v(z) = v(x)$, so that $x = uz$, where u is a unit in A^T. Furthermore, since the residue fields are the same, the unit u has the form $u_0(1 + m)$ where $u_0 \in F$ and m is in the extended maximal ideal. But the 2-henselian property implies, by Hensel's lemma for quadratics, that $1 + m$ is a square in $\widetilde{F}$. Thus we have $x = u_0 z y^2$ for some $y \in \widetilde{F}$ and $u_0 z \in F$. This gives $x\widetilde{Q} = u_0 z \widetilde{Q}$, so that $u_0 z Q \subseteq \widetilde{Q} \cap F = Q$. By definition $u_0 z \in T$. By [**15,** Theorem 3.18], T extends uniquely to $\widetilde{T} = \bigcap \widetilde{P}$, where $\widetilde{P}$ ranges over *all* orderings of $\widetilde{F}$, hence $\widetilde{T} = \widetilde{F}^2$ since $\widetilde{F}$ is pythagorean. But then $x = u_0 z y^2 \in T \cdot \widetilde{F}^2 = \widetilde{T} = \widetilde{F}^2$ as desired.

For the final statement, first note that we have $\widetilde{F}^2 \cap F = T$, since each ordering over T extends uniquely to $\widetilde{F}$ [**15,** Theorem 3.18], and $F \cdot \widetilde{F}^2 = \widetilde{F}$, the latter by the argument above for $x \in \widetilde{F}$, but ignoring the condition $x\widetilde{Q} \subseteq \widetilde{Q}$. From this we obtain $\dot{F}/\dot{T} \cong \dot{F}/(\dot{\widetilde{F}}^2 \cap \dot{F}) \cong (\dot{F} \cdot \dot{\widetilde{F}}^2)/\dot{\widetilde{F}}^2 \cong \dot{\widetilde{F}}/\dot{\widetilde{F}}^2$, and thus the inclusion of F in $\widetilde{F}$ induces an isomorphism $W_T(F) \cong W(\widetilde{F})$. ∎

We next show that for a pythagorean field, all quadratic semireal closures arise as above.

Proposition 2.2. *Let (K, Q) be a semiordered pythagorean field with quadratic semireal closure $(\widetilde{K}, \widetilde{Q})$. Let v be the valuation associated with $T = T_Q$ as above.*

(1) *There exists a maximal immediate extension L of K inside $\widetilde{K}$.*
(2) *If L_0 is an immediate quadratic extension of L, then $\widetilde{K}L_0$ is an immediate quadratic extension of $\widetilde{K}$.*
(3) *L is a 2-henselisation of K with respect to v.*
(4) *L is a quadratic semireal closure of (K, Q), so $L = \widetilde{K}$.*

Proof: (1) is an easy application of Zorn's lemma.

(2) Consider an immediate quadratic extension $L_0 = L(\sqrt{a})$. We must show that $\widetilde{K}(\sqrt{a})$ is an immediate extension of $\widetilde{K}$. Write v also for any extension of v. By hypothesis, $L(\sqrt{a})_v = L_v \subseteq \widetilde{K}_v$, so $\widetilde{K}_v = \widetilde{K}(\sqrt{a})_v$ and hence the residue degree $f_{\widetilde{K}(\sqrt{a})/\widetilde{K}} = 1$. Also, $v(\sqrt{a}) \in \Gamma_L$, we have $v(\sqrt{a}) \in \Gamma_{\widetilde{K}}$, so the ramification index $e_{\widetilde{K}(\sqrt{a})/\widetilde{K}} = 1$.

(3) Let L_0 be any immediate quadratic extension of L. The semiordering $\widetilde{Q}$ extends to $\widetilde{K}L_0$ since the extension is immediate [**20**, Lemma 8.2]. But this contradicts the quadratically semireal closed property of $(\widetilde{K}, \widetilde{Q})$. It follows that L must be a 2-henselisation of K with respect to the valuation v ([**12**, Section 26]).

(4) By Theorem 2.1, the field L is quadratically semireal closed with respect to the semiordering induced by $\widetilde{Q}$, so $L = \widetilde{K}$. ∎

From the previous two results, we immediately obtain our main theorem.

Theorem 2.3. *Let (F, Q) be a semiordered pythagorean field and let $(K, \widetilde{Q})$ be a quadratic semireal closure. Let T be the preordering covered by Q. Then $W_T(F) \cong W(K)$.*

As a corollary of the comments prior to Theorem 2.1 on valuation rings, we have the following, which generalises Bröcker's Trivialisation Theorem for fans [**15**, Theorem 12.6] to a much larger class of preorderings.

Corollary 2.4. *Let T be a preordering on a field F which is not an ordering and which has covering number one. Then there exists a nontrivial valuation on F which is fully compatible with T.*

Theorem 2.3 applies only to preorderings with covering number one. However, a field extension can always be made to lower the covering number (while increasing the number of orderings and the size of the Witt ring, but in a very predictable way). To prove this, we make use of the following theorem of Prestel.

THEOREM 2.5. ([20, Lemma 7.5, Lemma 7.7, Theorem 7.8].) *Let v be a real valuation on a field F with value group Γ, maximal ideal $\mathfrak{m}_v$, units U_v and residue class field F_v, and let $s\colon \Gamma \to \dot{F}$ be a semisection of v. There is a one-to-one correspondence between the set of semiorderings Q of F compatible with v and the set*

$$\{\,\mathfrak{P} \mid \mathfrak{P}\colon \Gamma/2\Gamma \to Y_{F_v}\,\} \times \{\,\sigma \mid \sigma\colon \Gamma/2\Gamma \to \{\pm 1\},\ \sigma(\overline{0}) = 1\,\},$$

given as follows: A semiordering Q induces mappings $\mathfrak{P}_Q$ and σ_Q such that

$$\text{(3)}\quad \sigma_Q(\overline{\gamma})s(\gamma) \in Q,\ \forall \gamma \in \Gamma, \quad \textit{and} \quad b + \mathfrak{m}_v \in \mathfrak{P}_Q(\overline{\gamma}) \iff bs(\gamma)\sigma_Q(\overline{\gamma}) \in Q,\ \forall b \in U_v,$$

and mappings σ and $\mathfrak{P}$ induce a semiordering Q by

$$\text{(4)}\qquad a \in Q \iff \frac{a}{s\big(v(a)\big)}\sigma\big(\overline{v(a)}\big) + \mathfrak{m}_v \in \mathfrak{P}\big(\overline{v(a)}\big),\ \forall a \in \dot{F}.$$

PROPOSITION 2.6. *Given a field F with preordering T, there exists a henselian extension K of F with residue class field F and with extension T' of T such that* $\operatorname{cn}(T') = 1$ *and* $T' = T \cdot K^2$.

PROOF: Let $\{\,S_i \mid i \in I\,\}$ be a cover for T. Form an extension field of iterated Laurent series $K = F\big((x_\alpha\colon \alpha \in A)\big)$, where the index set A is chosen so large that there exists an injection φ of I into $B = \left\{\,\prod_{j=1}^{n} x_{\alpha_j} \mid \alpha_j \in A\,\right\}$. Without loss of generality, we may assume that the empty product 1 is in the image of φ, say $\varphi(i_0) = 1$. (To make sense of the iterated Laurent series, one should well-order the set A and adjoin one indeterminate at a time, taking unions for limit ordinals.) Now K has a natural henselian valuation v with residue class field F and value group Γ satisfying

$$\text{(5)}\qquad |\Gamma/2\Gamma| = |2^A| \geqslant |B| \geqslant |I|.$$

Note that any element of K can be written in the form ay^2b, where $a \in U_v$, $y \in K$ and $b \in B$, since B serves as a set of representatives for all values modulo squares. Define a subset Q of K by

$$Q = \{\,ay^2b \mid y \in K,\ b \in B,\ a \in U_v,\ \text{with } \overline{a} \in \overline{S}_b\,\},$$

where we define

$$\overline{S}_b = \begin{cases} S_i, & \text{if } b = \varphi(i) \\ \text{any } S_j \neq S_{i_0}, & \text{if } b \notin \operatorname{im}(\varphi). \end{cases}$$

The set Q is a semiordering by Theorem 2.5. We claim that Q covers T', the preordering of K defined to be the intersection of all orderings of K extending those of T. Indeed, let $ay^2b \in T_Q$; that is, $ay^2bQ = Q$. By Theorem 2.5, $\overline{u} \in \overline{S}_1 \iff uab \in abQ = Q$. Therefore, $\overline{a}\overline{S}_1 = \overline{S}_b$, which can occur only if $b = 1$. Thus we have $aQ = Q$, we have $\overline{a}\overline{S}_{b'} = \overline{S}_{b'}$ for all $b' \in B$. Since $\{\overline{S}_{b'}\}_{b' \in B} = \{S_i\}_{i \in I}$ covers T, we obtain $\overline{a} \in T$. Therefore $a \in T \cdot K^2 \subseteq T'$. Furthermore, since all elements of $T \cdot K^2$ have the form ay^2 with $a \in U_v$ and sums of such elements again have this form, we obtain $T' = T \cdot K^2$. ∎

We see from the proof above that if $|I|$ (the covering number of T) is finite and of 2-power order, then we can have equality in (5). More generally, we have the following corollary.

Corollary 2.7. *Given any pythagorean field F with preordering T, there exists an extension field K of F which is quadratically semireal closed and such that $W(K)$ is isomorphic to a group ring $W_T(F)[G]$, where G is an elementary Abelian 2-group whose size depends on the covering number of T. If $\operatorname{cn}(T)$ is finite, then $|G| = 2^n$ with $n \geqslant \log_2 \operatorname{cn}(T)$ suffices.*

Proof: Let F', T' be as given in Proposition 2.6. Since F is pythagorean and the extension is henselian, the field F' is also pythagorean. From (5) we obtain the bound $|A| = n \geqslant \log_2 \operatorname{cn}(T)$ for the number of indeterminates that suffices. Let Q' be a semiordering which covers T'. We have $W_{T'}(F') \cong W_T(F)[G]$ essentially by a theorem of Springer (see [**16**, Section 5.7]). Now apply Theorem 2.3 to (F', Q') to obtain K. ∎

3. Witt ring computations

In this section we translate the concept of covering number into the language of Witt rings, and give an effective means of calculating covering numbers for Witt rings of elementary type. All work is done in the category of reduced Witt rings. In particular, the nilradical is zero. The construction which gives all the finitely generated rings in this category is described prior to Proposition 3.4 (in which one would take the group Δ to be finite). Although we are freely using the language of fields in this section, it is not difficult to show that all definitions and concepts are valid in the category of abstract Witt rings (of finite chain length), and thus also in the category of abstract spaces of orderings. The abstract situation will be explored further in a subsequent paper.

Recall that for T a preordering on a field F, the *chain length of* T, $\operatorname{cl}(T)$, can be defined in terms of elements represented by binary T-forms, that is, forms in $W_T(F)$ [**15**, Section 8]. In particular, $\operatorname{cl}(T)$ is the supremum of all integers k for which there exists a chain

$$D_T\langle 1, a_0\rangle \subsetneq D_T\langle 1, a_1\rangle \subsetneq \cdots \subsetneq D_T\langle 1, a_k\rangle.$$

We define the chain length of a reduced Witt ring R to be $\mathrm{cl}(R) = \mathrm{cl}(T)$, where $R \cong W_T(F)$, when it is finite. The lemma below follows directly from [**17,** Theorem 4.2.1].

Lemma 3.1. *Let $W(F)$ be a Witt ring and T a preordering on F.*

(1) $\mathrm{cl}(T) = 1$ *if and only if T is an ordering, if and only if* $W_T(F) \cong \mathbb{Z}$.
(2) *T is a fan if and only if* $\mathrm{cl}(T) \leqslant 2$. *Furthermore,* $\mathrm{cl}(T) = 2$ *if and only if* $W_T(F) \cong \mathbb{Z}[\Delta]$, *$\Delta$ a nontrivial elementary Abelian 2-group.*
(3) *If* $W_T(F) \cong R_1 \times \cdots \times R_m$, *where each R_i has finite chain length, then* $\mathrm{cl}\big(W_T(F)\big) = \sum_{i=1}^{m} \mathrm{cl}(R_i)$.
(4) *If* $W_T(F) \cong R[\Delta]$, *where Δ is an elementary Abelian 2-group and R is a reduced Witt ring with* $\mathrm{cl}(R) \geqslant 2$, *then* $\mathrm{cl}\big(W_T(F)\big) = \mathrm{cl}(R)$.

The chain length can also be computed (when it is finite) directly from $W_T(F)$, using the correspondence between the structure of $W_T(F)$ and $\mathcal{I}_T$, the involution subgroup of the W-group $\mathcal{G}_F$ corresponding to T, as described in [**9**] and [**18**]. We refer the reader to [**19**] for the definition of a W-group. Recall that $\mathcal{I}_T$ is a closed subgroup of the W-group, generated by involutions (none of which are in the Frattini subgroup $\Phi(\mathcal{G}_F)$), with the property that T is precisely the set of elements in F whose square roots are fixed by $\mathcal{I}_T$. These groups all lie in the category of pro-2-groups of exponent at most 4, and with squares central. Free products of W-groups in this category correspond to direct products of Witt rings (in the category of Witt rings), and semidirect products correspond to group ring constructions. The connection between the structure of $\mathcal{I}_T$ and $\mathrm{cl}(T)$ is given in [**9,** Theorem 4.2]. This is the W-group analog to [**11,** Lemma 2.1]. In particular, $\mathrm{cl}(T) = \mathrm{cl}(\mathcal{I}_T)$, where for G a pro-2-group, $\mathrm{cl}(G)$ is as defined in [**11,** Section 2].

We next show that the covering number of a preordering is also a Galois-theoretic property. While the proof given below is essentially analogous to [**11,** Theorem 5.1], note that the result is stronger, in that we are showing this to be true for any preordering in any field, not just for the set of squares in a pythagorean field.

Theorem 3.2. *Let T, T' be preorderings on fields F, F' respectively, and let $\mathcal{I}, \mathcal{I}'$ be corresponding involution subgroups in $\mathcal{G}_F$ and $\mathcal{G}_{F'}$ respectively. If $\mathcal{I} \cong \mathcal{I}'$, then* $\mathrm{cn}(T) = \mathrm{cn}(T')$.

Proof: We need to show that any cover of T can be detected using only properties of $\mathcal{I}$. Kummer theory and the definition of $\mathcal{I}$ give a canonical isomorphism $\dot{F}/\dot{T} \cong H^1(\mathcal{I}) = \mathrm{Hom}(\mathcal{I}, \mathbb{Z}/2\mathbb{Z})$. As in [**11,** proof of Theorem 5.1], we let ψ be the image of the class of -1 under this isomorphism. Suppose that T has a cover $S_i, i \in I$. This can be expressed in terms of $H^1(\mathcal{I})$ and ψ by translating the conditions that each S_i is a semiordering containing T, and that $\bigcap_{i \in I} \{x \in F \mid xS_i \subseteq S_i\} = T$, into conditions

https://doi.org/10.1017/S0004972700033797 Published online by Cambridge University Press

only involving $H^1(\mathcal{I})$ and ψ. It is the fact that each S_i must contain T that allows us to work with $\mathcal{I}$ instead of $\dot{F}/(\sum \dot{F}^2)$ in the translation below.

Following [**11**, proof of Theorem 5.1], for each $i \in I$, we let A_i be the subset of $H^1(\mathcal{I})$ corresponding to the set of $\dot{T}$-cosets of $\dot{F}$ contained in S_i. (Note that each $\dot{S}_i$ is a union of $\dot{T}$-cosets.) The condition that $1 \in S_i$ is translated as $0 \in A_i$. That $S_i \cap -S_i = \{0\}$ and $S_i \cup -S_i = F$ is expressed as $H^1(\mathcal{I}) = A_i \dot{\cup} (\psi + A_i)$. To express the condition that every (non-empty) sum of finitely many non-zero elements of S_i is non-zero uses the representation of the Witt-Grothendieck ring of T-forms in terms of generators and relations: $\widehat{W_T}(F) \cong \mathbb{Z}[H^1(\mathcal{I})]/J$, where J is the ideal generated by all formal sums (in the group ring) $a + b - c - d$ such that $a, b, c, d \in H^1(\mathcal{I})$, $a + b = c + d$ in $H^1(\mathcal{I})$, and $a \cup b = c \cup d$ in $H^2(\mathcal{I})$, the second cohomology group. (That these are the appropriate relations for J follows from [**9**, Theorem 3.3] or [**10**].) Using Witt's decomposition theorem ([**15**, Corollary 1.21]), the condition that sums of nonzero elements in S_i be nonzero is equivalent to the condition that for any $a_1, \dots, a_n \in A_i$, the formal sum $a_1 + \cdots + a_n$ in $\mathbb{Z}[H^1(\mathcal{I})]$ is not congruent to any formal sum $b_1 + \cdots + b_{n-2} + 0 + \psi$ modulo J. It now follows from [**2**, Section 2, Kor. to Satz 6] that ψ can be identified in $H^1(\mathcal{I})$ as being the only continuous homomorphism whose kernel contains no element of order 2 outside its Frattini subgroup. (This is essentially because T extends to $F(\sqrt{a})$ as long as $a \notin -T$. Therefore, such an extension is real, and the corresponding subgroup of the W-group will contain nontrivial involutions.) Thus the statement that each S_i is a semiordering containing T can be satisfied group theoretically in $\mathcal{I}$.

It remains to express, in terms of the group $\mathcal{I}$, the condition that $S_i, i \in I$, cover T. But this can be expressed as $S_i, i \in I$, cover T if and only if $\bigcap_{i \in I} \{a \in H^1(\mathcal{I}) \mid a + A_i = A_i\} = \{0\}$. $\square$

Since the covering number of a field (or in general any preordering) of finite chain length depends only on the isomorphism type of the corresponding reduced Witt ring, we can then make the following definition of the covering number of a reduced Witt ring, which is the Witt ring analogue to the definition of covering number of the absolute pro-2 Galois group of a field.

DEFINITION 3.3: Let F be a formally real field and let T be a preordering of finite chain length. We define the covering number of $W_T(F)$ to be $\mathrm{cn}(W_T(F)) = \mathrm{cn}\,(T)$. In particular, $\mathrm{cn}(W_{\mathrm{red}}(F)) = \mathrm{cn}\,(F)$.

It is well known (see [**6**, **16**]) that reduced Witt rings of finite chain length can be constructed recursively through the operations of direct product (in the category of reduced Witt rings) and group ring construction – that is, the reduced Witt rings of finite chain length are precisely the collection $\mathcal{R}$ of (isomorphism types of) rings such that

(1) $\mathbb{Z} \in \mathcal{R}$,
(2) if $R_1, \ldots, R_m \in \mathcal{R}$, then $R_1 \times \cdots \times R_m \in \mathcal{R}$ (where $\times$ denotes direct product in the category of Witt rings), and
(3) if $R \in \mathcal{R}$ and if Δ is an elementary Abelian 2-group, then $R[\Delta] \in \mathcal{R}$.

Also, we have the isomorphisms $\mathbb{Z} \times \mathbb{Z} \cong \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ and $(\mathbb{Z}[\Delta_1])[\Delta_2] \cong \mathbb{Z}[\Delta_1 \times \Delta_2]$. Other than these two isomorphisms and the obvious fact that the rings R_i in a direct product construction can be permuted, the construction of a given isomorphism type of reduced Witt ring of finite chain length is unique.

A reduced Witt ring will be called *decomposable* if it can be written as $R_1 \times R_2$ where R_1 and R_2 are reduced Witt rings, and otherwise it will be called *indecomposable.* The next proposition follows immediately from [**16**, Corollary 6.25].

PROPOSITION 3.4. *Let $R \not\cong \mathbb{Z}$ be a reduced Witt ring of finite chain length.*

(1) *There exists an elementary Abelian 2-group Δ (possibly trivial) together with indecomposable reduced Witt rings $R_1, \ldots, R_m$, $2 \leqslant m < \infty$, such that $R \cong (R_1 \times \cdots \times R_m)[\Delta]$. Moreover, $\mathrm{cl}(R_1), \ldots, \mathrm{cl}(R_m) < \mathrm{cl}(R)$.*
(2) *This presentation of R is unique up to a permutation of $R_1, \ldots, R_m$.*
(3) *R is indecomposable if and only if $\Delta \neq \{1\}$ in (1).*

We now describe an effective method for calculating $\mathrm{cn}(R)$ for a reduced Witt ring of finite chain length. This is the Witt ring version of [**11**, Propositions 5.6, 5.7].

PROPOSITION 3.5. *Let R be a reduced Witt ring of finite chain length.*

(1) *If $R \cong R_1 \times \cdots \times R_m$, then $\mathrm{cn}(R) = \mathrm{cn}(R_1) + \cdots + \mathrm{cn}(R_m)$.*
(2) *If $R = R'[\Delta]$, then*

$$\mathrm{cn}(R) = \begin{cases} 2, & \text{if } (\Delta, R') \cong (\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \\ \left\lceil \dfrac{\mathrm{cn}(R')}{|\Delta|} \right\rceil, & \text{if } |\Delta| < \infty \text{ and } (\Delta, R') \not\cong (\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \\ 1, & \text{if } |\Delta| = \infty. \end{cases}$$

A straightforward translation exercise now allows one to determine $\mathrm{cn}(R)$ for reduced Witt rings R of finite chain length. As in the final table of [**11**], we can easily write down the reduced Witt rings corresponding to pythagorean fields with a limited number of square classes, and determine their covering numbers. Those with covering number one correspond to semireal closed fields. This table is given in the Appendix for up to 32 square classes. Determining the covering number of a formally real field which is not pythagorean from the structure of its Witt ring is similarly straightforward. By Theorem 3.2 above, one simply needs to determine its reduced Witt ring and then compute the covering number for this.

4. Connections with strongly order closed fields

We have demonstrated that we can control the growth of the reduced Witt ring under special algebraic extensions by restricting ourselves to the orderings over a preordering with covering number one. This is in contrast to the work in [**7**], where the entire space of orderings was used and order closed and strongly order closed fields were investigated. (See the introduction to this paper for definitions.) In this section, we look at some connections between the notions of semireal closed and strongly order closed. In [**7**, Theorem 2.1] it is shown that a field F being strongly order closed is equivalent to F being pythagorean and having the property that every polynomial in $F[x]$ of odd degree has a root in F. In comparison, we have

Proposition 4.1. *A field F is semireal closed if and only if it is quadratically semireal closed and every polynomial in $F[x]$ of odd degree has a root in F.*

Proof: It is shown in [**11**, Lemma 4.1] that a field is semireal closed if and only if it is quadratically semireal closed and its absolute Galois group is a pro-2 group. Since this latter condition is equivalent to the field having no odd degree extensions, the result follows. ∎

From this, we easily obtain the fact that the semireal closed fields which we have been studying here are strongly order closed, and in particular, are order closed.

Proposition 4.2. *Every semireal closed field is strongly order closed.*

Proof: We know that any semireal closed field is pythagorean. From Proposition 4.1, we know that it has no odd degree extensions, and thus every minimal extension is quadratic. By [**7**, Theorem 2.1], it is strongly order closed. ∎

Corollary 4.3.

(1) *Every semireal closed field is an intersection of real closed fields.*
(2) *Every quadratically semireal closed field is an intersection of Euclidean fields.*

Proof: (1) By Proposition 4.2, all semireal closed fields are strongly order closed. It is clear that a strongly order closed field is order closed, and such fields are known to be equal to the intersections of all their real closures inside a fixed algebraic closure [**7**, Theorem 2.9].

(2) is rather trivial, in that every pythagorean field is, in fact, an intersection of Euclidean fields. This is easy to see; just take K to be the intersection of all Euclidean closures of a pythagorean field F. Then K/F is a 2-extension. But adjoining any square root to F must kill at least one ordering. Since all orderings of F extend to K, we must have $K = F$. ∎

Appendix: Table of Reduced Witt Rings with a small number of square classes

The notation in the following table is as follows: $\mathbb{Z}_n$ denotes the additive group of $\mathbb{Z}/n\mathbb{Z}$; following [**11**, p. 75], D_n denotes the free pro-2 product of n copies of $\mathbb{Z}_2$; the operations in the Galois group column are described in [**11**] and in more detail in [**13**]; the operations in the W-group column are defined in [**18**]; the notation in the Witt ring column is defined in [**16**]. In each case, the operations are defined within a specific category. For example, the direct product in the category of Witt rings is not the same as in the category of rings.

No. of sq. cls.	Pro-2 Galois group $G_F(2)$	W-group $\mathcal{G}_F$	Witt ring $W(F)$	cover. num.
2	D_1	$\mathbb{Z}_2$	$\mathbb{Z}$	1
4	D_2	$\mathbb{Z}_2 * \mathbb{Z}_2 \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_2$	$\mathbb{Z}[x]$	2
8	$\mathbb{Z}_2 \rtimes D_2$	$\mathbb{Z}_4 \rtimes (\mathbb{Z}_2 * \mathbb{Z}_2)$	$\mathbb{Z}[x, y]$	1
8	D_3	$\mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2$	$\mathbb{Z} \times \mathbb{Z}[x]$	3
16	$\mathbb{Z}_2^2 \rtimes D_2$	$\mathbb{Z}_4 \rtimes (\mathbb{Z}_4 \rtimes (\mathbb{Z}_2 * \mathbb{Z}_2))$	$\mathbb{Z}[x, y, z]$	1
16	$(\mathbb{Z}_2 \rtimes D_2) * D_1$	$\mathbb{Z}_2 * (\mathbb{Z}_4 \rtimes (\mathbb{Z}_2 * \mathbb{Z}_2))$	$\mathbb{Z} \times \mathbb{Z}[x, y]$	2
16	$\mathbb{Z}_2 \rtimes D_3$	$\mathbb{Z}_4 \rtimes (\mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2)$	$\mathbb{Z}^3[x]$	2
16	D_4	$\mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2$	$\mathbb{Z}[x] \times \mathbb{Z}[y]$	4
32	$\mathbb{Z}_2^2 \rtimes D_3$	$\mathbb{Z}_4 \rtimes (\mathbb{Z}_4 \rtimes (\mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2))$	$(\mathbb{Z} \times \mathbb{Z}[x])[y, z]$	1
32	$\mathbb{Z}_2^3 \rtimes D_2$	$\mathbb{Z}_4 \rtimes (\mathbb{Z}_4 \rtimes (\mathbb{Z}_4 \rtimes (\mathbb{Z}_2 * \mathbb{Z}_2)))$	$\mathbb{Z}[x, y, z, w]$	1
32	$\mathbb{Z}_2 \rtimes ((\mathbb{Z}_2 \rtimes D_2) * D_1)$	$\mathbb{Z}_4 \rtimes ((\mathbb{Z}_4 \rtimes (\mathbb{Z}_2 * \mathbb{Z}_2)) * \mathbb{Z}_2)$	$(\mathbb{Z} \times \mathbb{Z}[x, y])[z]$	1
32	$\mathbb{Z}_2 \rtimes D_4$	$\mathbb{Z}_4 \rtimes (\mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2)$	$(\mathbb{Z}[x] \times \mathbb{Z}[y])[z]$	2
32	$(\mathbb{Z}_2^2 \rtimes D_2) * D_1$	$(\mathbb{Z}_4 \rtimes (\mathbb{Z}_4 \rtimes (\mathbb{Z}_2 * \mathbb{Z}_2))) * \mathbb{Z}_2$	$\mathbb{Z} \times \mathbb{Z}[x, y, z]$	2
32	$(\mathbb{Z}_2 \rtimes D_2) * D_2$	$(\mathbb{Z}_4 \rtimes (\mathbb{Z}_2 * \mathbb{Z}_2)) * (\mathbb{Z}_2 * \mathbb{Z}_2)$	$\mathbb{Z}[x, y] \times \mathbb{Z}[z]$	3
32	$(\mathbb{Z}_2 \rtimes D_3) * D_1$	$(\mathbb{Z}_4 \rtimes (\mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2)) * \mathbb{Z}_2$	$\mathbb{Z} \times (\mathbb{Z}^3[x])$	3
32	D_5	$\mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2$	$\mathbb{Z} \times \mathbb{Z}[x] \times \mathbb{Z}[y]$	5

References

[1] R. Baer, *Linear algebra and projective geometry* (Academic Press, New York, 1952).

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

[3] E. Becker and E. Köpping, 'Reduzierte quadratische Formen und Semiordnungen reeller Körpern', *Abh. Math. Sem. Univ. Hamburg* **46** (1977), 143–177.

[4] L. Bröcker, 'Zur Theorie der quadratischen Formen über formal reellen Körpern', *Math. Ann.* **210** (1974), 233–256.

[5] T. Craven, 'The Boolean space of orderings of a field', *Trans. Amer. Math. Soc.* **209** (1975), 225–235.

[6] T. Craven, 'Characterizing reduced Witt rings of fields', *J. Algebra* **53** (1978), 68–77.

[7] T. Craven, 'Fields maximal with respect to a set of orderings', *J. Algebra* **115** (1988), 200-218.

[8] T. Craven, '∗-valuations and hermitian forms on skew fields', in *Valuation Theory and its Applications, Vol. 1*, Fields Inst. Commun. **32** (Amer. Math. Soc., Providence, RI, 2002), pp. 103–115.

[9] T. Craven and T. Smith, 'Formally real fields from a Galois theoretic perspective', *J. Pure Appl. Algebra* **145** (2000), 19–36.

[10] T. Craven and T. Smith, 'Witt ring quotients associated with W-groups', (unpublished notes).

[11] I. Efrat and D. Haran, 'On Galois groups over pythagorean semi-real closed fields', *Israel J. Math.* **85** (1994), 57–78.

[12] O. Endler, *Valuation theory* (Springer–Verlag, Berlin, Heidelberg, New York, 1972).

[13] B. Jacob and R. Ware, 'A recursive description of the maximal pro-2 Galois group via Witt rings', *Math. Z.* **200** (1989), 379–396.

[14] T. Jacobi and A. Prestel, 'Distinguished representations of strictly positive polynomials', *J. Reine Angew. Math.* **532** (2001), 223–235.

[15] T.Y. Lam, *Orderings, valuations and quadratic forms*, Conference Board of the Mathematical Sciences **52** (Amer. Math. Soc., Providence, RI, 1983).

[16] M. Marshall, *Abstract Witt rings*, Queen's Papers in Pure and Appl. Math. **57** (Queen's University, Kingston, Ontario, 1980).

[17] M. Marshall, *Spaces of orderings and abstract real spectra*, Lecture Notes in Math. **1636** (Springer–Verlag, Berlin, Heidelberg, New York, 1996).

[18] J. Mináč and T. Smith, 'Decomposition of Witt rings and Galois groups', *Canad. J. Math* **47** (1995), 1274–1289.

[19] J. Mináč and M. Spira, 'Witt rings and Galois groups', *Ann. of Math.* **144** (1996), 35–60.

[20] A. Prestel, *Lectures on formally real fields*, Lecture Notes in Math. **1093** (Springer–Verlag, Berlin, Heidelberg, New York, 1984).

[21] A. Prestel and C. Delzell, *Positive polynomials: from Hilbert's 17th problem to real algebra*, Springer Monographs in Math. (Springer–Verlag, Berlin, Heidelberg, New York, 2001).

Department of Mathematics
University of Hawaii
Honolulu, HI 96822–2273
United States of America
e-mail: tom@math.hawaii.edu

Department of Mathematical Sciences
University of Cincinnati
Cincinnati, OH 45221–0025
United States of America
e-mail: tsmith@math.uc.edu