Characterizing Reduced Witt Rings of Fields

THOMAS C. CRAVEN*

Department of Mathematics, University of Hawai'i, Honolulu, Hawai'i 96822

Communicated by Graham Higman
Received February 7, 1977

1. INTRODUCTION AND NOTATION

Let $W(F)$ denote the Witt ring of nondegenerate symmetric bilinear forms over a field $F$. In this paper we shall be concerned only with formally real fields, for which we write $W_{\text{red}}(F) = W(F)/\text{Nil} W(F)$ for the reduced Witt ring. In [13, 14] the rings $W(F)$ and $W_{\text{red}}(F)$ are shown to be special cases of abstract Witt rings and a great deal of the ring structure is developed in this setting. In [6] it is shown that not all of these abstract Witt rings can be Witt rings of fields and more examples are given in [7]. In this paper we shall show precisely which of the torsion free abstract Witt rings (subject to a certain finiteness restriction) can be reduced Witt rings of fields. In Section 2 we give an inductive construction of all reduced Witt rings of fields with only finitely many places into the real numbers $\mathbb{R}$. This construction provides a powerful tool for proving ring-theoretic facts about reduced Witt rings. We apply this construction in Section 3 to obtain an explicit description of the structure of these rings in terms of the real places on any field whose reduced Witt ring is isomorphic to the given ring. In Section 4 we look at another application of the inductive construction. We prove the following conjecture in the case that $F$ is a field with only finitely many places into $\mathbb{R}$: If $\varphi \in W(F)$ maps into $I^nF_{\alpha}$ for each real closure $F_{\alpha}$ of $F$, then $\varphi$ is in $W_{\text{red}}(F) \cup I^nF$, where $IF$ denotes the maximal ideal of all even dimensional forms over $F$ and $W_{n}(F)$ denotes the torsion subgroup of $W(F)$.

Before we begin our inductive construction, we shall need some definitions and notation. As in [13], we shall write $X(F)$ or $X(W_{\text{red}}(F))$ for the Boolean space of orderings of a field $F$, and we shall think of $W_{\text{red}}(F)$ as a subring of $\mathcal{C}(X(F), \mathbb{Z})$, the ring of all continuous functions from $X(F)$ to $\mathbb{Z}$, where $\mathbb{Z}$ has the discrete topology. Recall that the topology of $X(F)$ is induced by the Harrison subbasis, which consists of all sets of the form

$$W(a) = \{P \in X(F) \mid a \notin P\} \quad \text{for} \quad a \in F^* = F - \{0\}.$$
We shall write $F^\times$ for the group of nonzero squares in $F$ and $|S|$ for the cardinality of any set $S$. For any ring $A$, we write $A^\times$ for the group of units of $A$. Our valuation theoretic notation will follow [4]. In particular, $\mathcal{M}(F)$ will denote the set of all places from $F$ to $\mathbb{R}$. Let $\sigma, \tau$ be any places on $F$ with formally real residue class fields. We write $\Gamma_\sigma$ for the value group of $\sigma$ and $A_\sigma = \Gamma_\sigma/\Gamma_\sigma^2$. (All valuations will be written multiplicatively.) The valuation ring associated with $\sigma$ will be denoted by $A_\sigma$. We shall often think of $A_\sigma$ as a vector space over the field of 2 elements $\mathbb{F}_2$. We write $[\sigma, \tau]$ for the finest place through which both $\sigma$ and $\tau$ factor and $A_{\sigma, \tau} = A_{[\sigma, \tau]}$. Note that the valuation ring of $[\sigma, \tau]$ is the product $A_\sigma A_\tau$. We say an ordering $P \in X(F)$ is compatible with $\sigma \in M(F)$ if $\sigma(P) \geq 0$, and we shall denote the set of such orderings by $X_\sigma$. Thus $X(F)$ is the disjoint union of the sets $X_\sigma$ for $\sigma \in M(F)$.

2. The Inductive Characterization

For a Boolean space $X$, we consider Witt subrings of $\mathcal{C}(X, \mathbb{Z})$ as defined in [13]. We call a Witt subring $R$ of $\mathcal{C}(X, \mathbb{Z})$ realizable if there exists a formally real field $F$ and a homeomorphism of $X$ with $X(F)$ which induces an isomorphism of $W_{\text{red}}(F) \subseteq \mathcal{C}(X(F), \mathbb{Z})$ with $R \subseteq \mathcal{C}(X, \mathbb{Z})$. If we restrict ourselves to the case where $\mathcal{M}(F)$ is finite, we obtain the following characterization of realizable rings.

**Theorem 2.1.** Realizable rings for which the field has only finitely many places into $\mathbb{R}$ are precisely those given by the following inductive construction:

(a) $\mathbb{Z}$ is realizable.

(b) If $R_1$ and $R_2$ are realizable and $M_i$ is the unique maximal ideal of $R_i$ containing 2, then $R = \mathbb{Z} + M_1 \times M_2$ is realizable, where $\mathbb{Z}$ has the diagonal embedding in $R_1 \times R_2$.

(c) If $R_0$ is realizable, then so is the group ring $R_0[\Lambda]$ where $\Lambda$ is any group of exponent 2.

**Remarks 2.2.**

1. If $F_1$ and $F_2$ both have reduced Witt rings isomorphic to $R$, and $\mathcal{M}(F_1)$ is finite with cardinality less than $\mathcal{M}(F_2)$, then we shall see in Section 3 that $|\mathcal{M}(F_2)| \leq 2 |\mathcal{M}(F_1)|$. Thus the finiteness restriction on realizable rings is independent of the chosen field. As a special case, the theorem characterizes reduced Witt rings of fields with finitely many orderings.

2. In (b), the ideals $M_i$ coincide with $MF_i$ modulo torsion, where $R_i \simeq W_{\text{red}}(F_i)$. The ring $R$ is contained in $\mathcal{C}(X, \mathbb{Z})$ where $X$ is the disjoint union of the spaces for $R_1$ and $R_2$ (cf. [13]).

The proof of Theorem 2.1 will occupy the remainder of this section. We wish to thank Ron Brown for his help in simplifying the proof. We shall make
considerable use of the following reformulation of Brown's theorem that fields with finitely many real places are exact [4, Theorem 6.1].

**Proposition 2.3.** Let $F$ be a formally real field with $\mathcal{A}(F)$ finite and let $\chi_U \in \mathcal{C}(X(F), \mathbb{Z})$ be the characteristic function of a set $U \subseteq X(F)$. Then $2\chi_U \in W_{\text{red}}(F)$ if and only if

1. for each $\sigma \in \mathcal{A}(F)$, there exists $a_\sigma \in F$ with $U \cap X_\sigma = W(a_\sigma) \cap X_\sigma$; and
2. for all $\sigma, \tau \in \mathcal{A}(F)$, the elements $g_\sigma$ and $g_\tau$ have the same image in $\Lambda_{\sigma, \tau}$, where we define $g_\sigma$ to be the image of $a_\sigma$ under $F \to \Lambda_\sigma$.

Note that $g_\sigma$ is independent of the choice of $a_\sigma$ [12, Sect. 2], and $W_{\text{red}}(F)$ is determined by the knowledge of which elements $2\chi_U$ lie in it [13, Proposition 3.8].

Sets of the form $W(a) \cap X_\sigma$ are thus fundamental to understanding the structure of the ring. Each such set is empty, all of $X_\sigma$ or consists of exactly half the elements of $X_\sigma$ [12]. For a more detailed analysis of the structure, see [7].

The proof of our first lemma was inspired by a construction of Bröcker [2].

**Lemma 2.4.** All of the rings constructed by the inductive process of the theorem are realizable by a pythagorean field.

**Proof.** For (a), we can take the real numbers as our field. For construction (b), assume we have pythagorean fields $K_1, K_2$ such that $R_i = W_{\text{red}}(K_i)$. We shall construct a pythagorean field $F$ with Witt ring isomorphic to $R \cong \mathbb{Z} \cong IK_1 \times IK_2$. We first show that we can raise the transcendence degree of $K_i$ over $\mathbb{Q}$ without changing the reduced Witt ring. Let $\alpha$ be the $\alpha$-adic valuation on $K_1(\alpha)$, and let $M = K_1(\alpha^{1/2}, \alpha^{1/3}, \ldots)$ with $\alpha$ the extension of $\alpha$ to $M$. Then the residue class fields $M_\alpha$ and $K_1(\alpha)_\alpha$ are isomorphic to $K_1$, and the value group of $\alpha$ is 2-divisible. Let $\hat{K}_1$ be the henselization of $M$ with respect to $\alpha$. The field $\hat{K}_1$ is pythagorean with $W(\hat{K}_1) \cong W(K_1)$ and transcendence degree over $\mathbb{Q}$ one greater than the transcendence degree of $K_1$ over $\mathbb{Q}$.

Iterating the above construction (infinitely often, if necessary), we may assume that $L \subseteq K_1, K_2$, where $L$ is a purely transcendental extension of $\mathbb{Q}$ and the fields $K_1, K_2$ are algebraic over $L$. We consider two valuations on $L(\alpha)$: the $\alpha$-adic valuation will be denoted by $v$ and the degree valuation will be denoted by $w$. Note that $v$ and $w$ are independent, and for both of them the residue class field is isomorphic to $L$. Theorem 27.6 of [10] implies that there exists a field $L'$ algebraic over $L(\alpha)$ and extensions $v', w'$ of $v, w$, respectively, such that the value groups of $v'$ and $w'$ are 2-divisible and the residue class fields satisfy $L'_v \cong K_1$ and $L'_w \cong K_2$. Let $M_1, \hat{v}$ be the henselization of $L'$ at $v'$ and let $M_2, \hat{w}$ be the henselization of $L'$ at $w'$. Let $F = M_1 \cap M_2$. We have $W(M_i) \cong W(K_i)$ ($i = 1, 2$), so that $F, M_1$ and $M_2$ are all pythagorean. To show that $W(F) \cong \mathbb{Z} + IM_1 \times IM_2$, it will suffice to show that the canonical map $\varphi: F'F'^{-2} \to M_1^2 \times M_2^2$ is an isomorphism, since the Harrison
subbasis determines the reduced Witt ring. It is injective because \( F = M_1 \cap M_2 \).

Let \( v_0 = \hat{v} | F \) and \( w_0 = \hat{v} | F \). Then \( M_1 \) is the henselization of \( F \) at \( v_0 \) and \( M_2 \) is the henselization of \( F \) at \( w_0 \). The valuations \( v_0 \) and \( w_0 \) are independent since they are extensions of \( v \) and \( w \) on \( L(x) \). Given elements \( m_i \in M_i, \ i = 1, 2 \), we can first find elements \( a_i \in F^e \) such that \( m_i/a_i \equiv 1 \) modulo the maximal ideal of the valuation ring of \( \hat{v} \) (for \( i = 1 \)) or \( \hat{w} \) (for \( i = 2 \)). Then apply the approximation theorem for independent valuations [1, Sect. 7.2] to obtain an element \( a \in F \) such that \( \v(a - a_i) < \min(\v(a_i), 1) \) (\( i = 1, 2 \)). Then \( a/a_i - 1 \) lies in the maximal ideal of the valuation ring of \( v_0 \) (for \( i = 1 \)) or \( w_0 \) (for \( i = 2 \)). Thus \( am_i \in M_i^{\infty} \), so the map \( \varphi \) is surjective.

Finally we consider construction (c). Given a group ring \( W(K)[A] \) where \( K \) is a pythagorean field and \( A \) is a group of exponent 2, we may take \( F \) to be an iterated power series field over \( K \), the number of variables being equal to the cardinality of an \( \mathbb{F}_2 \) vector space basis for \( A \). Then \( F \) is pythagorean with \( W(F) \cong W(K)[A] \). This completes the proof of the lemma.

**Lemma 2.5.** If \( W_{\text{red}}(F) \) can be written as \( \mathbb{Z} + M_1 \times M_2 \) where \( M_i \) is the maximal ideal containing 2 in \( R_i \subseteq \mathbb{C}(X_i, \mathbb{Z}) \) (\( i = 1, 2 \)), then for each \( i \), the ring \( R_i \) is realizable by a field \( K_i \) with \( |A_i| < |A(F)| \).

**Proof.** For each \( \sigma \in \mathcal{M}(F) \), we have \( X_\sigma \subseteq X_1 \) or \( X_\sigma \subseteq X_2 \); furthermore, for all pairs \( \sigma, \tau \in \mathcal{M}(F) \), if \( A_{\sigma, \tau} \neq 1 \), then \( X_\sigma \) and \( X_\tau \) are contained in the same \( X_i \) by Proposition 2.3. There is thus an element \( d \in F^e \) close to 1 with respect to each place \( \sigma \) with \( X_\sigma \subseteq X_1 \) and close to \(-1\) with respect to each place \( \sigma \) with \( X_\sigma \subseteq X_2 \) [3, Theorem 2.1(B)]. In particular, the element \( d \) is positive on \( X_1 \), is negative on \( X_2 \) and is a unit in each valuation ring \( A_\sigma \). Let \( K_1 \) be the field \( F(d^{1/2}, d^{1/4}, \ldots) \). Note that [4, Lemma 8.3] applies to any place from \( F \) into a formally real field.

In particular, given any \( \sigma, \tau \in \mathcal{M}(F) \) with \( X_\sigma \subseteq X_1 \), the places \( \sigma, \tau \) and \( \{\sigma, \tau\} \) extend uniquely to places on \( K_1 \) with the same value groups, and so the groups \( A_{\sigma, \tau} \) remain the same. Thus Proposition 2.3 implies \( R_1 \cong W_{\text{red}}(K_1) \). Similarly, \( R_2 \cong W_{\text{red}}(K_2) \) where \( K_2 = F((-d)^{1/2}, (-d)^{1/4}, \ldots) \).

**Proof of Theorem 2.1.** Lemma 2.4 shows that all of the rings constructed are realizable. Conversely, we must show that if \( F \) is a formally real field with \( \mathcal{M}(F) \) finite, then \( R = W_{\text{red}}(F) \) is constructible using (a), (b) and (c). We proceed by induction on \( |\mathcal{M}(F)| \). If \( F \) has a unique place into \( \mathbb{R} \), then \( W_{\text{red}}(F) \) is an integral group ring [5], which can be constructed using (a) and (c). If \( R \) can be written as in Lemma 2.5, we are done by induction and an application of (b). We assume that \( R \) cannot be so written and that \( |\mathcal{M}(F)| > 1 \). Let \( \mathcal{M}(F) = \{\sigma_1, \ldots, \sigma_n\} \) and let \( A \) be the product \( A_1 A_2 \cdots A_n \subseteq F \) where \( A_i \) is the valuation ring of \( \sigma_i \).

We claim first that \( F/A \) is not 2-divisible. Assume the contrary. The subrings of \( F \) which occur as products \( A_1 A_i \), \( i = 2, \ldots, n \) all contain \( A_1 \) and hence are linearly ordered [1, Sect. 4.1]. Renaming the places if necessary, assume \( A_1 A_2 \) is the largest. Then \( A = \prod_{i=1}^n A_i = \prod_{i=1}^n (A_1 A_i) = A_1 A_2 \), so that \( A_{1,2} = 1 \).
since $F'/{A'}$ is 2-divisible. Now partition $\mathcal{M}(F)$ into two subsets $\mathcal{M}_1 \cup \mathcal{M}_2$ via $\sigma_i \in \mathcal{M}_1$ iff $A_{1,i} \neq 1$ for $i \neq 1$ and $\sigma_1 \in \mathcal{M}_1$. Thus $\mathcal{M}_1$ and $\mathcal{M}_2$ are nonempty and have the property that $\sigma \in \mathcal{M}_1$, $\tau \in \mathcal{M}_2$ implies $A_{\sigma, \tau} = 1$; indeed, if $\sigma = \sigma_1$ it is by definition, and if $\sigma \neq \sigma_1$, we have $A_{1, \sigma} \subset A_{1, \sigma} A_{\sigma, \tau} = A_{\sigma, \tau}$ since $A_{1, \sigma} = 1$ and $A_{1, \sigma} \neq 1$ implies $A_{1, \sigma} A_{\sigma, \tau} \neq A_{1, \tau}$. Thus Proposition 2.3 implies we can write $R$ as in Lemma 2.5 with $X_\tau := \bigcup_{\sigma \in \mathcal{M}_\tau} X_\sigma$, a contradiction.

Now let $K$ be the residue class field of the valuation ring $A$. The proof of Proposition 10 of [5] shows that $R \cong \text{W}_{\text{red}}(K)/[A,]$, where $\tau$ is a place with valuation ring $A$. Since $F'/{A'}$ is not 2-divisible, the group $A_{\tau}$ is nontrivial. If we knew that $\text{W}_{\text{red}}(K)$ arose from the inductive construction, we would be done by an application of (c). But $|\mathcal{M}(K)| = |\mathcal{M}(F)|$. Let $B$ be the product of the valuation rings of all the places in $\mathcal{M}(K)$. Then the group $K/B$ is 2-divisible, so that we can use the above argument to divide up the set $\mathcal{M}(K)$ in such a way that $\text{W}_{\text{red}}(K)$ is written as in Lemma 2.5. Thus Lemma 2.5 plus the inductive hypothesis implies the desired conclusion.

3. Characterization by Rooted Trees

In this section we shall make use of some of the language of graph theory. We shall consistently follow the terminology of [11]. To each formally real field $F$ with $\mathcal{M}(F)$ finite we associate a directed, rooted, labelled tree as follows: First look at the directed tree whose points are the valuation rings of $F$ which are products of the $A_\sigma$, $\sigma \in \mathcal{M}(F)$, and whose lines are the inclusion maps. (This is a tree since all valuation rings containing a given one are linearly ordered [1, Sect. 4.1].) Now replace each valuation ring $A$ by the group $F'/(A{A'}^2)$, and replace the inclusion maps by the induced surjections.

The following proposition is a corollary of Lemma 2.4. The proof of Lemma 2.4 gives an explicit construction for the field whose existence is asserted.

**Proposition 3.1.** Given any directed, rooted tree of groups of exponent 2 with the lines corresponding to surjective maps oriented toward the identity group at the root, there exists a pythagorean field which has that tree as its tree of reduced value groups.

We now restrict our attention to fields with a finite number of orderings. Note that knowledge of the actual groups and surjections is not needed. Up to isomorphism of the groups, such a tree is determined by any rooted tree where numbers are assigned to the points corresponding to the number of elements in an $F_2$-basis for $F/{A'}^2$. Thus we are looking at finite trees rooted at a point $v_0$ such that no vertex other than $v_0$ has degree 2 and such that each point $v$ has a nonnegative integer $\text{ord}(v)$ assigned to it satisfying
(3.2) If $v_0, v_1, \ldots, v_n$ is a path in the tree from the root to an endpoint $v_n$, then $0 = \text{ord}(v_0) < \text{ord}(v_1) < \cdots < \text{ord}(v_{n-1}) \leq \text{ord}(v_n)$. We obtain the strict inequalities by identifying isomorphic groups. We would like to know to what extent the tree is unique for a given ring $R$. We shall see that the following example shows essentially the only way in which we fail to get uniqueness.

**Example 3.3.** Let $F_1 = \mathbb{Q}(2^{1/2})(x)$ and $F_2 = \mathbb{Q}(y)$. Each field has four orderings and the nonzero elements of the field modulo sums of squares forms a group with eight elements. Thus the reduced Witt rings are each isomorphic to $\mathbb{Z}[\Lambda]$ where $\Lambda \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ [7, Theorem 3.8]. The tree for $F_1$ is

```
     1
      |
     /|
    / 1
   /   |
  /     0
```

since $F_1$ has two (equivalent) places into $\mathbb{R}$. The tree for $F_2$ is

```
  2
 /|
/ 0
```

In terms of our construction in Theorem 2.1, $W_{\text{red}}(F_1) \cong (\mathbb{Z} + (2\mathbb{Z} \times 2\mathbb{Z}))[\mathbb{Z}_2]$ and $W_{\text{red}}(F_2) \cong \mathbb{Z}[\mathbb{Z}_2 \oplus \mathbb{Z}_2]$.

Therefore, to obtain uniqueness of trees, we impose the additional condition

(3.4) If $v, w$ are endpoints with $\text{ord}(v) = \text{ord}(w)$ and both are adjacent to $u$, then $\text{ord}(u) < \text{ord}(v)$.

Given any tree satisfying (3.2), this can be achieved by changing any occurrence of

```
  v
   |
  /|
 /  w
```

where $\text{ord}(u) = \text{ord}(v) = \text{ord}(w)$ to

```
   v'
   |
 / u
```

where $\text{ord}(v') = \text{ord}(u) + 1$. (If this reduces the degree of $u$ to 2 and $u$ is not the root, then $u$ must be eliminated and $v'$ connected to the next lower point.) Proposition 2.3 shows that this does not change the associated ring since we are merely combining two places which are equivalent (modulo squares).
Theorem 3.5. There is a one-to-one correspondence between isomorphism classes of reduced Witt rings of fields with finitely many orderings and rooted trees, in which no point other than possibly the root has degree 2, together with an integer valued order function satisfying (3.2) and (3.4).

Proof. We have already seen that any such tree determines a ring. Conversely, let \( R \) be a realizable Witt ring. We prove the theorem by induction on the minimum number of points in any tree for \( R \). If the minimum is two, then \( R \) is isomorphic to an integral group ring \( \mathbb{Z}[A] \) and (3.4) implies that there is only one possible tree, namely

\[
\begin{array}{c}
\cdot \ n \\
\downarrow \ 0
\end{array}
\]

where \( 2^e \) is the order of \( A \). Now assume the minimum is greater than 2 and let \( T \) be a tree inducing \( R \) with the minimum number of points. We may assume \( T \) is a tree of reduced value groups for a field \( F \). We consider two cases corresponding to (b) and (c) of Theorem 2.1. In case (b), the tree \( T \) can be partitioned into two rooted subtrees \( T_1, T_2 \) with only the root in common. This corresponds to partitioning the space of orderings and gives us two quotient rings \( R_1 \) and \( R_2 \). The induction hypothesis implies \( T_1 \) and \( T_2 \) are the only possible trees inducing the proper Harrison subbase structure on \( \tilde{X}(R_1) \) and \( \tilde{X}(R_2) \). Hence \( T \) is the only possible tree for \( X(R) = \tilde{X}(R_1) \cup \tilde{X}(R_2) \). In case (c), assume \( R = R_0[A] \) where \( A \) has maximal size. The root \( v_0 \) of \( T \) has degree 1 and is connected to a point \( v_1 \) with \( 2^{\text{ord}(v_1)} \) equal to the order of \( A \). A tree \( T_0 \) for \( R_0 \) can be constructed from \( T \) by deleting \( v_0 \) and the line connecting \( v_0 \) to \( v_1 \), designating \( v_1 \) as the new root, and defining \( \text{ord}_d(v) = \text{ord}(v) - \text{ord}(v_0) \) for all the remaining points \( v \). The induction hypothesis implies \( T_0 \) with \( \text{ord}_d \) is uniquely determined and thus \( T \) is also.

Remarks 3.6. For a field with finitely many orderings, this theorem shows that the isomorphism class of the reduced Witt ring can be characterized by a finite set of integers. In fact, it is not hard to show that the number of integers needed is no more than the number of orderings of the field.

Many facts about the ring can be obtained quickly from the graph, besides the obvious ones such as the number of minimal prime ideals of the ring (i.e., the number of ordering of any associated field). The minimum number \( n \) such that \( R \) is \( n \)-stable (\( M^{n+1} = 2M^n \)) is \( \max \{ \text{ord}(v) \} \) by Theorem 4.3 of [7]. The cardinality of the Harrison subbasis (or equivalently, of the quotient group of \( F \) by the subgroup of sums of squares [8]) is computed in the next proposition.

Proposition 3.7. Let \( F \) be a field with a finite number of orderings and let \( T \) be the tree associated with \( W_{\text{red}}(F) \) by Theorem 3.5. Then the number of elements in the Harrison subbasis is \( 2^h \) where \( h = e - \sum \text{ord}(v) - \text{ord}(w) \), where \( e \) is the
number of endpoints of $T$ (not including the root if it is an endpoint) and the sum is over all lines $(v, w)$ in $T$.

**Proof.** If $W_{\text{red}}(F) \cong \mathbb{Z}$, then $h = e = 1$ is correct. If $W_{\text{red}}(F)$ can be written as in (b) of Theorem 2.1 with corresponding subtrees $T_1$ and $T_2$, we assume by induction that the Harrison subbasis for $R_1$ and $R_2$ have the number of elements given by the theorem: i.e., the number for $R_i$ is $2^{h_i} = e_i + \sum |\text{ord}(v) - \text{ord}(w)|$ with the sum over all lines in $T_i$. Then $h = h_1 + h_2$, which is correct since the Harrison subbasis for $W_{\text{red}}(F)$ is the direct product of the Harrison subbases for $R_1$ and $R_2$. Finally, assume $W_{\text{red}}(F) \cong R_0[A]$ as in (c) of Theorem 2.1 where $A$ has maximal order and the cardinality of the Harrison subbasis of $R_0$ is given by the tree $T_0$. As noted in the proof of Theorem 3.5, the tree $T$ looks like $T_0$ with a new point added for the root and ord increased by $n = \log_2 |A|$ for each point $v$ in $T_0$. If $h_0 = e + \sum |\text{ord}(v) - \text{ord}(w)|$ (sum over lines of $T_0$), then $h = h_0 + n$. This is just what we want. One way of seeing this is to let $F$ be any pythagorean field with $W_{\text{red}}(F) \cong R_n$. The Harrison subbasis for $R_0$ is isomorphic to $F^*/F^{*2}$ [8, Theorem 5]. For $R$, we can take the field $K = F((x_1)) \cdots ((x_n))$, for which it is well known that $|K^*/K^{*2}| = 2^n |F^*/F^{*2}|$. The proposition now follows from Theorem 2.1.

4. Powers of the Maximal Ideal

In this section we give one final example of the use of our inductive construction to prove ring-theoretic facts about Witt rings.

**Theorem 4.1.** Let $F$ be a formally real field with $\mathcal{M}(F)$ finite. Let $\varphi$ be an element of $W(F)$ which maps into $I^*F_n$ in each real closure $F_\alpha$ of $F$. Then $\varphi \in W_{\text{red}}(F) + I^nF$.

**Proof.** In terms of $W_{\text{red}}(F)$, this is equivalent to the statement that

$$W_{\text{red}}(F) \cap \mathcal{C}(X(F), 2^n\mathbb{Z}) \subseteq I^n_F.$$

(4.2)

Write $R = W_{\text{red}}(F)$ and $M = I_{\text{red}}F$. We shall be done if we show (4.2) holds for the rings constructed in Theorem 2.1. It certainly holds for $R = \mathbb{Z}$. For construction (b), assume it holds for $R_1$ and $R_2$ with maximal ideals $M_1$ and $M_2$. Then

$$R \cap \mathcal{C}(X(R), 2^n\mathbb{Z}) = M_1 \times M_2 \cap \mathcal{C}(X(R_1) \cup X(R_2), 2^n\mathbb{Z}) \subseteq M_1^n \times M_2^n = M^n.$$

The group ring construction (c) follows from the following somewhat more general proposition.
Proposition 4.3. If \( R_a \cap \mathcal{C}(X(R_a), 2^n\mathbb{Z}) \subseteq M^n \), then \( R \cap \mathcal{C}(X(R), 2^n\mathbb{Z}) \subseteq M^n \), where \( R = R_0[A] \), \( A \) is any group of exponent 2 and \( M \) is the maximal ideal of \( R \) containing 2.

Proof. We proceed by transfinite induction on the number of elements in an \( F_2 \)-basis of \( A \). We begin with the case of a successor ordinal. Since \( R_0[A] \) is canonically isomorphic to \( R_0[A_1 \times A_2] \), we may assume \( A = \{1, \lambda\} \) has only two elements. So an arbitrary element of \( R \) has the form \( a + b\lambda \) with \( a, b \in R \). Assume \( a + b\lambda \) lies in \( \mathcal{C}(X(R), 2^n\mathbb{Z}) \). Since \( X(R) \) is naturally homeomorphic to \( X(R_0) \times \{0, 1\} \) with \( \lambda \) being constantly 1 on one copy of \( X(R_0) \) and constantly \(-1\) on the other copy, we have \( a + b \) and \( a - b \) in \( \mathcal{C}(X(R_0), 2^n\mathbb{Z}) \). Thus \( 2b \in \mathcal{C}(X(R_0), 2^n\mathbb{Z}) \), so \( b \in \mathcal{C}(X(R_0), 2^{n-1}\mathbb{Z}) \). The induction hypothesis implies that \( a - b \in M^n \subseteq M^n \) and \( b \in M_0^{n-1} \subseteq M^{n-1} \), so \( a + b\lambda = b(1 + \lambda) + (a - b) \in M^n \).

Next consider the case of a limit ordinal \( \alpha \). We have \( R = \cup_{i<\alpha} R_i \), where \( R_i = R_0[A_i] \) and \( A_i \) is generated by the first \( i \) elements of the basis. Let \( M_i \) be the corresponding maximal ideal of \( R_i \). Then \( M = \cup_{i<\alpha} M_i \) and \( M^n = \cup_{i<\alpha} M_i^n \). By the induction hypothesis, \( R_i \cap \mathcal{C}(X(R_i), 2^n\mathbb{Z}) \subseteq M_i^n \). Since \( X(R) = \operatorname{lim} X(R_i) \), we obtain the desired conclusion for \( R \).

The above theorem has already been proved by Marshall for fields with finitely many orderings [15], by Elman et al. [9] for amenable fields and by Brown in the form stated above. Our proof extends known results in that it creates new examples whenever the result is already known for smaller rings. The conjecture has also been considered for arbitrary abstract Witt rings, where we can show that it is always true if \( n = 1 \) or 2 and fails for \( n = 3 \) by an example of R. S. Pierce.

References

9. R. Elman, T.-Y. Lam, and A. Wadsworth, Amenable fields and Pfister extensions, in "Proc. of the Quadratic Forms Conference, Queen's University, August 1976."

