

STABILITY IN WITT RINGS

BY

THOMAS C. CRAVEN⁽¹⁾

ABSTRACT. An abstract Witt ring R is defined to be a certain quotient of an integral group ring for a group of exponent 2. The ring R has a unique maximal ideal M containing 2. A variety of results are obtained concerning n -stability, the condition that $M^{n+1} = 2M^n$, especially its relationship to the ring of continuous functions from the space of minimal prime ideals of R to the integers. For finite groups, a characterization of integral group rings is obtained in terms of n -stability. For Witt rings of formally real fields, conditions equivalent to n -stability are given in terms of the real places defined on the field.

1. Introduction. In recent years, a fruitful way of studying quadratic or bilinear forms over a field F has been to look at the Witt ring $W(F)$ of equivalence classes of nondegenerate symmetric bilinear forms over the field. This has been generalized in various ways, in particular to equivalence classes of nondegenerate hermitian forms over a commutative ring C with involution [10]. If C is a connected semilocal ring, then most of the abstract structure theory for the Witt ring of a field still holds [10]. Knebusch, Rosenberg and Ware have defined the notion of an abstract Witt ring for an abelian q -group G [10, Definition 3.12], a ring of the form $R = \mathbf{Z}G/K$ where $\mathbf{Z}G$ is the integral group ring of G and K is an ideal such that R has only q -torsion. Witt rings of fields and commutative semilocal rings always have this form where G is a group of exponent 2 (in the case of a field, G is the square factor group of the field). In this paper the term Witt ring will always mean Witt ring for a group of exponent 2.

An abstract Witt ring R has a unique maximal ideal containing 2 [10, Lemma 2.13] and we shall always denote this ideal by M . In fact, M is the image of the maximal ideal of $\mathbf{Z}G$ which is the kernel of the homomorphism defined by composing the augmentation map $\mathbf{Z}G \rightarrow \mathbf{Z}$ with the projection $\mathbf{Z} \rightarrow \mathbf{Z}/2\mathbf{Z}$. The main purpose of this paper is to investigate the following condition on R .

Presented to the Society, January 22, 1976; received by the editors September 8, 1975.

AMS (MOS) subject classifications (1970). Primary 13A15, 12D15, 54H10; Secondary 15A63, 16A26.

Key words and phrases. Witt ring, n -stability, group ring, real place, Boolean space.

(¹) Partially supported by NSF Grant MPS75-06987.

© American Mathematical Society 1977

DEFINITION 1.1. A Witt ring R is n -stable if $M^{n+1} = 2M^n$, where n is any integer greater than or equal to 0 and by M^0 we mean the ring R .

The concept of n -stability was first introduced in [5] for Witt rings of formally real fields where it can be related to the theory of Pfister forms over the field. Note that if R is n -stable, then R is m -stable for all $m \geq n$.

In general, Witt rings can be divided into two large classes, those for which the torsion subgroup R_t equals R and those for which R_t equals the nilradical $\text{Nil } R$ [10, §3]. For Witt rings of fields, the latter case contains precisely those for which the field is formally real. If $R_t = R$, then R is a local ring with M as its unique prime ideal and $2^m = 0$ for some m [10, Proposition 3.16]. Thus if R is n -stable, then $M^{m+n} = 2^m M^n = 0$.

Consequently, our main interest is in the case where $R_t = \text{Nil } R$, and this will be the only case considered in §2, 3 and 4. In this case, the reduced Witt ring $R_{\text{red}} = R/\text{Nil } R$ is still a Witt ring for the same group [10, Remark 3.13] and can be embedded naturally in $\mathcal{C}(X, \mathbf{Z})$, the ring of continuous functions from the Boolean (compact, Hausdorff, totally disconnected) topological space X or $X(R)$ of all minimal prime ideals of R (with the induced Zariski topology) to the integers endowed with the discrete topology [9, §3]. The points of X also correspond to the homomorphisms $R \rightarrow \mathbf{Z}$, so the homomorphism $R \rightarrow \mathcal{C}(X, \mathbf{Z})$ takes an element $r \in R$ to "evaluation at r ". If $f \in R$, we shall write \bar{f} for the image of f in R_{red} and identify it with the corresponding function on X . For a field F the set X can be identified with the set of all (total) orderings of F . The map $W(F) \rightarrow \mathcal{C}(X, \mathbf{Z})$ is defined by taking a representative $\sum a_i x_i^2$ for a class in $W(F)$ and computing its signature at each ordering (the number of positive a_i minus the number of negative a_i). This can be generalized to semilocal rings [9, §2].

Corresponding to R there is a natural subbasis of clopen (both closed and open) sets $\mathcal{K}(R)$ for the topology on $X(R)$, and $R_{\text{red}} = \mathbf{Z} + \sum_{U \in \mathcal{K}} 2\mathbf{Z}\chi_U$ where χ_U is the characteristic function of U . The family \mathcal{K} consists of all sets $W(g) = \{x \in X \mid \psi(g)(x) = -1\}$ and their complements where $g \in G$ and ψ is the homomorphism $\mathbf{Z}G \rightarrow R_{\text{red}}$ [9, §3]. For the complement, we shall write $W(-g)$ and use the notation $\pm G$ for the set $\{\pm g \mid g \in G\}$, a subset of $\mathbf{Z}G$. The family \mathcal{K} contains X and is closed under the operation of symmetric difference (denoted by $+$) since $W(g) + W(h) = W(gh)$. Thus \mathcal{K} can be thought of as an \mathbf{F}_2 -vector space where \mathbf{F}_2 is the field of two elements. In §2 we investigate the relationship between n -stability and conditions on \mathcal{K} . In §3, we look specifically at finite spaces and find that a special role is played by the Witt rings R which are isomorphic to group rings. These rings have previously been studied from a different point of view for Witt rings of fields [5] and semilocal rings [15]. In §4 we apply our results to Witt rings of fields. Our main theorem gives a characterization of n -stability of the reduced Witt

ring of a formally real field in terms of the real places on the field, thus generalizing results in [5], [6], [14].

We close this section with two results which are valid even if $R_t = R$.

PROPOSITION 1.2. *Let R be an abstract Witt ring. Then M^n is additively generated by elements of the form $\prod_{i=1}^n (1 + g_i)$ where $g_i^2 = 1, g_i \in R$.*

PROOF. Let $G = \{g \in R | g^2 = 1\}$. Then R is a Witt ring for G [9, p. 219], and M is the image in R of $M_0 = \ker(\mathbf{Z}G + \mathbf{Z}/2\mathbf{Z}) = \{\sum n_i g_i \in \mathbf{Z}G | \sum n_i \text{ is even}\}$. Thus any element of M can be written in the form

$$\sum_{i=1}^{2m} g_i = \sum_{i=1}^m (g_i + 1) - \sum_{i=m+1}^{2m} (-g_i + 1) \quad (g_i \in G, -g_i \in G)$$

and the proposition is true for $n = 1$. For $n > 1$, the ideal M^n is generated by n -fold products of the generators of M .

REMARK 1.3. If $R_t = \text{Nil } R$, then as a function on $X(R)$, the element $\prod (1 - g_i)$ becomes

$$2^n \prod \chi_{W(g_i)} = 2^n \chi_{\cap W(g_i)}.$$

THEOREM 1.4. *Let R be a Witt ring. If M^n is a finitely generated abelian group for some $n \geq 1$ (with say r generators of the form $\prod_{i=1}^n (1 + g_i)$), then R is i -stable for some $i \geq n(r + 1) - 1$.*

PROOF. Let f_1, \dots, f_r be the generators of M^n , each of the form $\prod_{i=1}^n (1 + g_i)$. Then $M^{n(r+1)}$ is generated by all $(r + 1)$ -fold products of the elements f_i . Since $f_i^2 = 2^n f_i$ —because

$$\prod_{i=1}^n (1 + g_i)^2 = \prod_{i=1}^n (2 + 2g_i) = 2^n \prod_{i=1}^n (1 + g_i),$$

we see that

$$M^{n(r+1)} \subseteq 2^n M^{nr} \subseteq 2M^{n(r+1)-1} \subseteq M^{n(r+1)},$$

so that R is i -stable for $i = n(r + 1) - 1$.

2. Relationship of n -stability to \mathcal{K} . From now on we shall assume without explicitly stating it that $R_t = \text{Nil } R$ so that $X(R) \neq \emptyset$. In this section we present several theorems relating the condition of n -stability for R to the structure of the subbasis $\mathcal{K}(R)$. We shall see that in some sense n -stability measures how far the additive group $\mathcal{K}(R)$ is from being closed under the operation of intersection (the multiplication in the Boolean ring of all clopen subsets of X). Our first three results generalize results in [5] from Witt rings of fields to our abstract situation.

LEMMA 2.1. *Let R be a Witt ring for G . Let B be a closed subset of $X = X(R)$ and let α be any point of X not in B . Then there exist g_1, \dots, g_n elements of $\pm G$, such that*

$$\alpha \in D = \bigcap_{i=1}^n W(-g_i) \quad \text{and} \quad B \subseteq D^c = \bigcup_{i=1}^n W(g_i).$$

PROOF. Let β be any point in B . Since \mathcal{C} is a subbasis and X is Hausdorff, there exists an element g_β in $\pm G$ such that $\alpha \in W(-g_\beta)$ and $\beta \in W(g_\beta)$. Doing this for each point β in B we obtain an open cover $\{W(g_\beta) | \beta \in B\}$ of the compact set B . Hence there exist g_1, \dots, g_n in $\{g_\beta | \beta \in B\}$ such that $B \subseteq \bigcup_{i=1}^n W(g_i)$. By our choice of the elements g_β , we have $\alpha \in \bigcap_{i=1}^n W(-g_i)$.

PROPOSITION 2.2. *Let R be a Witt ring for G and let A, B be disjoint closed subsets of $X(R)$. Then there exist an integer n and an element $f \in M^n$ such that $\bar{f}(\beta) = 0$ for $\beta \in B$ and $\bar{f}(\alpha) = 2^n$ for $\alpha \in A$.*

PROOF. Let α be in A . Apply Lemma 2.1 and set f_α equal to the image in R of the group ring element $(1 + g_1)(1 + g_2) \cdots (1 + g_n)$ and $C_\alpha = \bigcap W(-g_i)$. Doing this for each $\alpha \in A$, the sets C_α form an open cover of A with $(\bigcup C_\alpha) \cap B = \emptyset$. Since A is compact there is a finite family C_1, \dots, C_m such that $A \subseteq \bigcup C_i$. Multiply the corresponding elements f_i by powers of 2 if necessary so that we may assume they each have r factors of the form $1 + g$; since $W(-1) = X(R)$, the sets C_i are unchanged. We now have

$$\bar{f}_i(x) = \begin{cases} 2^r & \text{if } x \in C_i, \\ 0 & \text{if } x \in B. \end{cases}$$

Set

$$f = 2^{(m-1)r} \sum_{i=1}^m f_i - 2^{(m-2)r} \sum_{i < j} f_i f_j + \cdots + (-1)^{m-1} f_1 \cdots f_m.$$

Then $f \in M^n$ where $n = mr$ and $\bar{f}(x) = 2^n$ for $x \in \bigcup C_i \supseteq A$ and $\bar{f}(x) = 0$ for $x \in (\bigcup C_i)^c \supseteq B$.

THEOREM 2.3. *Let R be a Witt ring for G . Assume R is n -stable, $n \geq 0$. Then the following condition holds:*

(2.4) *If A, B are disjoint closed subsets of $X(R)$, then there exists an element $f \in M^n$ such that $\bar{f}(\beta) = 0$ for $\beta \in B$ and $\bar{f}(\alpha) = 2^n$ for $\alpha \in A$.*

Furthermore, if M^{n+1} is torsion free, then (2.4) implies n -stability.

PROOF. First assume that R is n -stable, i.e., $M^{n+1} = 2M^n$. Let A, B be disjoint closed subsets of $X(R)$. By Proposition 2.2 there exist an integer r and an element $f_0 \in M^r$ such that $\bar{f}_0(\beta) = 0$ for $\beta \in B$ and $\bar{f}_0(\alpha) = 2^r$ for α

$\in A$. If $r \leq n$, set $f = 2^{n-r}f_0$. Then $f \in M^n$ and satisfies (2.4). If $r > n$, then n -stability implies that $f_0 = 2^{r-n}f$ for some f in M^n . But then again f satisfies (2.4).

Conversely, we must show $M^{n+1} = 2M^n$. Let f_0 be the image in R of the group ring element $\prod_{i=1}^{n+1} (1 + g_i)$, g_i in $\pm G$. By Proposition 1.2 it will suffice to show that $f_0 \in 2M^n$. Let $A = \{x \in X(R) \mid \bar{f}_0(x) \neq 0\}$, a clopen set equal to $\cap W(-g_i)$, and let B be the complement of A . Then (2.4) implies that there exists an element $f \in M^n$ such that $\bar{f}(x) = 2^n$ for $x \in A$ and $\bar{f}(x) = 0$ for $x \notin A$. But then $2\bar{f} = \bar{f}_0$ as elements of $\mathcal{C}(X, \mathbf{Z})$ and $2f, f_0 \in M^{n+1}$. Since M^{n+1} is torsion free we have $f_0 = 2f \in 2M^n$.

It follows from Theorem 2.3 that R_{red} is n -stable for some n if and only if there is a bound on the minimum choices for n in Proposition 2.2. This is related to Theorem 1.4 in that if some power M^r is finitely generated, then there does exist such a bound. We next look at the applications of Theorem 2.3 when $n = 1$.

DEFINITION 2.5. We say that R satisfies the *weak approximation property* (WAP) if $\mathcal{H}(R)$ is a basis, and R satisfies the *strong approximation property* (SAP) if $\mathcal{H}(R)$ is the entire Boolean algebra of clopen sets in $X(R)$.

The SAP condition was first introduced in [11] with more details appearing in [9, §3]. The WAP condition was introduced for Witt rings of fields in [5] in which context it was shown to be equivalent to SAP. For Witt rings of fields there are many equivalent formulations of WAP and SAP [5], [6], many of which have no analogue in the context in which we are working. In our situation, both conditions can be stated in terms of separating sets of points in $X(R)$ by elements of G , essentially as in the case for the Witt ring of a field $W(F)$ where G is the square factor group of the field. It is also known that WAP is not equivalent to SAP in general [4, §3], although it is possible to give a topological argument that they are equivalent if $X(R)$ has only countably many points. Our interest in SAP stems from the fact that R satisfies SAP if and only if $R_{\text{red}} = \mathbf{Z} + \mathcal{C}(X, 2\mathbf{Z})$ [9, Theorem 3.20]. The importance of SAP is evident from the fact that the Witt ring of any formally real algebraic extension of the rational numbers has the property [13, Chapter 3, Example 2.10].

COROLLARY 2.6. *Let R be a Witt ring for G . If R is 1-stable then R satisfies SAP. Furthermore, R_{red} is 1-stable if and only if R satisfies SAP.*

PROOF. We apply Theorem 2.3 with $n = 1$. Condition (2.4) says that for any clopen set A , the function $2\chi_A$ is in the image of M under the canonical map $R \rightarrow \mathcal{C}(X, \mathbf{Z})$. This implies $2\chi_A = \sum n_i 2\chi_{A_i}$ where $n_i \in \mathbf{Z}$, $A_i \in \mathcal{H}(R)$. Dividing by 2 and reducing modulo 2 we obtain $A = \sum A_i \in \mathcal{H}(R)$, where the sum is over all i for which $n_i \equiv 1 \pmod{2}$. Thus SAP holds. For the

converse it suffices to note that R_{red} is torsion free and apply the second part of Theorem 2.3.

REMARK 2.7. For the second part of the above corollary it is interesting to know when R is torsion free. For Witt rings of fields, this is equivalent to the field being formally real and pythagorean (any sum of squares is again a square). More generally, for a connected semilocal ring A with 2 a unit, the Witt ring of A is torsion free if and only if every unit in A which is a sum of squares is already a square and -1 is not a square [9, Corollary 4.20]. In general, R_{red} being 1-stable does not imply that R is 1-stable as shown by the following example.

EXAMPLE 2.8. Let \mathbf{Q} denote the field of rational numbers. Then $W_{\text{red}}(\mathbf{Q})$ is 1-stable since \mathbf{Q} satisfies SAP (the space of orderings X has only one point), but we shall see that $W(\mathbf{Q})$ is not 1-stable. Using the notation and terminology of [5], consider the bilinear form $\langle 1, 2, 5, -10 \rangle$. Since the Legendre symbol $(-2/5) = -1$, the form is anisotropic over \mathbf{Q} [7, Corollary 27c]; since $\langle 1, 2, 5, -10 \rangle$ is a four-dimensional form of determinant -1 (modulo squares), the ring $W(\mathbf{Q})$ is not 1-stable [5, Proposition 3.9]. It is true, however, that $W(\mathbf{Q})$ is 2-stable. Indeed [13, Chapter IV, Corollary 2.5] says that M^3 is additively generated by $8 = 8\langle 1 \rangle$. Thus we have $M^3 = 8W(\mathbf{Q}) \subseteq 2M^2 \subseteq M^3$, which implies $M^3 = 2M^2$.

As another application of Theorem 2.3, we shall determine what it means to be 0-stable. It is quite easy to see that the Witt ring of a formally real field is 0-stable if and only if the field has only two square classes, and this is equivalent to the Witt ring being \mathbf{Z} [5, p. 1176]. In fact, this is the case in general.

THEOREM 2.9. *Let R be a Witt ring for G . Then R is 0-stable if and only if $R = \mathbf{Z}$.*

PROOF. We first note that $X = X(R)$ has only one point. For, Theorem 2.3 implies that if there exist two disjoint nonempty subsets of X , then there exists an element f in R which induces a function which is 0 on one set and 1 on the other, a contradiction of [9, Proposition 3.8] which states that the values of \tilde{f} must all be congruent modulo 2. Thus $\mathcal{C}(X, \mathbf{Z}) = \mathbf{Z}$ and so $R_{\text{red}} = \mathbf{Z}$. Assume $\text{Nil } R \neq 0$.

Without loss of generality we may assume G is the group $\{g \in R \mid g^2 = 1\}$. Let K be the kernel of the homomorphism

$$\mathbf{Z}G \rightarrow R.$$

If G is infinite, let H be a finite subgroup of G with at least four elements. Replace R by $\mathbf{Z}H/(\mathbf{Z}H \cap K)$; then R is a Witt ring for H , $2R$ is a maximal ideal (i.e., R is still 0-stable), $R/\text{Nil } R = \mathbf{Z}$ and $\text{Nil } R \neq 0$ (since H has at least four elements, the ring R has at least four units, hence is not equal to \mathbf{Z}).

But now R is finitely generated as a \mathbf{Z} -module. We now get a contradiction by showing that $\text{Nil } R$ is 2-divisible and thus not finitely generated. Let $a \in \text{Nil } R \subseteq M = 2R$. Then $a = 2b$ for some $b \in R$. Since a is nilpotent, $a^n = 0$ for some n ; hence $2^n b^n = 0$. Thus b^n is torsion; but $R_2 = \text{Nil } R$, so b^n is nilpotent and $b \in \text{Nil } R$.

The converse is clear since \mathbf{Z} is certainly 0-stable.

The remainder of this section will be spent looking carefully at the relationship between n -stability and intersections of elements of \mathcal{K} .

THEOREM 2.10. *If R is n -stable, $n \geq 0$, then any intersection of elements of $\mathcal{K}(R)$ can be written as the symmetric difference of a finite number of n -fold intersections of elements of $\mathcal{K}(R)$. If $n = 1$, the converse holds for R_{red} since $\mathcal{K}(R)$ is closed under symmetric difference.*

PROOF. If $n = 0$, Theorem 2.9 implies that $X(R)$ has only one point, and so the conclusion holds since an empty intersection is the whole space. If $n > 0$, let R be a Witt ring for the group G . Consider an intersection $A = W(g_1) \cap \dots \cap W(g_m)$, $g_i \in \pm G$. If $m \leq n$ we are done, using $W(-1) = X$ if $m < n$; so assume $m > n$.

Assume R is a Witt ring for G with $\psi: \mathbf{Z}G \rightarrow R$ the corresponding surjection. Consider $\prod_{i=1}^m (1 - \psi(g_i)) \in M^m$; since R is n -stable, we have $M^m = 2^{m-n} M^n$. Then by Proposition 1.2, we can write

$$\prod (1 - \psi(g_i)) = 2^{m-n} \sum_j n_j \prod_{i=1}^n (1 - \psi(h_{ij})),$$

where $n_j \in \mathbf{Z}$, $h_{ij} \in \pm G$. Modulo $\text{Nil } R$, these elements become functions from $X(R)$ to \mathbf{Z} giving us the equation

$$2^m \chi_A = 2^{m-n} \sum n_j 2^n \chi_{\cap W(h_{ij})} = 2^m \sum n_j \chi_{\cap W(h_{ij})}.$$

Since 2 is not a zero divisor, we have $\chi_A = \sum n_j \chi_{\cap W(h_{ij})}$. Reducing this modulo 2 we obtain $\chi_A = \chi_{\sum \cap W(h_{ij})}$ where the sum is over all j for which $n_j \equiv 1 \pmod{2}$. Therefore $A = \sum \cap_{i=1}^n W(h_{ij})$ and the theorem is proved.

LEMMA 2.11. *For any sets A_{ij} , the set $\cup_{i=1}^r \cap_{j=1}^n A_{ij}$ can be written as a finite disjoint union of $(\sum_{i=1}^r n_i)$ -fold intersections of the sets A_{ij} and their complements.*

PROOF. We begin by assuming $r = 2$,

$$A = \bigcap_{i=1}^n A_i, \quad B = \bigcap_{i=1}^m B_i.$$

Then $A \cup B$ is the disjoint union of $A \cap B$, $A \cap B^c$ and $B \cap A^c$. We also have $A \cap B^c$ equal to a $(2^m - 1)$ -fold disjoint union of $(m + n)$ -fold intersections where we write B^c as the union over all possible ways of choosing

$B_i^* \in \{B_i, B_i^c\}$, not all $B_i^* = B_i$, of the intersections $\bigcap_{i=1}^m B_i^*$. Similarly, $B \cap A^c$ can be written as such a disjoint union, and thus $A \cup B$ can be written in the prescribed form. For $r > 2$, a simple induction argument completes the proof.

THEOREM 2.12. *Let R be a Witt ring for G . If there exists a number n such that every clopen subset of $X(R)$ can be written as a disjoint union of n -fold intersections of elements of $\mathcal{H}(R)$, then R_{red} is n -stable. If $n = 1$, the converse is also true.*

PROOF. Without loss of generality we may assume $R = R_{\text{red}}$, a subring of $\mathcal{C}(X(R), \mathbf{Z})$. Let $\psi: \mathbf{Z}G \rightarrow R$ be the usual map, and consider $\prod_{i=1}^{n+1} (1 - \psi(g_i)) = 2^{n+1} \chi_A \in M^{n+1}$ where $A = \bigcap W(g_i)$. By Proposition 1.2, it suffices to show that this lies in $2M^n$. By hypothesis, A can be written as a disjoint union of sets $B_k = \bigcap_{j=1}^n W(h_{jk})$, h_{jk} in $\pm G$. Then $\chi_A = \sum \chi_{B_k}$ in $\mathcal{C}(X(R), \mathbf{Z})$. Multiplying by 2^{n+1} to obtain elements of R , we get

$$\prod (1 - \psi(g_i)) = 2 \sum 2^n \chi_{B_k} = 2 \sum \prod_{j=1}^n (1 - \psi(h_{jk})) \in 2M^n.$$

If $n = 1$, Corollary 2.6 implies that $\mathcal{H}(R)$ contains all clopen sets, and thus the converse holds.

COROLLARY 2.13. *If there exist numbers m and n such that every clopen subset of $X(R)$ can be written as an m -fold union of n -fold intersections of elements of $\mathcal{H}(R)$, then R_{red} is (mn) -stable.*

PROOF. Immediate from Lemma 2.11 and Theorem 2.12.

3. Finite spaces and group rings. In this section we are primarily concerned with the case where $X(R)$ is finite. This is not as special as one might think since for any reduced Witt ring R , we can take a finite number of elements in $\mathcal{H}(R)$. The additive subgroup they generate corresponds to a subring S of R with $X(S)$ a finite space homeomorphic to the quotient space of $X(R)$ defined by identifying points of $X(R)$ which are not separated by the chosen subgroup of $\mathcal{H}(R)$.

We assume throughout this section that R is torsion free (i.e., $\text{Nil } R = 0$) and we identify R with its image in $\mathcal{C}(X, \mathbf{Z})$. We shall show that when $X(R)$ is finite, R is always n -stable for some n depending on the cardinality of X which we shall denote by $|X|$.

Our main application is to integral group rings. In Theorem 3.8 we give several conditions equivalent to the condition that R be a group ring. Group rings are important for several reasons. They have the property that the subbasis $\mathcal{H}(R)$ is as small as possible for the given number of points in X , the precise opposite of SAP. Furthermore, they illustrate the worst that can

happen in terms of stability. For these reasons Theorem 3.8 will play a central role in our characterization of n -stability in fields in §4. Also, Witt rings of fields (or semilocal rings) are group rings if and only if the field (or ring) has a particularly nice and well-understood structure [3], [5], [15].

We begin our study by noting a trivial but often-used fact.

LEMMA 3.1. *Let X be a Boolean space, Y a closed subset of X . If \mathcal{C} is an additive subbasis of clopen sets for X , then $\mathcal{C}_Y = \{H \cap Y \mid H \in \mathcal{C}\}$ is an additive subbasis of clopen sets for Y .*

PROOF. $(H_1 \cap Y) + (H_2 \cap Y) = (H_1 + H_2) \cap Y$ for $H_1, H_2 \in \mathcal{C}$.

LEMMA 3.2. *Let X be a finite discrete space with at least two points; let \mathcal{C} be an additive subbasis of clopen sets containing X . Then for any $x \in X$, there exists a set $H \in \mathcal{C}$ such that $x \in H$ and $|H| \leq \frac{1}{2}|X|$.*

PROOF. First note that the lemma is true if $|X| = 2$ since \mathcal{C} contains all subsets of X . Assume X, \mathcal{C} give a counterexample to the lemma with $n = |X|$ minimal. Take $x \in X$ and any $y \neq x$; set $Y = \{y\}^c$ and let \mathcal{C}_Y be as in Lemma 3.1. Let $x \in H' \in \mathcal{C}_Y$ with say $H' = H \cap Y, H \in \mathcal{C}$. Since $x \in H$, we have $|H| > \frac{1}{2}|X|$. If $y \notin H$, then $|H'| = |H| > \frac{1}{2}|X| > \frac{1}{2}|Y|$. If $y \in H$, then $|H'| = |H| - 1 > \frac{1}{2}|X| - 1 = \frac{1}{2}|Y| - \frac{1}{2}$; thus if $|X|$ is even, $|H'| \geq \frac{1}{2}|Y| + \frac{1}{2} > \frac{1}{2}|Y|$, a contradiction of the minimality of n since H' is an arbitrary element of \mathcal{C}_Y containing x . Thus we may assume n is odd. Also, minimality implies there is some H' containing x such that $|H'| \leq \frac{1}{2}|Y| = \frac{1}{2}(n - 1)$. If S is chosen in \mathcal{C} so that $H' = S \cap Y$, then $|S| = \frac{1}{2}(n + 1)$. Now consider the subbasis \mathcal{C}_S for the subspace S . Again the minimality of n implies there exists a set $H_0 \in \mathcal{C}$ containing x such that $|S \cap H_0| \leq \frac{1}{2}|S|$. Also $|H_0| \geq \frac{1}{2}(n + 1)$ since $x \in H_0$ and $|S + H_0| \leq \frac{1}{2}(n - 1)$ since $x \in (S + H_0)^c \in \mathcal{C}$. Therefore

$$\begin{aligned} \frac{1}{2}(n - 1) &\geq |S + H_0| = |S| + |H_0| - 2|S \cap H_0| \geq n + 1 - 2(\frac{1}{2}|S|) \\ &= \frac{1}{2}(n + 1), \end{aligned}$$

a contradiction.

THEOREM 3.3. *If $1 < |X(R)| < \infty$, then R is n -stable for $n \geq r$ where r is the largest integer such that $2^r \leq |X(R)|$.*

PROOF. For any $x \in X$, Lemma 3.2 implies that $\{x\}$ can be written as an intersection of r or less elements of $\mathcal{C}(R)$; hence any subset of X can be written as a disjoint union of r -fold intersections of elements of $\mathcal{C}(R)$. Therefore R is r -stable by Theorem 2.12.

REMARK 3.4. We shall see in Theorem 3.8 that this is the best result possible in the sense that, given X as in the theorem, there exists a ring R which is not

$(r - 1)$ -stable for which $X = X(R)$. In fact, if $|X| = 2^r$ then R is a group ring. If $|X| > 2^r$, one can choose the appropriate subbasis for a group ring (see below) for 2^r of the points and any subbasis for the remaining points; together these will correspond to a ring which has a group ring as a direct factor.

The next two lemmas are aimed at obtaining a stronger version of Lemma 3.2.

LEMMA 3.5. *Let X be a finite discrete space with additive subbasis \mathcal{K} containing X . Let x be an element of X with the property that any $H \in \mathcal{K}$ containing x satisfies $|H| \geq \frac{1}{2}|X|$. Then*

- (a) *for any $H_1, H_2 \in \mathcal{K}$ with $x \in H_1 \cap H_2$, we have $|H_1 \cap H_2| \geq \frac{1}{2}|H_1|$;*
 (b) *for any $H \in \mathcal{K}$ containing x , we have $|H|$ is a power of 2.*

PROOF. For (a), we note that

$$\begin{aligned} |H_1 \cap H_2| &= \frac{1}{2}(|H_1| + |H_2| - |H_1 + H_2|) \\ &\geq \frac{1}{2}(|H_1| + \frac{1}{2}|X| - \frac{1}{2}|X|) = \frac{1}{2}|H_1| \end{aligned}$$

since $x \in (H_1 + H_2)^c \in \mathcal{K}$.

To prove (b), let $E_1 \in \mathcal{K}$ be any set containing x and set $\mathcal{K}_1 = \{H \cap E_1 | H \in \mathcal{K}\}$. By Lemma 3.2 there exists $E_2 \in \mathcal{K}_1$ such that $x \in E_2$ and $|E_2| \leq \frac{1}{2}|E_1|$; so by (a), $|E_2| = \frac{1}{2}|E_1|$. Set $\mathcal{K}_2 = \{H \cap E_2 | H \in \mathcal{K}_1\}$. Again Lemma 3.2 implies there exists $E_3 \in \mathcal{K}_2$ such that $x \in E_3$ and $|E_3| \leq \frac{1}{2}|E_2|$. If possible, choose E_3 so that $|E_3| < \frac{1}{2}|E_2|$; otherwise $|E_3| = \frac{1}{2}|E_2|$, and we set $\mathcal{K}_3 = \{H \cap E_3 | H \in \mathcal{K}_2\}$ and continue. If $|E_1|$ is not a power of 2, then there exists a least integer k such that $|E_{k+1}| < \frac{1}{2}|E_k|$; then $E_{k+1} \in \mathcal{K}_k$ so there exists $J \in \mathcal{K}_{k-1}$ such that $J \cap E_k = E_{k+1}$. Now apply (a) with $X = E_{k-1}$, $\mathcal{K} = \mathcal{K}_{k-1}$, $H_1 = E_k$ and $H_2 = J$: it says that $|J \cap E_k| \geq \frac{1}{2}|E_k|$, a contradiction. Therefore $|E_1|$ must be a power of 2 and the lemma is proved.

LEMMA 3.6. *Let X be a finite discrete space with additive subbasis \mathcal{K} containing X . If $|\mathcal{K}| > 2|X|$, then for each $x \in X$ there exists $H \in \mathcal{K}$ containing x such that $|H| < \frac{1}{2}|X|$.*

PROOF. The lemma is trivially true if $|X| = 1$ or 2. Assume X, \mathcal{K} give a counterexample with X of minimal cardinality n . Then there exists an $x \in X$ such that $|H| \geq \frac{1}{2}n$ for all $H \in \mathcal{K}$ containing x . By Lemma 3.2 there exists a set $Y \in \mathcal{K}$ containing x such that $|Y| = \frac{1}{2}n$. Also, there exists a set $E \in \mathcal{K}$ such that $E \subseteq Y^c$ and $E \neq \emptyset, Y^c$: for if not, then for all $H_1, H_2 \in \mathcal{K}$ such that $H_1 \cap Y = H_2 \cap Y$, we have $H_1 + H_2 = \emptyset$ or Y^c ; in this case the set $\mathcal{K}_Y = \{H \cap Y | H \in \mathcal{K}\}$ has cardinality $\frac{1}{2}|\mathcal{K}|$, so by the minimality of n , there exists a set $H \in \mathcal{K}$ such that $|H \cap Y| < \frac{1}{4}n, x \in H \cap Y$, a contradiction of

Lemma 3.5(a). So let $S = Y \cup E = Y + E \in \mathcal{C}$. Then $x \in S$ and $\frac{1}{2}n < |S| < n$. Since Y and S cannot both have cardinality equal to a power of 2, we have a contradiction of Lemma 3.5(b).

We would like to thank Roy Olson for his valuable assistance in proving Lemmas 3.2 and 3.6.

LEMMA 3.7. *Let X be a Boolean space and \mathcal{C} an additive subbasis of clopen sets containing X . Then*

(a) *if A is a nonempty subset of X and $A = \bigcap_{i=1}^r H_i$ with $H_i \in \mathcal{C}$ and r minimal, then H_1, \dots, H_r, X are linearly independent in the \mathbb{F}_2 -vector space \mathcal{C} .*

For (b) and (c) assume also that $|X| = 2^n$ and $|H| = 2^{n-1}$ for all $H \in \mathcal{C}$; then

(b) *if H_1, \dots, H_r, X are \mathbb{F}_2 -linearly independent, then $|\bigcap_{i=1}^r H_i| = 2^{n-r}$;*

(c) *any nonempty r -fold intersection of elements of \mathcal{C} has cardinality 2^{n-j} for some $j, 0 \leq j \leq r$.*

PROOF. (a) Assume $\sum_{i=1}^p H_i = \emptyset$ or X , renumbering the sets if necessary. In the first case, we have $H_p = \sum_{i=1}^{p-1} H_i$. But then $\bigcap_{i=1}^p H_i = \bigcap_{i=1}^{p-1} H_i$ if p is even and is empty if p is odd, a contradiction of either $A \neq \emptyset$ or r minimal. Similarly, if $H_p + X = \sum_{i=1}^{p-1} H_i$, then $\bigcap_{i=1}^p H_i = \bigcap_{i=1}^{p-1} H_i$ if p is odd and is empty if p is even, again a contradiction.

(b) We prove this by induction on r . It is true by our hypothesis on \mathcal{C} if $r = 1$. Assume (b) holds for intersections of less than r sets, and consider $\bigcap_{i=1}^r H_i$ where H_1, \dots, H_r, X are linearly independent. It is easy to check that the following equation holds (for any family of sets):

$$\left| \sum_{i=1}^r H_i \right| = \sum_{i=1}^r |H_i| - 2 \sum_{i < j} |H_i \cap H_j| + \dots + (-1)^{r-1} 2^{r-1} \left| \bigcap_{i=1}^r H_i \right|.$$

Since $\sum H_i \in \mathcal{C}$ and is not equal to \emptyset or X by linear independence, we have $|\sum H_i| = 2^{n-1}$. Applying the induction hypothesis for the intersections of less than r sets, we obtain $|\bigcap_{i=1}^r H_i| = 2^{n-r}$.

(c) follows immediately from (a) and (b).

THEOREM 3.8. *Let R be a Witt ring, $R = R_{\text{red}}$ and $|X(R)| = 2^n, n \geq 0$. Then the following are equivalent:*

- (a) $R = \mathbb{Z}G$ (and G has order 2^n);
- (b) if $H \in \mathcal{C}(R), H \neq \emptyset, X$, then $|H| = 2^{n-1}$;
- (c) R is not $(n - 1)$ -stable;
- (d) R is i -stable if and only if $i \geq n$;
- (e) $|\mathcal{C}(R)| = 2^{n+1}$.

PROOF. If $n = 0$, the space X has only one point, so $R = \mathcal{C}(X, \mathbf{Z}) = \mathbf{Z}$ and (a)–(e) all hold. Henceforth we assume $n \geq 1$.

(a) \Rightarrow (b). We assume $R = \mathbf{Z}G$. Then X is the set of all ring homomorphisms $\mathbf{Z}G \rightarrow \mathbf{Z}$. Since G has exponent 2, these homomorphisms are in one-to-one correspondence with elements of $\text{Hom}(G, \{\pm 1\})$; and for any $g \in G$ other than the identity, the element g will be mapped to -1 by exactly half of the homomorphisms. Since the elements of \mathcal{C} are the sets $W(g)$ and their complements, we see that (b) holds.

(b) \Rightarrow (c). Assume R is $(n - 1)$ -stable. Then Theorem 2.10 states that any singleton $\{x\}$ can be written as the symmetric difference of a finite number of $(n - 1)$ -fold intersections of elements of \mathcal{C} . If (b) holds, then Lemma 3.7(c) implies that any $(n - 1)$ -fold intersection has an even number of elements; but symmetric differences of such sets must again have an even number of elements, a contradiction.

(c) \Rightarrow (d). Condition (c) implies that R is not i -stable for $i \leq n - 1$. On the other hand, Theorem 3.3 states that R is i -stable for $i \geq n$.

(d) \Rightarrow (e). Assume (d) holds and $|\mathcal{C}| < 2^{n+1}$, i.e., $|\mathcal{C}| \leq 2^n$. Let $H_1, \dots, H_r = X$ be an \mathbf{F}_2 -basis for \mathcal{C} , $r \leq n$. Since X is discrete and \mathcal{C} is a subbasis, each element of X can be written as the intersection of all elements of $\{H_1, \dots, H_{r-1}, H_1^c, \dots, H_{r-1}^c\}$ which contain it. But there are only $2^{r-1} < 2^n$ such intersections and $|X| = 2^n$. Therefore $|\mathcal{C}| \geq 2^{n+1}$; assume $|\mathcal{C}| > 2^{n+1}$. By Lemma 3.6, every singleton $\{x\}$ can be written as the intersection of at most $n - 1$ sets in \mathcal{C} ; Theorem 2.12 then implies the R is $(n - 1)$ -stable, a contradiction.

(e) \Rightarrow (a). Assume $|\mathcal{C}| = 2^{n+1}$. By [9, Proposition 3.8], $R = \sum_{H \in \mathcal{C}} \mathbf{Z}g_H$ where $g_H \in \mathcal{C}(X, \mathbf{Z})$ is defined by $g_H(x) = -1$ if $x \in H$ and equals 1 if $x \in H^c$. Let H_1, \dots, H_n, X be an \mathbf{F}_2 -basis for \mathcal{C} , and let \mathcal{S} be the subgroup of \mathcal{C} generated by H_1, \dots, H_n . Then $|\mathcal{S}| = 2^n$. Since $g_I g_J = g_{I+J}$ for $I, J \in \mathcal{C}$ and $g_H = -g_{H+X}$, we have $R = \sum_{H \in \mathcal{S}} \mathbf{Z}g_H$. Let G be the group $\{g_H | H \in \mathcal{S}\}$. Then we claim $\sum_{H \in \mathcal{S}} \mathbf{Z}g_H$ is the group ring $\mathbf{Z}G$. Indeed, we have a surjection $\psi: \mathbf{Z}G \rightarrow R$ which is a ring homomorphism. Let K be the kernel of ψ . For any ring homomorphism $\varphi: R \rightarrow \mathbf{Z}$, we certainly have $K \subseteq \ker(\varphi\psi)$. But $\varphi\psi \in X(\mathbf{Z}G)$ and $|X(R)| = 2^n = |X(\mathbf{Z}G)|$. Thus K is contained in the kernel of every map $\mathbf{Z}G \rightarrow \mathbf{Z}$ and hence is in every minimal prime ideal of $\mathbf{Z}G$ [10, Lemma 3.1]. But $\text{Nil } \mathbf{Z}G = 0$, hence $K = 0$ and the theorem is proved.

We shall now complete our study of n -stability in group rings by looking at infinite groups. This provides an example of how our results for finite spaces $X(R)$ can be used to obtain information in the infinite case.

LEMMA 3.9. *Let R be an n -stable abstract Witt ring. Then any Witt ring which is a quotient ring of R is also n -stable.*

PROOF. Since every abstract Witt ring has a unique maximal ideal containing 2, the conclusion is obtained by reducing the equation $M^{n+1} = 2M^n$ modulo the kernel of the homomorphism from R to its quotient ring.

THEOREM 3.10. *Let $R = \mathbb{Z}G$ where G is an infinite group of exponent 2. Then R is not n -stable for any integer n .*

PROOF. Let G_0 be any finite subgroup of G of cardinality at least 2^{n+1} and let R_0 be the group ring $\mathbb{Z}G_0$. Then Theorem 3.8 says that R_0 is not n -stable. Since there is an obvious surjection of R onto R_0 , the previous lemma implies that R is not n -stable.

4. **Stability for formally real fields.** In this section we apply our previous results to $W_{\text{red}}(F)$, the reduced Witt ring of a formally real field F . Our main theorem will be a complete characterization of the fields for which the reduced Witt ring is n -stable in terms of the real places of the field. The importance of n -stability for fields can be seen in [5] where it is related to K -theory of fields. We begin with some definitions and notation.

By a *formally real place* on a field F , we mean a place into a real closed field in the sense of [8] and [12]. By a *real place*, we shall mean a formally real place into the field of real numbers.

DEFINITION 4.1. Given a Witt ring R , we shall call a subset Y of X a 2^n -box if $|Y| = 2^n$ and the quotient ring obtained by restricting the functions in R to the set Y is an integral group ring; that is, it satisfies the equivalent conditions of Theorem 3.8.

For any formally real place σ on a field F , we shall let $\text{Ord}(\sigma)$ be the set of orderings of F compatible with σ (orderings for which any positive $a \in F$ has value $\sigma(a) \geq 0$ or $\sigma(a) = \infty$). By [2] or [8, Theorem 2.5], the set $\text{Ord}(\sigma)$ is always homeomorphic to a product of two point spaces and is a 2^n -box in $X(F) = X(W_{\text{red}}(F))$ whenever $|\text{Ord}(\sigma)| = 2^n$. For any formally real place σ , we shall use Λ_σ to denote the value group of σ reduced modulo 2. The (nonidentity) elements of this group correspond to (nontrivial) intersections of sets in $\mathcal{K}(F) = \mathcal{K}(W_{\text{red}}(F))$ with $\text{Ord}(\sigma)$, and $|\text{Ord}(\sigma)| = |\Lambda_\sigma|$ [2], [8]. Given two real places σ, τ , the field $K_{\sigma,\tau}$ will be the residue field of the finest (formally real) place through which both σ and τ factor, and $\Lambda_{\sigma,\tau}$ will denote the reduced value group of this place; note that this place has valuation ring generated by the valuation rings of σ and τ .

PROPOSITION 4.2. *Let F be a formally real field with a finite number of real places. If $|\text{Ord}(\sigma)| \leq 2^n$ for each real place σ , then $W_{\text{red}}(F)$ is $(n + 1)$ -stable.*

PROOF. Let $x \in X(F)$, say $x \in \text{Ord}(\sigma)$ (every ordering is associated with some real place). $\text{Ord}(\sigma)$ is a 2^m -box for $m \leq n$, so by Lemma 3.7 there exist sets $H_1, \dots, H_m \in \mathcal{K}(F)$ such that $\bigcap_{i=1}^m H_i \cap \text{Ord}(\sigma) = \{x\}$. By [1, Theorem

2.1(B)], there exists an element $a \in F$ such that $\text{Ord}(\sigma) = W(a) = \{x \in X(F) \mid a \text{ is negative in the ordering corresponding to } x\}$. Thus $\text{Ord}(\sigma) \in \mathcal{H}(F)$. Since x was arbitrary, Theorem 2.12 implies that $W_{\text{red}}(F)$ is $(n + 1)$ -stable.

In general, under the hypotheses of Proposition 4.2, $W_{\text{red}}(F)$ may or may not be n -stable. The following theorem shows precisely what added condition is needed to force n -stability.

THEOREM 4.3. *Let F be a formally real field with finitely⁽²⁾ many real places. Then the following statements are equivalent.*

- (a) $W_{\text{red}}(F)$ is n -stable.
- (b) Any group ring $\mathbb{Z}G$ which is a quotient ring of $W_{\text{red}}(F)$ has the order of G less than or equal to 2^n .
- (c) The space of orderings $X(F)$ has no 2^{n+1} -box.
- (d) For all formally real places σ on F , we have $|\text{Ord}(\sigma)| \leq 2^n$; and if $|\text{Ord}(\sigma)| = 2^n$, the residue class field of σ has a unique ordering.
- (e) For all real places σ , we have $|\text{Ord}(\sigma)| \leq 2^n$; and if $|\text{Ord}(\sigma)| = 2^n$, then for all real places $\tau \neq \sigma$, the kernel of the canonical homomorphism $\Lambda_\sigma \rightarrow \Lambda_{\sigma,\tau}$ is nontrivial.

PROOF. (a) \Rightarrow (b). By Lemma 3.9, any group ring which is a quotient ring is n -stable. By Theorems 3.8 and 3.10, the group G must have order no greater than 2^n .

(b) \Rightarrow (c). For any subset Y of $X(F)$, we obtain a quotient ring of $W_{\text{red}}(F) \subseteq \mathcal{C}(X(F), \mathbb{Z})$ by restricting the functions from $X(F)$ to Y . If Y is a 2^{n+1} -box, Theorem 3.8 implies that the corresponding quotient ring is a group ring where the group has order larger than 2^n .

(c) \Rightarrow (d). Since $\text{Ord}(\sigma)$ is a 2^m -box in $X(F)$ for some m , we have $|\text{Ord}(\sigma)| \leq 2^n$. Assume $|\text{Ord}(\sigma)| = 2^n$ and the residue class field K_σ has two orderings (or more). Corresponding to these two orderings are two real places σ_1, σ_2 on K_σ . Composing these with σ gives two real places on F , $\tau_i = \sigma_i \sigma$, $i = 1, 2$. Since $|\Lambda_\sigma| = 2^n$ is the maximum allowed, we must have $|\Lambda_{\sigma_i}| = 1$ ($i = 1, 2$). So there exists only one ordering of K_σ per place. Since the corresponding orderings are distinct we must have $\sigma_1 \neq \sigma_2$, and so the two real places τ_1, τ_2 on F are distinct. Since they agree as places into K_σ , the canonical homomorphisms $\Lambda_{\tau_i} \rightarrow \Lambda_{\tau_1, \tau_2}$ ($i = 1, 2$) are isomorphisms. This implies that $\text{Ord}(\tau_1) \cup \text{Ord}(\tau_2)$ is a 2^{n+1} -box [8, Theorem 2.5] which contradicts (c).

(d) \Rightarrow (e). Since every real place is a formally real place, we have $|\text{Ord}(\sigma)| \leq 2^n$ for all real places σ . Assume there exist real places σ, τ such that

(2) NOTE ADDED IN PROOF. R. Brown has pointed out that the finiteness hypothesis can be removed by using results in [L. Brocker, Math. Ann. 210 (1974), 233–256].

$|\text{Ord}(\sigma)| = 2^n$ and $\Lambda_\sigma \rightarrow \Lambda_{\sigma,\tau}$ is injective. Since $|\Lambda_\tau| \leq 2^n$, it must equal 2^n and thus both $\Lambda_\sigma \rightarrow \Lambda_{\sigma,\tau}$ and $\Lambda_\tau \rightarrow \Lambda_{\sigma,\tau}$ are isomorphisms. This implies that the reduced value groups, for the induced real places σ_* , τ_* on $K_{\sigma,\tau}$, are trivial. Thus σ_* and τ_* correspond uniquely to orderings on $K_{\sigma,\tau}$ [2]. Since (d) implies that $K_{\sigma,\tau}$ has a unique ordering, we must have $\sigma_* = \tau_*$, and so $\sigma = \tau$.

(e) \Rightarrow (a). Let $x \in X(F)$ and let σ be the associated real place. If $\text{Ord}(\sigma)$ is a 2^m -box, then by Lemma 3.7 we can find $H_1, \dots, H_m \in \mathfrak{H}(F)$ such that $\{x\} = \bigcap_{i=1}^m H_i \cap \text{Ord}(\sigma)$. If $m < n$, this is an intersection of at most n elements of $\mathfrak{H}(F)$. Now assume $m = n$. Since $\text{Ord}(\sigma)$ has the maximum possible size, the valuation ring corresponding to σ is minimal among the valuation rings of F corresponding to real places. Also, the subrings of F containing a valuation ring are linearly ordered. Thus the condition that $\Lambda_\sigma \rightarrow \Lambda_{\sigma,\tau}$ have nontrivial kernel for each $\tau \neq \sigma$ implies that there is some element λ of Λ_σ which maps to 1 in $\Lambda_{\sigma,\tau}$ for all $\tau \neq \sigma$. Let $b \in F$ be in the inverse image of λ under the canonical homomorphism from the multiplicative group of nonzero elements of F to Λ_σ . Then we can apply [1, Theorem 2.1(B)] to obtain an element $a \in F$ which is close to b under the place σ and close to 1 under each of the finite number of other real places. This means that we have found an element a such that $W(a) \subseteq \text{Ord}(\sigma)$ and $W(a) \neq \emptyset$, $\text{Ord}(\sigma)$. Again applying Lemma 3.7, we can choose our family H_1, \dots, H_m with $H_1 = W(a)$ or $H_1 = W(a) + \text{Ord}(\sigma)$, whichever contains x . Therefore $\{x\} = \bigcap_{i=1}^n H_i$, an n -fold intersection of elements of $\mathfrak{H}(F)$. By Theorem 2.12, the $W_{\text{red}}(F)$ is n -stable. Thus the theorem is proved.

We shall conclude this section by exploring some of the implications of this theorem.

REMARK 4.4. For the case $n = 1$, but without the restriction to a finite number of real places, the equivalence of (a) and (d) is the valuation theoretic characterization of SAP due to Elman, Lam and Prestel [5], [6], [14, Satz 2.2]. Our proof is much more direct, however, as theirs depends on work in all three of the above cited papers and requires a great deal of work with quadratic forms.

REMARK 4.5. It is easy to see that condition (c) of the theorem is equivalent to the following:

(f) Given any 2^{n+1} points in $X(F)$, there exists a set $H \in \mathfrak{H}(F)$ such that H contains at least one but less than 2^n of the points.

If we take $n = 1$, we obtain the statement that (under the hypotheses of the theorem) SAP is equivalent to being able to separate one point from any three others by an element of $\mathfrak{H}(F)$. Using [14, Satz 2.2], it is possible to improve [5, Theorem 3.5] to give this result in general.

EXAMPLE 4.6. It is not possible to generalize Theorem 4.3 to abstract Witt rings. Indeed, we shall now give an example where X has no 4-box but the ring is not 1-stable. It is constructed by taking X to be a set of six points and $\mathfrak{H}(R)$

to be all subsets of X containing an even number of points. Then (f) clearly holds with $n = 1$; hence there is no 4-box. On the other hand, R is not 1-stable by Corollary 2.6. This is, in fact, the only torsion free abstract Witt ring with $|X(R)| \leq 6$ which cannot be the reduced Witt ring of a field.

The author wishes to thank Ron Brown for many useful discussions regarding real places and applications of his approximation theorem [1].

REFERENCES

1. Ron Brown, *An approximation theorem for extended prime spots*, *Canad. J. Math.* **24** (1972), 167–184. MR #1884.
2. ———, *Real places and ordered fields*, *Rocky Mountain J. Math.* **1** (1971), 633–636. MR **44** #2730.
3. ———, *Superpythagorean fields*, *J. Algebra* (to appear).
4. T. Craven, *The Boolean space of orderings of a field*, *Trans. Amer. Math. Soc.* **209** (1975), 225–235.
5. R. Elman and T. Y. Lam, *Quadratic forms over formally real fields and pythagorean fields*, *Amer. J. Math.* **94** (1972), 1155–1194. MR **47** #3427.
6. R. Elman, T. Y. Lam and A. Prestel, *On some Hasse principles over formally real fields*, *Math. Z.* **134** (1973), 291–301. MR **48** #8384.
7. B. W. Jones, *The arithmetic theory of quadratic forms*, *Carus Math. Monos.*, no. 10, Math. Assoc. Amer.; distributed by Wiley, New York, 1950. MR **12**, 244.
8. M. Knebusch, *On the extension of real places*, *Comment. Math. Helv.* **48** (1973), 354–369. MR **49** #2681.
9. M. Knebusch, A. Rosenberg and R. Ware, *Signatures on emilocal rings*, *J. Algebra* **26** (1973), 208–250. MR **48** #6103.
10. ———, *Structure of Witt rings and quotients of Abelian group rings*, *Amer. J. Math.* **94** (1972), 119–155. MR **45** #5164.
11. ———, *Structure of Witt rings, quotients of abelian group rings, and orderings of fields*, *Bull. Amer. Math. Soc.* **77** (1971), 205–210. MR **42** #5974.
12. S. Lang, *The theory of real places*, *Ann. of Math. (2)* **57** (1953), 378–391. MR **14**, 841.
13. J. Milnor and D. Husemoller, *Symmetric bilinear forms*, *Ergebnisse Math. Grenzgebiete*, Band 73, Springer, Berlin, 1973.
14. A. Prestel, *Quadratische Semi-Ordnungen und quadratische Formen*, *Math. Z.* **133** (1973), 319–342. MR **49** #2682.
15. R. Ware, *When are Witt rings group rings?*, *Pacific J. Math.* **49** (1973), 279–284. MR **48** #10980.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAWAII, HONOLULU, HAWAII 96822