Reprinted from JOURNAL OF ALGEBRA
All Rights Reserved by Academic Press, New York and London
Vol. 26, No. 2, August 1973
Printed in Belgium

# Signatures on Semilocal Rings

MANFRED KNEBUSCH

*Mathematisches Institut, Universität des Saarlandes, D-6600 Saarbrücken, Germany*

ALEX ROSENBERG*

*Department of Mathematics, Cornell University, Ithaca, New York 14850‡*

AND

ROGER WARE†

*Department of Mathematics, Northwestern University, Evanston, Illinois 60201*

Received March 15, 1972

## 1. INTRODUCTION AND NOTATIONS

Most of the results of this paper have been announced in [31, Section 3] and, in slightly simplified form, in [32]. The reader is advised to consult these announcements for an outline of the contents of the present work.

One of our main purposes here is to extend part of the Artin–Schreier theory of real closed fields to commutative semilocal rings with involution. The central concept that enables us to accomplish this goal is that of a signature: Let $C$ denote a semilocal ring with an involution $J$ whose fixed ring we denote by $A$. A signature is a homomorphism $\sigma$ from $A^*$, the group of units of $A$, to $\{\pm 1\}$ with certain properties (Definition 2.1 and Proposition 2.4). If $A$ is a field the signatures correspond byectively with the set of total orderings of $A$ for which all the norms $N(c) = cJ(c)$ for $c$ in $C^*$ are positive. In particular then, if $J$ is the identity, this latter set consists of all orderings of $A$.

In Section 2 we study the notion of signature. By definition a signature $\sigma$ on $(C, J)$ corresponds with a unique homomorphism $\bar{\sigma}$ from the Witt ring $WF(C, J)$ of free Hermitian spaces over $(C, J)$ to $\mathbb{Z}$ and conversely. For the case $J$ the identity and $C = A$ a field this correspondence between orderings

* Partially supported by NSF Grant GP-25600.
† Partially supported by NSF Grant GP-28915.
‡ Present address: Department of Mathematics, University of Kansas, Lawrence, Kansas, 66044.

and homomorphisms of $W(A)$ to $\mathbb{Z}$ has also been noted in [36] and [25]. We then use the structure theory of such Witt rings developed in [33] as our main tool in the study of signatures. The relationship between signatures on $(C, J)$ and the signatures on $A$ is discussed as well as the relationship between the signatures of a semilocal domain and the orderings of its quotient field.

Since there is a bijection of the set of signatures with a set of prime ideals in a commutative ring, the Zariski topology induces a topology on the set of signatures on a semilocal ring with involution. With this topology the set of signatures becomes a compact totally disconnected Hausdorff space $X$. In Section 3, we study the space $X$ and in particular the embedding of $WF(C, J)_{\text{red}} = (WF(C, J))/\text{Rad}(WF(C, J))$ in the ring $C(X, \mathbb{Z})$ of continuous integer valued functions on $X$. Moreover, if $X$ is any compact totally disconnected Hausdorff space, we study arbitrary Witt subrings for groups of exponent two [33, Definition 3.12] of $C(X, \mathbb{Z})$ and characterize these in terms of the Boolean algebra of closed and open sets of $X$. We then use this information to obtain a necessary and sufficient condition for an approximation theorem for the orderings of a formally real field to hold. In the last part of Section 3, we give a description of the image of the map

$$(\bar{\sigma}_1, \ldots, \bar{\sigma}_n): WF(C, J) \to \mathbb{Z}^n$$

for a finite set $\sigma_1, \ldots, \sigma_n$ of signatures of $(C, J)$.

In Section 4 we further generalize Pfister's generalization [39, Satz 21] of Artin's characterization of sums of squares in a formally real field. To accomplish this we introduce the notion of the saturation $\hat{M}$ of an arbitrary subset $M$ of $A^*$. The subgroup $\hat{M}$ consists of all units of the form

$$\sum_{0 \leqslant i_k \leqslant 1} c_{i_1, \ldots, i_r} a_1^{i_1} \cdots a_r^{i_r},$$

with $r \geqslant 1$, $a_i$ in $M$ and $c_{i_1, \ldots, i_r}$ a sum of norms in $A$. We show that $\hat{M}$ is the set of all units $b$ in $A$ with $\sigma(b) = 1$ for all signatures $\sigma$ on $A$ such that $\sigma(M) = 1$. In the special case when $A$ is a field and $J$ is the identity [39, Satz 21] follows and further setting $M = 1$ yields the classical Artin result [3, Satz 1]. The latter part of Section 4 is devoted to the study of the torsion subgroup of $WF(C, J)$.

Section 5 deals with the problem of extending signatures. For the sake of simplicity we consider only semilocal rings with the identity involution. Most of our results concern the extensions of signatures of a semilocal ring $A$ to signatures on a Galois extension $B$ with group $G$, in the sense of [5] and [15]. Thus, we show that a signature on $A$ has either no or $[G : 1]$ extensions to $B$. Moreover, in the latter case all the extensions are conjugate under the action

of $G$. In the last part of Section 5 we obtain some information about the $G$-module structure of $W(B)$ and the cohomology groups $\hat{H}^i(G, W(B))$. In particular, we show that the localization of $W(B)$ with regard to the multiplicative semigroup $\{2^n\}$ is a free $G$-module of rank one. We have not been able to generalize the main results of this section from the case of a Galois extension to that of an arbitrary finite étale extension. This points up the most serious defect of the theory developed so far: Namely, no notion of "real closure" with respect to a fixed signature has yet been established.[1]

We close Section 1 by recalling a few facts and notations from [33]. For a semilocal ring $C$ with involution $J$, the fixed ring of $J$ is denoted by $A$, the groups of units of $C$ and $A$ are denoted by $C^*$ and $A^*$, respectively, and $N: C^* \to A^*$ is the homomorphism given by $N(c) = cJ(c)$. A $(C, J)$-space is a pair $(E, \Phi)$, where $E$ is a finitely generated projective left $C$-module and $\Phi: E \times E \to C$ is a Hermitian form. The relation of isometry is written as $\cong$. If $E$ is free with an orthogonal basis $e_1, \ldots, e_n$ such that $\Phi(e_i, e_i) = a_i$ we often write $(a_1, \ldots, a_n) \cong (E, \Phi)$. A space $(E, \Phi)$ is called nondegenerate if the natural map $E \to \hom_C(E, C)$ induced by $\Phi$ is an isomorphism and metabolic if it is nondegenerate and $E$ has a $C$-module direct summand $V$ with $V^\perp = V$. Two nondegenerate spaces $(E, \Phi)$ and $(E', \Phi')$ are called equivalent, written as $E \sim E'$, if there are metabolic spaces $U$ and $U'$ with $E \perp U \cong E' \perp U'$. The set of equivalence classes under $\sim$ form a commutative ring, the Witt ring, denoted by $W(C, J)$($WF(C, J)$ if only free $C$-modules are considered). The ring theoretic operations of $W(C, J)$ are induced by the orthogonal direct sum and the tensor product of spaces, respectively. The class of a space $(E, \Phi)$ in $W(C, J)$ is denoted by $[(E, \Phi)]$ or $[E]$. There is a ring surjection $\mathbb{Z}[A^*/NC^*] \twoheadrightarrow WF(C, J)$, where $\mathbb{Z}[A^*/NC^*]$ denotes the group algebra of the group $A^*/NC^*$ over $\mathbb{Z}$. For $a$ in $A^*$, we write $\{a\}$ for the element $aNC^*$ of $\mathbb{Z}[A^*/NC^*]$.

## 2. The Notion of Signature

Until the last part of this section $C$ will always be a connected (= no idempotents other than 0 and 1) semilocal ring with involution $J$ and $A$ will be the fixed ring of $J$.

Convention. If $\sigma: A^* \to \{\pm 1\}$ is a group homomorphism such that $\sigma(NC^*) = 1$ then the induced ring homomorphism $\mathbb{Z}[A^*/NC^*] \to \mathbb{Z}$ will also be denoted by $\sigma$.

[1] *Note added in proof.* We now know that a reasonable theory of real closures exists (cf. *Bull. Amer. Math. Soc.* **79** (1973), 78–81).

DEFINITION 2.1. A *signature* $\sigma$ of $(C, J)$ is a group homomorphism $\sigma: A^* \to \{\pm 1\}$ satisfying

(i) $\sigma(NC^*) = 1$.

(ii) If $G = A^*/NC^*$ and $\psi_C: \mathbb{Z}[G] \to W(C, J)$ is the canonical map then $\sigma(\ker \psi_C) = 0$.

$\mathrm{Sign}(C, J)$ will denote the set of signatures of $(C, J)$.

*Remark* 2.2. If $\sigma$ is a signature of $(C, J)$ we denote by $\bar{\sigma}$ the unique ring homomorphism from $W(C, J)$ to $\mathbb{Z}$ such that $\sigma: \mathbb{Z}[G] \to \mathbb{Z}$ equals $\bar{\sigma} \circ \psi_C$. Evidently we have a canonical bijection between $\mathrm{Sign}(C, J)$ and the set of ring homomorphisms from $W(C, J)$ to $\mathbb{Z}$. By [33, Example 3.11] if $\mathrm{Sign}(C, J) \neq \varnothing$ then these sets are in bijective correspondence with the set $\min W(C, J)$ of minimal prime ideals of $W(C, J)$. Specifically, if $\sigma$ is a signature then $\bar{\sigma}[(a_1, \ldots, a_n)] = \sigma(a_1) + \cdots + \sigma(a_n)$ and the associated prime ideal $P_\sigma$ is the kernel of $\bar{\sigma}$.

The inclusion $A \hookrightarrow C$ induces a morphism $(A, Id) \to (C, J)$ of pairs [33] from which we get a ring homomorphism $W(A) \to W(C, J)$, where $W(A) = W(A, Id)$. The commutative diagram

$$\begin{array}{ccc} \mathbb{Z}[A^*/(A^*)^2] & \twoheadrightarrow & W(A) \\ \downarrow & & \downarrow \\ \mathbb{Z}[A^*/NC^*] & \twoheadrightarrow & W(C, J) \end{array}$$

shows that $W(A) \to W(C, J)$ is surjective and that $\mathrm{Sign}(C, J)$ is a subset of $\mathrm{Sign}(A) = \mathrm{Sign}(A, Id)$.

In order to give a more explicit description of signatures we need the following lemma.

LEMMA 2.3. (i) *For any* $\sigma$ *in* $\mathrm{Sign}(C, J)$ *we have* $\sigma(-1) = -1$.

(ii) *Each* $\sigma$ *in* $\mathrm{Sign}(C, J)$ *has the following property for all* $r \geqslant 1$:

$(S_r)$ *Let* $a_1, \ldots, a_r$ *be units of* $A$ *with* $\sigma(a_1) = \cdots = \sigma(a_r) = 1$ *and* $c_1, \ldots, c_r$ *be elements of* $C$ *such that*

$$b = N(c_1)\, a_1 + \cdots + N(c_r)\, a_r$$

*is also a unit. Then* $\sigma(b) = 1$.

Note that for any $r \geqslant 1$, $(S_r)$ implies $(S_{r-1})$.

*Proof.* (i) is clear since $[(1)] + [(-1)] = 0$ in $W(C, J)$.

(ii) The element $b$ is represented by the space $(a_1, \ldots, a_r)$ over $(C, J)$. Hence, we have an isometry

$$(a_1, \ldots, a_r) \cong (b) \perp N,$$

for some space $N$. The space $N$ may not have an orthogonal basis, but $N \perp (1)$ is proper so that

$$N \perp (1) \cong (b_1, \ldots, b_r),$$

for some $b_i$ in $A^*$ [33, Lemma 1.12]. Hence,

$$(1, a_1, \ldots, a_r) \cong (b, b_1, \ldots, b_r).$$

Since $\sigma(a_1) = \cdots = \sigma(a_r) = 1$ we have $\bar{\sigma}[(b, b_1, \ldots, b_r)] = r + 1$, which can only happen if $\sigma(b) = \sigma(b_1) = \cdots = \sigma(b_r) = 1$.

PROPOSITION 2.4. *Let $\sigma: A^* \to \{\pm 1\}$ be a group homomorphism with $\sigma(NC^*) = 1$ and $\sigma(-1) = -1$.*

(i) *If $A$ is a field then $\sigma$ is a signature if and only if $\sigma(a) = 1$ implies $\sigma(1 + a) = 1$ for all $a$ in $A^*$.*

(ii) *Assume $C$ has no maximal ideal $\mathfrak{M}$ with $J(\mathfrak{M}) = \mathfrak{M}$ and $C/\mathfrak{M} = \mathbb{F}_2$.[2] Then $\sigma$ is a signature if and only if the property $(S_3)$ of Lemma 2.3 holds.*

(iii) *Assume in addition that $C$ has no maximal ideal $\mathfrak{M}$ with $J(\mathfrak{M}) = \mathfrak{M}$, $A/\mathfrak{M} \cap A = \mathbb{F}_2$, and $C/\mathfrak{M} = \mathbb{F}_4$. Then $\sigma$ is a signature if and only if $(S_2)$ holds.*

*Proof.* The "only if" is clear in all cases from Lemma 2.3. Moreover, it is easily seen that $(S_2)$ is equivalent to the property stated in (i) if $A$ is a field. In [33, Theorems 1.15 and 1.16, Corollary 1.17] it has been shown that the kernel of $\psi_C: \mathbb{Z}[A^*/NC^*] \to W(C, J)$ is generated by the elements $\{1\} + \{-1\}$ and

$$\sum_{i=1}^{r} \{a_i\} - \sum_{i=1}^{r} \{b_i\},$$

with $(a_1, \ldots, a_r) \cong (b_1, \ldots, b_r)$. It was shown there that $r = 2$ suffices in Cases (i) and (iii) and $r = 3$ in Case (ii) of our proposition. Thus, we need only prove that in any case for $r \leqslant 3$ the property $(S_r)$ implies $\sum_{i=1}^{r} \sigma(a_i) = \sum_{i=1}^{r} \sigma(b_i)$ for all units $a_1, \ldots, a_r$, $b_1, \ldots, b_r$ of $A^*$ such that $(a_1, \ldots, a_r) \cong (b_1, \ldots, b_r)$. If all $\sigma(a_i) = 1$ then it follows immediately from $(S_r)$ that all $\sigma(b_i) = 1$. If all $\sigma(a_i) = -1$ then we also have all $\sigma(b_i) = -1$, since $(-a_1, \ldots, -a_r) \cong (-b_1, \ldots, -b_r)$. Hence, we need only consider the case that neither all $\sigma(a_i)$ nor all $\sigma(b_i)$ have the same value. But by taking determinants we see that $\prod_{i=1}^{r} \{a_i\} = \prod_{i=1}^{r} \{b_i\}$ in $A^*/NC^*$. Hence, $\prod_{i=1}^{r} \sigma(a_i) = \prod_{i=1}^{r} \sigma(b_i)$ and since $r \leqslant 3$ it is clear that $\sigma(a_i) = -1$ occurs as often as $\sigma(b_i) = -1$.

[2] $\mathbb{F}_q$ denotes the field of $q$ elements.

We would like to give a more explicit characterization of $\mathrm{Sign}(C, J)$ as a subset of $\mathrm{Sign}(A)$. The following proposition will be proved in Section 6 since the proof uses techniques from [29] which will not be needed elsewhere in this paper.

PROPOSITION 2.5. *Assume that either $A$ is a field or $C$ has no maximal ideal $\mathfrak{M}$ such that one of the following exceptional cases occurs:*

(i) $C/\mathfrak{M} = \mathbb{F}_2$ *or* $\mathbb{F}_3$.

(ii) $\mathfrak{M} = J(\mathfrak{M})$, $C/\mathfrak{M} = \mathbb{F}_4$, *and* $A/\mathfrak{M} \cap A = \mathbb{F}_2$.

*Then the kernel of $W(A) \to W(C, J)$ is generated by the binary space classes $[(1, -Nc)]$ with $c$ in $C^*$.*

From this proposition and Definition 2.1 we immediately obtain the following.

COROLLARY 2.6. *Under the hypotheses of Proposition* 2.5, $\mathrm{Sign}(C, J)$ *is the set of all $\sigma$ in* $\mathrm{Sign}(A)$ *with $\sigma(NC^*) = 1$.*

*Remark* 2.7. (i) If $C$ is a field then Corollary 2.6 is an immediate consequence of Proposition 2.4(i) and Proposition 2.5 is not needed.

(ii) If $A$ is a field it follows from Proposition 2.4(i) that $\mathrm{Sign}(A)$ can be identified with the set of all orderings on $A$. This is done as follows (cf. [25; 36]):

If $<$ is an ordering on $A$ we define a signature $\sigma_<$ of $A$ by

$$\sigma_<(a) = \begin{cases} 1 & \text{if } a > 0, \\ -1 & \text{if } a < 0, \end{cases}$$

and if $\sigma$ is a signature of $A$ we define an ordering $<_\sigma$ on $A$ by $0 <_\sigma a$ if and only if $\sigma(a) = 1$.

Note that Corollary 2.6 shows that a signature $\sigma$ in $\mathrm{Sign}(A)$ is in $\mathrm{Sign}(C, J)$ if and only if $0 <_\sigma N(c)$ for all $c$ in $C^*$.

LEMMA 2.8. *Let $C$ be a field with $J \neq$ identity. Then a signature $\sigma$ in* $\mathrm{Sign}(A)$ *lies in* $\mathrm{Sign}(C, J)$ *if and only if the ordering $<_\sigma$ on $A$ does not extend to an ordering on $C$.*

*Proof.* Since $A$ must have characteristic 0 we can write $C = A(\theta)$, where $\theta^2 \in A$ and $J(\theta) = -\theta$. If $\sigma$ is in $\mathrm{Sign}(C, J)$ then $\theta^2 <_\sigma 0$ and, hence, $<_\sigma$ cannot be extended to an ordering on $C$. Suppose now that $<_\sigma$ does not extend to an ordering on $C$. Then $\theta^2 <_\sigma 0$ [9, p. 38] (see also Proposition 5.15), and, hence, for any $c = a + b\theta$ in $C^*$ we have $0 <_\sigma a^2 - b^2\theta^2 = N(c)$.

Let $C$ be a field with involution $J \neq$ identity, let $\sigma$ be a signature of $A$, and let $A_\sigma$ be a real closure of $A$ with respect to the ordering $<_\sigma$ (e.g. [9, p. 38]).

If $\bar{A}$ is the algebraic closure of $A_\sigma$ and $J_\sigma$ is the involution of $\bar{A}$ whose fixed field is $A_\sigma$ then $W(A_\sigma) \cong W(\bar{A}, J_\sigma) \cong \mathbb{Z}$ (Sylvester's law of inertia). Moreover, the homomorphism $W(A) \to \mathbb{Z}$ induced by $\sigma$ coincides with the homomorphism $W(A) \to W(A_\sigma)$ induced by the inclusion $A \hookrightarrow A_\sigma$ [36]. Finally, since the ordering $<_\sigma$ extends to $C$ if and only if $J_\sigma$ does not extend $J$, Lemma 2.8 shows that $J_\sigma$ extends $J$ if and only if $\sigma$ is in $\mathrm{Sign}(C, J)$. When this is the case the induced homomorphism $\bar{\sigma}: W(C, J) \to \mathbb{Z}$ is just the canonical map $W(C, J) \to W(\bar{A}, J_\sigma)$.

If the semilocal ring $A$ has no zero divisors we can still ask whether a given signature $\sigma$ of $A$ gives rise to an ordering $<$ of $A$; i.e., whether there exists an ordering $<$ of $A$ such that $\sigma(a) = 1$ if and only if $0 < a$ for all $a$ in $A^*$. In order to investigate this question we prove a lemma which will also be used to prove other results concerning extensions of signatures. We first need the following definition.

DEFINITION 2.9. Let $(C, J) \xrightarrow{f} (C', J')$ be a morphism of pairs and let $\sigma$ be a signature of $(C, J)$. We say that the signature $\sigma'$ of $(C', J')$ *extends* $\sigma$ (relative to $f$) if $\sigma'(f(a)) = \sigma(a)$ for all $a$ in $A^*$.

Note that $\sigma'$ in $\mathrm{Sign}(C', J')$ extends $\sigma$ in $\mathrm{Sign}(C, J)$ if and only if we have a commutative diagram

$$\begin{array}{ccc} W(C, J) & \xrightarrow{W(f)} & W(C', J') \\ & {\scriptstyle\bar{\sigma}} \searrow \quad \swarrow {\scriptstyle\bar{\sigma}'} & \\ & \mathbb{Z} & \end{array}$$

LEMMA 2.10. *Let $(C, J) \xrightarrow{f} (C', J')$ be a morphism of pairs and $\sigma$ a signature of $(C, J)$. Then $\sigma$ extends to a signature $\sigma'$ of $(C', J')$ if and only if* $\bar{\sigma}(\ker W(f)) = 0$.

*Proof.* If $\sigma$ extends to a signature $\sigma'$ of $(C', J')$ then the above diagram shows that $\bar{\sigma}(\ker W(f)) = 0$. Conversely, assume $\bar{\sigma}(\ker W(f)) = 0$ and let $R = \mathrm{Im}\, W(f)$. Then there exists a ring homomorphism $\varphi: R \to \mathbb{Z}$ such that $\varphi \circ W(f) = \bar{\sigma}$. Let $P = \ker \varphi$. Then $P$ is a minimal prime ideal of $R$ so there is a minimal prime ideal $P'$ of $W(C', J')$ such that $P' \cap R = P$ (e.g. [11, Proposition 16, p. 96]). The signature $\sigma'$ of $(C', J')$ corresponding to $P'$ clearly extends $\sigma$.

Since the intersection of all minimal prime ideals of a commutative ring is the set of nilpotent elements [11, Proposition 13, p. 95] we have the following.

COROLLARY 2.11. *Let $(C, J) \xrightarrow{f} (C', J')$ be a morphism of pairs. Then every signature of $(C, J)$ extends to a signature of $(C', J')$ if and only if* $\ker W(f)$ *is a nil ideal.*

We now return to the question of extending a signature of a semilocal integral domain $A$ to an ordering on $A$. Since any ordering on $A$ extends in a unique way to an ordering on the quotient field $F$ of $A$, it is enough to ask when a signature of $A$ extends to a signature (= ordering) of $F$. This question is answered by Lemma 2.10; namely, a signature $\sigma$ of $A$ extends to an ordering of $F$ if and only if $\ker(W(A) \to W(F))$ is contained in the kernel of the map $\bar{\sigma}: W(A) \to \mathbb{Z}$.

EXAMPLE 2.12. Let $A$ be the local ring of the affine curve $X^2 + Y^2 = 0$ over the real field $\mathbb{R}$ at (0, 0). Then the signature

$$\sigma: A^* \to \mathbb{R}^* \to \{\pm 1\},$$

obtained by composing the evaluation map at (0, 0) and the unique signature of $\mathbb{R}$, does not arise from an ordering of $A$. This follows because $-1$ is a square in the quotient field of $A$, and, hence, $A$ can have no orderings.

EXAMPLE 2.13. Let $A$ be a valuation ring with maximal ideal $\mathfrak{m}$. Then any $\sigma$ in $\mathrm{Sign}(A)$ can be extended to an ordering of $A$. If $A$ has rank one [12, p. 115] and $\sigma(1 + \mathfrak{m}) \neq \{1\}$, then $\sigma$ has exactly one extension to an ordering. If $A$ is discrete [12, p. 108] and $\sigma(1 + \mathfrak{m}) = \{1\}$, then $\sigma$ has exactly two extensions.

*Proof.* Let $F$ be the quotient field of $A$. Since $A$ is a Prüfer ring, $W(A) \to W(F)$ is injective [27, 11.1.1] so the first assertion follows from Corollary 2.11.

Now assume $A$ has rank one and $\sigma(1 + \mathfrak{m}) \neq \{1\}$. Then there exists an $a$ in $1 + \mathfrak{m}$ with $\sigma(a) = -1$, and, hence, $\bar{\sigma}[(1, -a)] = 2$. Let $W(A, \mathfrak{m})$ be the kernel of the natural map $W(A) \to W(A/\mathfrak{m})$. Then $[(1, -a)]$ lies in $W(A, \mathfrak{m})$, so since $W(A, \mathfrak{m})$ is an ideal in $W(F)$ [27, 12.1.1] it follows that for any $c$ in $F^*$ the class $[(c, -ca)]$ lies in $W(A)$. Therefore, if $\tau$ is any signature on $F$ extending $\sigma$ we must have

$$\begin{aligned}\bar{\sigma}[(c, -ca)] &= \bar{\tau}[(c, -ca)] = \tau(c)\,\bar{\tau}[(1, -a)] \\ &= \tau(c)\,\bar{\sigma}[(1, -a)] = 2\tau(c),\end{aligned}$$

for all $c$ in $F^*$. Hence, $\sigma$ can have only one extension.

If $A$ is discrete with $\mathfrak{m} = A\pi$ then any extension $\tau$ in $\mathrm{Sign}(F)$ of $\sigma$ is determined by the value $\tau(\pi)$. If $\sigma(1 + \mathfrak{m}) = \{1\}$ it is easily verified using Proposition 2.4(i) that for both $\alpha = 1$ and $\alpha = -1$ the functions $\tau_\alpha: F^* \to \{\pm 1\}$ defined by $\tau_\alpha(u\pi^n) = \sigma(u)\,\alpha^n$, for $u$ in $A^*$ and $n$ in $\mathbb{Z}$ are signatures of $F$ extending $\sigma$.

PROPOSITION 2.14. *Let $A$ be a Dedekind ring (not necessarily semilocal) with quotient field $F$.*

(i) *If all orderings on $F$ are Archimedian then $A/\mathfrak{p}$ is not formally real for all nonzero prime ideals $\mathfrak{p}$ of $A$.*

(ii) *If $A/\mathfrak{p}$ is not formally real for all $\mathfrak{p} \neq 0$ then the natural map of* Spec $W(F)$ *to* Spec $W(A)$ *is a homeomorphism. In particular, if $A$ is semilocal then the signatures of $A$ correspond bijectively with the orderings on $A$.*

*Proof.* (i) Assume there exists a prime ideal $\mathfrak{p}$ of $A$ such that $A/\mathfrak{p}$ is formally real; i.e., has at least one signature $\tau$. Composing $\tau$ with the reduction map from $A_{\mathfrak{p}}^* \to (A/\mathfrak{p})^*$ yields a signature $\sigma\colon A_{\mathfrak{p}}^* \to (A/\mathfrak{p})^* \xrightarrow{\tau} \{\pm 1\}$ of the valuation ring $A_{\mathfrak{p}}$. Then for any ordering $<$ of $F$ extending $\sigma$ we must have $a < 1$ for all $a$ in $\mathfrak{p}A_{\mathfrak{p}}$, since $\sigma(1 + \mathfrak{p}A_{\mathfrak{p}}) = 1$. Such an ordering is obviously non-Archimedian.

(ii) By [38, p. 93] there is an exact sequence

$$0 \to W(A) \to W(F) \to \coprod_{\mathfrak{p}} W(A/\mathfrak{p}),$$

where $\mathfrak{p}$ runs through the nonzero prime ideals of $A$. Since none of the $A/\mathfrak{p}$ is formally real, each $W(A/\mathfrak{p})$ is a 2-primary torsion group [39, Satz 16] as is $W(F)/W(A)$. Thus, a given homomorphism from $W(A)$ to $\mathbb{Z}$ or $\mathbb{F}_p$, $p$ odd, has at most one extension to $W(F)$. Furthermore, the unique homomorphism $W(A) \to \mathbb{F}_2$ [34, Remark 2.2] extends to the unique homomorphism $W(F) \to \mathbb{F}_2$. By [34, Remark 2.2] the prime ideals of $W(A)$ and $W(F)$ are exactly the kernels of such homomorphisms. Thus, the continuous map Spec $W(F) \to$ Spec $W(A)$ is injective. Since $W(F)$ is integral over $W(A)$, this map is also surjective and closed [12, Theorem 1, p. 38 and Remark 2, p. 39] and, hence, is a homeomorphism.

Note that Example 2.13 and the proof of Proposition 2.14(i) show that the converse of Proposition 2.14(ii) also holds.

*Remark.* If $A$ is the ring of integers in an algebraic number field $F$ then the hypothesis of Proposition 2.14(ii) is satisfied and so the nonmaximal prime ideals of $W(A)$ correspond bijectively with the real embeddings of $F$. This is a small part of [38, Corollary 4.5, p. 97].

Finally, we consider pairs $(C, J)$ with $C$ semilocal but not necessarily connected. In defining signatures $\sigma\colon A^* \to \{\pm 1\}$ of $(C, J)$ we replace $W(C, J)$ in Definition 1.1 by the Witt ring $WF(C, J)$ of *free* nondegenerate Hermitian spaces over $(C, J)$ [33, Remark 1.18]. The ring $WF(C, J)$ is a homomorphic image of $\mathbb{Z}[A^*/NC^*]$ and in fact a Witt ring for $A^*/NC^*$ in the sense of [33, Definition 3.12]. Note that $WF(C, J) = W(C, J)$ if $C$ is connected.

Lemma 2.3 and Proposition 2.4 still hold with identical proofs if $C$ is not connected.

The *pair* $(C, J)$ is called connected, if $C$ has no decomposition $C = C_1 \times C_2$ with $C_1$ and $C_2$ stable under $J$. If $(C, J)$ is connected but $C$ is not connected then $(C, J) \cong (A \times A, J_0)$ with $A$ connected and $J_0$ the involution $(x, y) \mapsto (y, x)$ on $A \times A$ [33, Lemma 1.8]. In this case $NC^* = A^*$ and, as is easily seen, $WF(C, J) = \mathbb{F}_2$ so $(C, J)$ has no signatures.

We shall now show that even in the case that $(C, J)$ is not connected the signatures of $(C, J)$ correspond bijectively with the ring homomorphisms from $W(C, J)$ to $\mathbb{Z}$. Let

$$(C, J) = (C_1, J_1) \times \cdots \times (C_t, J_t)$$

be the decomposition of $(C, J)$ into connected pairs. Then by [33, Lemma 1.9] we have a corresponding decomposition

$$W(C, J) = W(C_1, J_1) \times \cdots \times W(C_t, J_t)$$

of Witt rings. Assume $C_i$ is connected for $1 \leqslant i \leqslant s$ and not connected for $s < i \leqslant t$. ($s = 0$ if no $C_i$ is connected.) For any index $i$ with $1 \leqslant i \leqslant s$ we have a ring homomorphism

$$\mu_i \colon W(C, J) \longrightarrow W(C_i, J_i) \xrightarrow{\nu_i} \mathbb{F}_2,$$

where the first map is the canonical projection and the second map $\nu_i$ is reduction modulo the unique maximal ideal of $W(C_i, J_i)$ containing 2.

LEMMA 2.15. *If $s \geqslant 1$ the canonical map from $WF(C, J)$ to $W(C, J)$ is injective. The image consists of all elements $z$ in $W(C, J)$ with $\mu_1(z) = \cdots = \mu_s(z)$.*

*Proof.* Denote by $H_i$ the standard hyperbolic plane $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ over $(C_i, J_i)$ and by $H$ the standard hyperbolic plane over $(C, J)$. Note that $H = H_1 \times \cdots \times H_t$. We consider a free space $E$ over $(C, J)$ whose image in $W(C, J)$ is zero. This means that in the decomposition $E = E_1 \times \cdots \times E_t$ into spaces $E_i$ over $(C_i, J_i)$ every component $E_i$ has image zero in $W(C_i, J_i)$.

We first treat the case $i \leqslant s$. The Witt ring $W(C_i, J_i)$ is the quotient ring $K(C_i, J_i)/KM(C_i, J_i)$ of the Grothendieck ring $K(C_i, J_i)$ of nondegenerate spaces over $(C_i, J_i)$ modulo the ideal $KM(C_i, J_i)$ generated by the metabolic spaces [33, Corollary 1.6]. Thus, the class, $\mathrm{cl}(E_i)$ of $E_i$ in $K(C_i, J_i)$ lies in $KM(C_i, J_i)$. Since every projective $C_i$-module is free, the latter is additively generated by $\mathrm{cl}(H_i)$ [33, Lemma 1.3(i) and (iii)]. Hence, $\mathrm{cl}(E_i) = r_i \,\mathrm{cl}(H_i)$ for some integer $r_i$. Taking account of the definition of equality in

$K(C_i, J_i)$ shows that $r_i$ is positive. Hence, there exists a nondegenerate space $G_i$ over $(C_i, J_i)$ such that

$$E_i \perp G_i \cong r_i \times H_i \perp G_i .$$

Since $E$ is free, all the $E_i$ are free over $C_i$ of the same rank. Thus, $r_1 = \cdots = r_t$. By [33, Lemma 1.10], the spaces $G_i$ are free $C_i$-modules. Thus, by adding suitable spaces to the $G_i$ we may assume that the rank of $G_i$ over $C_i$ is $u$, independent of $i$.

Now assume $i > s$. Then since the rank of $E_i$ is the same as that of $E_1$, the previous considerations show that $E_i$ has even rank. It can then be easily shown, using [33, Example 1.7], that $E_i \cong r_1 \times H_i$. Let $G_i$ be an arbitrary nondegenerate free $C_i$-space of rank $u$. Then $G = G_1 \times \cdots \times G_t$ is a free space over $(C, J)$ and

$$E \perp G \cong r_1 \times H \perp G,$$

which shows that $WF(C, J) \to W(C, J)$ is injective.

For any $x$ in the image of $WF(C, J)$, in $W(C, J)$ we have $\mu_1(x) = \cdots = \mu_s(x)$, since there is only one ring homomorphism from $WF(C, J)$ to $\mathbb{F}_2$. Now consider an element $x$ in $W(C, J)$ with $\mu_1(x) = \cdots = \mu_s(x)$ and let $E = E_1 \times \cdots \times E_t$ be a space over $(C, J)$ representing $x$. Then, for $1 \leqslant i \leqslant s$, the $E_i$ are free spaces with rank $E_1 \equiv \cdots \equiv$ rank $E_s$ (mod 2). Adding a suitable multiple $r_i \times H_i$ to $E_i$, for $1 \leqslant i \leqslant s$, we get spaces $F_1, \ldots, F_s$ of the same rank $n$. For $s < i \leqslant t$, let $F_i$ be an arbitrary nondegenerate free space of rank $n$. Then the space $F = F_1 \times \cdots \times F_t$ is free over $(C, J)$ and since $W(C_i, J_i) = 0$ for $s < i \leqslant t$ [33, Example 1.7], $F$ represents the element $x$ of $W(C, J)$. Thus, $x$ lies in the image of $WF(C, J)$.

For $s \geqslant 1$ we shall identify $WF(C, J)$ with its image in $W(C, J)$.

PROPOSITION 2.16. *If $s \geqslant 1$ the restriction map defines a bijection of the set of ring homomorphisms from $W(C, J)$ to $\mathbb{Z}$ with the set of ring homomorphisms from $WF(C, J)$ to $\mathbb{Z}$.*

*Remark* 2.17. If $s = 0$ then by [33, Remark 1.7 and Lemma 1.9], $W(C, J) = 0$ and it is easily seen that $WF(C, J) = \mathbb{F}_2$. Thus, neither ring admits homomorphisms to $\mathbb{Z}$.

*Proof of Proposition* 2.16. Denote the subring $WF(C, J)$ of $W(C, J)$ by $R$ and $W(C_i, J_i)$ by $R_i$, so that $W(C, J) = \prod_{i=1}^{t} R_i$. Let $\varphi$ be a homomorphism from $WF(C, J)$ to $\mathbb{Z}$. By Lemma 2.15, $2x$ lies in $R$ for every $x$ in $\prod R_i$, and hence $\prod R_i/R$ is a group of exponent 2. Thus, $\varphi$ has at most one extension to a homomorphism from $\prod R_i$ to $\mathbb{Z}$. Moreover, such an extension always

exists. Indeed, the kernel $Q$ of $\varphi$ is a minimal prime ideal of $R$ so by [11, Proposition 16, p. 96] there is a prime ideal $P$ of $\prod R_i$ lying over $Q$. Clearly,

$$P = R_1 \times \cdots \times P_k \times \cdots \times R_t,$$

with a unique index $k$ and a unique minimal prime ideal $P_k$ of $R_k$. Since $\mathbb{Z} \cong R/Q$ embeds into $\prod R_i/P \cong R_k/P_k$, it follows that $\prod R_i/P \cong \mathbb{Z}$. The homomorphism $\lambda$ from $\prod R_i$ to $\mathbb{Z}$ with kernel $P$ extends $\varphi$.

We denote by $A_i$ the fixed ring of $J_i$ in $C_i$ and by $\pi_i$ the projection from $A = A_1 \times \cdots \times A_t$ onto $A_i$. The proof of Proposition 2.16 together with Remark 2.17 immediately imply the following.

COROLLARY 2.18. *The signatures $\sigma: A^* \to \{\pm 1\}$ on $(C, J)$ correspond bijectively with the homomorphisms $\lambda$ from $W(C, J)$ to $\mathbb{Z}$ via $\sigma(a) = \lambda[(a)]$. For any signature $\sigma$ on $(C, J)$ there exists exactly one index $k$ between 1 and $t$ and one signature $\sigma_k$ on $(C_k, J_k)$ such that*

$$\sigma = \sigma_k \circ \pi_k: A^* \to A_k^* \to \{\pm 1\}.$$

*Thus,* $\mathrm{Sign}(C, J)$ *can be identified with* $\coprod_{k=1}^{t} \mathrm{Sign}(C_k, J_k)$ *(disjoint union).*

As in the connected case we denote the homomorphism from $W(C, J)$ to $\mathbb{Z}$ which corresponds with the signature $\sigma$ of $(C, J)$ by $\bar{\sigma}$.

From Corollary 2.18 it is clear that problems about signatures may always be reduced to the connected case.

## 3. Topological Description of Reduced Witt Rings

In this section a *Witt ring* $R$ is always a Witt ring for some Abelian group $G$ of exponent 2 as defined in [33], i.e., $R$ is a nonzero homomorphic image of the integral group ring $\mathbb{Z}[G]$ and the torsion subgroup $R_t$ of $R$ is 2-primary. Clearly, for any Witt ring $R$, the group $G$ can always be chosen as $G(R) = \{x \text{ in } R \mid x^2 = 1\}$. Furthermore, if $G$ is an Abelian group of exponent 2, a homomorphic image $R$ of $\mathbb{Z}[G]$ is a Witt ring if and only if the reduced ring $R_{\mathrm{red}} = R/\mathrm{Nil}(R)$ is a Witt ring [33, Remark 3.13(ii)]. Our interest in these "abstract" Witt rings stems from the fact that the Witt ring $WF(C, J)$ of free spaces over a semilocal ring with involution is a Witt ring for the group $A^*/NC^*$ [33, Remark 1.18, Corollary 1.20, Theorem 3.9].

DEFINITION 3.1. (i) For any Witt ring $R$, let $X(R)$ denote the set of ring homomorphisms from $R$ to $\mathbb{Z}$.

(ii) For any topological space $X$ and discrete ring $D$, let $C(X, D)$ denote the ring of continuous functions from $X$ to $D$.

(iii) A *Boolean* topological space is a compact totally disconnected Hausdorff space.

*Remark* 3.2. If $R = WF(C, J)$ then the set $X(R)$ may be identified with $\mathrm{Sign}(C, J)$ as in Proposition 2.16, which explains its relevance to this paper.

LEMMA 3.3. *Let $R$ be a Witt ring. Then*

(i) *$R_t = R$ or $R_t = \mathrm{Nil}(R)$; the set $X(R)$ is empty if and only if $R_t = R$.*

(ii) *If $x$ is in $X(R)$ let $P_x = \ker x$. Then $x \mapsto P_x$ yields a bijection of $X(R)$ with the set of prime ideals of $P$ of $R$ such that $P \cap \mathbb{Z} = 0$. If $X(R) \neq \varnothing$ then $X(R)$ can be identified with the set $\min(R)$ of minimal prime ideals of $R$.*

*For the remainder of the lemma we assume $X(R) \neq \varnothing$.*

(iii) *In the Zariski topology the map $P \mapsto \mathbb{Q} \otimes P$[3] is a homeomorphism of the subspace $X(R)$ of $\mathrm{Spec}(R)$ with the Boolean space $\mathrm{Spec}(\mathbb{Q} \otimes R)$. Thus, we can regard $X(R)$ as the set of all $\mathbb{Q}$-algebra homomorphisms from $\mathbb{Q} \otimes R$ to $\mathbb{Q}$ under the correspondence $x \leftrightarrow 1 \otimes x$. The field $\mathbb{Q}$ is the only integral domain which occurs as a homomorphic image of $\mathbb{Q} \otimes R$.*

(iv) *For any element $s$ in $\mathbb{Q} \otimes R$, let $f_s$ be the function in $C(X(R), \mathbb{Q})$ defined by $f_s(x) = (1 \otimes x)(s)$. Then $s \mapsto f_s$ is an isomorphism of $\mathbb{Q}$-algebras.*

(v) *The image $1 \otimes R$ of $R$ in $\mathbb{Q} \otimes R$ is isomorphic to $R_{\mathrm{red}}$ and the isomorphism of* (iv) *maps $1 \otimes R$ into a subring of $C(X(R), \mathbb{Z})$.*

*Proof.* (i) That $R_t$ is either $R$ or $\mathrm{Nil}(R)$ follows from [33, Proposition 3.15]. Clearly, if $R_t = R$ then $X(R)$ is empty. If $X(R)$ is empty [33, Remark 3.2 and Proposition 3.4] show that $R_t = R$.

(ii) The map $x \mapsto P_x$ yields a bijection of $X(R)$ with the set of prime ideals $P$ of $R$ such that $R/P \cong \mathbb{Z}$, since $\mathbb{Z}$ has no automorphisms except the identity. The rest of (ii) then follows from [33, Remark 3.2, Theorem 3.9, Propositions 3.15 and 3.16].

(iii) If $S$ is the multiplicative semigroup $\mathbb{Z} - 0$ then $\mathbb{Q} \otimes R = S^{-1}\mathbb{Z}$. Hence, $P \mapsto \mathbb{Q} \otimes P$ is a bijection of the prime ideals $P$ of $R$ such that $P \cap \mathbb{Z} = 0$ and all the prime ideals of $\mathbb{Q} \otimes R$ [11, Proposition 11(ii), p. 91]. Furthermore, by [11, Corollary, p. 129] the foregoing map is a homeomorphism in the Zariski topology. Since by [33, Remark 2.6] $\mathbb{Q} \otimes R$ is von Neumann regular, [11, Exercise 16, p. 173] shows that $\mathrm{Spec}(\mathbb{Q} \otimes R)$ is a Boolean space.

[3] Unadorned $\otimes$ always denotes $\otimes_{\mathbb{Z}}$.

(iv) By (iii), for every prime ideal $M$ of $\mathbb{Q} \otimes R$ we have $\mathbb{Q} \otimes R/M \cong \mathbb{Q}$ so (iv) is a special case of [2, Theorem 2.3].

(v) It is clear that $\ker(R \to \mathbb{Q} \otimes R) = R_t$ which is $\mathrm{Nil}(R)$ by (i). Furthermore, by definition $f_{1\otimes r}(x) = x(r)$ lies in $\mathbb{Z}$, completing the proof.

Our main goal in this section is to study the embedding of $R_{\mathrm{red}}$ in $C(X(R), \mathbb{Z})$. However, we first shift our point of view by studying the Witt subrings of $C(X, \mathbb{Z})$ for an arbitrary Boolean space $X$.

DEFINITION 3.4. For any Boolean space $X$, let $\mathfrak{E}$ denote the basis of all clopen (closed and open) sets.

The proof of the following lemma will be omitted since its contents are either well known or the missing proofs can be easily supplied.

LEMMA 3.5. (i) *Let $U$, $V$ be in $\mathfrak{E}$ and set $U + V = U \cup V - U \cap V$, $UV = U \cap V$. Then $\mathfrak{E}$ is a Boolean ring with these operations.*

(ii) *If $D$ is an integral domain the only idempotents of $C(X, D)$ are the characteristic functions $e_U$, for $U$ in $\mathfrak{E}$. For an arbitrary commutative ring $D$, an element $f$ in $C(X, D)$ has the form*

$$f = \sum_1^n d_i e_{U_i},$$

*with $d_i$ in $D$ and $\{U_i\}$ a partition of $X$ by elements of $\mathfrak{E}$.*

(iii) $\mathfrak{E} \cong C(X, \mathbb{F}_2)$ *via* $U \to e_U$.

(iv) *The units of $C(X, \mathbb{Z})$ are precisely the functions $g_U = 1 - 2e_U$ for $U$ in $\mathfrak{E}$; $g_U$ is $-1$ on $U$, $1$ on $X - U$, and $g_U{}^2 = 1$.*

(v) $g_U g_V = g_{U+V}$.

DEFINITION 3.6. For any subring $T$ of $C(X, \mathbb{Z})$ let $\mathfrak{H}(T)$ denote the set of $U$ in $\mathfrak{E}$ with $g_U$ in $T$.

COROLLARY 3.7. (i) *If $T$ is a subring of $C(X, \mathbb{Z})$ then $\mathfrak{H}(T)$ is an additive subgroup of $\mathfrak{E}$ containing $X$. The units of $T$ are precisely the $g_U$ with $U$ in $\mathfrak{H}(T)$.*

(ii) *$C(X, \mathbb{Z})$ is the integral closure of $\mathbb{Z}$ in $C(X, \mathbb{Q})$.*

*Proof.* (i) By Lemma 3.5(v), $\mathfrak{H}(T)$ is a subgroup, and $X$ is in $\mathfrak{H}(T)$ since $g_X = -1$ lies in $T$. The last part is clear from Lemma 3.5 (iv).

(ii) By Lemma 3.5(ii), every element of $C(X, \mathbb{Z})$ is an integral linear combination of idempotents and so $C(X, \mathbb{Z})$ is integral over $\mathbb{Z}$. If $f$ in $C(X, \mathbb{Q})$ is integral over $\mathbb{Z}$, its values are elements of $\mathbb{Q}$ integral over $\mathbb{Z}$, and so lie in $\mathbb{Z}$. Hence, $f$ is in $C(X, \mathbb{Z})$.

PROPOSITION 3.8. *Let $\mathfrak{A}$ be an additive subgroup of $\mathfrak{E}$ containing $X$ and let*

$$S(\mathfrak{A}) = \sum_{U \in \mathfrak{A}} \mathbb{Z} g_U = \mathbb{Z} + \sum_{U \in \mathfrak{A}} 2\mathbb{Z} e_U .$$

*Then $S(\mathfrak{A})$ is a Witt subring of $C(X, \mathbb{Z})$ and the maps $\mathfrak{A} \mapsto S(\mathfrak{A})$, $T \mapsto \mathfrak{H}(T)$ are inverse isomorphisms of the lattice of additive subgroups $\mathfrak{A}$ of $\mathfrak{E}$ containing $X$, and the lattice of Witt subrings $T$ of $C(X, \mathbb{Q})$.*

*Proof.* Since any Witt subring of $C(X, \mathbb{Q})$ is integral over $\mathbb{Z}$, it is a subring of $C(X, \mathbb{Z})$ by Corollary 3.7 (ii). Because any subring $T$ of $C(X, \mathbb{Z})$ is torsion free and all units of $C(X, \mathbb{Z})$ have (multiplicative) order $\leqslant 2$, the subring $T$ is a Witt ring if and only if it is additively generated by its units. Thus, in view of Corollary 3.7 (i), we have the equality $S(\mathfrak{H}(T)) = T$, for any Witt subring $T$ of $C(X, \mathbb{Q})$. Furthermore, by Lemma 3.5 (v), $S(\mathfrak{A})$ is a ring and, hence, a Witt ring.

It remains to show that for any additive subgroup $\mathfrak{A}$ of $\mathfrak{E}$ containing $X$, we have $\mathfrak{H}(S(\mathfrak{A})) = \mathfrak{A}$. Thus, let $U$ in $\mathfrak{E}$ be an element of $\mathfrak{H}(S(\mathfrak{A}))$. Then $g_U$ and, hence, $2e_U$ lie in $S(\mathfrak{A})$. Therefore, there are integers $n_0$, $m_i$ such that

$$2e_U = n_0 + \sum_1^k 2m_i e_{U_i} ,$$

with $U_i$ in $\mathfrak{A}$. Evaluating both sides at a point of $X$ shows that $n_0$ is even so that we have

$$e_U = \sum_0^k m_i e_{U_i} ,$$

where $U_0 = X$ and $m_0 = n_0/2$. Thus, in $C(X, \mathbb{F}_2)$ we have

$$e_U = \sum_0^k \epsilon_i e_{U_i} ,$$

with $\epsilon_i = 0$ or 1, so by Lemma 3.5 (iii), $U = \sum_0^n \epsilon_i U_i$ in $\mathfrak{E}$. Hence, $U$ lies in the subgroup $\mathfrak{A}$, completing the proof of the proposition.

EXAMPLE 3.9. $S(\mathfrak{E}) = \mathbb{Z} + C(X, 2\mathbb{Z})$ is the largest Witt subring of $C(X, \mathbb{Q})$ while $S(\{\varnothing, X\}) = \mathbb{Z}$ is the smallest such. Furthermore, it is easily verified that $X(S(\mathfrak{E}))$ is homeomorphic to $X$. This follows as in the proof of Proposition 2.14 from the facts that $C(X, \mathbb{Z})/S(\mathfrak{E})$ is a group of exponent 2 and $\min(C(X, \mathbb{Z}))$ is homeomorphic to $X$ [1, Proposition 1.2], [40, Theorem 1.6.1].

Next, we need the following version of the Stone–Weierstrass theorem [26, Theorem 32] or [18, Proposition 1 and remark on p. 236].

THEOREM 3.10. *Let $F$ be a discrete field, $X$ a Boolean space, and $\mathscr{A}$ an $F$-subalgebra of $C(X, F)$ separating points. Then $\mathscr{A} = C(X, F)$.*

Proposition 3.11 is a slight recasting of Proposition 3 of [18].

PROPOSITION 3.11. *For any Boolean space $X$ let $Y = X/\sim$ run through the Boolean quotient spaces of $X$, and let $F$ be a discrete field. Then $Y \mapsto C(Y, F)$ yields a lattice antiisomorphism between the family of all Boolean quotient spaces of $X$ and the $F$-subalgebras of $C(X, F)$.*

*Proof.* For any $F$-subalgebra $\mathscr{A}$ of $C(X, F)$ we define an equivalence relation on $X$ by $x \sim y$ if $f(x) = f(y)$ for all $f$ in $\mathscr{A}$. Let $Y = X/\sim$. Since the projection $X \to Y$ is continuous, $Y$ is compact. By definition, $\mathscr{A}$ induces an $F$-algebra of continuous functions on $Y$ which separates points. Since $F$ is discrete, this shows immediately that $Y$ is Hausdorff and totally disconnected. Thus, by (3.10), $\mathscr{A} = C(Y, F)$.

Conversely, let $Y = X/\sim$ be a Boolean quotient space of $X$ with projection $\pi$ and let $\mathscr{A} = C(Y, F)$. Let $\sim'$ be the equivalence relation defined by $\mathscr{A}$ on $X$. Clearly, $x \sim y$ implies $x \sim' y$. On the other hand, if $x \sim' y$ then for every continuous function $\bar{f}: Y \to F$ we have $\bar{f}(\pi(x)) = \bar{f}(\pi(y))$. Since $Y$ is totally disconnected, $C(Y, F)$ separates points so that $\pi(x) = \pi(y)$, i.e., $x \sim y$. Thus, $\sim = \sim'$, proving the proposition.

COROLLARY 3.12. *Let $\mathfrak{B}$ be a subring of $\mathfrak{E}$ and set $\mathscr{S}(\mathfrak{B}) = \mathbb{Q}S(\mathfrak{B}) = \sum_{U \in \mathfrak{B}} \mathbb{Q}e_U$. Then $\mathscr{S}(\mathfrak{B})$ is a $\mathbb{Q}$-subalgebra of $C(X, \mathbb{Q})$ and the maps $\mathfrak{B} \mapsto \mathscr{S}(\mathfrak{B})$, $\mathscr{A} \to \mathfrak{H}(\mathscr{A})$ are inverse isomorphisms of the lattice of subrings of $\mathfrak{E}$ and the lattice of $\mathbb{Q}$-subalgebras of $C(X, \mathbb{Q})$.*

*Proof.* We identify $\mathfrak{E}$ with $C(X, \mathbb{F}_2)$ by the isomorphism of Lemma 3.5 (iii) so that subrings of $\mathfrak{E}$ correspond with $\mathbb{F}_2$-subalgebras of $C(X, \mathbb{F}_2)$. By Proposition 3.11, the lattice of $\mathbb{Q}$-subalgebras of $C(X, \mathbb{Q})$ and the lattice of $\mathbb{F}_2$-subalgebras of $C(X, \mathbb{F}_2)$ are both antiisomorphic to the lattice of Boolean quotient spaces of $X$. We, thus, obtain a lattice isomorphism between the two by associating subalgebras corresponding to the same quotient spaces. Let a subalgebra $\mathscr{A}$ of $C(X, \mathbb{Q})$ correspond to a quotient space $Y = X/\sim$. Now $g_U = 1 - 2e_U$ lies in $\mathscr{A}$ if and only if $e_U$ does. Thus,

$$\mathfrak{H}(\mathscr{A}) = \{U \text{ in } \mathfrak{E} \mid e_U(x) = e_U(y) \text{ if } x \sim y\},$$

which under the isomorphism of Lemma 3.5 (iii) is precisely the $\mathbb{F}_2$-subalgebra of $C(X, \mathbb{F}_2)$ corresponding to $Y$. If a subring $\mathfrak{B}$ of $\mathfrak{E}$ correspond to a quotient space $Y = X/\sim$, it is clear that the equivalence relation defined by $\mathscr{S}(\mathfrak{B})$ on $X$ is precisely $\sim$ so that the inverse isomorphism carries $\mathfrak{B}$ to $\mathscr{S}(\mathfrak{B})$.

COROLLARY 3.13. *If $R$ is a Witt subring of $C(X, \mathbb{Q})$ then $\mathfrak{H}(\mathbb{Q}R) = \langle \mathfrak{H}(R) \rangle$, the subring of $\mathfrak{E}$ generated by $\mathfrak{H}(R)$.*

*Proof.* Since $\mathfrak{H}(\mathbb{Q}R)$ is a subring of $\mathfrak{E}$ by Corollary 3.12 and $\mathfrak{H}(\mathbb{Q}R) \supset \mathfrak{H}(R)$, it is clear that $\mathfrak{H}(\mathbb{Q}R) \supset \langle \mathfrak{H}(R) \rangle$. On the other hand, from Proposition 3.8 it is clear that $\mathscr{S}(\langle \mathfrak{H}(R) \rangle) \supset \mathbb{Q}R$, whence by Corollary 3.12 we have $\langle \mathfrak{H}(R) \rangle \supset \mathfrak{H}(\mathbb{Q}R)$.

COROLLARY 3.14. *Let $R$ be a Witt subring of $C(X, \mathbb{Q})$. Then the following are equivalent.*

(i) *$C(X, \mathbb{Z})/R$ is a torsion group.*

(ii) *$\mathfrak{H}(R)$ is a subbasis of $X$.*

(iii) *$R$ separates the points of $X$.*

*Proof.* Statement (i) is equivalent to $\mathbb{Q}R = C(X, \mathbb{Q})$ and since $e_{U_1} e_{U_2} \cdots e_{U_n} = e_{U_1 \cap U_2 \cap \cdots \cap U_n}$ and $X$ is compact, (ii) is equivalent to the statement that $\langle \mathfrak{H}(R) \rangle = \mathfrak{E}$. Thus, the equivalence of (i) and (ii) follows from Corollaries 3.12 and 3.13. The implication (i) $\Rightarrow$ (iii) is clear and (iii) $\Rightarrow$ (i) follows from (3.10).

LEMMA 3.15. *If $R$ is a Witt subring of $C(X, \mathbb{Q})$ then the torsion subgroup of $C(X, \mathbb{Z})/R$ is 2-primary. In particular, if $C(X, \mathbb{Z})/R$ is torsion then*

$$2^{-\infty}C(X, \mathbb{Z}) = C(X, 2^{-\infty}\mathbb{Z}) = 2^{-\infty}R,$$

*where, for any commutative ring $T$, $2^{-\infty}T$ denotes the ring of fractions of $T$ with respect to the multiplicative semigroup $\{2^n\}$.*

*Proof.* Let $\tilde{R}$ be the integral closure of $R$ in $\mathbb{Q}R$. In view of Corollary 3.7 (ii), it is readily verified that the torsion subgroup of $C(X, \mathbb{Z})/R$ equals $\tilde{R}/R$, which is 2-primary by [33, Proposition 3.17].

PROPOSITION 3.16. *Let $R$ be a Witt subring of $C(X, \mathbb{Q})$ and $\psi\colon Z[G] \to R$ a ring surjection with $G$ an Abelian group of exponent 2. Then the elements of $\mathfrak{H}(R)$ are precisely the sets*

$$W(a) = \{x \text{ in } X \mid \psi(a)(x) = -1\}$$

*and their complements $X - W(a)$, where $a$ runs through the elements of $G$.*

*Proof.* Since $a^2 = 1$ we must have $\psi(a)(y) = \pm 1$ for all $y$ in $X$. Hence, $g_{W(a)} = \psi(a)$ and $g_{X-W(a)} = -\psi(a)$. Since $\mathrm{Nil}(R) = 0$, [33, Remark 3.22 and Theorem 3.23] shows that every unit of $R$ is of the form $\pm\psi(a)$, proving the proposition.

*Remark* 3.17. Following Belskii [7] we call a Witt ring for an Abelian group $G$ of exponent 2 "small" if there is an element $a$ in $G$ such that $\psi(a) = -1$. For example, the Witt ring $R = WF(C, J)$ of free nondegenerate Hermitian spaces over a semilocal ring $C$ with involution $J$ is small for $G = A^*/NC^*$. If $R$ is a small Witt ring for $G$, Proposition 3.15 shows that $\mathfrak{H}(R)$ is the family $W(a)$, with $a$ running through $G$. It should be noted that any Witt ring $R$ is small for $G = G(R) =$ the group of all $r$ in $R$ with $r^2 = 1$.

If $R$ is a Witt ring and $X = X(R)$ is the Boolean space of Definition 3.1 (i) and Lemma 3.3 (iii), our results yield the following theorem.

THEOREM 3.18. *Let $R$ be a Witt ring with $R_t \neq R$ and $\psi: \mathbb{Z}[G] \to R$ a ring surjection for some Abelian group $G$ of exponent 2. If $X = X(R)$ then*

(i) *$C(X, \mathbb{Z})/R_{\text{red}}$ is a 2-primary torsion group and $C(X, \mathbb{Z})$ is the integral closure of $R_{\text{red}}$ in $C(X, \mathbb{Q})$.*

(ii) *The sets $W(a) = \{x \text{ in } X \mid \psi(a)(x) = -1\}$ and their complements form a subbasis $\mathfrak{H}_R$ of the topology of $X$.*

(iii) *$\mathfrak{H}_R$ is the family of all clopen subsets $U$ of $X$ such that $2e_U$ is in $R_{\text{red}}$, i.e., in the notation of Definition 3.6, $\mathfrak{H}_R = \mathfrak{H}(R)$. Hence, $\mathfrak{H}_R$ depends only on $R$ and is independent of $G$ and $\psi$. Furthermore, $\mathfrak{H}_R$ is an additive subgroup of $\mathfrak{E}$, the Boolean ring of all clopen subsets of $X$, containing $X$.*

(iv) $R_{\text{red}} = \mathbb{Z} + \sum_{U \in \mathfrak{H}_R} 2\mathbb{Z}e_U$.

*Proof.* From the definition of $X(R)$ and the map $R \to C(X, \mathbb{Z})$ of Lemma 3.3 (v), it is clear that the Witt subring $R_{\text{red}}$ of $C(X, \mathbb{Q})$ separates points of $X$. Thus, (i) follows from Corollary 3.14, Lemma 3.15, and Corollary 3.7 (ii). Statement (ii) is an immediate consequence of Proposition 3.16 and Corollary 3.14, while (iii) and (iv) follow from Proposition 3.8.

*Remark* 3.19. In case $R = W(F)$ is the Witt ring of a formally real field $F$, $X(R)$ may be identified with the set of all orderings of $F$, as was pointed out in Remark 2.7 (ii), and $G$ may be taken as $F^*/F^{*2}$. Harrison (unpublished) first proposed that the set of orderings be topologized by taking the sets $W(a) = \{< \text{ in } X(R) \mid a < 0\}$, for $a$ in $F^*$, as a subbasis of the topology.

THEOREM 3.20. *Let $G$ be an Abelian group of exponent 2, $\psi: \mathbb{Z}[G] \to R$ a ring surjection making $R$ into a Witt ring, and $X = X(R)$. If $R_t \neq R$ the following statements are equivalent.*

(i) $R_{\text{red}} = \mathbb{Z} + C(X, 2\mathbb{Z})$.

(ii) *$C(X, \mathbb{Z})/R_{\text{red}}$ is a group of exponent 2.*

(iii) $\mathfrak{H}_R = \mathfrak{E}$.

(iv) *For any two disjoint closed subsets $Y_1$, $Y_2$ of $X$ there is an element $r = \pm\psi(a)$ with $a$ in $G$ such that $y_1(r) = 1$ for all $y_1$ in $Y_1$ and $y_2(r) = -1$ for all $y_2$ in $Y_2$.*

*Proof.* The implication (i) $\Rightarrow$ (ii) is obvious, (ii) $\Rightarrow$ (iii) follows from Theorem 3.18 (iii), and (iii) $\Rightarrow$ (i) follows from Proposition 3.8 and Example 3.9.

(iii) $\Rightarrow$ (iv). The compact Hausdorff space $X$ is normal so there is an open set $E$ in $X$ such that $Y_1 \subset E$ and $E \cap Y_2 = \varnothing$. Since $X$ is totally disconnected, $E$ is a union of clopen sets and since $Y_1$ is compact there exist clopen sets $U_1, \ldots, U_n$ such that $Y_1 \subset U_1 \cup \cdots \cup U_n \subset E$. Then $U = U_1 \cup \cdots \cup U_n$ is a clopen set with $Y_1 \subset U$ and $Y_2 \subset X - U$. By (iii), $U$ is in $\mathfrak{H}_R$ and so by Theorem 3.18 (ii) there is an element $r = \pm\psi(a)$ having the desired properties.

(iv) $\Rightarrow$ (iii). Let $U$ be a clopen subset of $X$. Applying (iv) to $Y_1 = U$, $Y_2 = X - U$ shows that $U$ lies in $\mathfrak{H}_R$ in view of Theorem 3.18 (ii).

In view of Remark 3.19 we have the following corollary.

COROLLARY 3.21. *Let $F$ be a formally real field, $X$ the Boolean space of all orderings of $F$, and $W(F)$ the Witt ring of $F$. Then the following statements are equivalent.*

(i) $W(F)_{\text{red}} \cong \mathbb{Z} + C(X, 2\mathbb{Z})$.

(ii) $C(X, \mathbb{Z})/W(F)_{\text{red}}$ *is a group of exponent* 2.

(iii) *If $U$ is a clopen subset of $X$ there exists an element $a$ of $F^*$ such that an ordering $< $ is in $U$ if and only if $a < 0$.*

(iv) (*Approximation*). *Given any two disjoint closed sets $Y_1$, $Y_2$ of orderings of $F$ there is an element $a$ in $F^*$ with $a < 0$ for $<$ in $Y_1$ and $0 < a$ for $<$ in $Y_2$.*

*Remark* 3.22. (i) In [23, Theorem 3.5] it is shown that condition (iii) of Corollary 3.21 is also equivalent to $\mathfrak{H}_{W(F)}$ being a basis of the open sets of $X = X(W(F))$.

(ii) It is shown in [13, Theorem 2.1], [38, Example 2.10, p. 64], and [23, Section 3, Example 1] that the equivalent conditions of Corollary 3.21 hold for an arbitrary formally real algebraic extension of $\mathbb{Q}$. Moreover, Elman and Lam have also shown that the conditions of Corollary 3.21 hold for a formally real extension of transcendence degree 1 of a real closed field [23, Section 3, Example 2].

COROLLARY 3.23. *Let $R = \psi(\mathbb{Z}[G])$ be a small Witt ring for an Abelian group $G$ (Remark* 3.17) *and let $x_1, \ldots, x_n$ be $n$ distinct elements of $X(R)$, i.e.,*

*$x_i: R \to \mathbb{Z}$ are distinct ring homomorphisms. Let $B$ denote the subring of $\mathbb{Z} \times \cdots \times \mathbb{Z}$ ($n$ factors) of all elements $(b_1, \ldots, b_n)$ with $b_i \equiv b_j \pmod 2$, i.e., $B = \mathbb{Z} + (2\mathbb{Z})^n$. Then*

(i) $\mathrm{Im}(x_1, \ldots, x_n) \subset B$.

(ii) *The following statements are equivalent.*

(a) $\mathrm{Im}(x_1, \ldots, x_n) = B$.

(b) *For any $i$, $1 \leqslant i \leqslant n$, there exists an element $a_i$ in $G$ with $x_i(\psi(a_i)) = -1$, $x_j(\psi(a_i)) = 1$, $i \neq j$.*

(c) *The characters $\chi_i: G \to \{\pm 1\}$, defined by $\chi_i(a) = x_i(\psi(a))$ for $a$ in $G$, are linearly independent in the $\mathbb{F}_2$-vector space $\hat{G}$ of all characters of $G$.*

*Proof.* By [33, Proposition 3.14], $\bar{R} = R/\bigcap_{i=1}^{n} \ker x_i$ is a reduced Witt ring for $G$. Thus, without loss of generality we may assume $\bar{R} = R$ so that $X(R) = \{x_1, \ldots, x_n\}$. Then (i) follows from Theorem 3.18 (iv) and the equivalence of (a) and (b) of (ii) is easily deduced from the equivalence of (i) and (iv) of Theorem 3.20.

(c) $\Leftrightarrow$ (b). If we write $G$ additively as an $\mathbb{F}_2$-vector space then $\hat{G}$ becomes the dual space $\hom_{\mathbb{F}_2}(G, \mathbb{F}_2)$ and the equivalence of (c) and (b) is a standard result of linear algebra [8, Corollary 2(i), p. 160].

EXAMPLES 3.24. (i) Let $F$ be a formally real field with $F^*/F^{*2}$ a finite group of order $2^n$. Then $W(F)$ is a small Witt ring for $F^*/F^{*2}$, and since an element $x$ in $X(W(F))$ is completely determined by the corresponding character it follows that the set of orderings of $F$ can be regarded as a subset of the set of all characters of $F^*/F^{*2}$ sending $-1 \cdot F^{*2}$ to $-1$. Thus, there are at most $2^{n-1}$ orderings on $F$.

According to [20, Satz 4], $F$ has $2^{n-1}$ orderings if and only if $-1$ is a not a square in $F$ and all extensions $F(q^{1/2})$ with $q$ in $F^*$, $-q$ not a square, are Pythagorean fields, i.e., sums of squares are squares. See also [23, Corollary 4.5].

If the conditions of Corollary 3.21 hold then by Corollary 3.23 (ii) (c), $F$ has at most $n$ orderings. In Section 4, Example 4.10 (iii) and [23, Corollary 5.7] it is shown that if $F$ is a Pythagorean field then $F$ has exactly $n$ orderings if and only if the conditions of Corollary 3.21 hold.

(ii) Let $F$ be a formally real field and $x_1, \ldots, x_n$ elements of $X(W(F))$ corresponding to Archimedean orderings of $F$. Then each $x_i$ yields an order isomorphism of $F$ into the field of real numbers [9, Example 11a, p. 57] and so as is well known [4, Theorem 8, p. 10] condition (b) of Corollary 3.23 (ii) is fulfilled. Hence, $\mathrm{Im}(x_1, \ldots, x_n) = B$.

(iii) Let $R$ be an arbitrary Witt ring with $R \neq R_t$ and let $x_1, \ldots, x_n$, $n \leqslant 3$, be elements of $X(R)$. Then we always have $\mathrm{Im}(x_1, \ldots, x_n) = B$. To

see this note that the ring $R$ may be taken to be a small Witt ring for $G = \{r \in R \mid r^2 = 1\}$. Then condition (c) of Corollary 2.23 (ii) is easily seen to be fulfilled for this $G$. Indeed, since none of the $\chi_i$, $i \leqslant 3$, can be the identity character, the cases $n = 1$, 2 are clear and if $n = 3$, a relation $\chi_1\chi_2\chi_3 = 1$ would lead to a contradiction when applied to $-1$.

(iv) Let $F = \mathbb{R}((x))((y))$ be the field of iterated formal power series in two variables over the real field. Then by a theorem of Springer [45], $W(F)$ is isomorphic to $\mathbb{Z}[G]$, with $G$ the Klein four group. Hence, there are exactly four homomorphisms $W(F) = Z[G] \to \mathbb{Z}$ corresponding to the four characters of $G$. Since these are linearly dependent, $\mathrm{Im}(x_1, x_2, x_3, x_4) \subsetneq B$ in this case. Thus, the orderings of $F$ do not satisfy the conditions of Corollary 3.21.

Our final result of this section yields a lower bound on $\mathrm{Im}(x_1, \ldots, x_n)$.

PROPOSITION 3.25. *Let $R$ be a Witt ring and $x_i: R \to \mathbb{Z}$ distinct elements of $X(R)$, $i = 1, \ldots, n$. Then* $\mathrm{Im}(x_1, \ldots, x_n)$ *contains* $(2^{[n/2]}\mathbb{Z})^n$ $(= 2^{[n/2]}\mathbb{Z} \times \cdots \times 2^{[n/2]}\mathbb{Z})$, *where as usual* $[k]$ *denotes the greatest integer* $\leqslant k$.

*Proof.* If $n = 1$ the conclusion is vacuous and for $n = 2, 3$ it follows from Example 3.24 (iii). We proceed by induction. Thus, suppose the proposition is true for all $k < n$ and $n \geqslant 4$.

To prove the result, it suffices to find an $r$ in $R$ such that $x_1(r) = 2^{[n/2]}$ and $x_i(r) = 0$, $i > 1$, for then similar elements will exist with $x_i$ replacing $x_1$ and it will follow that $\mathrm{Im}(x_1, \ldots, x_n) \supset (2^{[n/2]}\mathbb{Z})^n$. Since $[(n-2)/2] = [n/2] - 1$, the induction hypothesis guarantees the existence of $s$ and $t$ in $R$ with

$$(x_1(s), \ldots, x_n(s)) = (2^{[n/2]-1}, 0, \ldots, 0, *, *),$$
$$(x_1(t), \ldots, x_n(t)) = (2, *, *, \ldots, *, 0, 0),$$

where the asterisks stand for arbitrary integers. Then the required element is $r = st$.

## 4. A Generalization of a Theorem of Artin–Pfister

In this section the results obtained so far are applied to obtain a generalization of [39, Satz 21] which in turn is an extension of [3, Satz 1]. We also prove a result concerning extensions of signatures and study certain ideals in Witt rings. We continue to use the notations of Sections 2 and 3 and in this section $C$ will always denote a connected semilocal ring with involution $J$.

DEFINITION 4.1. A subset $M$ of $A^*$ is *saturated* with respect to $(C, J)$

if $M$ is a subgroup of $A^*$ and every unit of the form $N(c_1)a_1 + \cdots + N(c_r)a_r$ with $c_1, \ldots, c_r$ in $C$ and $a_1, \ldots, a_r$ not necessary distinct elements of $M$, lies in $M$.

The last condition is equivalent to asserting that for $a_1, \ldots, a_r$ in $M$ every unit represented by the space $(a_1, \ldots, a_r)$ lies in $M$.

Clearly, $A^*$ is saturated and the intersection of saturated sets is saturated. Hence, any subset $M$ of $A^*$ is contained in a smallest saturated subset of $A^*$ which is called the *saturation* of $M$ and is denoted by $\hat{M}$. Since for any $a$ in $A^*$ we have $a^{-1} = aN(a^{-1})$, the group $\hat{M}$ consists of the units in the semiring generated by $N(C)$ and the elements of $M$; i.e., if $M \neq \varnothing$ the elements of $\hat{M}$ are all the units of the form

$$\sum_{0 \leqslant i_j \leqslant 1} c_{(i)} a^{i_1} \cdots a_r^{i_r},$$

with $a_1, \ldots, a_r$ in $M$, $(i) = (i_1, \ldots, i_r)$, and $c_{(i)}$ a sum of norms.

DEFINITION 4.2. For any subset $M$ of $A^*$ let $V(M) = \{\sigma \text{ in } \mathrm{Sign}(C, J) \mid \sigma(m) = 1 \text{ for all } m \text{ in } M\}$ and for any subset $Y$ of $\mathrm{Sign}(C, J)$ let $\Gamma(Y) = \{a \text{ in } A^* \mid \sigma(a) = 1 \text{ for all } \sigma \text{ in } Y\}$. We write $V(m)$ and $\Gamma(\sigma)$ for the sets $V(\{m\})$ and $\Gamma(\{\sigma\})$.

LEMMA 4.3. (i) *$V(M)$ is a closed subset of* $\mathrm{Sign}(C, J)$.

(ii) $V(M) = V(\hat{M})$.

(iii) *$\Gamma(\sigma)$ is a saturated subgroup of index two.*

*Proof.* Since $V(m) = W(-mNC^*)$, Proposition 3.16 shows that the set $V(m)$ is clopen in $\mathrm{Sign}(C, J)$ for any $m$ in $A^*$. Hence, $V(M) = \bigcap_{m \text{ in } M} V(M)$ is closed, proving (i).

The last two statements follows immediately from Definition 4.2 and Lemma 2.3 (ii).

DEFINITION 4.4. The involution $J$ is called *tracique* if there is an element $c$ in $C$ with $c + J(c) = 1$.

LEMMA 4.5. *Let $C$ be an arbitrary commutative ring with involution $J$. If $J$ is tracique then for any metabolic space $M$ over $(C, J)$ we have $M \cong H \perp \cdots \perp H$, where $H$ denotes the hyperbolic plane given by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. In particular, for each unit $a$ of $A$ the metabolic space $(a) \perp (-a) \cong H$.*

*Proof.* By [33, Lemma 1.3 (iii)] every metabolic space is isometric to an orthogonal sum of spaces $\left(\begin{smallmatrix} a & 1 \\ 1 & 0 \end{smallmatrix}\right)$ for arbitrary elements $a$ of $A$. Let $\Phi$ denote the form of $H$ and $\{x_1, x_2\}$ a basis of $H$ with $\Phi(x_1, x_1) = \Phi(x_2, x_2) = 0$, $\Phi(x_1, x_2) = 1$. Let $c$ be an element of $C$ such that $c + J(c) = 1$. Then $y_1 = x_1 + acx_2$ and $x_2$ are also a basis of $H$ and $\Phi(y_1, y_1) = a$, $\Phi(x_2, x_2) = 0$, $\Phi(y_1, x_2) = 1$. If $a$ is in $A^*$ then $y_1$ and $y_2 = x_1 - aJ(c)x_2$ constitute an orthogonal basis of $H$ with $\Phi(y_1, y_1) = a$, $\Phi(y_2, y_2) = -a$.

EXAMPLES 4.6. (i) If 2 is a unit in $A$ then every involution is tracique with $c = 1/2$.

(ii) Let $J$ be tracique and $M$ a saturated subset of $A^*$. If $M$ contains $-1$, the set $M$ equals $A^*$, since by Lemma 4.5 every unit is represented by the space $(1, -1)$.

(iii) Assume $C$ contains no maximal ideal $\mathfrak{m}$ with $C/\mathfrak{m} = \mathbb{F}_2$. If $M$ is a saturated subset of $A^*$ with $-1$ not in $M$ and $[A^* : M] = 2$ then by Proposition 2.4 (ii) there is a $\sigma$ in $\mathrm{Sign}(C, J)$ such that $M = \Gamma(\sigma)$.

Before stating the main theorem of this section we quote the following result which can be found in [6]. In case $J$ is the identity the result can be found in [28] or [42].

THEOREM 4.7. *Let $J$ be tracique. If $E_1$, $E_2$, and $F$ are nondegenerate spaces over $(C, J)$ such that $E_1 \perp F \cong E_2 \perp F$ then $E_1 \cong E_2$. Thus, if $[E_1] = [E_2]$ in $W(C, J)$ and $E_1$, $E_2$ have the same rank over $C$ then $E_1 \cong E_2$.*

THEOREM 4.8. *For every subset $M$ of $A^*$,*

$$\hat{M} = \Gamma(V(M))$$

*with the convention that $\Gamma(\varnothing) = A^*$.*

*Proof.* The sets $\{1\}$ and $\varnothing$ have the same saturation and $V(1) = V(\varnothing)$ so we may assume that $M$ is nonempty. Since for all $\sigma$ in $V(M)$ we have $M \subset \Gamma(\sigma)$ and by Lemma 4.3 (iii) the subgroup $\Gamma(\sigma)$ is saturated, it follows that $\hat{M} \subset \bigcap_{\sigma \text{ in } M} \Gamma(\sigma) = \Gamma(V(M))$.

We first prove the reverse inclusion for the case $M = \{a_1, \ldots, a_r\}$ is a finite subset of $A^*$. Let $a$ in $A^*$ be such that $\sigma(a) = 1$ for all $\sigma$ in $V(M)$ and let $E$ be the space $(1, -a) \otimes (1, a_1) \otimes \cdots \otimes (1, a_r)$. Then $\bar{\sigma}([E]) = 0$ for all $\sigma$ in $\mathrm{Sign}(C, J)$, and, thus, $[E]$ is a nilpotent element of $W(C, J)$. (If $\mathrm{Sign}(C, J) = \varnothing$ this is still true since the rank of $E$ is even [33, Proposition 3.16 and Example 3.11]). Then by [33, Example 3.11] there is an integer $m$ such that $2^m[E] = 0$ in $W(C, J)$, i.e.,

$$[2^m \times (1, a_1) \otimes \cdots \otimes (1, a_r)] = [2^m \times (a) \otimes (1, a_1) \otimes \cdots \otimes (1, a_r)].$$

But then by Theorem 4.7 we have

$$2^m \times (1, a_1) \otimes \cdots \otimes (1, a_r) \cong 2^m \times (a) \otimes (1, a_1) \otimes \cdots \otimes (1, a_r)$$

over $(C, J)$. Since $a$ is represented by the form on the right, it is also represented by the form on the left so $a$ lies in $\hat{M}$. Thus, we have proved Theorem 4.8 if $M$ is finite.

Now let $M$ be an arbitrary nonempty subset of $A^*$ and again let $a$ be a unit in $A$ with $\sigma(a) = 1$ for all $\sigma$ in $V(M)$, i.e., $V(a) \supset V(M)$. Let $\{M_i\}_{i\in I}$ be the family of finite subsets of $M$ and let $Y_i = V(M_i) \cap V(-a)$. By Lemma 4.3 (i) the $Y_i$ are a family of closed subsets of $\mathrm{Sign}(C, J)$ and this family is closed under finite intersections. Since $\bigcap_{i\in I} Y_i = V(M) \cap V(-a) = \varnothing$ and by Lemma 3.3, $\mathrm{Sign}(C, J)$ is compact, it follows that for some index $i_0$ the set $Y_{i_0}$ is empty. Thus, $V(a) \supset V(M_{i_0})$ which by the first part of the proof shows that $a$ is in $\hat{M}_{i_0} \subset \hat{M}$.

*Remark* 4.9. In the case $J$ is the identity and $A$ is a field, Theorem 4.8 is Satz 21 of [39] for $M$ finite, and for arbitrary $M$ is due to Witt (unpublished). Witt's proof is quite different from ours. He shows by a simple argument, valid only in fields (cf. [9, p. 35]) that for any proper saturated subset $M$ of $A^*$ and any element $a$ of $A^*$ not lying in $M$ the saturated set generated by $M$, and $-a$ is different from $A^*$. From this it follows that the maximal proper saturated subsets of $A^*$ are the $\Gamma(\sigma)$ with $\sigma$ running through the signatures (= orderings) of $A$. Then an application of Zorn's lemma yields the statement of Theorem 4.8.

EXAMPLES 4.10. (i) Assume that $J$ is tracique and let $M = \{1\}$. Then the units $a$ of $A$ with $\sigma(a) = 1$ for all $\sigma$ in $\mathrm{Sign}(C, J)$ are the sums of norms (cf. [3, Satz 1]). Furthermore, $\mathrm{Sign}(C, J) = \varnothing$ if and only if $-1$ is a sum of norms and in that case all units of $A$ are sums of norms.

(ii) Assume that $J$ is tracique and $\mathrm{Sign}(C, J) \neq \varnothing$. If $M$ is any proper saturated subset of $A^*$ then there is a signature $\sigma$ such that $M \subset \Gamma(\sigma)$. In particular, the maximal saturated proper subsets of $A^*$ are exactly the $\Gamma(\sigma)$ with $\sigma$ running through $\mathrm{Sign}(C, J)$.

(iii) Assume that $J$ is tracique and $A$ has the property that every unit which is a sum of norms is itself a norm. If $\mathrm{Sign}(C, J)$ is finite with $r \geqslant 0$ signatures then $A^*/NC^*$ is a finite group of order $2^n \leqslant 2^r$ with equality if and only if the conditions of Corollary 3.23 (ii) hold for $\mathrm{Sign}(C, J)$ (cf. [23, Corollary 5.7]).

(iv) Let $C'$ be a connected semilocal ring with tracique involution $J'$ and fixed ring $A'$. Let $C$ be a semilocal subring of $C'$ with $J'(C) = C$, let $J$ be the restriction of $J'$ to $C$, and let $A$ be the fixed ring of $J$. Then an element $\sigma$ in $\mathrm{Sign}(C, J)$ does *not* extend to an element $\sigma'$ in $\mathrm{Sign}(C', J')$ if and only if there are elements $a_1, \ldots, a_r$ in $A^*$ with $\sigma(a_1) = \cdots = \sigma(a_r) = 1$ and elements $c_1', \ldots, c_r'$ in $C'$ such that

$$-1 = N(c_1')\, a_1 + \cdots + N(c_r')\, a_r \tag{4.11}$$

(cf. [9, Theorem 1, p. 35]).

*Proof.* (i) and (ii) are immediate consequences of Theorem 4.8. For (iii) assume $J$ is tracique and $NC^* = \{a \text{ in } A^* \mid a \text{ is a sum of norms}\}$. Then, by (i), $\text{Sign}(C, J) = \varnothing$ if and only if $A^* = NC^*$ so we may assume $r \geqslant 1$. Let $\sigma_1, \ldots, \sigma_r$ be the distinct elements of $\text{Sign}(C, J)$. Then it is easy to see that the equivalent conditions of Corollary 3.23 (ii) hold for the $\sigma_i$ if and only if the natural map,

$$A^* \to \prod_{i=1}^{r} A^*/\Gamma(\sigma_i),$$

is surjective. Moreover, from the fact that the induced map,

$$A^*\Big/\bigcap_{i=1}^{r} \Gamma(\sigma_i) \to \prod_{i=1}^{r} A^*/\Gamma(\sigma_i),$$

is injective we note that

$$\left[A^*: \bigcap_{i=1}^{r} \Gamma(\sigma_i)\right] \leqslant 2^r,$$

with equality if and only if the conditions of Corollary 3.23 (ii) hold. By (i), $\bigcap_{i=1}^{r} \Gamma(\sigma_i) = \{a \text{ in } A^* \mid a \text{ is a sum of norms}\} = NC^*$ completing the proof.

(iv) It is easily verified that an element $\sigma'$ of $\text{Sign}(C', J')$ extends $\sigma$ if and only if $\sigma'(\Gamma(\sigma)) = 1$. Hence, applying Theorem 4.8 to the saturation $M'$ of $\Gamma(\sigma)$ with respect to $(C', J')$ we see that $\sigma$ does not extend to $(C', J')$ if and only if $M' = (A')^*$. Moreover, by Example 4.6 (ii), $M' = (A')^*$ if and only if $-1$ is in $M'$, i.e., if and only if (4.11) holds.

COROLLARY 4.12. *If $J$ is tracique and the sets $V(a)$, $a$ in $A^*$, form a basis for the open sets of* $\text{Sign}(C, J)$ (cf. *Theorem* 3.20) *then the correspondence $M \mapsto V(M)$ yields a lattice antiisomorphism between the family of saturated subsets of $A^*$ and the closed subsets of* $\text{Sign}(C, J)$.

*Proof.* By Theorem 4.8, $\hat{M} = \Gamma(V(M))$ for any subset $M$ of $A^*$ which shows that the correspondence is injective. On the other hand, if $Y$ is a closed subset of $\text{Sign}(C, J)$ the complement of $Y$ is open and, hence, is a union of sets $V(a)$ with $a$ in $A^*$. Therefore, $Y$ is the intersection of the complements of these sets which are again of the form $V(b)$, $b$ in $A^*$. Thus, there is a set $M$ in $A^*$ such that $Y = \bigcap_{b \in M} V(b) = V(M)$. Since $V(M) = V(\hat{M})$, the proof is complete.

In the last part of this section we study the torsion subgroup $W(C, J)_t$ and some other ideals of $W(C, J)$. It is easily checked that all the following results remain valid even if $C$ fails to be connected provided $W(C, J)$ is replaced by $WF(C, J)$, the Witt ring of free spaces.

PROPOSITION 4.13. (cf. [36, Satz 3; 43, Lemma 2.2.4, p. 49]). *If* $W(C, J)_t = 0$ *then any element* $a$ *in* $A^*$ *which is a sum of norms is itself a norm but* $-1$ *is not a norm.*

*Proof.* If $a$ in $A^*$ is a sum of norms it follows from Lemma 2.3 (ii) that $\sigma(a) = 1$ for all $\sigma$ in $\mathrm{Sign}(C, J)$. Hence, $[(1, -a)]$ lies in $W(C, J)_t = 0$. Thus, $[(a)] = [(1)]$, i.e., there exist metabolic spaces $(U_i, \Phi_i)$, $i = 1, 2$, over $(C, J)$ with

$$(a) \perp U_1 \cong (1) \perp U_2 . \tag{4.14}$$

Since $C$ is connected and semilocal the $U_i$ are free $C$-modules of equal rank $2m$, say. It is easily verified that the determinants of both spaces $(U_i, \Phi_i)$ are the norm class $(-1)^m NC^*$. Thus, taking determinants of both sides of (4.14), it follows that $a \equiv 1 \pmod{NC^*}$, i.e., $a$ is a norm. Furthermore, since $W(C, J)_t = 0$ it follows that $W(C, J) \neq W(C, J)_t$ so by Lemma 3.3, $\mathrm{Sign}(C, J) \neq \varnothing$. Hence, by Lemma 2.3, $-1$ is not a norm.

If $C$ is a field such that any sum of norms is a norm, but $-1$ is not a norm it can be shown as in [43, Lemma 2.2.4, p. 49] that if $(E, \Phi)$ is an anisotropic space over $(C, J)$ then so are $E \perp E$, $E \perp E \perp E$,..., which implies that $W(C, J)_t = 0$. However, for arbitrary semilocal rings with tracique involution it is not immediately clear how to obtain a converse to Proposition 4.13. After some preliminary work, we only fully treat the case that $J$ is the identity.

We introduce some notation. For any subset $Y$ of $\mathrm{Sign}(C, J)$ we denote by $I(Y)$ the ideal

$$\bigcap_{\sigma \text{ in } Y} P_\sigma = \{x \text{ in } W(C, J) \mid \bar{\sigma}(x) = 0 \text{ for all } \sigma \text{ in } Y\},$$

with the convention that if $Y = \varnothing$ then $I(Y) = \mathfrak{M}_0$, the unique prime ideal of $W(C, J)$ containing 2 [33, Example 3.11]. If $\mathfrak{a}$ is an ideal of $W(C, J)$, we write $\mathfrak{a}^{1/2}$ for the radical of $\mathfrak{a}$. For any subset $T$ of $W(C, J)$ we let $\mathrm{Ann}\, T = \{x \text{ in } W(C, J) \mid xT = 0\}$. If $M$ is a subset of $A^*$ we denote by $\mathfrak{a}(M)$ the ideal of $W(C, J)$ generated by $[(1, -a)]$ for all $a$ in $M$.

LEMMA 4.15. *For any subset* $M$ *of* $A^*$, $W(C, J)/\mathfrak{a}(M)$ *is a Witt ring for an Abelian group of exponent* 2 (cf. [33, Definition 3.12]).

*Proof.* Write $W(C, J) = \mathbb{Z}[G]/K$ with $G = A^*/NC^*$. Then $W(C, J)/\mathfrak{a}(M) = \mathbb{Z}[G]/K'$, where $K'$ is generated by $K$ and all elements $1 - \{a\}$ with $a$ in $M$ and $\{a\} = aNC^*$ in $\mathbb{Z}[G]$. For any ring homomorphism $\varphi$ from $\mathbb{Z}[G]$ to $\mathbb{Z}$, $\varphi(K)$ equals $2^n\mathbb{Z}$ for some $n > 0$, or 0 [33, Corollary 1.21] and $\varphi(1 - \{a\})$ equals 0 or 2. Thus, $\varphi(K')$ equals $2^m\mathbb{Z}$ for some $m > 0$, or 0 which means that $W(C, J)/\mathfrak{a}(M)$ is a Witt ring for $G$ [33, Definition 3.12].

COROLLARY 4.16. *For any subset $M$ of $A^*$, $(\mathfrak{a}(M))^{1/2} = I(V(M))$.*

*Proof.* Since $\bar{\sigma}([1, -a)]) = 0$ if and only if $\sigma(a) = 1$ it is clear that $\mathfrak{a}(M) \subset P_\sigma$ if and only if $\sigma$ lies in $V(M)$. Thus, by [33, Theorem 3.9 (v)], $(\mathfrak{a}(M))^{1/2} = I(V(M))$.

LEMMA 4.17. *For any subset $M$ of $A^*$ containing 1 and each integer $r_0 \geqslant 1$ we have*

$$(\mathfrak{a}(M))^{1/2} = \bigcup \operatorname{Ann}[(1, a_1) \otimes \cdots \otimes (1, a_r)],$$

*where the $a_i$ run through the elements of $M$ and $r$ runs through the integers $\geqslant r_0$.*

*Proof.* Let $\mathfrak{c}$ denote the right hand side. Then for an element $x$ in $\mathfrak{c}$ we have

$$x[(1, a_1)][(1, a_2)] \cdots [(1, a_r)] = 0,$$

for some $a_1, \ldots, a_r$ in $M$. Hence, for any $\sigma$ in $V(M)$ we obtain $2^r\bar{\sigma}(x) = 0$, i.e., $\bar{\sigma}(x) = 0$. Thus, $x$ lies in $I(V(M)) = (\mathfrak{a}(M))^{1/2}$. (If $V(M) = \varnothing$, $x$ lies in $\mathfrak{M}_0$ by [33, Theorem 3.9 (iv) and Example 3.11]). Hence, $\mathfrak{c} \subset (\mathfrak{a}(M))^{1/2}$.

Now let $x$ be an element of $(\mathfrak{a}(M))^{1/2}$. Since by Corollary 4.17 (i), $R = W(C, J)/\mathfrak{a}(M)$ is a Witt ring for an Abelian 2-group, the image of $x$ in $R$ is a torsion element [33, Proposition 3.15 and 3.16]. Hence, there is an integer $n$ with $2^n x$ lying in $\mathfrak{a}(M)$. Thus, we have

$$2^n x = \sum_1^r y_i[(1, -a_i)],$$

for $a_1, \ldots, a_r$ in $M$ and $r \geqslant 1$. Since $[(1, -a)][(1, a)] = 0$ in $W(C, J)$ it is clear that for all integers $m \geqslant n$

$$x[(1, 1)^m \otimes (1, a_1) \otimes \cdots \otimes (1, a_r)] = 0,$$

so that $x$ lies in $\mathfrak{c}$, which completes the proof of Lemma 4.17.

For the remainder of this section we only consider the case $J =$ identity, i.e., $C = A$.

THEOREM 4.18. *Assume 2 is a unit in $A$. Then for any subset $M$ of $A^*$*

$$(\mathfrak{a}(M))^{1/2} = \mathfrak{a}(\hat{M}).$$

*Proof.* Since $\hat{M}$ and $\mathfrak{a}(M)$ do not change is we adjoin 1 to $M$, we may assume 1 lies in $M$. Now by [29, Theorem 4.1] and Lemma 4.17, the ideal

$(\mathfrak{a}(M))^{1/2} = I(V(M))$ is generated by elements of the form $[(1, -a)]$. Clearly, $[(1, -a)]$ lies in $I(V(M))$ if and only if $\sigma(a) = 1$ for all $\sigma$ in $V(M)$, i.e., if and only if $a$ lies in $\Gamma(V(M))$ which equals $\hat{M}$ by Theorem 4.8. Thus, $(\mathfrak{a}(M))^{1/2} = \mathfrak{a}(\hat{M})$.

Taking $M = \{1\}$ in Theorem 3.18 we obtain the following.

COROLLARY 4.19. (cf. [39, Satz 22]). *Let $A$ be a connected semilocal ring with 2 a unit. If $W(A)_t \neq W(A)$ then $W(A)_t$ is generated by the elements $[(1, -a)]$ where $a$ is a sum of squares.*

Corollary 4.19 and Proposition 4.13 yield.

COROLLARY 4.20. *Let $A$ be a connected semilocal ring with 2 a unit. Then $W(A)$ is torsion free if and only if every unit which is a sum of squares is already a square but $-1$ is not a square.*

We conjecture that [29, Theorem 4.1] remains true for the annihilator of a multiplicative Hermitian space $E$ in $W(C, J)$ if $J$ is tracique and if $\dim E$ is not too small. This would imply that (4.18)–(4.20) can be extended to $W(C, J)$ if $J$ is tracique.

## 5. EXTENSIONS OF SIGNATURES

In this section, for the sake of simplicity we consider only semilocal rings $A$ with the identity involution. For a finite étale extension $B$ of such a ring $A$, i.e., $B$ is a finitely generated projective $A$-module and a projective $B \otimes_A B$-module [24, Proposition 18.3.1, p. 114] we want to study the signatures $\tau\colon B^* \to \{\pm 1\}$ extending a given signature $\sigma\colon A^* \to \{\pm 1\}$. It should be noted that a finite extension of a semilocal ring is again semilocal.

We begin by considering a commutative Frobenius extension $B$ of $A$, i.e., $B$ is a finitely generated projective $A$-module and there exists an $A$-linear form $s\colon B \to A$ such that the $A$-bilinear form $(b_1, b_2) \mapsto s(b_1 b_2)$ on $B$ is nondegenerate [22]. Indeed, for $B/A$ finite étale the trace $\mathrm{Tr}_{B/A}$ [5, p. 397; 19, p. 91 ff.] has this property.

Any $A$-linear form $s$ making $B/A$ Frobenius yields a homomorphism of additive groups,

$$s_*\colon W(B) \to W(A),$$

mapping the class of a $B$-space $(E, \Phi)$ to the class $[(E, s \circ \Phi)]$ of $E$ considered as an $A$-module carrying the nondegenerate form $s \circ \Phi\colon E \times E \xrightarrow{\Phi} B \xrightarrow{s} A$ [21, Lemma 2.2].

Before considering extensions of signatures we make some simple and well

known remarks about this transfer map. It is easily proved that $s_*$ is $W(A)$-linear

$$xs_*(y) = s_*(r(x)y) \tag{5.1}$$

for $x$ in $W(A)$, $y$ in $W(B)$, with $r$ denoting the canonical map from $W(A)$ to $W(B)$ [44]. If $s'\colon B \to A$ is another $A$-linear form such that the bilinear form $s'(b_1b_2)$ is nondegenerate, then the nondegeneracy of $s$ shows that there is an element $u$ in $B$ with $s'(b) = s(ub)$ for all $b$ in $B$. The fact that $s'(b_1b_2)$ is also a nondegenerate bilinear form forces $u$ to be a unit in $B$. Since a $B$-space $(E, \Phi)$ is nondegenerate if and only if $(E, u\Phi)$ is, we have $\operatorname{Im} s_* = \operatorname{Im} s_*'$. This image, which by (5.1) is an ideal of $W(A)$, will be denoted by $I(B, A)$, while the kernel of $r\colon W(A) \to W(B)$ will be written as $K(A, B)$. Again from (5.1) we obtain

$$I(A, B)\, K(A, B) = 0. \tag{5.2}$$

Now let $\sigma$ be in Sign $A$. As usual we write $\bar{\sigma}$ for the corresponding ring homomorphism from $W(A)$ to $\mathbb{Z}$ (cf. the end of Section 2). The signatures $\tau\colon B^* \to \{\pm 1\}$ extending $\sigma$ correspond bijectively with the homomorphisms $\bar{\tau}\colon W(B) \to \mathbb{Z}$ such that $\bar{\tau} \circ r = \bar{\sigma}$ (cf. Definition 2.9).

LEMMA 5.3. *Let $B/A$ be Frobenius. Then a signature $\sigma$ of $A$ can be extended to $B$ if and only if $\bar{\sigma}(K(A, B)) = 0$. In particular this is the case if $\bar{\sigma}(I(A, B)) \neq 0$.*

*Proof.* The considerations at the end of Section 2 show that Lemma 2.10 is still valid in the nonconnected case. Hence, the first assertion is just a special case of this lemma. The second one follows from (5.2).

PROPOSITION 5.4. *Let $B/A$ be a Frobenius extension. Assume that for all maximal ideals $\mathfrak{m}$ of $A$, the free $A_{\mathfrak{m}}$-module $B_{\mathfrak{m}}$ has odd rank. Then*

(i) $K(A, B) = 0$.

(ii) *Every signature of $A$ extends to one of $B$.*

*Proof.* The element $s_*(1)$ of $I(B, A)$ is represented by an $A$-space whose underlying module is $B$. By [33, Lemma 1.9], $W(A) = \prod W(A_i)$ where the rings $A_i$ are the connected components of $A$. The components $x_i$ of $s_*(1)$ in $W(A_i)$ are represented by free $A_i$-modules of odd rank since the rank of a projective module is constant on the connected components. Thus, by [33, Example 3.11], the $x_i$'s are not zero divisors in $W(A_i)$, and, consequently, $s_*(1)$ is not a zero divisor in $W(A)$. Then by (5.2), $K(A, B) = 0$ which, in view of Lemma 5.3, completes the proof.

The next proposition generalizes [9, Proposition 3, p. 36].

PROPOSITION 5.5. *Let $f(x)$ be a monic polynomial in $A[x]$ and let $B = A[x]/(f(x))$.*

(i) *If there is an element $c$ in $A$ with $f(c)$ in $A^*$, then $B$ is a Frobenius extension of $A$.*

(ii) *Let $\sigma$ be in* Sign *$A$. If there exists an element $c$ as in* (i) *with $\sigma(f(c)) = -1$, then $\sigma$ extends to a signature of $B$.*

*Proof.* By replacing $x$ by $x - c$ we may suppose $c = 0$. Thus, $f(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0$, with $a_0$ a unit in $A$. Then the $A$-algebra $B$ has a basis $\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}$ and a multiplication table given by

$$\bar{x}^n = a_{n-1}\bar{x}^{n-1} + \cdots + a_0\bar{1}.$$

Following [44] we define $s$ in $\hom_A(B, A)$ by $s(\bar{x}^i) = \delta_{0i}$. Then $s_*(1)$ is the class of the $A$-module $B$ with form $s(b_1b_2)$. Clearly $\sum_1^{n-1\oplus} A\bar{x}_i = (A\bar{1})^\perp$ and, since with respect to this basis of $(A\bar{1})^\perp$ the form has a matrix of determinant $a_0^{n-1}$, the spaces $(A\bar{1})^\perp$ and $s_*(1)$ are nondegenerate, proving (i).

Now, if $n$ is even, $n = 2k + 2$ say, $s(\bar{x}^{k+1}\bar{x}^{k+1}) = a_0$ so that by [33, Lemma 1.1] $A(\bar{1})^\perp = (A\bar{x}^{k+1}) \perp (A\bar{x}^{k+1})^\perp$. But $M = \sum_1^k A\bar{x}_i$ is clearly a direct summand of $(A\bar{x}^{k+1})^\perp$ such that $M^\perp = M$ so that $(A\bar{x}^{k+1})^\perp$ is metabolic. Hence, $s_*(1)$ is also the class of the space $A\bar{1} \perp A\bar{x}^{k+1}$, i.e., $s_*(1) = [(1, a_0)]$. Since by hypothesis $\sigma(a_0) = 1$, we have $\bar{\sigma}(s_*(1)) = 2$ and so by Lemma 5.3, $\bar{\sigma}$ extends to a signature of $B$. If $n = 2k + 1$, the result follows from Proposition 5.4 or can be proved directly as in the case of even $n$ since $(A\bar{1})^\perp$ is then metabolic.

*Remark* 5.6. If $B/A$ is a finite étale extension, $B$ has the form given in Proposition 5.5 if either $A$ is local with infinite residue class field or $B$ itself is local [24, 18.4.5, p. 119].

We shall obtain a better insight into the extension problem of signatures if $B/A$ is a finite Galois extension as defined in [5; 15]. Note that by [15, Theorem 1.3] a Galois extension is always finite étale. We first need the following lemma.

LEMMA 5.7. *Let $B/A$ be a Galois extension with group $G$ and $g \neq 1$ an element of $G$. Assume that no residue class field of $B$ contains only two elements. Then there is an element $b$ in $B$ such that $g(b) - b$ is a unit.*

*Proof.* Let $A'$ be the fixed ring of $g$. Since $A' \supset A$, the ring $B$ is a finitely generated $A'$-module. Thus, since $B$ is semilocal $A'$ is also. By [15, Theorem 2.2] $B/A'$ is a Galois extension with group generated by $g$. Thus, it suffices to prove the lemma in case $B$ is a Galois extension of $A$ with finite cyclic Galois group.

We first consider the case that $A$ is a field. Then $B = \prod_1^k F_i$, where the $F_i$'s are isomorphic extension of $A$ and $G$ permutes the factors transitively [17, Lemmas 5.2 and 5.6; 46]. Thus, we may write $B = \prod_0^{k-1} g^i(F)$ with $g^k(F) = F$. Of course, $k$ need not be the order of $G$. If $k = 2k'$ is even the element

$$b = (0, g(1), 0, g^3(1), \ldots, 0, g^{2k'-1}(1))$$

will do. If $k = 1$, the field $B$ is a Galois extension of $A$ and so for each element $b$ in $B$ not in $A$, we have that $g(b) - b \neq 0$ is a unit. If $k = 2k' + 1$ with $k' \geqslant 1$, let $c$ be an element in $F$ differing from 0 or 1, then

$$b = (0, g(1), 0, g^3(1), \ldots, g^{2k'-1}(1), g^{2k'}(c))$$

will do.

To treat the general case we first note that if $\mathfrak{m}$ is a maximal ideal of $A$, the ring $B/\mathfrak{m}B$ is a Galois extension of $A/\mathfrak{m}$ with group $G$ [15, Lemma 1.7]. Since the ideals $\mathfrak{m}B$ are comaximal, the Chinese Remainder Theorem shows that $B/(\bigcap \mathfrak{m}B) \cong \prod B/\mathfrak{m}B$. By the first part of the proof there is an element $\bar{b}$ in $B/\bigcap \mathfrak{m}B$ with $g(\bar{b}) - \bar{b}$ a unit. Since $B/\mathfrak{m}B$ is a semisimple algebra, it is clear that $\bigcap \mathfrak{m}B = \mathrm{Rad}(B)$. Thus, for $b$ in $B$ with image $\bar{b}$, the element $g(b) - b$ is a unit.

*Remark.* Let $B/A$ be a finite étale extension with $B$ connected and $g \neq 1$ an automorphism of $B$ which is the identity on $A$. If no residue class field of $B$ contains only two elements, the conclusion of Lemma 5.7 still holds. Indeed, by [15, Theorem 3.5] $B$ is then Galois over the fixed ring of $g$.

PROPOSITION 5.8. *Assume $B/A$ is Galois with group $G$ and that no residue class field of $B$ contains only two elements. Then for any element $g \neq 1$ of $G$ and any signature $\tau$: $B^* \to \{\pm 1\}$ the map $\tau g$: $B^* \to \{\pm 1\}$ is a signature of $B$ distinct from $\tau$.*

*Proof.* From Definition 2.1, it is clear that $\tau g$ is in Sign $B$. The automorphism $g$ has finite order $n$, say, and by Lemma 5.7 there is an element $b$ in $B$ with $g(b) - b$ in $B^*$. Replacing $b$ by $-b$ if necessary, we may assume that $\tau(g(b) - b) = 1$. Now

$$g^{n-1}(b) - b = (g^{n-1}(b) - g^{n-2}(b)) + (g^{n-2}(b) - g^{n-3}(b)) + \cdots + (g(b) - b).$$

If $\tau g = \tau$, then $\tau g^k = \tau$ and so $(\tau g^{k-1})(g(b) - b) = \tau(g^k(b) - g^{k-1}(b)) = 1$ for all $k$. On the other hand, $g(g^{n-1}(b) - b) = b - g(b)$, whence $\tau(g^{n-1}(b) - b) = -1$. This is impossible by Lemma 2.3.

We continue to assume that $B/A$ is a Galois extension with group $G$. Any $g$ in $G$ is an automorphism of the pair $(B, Id)$ and, hence, induces an auto-

morphism of $W(B)$. Thus, $G$ operates on $W(B)$. If an element $x$ of $W(B)$ is represented by the space $(M, \Phi)$ then $gx$ is represented by $(B \otimes_g M, B \otimes_g \Phi)$. Here $B \otimes_g M$ and $B \otimes_g \Phi$ denote the $B$ module and bilinear form obtained from $M$ and $\Phi$ by base extension with $B \xrightarrow{g} B$, i.e.,

$$b_1 \otimes_g b_2 m = b_1 g(b_2) \otimes_g m \quad \text{and} \quad \Phi(b_1 \otimes m_1, b_2 \otimes m_2) = b_1 b_2 g(\Phi(m_1, m_2))$$

(cf. [9, p. 14]). If $M$ is a free $B$-module and $\Phi$ has matrix $(b_{ij})$ with respect to a basis $m_1, \ldots, m_n$ of $M$, then $B \otimes_g \Phi$ has matrix $(g(b_{ij}))$ with respect to the basis $1 \otimes_g m_1, \ldots, 1 \otimes_g m_n$ of $B \otimes_g M$ (cf. [41]).

This action of $G$ on $W(B)$ induces an action of $G$ on the set $X$ of prime ideals $P$ of $W(B)$ with $W(B)/P = \mathbb{Z}$. As usual, we consider $X$ as a right $G$-set via

$$Pg = g^{-1}(P).$$

On the other hand, $G$ operates from the right on the set Sign $B$ via

$$(\tau g)(b) = \tau(g(b))$$

for $\tau$ in Sign $B$ and $b$ in $B^*$. As described in Corollary 2.17 there is a canonical bijection Sign $B \rightarrowtail X$. It is easily verified that this is an isomorphism of right $G$-sets. If no residue class field of $B$ contains only two elements, Proposition 5.8 shows that any element $g \neq 1$ of $G$ operates on Sign $B$ and, hence, on $X$ without fixed points. In particular if $X \neq \varnothing$, no $g \neq 1$ operates on $W(B)$ as the identity. This is not always true if $X = \varnothing$, as the example $A = \mathbb{R}$, $B = \mathbb{C}$ shows.

LEMMA 5.9. *Let $B/A$ be a Galois extension with group $G$ and denote the trace map* $\mathrm{Tr}_{B/A}$ *by* Tr. *Then for any $z$ in $W(B)$*

$$r(\mathrm{Tr}_*(z)) = \sum_{g \text{ in } G} g(z)$$

(cf. [35, *Satz* 1.5]).

*Proof.* By [15, Theorem 1.31(e)] the map $B \otimes_A B \to \coprod_{g \text{ in } G} B$ given by $b_1 \otimes_A b_2 \to \coprod b_1 g(b_2)$ is an isomorphism of rings. Since $b_1 \otimes_g b_2 \to b_1 g(b_2)$ yields an isomorphism of $B \otimes_g B$ with $B$ as Abelian groups, the map $\theta\colon B \otimes_A B \to \coprod_{g \text{ in } G} B \otimes_g B$ given by $\theta(b_1 \otimes_A b_2) = \coprod b_1 \otimes_g b_2$ is a bijection and is readily verified to be an isomorphism of two-sided $B$-modules. Therefore, if $M$ is any left $B$-module the composite map,

$$\lambda\colon B \otimes_A M \to (B \otimes_A B) \otimes_B M \xrightarrow{\theta \otimes 1} \coprod_{g \text{ in } G} (B \otimes_g B) \otimes_B M \to \coprod_{g \text{ in } G} B \otimes_g M,$$

is an isomorphism of left $B$-modules; explicitly, $\lambda(b \otimes_A m) = \coprod_{g \text{ in } G} (b \otimes_g m)$ for $b$ in $B$, $m$ in $M$.

Now let $(M, \Phi)$ be a $B$-space. By [5, Proposition A.3] $\mathrm{Tr}(b) = \sum_{\sigma \in G} g(b)$ for all $b$ in $B$. Hence, it is readily verified that $\lambda$ is an isometry of $(B \otimes_A M, B \otimes_A \mathrm{Tr} \circ \Phi)$ with $\perp_{\sigma \in G} (B \otimes_\sigma M, B \otimes_\sigma \Phi)$. Let $z$ in $W(B)$ be represented by $(M, \Phi)$. The fact that $\lambda$ is an isometry asserts $r(\mathrm{Tr}_*(z)) = \sum_{\sigma \in G} g(z)$.

For any Galois extension $B/A$ with group $G$, the $A$-module $B$ is free of rank $[G : 1]$ [15, Theorem 4.2(c)]. We denote this rank by $[B : A]$. Then Lemma 5.9 implies the following corollary.

COROLLARY 5.10. *As usual let $W(B)^G$ denote the fixed ring of $G$ in $W(B)$. For any $z$ in $W(B)^G$*

$$r(\mathrm{Tr}_*(z)) = [B : A]z.$$

*Hence,* $\mathrm{Coker}(r: W(A) \to W(B)^G)$ *and* $\ker(\mathrm{Tr}_*: W(B)^G \to W(A))$ *are annihilated by* $[B : A]$.

*Remark.* The proofs of Lemma 5.9 and Corollary 5.10 remain valid for a Galois extension $B/A$ of an arbitrary commutative ring $A$. Indeed, the $A$-module $B$ is also projective of constant rank $[G : 1]$ [15, Lemma 4.1]. This rank is also denoted by $[B : A]$.

PROPOSITION 5.11. *Let $B/A$ be a Galois extension and $[B : A]_2$ be the highest power of 2 dividing $[B : A]$. Then*

(i) $[B : A]_2(\ker(\mathrm{Tr}_*: W(B)^G \to W(A))) = 0.$

(ii) $[B : A]_2(\mathrm{Coker}(r: W(A) \to W(B)^G)) = 0.$

(iii) *If $[B : A]$ is odd, $r: W(A) \to W(B)^G$ is an isomorphism.*

*Proof.* By [33, Lemma 1.9 and Example 3.11], the torsion subgroup of $W(B)$ is 2-primary, which in view of Corollary 5.10 proves (i). For an odd prime $p$ the ring $W(A)/pW(A)$, and, therefore, its homomorphic image $r(W(A))/p \cdot r(W(A))$ is von Neumann regular [33, Lemma 1.9 and Example 2.6 (ii)]. Since $W(B)^G$ has zero $p$-torsion, [33, Lemma 2.8] shows that $W(B)^G/r(W(A))$ also has zero $p$-torsion proving (ii). Statement (iii) is immediate from (ii) and Proposition 5.4.

*Remark.* Proposition 5.11 (iii) was first proved for $A$ and $B$ fields in [41]. Essentially the present proof is contained in [33, Remark 2.11] and a slightly different version can be found in [35].

PROPOSITION 5.12. *Let $B/A$ be a Galois extension with group $G$ and assume that no residue class field of $B$ contains only two elements. For $\sigma$ in* Sign $A$ *we write $\tau \mid \sigma$ if $\tau$ is an element of* Sign $B$ *extending $\sigma$.*

(i) *Let $T$ be the set of signatures of $B$ extending a given signature $\sigma$ of $A$. If $T \neq \varnothing$, the group $G$ acts faithfully and transitively on $T$. Hence, $T = \varnothing$ or has $[B : A]$ elements.*

(ii) *For $z$ in $W(B)$ we have $\bar{\sigma}(\mathrm{Tr}_*(z)) = \sum_{\tau|\sigma} \bar{\tau}(z)$, with the empty sum being 0.*

(iii) Card $T = \bar{\sigma}(\mathrm{Tr}_*(1))$.

*Proof.* (i) By Corollary 2.17 the correspondence $\tau \mapsto P_\tau = \ker \bar{\tau}$ defines a bijection of Sign $B$ with the set of prime ideals $P$ of $W(B)$ such that $W(B)/P$ is not a torsion group. Thus, $\tau \mapsto \mathbb{Q} \otimes P_\tau$ is a bijection from Sign $B$ to $\mathrm{Spec}(\mathbb{Q} \otimes W(B))$ (cf. Lemma 3.3 (iii)). Clearly, $\tau \mid \sigma$ if and only if $\mathbb{Q} \otimes P_\tau$ lies over $\mathbb{Q} \otimes P_\sigma$ with respect to $1 \otimes r: \mathbb{Q} \otimes W(A) \to \mathbb{Q} \otimes W(B)$.

As usual for $g$ in $G$, $q$ in $\mathbb{Q}$, and $z$ in $W(B)$, we set $g(q \otimes z) = q \otimes g(z)$. Then $G$ operates on $\mathbb{Q} \otimes W(B)$ from the left and, hence, from the right on $\mathrm{Spec}(\mathbb{Q} \otimes W(B))$. The considerations before Lemma 5.9 show that Sign $B \to \mathrm{Spec}(\mathbb{Q} \otimes W(B))$ is an isomorphism of $G$ sets.

Let $v$ be an element of $(\mathbb{Q} \otimes W(B))^G$. Then by Lemma 5.9

$$v = (1 \otimes r)(1 \otimes \mathrm{Tr}_*)[B : A]^{-1}$$

so that $v$ lies in $\mathbb{Q} \otimes r(W(A))$. Since $\mathbb{Q} \otimes r(W(A))$ clearly is contained in $(\mathbb{Q} \otimes W(B))^G$, we have $(\mathbb{Q} \otimes W(B))^G = \mathbb{Q} \otimes r(W(A))$. Hence, [12, Theorem 2, p. 42] shows that $G$ operates transitively on the $\mathbb{Q} \otimes P_\tau$ for $\tau \mid \sigma$, i.e., $G$ operates transitively on $T$. That $G$ operates faithfully on $T$ is a consequence of Proposition 5.8.

(ii) Assume first that $\sigma$ has at least one extension $\tau_0$. By Lemma 5.9 we have $r(\mathrm{Tr}_*(z)) = \sum g(z)$. Thus,

$$\bar{\sigma}(\mathrm{Tr}_*(z)) = \bar{\tau}_0(r(\mathrm{Tr}_*(z))) = \sum_{g \,\mathrm{in}\, G} \tau_0(g(z)) = \sum_{\tau|\sigma} \tau(z), \quad \text{by (i).}$$

If $\sigma$ does not extend to $B$, then by Lemma 5.3, $\bar{\sigma}(\mathrm{Tr}_*(z)) = 0$.

(iii) This is assertion (ii) for $z = 1$.

As an application of Proposition 5.12 we treat the case $[B : A] = 2$. We first determine the structure of such extensions explicitly.

LEMMA 5.13. (i) *Let $A$ be an arbitrary commutative ring and let $B/A$ be a free étale extension of rank 2. Then $B \cong A[x]/(x^2 - dx - c)$ with $d^2 + 4c$ a unit in $A$. Conversely, any such algebra is a free étale extension of $A$ of rank 2.*

(ii) *If $A$ is semilocal, then $d$ in* (i) *can be chosen as* 1.

*Proof.* By [11, Exercise 4, p. 176] the natural map $A \to B$ splits. By the usual exterior power argument there is an element $t$ in $B$ such that $\{1, t\}$ is a

basis of $B$ over $A$. If $t^2 = c + dt$ with $c$, $d$ in $A$, it is clear that $B \cong A[x]/(x^2 - dx - c)$. By [19, Theorem 4.4, p. 111], $B$ is étale if and only if

$$\begin{vmatrix} \mathrm{Tr}_{B/A}(1) & \mathrm{Tr}_{B/A}(t) \\ \mathrm{Tr}_{B/A}(t) & \mathrm{Tr}_{B/A}(t^2) \end{vmatrix}$$

is a unit in $A$. A routine computation shows that this determinant is $d^2 + 4c$, proving (i).

(ii) If $\{1, t'\}$ is another $A$-basis of $B$ we have $t' = a_0 + a_1 t$ with $a_1$ in $A^*$ and $t'^2 = c' + d't'$ where $d' = 2a_0 + a_1 d$. Thus, to prove (ii) it suffices to show that

$$2x + yd = 1 \tag{5.14}$$

has a solution in $A$ with $y$ a unit. Now, it is readily verified that if $A$ is a field (5.14) has a solution with $y \neq 0$. Hence, (5.14) has a solution in any finite direct product of fields with $y$ a unit. Thus, if $A$ is semilocal (5.14) has a solution mod Rad $A$ with $y$ a unit. But then clearly (5.14) has a desired solution in $A$.

From now on $A$ again denotes a semilocal ring.

PROPOSITION 5.15. *Let $B/A$ be a free étale extension of rank two. Thus, by Lemma* 5.13 (ii) $B \cong A[x]/(x^2 - x - c)$ *with* $1 + 4c$ *in* $A^*$. *If no residue class field of $B$ has only two elements, an element $\sigma$ in* Sign $A$ *extends to $B$ if and only if* $\sigma(1 + 4c) = 1$.

*Proof.* Any element $b$ of $B$ can be uniquely written as $a_0 + a_1 t$ with $a_0$, $a_1$ in $A$ and $t^2 = t + c$. Define $g: B \to B$ by $g(a_0 + a_1 t) = (a_0 + a_1) - a_1 t$. It is readily verified that $g$ is an $A$-automorphism of $B$ of period two. Moreover, $g(t) - t = 1 - 2t$ and $(1 - 2t)^2 = 1 + 4c$, so that $1 - 2\bar{x}$ is in $B^*$. By [15, Theorem 1.3 (f)], the extension $B/A$ is Galois with group $G = \{1, g\}$. Thus, by Proposition 5.12 (ii) it suffices to prove

$$\bar{\sigma}(\mathrm{Tr}_*(1)) = 1 + \sigma(1 + 4c).$$

Now $\mathrm{Tr}_*(1)$ is represented by the $A$-module $B$ varrying the form $\Phi$ whose matrix with respect to the basis $\{1, t\}$ is $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1+2c \end{smallmatrix}\right)$. By [33, Lemma 1.12], $(B, \Phi) \perp (-1)$ is isometric to a diagonal form $(a_1, a_2, a_3)$ with $a_i$ in $A$, so that $\bar{\sigma}(\mathrm{Tr}_*(1)) - 1 = \sigma(a_1) + \sigma(a_2) + \sigma(a_3)$. Taking determinants of both forms and applying $\sigma$ we find

$$-\sigma(1 + 4c) = \sigma(a_1)\,\sigma(a_2)\,\sigma(a_3).$$

On the other hand, it is clear that $(B, \Phi) \perp (-1)$ represents both $+1$ and $-1$. It follows from Lemma 2.3 (ii) that we cannot have $\sigma(a_i) = 1$, $i = 1, 2, 3$ or $\sigma(a_i) = -1$, $i = 1, 2, 3$. Thus, the values of the $\sigma(a_i)$ will include either two $+1$'s or one $+1$. In the former case $\sigma(a_1)\,\sigma(a_2)\,\sigma(a_3) = -1$ and

$\sigma(a_1) + \sigma(a_2) + \sigma(a_3) = 1$, while in the latter $\sigma(a_1)\,\sigma(a_2)\,\sigma(a_3) = 1$ and $\sigma(a_1) + \sigma(a_2) + \sigma(a_3) = -1$. In both cases, $\bar{\sigma}(\mathrm{Tr}_*(1)) = 1 + \sigma(1 + 4c)$, proving the proposition.

We have not been able to generalize Proposition 5.12 to arbitrary finite étale extensions. However, we make the following conjecture.

CONJECTURE 5.16.[4] *Let $B|A$ be a finite étale extension and assume that no residue class field of $B$ contains only two elements. Then for any $z$ in $W(B)$*

$$\bar{\sigma}(\mathrm{Tr}_*(z)) = \sum_{\tau|\sigma} \bar{\tau}(z).$$

The conjecture is known to hold if $A$ is a field [30, Section 5]. For $z = 1$ the conjecture asserts that $\sigma$ has exactly $\bar{\sigma}(\mathrm{Tr}_*(1))$ extensions to $B$. By [19, Corollary 2.3, p. 94] the form $\mathrm{Tr}: B \times B \to A$ is proper and so, if $B$ is a free $A$-module, it has an orthogonal basis [33, Lemma 1.12]. Hence, $\bar{\sigma}(\mathrm{Tr}_*(1)) = [B : A] - 2k$ for some natural number $k$. Thus, if Conjecture 5.16 holds there can be at most $[B : A]$ extensions of $\sigma$ and the number of extensions differs from $[B : A]$ by an even integer. Further evidence for the truth of conjecture 5.16 is given by the following proposition.

PROPOSITION 5.17. *Let $B|A$ be a finite étale extension. For any $\sigma$ in* Sign $A$ *we have $\bar{\sigma}(\mathrm{Tr}_*(1)) \geqslant 0$, and $\sigma$ extends to $B$ if and only if $\bar{\sigma}(\mathrm{Tr}_*(1)) > 0$.*

This proposition can be proved essentially in the same way as in the special case when $A$ and $B$ are fields [30, Lemma 4.1].

A special case of our final result was already announced in [35, Bemerkung 1.3]. We begin with a topological lemma and refer to Section 3 for the terminology.

LEMMA 5.18. (i) *Let $Y$ be a Boolean space and $G$ a finite group of fixed point free homeomorphisms of $Y$. Then there is a clopen fundamental domain $\Omega$ for $G$ in $Y$.*

(ii) *Let $X = Y/G$ and for any discrete ring $D$, denote $C(X, D)$ by $R$ and $C(Y, D)$ by $S$. We identify $R$ with the subring of $S$ consisting of the functions constant on the orbits of $G$. By letting $(gf)(y) = f(g^{-1}y)$ we obtain an action of $G$ as a group of $R$-automorphisms of $S$. Let $e_g$ in $S$ be the characteristic function of $g(\Omega)$ for $g$ in $G$. Then $S = \sum R\, e_g$, the $e_g$ are orthogonal idempotents of $S$, the $R$-modules $R\, e_g$ are free of rank one, and $g'(e_g) = e_{g'g}$. Thus, $S$ is ring isomorphic to a direct product of $[G : 1]$ copies of $R$ and the map $\sum_g r_g g \mapsto \sum_g r_g e_g$ from the group ring $R[G]$ of $G$ over $R$ to $S$ is an isomorphism of left $R[G]$-modules.*

[4] *Note added in proof.* We now know that this conjecture holds true even without any assumption about the residue class fields of $B$ (cf. *Bull. Amer. Math. Soc.* **79** (1973), 79).

*Proof.* (i) It is easily verified that the canonical projection $\pi: Y \to Y/G$ possesses a continuous cross section $\theta$ [37, Proposition 3.1]. Let $\Omega = \operatorname{Im}\theta$. Since $\theta\pi$ is the identity of $\Omega$, it is clear that $\Omega$ is a fundamental domain for $G$ so that $Y$ is a finite disjoint union of the sets $g(\Omega)$ for $g$ in $G$. Since $Y/G$ is compact, $\Omega$ is also, and, thus, since $Y$ is Hausdorff, $\Omega$ is a closed subset of $Y$. Hence, $Y - \Omega$ is also closed so that $\Omega$ is clopen.

(ii) Since $G$ is finite, it is well known that $\pi$ is both open and closed. Hence, $\pi \mid g(\Omega)$ is a homeomorphism of $g(\Omega)$ onto $X$. Denote its inverse by $\varphi_g$. For $s$ in $S$ let $r_g(s) = s \circ \varphi_g \circ \pi$. Clearly $r_g(s)$ is a continuous function from $Y$ to $D$ constant on the orbits of $G$ and so lies in $R$. Moreover, for any $y$ in $Y$ there is a unique $h$ in $G$ with $h(\Omega)$ containing $y$. Then for an element $s$ in $S$, we have $s(y) = r_h(s)(y)\, e_h(y)$, so that $s(y) = \sum_{g \text{ in } G} r_g(s)\, e_g(y)$, i.e., $s = \sum_{g \text{ in } G} r_g(s)\, e_g$. If $re_g = 0$ for some $r$ in $R$, then $r(g(\Omega)) = 0$, and since $r$ is constant on the orbits of $G$, this forces $r = 0$. Thus, since the $e_g$ are clearly orthogonal, $S = \prod R e_g$. It is clear that $R \subset S^G$ and easily verified that $g'(e_g) = e_{g'g}$. Thus, the last assertion of Lemma 5.18 is also evident.

PROPOSITION 5.19. *Let $B/A$ be a galois extension with group $G$ and assume that no residue class field of $B$ contains only two elements. Let $\widetilde{W(A)} = r(W(A))$, the image of $W(A)$ in $W(B)$. Then $2^{-\infty}W(B)$ is a free module of rank one over the group ring $2^{-\infty}\widetilde{W(A)}[G]$.*

*Proof.* Let $Y = \operatorname{Sign} B$. By Lemma 2.15 we have $2^{-\infty}W(B) = 2^{-\infty}WF(B)$ and, as stated just before Definition 3.1, $WF(B)$ is a Witt ring for some group of exponent 2 in the sense of [33]. Thus, from Lemma 3.15 and Theorem 3.18 (i) we obtain $2^{-\infty}W(B) = 2^{-\infty}W(B)_{\text{red}} \cong C(Y, 2^{-\infty}\mathbb{Z})$. Furthermore, by Proposition 5.11 (ii) we have $[2^{-\infty}W(B)]^G = 2^{-\infty}\widetilde{W(A)}$. Since $G$ consists of automorphisms of $B$, it induces homeomorphisms on the space of minimal ideals of $W(B)$ and so on $Y$. By Proposition 5.8 any element $g \neq 1$ of $G$ induces a homeomorphism without fixed points. Let $X = Y/G$. If we define an action of $G$ as automorphism of $C(Y, 2^{-\infty}\mathbb{Z})$ as in Lemma 5.18 (ii), it is easily verified that $C(Y, 2^{-\infty}\mathbb{Z}) \cong 2^{-\infty}W(B)$ is a $G$-isomorphism also. Hence, $C(X, 2^{-\infty}\mathbb{Z}) \cong C(Y, 2^{-\infty}\mathbb{Z})^G \cong 2^{-\infty}\widetilde{W(A)}$ and Lemma 5.18 (ii) completes the proof.

COROLLARY 5.20. *As in Proposition 5.11 let $[B : A]_2$ denote the highest power of 2 dividing $[B : A]$. Then $[B : A]_2(\hat{H}^i(G, W(B)) = 0, -\infty < i < \infty$, where $\hat{H}^i(G,...)$ denote the Tate cohomology groups of $G$.*

*Proof.* Since $2^{-\infty}\mathbb{Z}$ is flat over $\mathbb{Z}$, we have $2^{-\infty}\hat{H}^i(G, W(B)) \cong \hat{H}^i(G, 2^{-\infty}W(B))$ [14, Theorem 3.3, p. 113]. Thus, by Proposition 5.19 we have $2^{-\infty}\hat{H}^i(G, W(B)) = 0$, i.e., all the $\hat{H}^i(G, W(B))$ are 2-torsion groups. Now,

since $G$ is finite of order $[B : A]$, we have $[B : A]\,\hat{H}^i(G, W(B)) = 0$ [14, Proposition 2.5, p. 236] so that $[B : A]_2\hat{H}^i(G, W(B)) = 0$.

*Remark.* If $A$ is a field, Dress [31] proves the following generalization of Corollary 5.20: Let $B/A$ be an arbitrary finite étale extension of $A$ and $E$ a finite Galois field extension of $A$ with the property that all the fields which are the simple components of $B$ have $A$-isomorphism into $E$. Let $H^i(B/A, W)$, $i = 0, 1, 2,...$, denote the Amitsur cohomology groups of $B/A$ with coefficients in the Witt ring functor [16, Section 3] and write $\hat{H}^i(B/A, W)$ for $H^i(B/A, W)$, $i > 0$, and $\hat{H}^0(B/A, W)$ for $\mathrm{Coker}(W(A) \to H^0(B/A, W))$. Then

$$[E : A]_2\hat{H}^i(B/A, W) = 0, \qquad i = 0, 1, 2,...$$

[21, Corollary 2.3 and p. A.26]. It should be noted that in [21] the usual indexing of the Amitsur cohomology groups is shifted by one. Furthermore, if $A$ is an arbitrary commutative ring and $B \cong A[x]/(f(x))$, where $f(x)$ is a monic polynomial of odd degree [21, Corollary 2.3 and Lemma 2.3] shows that $\hat{H}^i(B/A, W) = 0$, $i = 0, 1, 2,...$ .

## 6. Proof of Proposition 2.5

In this section $C$ always denotes a connected semilocal ring with involution $J : \gamma \to \bar{\gamma}$ and $A$ the fixed ring of $J$. We shall consistently use Roman letters for elements of $A$ and Greek letters for elements of $C$.

Lemma 6.1. *Assume that either $A$ is a field or that $C$ has no maximal ideal $\mathfrak{M}$ such that one of the following exceptional cases occurs*

(i) $C/\mathfrak{M} = \mathbb{F}_2$ *or*

(ii) $\mathfrak{M} = \overline{\mathfrak{M}}$, $C/\mathfrak{M} = \mathbb{F}_4$ *and* $A/\mathfrak{M} \cap A = \mathbb{F}_2$.

*Then the kernel of the canonical surjection $r$: $W(A) \twoheadrightarrow W(C, J)$ is the ideal generated by the elements $[(1, -N\rho)]$ with $\rho$ in $C^*$ and $[(1, a)][(1, -(N\lambda + aN\mu))]$ with $a$ in $A^*$, $\lambda$, $\mu$ in $C$ and $N\lambda + aN\mu$ in $A^*$.*

*Proof.* The commutative diagram,

$$\begin{array}{ccc} \mathbb{Z}[A^*/A^{*2}] & \xrightarrow{\psi} & W(A) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle r} \\ \mathbb{Z}[A^*/NC^*] & \xrightarrow{\psi_1} & W(C, J) \end{array}$$

shows that $\ker r = \psi(\ker(\psi_1\pi))$. For $x$ in $A^*$ let $\{x\}$ denote the element $xA^{*2}$ in $\mathbb{Z}[A^*/A^{*2}]$. Now $\ker(\psi_1\pi) = \pi^{-1}(\ker\psi_1)$. Thus, $\ker(\psi_1\pi)$ is generated by

ker $\pi$ and the elements $\{1\} + \{-1\}$, $(\{1\} + \{a\})(\{1\} - \{N\lambda + aN\mu\})$ with $a$ in $A^*$, $\lambda$, $\mu$ in $C$, and $N\lambda + aN\mu$ in $A^*$ [33, Theorem 1.16, Corollary 1.17, and Lemma 1.19]. Since ker $\pi$ is generated by the elements $\{1\} - \{N\rho\}$ with $\rho$ in $C^*$, the lemma follows.

For a fixed $a$ in $A^*$ let $\mathscr{H}$ denote the set of units of $A$ of the form $N\lambda + aN\mu$ with $\lambda$, $\mu$ in $C$. Since

$$(N\lambda_1 + aN\mu_1)(N\lambda_2 + aN\mu_2) = N(\lambda_1\lambda_2 - a\mu_1\mu_2) + aN(\lambda_1\bar{\mu}_2 + \mu_1\bar{\lambda}_2)$$

and

$$(N\lambda + aN\mu)^{-1} = N\left(\frac{\lambda}{N\lambda + aN\mu}\right) + aN\left(\frac{\mu}{N\lambda + aN\mu}\right),$$

$\mathscr{H}$ is a subgroup of $A^*$.

Let $\mathscr{G}$ be the set of all $c$ in $A^*$ such that the element $[(1, a)][(1, -c)]$ of $W(A)$ lies in the ideal generated by the elements $[(1, -N\rho)]$ with $\rho$ in $C^*$. In $W(A)$ we have $[(c_2)][(1, a)][(1, -c_1)] + [(1, a)][(1, -c_2)] = [(1, a)][(1, -c_1c_2)]$, and $[(1, -c^{-1})] = [(1, -c)]$. Hence, $\mathscr{G}$ is also a subgroup of $A^*$. By Lemma 6.1, Proposition 2.5 will be proved if we show $\mathscr{H} \subset \mathscr{G}$ for every $a$ in $A^*$.

LEMMA 6.2. *Every unit of the form $b^2 + ad^2$ with $b$, $d$ in $A$ lies $\mathscr{G}$. Furthermore, every unit of the form $N\xi + ab^2N\eta$ with $\xi$, $\eta$ in $C^*$ and $b$ in $A$, also lies in $\mathscr{G}$.*

*Proof.* In $W(A)$ it is easily verified that $[(1, a)] = [(b^2 + ad^2)][(1, a)]$. Hence, $[(1, a)][(1, -(b^2 + ad^2))] = 0$ in $W(A)$ and so $b^2 + ad^2$ lies in $\mathscr{G}$. Since all $N\eta$ with $\eta$ in $C^*$ lie in $\mathscr{G}$ it suffices to consider a unit $c = N\xi + ab^2$ with $\xi$ in $C^*$ and $b$ in $A$. Since the space $(a, -c)$ over $A$ represents $-N\xi$

$$[(a, -c)] = [(-N\xi)][(1, -ac)]$$

in $W(A)$. Thus, $[(1, a)][(1, -c)] = [(1, -N\xi)][(1, -ac)]$, which shows that $c$ is in $\mathscr{G}$.

The proof that $\mathscr{H} \subset \mathscr{G}$ and thus of Proposition 2.5 will be completed with the proof of the following lemma.

LEMMA 6.3. *Assume that either $A$ is a field or that $C$ has no maximal ideal $\mathfrak{M}$ such that one of the following exceptional cases occurs*

(i) $C/\mathfrak{M} = \mathbb{F}_2$ *or* $\mathbb{F}_3$ *or*

(ii) $\mathfrak{M} = \overline{\mathfrak{M}}$, $C/\mathfrak{M} = \mathbb{F}_4$ *and* $A/A \cap \mathfrak{M} = \mathbb{F}_2$.

*Then the units $b^2 + ad^2$ and $N\xi + ab^2N\eta$ described in Lemma 6.2 generate the group $\mathscr{H}$ of all units $N\lambda + aN\mu$ with $\lambda, \mu$ in $C$*(cf. [29, *Satz* 1.2 *and its proof*]).

*Proof.* Let $\mathscr{H}_0$ denote the group generated by the units $b^2 + ad^2$ and $N\xi + ab^2N\eta$ with $b$, $d$ in $A$ and $\xi$, $\eta$ in $C^*$. If $A$ is a field an element $\gamma$ in $C$ is a unit if and only if $N\gamma \neq 0$. Putting $\xi = \lambda \neq 0$, $b = 0$, $\eta = 1$ shows that $N\lambda$ lies in $\mathscr{H}_0$ and, clearly, $aN\lambda$ does also. This finishes the proof if $A$ is a field.

The remainder of the proof is a series of reductions. Note that if $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ are all the maximal ideals of a semilocal ring $D$ and $d_1, \ldots, d_t$ are prescribed elements of $D$, the Chinese Remainder Theorem guarantees the existence of an element $d$ in $D$ with $d \equiv d_i(\mathfrak{m}_i)$.

(1) Let $c = N\lambda + aN\mu$ be a unit. We have

$$c(b^2 + ad^2) = N(b\lambda - ad\mu) + aN(d\lambda + b\mu).$$

Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ be all the maximal ideals of $A$. Since $c$ is a unit, if $N\lambda \equiv 0(\mathfrak{m}_i)$ then $N\mu \not\equiv 0(\mathfrak{m}_i)$. Thus, if $b$ and $d$ are elements of $A$ such that $b \equiv 1$, $d \equiv 0(\mathfrak{m}_i)$ if $N\lambda \not\equiv 0(\mathfrak{m}_i)$, and $b \equiv 0$, $d \equiv 1(\mathfrak{m}_i)$ if $N\lambda \equiv 0(\mathfrak{m}_i)$, both the elements $b^2+ad^2$ and $b\lambda-ad\mu$ are units of $A$. Multiplying by $(N(b\lambda-ad\mu))^{-1}$ we find $c \equiv 1 + aN\mu' \bmod \mathscr{H}_0$. Thus, it suffices to consider the case $c = 1 + aN\mu$.

(2) We have

$$c(1 + ab^2N\xi) = N(1 - ab\mu\xi) + aN(b\bar{\xi} + \mu).$$

Thus, the proof will be complete if we can find elements $b$ in $A$ and $\xi$ in $C^*$ such that $1 + ab^2N\xi$, $1 - ab\mu\xi$ and $b\bar{\xi} + \mu$ are units.

Over each maximal ideal $\mathfrak{m}$ of $A$ there is either a unique maximal ideal $\mathfrak{M}$ of $C$ with $\overline{\mathfrak{M}} = \mathfrak{M}$ or there are two maximal ideals $\mathfrak{M}$, $\overline{\mathfrak{M}}$ of $C$ [12, Theorem 2, p. 42]. Hence, in order to complete the proof we must show that for each maximal ideal $\mathfrak{m}$ of $A$ there exist elements $\xi$ in $C$ and $b$ in $A$ satisfying the following congruences:

(iii) $\xi \not\equiv 0 \bmod \mathfrak{M}$ and $\overline{\mathfrak{M}}$;

(iv) $1 + ab^2N\xi \not\equiv 0(\mathfrak{m})$;

(v) $1 - ab\mu\xi \not\equiv 0 \bmod \mathfrak{M}$ and $\overline{\mathfrak{M}}$;

(vi) $b\bar{\xi} + \mu \not\equiv 0 \bmod \mathfrak{M}$ and $\overline{\mathfrak{M}}$.

If $N\mu \not\equiv 0(\mathfrak{m})$, choosing $b \equiv 0(\mathfrak{m})$ and $\xi \equiv 1 \bmod \mathfrak{M}$ and $\overline{\mathfrak{M}}$ satisfies (iii)–(vi). For the remainder of the proof, therefore, we assume $N\mu \equiv 0(\mathfrak{m})$.

(3) Let $\mathfrak{M} \neq \overline{\mathfrak{M}}$. By [12, Corollary 1, p. 47] the canonical mappings $A/\mathfrak{m} \to C/\mathfrak{M}$ and $A/\mathfrak{m} \to C/\overline{\mathfrak{M}}$ are bijective. Hence, there are rings isomorphisms

$$A/\mathfrak{m} \times A/\mathfrak{m} \cong C/\mathfrak{M} \times C/\mathfrak{M} \cong C/(\mathfrak{M} \cap \overline{\mathfrak{M}}).$$

It is easily checked that the involution induced by $J$ on $C/(\mathfrak{M} \cap \overline{\mathfrak{M}})$ is carried to the involution $(\bar{a}_1, \bar{a}_2) \mapsto (\bar{a}_2, \bar{a}_1)$ of $A/\mathfrak{m} \times A/\mathfrak{m}$ by these isomorphisms. Hence, for a given element $\xi$ in $C$ there exist elements $d_1$, $d_2$ in $A$ with $\xi \equiv d_1(\mathfrak{M})$, $\xi \equiv d_2(\overline{\mathfrak{M}})$ and $N\xi \equiv d_1 d_2(\mathfrak{m})$. Since $N\mu \not\equiv 0(\mathfrak{m})$, the element $\mu$ lies in either $\mathfrak{M}$ or $\overline{\mathfrak{M}}$. By interchanging $\mathfrak{M}$ and $\overline{\mathfrak{M}}$ if necessary we may suppose $\mu$ lies in $\overline{\mathfrak{M}}$. Then conditions (iii)–(vi) become

(iii)′ $d_1 \not\equiv 0(\mathfrak{m})$ and $d_2 \not\equiv 0(\mathfrak{m})$;

(iv)′ $1 + ab^2 d_1 d_2 \not\equiv 0(\mathfrak{m})$;

(v)′ $1 - ab\mu d_1 \not\equiv 0(\mathfrak{M})$;

(vi)′ $bd_2 + \mu \not\equiv 0(\mathfrak{M})$ and $bd_1 \not\equiv 0(\mathfrak{m})$.

We choose $b \equiv 1(\mathfrak{m})$. By the hypotheses (i) and (ii) $A/\mathfrak{m}$ has at least three nonzero elements. Hence, we can choose $d_2$ so that the conditions involving $d_2$ in (iii)′ and (vi)′ are satisfied. Having fixed $d_2$ mod$(\mathfrak{m})$ we can then pick $d_1$ to satisfy the remaining conditions.

(4) Let $\mathfrak{M} = \overline{\mathfrak{M}}$. Then $\mu$ is in $\mathfrak{M}$ and (v) is automatically satisfied. The remaining conditions now become

$$b \not\equiv 0(\mathfrak{m}), \qquad \xi \not\equiv 0(\mathfrak{M}) \qquad \text{and} \qquad ab^2 N\xi \not\equiv -1(\mathfrak{m}).$$

Assume first that $A/\mathfrak{m}$ contains at least four elements. Choose $\xi \equiv 1(\mathfrak{M})$. Since $A/\mathfrak{m}$ contains at least two distinct nonzero squares we can also choose $b$ to satisfy these conditions.

Assume now that $A/\mathfrak{m} = \mathbb{F}_2$ or $\mathbb{F}_3$. Since $A/\mathfrak{m}$ is perfect [12, Theorem 2 (ii), p. 42] shows that $[C/\mathfrak{M} : A/\mathfrak{m}] \leqslant 2$. By hypothesis (ii) we need only consider the case $A/\mathfrak{m} = \mathbb{F}_3$, $C/\mathfrak{M} = \mathbb{F}_9$. By the same theorem of [12], $J$ does not induce the identity on $C/\mathfrak{M}$. Hence, $N\colon C \to A$ induces the usual field norm $\mathbb{F}_9 \to \mathbb{F}_3$ which is well known to be surjective. Hence, if we choose $b \equiv 1(\mathfrak{m})$ there is an element $\xi$ in $C$ to fullfill our conditions. This completes the proof of Lemma 6.3 and, thus, of Proposition 2.5.

## References

1. N. L. Alling, Rings of continuous integer-valued functions and nonstandard arithmetic, *Trans. Amer. Math. Soc.* **118** (1965), 498–525.
2. R. Arens and I. Kaplansky, Topological representation of algebras, *Trans. Amer. Math. Soc.* **63** (1948), 457–481.
3. E. Artin, Über die Zerlegung definiter Funktionen in Quadrate, *Abh. Math. Sem. Univ. Hamburg* **5** (1927), 100–115.
4. E. Artin, "Algebraic Numbers and Algebraic Functions," Gordon and Breach, New York, 1967.

5. M. AUSLANDER AND O. GOLDMAN, The Brauer group of a commutative ring, *Trans. Amer. Math. Soc.* **97** (1960), 367–409.
6. R. BAEZA, Eine Zerlegung der unitären Gruppe über lokalen Ringen, *Archiv. d. Math.* **24** (1973), 144–157.
7. A. A. BEL'SKII, Cohomological Witt rings, *Izv. Akad. Nauk SSSR Ser. Mat.* **32** (1968), 1147–1161; *Math. USSR Izv.* **2** (1968), 1101–1115.
8. N. BOURBAKI, "Algèbre," Chapter 2, 3rd ed., Hermann, Paris, 1962.
Hermitian forms over Dedekind rings, *Pacific J. Math.*, to appear.
9. N. BOURBAKI, "Algèbre," Chap. 6, 2nd ed., Hermann, Paris, 1964.
10. N. BOURBAKI, "Algèbre," Chap. 9, Hermann, Paris, 1959.
11. N. BOURBAKI, "Algèbre commutative," Chaps. 1–2, Hermann, Paris, 1961.
12. N. BOURBAKI, "Algèbre commutative," Chaps. 5–6, Hermann, Paris, 1964.
13. R. BROWN, An approximation theorem for extended prime spots, *Canad. J. Math.* **24** (1972), 167–184.
14. H. CARTAN AND S. EILENBERG, "Homological Algebra," Princeton University Press, Princeton, NJ, 1956.
15. S. U. CHASE, D. K. HARRISON, AND A. ROSENBERG, Galois theory and Galois cohomology of commutative rings, *Mem. Amer. Math. Soc.* **52** (1965), 15–33.
16. S. U. CHASE AND A. ROSENBERG, Amitsur Cohomology and the Brauer group, *Mem. Amer. Math. Soc.* **52** (1965), 34–79.
17. S. U. CHASE AND A. ROSENBERG, A theorem of Harrison, Kummer theory, and Galois algebras, *Nagoya Math. J.* **27** (1966), 663–685.
18. P. R. CHERNOFF, R. A. RASALA, AND W. C. WATERHOUSE, The Stone–Weierstrass theorem for valuable fields, *Pacific J. Math.* **27** (1968), 233–240.
19. F. DEMEYER AND E. INGRAHAM, "Separable Algebras over Commutative Rings," Lecture Notes in Mathematics 181, Springer Verlag, New York, 1971.
20. J. DILLER AND A. DRESS, Zur Galoistheorie pythagoreischer Körper, *Arch. Math.* **16** (1965), 148–152.
21. A. DRESS, "The Witt Ring as Mackey Functor, Notes on the Theory of Representations of Finite Groups I," Chapter 2, Appendix A, University of Bielefeld, Bielefeld, W. Germany, 1971.
22. S. EILENBERG AND T. NAKAYAMA, On the dimension of modules and algebras II (Frobenius algebras and quasi-Frobenius rings), *Nagoya Math. J.* **9** (1955), 1–16.
23. R. ELMAN AND T. Y. LAM, Quadratic forms over formally real fields and pythagorean fields, *Amer. J. Math.* **94** (1972), 1155–1194.
24. A. GROTHENDIECK, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. IV, *Inst. Hautes Études Sci. Publ. Math.* **32** (1967), 361.
25. D. K. HARRISON, Witt rings, Lecture Notes, Department of Mathematics, University of Kentucky, Lexington, 1970.
26. I. KAPLANSKY, Topological rings, *Amer. J. Math.* **69** (1947), 153–183.
27. M. KNEBUSCH, Grothendieck-und Wittringe von nichtausgearteten symmetrischen Bilinearformen, *S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl.* 1969, 93–157.
28. M. KNEBUSCH, Isometrien über semilokalen Ringen, *Math. Z.* **108** (1969), 255–268.
29. M. KNEBUSCH, Runde Formen über semilokalen Ringen, *Math. Ann.* **193** (1971), 21–34.
30. M. KNEBUSCH, On the uniqueness of real closures and the existence of real places, *Comm. Math. Helv.* **47** (1972), 260–269.
31. M. KNEBUSCH, A. ROSENBERG, AND R. WARE, Structure of Witt rings, quotients

of Abelian group rings, and orderings of fields, *Bull. Amer. Math. Soc.* **77** (1971), 205–210.

32. M. KNEBUSCH, A. ROSENBERG, AND R. WARE, Signatures on semilocal rings, *Bull. Amer. Math. Soc.* **78** (1972), 62–64.
33. M. KNEBUSCH, A. ROSENBERG, AND R. WARE, Structure of Witt rings and quotients of Abelian group rings, *Amer. J. Math.* **94** (1972), 119–155.
34. M. KNEBUSCH, A. ROSENBERG, AND R. WARE, Grothendieck and Witt rings of Hermitian forms over Dedekind rings, *Pacific J. Math.* **43** (1972), 657–673.
35. M. KNEBUSCH AND W. SCHARLAU, Über das Verhalten der Witt-Gruppe bei galoischen Körpererweiterungen, *Math. Ann.* **193** (1971), 189–196.
36. F. LORENZ AND J. LEICHT, Die Primideale des Wittschen Ringes, *Invent. Math.* **10** (1970), 82–88.
37. A. MAGID, Galois groupoids, *J. Algebra* **18** (1971), 89–102.
38. J. MILNOR AND D. HUSEMOLLER, "Symmetric Bilinear Forms," Ergebnisse d. Math., Vol. 73, Springer, Berlin-Heidelberg-New York, 1973.
39. A. PFISTER, Quadratische Formen in beliebigen Körpern, *Invent. Math.* **1** (1966), 116–132.
40. R. S. PIERCE, Rings of integer-valued continuous functions, *Trans. Amer. Math. Soc.* **100** (1961), 371–394.
41. A. ROSENBERG AND R. WARE, The zero-dimensional galois cohomology of Witt rings, *Invent. Math.* **11** (1970), 65–72.
42. A. ROY, Cancellation of quadratic forms over commutative rings, *J. Algebra* **10** (1968), 286–298.
43. W. SCHARLAU, Quadratic forms, Queen's papers on pure and applied mathematics, No. 22, Queen's University, Kingston, Canada, 1969.
44. W. SCHARLAU, Zur Pfisterschen Theorie der quadratischen Formen, *Invent. Math.* **6** (1969), 327–328.
45. T. A. SPRINGER, Quadratic forms over fields with a discrete valuation, *Indag. Math.* **17** (1955), 352–362.
46. O. TEICHMÜLLER, Verschränkte Produkte mit Normalringen, *Deutsche Math.* **1** (1936), 92–102.

Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium.