

## Signatures on Frobenius Extensions

MANFRED KNEBUSCH

UNIVERSITÄT REGENSBURG  
REGENSBURG, WEST GERMANY

### Introduction

Let  $A$  be a commutative ring equipped with an involution  $J_A$ . For conciseness, we write  $A$  instead of the pair  $(A, J_A)$ , and denote the ring  $A$  without involution by  $|A|$ . A *signature*  $\sigma$  on  $A$  is defined as a homomorphism from the Witt ring  $W(A)$  of nondegenerate hermitian forms over  $A$  to the ring of integers  $\mathbb{Z}$ . If  $|A|$  has a connected spectrum, either  $A$  has no signatures at all or the kernels of the signatures are precisely all minimal prime ideals of  $W(A)$ , as has been shown in Knebusch [7, I, §2] and Dress [3]. It also can be shown that  $A$  has no signatures if and only if  $-1$  is a sum of norms  $xJ_A(x)$  in  $A$  (proof to be published, cf. [8] for  $|A|$  semilocal). In the case that  $A$  is a field and  $J_A$  is trivial it is well known that the signatures of  $A$  correspond uniquely to the orderings of  $A$  [5, 11]. For  $|A|$  a semilocal ring, a general study of signatures and related topics can be found in Knebusch *et al.* [10] and [8].

For a homomorphism  $\varphi: A \rightarrow B$  into another ring with involution  $B$  an *extension*  $\tau$  of a signature  $\sigma$  on  $A$  to  $B$  (with respect to  $\varphi$ ) is defined as a

signature  $\tau$  on  $B$  such that the diagram

$$\begin{array}{ccc} W(A) & \xrightarrow{\varphi_*} & W(B) \\ \sigma \searrow & & \swarrow \tau \\ & \mathbb{Z} & \end{array}$$

with  $\varphi_*$  induced by  $\varphi$  is commutative. Recently I developed a theory of “real closures” of a pair  $(A, \sigma)$  with  $A$  an arbitrary commutative ring with involution and  $\sigma$  a signature on  $A$  (cf. [7]), which generalizes Artin–Schreier’s well-known theory of real closures of ordered fields. This theory is tied up with a theory of extensions of  $\sigma$  for  $\varphi$  finite etale {i.e.,  $|\varphi|: |A| \rightarrow |B|$  finite etale}. As has been shown in [7] there exist only finitely many extensions of  $\sigma$  to  $B$  in this case. Moreover the regular trace  $\text{Tr}_{B/A}$  from  $B$  to  $A$  yields a  $W(A)$ -linear map

$$\text{Tr}_{B/A}^*: W(B) \rightarrow W(A),$$

(cf. [12, 7]) and for  $z$  in  $W(B)$  the following trace formula holds true [7, I, §3]:

$$\sigma(\text{Tr}_{B/A}^*(z)) = \sum_{\tau|\sigma} n(\tau)\tau(z).$$

In this sum  $\tau$  runs through the extensions of  $\sigma$  to  $B$ , and the “multiplicities”  $n(\tau)$  are positive integral numbers, uniquely determined by  $\tau$  and  $\varphi$ . If  $|A|$  is semilocal and  $J_A$  is trivial, all these multiplicities are 1 [7, II, §8].

Inserting  $z = 1$  in this trace formula we see that the number  $r$  of signatures of  $B$  extending  $\sigma$  is at most equal to the rank  $[B : A]$  of the projective  $A$ -module  $B$ . If  $|A|$  is semilocal and  $J_A = \text{id}$ , moreover  $r \equiv [B : A] \pmod{2}$ .

In the present paper we study the extensions of  $\sigma$  to  $B$  in the case that  $B$  is a “Frobenius extension” of  $A$ . For any element  $a$  of a ring with involution we denote the image of  $a$  under this involution by  $\bar{a}$ . We call  $B$  a *Frobenius extension* of  $A$  if  $B$  is as an  $A$ -module finitely generated and projective and if there exists a linear form  $s: B \rightarrow A$  on this module such that  $s(\bar{b}) = \overline{s(b)}$  for  $b$  in  $B$  and the hermitian form  $s(\bar{x}y)$  on the  $A$ -module  $B$  is nondegenerate. If the involutions are trivial, this is indeed the usual notion of Frobenius extension occurring in the literature (cf. Eilenberg and Nakayama [4]). We also say that  $s$  is a *Frobenius form* on  $B$ .

If  $B$  is finite etale, the trace  $\text{Tr}_{B/A}$  is a Frobenius form on  $B$ . But the class of Frobenius extensions is much larger than the class of finite etale extensions. This is the reason the present paper seems to be a necessary step in the theory of hermitian forms over rings. For example, let  $a$  be an element in  $A$  with  $\bar{a} = a$ . The extension  $B := A[X]/(X^2 - a) = A[x]$  with  $J_B$  extending  $J_A$  and  $\bar{x} = x$  is Frobenius. But if 2 or  $a$  is not a unit in  $A$ , then  $B$  is not etale.

Certainly such extensions are important for a study of hermitian forms. A useful example of a cubic Frobenius extension occurs in [9].

We essentially apply the same methods as in [7], cf. in particular §§3 and 4 of [7], and we use also the terminology and the notations of [7]. Our results are satisfactory only in the case that  $|A|$  is semilocal. Much work remains to be done. For example, we do not know in general whether a given signature  $\sigma$  of  $A$  has only finitely many extensions to a given Frobenius extension  $B$  of  $A$ . As has been shown in [7, §3] this is true if  $B$  is finite étale over  $A$ .

## 1. The Transfer Formula

In this section  $A$  is an arbitrary commutative ring with involution. Let  $\varphi: A \rightarrow B$  be a Frobenius extension of  $A$  and  $s: B \rightarrow A$  a Frobenius form. Then  $s$  induces an additive map

$$s^*: W(B) \rightarrow W(A),$$

which is defined as follows. Let  $(E, \Phi)$  be a hermitian space over  $B$ , i.e., a finitely generated projective  $B$ -module  $E$  equipped with a nondegenerate hermitian form  $\Phi$ . ( $\Phi$  is assumed to be antilinear in the first and linear in the second variable.) Then  $s^*$  maps the Witt class  $[E, \Phi]$  of this hermitian space to the Witt class  $[E, s \circ \Phi]$  of the  $A$ -module  $E$  equipped with the hermitian form  $s \circ \Phi$  (cf. Scharlau [12]). Clearly  $s^*$  is  $W(A)$ -linear, i.e., we have

$$s^*(\varphi_*(x)y) = x \cdot s^*(y) \tag{1.1}$$

for  $x$  in  $W(A)$  and  $y$  in  $W(B)$ .

Now let  $\sigma$  be a signature on  $A$ . We denote by  $S(\varphi, \sigma)$  the set of all signatures  $\tau$  of  $B$  that extend  $\sigma$ .

**Theorem 1.1** *There exists a unique family  $(m(\tau) \mid \tau \in S(\varphi, \sigma))$  of integral numbers such that almost all  $m(\tau) = 0$  and for every  $z$  in  $W(B)$  the following equation holds true:*

$$\sigma(s^*(z)) = \sum_{\tau \mid \sigma} m(\tau)\tau(z).$$

Here  $\tau$  runs through the set  $S(\varphi, \sigma)$  of all extensions of  $\sigma$  to  $B$ . (If this set is empty, the equation reads  $\sigma(s^*(z)) = 0$ .)

*Proof* The kernel  $P(\tau)$  of a signature  $\tau: W(B) \rightarrow \mathbb{Z}$  is a minimal prime ideal of  $W(B)$  [3, 7]. Thus there do not exist any inclusion relations between the kernels of different signatures of  $B$ . This already implies that there exists at most one family  $(m(\tau) \mid \tau \in S(\varphi, \sigma))$  for given  $\varphi, \sigma, s$  with the above properties; cf. Knebusch [7, I, p. 72].

To prove the existence of such a family  $(m(\tau))$  we choose a homomorphism  $\alpha$  from  $A$  into a real closed field with involution  $R$  inducing  $\sigma$ . In more explicit terms this means the following.  $|R|$  is an algebraic closed field.  $J_R$  is nontrivial, and thus the fixed field  $R_0$  of  $J_R$  is a real closed field in the sense of Artin-Schreier. We have

$$W(R) \cong W(R_0) \cong \mathbb{Z}$$

( $R_0$  equipped with the trivial involution), and denoting the unique signature of  $R$  by  $\rho$  we have  $\rho \circ \alpha_* = \sigma$ . Such a homomorphism  $\alpha$  exists according to [7, I, §4].

The tensor product  $B \otimes_A R$  with respect to  $\varphi$  and  $\alpha$ , equipped with the involution  $J_B \otimes J_R$ , is a Frobenius extension of  $R$  with the Frobenius form  $s \otimes 1$  from  $B \otimes_A R$  to  $R$ . It is easily checked that the following diagram commutes:

$$\begin{array}{ccc} W(B) & \xrightarrow{(1 \otimes \alpha)_*} & W(B \otimes_A R) \\ \downarrow s_* & & \downarrow (s \otimes 1)_* \\ W(A) & \xrightarrow{\alpha_*} & W(R) \end{array}$$

We have a unique direct decomposition

$$B \otimes_A R = \prod_{i=1}^g B_i$$

into connected rings with involution  $B_i$ . Let  $\varphi_i: R \rightarrow B_i$  denote the components of the homomorphism  $\varphi \otimes 1$  from  $R$  to  $B \otimes_A R$ , and  $\alpha_i: B \rightarrow B_i$  the components of the homomorphism  $1 \otimes \alpha$  from  $B$  to  $B \otimes_A R$ . We may assume that for some  $r, 0 \leq r \leq g$  all rings  $|B_i|$  with  $1 \leq i \leq r$  are connected and all  $|B_i|$  with  $r < i \leq g$  are not connected. Then for  $i > r$ , the ring  $B_i$  with involution is isomorphic to a product  $D_i \times D_i$  of two copies of a ring  $D_i$  with the “switch” of the factors as involution. Thus  $W(B_i) = 0$  for  $i > r$ . For  $i \leq r$ , we denote by  $N_i$  the nil radical of  $B_i$  and we have

$$B_i = \varphi_i(R) \oplus N_i.$$

Since 2 is a unit in  $R$  and  $N_i$  is nilpotent,  $\varphi_i$  induces an isomorphism  $\varphi_{i*}$  from  $W(R) \cong \mathbb{Z}$  onto  $W(B_i)$  (cf., e.g., [14, Theorem 2.2.1]).

Let  $s_i: B_i \rightarrow R$  denote the restriction of the  $R$ -linear form  $s \otimes 1$  to the direct summand  $B_i$  of the  $R$ -module  $B \otimes_A R$ . Clearly,  $s_i$  is a Frobenius form with respect to  $\varphi_i: R \rightarrow B_i$ . Denoting finally the projection from  $B \otimes_A R$  to  $B_i$ , by  $p_i$ , the induced maps  $p_{i*}$  from  $W(B \otimes_A R)$  to  $W(B_i)$  yield an

isomorphism

$$(p_{1*}, \dots, p_{r*}): W(B \otimes_A R) \xrightarrow{\sim} \prod_{i=1}^r W(B_i),$$

and for  $u$  in  $W(B \otimes_A R)$  we have

$$(s \otimes 1)^*(u) = \sum_{i=1}^r s_i^* p_{i*}(u).$$

Now it is not difficult to prove the desired formula for  $\sigma s^*(z)$ , with  $z$  in  $W(B)$ . We have

$$\begin{aligned} \sigma s^*(z) &= \rho \alpha_* s^*(z) = \rho (s \otimes 1)^* (1 \otimes \alpha)_*(z) \\ &= \sum_{i=1}^r \rho s_i^* p_{i*} (1 \otimes \alpha)_*(z) = \sum_{i=1}^r \rho s_i^* \alpha_{i*}(z). \end{aligned}$$

Let  $\gamma_i$  denote the unique homomorphism from  $B_i$  to  $R$  with  $\gamma_i \circ \varphi_i = \text{id}$  ( $1 \leq i \leq r$ ). We have  $\gamma_{i*} \circ \varphi_{i*} = \text{id}$ . Since  $\varphi_{i*}$  is an isomorphism this implies  $\varphi_{i*} \circ \gamma_{i*} = \text{id}$ . We obtain

$$\sigma s^*(z) = \sum_{i=1}^r \rho s_i^* \varphi_{i*} \gamma_{i*} \alpha_{i*}(z) = \sum_{i=1}^r \rho s_i^* \varphi_{i*} \beta_{i*}(z),$$

with  $\beta_i$  denoting the homomorphism  $\gamma_i \circ \alpha_i$  from  $B$  to  $R$ . Applying (1.1) this can be simplified to

$$\sigma s^*(z) = \sum_{i=1}^r \rho s_i^*(1) \cdot \rho \beta_{i*}(z).$$

Notice that the  $\beta_i$  are precisely all homomorphisms  $\beta$  from the ring with involution  $B$  to  $R$  with  $\beta \circ \varphi = \alpha$ . For any signature  $\tau$  in  $S(\sigma, \varphi)$ , we denote by  $I(\tau)$  the set of all indices  $i$ ,  $1 \leq i \leq r$ , such that  $\rho \circ \beta_{i*} = \tau$ . Of course only finitely many  $I(\tau)$  are nonempty. Further, we denote by  $B(\tau)$  the product of all  $B_i$  with  $i$  in  $I(\tau)$ . We have

$$B \otimes_A R = \prod_{\tau \in \sigma} B(\tau).$$

Finally, we denote by  $s_\tau$  the restriction of  $s \otimes 1$  to the direct summand  $B(\tau)$  of the  $R$ -module  $B \otimes_A R$ . Clearly,  $s_\tau$  is a Frobenius form on the extension  $B(\tau)$  of  $R$ . Using these notations we can write

$$\sigma s^*(z) = \sum_{\tau \in \sigma} m(\tau) \tau(z)$$

with

$$m(\tau) := \rho s_\tau^*(1). \tag{1.2}$$

In more explicit terms,  $m(\tau)$  is the signature of the hermitian form  $s_\tau(\bar{x}y)$  on the vector space  $B(\tau)$  over  $R$ .

This proves our Theorem 1.2 and also gives some insight into the nature of the coefficients  $m(\tau)$ .

The coefficients  $m(\tau)$  depend only on  $\varphi$  and  $\tau$ . We denote them hereafter by  $n(\tau, s)$ . The notation  $n(\tau, \varphi, s)$  or  $n(\tau, A, s)$  will be appropriate whenever it is not clear from the context which base ring  $A$  is under consideration. The formula

$$\sigma s^*(z) = \sum_{\tau|\sigma} n(\tau, s)\tau(z)$$

will be called the *transfer formula* for  $\varphi: A \rightarrow B$  and  $s$ .

From (1.2) we deduce in the case that the rank  $[B : A]$  of the projective  $A$ -module is constant, the modest information

$$\sum_{\tau|\sigma} |n(\tau, s)| \leq [B : A] \quad (1.3)$$

Furthermore,

$$n(\tau, s) \equiv [B(\tau) : R] \pmod{2}.$$

Thus if  $[B : A]$  is constant, we see that

$$\sum_{\tau|\sigma} n(\tau, s) \equiv [B : A] \pmod{2}. \quad (1.4)$$

From our proof of the transfer formula also the following corollary is evident.

**Corollary 1.2** *Let  $s$  be a Frobenius form on  $B$  with respect to  $\varphi: A \rightarrow B$ . Let  $\sigma$  be a signature on  $A$  and  $\tau$  be an extension of  $\sigma$  to  $B$  with  $n(\tau, s) \neq 0$ . Then for any homomorphism  $\alpha: A \rightarrow R$  into a real closed field with involution  $R$  that induces  $\sigma$  there exists a homomorphism  $\beta: B \rightarrow R$  that induces  $\tau$  and extends  $\alpha$ , i.e.,  $\beta \circ \varphi = \alpha$ .*

In general  $n(\tau, s)$  may well be zero (cf. Section 2). We mention two cases in which  $n(\tau, s) \neq 0$  for all extensions  $\tau$  of  $\sigma$  to  $B$ .

**Remark 1.3** If  $\varphi$  is finite etale and  $s$  is the regular trace  $\text{Tr}_{B/A}$ , then all  $n(\tau, s)$  are positive numbers. Moreover, given a homomorphism  $\alpha$  from  $A$  into a real closed field with involution  $R$  inducing  $\sigma$  the number  $n(\tau, s)$  coincides with the cardinality  $n(\tau, \alpha)$  of the set of homomorphisms  $\beta$  from  $B$  to  $R$  that induce  $\tau$  and extend  $\alpha$  (cf. Knebusch [7, I, §3]). Indeed, in the proof of the transfer formula now the ideals  $N_i$ ,  $1 \leq i \leq r$ , are zero, and the Frobenius forms  $s_i: B_i \rightarrow R$  are the inverse maps of the isomorphisms  $\varphi_i: R \xrightarrow{\sim} B_i$ . This implies immediately  $n(\tau, s) = n(\tau, \alpha)$ .

If  $E$  is an hermitian space<sup>†</sup> over  $A$  of constant rank  $n$  then  $|\sigma(E)| \leq n$  for every signature  $\sigma$  on  $A$ . Indeed, let  $\alpha: A \rightarrow R$  be a homomorphism into a real closed field with involution  $R$  inducing  $\sigma$ . Then  $\sigma(E)$  is the usual Sylvester signature of the hermitian space  $E \otimes_A R$  over  $R$ . We call  $E$  *positive definite* at  $\sigma$  if  $\sigma(E) = n$ . Returning to our extension  $\varphi: A \rightarrow B$  with Frobenius form  $s: B \rightarrow A$  we denote by  $s^*\langle 1 \rangle$  the hermitian space  $B$  over  $A$ , equipped with the hermitian form  $s(\bar{x}y)$ .

**Proposition 1.4** *If  $B$  has constant rank over  $A$  and  $s^*\langle 1 \rangle$  is positive definite at  $\sigma$ , then for every signature  $\tau$  on  $B$  extending  $\sigma$  the coefficient  $n(\tau, s)$  is positive. Moreover, given a homomorphism  $\alpha$  from  $A$  to a real closed field with involution  $R$  inducing  $\sigma$  we have  $n(\tau, s) = n(\tau, \alpha)$ .*

*Proof* Returning to the proof of the transfer formula we see that all spaces  $s_i^*\langle 1 \rangle$ ,  $1 \leq i \leq g$ , are positive definite over  $R$ . Thus  $r = g$ . Furthermore, the ideals  $N_i$  must be zero since otherwise the highest power  $N_i^{d_i}$  of  $N_i$  that is nonzero would be an isotropic subspace of  $s_i^*\langle 1 \rangle$ . Thus  $s_i^*\langle 1 \rangle$  has rank one and  $s_i^*\langle 1 \rangle$  has rank  $n(\tau, \alpha)$ . We obtain

$$n(\tau, s) = \rho s_i^*\langle 1 \rangle = n(\tau, \alpha).$$

We still have to show  $n(\tau, s) > 0$  for a given extension  $\tau$  of  $\sigma$  to  $B$ . We choose a homomorphism  $\beta$  from  $B$  into a real closed field with involution  $R$  inducing  $\tau$ , and we put  $\alpha := \beta \circ \varphi$ . Then certainly  $n(\tau, \alpha) > 0$  for this particular  $\tau$ , hence  $n(\tau, s) > 0$ . QED

We now look at what happens to the coefficients  $n(\tau, s)$  if we replace  $s$  by another Frobenius form  $s'$  with respect to  $\varphi$ . We have

$$s'(x) = s(bx)$$

where  $b$  is an element of  $B$  with  $\bar{b} = b$  uniquely determined by  $s$  and  $s'$ . Since the hermitian form  $s'(\bar{x}y)$  is nondegenerate,  $b$  must be a unit of  $B$ . Let  $\langle b \rangle$  denote the hermitian space over  $B$  consisting of the  $B$ -module  $B$  and the hermitian form  $b\bar{x}y$ . We denote the class of this space in  $W(B)$  again by  $\langle b \rangle$ , and the value of this class under a signature  $\tau$  on  $B$  by  $\tau(b)$ . Clearly

$$s'^*(z) = s^*(\langle b \rangle z)$$

for  $z$  in  $W(B)$ , hence

$$\sigma s'^*(z) = \sum_{\tau|\sigma} n(\tau, s)\tau(\langle b \rangle z) = \sum_{\tau|\sigma} n(\tau, s)\tau(b)\tau(z).$$

Thus we have

$$n(\tau, s') = \tau(b)n(\tau, s) \tag{1.5}$$

for every signature  $\tau$  on  $B$ . Notice that  $\tau(b) = \pm 1$  since  $\langle b \rangle^2 = 1$ .

<sup>†</sup> We write for brevity  $E$  instead of the pair  $(E, \Phi)$ .

## 2. Some Examples

We first study quadratic extensions. Let  $A$  be an arbitrary commutative ring with involution, and let  $a$  be a unit in  $A$  with  $\bar{a} = a$ . We consider the ring

$$B := A[T]/(T^2 - a).$$

We have  $B = A \oplus At$  with the relation  $t^2 = a$ . We extend the involution  $J_A$  to  $B$  either by prescribing  $\bar{t} = t$  (case I) or by prescribing  $\bar{t} = -t$  (case II).

We introduce the  $A$ -linear form  $s$  on  $B$  with  $s(1) = 1, s(t) = 0$ . Then in both cases  $s(\bar{x}) = \overline{s(x)}$  for every  $x$  in  $B$ . Using the basis  $1, t$  of  $B$  over  $A$ , we obtain

$$s^*\langle 1 \rangle \cong \langle 1, a \rangle \quad (\text{case I}),$$

$$s^*\langle 1 \rangle \cong \langle 1, -a \rangle \quad (\text{case II}).$$

Thus  $s$  is a Frobenius form on  $B$  over  $A$ .

Let  $\sigma$  be a signature on  $A$ .

**Proposition 2.1** (i) *Assume  $\bar{t} = t$ . If  $\dagger \sigma(a) = -1$ , then  $\sigma$  has no extension to  $B$ . If  $\sigma(a) = +1$ , then  $\sigma$  has precisely two extensions  $\tau_1, \tau_2$  to  $B$ , and  $n(\tau_1, s) = n(\tau_2, s) = 1$ .*

(ii) *Assume  $\bar{t} = -t$ . If  $\sigma(a) = +1$ , then  $\sigma$  has no extension to  $B$ . If  $\sigma(a) = -1$ , then  $\sigma$  has a unique extension  $\tau$  to  $B$  and  $n(\tau, s) = 2$ .*

*Proof* If  $\bar{t} = t$ , then  $a = t\bar{t}$  is a norm in  $B$ , and a signature  $\sigma$  on  $A$  with  $\sigma(a) = -1$  cannot be extended to  $B$ . If  $\bar{t} = -t$ , then  $-a = t\bar{t}$  is a norm in  $B$ , and a signature  $\sigma$  with  $\sigma(a) = +1$  cannot be extended to  $B$ . In the remaining cases  $s^*\langle 1 \rangle$  is positive definite at  $\sigma$ . Thus by Proposition 1.4 every extension  $\tau$  of  $\sigma$  to  $B$  has coefficient  $n(\tau, s) > 0$ . Furthermore,

$$\sum_{\tau|\sigma} n(\tau, s) = \sigma s^*(1) = 2.$$

Thus one of the following two possibilities must occur:

- (A)  $\sigma$  has precisely two extensions  $\tau_1, \tau_2$ , and  $n(\tau_1, s) = n(\tau_2, s) = 1$ .
- (B)  $\sigma$  has a unique extension  $\tau$ , and  $n(\tau, s) = 2$ .

Anyway,  $\sigma$  has at least one extension to  $B$ , and we choose such an extension  $\tau_1$ . We further choose a homomorphism  $\beta_1$  from  $B$  to a real closed field with involution  $R$  inducing  $\tau_1$ . We put  $\alpha := \beta_1 \circ \varphi$ , with  $\varphi$  the inclusion map from  $A$  to  $B$ . Then  $\alpha$  induces  $\sigma$ . Let  $\gamma$  denote the automorphism of  $B$  over  $A$  of order 2, defined by  $\gamma(t) = -t$ . Notice that  $\gamma$  is indeed compatible with the involution  $J_B$  in both cases. Consider the homomorphism  $\beta_2 := \beta_1 \circ \gamma$  from

† Cf. the notations at the end of Section 1.

$B$  to  $R$ . We have  $\beta_2(t) \neq \beta_1(t)$  and thus  $\beta_2$  is different from  $\beta_1$ . Clearly,  $\beta_1$  and  $\beta_2$  are all homomorphisms from  $B$  to  $R$  extending  $\alpha$ . Let  $\rho$  denote the unique signature of  $R$ . If  $\bar{t} = t$ , then we have a hermitian space  $\langle t \rangle$  over  $B$  consisting of the  $B$ -module  $B$  and the hermitian form  $t\bar{x}y$ . We have

$$(\rho \circ \beta_{2*})\langle t \rangle = -(\rho \circ \beta_{1*})\langle t \rangle.$$

Thus there exist two different signature  $\rho \circ \beta_{1*}$  and  $\rho \circ \beta_{2*}$  extending  $\sigma$ , and possibility (A) is realized. If  $\bar{t} = -t$ , then

$$\beta_2 = J_R \circ \beta_1.$$

Now  $J_R$  is an automorphism of the field with involution  $R$  that induces the identity on  $W(R)$  (cf. [7, I, Lemma 3.11]). Thus  $\rho \circ \beta_{2*} = \rho \circ \beta_{1*} = \tau_1$ , and we obtain  $n(\tau_1, \alpha) = 2$ . According to Proposition 1.4, we have  $n(\tau_1, s) = 2$ , and possibility (B) is realized.

If  $B = A[T]/(T^2 - a)$  but  $a$  is not a unit in  $A$ , the situation may be very different.

**Example 2.2** Let  $A$  be the localization of the polynomial ring  $\mathbb{R}[x_1, \dots, x_n]$  in  $n \geq 2$  variables  $x_i$  with respect to the maximal ideal generated by  $x_1, \dots, x_n$ , and let  $\mathfrak{m}$  denote the maximal ideal  $Ax_1 + \dots + Ax_n$  of  $A$ . We choose the element

$$a := -(x_1^2 + \dots + x_n^2)$$

in  $\mathfrak{m}$  and study the extension

$$B = A \oplus At, \quad t^2 = a,$$

of  $A$ , both  $A$  and  $B$  being equipped with the trivial involution. The  $A$ -linear form  $s$  on  $B$  defined by  $s(1) = 0$ ,  $s(t) = 1$  is a Frobenius form over  $A$ . Indeed,

$$s^*\langle 1 \rangle \cong \begin{bmatrix} 0 & 1 \\ 1 & a \end{bmatrix}.$$

The ideal  $\mathfrak{M} := \mathfrak{m}B$  is the unique prime ideal of  $B$  lying over  $A$ , and

$$A/\mathfrak{m} \cong B/\mathfrak{M} \cong \mathbb{R}.$$

We consider the evident signatures attached to  $\mathfrak{m}$  and  $\mathfrak{M}$ .

$$\sigma: W(A) \rightarrow W(A/\mathfrak{m}) \xrightarrow{\sim} \mathbb{Z}, \quad \tau: W(B) \rightarrow W(B/\mathfrak{M}) \xrightarrow{\sim} \mathbb{Z}.$$

Notice that  $\tau$  extends  $\sigma$ . Since  $A$  is regular,  $\sigma$  can also be extended to a signature of the quotient field  $\mathbb{R}(x_1, \dots, x_n)$  of  $A$ , equipped with the trivial involution, as has been shown by Craven, Rosenberg, and Ware [2]. Thus there exists an injection  $\alpha$  of  $A$  into a real closed field with involution  $R$

inducing  $\sigma$ . But this homomorphism  $\alpha$  certainly does not extend to a homomorphism  $\beta$  from  $B$  to  $R$  since  $\alpha(a)$  is a negative element of the fixed field  $R_0$  of  $J_R$ , and  $\beta(t)$  would be an element  $\lambda$  of  $R_0$  with  $\lambda^2 = \alpha(a)$ . In particular  $n(\tau, s) = 0$ .

**Remark 2.3** From Theorem 3.1 in the next section it can be easily deduced that  $\tau$  is the only extension of  $\sigma$  to  $B$ .

We now shall study extensions of type  $B = A[T]/(T^n)$ . We have the following general fact.

**Lemma 2.4** *Let  $\varphi: A \rightarrow B$  be a homomorphism in the category of commutative rings with involution. Let  $\mathfrak{N}_A$  and  $\mathfrak{N}_B$  denote the nil radicals of  $A$  and  $B$  and  $\bar{A}, \bar{B}$  denote the reductions  $A/\mathfrak{N}_A$  and  $B/\mathfrak{N}_B$ . Assume that  $\varphi$  induces an isomorphism  $\bar{\varphi}: \bar{A} \rightarrow \bar{B}$ . Then every signature of  $A$  extends in a unique way to a signature of  $B$  with respect to  $\varphi$ .*

*Proof* We have a commutative diagram

$$\begin{array}{ccc}
 A & \xrightarrow{\varphi} & B \\
 \pi \downarrow & & \downarrow \pi' \\
 \bar{A} & \xrightarrow{\bar{\varphi}} & \bar{B}
 \end{array}$$

with  $\pi$  and  $\pi'$  the canonical surjections. It suffices to prove the lemma for the homomorphisms  $\pi$  and  $\pi'$ . Then it will be evident for  $\varphi$  too. Thus we assume hereafter that  $B = \bar{A}$  and  $\varphi$  is the canonical surjection from  $A$  onto  $\bar{A}$ .

Let  $\sigma$  be a signature on  $A$ . We choose a homomorphism  $\alpha$  from  $A$  into a real closed field with involution  $R$  inducing  $\sigma$ . We have a unique homomorphism  $\bar{\alpha}$  from  $\bar{A}$  to  $R$  with  $\bar{\alpha} \circ \varphi = \alpha$ . Let  $\tau$  denote the signature on  $\bar{A}$  induced by  $\bar{\alpha}$ . Then  $\tau$  extends  $\sigma$ . The remaining assertion that  $\tau$  is the unique extension of  $\sigma$  now follows from the fact that the map  $\varphi_*$  from  $W(A)$  to  $W(\bar{A})$  is surjective. Since I did not find a reference for this probably well-known fact in full generality, I indicate a proof.

We show that for a given hermitian space  $(U, h)$  over  $\bar{A}$  there exists a hermitian space  $(E, \Phi)$  over  $A$  whose reduction mod  $\mathfrak{N}_A$  is isometric to  $(U, h)$ . There exists a finitely generated projective  $A$ -module  $E$ , unique up to isomorphism, such that  $E/\mathfrak{N}_A E$  is isomorphic to  $U$  (cf., e.g., Swan [13, Theorem 2.26, p. 89]). Thus we assume a priori that  $U$  is the reduction  $\bar{E}$  of a given finitely generated projective  $A$ -module  $E$  modulo  $\mathfrak{N}_A$ . We now can find another hermitian space  $(V, h')$  over  $\bar{A}$  such that  $U \oplus V$  is a free module over  $\bar{A}$ . Indeed, let  $W$  be a module over  $\bar{A}$  such that  $U \oplus W$  is a free  $\bar{A}$ -module of finite rank. Then take

$$(V, h') := (U, -h) \perp H(W)$$

with  $H(W)$  the hyperbolic space  $W \oplus W^*$  constructed from  $W$ . ( $W^*$  = antidual module of  $W$ ,  $W \oplus W^*$  equipped with the obvious hermitian form which is zero on  $W \times W$  and on  $W^* \times W^*$ .) We again regard  $V$  as the reduction mod  $\mathfrak{R}_A$  of a finitely generated projective  $A$ -module  $F$ . The module  $G := E \oplus F$  over  $A$  is free. Let  $g_1, \dots, g_n$  be a basis of  $G$  over  $A$ , and let  $\bar{g}_1, \dots, \bar{g}_n$  denote the corresponding basis of the reduction  $\bar{G} = U \oplus V$ . We now lift the hermitian form  $h \perp h'$  of  $\bar{G}$  to a hermitian form  $\psi$  of  $G$  by lifting the hermitian matrix of  $h \perp h'$  with respect to the basis  $\bar{g}_1, \dots, \bar{g}_n$  to a hermitian matrix over  $A$  in an arbitrary way. Let  $\Phi$  denote the restriction of  $\psi$  to  $E$ . Clearly,  $\Phi$  reduces mod  $\mathfrak{R}_A$  to the nondegenerate form  $h$  on  $U$ , hence  $\Phi$  itself is nondegenerate. Thus  $(E, \Phi)$  is a hermitian space over  $A$  that has mod  $\mathfrak{R}_A$  the reduction  $(U, h)$ .

*Remark* If  $A$  contains an element  $\mu$  with  $\mu + \bar{\mu} = 1$  (e.g., 2 is a unit in  $A$ ), then by well-known arguments any two hermitian spaces over  $A$  that have isometric reductions mod  $\mathfrak{R}_A$  are themselves isometric. Thus the canonical map from  $W(A)$  to  $W(\bar{A})$  is an isomorphism. We do not need this fact.

We now consider an arbitrary commutative ring  $A$  with involution and study the extension  $B = A[T]/(T^n)$  for some  $n \geq 2$ . We have

$$B = A \oplus At \oplus \cdots \oplus At^{n-1}, \quad t^n = 0,$$

and we extend  $J_A$  to an involution  $J_B$  on  $B$  by prescribing  $\bar{t} = t$ .

**Proposition 2.5** *The  $A$ -linear form  $s$  on  $B$  defined by*

$$s(1) = s(t) = \cdots = s(t^{n-2}) = 0, \quad s(t^{n-1}) = 1$$

*is a Frobenius form over  $A$ . Every signature  $\sigma$  on  $A$  has a unique extension  $\tau$  to  $B$  (cf. the preceding Lemma 2.4).  $n(\tau, s) = 1$  if  $n$  is odd, and  $n(\tau, s) = 0$  if  $n$  is even.*

*Proof* We have indeed  $s(\bar{x}) = \overline{s(x)}$  for  $x$  in  $B$ . If  $n = 2m + 1$ , the space  $s^*\langle 1 \rangle$  has the orthogonal decomposition

$$s^*\langle 1 \rangle = (At^m) \perp \bigoplus_{i=0}^{m-1} (At^i + At^{2m-i}).$$

Thus using an obvious notation

$$s^*\langle 1 \rangle \cong \langle 1 \rangle \perp m \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

If  $n = 2m$ , we have the orthogonal decomposition

$$s^*\langle 1 \rangle = \bigoplus_{i=0}^{m-1} (At^i + At^{2m-1-i})$$

and

$$s^*\langle 1 \rangle \cong m \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Thus on the Witt ring level  $s^*(1) = 1$  if  $n$  odd and  $s^*(1) = 0$  if  $n$  even. Let now  $\sigma$  be a signature on  $A$  and  $\tau$  be the unique extension of  $\sigma$  to  $B$ . By the transfer formula

$$n(\tau, s) = \sigma s_*(1) = \begin{cases} 1, & n \text{ odd} \\ 0, & n \text{ even.} \end{cases}$$

### 3. Integral Extensions of Semilocal Rings

We now assume that our ring with involution  $A$  is semilocal, i.e.,  $|A|$  has only finitely many maximal ideals. In this case there exists for every signature  $\sigma$  on  $A$  a prime ideal  $\mathfrak{p}(\sigma)$  of  $A$  intimately related to  $\sigma$ , whose definition and relevant properties I want to recall (cf. [7, I, §4 and Appendix B]).

Let  $A_0$  denote the fixed ring of  $J_A$ , equipped with the trivial involution. We introduce for  $\sigma$  a given signature on  $A$  the set  $\Gamma(\sigma)$  consisting of all units  $a$  of  $A_0$  with  $\sigma(a) = +1$ , and the set  $Q(\sigma)$  consisting of all finite sums

$$N(\lambda_1)a_1 + \cdots + N(\lambda_r)a_r,$$

with  $a_i$  in  $\Gamma(\sigma)$  and “norms”  $N(\lambda_i) = \lambda_i \bar{\lambda}_i$  of elements  $\lambda_i$  of  $A$  such that the ideal generated by  $\lambda_1, \dots, \lambda_r$  is the whole of  $A$ . Clearly  $Q(\sigma)$  is a multiplicative subsemigroup of  $A_0$ . Let  $-Q(\sigma)$  denote the set of all elements  $-x$  with  $x$  in  $Q(\sigma)$  and  $\mathfrak{p}(\sigma)_0$  the complement of  $Q(\sigma) \cup (-Q(\sigma))$  in  $A$ . The following facts have been proved in [7] and in a more special situation already by Kanzaki and Kitamura [6].

**P1**  $A_0$  is the disjoint union of  $Q(\sigma)$ ,  $-Q(\sigma)$ , and  $\mathfrak{p}(\sigma)_0$ .

**P2**  $\mathfrak{p}(\sigma)_0$  is a prime ideal of  $A_0$ .

**P3** The set of all  $x$  in  $A$  with  $N(x)$  lying in  $\mathfrak{p}(\sigma)_0$  is a prime ideal  $\mathfrak{p}(\sigma)$  of  $A$ , obviously stable under  $J_A$ , and this is the only prime ideal of  $A$  lying over  $\mathfrak{p}(\sigma)_0$ .

**P4** There exists a unique signature  $\bar{\sigma}$  on the quotient field  $A(\mathfrak{p}(\sigma))$  of the ring with involution  $A/\mathfrak{p}(\sigma)$  extending  $\sigma$  with respect to the natural map from  $A$  to  $A(\mathfrak{p}(\sigma))$ .

**P5**  $\mathfrak{p}(\sigma)$  contains every other prime ideal  $\mathfrak{q}$  of  $A$  such that  $\mathfrak{q}$  is stable under the involution of  $A$  and  $\sigma$  extends to some signature on  $A(\mathfrak{q})$ .

Let  $\sigma_0$  denote the restriction of  $\sigma$  to  $A_0$ . Since the natural map from  $W(A_0)$  to  $W(A)$  is surjective,  $\sigma$  is the only extension of  $\sigma_0$  to  $A$ . Clearly  $\Gamma(\sigma_0)$  coincides with  $\Gamma(\sigma)$ .

**P6**  $Q(\sigma_0)$  coincides with  $Q(\sigma)$  and  $\mathfrak{p}(\sigma_0)$  coincides with  $\mathfrak{p}(\sigma)_0$ . The natural map from  $A_0(\mathfrak{p}(\sigma_0))$  to  $A(\mathfrak{p}(\sigma))$  identifies  $A_0(\mathfrak{p}(\sigma_0))$  with the fixed field  $A(\mathfrak{p}(\sigma))_0$  of the involution of  $A(\mathfrak{p}(\sigma))$ . The signature  $\bar{\sigma}$  is the unique extension of  $\bar{\sigma}_0$  to  $A(\mathfrak{p}(\sigma))$ .

**P7**  $\Gamma(\bar{\sigma}_0)$  is the set of all fractions  $\bar{u}\bar{v}^{-1}$  with  $\bar{u}, \bar{v}$  the images in  $A_0/\mathfrak{p}(\sigma_0)$  of elements  $u, v$  of  $Q(\sigma)$ . Notice that  $\Gamma(\bar{\sigma}_0)$  is just the set of positive elements of the ordering of  $A_0(\mathfrak{p}(\sigma_0))$  corresponding to  $\bar{\sigma}_0$ .

**P8** Every element  $s$  of  $Q(\sigma)$  can be written in the form

$$s = a_1 + N(\lambda_2)a_2 + \cdots + N(\lambda_r)a_r$$

with  $a_1, \dots, a_r$  in  $\Gamma(\sigma)$  and  $\lambda_2, \dots, \lambda_r$  in  $A$ . (If  $A_0$  has no residue class fields with fewer than four elements, then even  $s = a_1 + a_2$  with  $a_1, a_2$  in  $\Gamma(\sigma)$ .)

**P9**  $\Gamma(\sigma)$  is the intersection of  $Q(\sigma)$  and the set  $A_0^*$  of units in  $A_0$ .

**P10**  $Q(\sigma) + \mathfrak{p}(\sigma)_0 = Q(\sigma)$ .

**P11** For  $x$  in  $A$  but  $x$  not in  $\mathfrak{p}(\sigma)$ , the norm  $N(x)$  lies in  $Q(\sigma)$ .

We call  $\mathfrak{p}(\sigma)$  (resp.  $\mathfrak{p}(\sigma)_0$ ) the *prime ideal* of  $A$  (resp. of  $A_0$ ) *associated* with  $\sigma$ .

Let now  $\varphi: A \rightarrow B$  be a homomorphism from  $A$  to another semilocal ring with involution  $B$ , and let  $\varphi_0: A_0 \rightarrow B_0$  denote the restriction of  $\varphi$  to the fixed rings of the involutions. Let further  $\tau$  be a signature on  $B$  and let  $\sigma$  denote the restriction  $\tau \circ \varphi_*$  of  $\tau$  to  $A$  with respect to  $\varphi$ .

**Theorem 3.1** *Assume  $\varphi$  is integral, i.e., every element of  $B$  is integral over the subring  $\varphi(A)$ . Then  $\mathfrak{p}(\sigma)$  is the preimage of  $\mathfrak{p}(\tau)$  under  $\varphi$ , and  $\mathfrak{p}(\sigma)_0$ , resp.  $Q(\sigma)$ , are the preimages of  $\mathfrak{p}(\tau)_0$ , resp.  $Q(\tau)$ , under  $\varphi_0$ .*

*Proof*  $\mathfrak{p}(\tau)$  is the unique prime ideal of  $B$  lying over  $\mathfrak{p}(\tau)_0$ , and  $\mathfrak{p}(\sigma)$  is the unique prime ideal of  $A$  lying over  $\mathfrak{p}(\sigma)_0$ . Thus it suffices to prove the statements about  $\mathfrak{p}(\sigma)_0 = \mathfrak{p}(\sigma_0)$  and  $Q(\sigma) = Q(\sigma_0)$ . Replacing  $\varphi$  by  $\varphi_0$ , we assume without loss of generality that  $A$  and  $B$  both have trivial involutions.

Without any assumption about  $\varphi$  it is clear that  $Q(\sigma)$  is contained in  $\varphi^{-1}Q(\tau)$  and  $-Q(\sigma)$  is contained in  $\varphi^{-1}(-Q(\tau))$ . Considering the complement of  $Q(\sigma) \cup (-Q(\sigma))$  in  $A$  we learn that  $\mathfrak{p}(\sigma)$  contains  $\varphi^{-1}\mathfrak{p}(\tau)$ . (This also follows from the fact that  $\sigma$  extends to a signature on  $B(\mathfrak{p}(\tau))$  with respect to the obvious map.) To finish the proof of the theorem it will suffice to show that  $Q(\sigma)$  coincides with  $\varphi^{-1}Q(\tau)$ . Indeed, considering again the complement of  $Q(\sigma) \cup (-Q(\sigma))$  in  $A$ , this will imply that also  $\mathfrak{p}(\sigma)$  coincides with  $\varphi^{-1}\mathfrak{p}(\tau)$ .

Suppose there exists an element  $t$  in  $\varphi^{-1}Q(\tau)$  that does not lie in  $Q(\sigma)$ . Clearly,  $t$  also does not lie in  $-Q(\sigma)$  since this set is contained in

$\varphi^{-1}(-Q(\tau))$ . Thus  $t$  must lie in  $\mathfrak{p}(\sigma)$ . On the other hand, we have an equation (cf. P8)

$$\varphi(t) = b_1 + \lambda_2^2 b_2 + \cdots + \lambda_r^2 b_r, \tag{*}$$

with  $b_1, \dots, b_r$  in  $\Gamma(\tau)$  and  $\lambda_2, \dots, \lambda_r$  in  $B$ .

We consider the field  $L := B(\mathfrak{p}(\tau))$ , equipped with the ordering corresponding to the signature  $\bar{\tau}$ . For  $b$  in  $B$ , we denote the natural image in  $L$  by  $\tilde{b}$ ; and for  $a$  in  $A$ , we denote the natural image of  $\varphi(a)$  in  $L$  also by  $\tilde{a}$  for conciseness. We now make the following observation. Let  $a$  be an arbitrary element of  $A$ . Then  $1 - at$  lies in  $Q(\sigma)$  since  $t$  lies in  $\mathfrak{p}(\sigma)$  (cf. P10). Thus  $1 - \varphi(at)$  lies in  $Q(\tau)$ , and the element  $1 - \tilde{a}\tilde{t}$  in  $L$  is positive. Now  $\tilde{b}_1 > 0$  and, according to (\*),  $\tilde{b}_1 \leq \tilde{t}$ . Thus we learn that

$$\tilde{a}\tilde{b}_1 < 1$$

for every  $a$  in  $A$ . Introducing the element  $d := b_1^{-1}$  of  $B_1$  we have

$$\tilde{a} < \tilde{d} \tag{**}$$

for every  $a$  in  $A$ . But this is impossible since  $B$  is integral over  $A$ . Indeed, we have an equation

$$d^n + \varphi(a_1)d^{n-1} + \cdots + \varphi(a_n) = 0$$

with some  $n \geq 1$  and elements  $a_i$  of  $A$ . This implies the equation

$$\tilde{d}^n + \tilde{a}_1 \tilde{d}^{n-1} + \cdots + \tilde{a}_n = 0. \tag{***}$$

Consider the element

$$c := 1 + \varepsilon_1 a_1 + \cdots + \varepsilon_n a_n$$

with  $\varepsilon_i = +1$  if  $\tilde{a}_i \geq 0$  and  $\varepsilon_i = -1$  if  $\tilde{a}_i < 0$ . Then in an obvious notation

$$\tilde{c} = 1 + |\tilde{a}_1| + \cdots + |\tilde{a}_n|.$$

By a well-known lemma the equation (\*\*\*) implies  $\dagger \tilde{d} \leq \tilde{c}$ , which contradicts (\*\*). Thus an element  $t$  as above cannot exist, and we have  $Q(\sigma) = \varphi^{-1}Q(\tau)$ . This finishes the proof of Theorem 3.1.

This theorem has the following consequence which is important in view of the preceding sections.

**Corollary 3.2** *We assume again that  $\varphi: A \rightarrow B$  is an integral homomorphism between semilocal rings, that  $\sigma$  is a signature on  $A$ , and  $\tau$  an extension of  $\sigma$  to  $B$ . Let  $\alpha$  be a homomorphism from  $A$  to a real closed field with involution  $R$  that induces  $\sigma$  and has kernel  $\mathfrak{p}(\sigma)$ . (Such a homomorphism clearly exists.) If the field  $L := B(\mathfrak{p}(\tau))$  has trivial involution or if the field  $K := A(\mathfrak{p}(\sigma))$  has nontrivial involution, then there exists a unique homomorphism  $\beta$  from  $B$  to  $R$*

$\dagger$  In fact,  $\tilde{d} \leq \text{Max}(1, |\tilde{a}_1| + \cdots + |\tilde{a}_n|)$ .

that extends  $\alpha$ , i.e.,  $\alpha = \beta \circ \psi$ , and induces  $\tau$ . In the remaining case that  $K$  has trivial involution but  $L$  has nontrivial involution there exist precisely two such homomorphisms  $\beta_1$  and  $\beta_2$ , and  $\beta_2 = J_R \circ \beta_1$ .

*Proof*  $\alpha$  factors through a unique homomorphism  $\bar{\alpha}$  from  $K$  to  $R$ , and  $\bar{\alpha}$  induces the signature  $\bar{\sigma}$  on  $K$ . The field  $L$  is an algebraic extension of  $K$  and the signature  $\bar{\tau}$  of  $L$  extends  $\bar{\sigma}$ . We want to investigate how many homomorphisms  $\beta$  from  $L$  to  $R$  exist that extend  $\bar{\alpha}$  and induce  $\bar{\tau}$ . This is possible by the classical Artin–Schreier theory of orderings and real closures.

Assume first that  $L$ , hence also  $K$ , has trivial involution. Then  $\bar{\alpha}$  maps  $K$  into the field  $R_0$  which is real, closed in the classical sense, and also  $\beta$  must have its image in  $R_0$ . By Artin–Schreier’s theory there exists a unique homomorphism  $\bar{\beta}$  from  $L$  to  $R_0$  that extends  $\bar{\alpha}$  and induces  $\bar{\tau}$ .

Assume now that  $K$ , hence also  $L$ , has nontrivial involution. Let  $\bar{\alpha}_0: K_0 \rightarrow R_0$  be the restriction of  $\bar{\alpha}$  to  $K_0$ . Again we have a unique homomorphism  $\bar{\beta}_0$  from  $L_0$  to  $R$  that extends  $\bar{\alpha}_0$  and induces the signature  $\bar{\tau}_0$  on  $L_0$  ( $\bar{\tau}_0 :=$  restriction of  $\bar{\tau} =$  signature induced on  $B_0(\mathfrak{p}(\tau_0))$  by  $\tau_0$ ). Now  $L$  is the tensor product of  $L_0$  and  $K$  over  $K_0$ . Thus there exists a unique homomorphism  $\bar{\beta}$  from  $L$  to  $R$  that extends both  $\bar{\alpha}$  and  $\bar{\beta}_0$ . The signature induced on  $L$  by  $\bar{\beta}$  extends  $\bar{\tau}_0$  and thus coincides with  $\bar{\tau}$ . Clearly  $\bar{\beta}$  is the unique homomorphism from  $L$  to  $R$  that extends  $\bar{\alpha}$  and induces  $\bar{\tau}$ .

Assume finally that  $K$  has trivial involution and  $L$  has nontrivial involution. We have a unique homomorphism  $\bar{\beta}_0$  from  $L_0$  to  $R$  that extends  $\bar{\alpha}$  and induces  $\bar{\tau}_0$ . There exist precisely two homomorphisms  $\bar{\beta}_1$  and  $\bar{\beta}_2$  from  $L$  to  $R$  that extend  $\bar{\beta}_0$  since  $L$  is a quadratic extension of  $L_0$  and  $|R|$  is algebraically closed, and  $\bar{\beta}_2 = J_R \circ \bar{\beta}_1$ . Both homomorphisms induce signatures on  $L$  that extend  $\bar{\tau}_0$ . Thus these signatures both coincide with  $\bar{\tau}$ .

In this way we have found the homomorphisms  $\bar{\beta}$  from  $L$  to  $R$  that induce  $\bar{\tau}$  and extend  $\bar{\alpha}$  in all cases. Composing these homomorphisms  $\bar{\beta}$  with the natural map from  $B$  to  $L$  we obtain all homomorphisms from  $B$  to  $R$  that have kernel  $\mathfrak{p}(\tau)$ , induce  $\tau$  on  $B$ , and extend  $\alpha$ .

To complete the proof of our corollary it remains to be shown that any homomorphism  $\beta$  from  $B$  to  $R$  that extends  $\alpha$  and induces  $\tau$  has kernel  $\mathfrak{p}(\tau)$ . Let  $\mathfrak{q}$  denote the kernel of  $\beta$ . Then  $\mathfrak{q}$  lies over the prime ideal  $\mathfrak{p}(\sigma)$  of  $A$ . Furthermore, we obtain from  $\beta$  a signature on  $B(\mathfrak{q})$  that extends  $\tau$ . Thus  $\mathfrak{q} \subset \mathfrak{p}(\tau)$ . Since also  $\mathfrak{p}(\tau)$  lies over  $\mathfrak{p}(\sigma)$  the prime ideals  $\mathfrak{p}(\tau)$  and  $\mathfrak{q}$  must be equal, according to a well-known theorem of Cohen–Seidenberg about prime ideals of integral extensions (e.g., [1, §2, 1, Corollary 2]).

From this Corollary 3.2, now proved, we obtain immediately

**Corollary 3.3** *Let  $\varphi: A \rightarrow B$  be a finite homomorphism between semilocal rings with involution, and assume that  $B$  can be generated as a module over  $A$  by  $n$  elements. Then an arbitrary signature on  $A$  has at most  $n$  extensions to  $B$ .*

Indeed, just observe that in the situation of Corollary 3.2 the homomorphisms from  $B$  to  $R$  that extend  $\alpha$  correspond one to one with the homomorphisms from  $B \otimes_A A(\mathfrak{p})$  to  $R$  that extend the homomorphism  $\bar{\alpha}$  from  $A(\mathfrak{p})$  to  $R$  induced by  $\alpha$ . The algebra  $B \otimes_A A(\mathfrak{p})$  has rank at most  $n$  over  $A(\mathfrak{p})$ .

If we study the extensions of a signature  $\sigma$  on  $A$  with respect to our integral homomorphism  $\varphi: A \rightarrow B$ , we may pass from  $A$  and  $B$  to their localizations with respect to  $\mathfrak{p}(\sigma)$ . This is a consequence of the following localization lemma.

**Lemma 3.4** *Let  $\sigma$  be a signature of the semilocal ring with involution  $A$ , and let  $S$  be a multiplicative subset (= subsemigroup) of  $Q(\sigma)$ . Assume that the localization  $S^{-1}A$  of  $A$  with respect to  $S$  is again semilocal. Then there exists a unique signature  $\bar{\sigma}$  of  $S^{-1}A$  extending  $\sigma$  with respect to the natural map from  $A$  to  $S^{-1}A$ . We have  $\mathfrak{p}(\bar{\sigma}) = S^{-1}\mathfrak{p}(\sigma)$ ,  $\mathfrak{p}(\bar{\sigma})_0 = S^{-1}\mathfrak{p}(\sigma)_0$ , and  $Q(\bar{\sigma}) = S^{-1}Q(\sigma)$ .*

*Proof* Since the natural map from  $A$  to  $A(\mathfrak{p}(\sigma))$  factors through the map from  $A$  to  $S^{-1}A$ , there exist extensions of  $\sigma$  to  $S^{-1}A$ . Let  $\tau$  be one of them. Clearly,  $S^{-1}\Gamma(\sigma)$  is contained in  $\Gamma(\tau)$ , hence  $S^{-1}Q(\sigma)$  is contained in  $Q(\tau)$ . Let  $u$  be a unit of the fixed ring  $S^{-1}A_0$  of the involution of  $S^{-1}A$ . The set  $S^{-1}A_0$  is the disjoint union of the prime ideal  $S^{-1}\mathfrak{p}(\sigma)_0$  and the sets  $\pm S^{-1}Q(\sigma)$ . Thus  $u$  lies in one of the sets  $\pm S^{-1}Q(\sigma)$ . According to Property P9, applied to  $\tau$ , we have  $\tau(u) = +1$  if  $u$  lies in  $S^{-1}Q(\sigma)$ , and  $\tau(u) = -1$  if  $u$  lies in  $-S^{-1}Q(\sigma)$ . Since  $\tau$  is determined by the values on the hermitian spaces of rank one [Knebusch *et al.* 10, Proposition 2.16], we see that  $\tau$  is the only signature of  $S^{-1}A$  extending  $\sigma$ .

We have a natural map from  $S^{-1}A$  to  $A(\mathfrak{p}(\sigma))$  that identifies the field  $A(\mathfrak{p}(\sigma))$  with the residue class field of  $S^{-1}A$  with respect to the prime ideal  $S^{-1}\mathfrak{p}(\sigma)$ . The restriction of the signature  $\bar{\sigma}$  on  $A(\mathfrak{p}(\sigma))$  to  $S^{-1}A$  is an extension of  $\sigma$  and thus coincides with  $\tau$ . This implies that  $S^{-1}\mathfrak{p}(\sigma)$  is contained in  $\mathfrak{p}(\tau)$ . We now know that  $S^{-1}\mathfrak{p}(\sigma)_0$  is contained in  $S^{-1}\mathfrak{p}(\tau)_0$  and from above that  $S^{-1}Q(\sigma)$  is contained in  $Q(\tau)$ . Since  $S^{-1}A_0$  is the disjoint union of the sets  $S^{-1}\mathfrak{p}(\sigma)_0$ ,  $\pm S^{-1}Q(\sigma)$ , and also the disjoint union of the sets  $\mathfrak{p}(\tau)_0$ ,  $\pm Q(\tau)$ , we have

$$S^{-1}\mathfrak{p}(\sigma)_0 = \mathfrak{p}(\tau)_0, \quad S^{-1}Q(\sigma) = Q(\tau).$$

It remains to be shown that  $S^{-1}\mathfrak{p}(\sigma)$  coincides with  $\mathfrak{p}(\tau)$ . Let  $x$  be an element of  $S^{-1}A$  that does not lie in  $S^{-1}\mathfrak{p}(\sigma)$ . Then  $x = s^{-1}y$  with  $s$  in  $S$  and  $y$  in  $A$  but  $y$  not in  $\mathfrak{p}(\sigma)$ . According to Property P11, the norm  $N(y)$  lies in  $Q(\sigma)$ , hence  $N(x)$  lies in  $S^{-1}Q(\sigma)$ , which coincides with  $Q(\tau)$ . Thus, again by P11,  $x$  does not lie in  $\mathfrak{p}(\tau)$ , and we see that the subset  $S^{-1}\mathfrak{p}(\sigma)$  of  $\mathfrak{p}(\tau)$  actually coincides with  $\mathfrak{p}(\tau)$ . This finishes the proof of Lemma 3.4.

**Proposition 3.5** (i) *Let  $\varphi: A \rightarrow B$  be a finite homomorphism between semilocal rings with involution. Let  $\sigma$  be a signature on  $A$  and let  $\mathfrak{p}$  denote the associated prime ideal  $\mathfrak{p}(\sigma)$ . Then  $\sigma$  has a unique extension  $\bar{\sigma}$  to  $A_{\mathfrak{p}}$ , and every*

extension  $\tau$  of  $\sigma$  to  $B$  has a unique extension  $\tilde{\tau}$  to  $B_{\mathfrak{p}}$ . Thus we have a one-to-one correspondence between the extensions of  $\sigma$  to  $B$  and the extensions of  $\tilde{\sigma}$  to  $B_{\mathfrak{p}}$ .

(ii) The set  $Q(\tilde{\tau})$  consists of the elements  $uv^{-1}$  with  $u$  in  $Q(\tau)$  and  $v$  in  $Q(\sigma)$ , and  $\mathfrak{p}(\tilde{\tau})$  is the localization  $\mathfrak{p}(\tau)B_{\mathfrak{p}}$  of  $\mathfrak{p}(\tau)$ .

(iii) Assume that in addition  $\varphi$  is a Frobenius extension and that  $s$  is a Frobenius form on  $B$  over  $A$ . Let  $\tilde{s}: B_{\mathfrak{p}} \rightarrow A_{\mathfrak{p}}$  denote the induced Frobenius form on  $B_{\mathfrak{p}}$  over  $A_{\mathfrak{p}}$ . Then  $n(\tau, s) = n(\tilde{\tau}, \tilde{s})$  for every extension  $\tau$  of  $\sigma$  to  $B$ .

*Proof* Parts (i) and (ii) of the proposition follow from the preceding lemma, applied to both  $A$  and  $B$  and the multiplicative set  $S := Q(\sigma)$ . Indeed, by Property P11 we have  $S^{-1}A = A_{\mathfrak{p}}$  and  $S^{-1}B = B_{\mathfrak{p}}$ . Notice that  $S$  is contained in  $Q(\tau)$  for every extension  $\tau$  of  $\sigma$  to  $B$ .

Assume now that  $s: B \rightarrow A$  is a Frobenius form over  $A$ . For  $y$  in  $W(A)$ , we denote the image in  $W(A_{\mathfrak{p}})$  by  $\tilde{y}$  and for  $z$  in  $W(B)$  the image in  $W(B_{\mathfrak{p}})$  by  $\tilde{z}$ . We have

$$\sigma s^*(z) = \tilde{\sigma}(s^*(z)) \sim \tilde{\sigma}(\tilde{s}^*(\tilde{z})) = \sum_{\tau|\sigma} n(\tilde{\tau}, \tilde{s}) \tilde{\tau}(\tilde{z}) = \sum_{\tau|\sigma} n(\tilde{\tau}, \tilde{s}) \tau(z).$$

Thus indeed  $n(\tilde{\tau}, \tilde{s}) = n(\tau, s)$  for all signatures  $\tau$  on  $B$  extending  $\sigma$ .

**Example 3.6** Assume in the situation of part (iii) of the preceding proposition that  $B_{\mathfrak{p}}$  is finite etale over  $A_{\mathfrak{p}}$ . Then  $n(\tau, s) \neq 0$  for every signature  $\tau$  on  $B$  extending  $\sigma$ . More precisely,  $|n(\tau, s)| = 2$  if  $A(\mathfrak{p}(\sigma))$  has trivial involution and  $B(\mathfrak{p}(\tau))$  has nontrivial involution, and  $|n(\tau, s)| = 1$  otherwise.

This follows from our Proposition 3.5 using (1.5) and the determination of the multiplicities  $n(\tau)$  for finite etale extensions of semilocal rings in [7, II, Proposition 8.5]. (In [7] it is assumed that  $A$  and  $B$  are connected. This restriction can be removed easily in our situation.)

Our theory of prime ideals associated with signatures on semilocal rings and the consequences drawn from this theory in the present section immediately generalize to “weakly semilocal rings” as considered in [7]. I call a ring  $A$  with involution *weakly semilocal* if  $A$  contains a semilocal ring  $A'$  (stable under the involution) such that  $A$  is integral over  $A'$ . Then  $A$  is the limit of an inductive system of semilocal rings with involution with finite transition morphisms. Weakly semilocal rings with involution are a more natural category for the present section than semilocal rings with involution since an integral extension of a weakly semilocal ring is again weakly semilocal.

#### 4. Frobenius Extensions with One Generator

Let  $A$  be a commutative ring with involution.

**Proposition 4.1** *Assume  $B$  is a Frobenius extension of  $A$  generated by one*

element  $\vartheta$ ;  $B = A[\vartheta]$ . Let  $\sigma$  be a signature on  $A$  and  $\alpha$  a homomorphism from  $B$  to a real closed field with involution  $R$  inducing  $\sigma$ . Then for any extension  $\tau$  of  $\sigma$  to  $B$  and any Frobenius form  $s$  on  $B$  over  $A$ , we have

$$|n(\tau, s)| \leq n(\tau, \alpha)$$

with  $n(\tau, \alpha)$  denoting the number of homomorphisms  $\beta$  from  $B$  to  $R$  that extend  $\alpha$  and induce  $\tau$ .

This is an improvement of a previous inequality (1.4). To prove the proposition we run through the proof of Theorem 1.1, and we see that it suffices to show that for the Frobenius extensions  $B_i$  of  $R$  ( $1 \leq i \leq r$ ) occurring there we have  $\rho s_i^*(1) = 0$  or  $= \pm 1$ . Now every  $B_i$  is generated over  $R$  by one element. Thus our proposition is evident if we verify the following lemma.

**Lemma 4.2** *Let  $B$  be a finite extension of a real closed field with involution  $R$ , and assume that  $B$  is generated over  $R$  by one element. Then  $B$  is a Frobenius extension of  $R$ . For any Frobenius form  $s$  on  $B$  we have  $s^*(1) = \pm 1$  if  $[B : R]$  is odd and  $s^*(1) = 0$  if  $[B : R]$  is even.*

*Proof*  $B = R \oplus N$  with  $N$  the nil radical of  $B$ . We assume  $N \neq 0$ . Let  $\vartheta$  be a generator of  $B$  over  $R$ . We have  $\vartheta = c + u$  with  $c$  in  $R$ ,  $u$  in  $N$ , and  $u$  is again a generator of  $B$ . Let  $n$  denote the smallest natural number with  $u^n = 0$  ( $n \geq 2$ ). Then  $1, u, \dots, u^{n-1}$  is a basis of  $B$  over the field  $R$ . Clearly

$$\bar{u} = u(\lambda + v)$$

with  $\lambda$  in  $R$ ,  $\lambda \neq 0$ , and  $v$  in  $N$ . Denoting the unit  $\lambda + v$  by  $\varepsilon$  we have  $\varepsilon\bar{\varepsilon} = 1$  since  $\bar{u} = u$ . There exists an element  $\mu$  in  $R$  such that  $\mu + \lambda\bar{\mu} \neq 0$ . Then  $\beta := \mu + \varepsilon\bar{\mu}$  is a unit of  $B$ , and  $\bar{\beta} = \varepsilon\beta$ . (This is the classical procedure for solving the equation  $\varepsilon = \beta\bar{\beta}^{-1}$ .) Introducing the element  $t := \beta u$ , we have  $\bar{t} = t$ , and  $1, t, \dots, t^{n-1}$  is again a basis of  $B$  over  $R$ . We introduce the  $R$ -linear form  $s$  on  $B$  with

$$s(1) = \dots = s(t^{n-2}) = 0, \quad s(t^{n-1}) = 1.$$

According to Proposition 2.5 this form is a Frobenius form and  $s^*(1) = 1$  if  $n$  is odd,  $s^*(1) = 0$  if  $n$  is even. If  $s'$  is another Frobenius form on  $B$ , then  $s'^*(1) = \pm s^*(1)$  (cf. end of Section 1). This finishes the proof of the lemma.

As a relevant example we consider an extension

$$B = A[T]/f(T)$$

with  $f(T)$  a normed polynomial in  $A_0[T]$  of degree  $n \geq 2$ . Let  $t$  denote the image of  $T$  in  $B$ . Then  $1, t, \dots, t^{n-1}$  is a free basis of the  $A$ -module  $B$ . We extend the involution  $J_A$  to  $B$  prescribing  $\bar{t} = t$ . We consider the  $A$ -linear

form  $s$  on  $B$  defined by

$$s(1) = s(t) = \cdots = s(t^{n-2}) = 0, \quad s(t^{n-1}) = 1.$$

The hermitian matrix of the hermitian form  $s(\bar{x}y)$  with respect to our basis  $1, t, \dots, t^{n-1}$  has the shape

$$\begin{bmatrix} & & & & 1 \\ & 0 & & & \\ & & \ddots & & \\ & 1 & & & * \\ 1 & & & & \end{bmatrix}$$

and thus is nonsingular, hence  $s$  is a Frobenius form.

We now assume in addition that  $A$  is semilocal. Let  $\sigma$  be a signature on  $A$ , and let  $\mathfrak{p}$  respectively  $\mathfrak{p}_0$  denote the prime ideal of  $A$ , resp.  $A_0$ , associated with  $\sigma$ . Let further  $K$  denote the residue class field  $A(\mathfrak{p})$ , and as always let  $K_0$  denote the fixed field of the involution  $J_K$ , which coincides with  $A_0(\mathfrak{p}_0)$ . The image  $\bar{f}(T)$  of our polynomial  $f(T) \in A_0[T]$  in  $K_0[T]$  has a decomposition

$$\bar{f}(T) = \prod_{i=1}^s \bar{p}_i(T)^{e_i}$$

with pairwise different normed irreducible polynomials  $\bar{p}_i(T)$  over  $K_0$ . Let  $\tau$  be a signature on  $B$  extending  $\sigma$ . Then  $\mathfrak{p}(\tau)_0$  is a prime ideal of  $B_0$  lying over  $\mathfrak{p}_0$  and thus

$$\mathfrak{p}(\tau)_0 = \mathfrak{p}_0 B_0 + p_j(T) B_0$$

with  $j$  uniquely determined by  $\tau$ ,  $1 \leq j \leq s$ , and  $p_j(T)$  a preimage of  $\bar{p}_j(T)$  in  $A_0[T]$ . Since  $\mathfrak{p}(\tau)$  is the unique prime ideal of  $B$  lying over  $\mathfrak{p}(\tau)_0$ , the polynomial  $\bar{p}_j(T)$  remains irreducible over  $K$ , and

$$\mathfrak{p}(\tau) = \mathfrak{p}B + p_j(T)B.$$

We call  $\bar{p}_j(T)^{e_j}$  the factor of  $f(T)$  corresponding to  $\tau$ .

**Proposition 4.3** *Let  $\bar{p}_j(T)^{e_j}$  be the factor of  $\bar{f}(T)$  corresponding to  $\tau$ . Then  $n(\tau, s) = \pm 1$  if  $e_j$  is odd and  $n(\tau, s) = 0$  if  $e_j$  is even.*

*Proof* We choose a homomorphism  $\alpha$  from  $A$  to a real, closed field with involution  $R$  that has kernel  $\mathfrak{p}(\sigma)$  and induces  $\sigma$ . There exist either one homomorphism  $\beta$  or two homomorphisms  $\beta, \beta'$  from  $B$  to  $R$  which extend  $\alpha$ , and in the second case  $\beta' = J_R \circ \beta$  (cf. Corollary 3.2). Let  $\lambda$  denote the image of  $t$  under  $\beta$  in both cases. Then  $\bar{\lambda} = \lambda$ , and  $\lambda$  is a zero of the polynomial  $\bar{p}_j[T]$  obtained from  $p_j(T)$  by applying  $\alpha$  to the coefficients since  $\beta$  factors through  $B(\mathfrak{p}(\tau))$ . Going through the proof of Theorem 1.1, we see that with the

notations introduced there

$$B(\tau) = R[T]/(T - \lambda)^{e_j}.$$

Our proposition now follows from Lemma 4.2 or already from Proposition 2.5.

It would be more difficult to determine the sign of  $n(\tau, s)$  if  $e_j$  were odd. We do not enter into this.

#### REFERENCES

- [1] N. Bourbaki, "Algèbre commutative," Chap. V. Hermann, Paris, 1964.
- [2] T. C. Craven, A. Rosenberg, and R. Ware, The map of the Witt ring of a domain into the Witt ring of its field of fractions, *Proc. Amer. Math. Soc.* **51** (1975), 25–30.
- [3] A. Dress, The weak local global principle in algebraic K-theory, *Comm. Algebra* **3** (1975), 615–661.
- [4] S. Eilenberg and T. Nakayama, On the dimension of modules and algebras II (Frobenius algebras and quasi-Frobenius rings), *Nagoya Math. J.* **9** (1959), 1–16.
- [5] D. K. Harrison, "Witt rings." Lecture Notes, Dept. of Math., University of Kentucky, Lexington, 1970.
- [6] T. Kanzaki and K. Kitamura, On prime ideals of a Witt ring over a local ring, *Osaka J. Math.* **9** (1972), 225–229.
- [7] M. Knebusch, Real closures of commutative rings I, *J. Reine Angew. Math.* **274/275** (1975), 61–89; II, *J. Reine Angew. Math.* **286/287** (1976), 278–313.
- [8] M. Knebusch, Generalization of a theorem of Artin-Pfister to arbitrary semilocal rings, and related topics, *J. Algebra* **36** (1975), 46–67.
- [9] M. Knebusch, Remarks on the paper "Equivalent topological properties of the space of signatures of a semilocal ring" by A. Rosenberg and R. Ware, *Publ. Math. Debrecen*, to appear.
- [10] M. Knebusch, A. Rosenberg, and R. Ware, Signatures on semilocal rings, *J. Algebra* **26** (1973), 208–250.
- [11] F. Lorenz and J. Leicht, Die Primideale des Wittschen Ringes, *Invent. Math.* **10** (1970), 82–88.
- [12] W. Scharlau, Zur Pfisterschen Theorie der quadratischen Formen, *Invent. Math.* **6** (1969), 327–328.
- [13] R. G. Swan, "Algebraic K-theory," Lecture Notes Math. 76, Springer-Verlag, Berlin-Heidelberg-New York, 1969.
- [14] G. E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, *J. Austral. Math. Soc.* **3** (1963), 1–62.

AMS (MOS) 1970 subject classification: 18F25.