Journal für die reine und angewandte Mathematik
Herausgegeben von Helmut Hasse und Hans Rohrbach
Sonderdruck aus Band 274/275, Seite 61 bis 89
Verlag Walter de Gruyter · Berlin · New York 1975

Real closures of commutative rings*). I

By *Manfred Knebusch* at Regensburg

Dedicated to Helmut Hasse on his 75th birthday

Introduction

Let A be a connected commutative ring with 1, and let $\bar{A}$ denote the universal covering (= separable closure) of A in the sense of Galois theory (cf. e. g. [8]). The main goal of the present paper is to give a contribution to the following problem: Classify all coverings $B \subset \bar{A}$ of A (= direct limits of finite etale connected extensions of A), such that $1 < [\bar{A} : B] < \infty$. For A a field a complete answer to this problem has been given by Artin and Schreier [2], [3]: For every such covering B we have $[\bar{A} : B] = 2$, and B is a real closure of A with respect to an ordering of A. In this way the isomorphy classes of coverings B of A with $1 < [\bar{A} : B] < \infty$ correspond uniquely to the orderings of A.

To generalize Artin-Schreier's theory to rings we have to find a suitable substitute for the orderings of a field. To my firm conviction this substitute are the signatures. A *signature* σ of the ring A is defined as a homomorphism from the Witt ring $W(A)$ of symmetric inner product spaces over A [20] to the ring $\mathbb{Z}$ of integers. This definition is motivated by a result due to Harrison [10] and Leicht-Lorenz [19], which says that for A a field the signatures of A correspond uniquely to the orderings of A. The value of the signature σ corresponding to a given ordering on a inner product space E is Sylvester's index of inertia of E with respect to the ordering, i. e. the number of positive coefficients minus the number of negative coefficients in an arbitrarily chosen diagonalization of E.

Thus we consider pairs (A, σ) consisting of a connected commutative ring A and a signature σ of A. There is an evident notion of morphism $\varphi : (A, \sigma) \to (B, \tau)$ between pairs (cf. § 2), which for A and B fields just means, that φ is a homomorphism from A to B compatible with the orderings corresponding to σ and τ. We call φ a *covering*, if the ring homomorphism $\varphi : A \to B$ is a covering. We further call a pair (R, ϱ) *real closed*, if (R, ϱ) does not admit coverings except isomorphisms. Finally we call a covering $\alpha : (A, \sigma) \to (R, \varrho)$ with (R, ϱ) real closed a *real closure* of the pair (A, σ). Using Zorn's lemma, it is easily seen that every pair (A, σ) has at least one real closure.

Let $\alpha : (A, \sigma) \to (R, \varrho)$ denote a fixed real closure of (A, σ). We shall prove in § 3 and § 5 the following two general theorems:

(0. 1) *Any other real closure of* (A, σ) *is isomorphic to* α *over* A[1]).

*) A part of the results of this paper has been announced in [13].

[1]) In the case of fields a proof of (0. 1) by the methods of this paper is already contained in [14].

(0. 2) $[\bar{A} : R] \leqq 2$. *If some prime number p is a unit in A, then* $[\bar{A} : R] = 2$. *Furthermore in the case that* 2 *is a unit,* $\bar{A} = R[\sqrt{-1}]$.

In part II of this paper we shall see, that the real closures of a local ring A have nearly all the pleasant properties discovered by Artin and Schreier in the case of fields:

(0. 3) *ϱ is the unique signature of R. Furthermore $W(R) = \mathbb{Z}$ if in addition 2 is a unit in R. This is generally false if 2 is not a unit. But the Witt ring $W(\bar{A}, J)$ of hermitian inner product spaces over $\bar{A}$ with respect to the involution $J \neq \mathrm{id}$ of $\bar{A}/R$ always equals $\mathbb{Z}$. Thus our signature σ may be identified with the canonical map from $W(A) = W(A, \mathrm{id})$ to $W(\bar{A}, J)$.*

(0. 4) *R has no automorphisms over A except the identity.*

(0. 5) *The signatures σ of A correspond uniquely to the conjugacy classes of involutions $J \neq \mathrm{id}$ in the Galois group of $\bar{A}/A$, the fixed ring of such an involution J being a real closure of (A, σ).*

Slightly more generally the results (0. 3) (0. 4) and probably also (0. 5) remain true for A semi-local. I further obtained much evidence, that for A semi-local indeed all coverings B of A with $1 < [\bar{A} : B] < \infty$ are real closures of A.

Basic tools to prove the results (0. 1)—(0. 5) are provided by two papers [16], [17] written jointly with A. Rosenberg and R. Ware, and by an important theorem of A. Dress (see Theorem 2. 1 in § 2). In particular, the statement (0. 4) follows almost immediately from (0. 3) and the arguments in the proof of Proposition 4. 8 of [17].

The result (0. 3) strongly suggests to study more generally rings A equipped with involutions J_A (which are allowed to be the identity). This will be done in this paper. In § 1 we develop a theory of coverings for such rings and more generally without additional work for rings on which an arbitrary fixed finite group π is acting. Signatures and real closures can be defined for connected rings with involution in an analogous way as above, and results similar to (0. 1)—(0. 5) will be proved.

If A is a ring with $J_A = \mathrm{id}$, and σ is a signature of A, then we call, since now, a real closure of (A, σ) in the category of rings without involution, as defined above, a *strict real closure* of (A, σ), and we reserve the notion "real closure" to the maximal coverings of (A, σ) in the category of rings with involution. These notions are closely related: Let $\bar{A}$ denote as before the universal covering of A in the category of rings without involution, and let (R, ϱ) be a strict real closure of (A, σ). In the case $[\bar{A} : R] = 1$ the pair (R, ϱ) is also a real closure of (A, σ) $\{J_R = \mathrm{id}\}$. In the case $[\bar{A} : R] = 2$ a real closure of (A, σ) is given by the ring $\bar{A}$ equipped with the automorphism $J \neq \mathrm{id}$ of $\bar{A}/R$ as involution and a suitable signature of $(\bar{A}, J)$.

We call the involution J_A *non degenerate*, if A is finite etale of degree two over the ring A_0 of fixed elements of J_A. We shall prove in § 6 the rather surprising fact, that for a connected ring A equipped with an arbitrary involution and an arbitrary signature σ a real closure of (A, σ) has a *non degenerate* involution, if at least one prime number p is a unit in A.

If $J_A = \mathrm{id}$ or J_A is non degenerate, then the theory of real closures of A can be reduced to the theory of strict real closures of A_0. For A a field we always meet one of these cases. Thus it is reasonable from our point of view, that Artin and Schreier never studied fields with involution.

I wish to thank A. Dress, A. Rosenberg, and R. Ware for discussions and letters which have proved to be helpful for the theory presented here. The experienced reader will perceive the close connections between the methods used in this paper and Dress' theory of Mackey-functors, in particular in Section 3.

§ 1. Equivariant coverings

We study commutative rings (with 1) on which a fixed finite group π acts from the left by ring automorphisms. Such rings will be called π-rings. For our applications in this paper only the case $\pi = \mathbb{Z}/2\mathbb{Z}$ is needed, but the purely formal study of this section does not present serious additional difficulties for arbitrary finite π, and could equally well be done for schemes. All propositions of this section are well known in the case $\pi = 1$.

A homomorphism $\varphi: A \to B$ from a π-ring A to a π-ring B is of course an ordinary ring homomorphism, mapping 1 to 1, which is compatible with the π-actions. The homomorphism φ is called *finite etale*, if φ is finite etale as an ordinary ring homomorphism ([9], § 18. 3). A π-ring A is called *connected*, if A does not contain any idempotent different from 0 and 1 which is invariant under π. Assume A is connected. Then clearly A has only finitely many primitive idempotents $e_1, \ldots, e_r$, on which π acts transitively. Assume in addition that $\varphi: A \to B$ is a finite etale homomorphism into a π-ring B. Then the projective module $B\varphi(e_i)$ over Ae_i has for every e_i constant rank, since Ae_i is a connected ring in the ordinary sense. Since π acts transitively on the e_i, these ranks are all equal. Thus the ring B without π-action, which is denoted by $|B|$, is a projective module of constant rank over $|A|$. This rank will be denoted by $[B:A]$ and will be called the *degree* of the finite etale homomorphism φ. Notice that in the case $[B:A] > 0$, i. e. $B \neq 0$, the map φ must be injective. Unless the contrary is explicitly stated, we assume since now in this paper, that all occurring rings are $\neq 0$.

An idempotent e of a π-ring A will be called a *π-idempotent*, if e is invariant under π, and a π-idempotent $e \neq 0$ will be called *π-primitive*, if e is not the sum of two orthogonal π-idempotents e_1 and e_2 which are both $\neq 0$. In this paper only π-rings A will occur with $|A|$ containing only finitely many idempotents. Let $\{e_1, \ldots, e_t\}$ be the set of π-primitive π-idempotents of A. We call the π-rings $A_i := Ae_i$ the *components* of A (and regard them as subsets of A). Clearly A is the direct product $\prod_{i=1}^{t} A_i$ of the A_i in the category of π-rings, the projections $p_i: A \to A_i$ being defined by $p_i(a) = ae_i$.

For two π-homomorphisms $\varphi: A \to B$ and $\alpha: A \to C$ the *tensor product* $B \otimes_A C$ with respect to φ and α is defined as the usual tensor product $|B| \otimes_{|A|} |C|$, equipped with the π-action $g(b \otimes c) = (gb) \otimes (gc)$ for g in π. We denote the π-homomorphism $B \to B \otimes_A C$, $b \mapsto b \otimes 1$, by $1 \otimes \alpha$ and the π-homomorphism $C \to B \otimes_A C$, $c \mapsto 1 \otimes c$, by $\varphi \otimes 1$. The commutative diagram

$$\text{(1. 0)} \qquad \begin{array}{ccc} B & \xrightarrow{1\otimes\alpha} & B \otimes C \\ \uparrow{\scriptstyle\varphi} & & \uparrow{\scriptstyle\varphi\otimes 1} \\ A & \xrightarrow{\alpha} & C \end{array}$$

is a pushout in the category of π-rings.

Let A be a connected π-ring. We call a π-homomorphism $\varphi: A \to B$ a *finite covering*, if φ is finite etale, the π-ring B is connected, and $B \neq 0$.

Lemma 1. 1. *Let $\varphi : A \to B$ and $\beta : B \to C$ be homomorphisms between connected π-rings A, B, C. Assume φ and $\beta \circ \varphi$ are finite coverings. Then also β is a finite covering.*

Proof. Consider the diagram (1. 0) with $\alpha := \beta \circ \varphi$. Here $B \otimes C$ is a finite product $\prod_{i=1}^{r} E_i$ of connected φ-rings E_i. Let $\alpha_1, \ldots, \alpha_r$ denote the components of $1 \otimes \alpha$ and $\varphi_1, \ldots, \varphi_r$ denote the components of $\varphi \otimes 1$. Since $1 \otimes \alpha$ and $\varphi \otimes 1$ are finite etale, all α_i and φ_j are coverings. By the pushout property of our diagram there exists a unique homomorphism μ from $B \otimes C$ to C with $\mu \circ (\varphi \otimes 1) = \mathrm{id}_C$ and $\mu \circ (1 \otimes \alpha) = \beta$. Since C is connected and $\neq 0$, the homomorphism μ maps all π-primitive π-idempotents of $B \otimes C$ to 0 except one. Thus μ factors through a unique canonical projection $p_i : B \otimes C \to E_i$, $\mu = \gamma \circ p_i$. From $\mu \circ (\varphi \otimes 1) = \mathrm{id}_C$ we obtain $\gamma \circ \varphi_i = \mathrm{id}_C$. This implies in particular, that the kernel of $\gamma : E_i \to C$ is generated by an idempotent ([8], p. 96), which must be invariant under π. Since E_i is connected this idempotent must be 0, i. e. γ is injective. Thus we see that γ is an isomorphism. Since $\beta = \gamma \circ p_i \circ (1 \otimes \alpha) = \gamma \circ \alpha_i$ and α_i is a finite covering, also β is a finite covering.

We call a homomorphism $\varphi : A \to B$ from a connected π-ring A to a π-ring B a *covering*, if φ is the direct limit of a direct system $(\varphi_i : A \to B_i, \psi_{ij}, i, j \in I)$ of finite coverings. By Lemma 1. 1 then also all $\psi_{i,j} : B_i \to B_j$ are coverings, and in particular injective. Thus the canonical maps $\psi_i : B_i \to B$ from the B_i into the direct limit B are injective, B is connected, and $\varphi : A \to B$ is injective. Regarding B as an overring of A we can say more simply that an injection $A \to B$ is a covering, if every finite subset of B is contained in a ring B' with $A < B' < B$ and $A \hookrightarrow B'$ a finite covering.

Proposition 1. 2. *The composite $\psi \circ \varphi$ of two coverings $\varphi : A \to B$ and $\psi : B \to C$ is again a covering.*

Proof. We regard φ and ψ as inclusion maps. It suffices to show that for every finite subcovering $B \hookrightarrow C'$ of $B \hookrightarrow C$ the composite $A \hookrightarrow C'$ is a covering. Thus we may assume that C is finite over B. It is not difficult to show, that there exists a finite subcovering $A \hookrightarrow B'$ of $A \hookrightarrow B$ and a finite covering $\chi : B' \to D$, such that $1 \otimes \chi : B \to B \otimes_{B'} D$ is a covering of B isomorphic to $B \hookrightarrow C$. But $(1 \otimes \chi) \circ \varphi$ can also be written as the composite

$$A \hookrightarrow B' \xrightarrow[\chi]{} D \xrightarrow[i \otimes 1]{} B \otimes_{B'} D$$

with i the inclusion map from B' to B. Now $i : B' \hookrightarrow B$ is the direct limit of inclusion maps $j : B' \hookrightarrow B''$ with $A \hookrightarrow B''$ finite coverings. By Lemma 1. 1 each $j : B' \hookrightarrow B''$ is a finite covering. $(1 \otimes \chi) \circ \varphi$ is the direct limit of the finite coverings

$$A \hookrightarrow B' \xrightarrow[\chi]{} D \xrightarrow[j \otimes 1]{} B'' \otimes_{B'} D.$$

Thus $(1 \otimes \chi) \circ \varphi$ is a covering of A, hence also $\psi \circ \varphi$.

Proposition 1. 3. *Assume $\varphi : A \to B$ and $\alpha : A \to C$ are coverings of a connected π-ring A. Then every homomorphism $\beta : B \to C$ with $\beta \circ \varphi = \alpha$ is also a covering.*

Proof. This had been stated for α and φ finite already in Lemma 1. 1. We regard C as an overring of A and α as the inclusion map from A to C.

i) The assertion is true if φ is a finite covering. Indeed, C is the union of a directed system $(C_i, i \in I)$ of subrings containing $\varphi(B)$ such that all $A \hookrightarrow C_i$ are finite coverings. By Lemma 1. 1 the maps $B \to C_i$ induced by β are also finite coverings. Thus β is a covering.

ii) In the general case the map β is certainly injective. For we can write B as a union of a directed system $(B_j, j \in J)$ of subrings containing $\varphi(A)$ such that all maps $A \to B_j$ induced by φ are finite coverings. By part i) of our proof all restrictions $\beta \mid B_j$ are coverings and hence injections. Thus β is injective.

iii) We now prove the proposition in the general case. We choose a directed system $(C_i, i \in I)$ of subrings of C containing A such that all inclusions $A \hookrightarrow C_i$ are finite coverings. Let D_i denote the ring generated by $\beta(B)$ and C_i in C. We shall show that for every $i \in I$ the homomorphism $B \to D_i$ induced by β is a finite covering. Then it will be clear that β is a covering. We fix some C_i and call it C', and we denote the corresponding D_i by D'. The tensor product $B \otimes_A C'$ is finite etale over B, and thus is a finite product $\prod_{j=1}^{t} E_j$ of connected π-rings E_j. Let $\varphi_1, \ldots, \varphi_t$ denote the components of $\varphi \otimes 1 : C' \to B \otimes C'$, and let $\gamma_1, \ldots, \gamma_t$ denote the components of the canonical map from B to $B \otimes C'$. The γ_i are finite coverings. By the pushout property of $B \otimes_A C'$ we obtain from $\beta : B \to C$ and from the inclusion map $C' \hookrightarrow C$ a map $B \otimes_A C' \to C$, whose image in C is clearly D'. The corresponding map $\tilde{\delta} : B \otimes_A C' \to D'$ must factor through a canonical projection $B \otimes_A C' \twoheadrightarrow E_j$ for a unique j with $1 \leqq j \leqq t$. We denote the map from E_j to D' corresponding to $\tilde{\delta}$ by δ, and obtain a commutative diagram

$$\begin{tikzcd}
& & & C \\
B \arrow[r, "\gamma_j"] & E_j \arrow[r, two heads, "\delta"] & D' \arrow[ur, hook] & \\
A \arrow[u, "\varphi"] \arrow[r, hook] & C' \arrow[u, "\varphi_j"] \arrow[ur, hook] & &
\end{tikzcd}$$

φ is a covering and γ_j is a finite covering. Since also $A \hookrightarrow C'$ is a finite covering we obtain from Proposition 1. 2 and part i) of the proof that φ_j is a covering. Since $C' \hookrightarrow C$ is a covering we further obtain from part ii) of our proof that δ is injective. Thus δ is an isomorphism. The map $B \to D'$ induced by β is clearly $\delta \circ \gamma_j$. It is a finite covering.

We call a π-ring C *simply connected*, if C is connected and every covering of C is an isomorphism. We further call any covering $\varphi : A \to C$ of a connected π-ring A with C simply connected a *universal covering* of A.

Lemma 1. 4. *Assume C is a connected π-ring which neglecting the π-action has a decomposition $|C| = C_1 \times \cdots \times C_n$ with n the order of π and thus all C_i connected. Assume all C_i are simply connected in the usual sense (= "separably closed" in* [8]*). Then C is simply connected.*

Proof. Let $\varphi : C \to D$ be a finite covering, and let $e_1, \ldots, e_n$ be the primitive idempotents of C. The homomorphism φ induces finite etale homomorphisms $\varphi_i : C e_i \to D\varphi(e_i)$ of rings without π-action. All $\varphi(e_i)$ are $\neq 0$ and thus all $D\varphi(e_i)$ must be connected, since otherwise D would contain more than n primitive idempotents. Since $C e_i \cong C_i$ is simply connected, every φ_i is bijective. Thus φ is bijective.

Proposition 1. 5. *Every connected π-ring A has universal coverings.*

We prove this now only in the special case that π is a group $\{1, J\}$ with 2 elements, sufficient for our applications. The general case will be settled in an appendix of this paper[2]). Consider first the case that $|A|$ is connected, and let $|A| \to D$ be a universal

[2]) See end of this paper.

covering of $|A|$, regarded as an inclusion map. We introduce on $D \times D$ the π-action $J(x, y) = (y, x)$, and denote this π-ring by C. The map $\varphi: A \to C$, $z \to (z, Jz)$ is a π-homomorphism and in fact a covering. Furthermore C is simply connected by Lemma 1.4. We now consider the case that $|A|$ is not connected. Then $A \cong B \times B$ with a connected ring B and the π-action on $B \times B$ given by $J(x, y) = (y, x)$. Let $\psi: B \to D$ be a universal covering of B in the usual sense. We define a π-action on $D \times D$ again by $J(x, y) = (y, x)$. Then $\psi \times \psi: B \times B \to D \times D$ is a π-covering, and $D \times D$ is a simply connected π-ring by Lemma 1. 4.

Proposition 1. 6. *Let A be a connected[3]) π-ring and $\alpha: A \to C$ be a homomorphism into a simply connected π-ring C (e. g. a universal covering of A). Furthermore let $\varphi: A \to B$ be a finite etale π-homomorphism. Then there exist exactly $[B:A]$ π-homomorphisms $\beta: B \to C$ with $\beta \circ \varphi = \alpha$.*

Proof. We regard the tensor product $B \otimes_A C$ with respect to φ and α, see diagram (1. 0). The homomorphism $\varphi \otimes 1: C \to B \otimes_A C$ is again finite etale. Thus $B \otimes C$ is a finite product $\prod_{i=1}^{t} E_i$ of connected π-rings E_i. Let $\alpha_1, \ldots, \alpha_t$ and $\varphi_1, \ldots, \varphi_t$ denote the components of $1 \otimes \alpha$ and $\varphi \otimes 1$ respectively. The φ_i are (finite) coverings and thus isomorphisms, since C is simply connected. In particular $t = [B \otimes C : C] = [B : A]$. The homomorphisms $\beta_i := \varphi_i^{-1} \circ \alpha_i$ from B to C clearly all satisfy $\alpha = \beta_i \circ \varphi$. On the other hand an arbitrary π-homomorphism $\beta: B \to C$ with $\beta \circ \varphi = \alpha$ corresponds by the push-out property of the tensor product to a unique homomorphism $\gamma: B \otimes C \to C$ with $\gamma \circ (\varphi \otimes 1) = \mathrm{id}_C$ and $\gamma \circ (1 \otimes \alpha) = \beta$. Since C is connected, γ factors through a unique canonical projection $p_i: B \otimes C \to E_i$. From $\gamma \circ (\varphi \otimes 1) = \mathrm{id}_C$ we obtain $\gamma = \varphi_i^{-1} \circ p_i$, and from $\gamma \circ (1 \otimes \alpha) = \beta$ we obtain $\beta = \varphi_i^{-1} \circ \alpha_i = \beta_i$.

From this Proposition 1. 6 we immediately obtain by use of Zorn's lemma the following

Corollary 1. 7. *Let $\varphi: A \to B$ be a covering of a connected π-ring A and let $\alpha: A \to C$ be a homomorphism into a simply connected π-ring C. Then there exists at least one homomorphism $\beta: B \to C$ with $\beta \circ \varphi = \alpha$.*

Applying this corollary and the previous Proposition 1. 3 to the case that φ and α are both universal coverings of A, we obtain

Theorem 1. 8. *Any two universal coverings of a given connected π-ring A are isomorphic over A.*

In the sequel we choose a fixed universal covering of our connected π-ring A and regard this as an inclusion map. We denote this universal covering by $A \hookrightarrow \tilde{A}$. We call a subring $B < \tilde{A}$ a covering of A if B contains A and the inclusion map $A \hookrightarrow B$ is a covering.

Proposition 1. 9. *Assume $(B_i, i \in I)$ is a family of coverings of A with $B_i < \tilde{A}$. Then the ring B generated by the B_i in $\tilde{A}$ is also a covering of A.*

Proof. Since the B_i themselves are generated by families of finite coverings of A, we may assume that all B_i are finite over A. Furthermore B is the union of the rings generated by the finite subfamilies of $(B_i, i \in I)$. Thus we may assume in addition that I is finite, and then even that our family consists of two rings B_1, B_2. The map $b_1 \otimes b_2 \mapsto b_1 b_2$ from $B_1 \otimes_A B_2$ to $\tilde{A}$ factors through a component E of $B_1 \otimes B_2$. Since E is a finite cov-

[3]) It suffices to assume that the ring B is an A-module of constant rank.

ering of A, E is mapped injectively into $\tilde{A}$ by Proposition 1. 3 (already Lemma 1. 1 suffices). E has the image B in $\tilde{A}$ which hence is also a covering of A.

We denote by $G(A)$ the *Galois-group* of A, i. e. the automorphism group of $\tilde{A}/A$. From the Propositions 1. 2 and 1. 3 and from Theorem 1. 8 we immediately obtain

Proposition 1. 10. *If $B < \tilde{A}$ is a covering of A and $\lambda: B \to \tilde{A}$ is a homomorphism from B to $\tilde{A}$ over A, then λ can be extended to some σ in $G(A)$.*

We call the covering $B < \tilde{A}$ of A *galois* over A, if every such λ maps B into B; in other terms, B is galois if and only if every σ in $G(A)$ keeps B stable. The automorphism group of a galois covering B/A will be denoted by $G(B/A)$. If B is finite over A this group has order $[B : A]$ by Proposition 1. 6.

For an arbitrary covering $B < \tilde{A}$ of A the subring C of A generated by the images $\lambda(B)$ of all A-homomorphisms λ from B to $\tilde{A}$ is a covering of A by Proposition 1. 9, which clearly is galois. We call C the *galois hull* of B/A. If B is finite over A, then B admits only finitely many A-homomorphisms into A by Proposition 1. 6, and hence C is also finite over A.

In particular the finite galois coverings $C < \tilde{A}$ of A constitute a directed family of subrings of A, whose union is $\tilde{A}$. The restriction maps $G(A) \twoheadrightarrow G(C/A)$ induce an isomorphism

$$G(A) \xrightarrow{\sim} \varprojlim G(C/A)$$

with C running through all finite galois coverings of A in $\tilde{A}$. We use this isomorphism to make $G(A)$ a profinite topological group.

For any subgroup H of $G(A)$ we denote as usual by $\tilde{A}^H$ the ring of all elements in $\tilde{A}$ fixed under H. Clearly $\tilde{A}^H = \tilde{A}^{\bar{H}}$ with $\bar{H}$ the closure of H in $G(A)$. We now state the fundamental theorem of equivariant Galois theory.

Theorem 1. 11. *The coverings $B < \tilde{A}$ of A correspond uniquely to the closed subgroups H of $G(A)$ by the relations*

$$B = \tilde{A}^H, \qquad H = G(B).$$

The covering B is finite over A if and only if $G(B)$ has finite index in $G(A)$, and then $(G(A) : G(B)) = [B : A]$.

For the proof we need two lemmas.

Lemma 1. 12. *Assume $B < \tilde{A}$ is a covering of the connected π-ring A, and G is a group of automorphisms of B over A. Then the ring $A' = B^G$ is a covering of A and B is a galois covering of A'. If G is finite then $G = G(B/A')$.*

Proof. In B the subrings $B' > A$ which are finite coverings of A and stable under all automorphisms of B/A constitute a filtered family whose union is B. This remark allows to reduce the proof to the case that B is finite over A. Then also G is finite by Proposition 1. 6. We now verify that $|B|$ is with respect to G a galois extension of $|A'|$ in the sense of Auslander-Goldman and Chase-Harrison-Rosenberg [5]. For this it suffices to show the following (cf. [5], p. 18):

i) $|B|$ is separable over $|A'|$.

ii) For every idempotent $e \neq 0$ of B and different elements σ_1, σ_2 of G there exists some b in B with $\sigma_1(b)e \neq \sigma_2(b)e$.

Now i) is clear, since $|B|$ is separable over the smaller ring $|A|$. To prove ii) we may assume that e is primitive. Suppose σ_1 and σ_2 are elements of G with $\sigma_1(b)e = \sigma_2(b)e$ for all b in B. Applying some g in π to this equation we obtain $\sigma_1(b)g(e) = \sigma_2(b)g(e)$ for all b in B. Since π permutes the primitive idempotents of B transitively we obtain $\sigma_1(b) = \sigma_2(b)$ for all b and thus $\sigma_1 = \sigma_2$.

Since $|B|$ is a galois extension of $|A'|$ with respect to G, the ring $|B|$ is finite etale over $|A'|$ and $[B:A'] = |G|$. We may conclude that also $|A'|$ is finite etale over $|A|$ (e. g. [8], p. 95). We obtain that A' is a covering of A and B is a covering of A'. From $[B:A'] = |G|$ and Proposition 1. 6 it follows that B is a galois covering of A' and $G = G(B/A')$.

Lemma 1. 13. *Assume $B < \tilde{A}$ is finite and galois over A with group G. Then $B^G = A$. If H is a subgroup of G with $B^H = A$, then $H = G$.*

Proof. By Lemma 1. 12 the ring B^G is a covering of A and

$$[B : B^G] = |G| = [B : A].$$

Thus $B^G = A$. Further again from Lemma 1. 12 we obtain $|H| = [B:A] = |G|$. Thus $H = G$.

From the Lemmas 1. 12 and 1. 13 the proof of Theorem 1. 11 is immediate.

The Theorem 1. 11 clearly has the following

Corollary 1. 14. *Assume $(B_i, i \in I)$ is a family of subrings of $\tilde{A}$ which are coverings of A. Then also the intersection of the B_i is a covering of A.*

Assume B is a finite galois covering of A with group G. For every g in G we consider the π-homomorphism

$$f_g : B \otimes_A B \to B, \qquad f_g(b_1 \otimes b_2) = g(b_1)b_2.$$

Let $f : B \otimes_A B \to \prod_G B$ denote the homomorphism into the product of $|G|$ copies of B, indexed by G, whose components are the f_g. Since $|B|$ is a galois extension of $|A|$ (cf. proof of Lemma 1. 12), we obtain from [5], Theorem 1. 3 the following

Proposition 1. 15. *For any finite galois covering B of A the* π-homomorphism $f : B \otimes_A B \to \prod_G B$ is an isomorphism.

We shall also need the following corollary of this proposition.

Corollary 1. 16. *Assume $\varphi : A \to B$ is a galois covering and $\alpha : A \to C$ is a homomorphism into a connected π-ring C, such that there exists at least one homomorphism $\beta : B \to C$ with $\beta \circ \varphi = \alpha$. Then there exist exactly $[B:A]$ such homomorphisms. For any two of them, β_1, β_2, there exists a unique σ in $G(B/A)$ with $\beta_2 = \beta_1 \circ \sigma$.*

Proof. It clearly suffices to consider the case $[B:A] < \infty$. The homomorphisms $\beta : B \to C$ with $\beta \circ \varphi = \alpha$ correspond uniquely to the π-primitive π-idempotents e of $D := B \otimes_A C$ with $[De : C] = 1$ (cf. proof of Proposition 1. 6). Now we can write

$$D = (B \otimes_A B) \otimes_{\beta_0} C$$

with some fixed homomorphism $\beta_0 : B \to C$ over A. It follows from Proposition 1. 15, that D has exactly $|G|$ idempotents of the type described above, on which G acts freely and transitively. Thus G also acts freely and transitively on the corresponding set $\mathrm{Hom}_A(B, C)$. This is our assertion.

§ 2. Definition of signatures and real closures

Since now π is always a group consisting of two elements $1, J$. For any π-ring A we denote by J_A the involution on A induced by J. For a in A we often write $\bar{a}$ instead of $J_A(a)$. We say that the ring A is local, resp. semilocal, resp. Dedekind, etc. if the ring $|A|$ without π-operation has this property. The ring of elements fixed under J_A will be denoted by A_0 and will usually be regarded as a π-ring with trivial operation.

Let $W(A)$ denote the Witt ring of hermitian inner product spaces over A. The elements of $W(A)$ are suitable equivalence classes of pairs (E, Φ) with E a finitely generated projective A-module and Φ a non singular hermitian form on E, linear in the first argument and antilinear with respect to J_A in the second. The case $J_A = \mathrm{id}$ is allowed. We refer the reader to [16], § 1 and to [20] for the basic definitions. (In [16] the term "non degenerate" is used instead of "non singular".)

The equivalence relation for hermitian inner product spaces used in the definition of $W(A)$ will be denoted by $\sim$, and the equivalence class of an inner product space (E, Φ) will be denoted by $[E, \Phi]$. We often write E instead of (E, Φ) and $[E]$ instead of $[E, \Phi]$. For any π-homomorphism $\varphi: A \to B$ we denote the induced ring homomorphism $[E] \mapsto [E \otimes_A B]$ from $W(A)$ to $W(B)$ by φ_*.

If A is connected but $|A|$ is not connected then $W(A) = 0$ (e. g. [16], p. 125). If $|A|$ is connected, then every inner product space E over A has a constant rank, denoted by $\dim E$, and the map $[E] \mapsto \dim E \bmod 2$ from $W(A)$ to $\mathbb{Z}/2\mathbb{Z}$ is well defined. We call this homomorphism the *dimension index* ν and its kernel the *fundamental ideal* $I(A)$ of $W(A)$.

An inner product space (E, Φ) with E a free A-module will often be denoted by an hermitian matrix (a_{ij}) with $a_{ij} = \Phi(e_i, e_j)$ for some basis $e_1, \ldots, e_n$ of E. In particular every unit a of A_0 yields a free space (a) of rank one. An orthogonal sum

$$(a_1) \perp \cdots \perp (a_n)$$

will also be denoted by $(a_1, \ldots, a_n)$.

Definition 2. 1. A *signature* σ of a commutative ring A is a homomorphism from the ring $W(A)$ to the ring $\mathbb{Z}$ of integers, cf. Introduction. The ring A is called *real*, if the set $\mathrm{Sign}(A)$ of signatures of A is not empty. Otherwise A is called *non real.*

Remark 2. 2. If A is semi-local and $|A/\mathfrak{M}| > 4$ for all maximal ideals $\mathfrak{M}$ of A, then A is non real if and only if there exists an equation

$$-1 = a_1\bar{a}_1 + \cdots + a_r\bar{a}_r$$

with finitely many a_i in A. This has been proved in [17], § 4 under the additional assumption that A contains an element μ with $\mu + \bar{\mu} = 1$. A proof not using this assumption will be published in the near future [15]. (The assumption about the residue class fields $A/\mathfrak{M}$ above is only needed in the case $J_A \neq \mathrm{id}$, and perhaps can also be eliminated in this case.)

For E an inner product over A and σ a signature of A we usually write $\sigma(E)$ instead of $\sigma([E])$. The rôle played by the signatures in the theory of Witt rings is indicated by the following

Theorem 2. 3. *Assume $|A|$ is connected. If A is non real then $I(A)$ is the only prime ideal of $W(A)$, and $2^n \cdot W(A) = 0$ for some $n \geq 1$. If A is real then the minimal prime ideals P of $W(A)$ correspond uniquely to the signatures σ of A, the prime ideal P corresponding to σ being the kernel of σ.*

This has been shown for A semi-local in [16]. From the semi-local case one easily obtains a proof of Theorem 2. 3 in general by use of the following theorem, due to A. Dress.

Theorem 2. 4. *Let A be an arbitrary commutative π-ring. For every minimal prime ideal P of $W(A)$ there exists a maximal ideal $\mathfrak{m}$ of A_0 and a minimal prime ideal Q of $W(A_{\mathfrak{m}})$, such that P is the inverse image of Q with respect to the canonical map from $W(A)$ to $W(A_{\mathfrak{m}})$.*

The proof of this important theorem, whose details have been thoroughly checked by the present author, will appear in the near future (Dress, oral communication*)). The main tool used in this proof is Lemma 10. 1 in [6] (with the group G there being 1).

Assume $\varphi: A \to B$ is a π-homomorphism, σ is a signature of A and τ a signature of B. We say that τ *extends* σ (with respect to φ), or that σ is the *restriction* of τ to A, if the diagram

$$\begin{tikzcd} W(A) \arrow[rr, "\varphi_*"] \arrow[dr, "\sigma"'] & & W(B) \arrow[dl, "\tau"] \\ & \mathbb{Z} & \end{tikzcd}$$

commutes. We often denote the restriction σ by $\tau | A$, if there is no doubt which map φ is considered.

According to the Theorems 2. 3 and 2. 4 every signature of A extends to at least one localization $A_{\mathfrak{m}}$. In § 4 we shall prove the sharper statement that every signature of A extends to a residue class field $A(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ with $\mathfrak{p}$ a suitable prime ideal of A stable under J_A.

Let σ be a signature of A. For any unit a of A_0 we have $[(a)]^2 = 1$ in $W(A)$ and hence $\sigma(a) = \pm 1$. Thus σ yields a character of A_0^* with values ± 1. If A is semi-local, then σ is uniquely determined by this character. This is evident if $|A|$ is connected, since then $W(A)$ is generated by the elements $[(a)]$. But it is also true if $|A|$ is not connected, cf. [17], end of § 2. In the semi-local case we usually identify σ with the corresponding character of A_0^*. The reader is advised to consult § 2 of the paper [17] for a more detailed description of these characters, and to consult § 4 of the same paper, if he wants to see how to deal with signatures of semi-local rings in much the same way as with orderings of fields.

Later on we shall need the following

Proposition 2. 5. *Assume A is a commutative π-ring with $|A|$ connected. Then for every signature σ of A and z in $W(A)$*

$$\nu(z) = \sigma(z) \bmod 2.$$

Proof. Let $\mathfrak{m}$ be a maximal ideal of A_0 such that σ extends to a signature τ of $A_{\mathfrak{m}}$, and let z' denote the image of z in $W(A_{\mathfrak{m}})$. Then $\sigma(z) = \tau(z')$ and $\nu(z) = \nu(z')$. Thus we have to show $\nu(z') = \tau(z') \bmod 2$, i. e. we have reduced the proof to the case that A_0 is a local ring. In this case Proposition 2. 5 is clear from the fact that $W(A)$ is generated by the classes of free spaces (a) of rank one (or cf. [16], Example 3. 11 last line).

We now consider pairs (A, σ) consisting of a π-ring A and a signature σ of A. A *morphism* $\varphi: (A, \sigma) \to (B, \tau)$ between such pairs is a π-homomorphism φ from A to B such that $\sigma = \tau \circ \varphi_*$, i. e. τ extends σ with respect to φ. The pair (A, σ) is called *con-*

*) *Added in proof*: A. Dress, The weak local-global principle in algebraic K-theory, to appear in Communications in Algebra.

nected if A is connected. In a similar way we use terms like "local", "semilocal", "Dedekind", etc. for pairs. If (A, σ) is connected then $|A|$ is connected, since otherwise $W(A) = 0$ and A would not possess signatures.

A *covering* (resp. *finite covering*) of a connected pair (A, σ) is a morphism

$$\varphi : (A, \sigma) \to (B, \tau)$$

into a connected pair (B, τ) such that the π-homomorphism $\varphi : A \to B$ is a covering (resp. finite covering) as explained in § 1. We call a pair (R, ϱ) *real closed*, if (R, ϱ) is connected and does not admit coverings except isomorphisms. Any covering $\varphi : (A, \sigma) \to (R, \varrho)$ with (R, ϱ) real closed is called a *real closure* of (A, σ).

By § 1 every covering $\varphi : (A, \sigma) \to (B, \tau)$ of (A, σ) is isomorphic to a covering $\psi : (A, \sigma) \to (B', \tau')$ with $A < B' < \tilde{A}$ and $\psi : A \to B'$ the inclusion map. From this remark one easily obtains by use of Zorn's lemma

Proposition 2. 6. *Every connected pair (A, σ) has at least one real closure*

$$\varphi : (A, \sigma) \to (R, \varrho).$$

Remark 2. 7. If $\varphi : (A, \sigma) \to (R, \varrho)$ is a real closure of (A, σ), then certainly $\varphi : A \to R$ is *not* a universal covering, since by the proof of Proposition 1. 5 the ring $|\tilde{A}|$ is not connected.

In the next section we shall see (Theorem 3. 9) that any two real closures of (A, σ) are isomorphic over (A, σ).

A pair (T, τ) is called *strictly real closed*, if T has trivial involution $J_T = \mathrm{id}_T$, and (T, τ) is connected and does not admit coverings by pairs with trivial involution except isomorphisms. A *strict real closure* of a connected pair (A, σ) with trivial involution is a covering $\varphi : (A, \sigma) \to (T, \tau)$ with (T, τ) strictly real closed.

Proposition 2. 8. (i) *Every connected pair (A, σ) with trivial involution has at least one strict real closure.* (ii) *If (T, τ) is strictly real closed and $\psi : (T, \tau) \to (R, \varrho)$ is a real closure of (T, τ), then $\psi(T) = R_0$ and $[R : R_0] \leqq 2$.*

Proof. The first assertion is again clear by Zorn's lemma. To prove the second we may assume without loss of generality $T < R$ and that ψ is the inclusion map. Clearly $T < R_0$. Now the ring R_0 is a covering of T by Lemma 1. 12. Since the signature $\varrho | R_0$ extends τ we must have $R_0 = T$. Furthermore by the same lemma $[R : R_0] = 2$ if $J_R \neq \mathrm{id}$, otherwise $R = R_0$.

Since now we also use the following terminology: Let (A, σ) be a connected pair and remember that $\tilde{A}$ denotes an arbitrarily chosen fixed universal covering of A. We say that a connected pair (B, τ) is a covering (resp. real closure, etc.) of (A, σ), if $A < B < \tilde{A}$ and the inclusion map $i : A \hookrightarrow B$ is a morphism from (A, σ) to (B, τ) which is a covering (resp. real closure, etc.).

§ 3. The trace formula

Let A be a π-ring and $\varphi : A \to B$ a finite etale π-homomorphism. Then the trace $\mathrm{Tr}_\varphi : B \to A$ of this finite etale extension ([8], p. 91 ff.) is an A-linear map, which is compatible with the π-actions. We have a well known transfer homomorphism in

$$\mathrm{Tr}_\varphi^* : W(B) \to W(A)$$

of additive groups mapping the class of a space (E, Φ) over B to the class $[E_\varphi, \mathrm{Tr}_\varphi \circ \Phi]$, with E_φ denoting E considered as an A-module by φ, cf. [7], § 2. We shall use the following criterion for extending signatures.

Lemma 3. 1. *Let σ be a signature of A and assume there exists an element y in $W(B)$ with $\sigma\left(\mathrm{Tr}_\varphi^*(y)\right) \neq 0$. Then σ can be extended to B.*

This can be proved by the same argument as used in [17] in the semi-local case, cf. the proof of Lemma 5. 3 in that paper.

Let now σ be a fixed signature of A and let $\varphi: A \to B$ be a fixed finite etale π-homomorphism. We denote by $S(\varphi, \sigma)$ the set of all signatures τ of B which extend σ with respect to φ.

Definition. A *trace formula* with respect to φ and σ is a map $n: S(\varphi, \sigma) \to \mathbb{Z}$ such that $n(\tau) = 0$ except for finitely many τ in $S(\varphi, \sigma)$, and

$$\sigma\left(\mathrm{Tr}_\varphi^*(z)\right) = \sum_{\tau|\sigma} n(\tau)\tau(z) \tag{3. 2}$$

for all z in $W(B)$. Here the sum is taken over all τ in $S(\varphi, \sigma)$, with the convention that this sum is zero if $S(\varphi, \sigma)$ is empty.

Remark. We shall see below that actually $S(\varphi, \sigma)$ is always a finite set.

Lemma 3. 3. *For given φ and σ there exists at most one trace formula.*

Proof. Assume n and n' are two different trace formulas for a. We choose some τ_0 in $S(\varphi, \sigma)$ with $n(\tau_0) \neq n'(\tau_0)$. Let M denote the finite set of all τ in $S(\varphi, \sigma)$ such that $n(\tau)$ and $n'(\tau)$ are not both zero. For every τ in M let $P(\tau)$ denote the kernel of

$$\tau: W(B) \to \mathbb{Z}.$$

Since all these $P(\tau)$ are minimal prime ideals of $W(B)$, the intersection of all $P(\tau)$ with τ in M and $\tau \neq \tau_0$ is not contained in $P(\tau_0)$. Thus we can find some z in $W(B)$ with $\tau_0(z) \neq 0$ but $\tau(z) = 0$ for all other τ in M. Now evaluating $\sigma\left(\mathrm{Tr}_\varphi^*(z)\right)$ using both trace formulas n and n' we obtain the contradiction

$$n(\tau_0)\tau_0(z) = n'(\tau_0)\tau_0(z).$$

We now state the main result of this section.

Theorem 3. 4. (i) *For given φ and σ there exists a trace formula n.* (ii) *In this formula $n(\tau) > 0$ for every τ in $S(\varphi, \sigma)$. In particular $S(\varphi, \sigma)$ is finite.* (iii) *If $\alpha: (A, \sigma) \to (R, \varrho)$ is a morphism into a real closed pair (R, ϱ) then for any τ in $S(\varphi, \sigma)$ the number $n(\tau)$ equals the cardinality of the set of all morphisms from (B, τ) to (R, ϱ) over (A, σ).*

Remark 3. 5. For every pair (A, σ) there exists some morphism α into a real closed pair (R, ϱ). Indeed, if A is connected you can take a real closure of (A, σ). If A is arbitrary there exists by Theorem 2. 4 some morphism $(A, \sigma) \to (A_\mathfrak{m}, \gamma)$ with $\mathfrak{m}$ a maximal ideal of A_0. This morphism can be composed with a real closure of $(A_\mathfrak{m}, \gamma)$.

We postpone the proof of Theorem 3. 4, and first draw some consequences from this theorem. For the coefficients $n(\tau)$ of the unique trace formula belonging to φ and σ we now write more precisely $n(\tau, \varphi)$ or $n(\tau, A)$, and we call $n(\tau, \varphi)$ the *multiplicity* of τ with respect to φ or A.

Inserting the unit element of $W(B)$ into our trace formula we obtain

$$\sigma\left(\mathrm{Tr}_\varphi^*(1)\right) = \sum_{\tau|\sigma} n(\tau, \varphi). \tag{3. 6}$$

In the case that A is connected there exist by Proposition 1. 6 at most $[B : A]$ π-homomorphisms from B to R over A in the situation described in Theorem 3. 4. (iii). Thus our Theorem 3. 4 has the following

Corollary 3. 7. *Let $\varphi : A \to B$ be a finite etale π-homomorphism. Then $\sigma(\mathrm{Tr}_\varphi^*(1)) \geqq 0$ for every signature σ of A, and σ is extendable to B if and only if $\sigma(\mathrm{Tr}_\varphi^*(1)) > 0$. If A is connected, then σ has at most $[B : A]$ extensions to B.*

We mention a rather trivial application of this handy criterion for extendability of signatures.

Proposition 3. 8. *Assume $\varphi : A \to B$ is finite etale and $[B_\mathfrak{m} : A_\mathfrak{m}]$ is odd for all maximal ideals $\mathfrak{m}$ of A_0. Then every signature σ of A can be extended to B.*

Proof. There exists some maximal ideal $\mathfrak{m}$ of A_0 such that σ extends to a signature γ of $A_\mathfrak{m}$. Let z denote the image of $\mathrm{Tr}_\varphi^*(1)$ in $W(A_\mathfrak{m})$. We have $\nu(z) = 1$ and thus by Proposition 2. 5

$$\sigma(\mathrm{Tr}_\varphi^*(1)) = \gamma(z) \equiv 1 \mod 2.$$

This implies $\sigma(\mathrm{Tr}_\varphi^*(1)) \neq 0$.

For another proof of Proposition 3. 8 cf. [17], Proposition 5. 4.

Theorem 3. 9. *Assume (A, σ) is connected and $\alpha : (A, \sigma) \to (R, \varrho)$ is a morphism with (R, ϱ) real closed. Let $\varphi : (A, \sigma) \to (B, \tau)$ be a covering.*

(i) *There exists at least one morphism $\beta : (B, \tau) \to (R, \varrho)$ with $\alpha = \beta \circ \varphi$.*

(ii) *If α and φ are real closures then every such β is an isomorphism.*

Proof. (i) We may assume $A < B$ and that φ is the inclusion map from A to B. By Zorn's lemma there exists a maximal ring $C < B$ with $A < C$ and $A \hookrightarrow C$ a covering, such that there exists a morphism β_1 from $(C, \tau | C)$ to (R, ϱ) extending α. If $C \neq B$ then we can find a ring D with $C \subsetneqq D < B$ and $C \hookrightarrow D$ a finite covering. By Theorem 3. 4 the morphism β_1 can be extended to a morphism from $(D, \tau | D)$ to (R, ϱ). This contradicts the maximality of C. Thus $C = B$.

(ii) If α is a covering, then by Proposition 1. 3 also β is a covering. Thus if in addition φ is a real closure then β must be an isomorphism.

Corollary 3. 10. *Assume A and B have trivial involutions. Then Theorem 3. 9 remains true with the words "real closed" and "real closure" replaced by "strictly real closed" and "strict real closure".*

Proof. Statement (ii) is clear by the same argument as above. To prove (i) we choose a real closure $\gamma : (R, \varrho) \to (S, \eta)$ of the strictly real closed ring (R, ϱ). We regard γ and φ as inclusion maps. By Theorem 3. 9. we can extend $\gamma \circ \alpha$ to some morphism $\delta : (B, \tau) \to (S, \eta)$. Clearly $\delta(B) < S_0$. By Proposition 2. 8 the ring S_0 coincides with R. The morphism $\beta : (B, \tau) \to (R, \varrho)$ induced by δ fullfills $\beta \circ \varphi = \alpha$.

We now enter the proof of Theorem 3. 4. We consider the situation described in part (iii) of this theorem. Starting from the diagram (1. 0) with the letter C there replaced by R we obtain a diagram

$$\begin{array}{ccc} W(B) & \xrightarrow{(1 \otimes \alpha)_*} & W(B \otimes_A R) \\ {\scriptstyle \mathrm{Tr}_\varphi^*} \big\downarrow & & \big\downarrow {\scriptstyle \mathrm{Tr}_{(\varphi \otimes 1)}^*} \\ W(A) & \xrightarrow{\alpha_*} & W(R). \end{array}$$

It is easily checked that this diagram is commutative, cf. [7], Lemma 2. 1. Thus for z in $W(B)$

$$\sigma \circ \mathrm{Tr}_\varphi^*(z) = \varrho \circ \alpha_* \circ \mathrm{Tr}_\varphi^*(z) = \varrho \circ \mathrm{Tr}_{\varphi \otimes 1}^* \circ (1 \otimes \alpha)_*(z).$$

Now $B \otimes R$ is a direct product $\prod_{i=1}^{t} E_i$ of finitely many connected π-rings E_i. Let $p_i \colon B \otimes R \to E_i$ denote the corresponding projections, $1 \leqq i \leqq t$, further let

$$\alpha_i \colon = p_i \circ (1 \otimes \alpha) \quad \text{and} \quad \varphi_i \colon = p_i \circ (\varphi \otimes 1)$$

be the components of $1 \otimes \alpha$ and $\varphi \otimes 1$ respectively. The $\varphi_i \colon R \to E_i$ are finite coverings. We have

$$\varrho \circ \mathrm{Tr}_{\varphi \otimes 1}^* \circ (1 \otimes \alpha)_*(z) = \sum_{i=1}^{t} \varrho \circ \mathrm{Tr}_{\varphi_i}^* \circ p_{i*} \circ (1 \otimes \alpha)_*(z) = \sum_{i=1}^{t} \varrho \circ \mathrm{Tr}_{\varphi_i} \circ \alpha_{i*}(z).$$

Let i be a fixed index in $[1, t]$. If $[E_i \colon R] > 1$, then ϱ cannot be extended to E_i, since (R, ϱ) is real closed. Thus by Lemma 3. 1 the corresponding summand $\varrho \circ \mathrm{Tr}_{\varphi_i}^* \circ \alpha_{i*}(z)$ is zero. If $[E_i \colon R] = 1$ then $\mathrm{Tr}_{\varphi_i}^* = (\varphi_{i*})^{-1}$ as is easily verified, and we obtain

$$\mathrm{Tr}_{\varphi_i}^* \circ \alpha_{i*}(z) = \beta_{i*}(z)$$

with $\beta_i = \varphi_i^{-1} \circ \alpha_i$. Now these β_i are precisely all homomorphisms from B to R over A, cf. the proof of Proposition 1. 6. We thus obtain

$$\sigma \circ \mathrm{Tr}_\varphi^*(z) = \sum_{\beta} \varrho \circ \beta_*(z)$$

with β running through the finitely many homomorphisms from B to R over A. For every such β the signature $\varrho \circ \beta_*$ clearly extends σ. We now *define* for every signature τ in $S(\varphi, \sigma)$ the natural number $n(\tau)$ as the number of all β with $\varrho \circ \beta_* = \tau$. Clearly $n(\tau) = 0$ except for finitely many τ, and as we have just seen

$$\sigma \circ \mathrm{Tr}_\varphi^*(z) = \sum_{\tau | \sigma} n(\tau) \tau(z)$$

for z in $W(B)$. Keeping Lemma 3. 3 in mind the assertions (i) and (iii) of Theorem 3. 4 are proved.

Let now τ_0 denote a fixed signature in $S(\varphi, \sigma)$ and choose some morphism β_0 from (B, τ_0) into a real closed pair (R, ϱ) (cf. Remark 3. 5). Applying assertion (iii) of Theorem 3. 4 to the morphism $\alpha \colon = \beta_0 \circ \varphi$ we see $n(\tau_0) > 0$. Thus also assertion (ii) is proved.

In the case that A and B are semi-local and have trivial involutions the trace formula (3. 2) had been conjectured in [17], 5. 16 with multiplicities $n(\tau) = 1$. We shall see in part II of the paper, that indeed all $n(\tau) = 1$ in this case.

We now discuss a case where multiplicities $n(\tau) = 2$ occur in a trivial way. Let A be a π-ring. The involution J_A is a π-automorphism of A. We denote for z in $W(A)$ the image $(J_A)_*(z)$ by $\bar{z}$.

Lemma 3. 11. *For every signature σ of A and every element z of $W(A)$ we have $\sigma(z) = \sigma(\bar{z})$. In other words, J_A is an automorphism of (A, σ).*

Proof. σ extends to a signature τ of $B \colon = A_{\mathfrak{m}}$ with $\mathfrak{m}$ a suitable maximal ideal of A_0. Let x denote the image of z in $W(B)$. Then $\bar{x}$ is the image of $\bar{z}$, and it suffices to prove $\tau(x) = \tau(\bar{x})$. Now $W(B)$ is generated by elements $[(a)]$ which are fixed under $(J_B)_*$. Thus $y = \bar{y}$ for all y in $W(B)$.

We call the involution J_A *non degenerate* if A is finite etale over A_0 and $[A_{\mathfrak{m}} : A_{0\mathfrak{m}}] = 2$ for all maximal ideals $\mathfrak{m}$ of A_0. If A is connected and J_A is non degenerate then the inclusion map $A_0 \hookrightarrow A$ is a covering of π-rings.

Proposition 3. 12. *Assume J_A is non degenerate. Then $n(\tau, A_0) = 2$ for every signature τ of A. A signature σ of A_0 has at most one extension to A.*

Proof. Let σ denote the restriction $\tau | A_0$ of a given signature τ of A. Then J_A is an automorphism of (A, τ) over (A_0, σ_0), and we see from Theorem 3. 4 (iii), that $n(\tau, A_0) \geqq 2$. Again by this theorem and by Proposition 1. 6 we have

$$\sum_{\tau' | \sigma} n(\tau', A_0) \leqq [A : A_0] = 2.$$

This implies both assertions.

We now present some applications of Theorem 3. 9.

Proposition 3. 13. *Let (A, σ) be a connected pair with J_A non degenerate, let σ_0 denote the restriction $\sigma | A_0$, and let (R, ϱ) be a real closure of (A_0, σ_0) with $A_0 < R < \tilde{A}_0 = \tilde{A}$. Then $A < R$ and (R, ϱ) is a real closure of (A, σ).*

Proof. (A, σ) is a covering of (A_0, σ_0). By Theorem 3. 9 there exists a morphism χ from (A, σ) to (R, ϱ) over (A_0, σ_0). Since A is a galois covering of A_0, we have

$$A = \chi(A) < R.$$

Now $\varrho | A$ extends σ_0 and Proposition 3. 12 implies $\varrho | A = \sigma$. Finally by Proposition 1. 3 (R, ϱ) is a covering of (A, σ). Thus (R, ϱ) is a real closure of (A, σ).

Proposition 3. 14. *Assume (A, σ) is connected and has trivial involution. Let (R, ϱ) be a real closure of (A, σ). Then $(R_0, \varrho | R_0)$ is a strict real closure of (A, σ).*

This follows from Proposition 2. 8, since by Theorem 3. 9 any two real closures of (A, σ) are isomorphic over (A, σ).

Theorem 3. 15. *Let $\varphi : A \to B$ be a finite etale π-homomorphism and $\alpha : A \to C$ be an arbitrary π-homomorphism. Let τ_1 be a signature of B and τ_2 be a signature of C whose restrictions $\tau_1 \circ \varphi_*$ and $\tau_2 \circ \alpha_*$ are equal. Then there exists at least one signature η of the tensor product $B \otimes_A C$ with respect to φ and α such that $\eta | B = \tau_1$ and $\eta | C = \tau_2$, the restrictions being taken with respect to the canonical homomorphisms $1 \otimes \alpha : B \to B \otimes C$ and $\varphi \otimes 1 : C \to B \otimes C$.*

Proof. Let σ denote the signature $\tau_1 | A = \tau_2 | A$. We choose some morphism $\gamma : (C, \tau_2) \to (R, \varrho)$ into a real closed pair (R, ϱ) (cf. 3. 5). Applying Theorem 3. 9 to the morphisms $\varphi : (A, \sigma) \to (B, \tau_1)$ and

$$\gamma \circ \alpha : (A, \sigma) \to (C, \tau_2) \to (R, \varrho)$$

we know that there exists a morphism $\beta : (B, \tau_1) \to (R, \varrho)$ with $\beta \circ \varphi = \gamma \circ \alpha$. By the pushout property of the tensor product we have a homomorphism $\delta : B \otimes_A C \to R$ with $\delta \circ (1 \otimes \alpha) = \beta$ and $\delta \circ (\varphi \otimes 1) = \gamma$. The signature $\eta := \varrho \circ \delta_*$ has the restrictions $\eta \circ (1 \otimes \alpha)_* = \tau_1$ and $\eta \circ (\varphi \otimes 1)_* = \tau_2$.

We investigate the situation described in Theorem 3. 15 in a special case.

Proposition 3. 16. *Let (A, σ) be a connected pair with J_A non degenerate, let σ_0 denote the restriction $\sigma | A_0$ and let $\alpha : (A_0, \sigma_0) \to (T, \tau)$ be a morphism into a strictly real closed pair (T, τ). Let R denote the tensor product $A \otimes_{A_0} T$ with respect to α.* (i) *τ extends to a unique* *signature ϱ of R, and (R, ϱ) is real closed.* (ii) *This signature ϱ extends σ with respect to $1 \otimes \alpha : A \to R$.* (iii) *If $\alpha : (A_0, \sigma_0) \to (T, \tau)$ is a strict real closure of (A_0, σ_0), then*

$$1 \otimes \alpha : (A, \sigma) \to (R, \varrho)$$

is a real closure of (A, σ).

Proof. We regard T as a subring of R, which is possible since $T \to R$ is finite etale. Clearly $R_0 = T$ and J_R is non degenerate. By Theorem 3. 15 there exists a signature ϱ on R extending both σ and τ, and by Proposition 3. 12 there exists no other signature of R extending τ. If (R', ϱ') is a real closure of (T, τ), then $[R' : T] \leqq 2$ by Proposition 2. 8. We now see from Theorem 3. 9 that (R, ϱ) is isomorphic to (R', ϱ') over (T, τ), and hence (R, ϱ) is real closed. Thus the assertions (i) and (ii) are proved. If α is a covering then also $1 \otimes \alpha$ is a covering, which proves (iii).

Proposition 3. 17. *Let (R, ϱ) be a real closed pair. Then the pair (R_0, ϱ_0) with $\varrho_0 = \varrho \mid R_0$ is strictly real closed.*

Proof. Let $\varphi : (R_0, \varrho_0) \to (T, \tau)$ be a strict real closure of (R_0, ϱ_0). We consider the diagram

$$\begin{array}{ccc} T & \xrightarrow{1 \otimes \alpha} & T \otimes_{R_0} R \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi \otimes 1} \\ R_0 & \xrightarrow{\alpha} & R \end{array}$$

with α the inclusion map. We may also regard $1 \otimes \alpha$ as an inclusion map, since φ is a covering. One easily verifies $T = (T \otimes R)_0$. Thus $T \otimes R$ is certainly connected and $\varphi \otimes 1$ is a covering. By Theorem 3. 15 there exists a signature η of $T \otimes R$ extending both τ and ϱ. Since (R, ϱ) is real closed this implies $[T : R_0] = [T \otimes R : R] = 1$. Thus (R_0, ϱ_0) is strictly real closed.

We close this section with a description of the real closures of pairs (A, σ) with A a field in classical terms. Temporarily we write a π-ring A as a pair (B, J) with $B = |A|$ and $J = J_A$.

Example 3. 18. Let K be a field, J be an involution of K, and σ be a signature of (K, J). This means that on the fixed field K_0 of J an ordering $<$ is given with $x\bar{x} > 0$ for all x in K^*, cf. Proposition 3. 12 and [17], 1. 6. Let $\bar{K}$ denote the algebraic closure of K. Since every covering of K (in the category of rings without involution) is a field, $\bar{K}$ is the universal covering of K. By the proof of Proposition 1. 5 the universal covering $(K, J)^\sim$ is the pair $(\bar{K} \times \bar{K}, \beta)$ with $\beta(x, y) = (y, x)$. Regarding (K, J) as a π-subring of $(K, J)^\sim$ we have to identify an element x of K with the element $(x, J(x))$ of $\bar{K} \times \bar{K}$.

Let $T < \bar{K}$ be a real closure of K_0 with respect to the ordering $<$ in the classical sense ([2], p. 89). By the fundamental theorem of algebra $\bar{K} = T[\sqrt{-1}]$ and $[\bar{K} : T] = 2$, cf. [2], p. 89. Let α denote the generator of the Galois group of $\bar{K}/T$. We have

$$W(T, \mathrm{id}) = W(\bar{K}, \alpha) = \mathbb{Z},$$

and we denote by τ and ϱ the unique signatures of (T, id) and $(\bar{K}, \alpha)$ respectively. We further denote by σ_0 the signature of K_0 corresponding to the ordering $<$, i. e. the restriction of σ to (K_0, id). Clearly ϱ extends τ and τ extends σ_0. If $J \neq \mathrm{id}$, then J is non degenerate, and we see from Proposition 3. 12 — or by a direct argument — that ϱ also extends σ. We embed $(\bar{K}, \alpha)$ into $(K, J)^\sim$ identifying an element x of $\bar{K}$ with the element $(x, \alpha(x))$ of $(K, J)^\sim$.

Case 1: $J = \mathrm{id}$. Clearly (T, id, τ) is a strict real closure of (K, id, σ). The signature ϱ of $(\bar{K}, \alpha)$ can not be extended to the unique non trivial covering $(\bar{K} \times \bar{K}, \beta)$ of $(\bar{K}, \alpha)$, since $W(\bar{K} \times \bar{K}, \beta) = 0$. Thus $(\bar{K}, \alpha, \varrho)$ is a real closure of (K, id, σ). (This also follows from Proposition 3. 14.)

Case 2: $J \neq \mathrm{id}$. As just proved $(\bar{K}, \alpha, \varrho)$ is a real closure of $(K_0, \mathrm{id}, \sigma_0)$, hence also a real closure of (K, J, σ) (cf. Proposition 3. 13).

§ 4. Extension of signatures to fields

We first consider the case that σ is a signature of a *local ring* A with *trivial involution*. We are looking for prime ideals $\mathfrak{p}$ of A such that σ can be extended to the quotient field $A(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ of $A/\mathfrak{p}$. Let P denote the set of all a in A^* with $\sigma(a) = 1$ and let Q denote the set of all finite sums $a_1 + \cdots + a_r$ with a_i in P. Then Q is a multiplicative subset of A which clearly does not meet any prime ideal $\mathfrak{p}$ of A such that σ extends to a signature τ of $A(\mathfrak{p})$, since the images of the elements of Q in $A(\mathfrak{p})$ must be positive with respect to the ordering corresponding to τ (cf. the introduction). Thus it is very natural to investigate the maximal prime ideals of A which do not meet Q. It turns out that we are in a very pleasant situation: The complement of $Q \cup (-Q)$ in A is already a prime ideal. In the case that 2 is a unit in A the following theorem has already been proved by Kanzaki and Kitamura [11].

Theorem 4. 1. i) *The sets Q and $-Q$ are disjoint.* ii) *The complement $\mathfrak{p}$ of $Q \cup (-Q)$ in A is a prime ideal.* iii) *For x in $\mathfrak{p}$ and y in Q the sum $x + y$ lies in Q.*

Remark 4. 2. By [17], 2. 3 we have $Q \cap A^* = P$. Thus since A is local, every element of Q is an element of P or the sum of two elements of P.

Before proving Theorem 4. 1 we deduce from this theorem as in [11] the following

Corollary 4. 3. *There is a unique signature of $A(\mathfrak{p})$, denoted by $\bar{\sigma}$, which extends σ. The positive elements of $A/\mathfrak{p}$ with respect to the ordering of $A(\mathfrak{p})$ corresponding to $\bar{\sigma}$ are precisely the images of all a in Q.*

Proof. As follows immediately from Theorem 4. 1 we have on the ring $A/\mathfrak{p}$ a total ordering compatible with addition and multiplication, defined in the following way: The image $\bar{a}$ of an element a of A is positive if and only if a lies in Q. We extend this ordering in the unique possible way to $A(\mathfrak{p})$. For the corresponding signature $\bar{\sigma}$ of $A(\mathfrak{p})$ we have $\sigma(\bar{a}) = 1$ for all a in P. Thus $\bar{\sigma}$ extends σ. Clearly there is no other possibility to extend σ to $A(\mathfrak{p})$.

We now start with the proof of Theorem 4. 1. Assume $Q \cap (-Q)$ is not empty. Then there exists an equation

$$a_1 + \cdots + a_r = -b_1 - \cdots - b_s$$

with a_i and b_j in P. If the left hand side is a unit, then we have $\sigma(a_1 + \cdots + a_r) = 1$ by [17], 2. 3, and also $\sigma(b_1 + \cdots + b_s) = 1$. This is impossible. If the left hand side lies in the maximal ideal $\mathfrak{m}$ of A, then we obtain a contradiction considering the equation

$$a_1 + \cdots + a_{r-1} = -a_r - b_1 - \cdots - b_s.$$

Thus $Q \cap (-Q) = \emptyset$. The remaining assertions of Theorem 4. 1 will easily follow from

Lemma 4. 4 (cf. [11], p. 227 for $2 \in A^*$). *If x and y are elements of A with $x + y$ in Q then at least one of the elements x and y lies in Q.*

Proof. We have an equation $x + y = a_1 + \cdots + a_r$ with a_i in Q. If y is a unit then either $y \in P$ or $y \in -P$. In the second case $x = (-y) + a_1 + \cdots + a_r$ lies in Q. Thus the assertion is proved if y is a unit and also if x is a unit. Assume now that x and y lie in $\mathfrak{m}$. Certainly $r \geqq 2$. We obtain from the equation

$$x + (y - a_1) = a_2 + \cdots + a_r$$

that x or $y - a_1$ lies in Q. If $y - a_1 \in Q$ then also $y \in Q$.

From this lemma it is clear, that the sum $x + y$ of two elements x and y in $\mathfrak{p}$ again lies in $\mathfrak{p}$, since otherwise $x + y \in \pm Q$ and thus $x \in \pm Q$ or $y \in \pm Q$. It follows from the definition of $\mathfrak{p}$ that $-\mathfrak{p} = \mathfrak{p}$. Thus $\mathfrak{p}$ is an additive subgroup of A.

Assume now that x is an element of $\mathfrak{p}$ and y an element of Q. If $z := x + y$ would lie in $-Q$ then $x = (-y) + z$ also would lie in $-Q$, and if z would lie in $\mathfrak{p}$ then $y = z - x$ would lie in $\mathfrak{p}$. Thus z lies in Q.

We finally show that $\mathfrak{p}$ is a prime ideal. Let x be in A and y be in $\mathfrak{p}$. We want to show $xy \in \mathfrak{p}$. This is clear from the definition of $\mathfrak{p}$ if x lies in Q or in $-Q$. If x lies in $\mathfrak{p}$ then, as we have already shown, $1 + x$ lies in Q, hence

$$xy = (1 + x)y - y \in \mathfrak{p}.$$

Thus $\mathfrak{p}$ is an ideal. The complement $Q \cup (-Q)$ of $\mathfrak{p}$ is closed under multiplication, hence $\mathfrak{p}$ is prime. The proof of Theorem 4. 1 is finished.

We call $\mathfrak{p}$ the prime ideal of A *associated* with the signature σ, and $\bar{\sigma}$ the signature of $A(\mathfrak{p})$ *induced* by σ. For the sets P and Q we write more precisely $\Gamma(\sigma)$[4]) and $Q(\sigma)$.

We return to π-rings. For x an element of a π-ring A we use the notations

$$S(x) = x + \bar{x}, \qquad N(x) = x\bar{x}. \tag{4. 5}$$

Notice that $S(x)$ and $N(x)$ lie in A_0 and $N(xy) = N(x)N(y)$.

Let (A, σ) be a pair with A_0 a *local* ring. Let σ_0 denote the restriction of σ to A_0, let $\mathfrak{p}_0$ denote the prime ideal of A_0 associated with σ_0 and $\bar{\sigma}_0$ denote the signature on $A_0(\mathfrak{p}_0)$ induced by σ_0.

Theorem 4. 6. (i) *There exists a unique prime ideal $\mathfrak{p}$ of A with $\mathfrak{p} \cap A_0 = \mathfrak{p}_0$. This prime ideal $\mathfrak{p}$ is the set of all x in A with $N(x) \in \mathfrak{p}_0$.*

(ii) *For every $x \in A \setminus \mathfrak{p}$ we have $N(x) \in Q(\sigma_0)$.*

(iii) *There exists a unique signature $\bar{\sigma}$ of $A(\mathfrak{p})$ which extends σ. (Notice that $\mathfrak{p}$ is stable under J_A.)*

(iv) *Regarding $A_0(\mathfrak{p}_0)$ as a subfield of $A(\mathfrak{p})$ we have $A_0(\mathfrak{p}_0) = A(\mathfrak{p})_0$, and $\bar{\sigma} | A_0(\mathfrak{p}_0) = \bar{\sigma}_0$.*

Proof. a) We shortly write Q instead of $Q(\sigma_0)$. We first show that the norm $N(x)$ of an arbitrary element x of A is not contained in $-Q$. Indeed, otherwise we would have an equation

$$N(x) + a_1 + \cdots + a_r = 0$$

with some a_i in $\Gamma(\sigma_0)$. From this we obtain

$$-a_1 = N(x) + a_2 + \cdots + a_r,$$

resp. $-a_1 = N(x)$ in the case $r = 1$, which contradicts [17], 2. 3.

[4]) The notation $\Gamma(\sigma)$ already occurs in [17].

b) We *define* $\mathfrak{p}$ as the set of all x in A with norm $N(x)$ in $\mathfrak{p}_0$. Let x and y be elements of $\mathfrak{p}$. We shall show that $z := x + y$ again lies in $\mathfrak{p}$. Suppose this is not true. Then by part a) of the proof $N(z) \in Q$. Now

$$N(z) = N(x) + N(y) + S(xy).$$

Since $N(x)$ and $N(y)$ lie in $\mathfrak{p}_0$, we obtain from Theorem 4. 1 (iii), that $S(xy)$ lies in Q. Again by Theorem 4. 1 (iii)

$$N(x - y) = N(x) + N(y) - S(xy) \in -Q.$$

This cannot be true by part a). Thus $N(z) \in \mathfrak{p}_0$. For x in A and y in $\mathfrak{p}$ the norm

$$N(xy) = N(x)N(y)$$

lies in $\mathfrak{p}_0$, hence $xy \in \mathfrak{p}$. Thus $\mathfrak{p}$ is an ideal. This ideal is prime, since $A \setminus \mathfrak{p}$ is multiplicatively closed.

c) Clearly $\mathfrak{p} \cap A_0 = \mathfrak{p}_0$. Assume $\mathfrak{a}$ is an ideal of A with $\mathfrak{a} \cap A_0 < \mathfrak{p}_0$. For x in $\mathfrak{a}$ the norm $x\bar{x}$ lies in $\mathfrak{a} \cap A_0 < \mathfrak{p}_0$, hence $x \in \mathfrak{p}$. Thus $\mathfrak{p} \supset \mathfrak{a}$. Since A is integral over A_0 this implies that $\mathfrak{p}$ is the only prime ideal of A lying over $\mathfrak{p}_0$ ([4], § 2, No. 1, p. 36). The field $A_0(\mathfrak{p}_0)$ has characteristic zero since it is real. Thus by [4], § 2, No. 2, Theorem 2, $A_0(\mathfrak{p}_0)$ is the field of fixed elements of the involution of $A(\mathfrak{p})$.

d) Since $N(x) \in Q$ for all x in $A \setminus \mathfrak{p}$, we have $\bar{\sigma}_0(N(c)) = 1$ for all elements $c \neq 0$ of $A(\mathfrak{p})$. (Of course $N(c)$ is again defined by 4. 5.)

Thus $\bar{\sigma}_0$ extends to a unique signature $\bar{\sigma}$ of $A(\mathfrak{p})$, cf. [17], Corollary 1. 6. Let τ denote the restriction of $\bar{\sigma}$ to A. Then $\tau \,|\, A_0 = \sigma_0$. This implies $\tau = \sigma$, since the canonical map from $W(A_0)$ to $W(A)$ is surjective. Assume finally that η is a signature on $A(\mathfrak{p})$ which extends σ. Then the restriction of η to A_0 is σ_0 and thus $\eta \,|\, A_0(\mathfrak{p}_0) = \bar{\sigma}_0$. This implies $\eta = \bar{\sigma}$. Theorem 4. 6 is proved.

We again call $\mathfrak{p}$ the prime ideal of A associated with σ and $\bar{\sigma}$ the signature of $A(\mathfrak{p})$ induced by σ. The following corollary of Theorem 4. 6 has central importance for the later sections of this paper.

Theorem 4. 7. *Let (A, σ) be an arbitrary pair. Then there exists a prime ideal $\mathfrak{p}$ of A stable under J_A such that σ can be extended to the field $A(\mathfrak{p})$.*

Proof. By Theorem 2. 4 there exists a signature τ of $A_{\mathfrak{m}}$ extending σ with $\mathfrak{m}$ a suitable maximal ideal of A_0. Let $\mathfrak{q}$ denote the prime ideal of $A_{\mathfrak{m}}$ associated with τ, and let $\mathfrak{p}$ be the inverse image of $\mathfrak{q}$ in A. The signature $\bar{\tau}$ of $A_{\mathfrak{m}}(\mathfrak{q}) = A(\mathfrak{p})$ extends σ.

For a given pair (A, σ) it would be desirable to have a description of the set $Z(\sigma)$ of all prime ideals $\mathfrak{p}$ of A with the properties states in Theorem 4. 7, or at least of the maximal elements in $Z(\sigma)$. If A is semilocal, then by the following theorem this set has still just one maximal element.

Theorem 4. 8.[5]) i) *Let (A, σ) be semi-local with trivial involution. Let $Q = Q(\sigma)$ denote the set of all finite sums $\lambda_1^2 a_1 + \cdots + \lambda_r^2 a_r$ with λ_i in A, a_i in A^*, $\sigma(a_i) = 1$ of $1 \leq i \leq r$, and $\lambda_1 A + \cdots + \lambda_r A = A$. Then the statements made in Theorem* 4. 1 *and Corollary* 4. 3 *about Q and the complement $\mathfrak{p}$ of $Q \cup (-Q)$ in A remain true.*

ii) *If (A, σ) is an arbitrary semi-local pair, then the statements of Theorem* 4. 6 *remain true.*

[5]) Theorem 4. 8 remains true for the weakly semi-local rings introduced in § 5.

The proof would interrupt our study of real closures too much, and will be postponed to Appendix B of this paper. We use the terms "prime ideal $\mathfrak{p}$ associated with σ" and "signature $\bar{\sigma}$ induced by σ on $A(\mathfrak{p})$" for semi-local pairs (A, σ) as above.

In general $Z(\sigma)$ will have several maximal elements.

Example 4. 9. Let $X \subset \mathbb{C}^n$ be an irreducible affine curve, defined over the field $\mathbb{R}$ of real numbers, which has real points. Let $Z_1, \ldots, Z_r$ denote the connected components of the set $X(\mathbb{R})$ of real points of X with respect to the strong topology, and let A denote the ring $\mathbb{R}[X]$ of regular functions on X, which are defined over $\mathbb{R}$, equipped with the trivial involution. We identify the points $\mathfrak{p} \in X(\mathbb{R})$ with the maximal ideals $\mathfrak{p}$ of A such that $A/\mathfrak{p} = \mathbb{R}$. Every $\mathfrak{p} \in X(\mathbb{R})$ yields a signature

$$\sigma_{\mathfrak{p}} : W(A) \to W(A/\mathfrak{p}) = \mathbb{Z}.$$

Since the functions in $\mathbb{R}[X]$ are continuous on $X(\mathbb{R})$ in the strong topology, all $\sigma_{\mathfrak{p}}$ with $\mathfrak{p}$ running through a fixed component Z_i coincide (cf. [12], 14. 2. 2). We denote this signature by σ_i. Since $\sigma_i \neq \sigma_j$ for $i \neq j$ (cf. [12], 14. 2. 2), we have

$$Z_i \subset Z(\sigma_i) \subset Z_i \cup \{0\}.$$

If Z_i consists of a single singular point of X, then it may happen that $Z(\sigma_i) = Z_i$, cf. [17], Example 1. 12. Otherwise Z_i contains a regular point $\mathfrak{p}$. Then σ_i extends to $A(\mathfrak{p})$ and a fortiori to $A_{\mathfrak{p}}$. Now every signature of $A_{\mathfrak{p}}$ can be extended to the quotient field $F = \mathbb{R}(X)$, cf. [17], Example 1. 13. Thus $Z(\sigma_i) = Z_i \cup \{0\}$.

We close this section mentioning a remarkable consequence of Theorem 4. 7. Let A be a real π-ring and let S denote the set of all finite sums $N(\lambda_1) + \cdots + N(\lambda_r)$ with λ_i in A and $\lambda_1 A + \cdots + \lambda_r A = A$. It is easily seen that S is multiplicatively closed.

Proposition 4. 10. *Every signature of A extends to the localization $S^{-1}A$. Thus $S^{-1}A$ again is real and the kernel of the canonical map from $W(A)$ to $W(S^{-1}A)$ consists of nilpotent elements.*

Proof. Let σ be a signature of A, and let $\mathfrak{p}$ be a prime ideal of A stable under J_A, such that σ extends to a signature τ of $A(\mathfrak{p})$. Every element s of S has image $\bar{s} \neq 0$ in $A(\mathfrak{p})$, since $A(\mathfrak{p})$ is real (cf. 2. 2). Thus the canonical map from A to $A(\mathfrak{p})$ factors through $S^{-1}A$. The restriction of τ to $S^{-1}A$ extends σ.

Corollary 4. 11. *Every signature of A extends to $\mathbb{Q} \otimes_{\mathbb{Z}} A$.*

This is clear since $\mathbb{Q} \otimes A$ is the localization of A with respect to the set of positive natural numbers, embedded into S.

§ 5. Generalization of the fundamental theorem of algebra

For A a connected ring with trivial involution we denote by $\bar{A}$ the universal covering of A in the category of rings without involution, reserving the notation $\tilde{A}$ as in the previous sections for the universal covering in the category of π-rings. We regard $\bar{A}$, equipped with the trivial involution, as a subring of $\tilde{A}$. This subring of $\tilde{A}$ is uniquely determined since $\bar{A}$ is galois over A. By the proof of Proposition 1. 5 the covering $\tilde{A}$ of $\bar{A}$ has degree $[\tilde{A} : \bar{A}] = 2$.

Theorem 5. 1. i) *Let (R, ϱ) be a real closed pair. Then $|R|$ is simply connected in the category of rings without involution, and $[\tilde{R} : R] = 2$.*

ii) *Let (T, τ) be a strictly real closed pair. Then $[\bar{T} : T] \leqq 2$.*

Proof. i) By Theorem 4. 7 there exists a morphism φ from (R, ϱ) into a pair (K, τ) with $|K|$ a field. Passing to a real closure of (K, τ) we may assume in addition that (K, τ) is real closed. By Proposition 1. 6 there exists a π-homomorphism ψ from $\tilde{R}$ to $\tilde{K}$ such that the diagram

$$\begin{tikzcd} \tilde{R} \arrow[r, "\psi"] & \tilde{K} \\ R \arrow[u, hook] \arrow[r, "\varphi"] & K \arrow[u, hook] \end{tikzcd}$$

commutes, the vertical maps being the inclusions. Now $[\tilde{K} : K] = 2$ by the classical fundamental theorem of algebra, cf. 3. 18. Let α' be the generator of $G(\tilde{K}/K)$. We see from Corollary 1. 16 that there exists a unique element α in $G(\tilde{R}/R)$ with $\psi \circ \alpha = \alpha' \circ \psi$. This implies $\psi \circ \alpha^2 = \psi$ and, again by Corollary 1. 16, $\alpha^2 = 1$. Let S denote the fixed ring of the π-automorphism α. Then $R < S$ and by Lemma 1. 12, S is a covering of R. Clearly $\psi(S)$ is contained in the fixed ring K of α'. Let $\chi : S \to K$ denote the restriction of ψ to S. The signature $\tau \circ \chi_*$ extends ϱ. But (R, ϱ) is real closed. Thus $R = S$. Again from Lemma 1. 12 we obtain $[\tilde{R} : R] \leqq 2$. But $|R|$ is connected and $|\tilde{R}|$ is not. Thus $[\tilde{R} : R] = 2$. From the proof of Proposition 1. 5 it now is immediately seen that $|R|$ is simply connected in the category of rings without involution.

ii) Let (T, τ) be a strictly real closed pair and let (R, ϱ) be a real closure of (T, τ). By Proposition 2. 8 we know $T = R_0$ and $[R : T] \leqq 2$. Since $|R|$ is simply connected we also have $[\bar{T} : T] \leqq 2$. (N. B. There exists an isomorphism from $|R|$ to $\bar{T}$ over T, but the subrings R and $\bar{T}$ of $\tilde{T}$ are certainly different if $T \neq \bar{T}$.) Another possibility to prove assertion (ii) is to repeat the main arguments used in the proof of (i), the category of π-rings being replaced by the category of rings without involution.

It may happen that $\bar{T} = T$ for a strictly real closed pair (T, τ) as show the following

Examples 5. 2. Let A be the ring $\mathbb{Z}$ with trivial involution. Then $W(A) = \mathbb{Z}$ ([20], p. 90). Furthermore by a theorem of Minkowski, $A = \bar{A}$ (e. g. [1], p. 162). The pair (A, σ) with σ the unique signature of A is certainly real closed and strictly real closed. An example of similar type is given by the ring B of integral algebraic numbers in $\mathbb{Q}(\sqrt{5})$. Again by use of Minkowski's lower estimate for the discriminant of algebraic number fields (cf. [1], p. 162) one easily sees that every proper algebric field extension of $\mathbb{Q}(\sqrt{5})$ is ramified over $\mathbb{Q}(\sqrt{5})$, i. e. $\bar{B} = B$. We further have $W(B) \cong \mathbb{Z} \times \mathbb{Z}$ ([20], p. 96). For both signatures ϱ_1 and ϱ_2 of B the pair (B, ϱ_i) is real closed and strictly real closed.

We now discuss two cases in which $[\bar{T} : T] = 2$. For any unit a of a ring A (no involution considered) we denote by $A[\sqrt{a}]$ the extension $B := A[X]/(X^2 - a)$. This extension B/A is finite etale if and only if 2 is a unit in A, as is immediately seen by reducing B modulo the maximal ideals of A.

Corollary 5. 3. *Assume (T, τ) is strictly real closed and 2 is a unit in T. Then $[\bar{T} : T] = 2$ and $\bar{T} \cong T[\sqrt{-1}]$.*

Proof. The π-ring $S := T[\sqrt{-1}]$ with trivial involution is non real, since the inner product space $(1, 1)$ over S is ~ 0 and thus $2\, W(S) = 0$. If S would not be connected, then S would be isomorphic to $T \times T$, but $T \times T$ is real. Thus S is a covering of T of degree 2. Since $[\bar{T} : T] \leqq 2$ we must have $\bar{T} \cong S$.

Let A be a ring (no involution considered). We call an extension $B > A$ of A a *quadratic Artin-Schreier extension*, if there exists a free basis of B over A consisting of two elements 1, ω such that $\omega^2 = \omega + a$ for some a in A with $1 + 4a \in A^*$. We call ω a Artin-Schreier-generator of B and often write $\omega = \frac{1}{\mathfrak{p}} a$. Clearly

$$A\left[\frac{1}{\mathfrak{p}} a\right] \cong A[X]/(X^2 - X - a),$$

and $A\left[\frac{1}{\mathfrak{p}} a\right]$ is finite etale over A, cf. [16], 5. 13. Notice that $A\left[\frac{1}{\mathfrak{p}} a\right] \cong A[\sqrt{1 + 4a}\,]$ if $2 \in A^*$, since $(1 - 2\omega)^2 = 1 + 4a$.

We call a π-ring C *weakly semi-local*, if C contains a semi-local π-subring C' such that C is integral over C'. Notice that coverings of semi-local rings in general are not semi-local but only weakly semi-local. The whole theory developed in [17] for semi-local rings immediately generalizes to weakly semi-local rings.

Assume now that our ring A with trivial involution is weakly semi-local. Then we can find some natural number $h \geqq 1$ such that $1 - 4h$ is a unit in A. Indeed, let A' be a semi-local subring of A with A integral over A'. Choose h in such a way that h is divided by all prime numbers $p \neq 2$ which occur as the characteristic of a field $A'/\mathfrak{m}'$ with $\mathfrak{m}'$ a maximal ideal of A'. For any such h clearly $1 - 4h$ is a unit in A.

Corollary 5. 4. *Let (T, τ) be strictly real closed and weakly semi-local. Let h be a positive natural number with $1 - 4h$ a unit of T. Then $[\overline{T} : T] = 2$ and $\overline{T} \cong T\left[\frac{1}{\mathfrak{p}}(-h)\right]$.*

Proof. As in the proof of Corollary 5. 2 it suffices to show that the π-ring $S := T\left[\frac{1}{\mathfrak{p}}(-h)\right]$ with trivial involution is non real. For $\omega := \frac{1}{\mathfrak{p}}(-h)$ we have $(1 - 2\omega)^2 = 1 - 4h$. If S would possess a signature σ, then $\sigma(4h - 1) = 1$, cf. [17], 1. 3. But $[(4h - 1)] = [(-1)]$ in $W(S)$, which implies $\sigma(4h - 1) = -1$. Thus S is indeed non real.

The following proposition generalizes parts of the Corollaries 5. 3 and 5. 4.

Proposition 5. 5. *Assume (T, τ) is strictly real closed, and that there exists a prime number p which is a unit in T. Then $[\overline{T} : T] = 2$.*

Proof. Let $p^{-\infty}\mathbb{Z}$ denote the ring of rational numbers whose denominator is a power of p, and let C denote the ring of algebraic numbers generated over $p^{-\infty}\mathbb{Z}$ by the p^r-th roots of unity with r running through all natural numbers. (It would suffice to consider the ring generated by the p-th roots of unity.) We regard C as a π-ring with trivial involution. The quotient field K of C is non real. Since by Corollary 4. 11 every signature of C extends to K (in a unique way, cf. [17], 2. 14), also C is non real. As is well known C is a covering of $p^{-\infty}\mathbb{Z}$. Since p is a unit in $\overline{T}$ we have a canonical map α from $p^{-\infty}\mathbb{Z}$ to $\overline{T}$. By Corollary 1. 7 there exists a homomorphism β from C to $\overline{T}$ such that the diagram

$$\begin{tikzcd} C \arrow[dr, "\beta"] & \\ p^{-\infty}\mathbb{Z} \arrow[u] \arrow[r, "\alpha"] & \overline{T} \end{tikzcd}$$

commutes. The image $\beta(C)$ cannot be contained in T since otherwise β and τ would yield a signature on C. Thus certainly $T \neq \overline{T}$. Now Theorem 5. 1 (ii) implies the assertion.

Appendix A. Complements on equivariant coverings

The goal of this appendix is to give some complements to the theory of equivariant coverings developed in § 1. In particular we shall prove here Proposition 1. 5 on the existence of universal coverings in full generality, thus closing a gap in § 1.

In contrast to the main body of the paper π here denotes an arbitrary finite group. Assume that ω is a subgroup of π and A is an ω-ring. We construct from A an "induced" π-ring $B = A^{\omega\to\pi}$ in the following way: As $\mathbb{Z}\pi$-module B is induced from A in the usual way, $B = \mathbb{Z}\pi \otimes_{\mathbb{Z}\omega} A$. For g in π and a in A we write (g, a) instead of $g \otimes a$. These symbols satisfy the relations

$$(gh, a) = (g, ha) \qquad \text{for } h \text{ in } \omega,$$

$$(g, a_1) + (g, a_2) = (g, a_1 + a_2), \quad g'(g, a) = (g'g, a).$$

Any element z in B can be written in the form

$$z = \sum_{i=1}^{r} (g_i, a_i)$$

with $\{g_1, \ldots, g_r\}$ a fixed set of representatives of π/ω, and the $a_i \in A$ uniquely determined by z. We make B a commutative ring by prescribing as multiplication

$$(g_i, a)(g_j, b) = \delta_{ij}(g_i, ab).$$

Then $(g, a)(g, b) = (g, ab)$ for arbitrary g in π and a, b in A, and $(g, a)(g', b) = 0$ if g and g' belong to different cosets of ω. Clearly B is a π-ring with unit element $\sum_{i=1}^{r} (g_i, 1)$.

Let γ_A denote the map from $A^{\omega\to\pi}$ to A with $\gamma_A(g, a) = 0$ if g is not in ω and $\gamma_A(1, a) = a$. Clearly γ_A is an ω-homomorphism, i. e. a ring homomorphism compatible with the actions of ω on both rings. Our construction of $A^{\omega\to\pi}$ is canonical in the following sense:

Proposition A. 1. *Let φ be an ω-homomorphism from a π-ring C to A. Then there exists a unique π-homomorphism $\psi: C \to A^{\omega\to\pi}$ with $\gamma_A \circ \psi = \varphi$. This homomorphism ψ is given by the formula*

$$\psi(c) = \sum_{i=1}^{r} (g_i, \varphi(g_i^{-1} c)).$$

The proof is an easy exercise. Proposition A. 1 implies in particular that every homomorphism $\alpha: A \to B$ between ω-rings induces a unique π-homomorphism β from $A^{\omega\to\pi}$ to $B^{\omega\to\pi}$ such that the diagram

$$\begin{tikzcd} A \arrow[r, "\alpha"] & B \\ A^{\omega\to\pi} \arrow[u, "\gamma_A"] \arrow[r, "\beta"] & B^{\omega\to\pi} \arrow[u, "\gamma_B"'] \end{tikzcd}$$

commutes. We denote β by $\alpha^{\omega\to\pi}$.

Proposition A. 2. *If A is a connected ω-ring then $A^{\omega\to\pi}$ is a connected π-ring.*

Proof. Let $f_1, \ldots, f_s$ denote the primitive idempotents of A. Then the elements (g_i, f_j) with $1 \leqq i \leqq r$, $1 \leqq j \leqq s$ are the primitive idempotents of $A^{\omega\to\pi}$. For a given (g_i, f_j) there exists some h in ω with $hf_1 = f_j$. Then $(g_i h)(1, f_1) = (g_i, f_j)$. Thus π acts transitively on the (g_i, f_j).

Assume now that A is a π-ring, e is an idempotent of A, and A_0 is the ring Ae, regarded as an ω-ring with ω the stability subgroup of e in A.

Proposition A. 3. *The π-homomorphism $\varphi: A \to A_0^{\omega\to\pi}$ induced by the canonical projection $p: A \to A_0$, $p(a) = ae$* (see Proposition A. 1), *is an isomorphism.*

Proof. We write B instead of $A_0^{\omega\to\pi}$ and e' for the idempotent $(1, e)$ of B. For every a in $A_0 = Ae$ we have $\varphi(a) = (1, a)$. Thus φ maps Ae bijectively to Be'. Since as additive groups

$$A = \bigoplus_{i=1}^{r} g_i(Ae), \qquad B = \bigoplus_{i=1}^{r} g_i(Be'),$$

clearly φ maps A bijectively to B.

In particular by taking as e a primitive idempotent we see that every connected π-ring A is isomorphic to a ring $A_0^{\omega\to\pi}$ with $|A_0|$ connected.

Lemma A. 4. *If $\varphi: A \to B$ is a covering of a connected ω-ring A, with ω a subgroup of π, then the map $\varphi': A^{\omega\to\pi} \to B^{\omega\to\pi}$ induced by φ is a covering of the connected π-ring $A^{\omega\to\pi}$.*

Proof. In fact, if φ is a finite covering then φ' is certainly finite etale, and thus again a finite covering, since by Proposition A. 2 both $A^{\omega\to\pi}$ and $B^{\omega\to\pi}$ are connected. From this the assertion follows for an arbitrary covering φ, since the functor $A \rightsquigarrow A^{\omega\to\pi}$ respects direct limits.

We now construct a universal covering of an arbitrary connected π-ring A, as promised in § 1. We choose a primitive idempotent e of A and regard the component $A_0 := Ae$ of $|A|$ as a ring without group action. We choose a universal covering $\psi_0: A_0 \to D$ of A_0 and denote by ψ the induced map from $A_0^{1\to\pi}$ to $D^{1\to\pi}$. We further denote by $\varphi: A \to A_0^{1\to\pi}$ the π-homomorphism associated in the sense of Proposition A. 1 to the canonical projection $a \to ae$ from A to A_0. Clearly for any a in A

$$\varphi(a) = \sum_g (g, g^{-1}a)$$

with g running through all elements of G with $g^{-1}a \in A_0$.

Theorem A. 5. $\psi \circ \varphi: A \to A_0^{1\to\pi} \to D^{1\to\pi}$ *is a universal covering of A.*

Proof. $A_0^{1\to\pi}$ and $D^{1\to\pi}$ are connected π-rings by Proposition A. 2. Furthermore $D^{1\to\pi}$ is simply connected by Lemma 1. 4, and ψ is a covering by Lemma A. 4. We now show that φ is finite etale and thus a finite covering. Then the theorem is proved. Let B denote the ring $A_0^{1\to\pi}$. The restriction $Ae \to B\varphi(e)$ of φ can be regarded as the diagonal map $A_0 \to A_0 \times \cdots \times A_0$ into a finite product of copies of A_0, and thus is finite etale. Since π acts transitively on the primitive idempotents of A, the map φ itself is finite etale.

Thus we have filled out the gap in § 1 and may now use the whole content of § 1.

We are able to state very precisely the relations between the coverings of a connected ω-ring A with ω a subgroup of π and the coverings of $A^{\omega\to\pi}$. Let $\varphi: A \to \tilde{A}$ be a universal covering of A. We denote the π-rings $A^{\omega\to\pi}$ and $(\tilde{A})^{\omega\to\pi}$ by A' and $\tilde{A}'$ respectively. By Lemma A. 4, φ induces a covering $\varphi': A' \to \tilde{A}'$. We regard φ and φ' as inclusion maps. Furthermore we identify $\tilde{A}$ with the subring $\tilde{A}'e$ of $\tilde{A}'$, where e denotes the idempotent $(1, 1)$ of A'. Thus we have a diagram of inclusions

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d, hook] & \tilde{A} \arrow[d, hook] \\ A' \arrow[r, hook] & \tilde{A}'. \end{tikzcd}$$

Proposition A. 7. *$\varphi' : A' \hookrightarrow \tilde{A}'$ is a universal covering of A'. The restriction map $\tau \to \tau | \tilde{A}$ from $G(A') = \mathrm{Aut}(\tilde{A}'/A')$ to $G(A)$ is an isomorphism. The inverse map sends $\sigma \in G(A)$ to $\sigma^{\omega \to \pi}$. The coverings $B < \tilde{A}$ of A correspond uniquely to the coverings $C < \tilde{A}'$ of A' by the relations*

$$C = B^{\omega \to \pi}, \qquad B = Ce.$$

If we identify $G(A')$ with $G(A)$ by the isomorphism described, then C and B correspond to the same closed subgroup of $G(A)$ (see Theorem 1. 11).

The proof is left to the reader. We finally describe a relation between the Galois group of a connected π-ring A and the ordinary Galois group of a component of $|A|$. According to the Propositions A. 3 and A. 7 we assume without serious loss of generality that $|A|$ itself is connected. Let D denote a universal covering of $|A|$, and let B denote the π-ring $|A|^{1 \to \pi}$. Finally let

$$A \underset{\varphi}{\hookrightarrow} B \to D^{1 \to \pi} = \tilde{A}$$

be the universal covering of A considered in Theorem A. 5. We clearly have an injective group homomorphism $r : \pi \to \mathrm{Aut}(B/A)$ defined by the formula

$$r(g)\,(g', a) = (g' g^{-1}, g a)$$

$\{g, g'$ in π, a in $A\}$. Since $[B : A]$ equals the order of π, this implies that B is galois over A with group $r(\pi)$. Now the restriction map from $G(A)$ to $G(B | A)$ is surjective, and the kernel $G(B)$ can be identified with $G(|A|)$ by Proposition A. 7. Thus we obtain

Proposition A. 8. *The sequence*

$$1 \to G(|A|) \xrightarrow{\Phi} G(A) \xrightarrow{\Psi} \pi \to 1,$$

defined by $\varphi(\alpha) = \alpha^{1 \to \pi}$, $\psi(\beta) = r^{-1}(\beta | B)$, $\{\alpha$ in $G(|A|)$, β in $G(A)\}$ is an exact sequence of continuous group homomorphisms.

One may ask whether this sequence splits.

Proposition A. 9. *The sequence in Proposition* A. 8 *splits if and only if there exists a π-action on the universal covering D of $|A|$ which extends the given π-action on A. More precisely these π-actions $\mu : \pi \times D \to D$ correspond uniquely to the multiplicative sections $s : \pi \to G(A)$ of ψ by the formula*

$$s(g)\,(g', a) = \big(g' g^{-1}, \mu(g, a)\big)$$

$\{g, g'$ in π, a in $D\}$. The fixring C of $s(\pi)$ in $\tilde{A}$ is isomorphic to the π-ring (D, μ), an isomorphism from (D, μ) to C being given by

$$a \mapsto \sum_{g \in \pi} \big(g, \mu(g^{-1}, a)\big).$$

We leave the proof, which is not difficult, to the reader. We see from Proposition A. 9 and the fundamental Theorem 1. 11, that if a π-action on the universal covering D of $|A|$ is known which extends the π-action on A, then in principle all equivariant coverings of A can be found from the ordinary coverings of $|A|$.

If A is a field, π has order > 2, and π operates faithfully on A, then certainly an action of π on D extending the action on A does not exist [3], and thus the sequence in Proposition A. 8 does not split. On the other hand, if π has order 2 then such actions on D are provided for arbitrary rings A by the signatures of A according to Theorem 5. 1.

Appendix B. The prime ideal associated with a signature of a semi-local ring

We prove Theorem 4. 8 stated in § 4 of the paper and give some further complements to § 4.

A always denotes a semi-local ring with involution, but everything done in this appendix can easily be generalized to the case that A is only weakly semi-local. Let σ be a fixed signature of A. We denote by P the set $\Gamma(\sigma)$ of all units a of A_0 with $\sigma(a) = 1$, and we denote by $Q(\sigma)$, or shortly by Q, the set of all sums

$$N(\lambda_1)a_1 + \cdots + N(\lambda_n)a_n$$

with arbitrary $n \geqq 1$, a_i in P, λ_i in A, and $A\lambda_1 + \cdots + A\lambda_n = A$.

Lemma B. 1. *The sets Q and $-Q$ have empty intersection.*

Proof. Suppose there exists an equation

$$N(\lambda_1)a_1 + \cdots + N(\lambda_r)a_r = -N(\mu_1)b_1 - \cdots - N(\mu_s)b_s$$

with a_i, b_j in P, λ_i, μ_j in A, and

$$A\lambda_1 + \cdots + A\lambda_r + A\mu_1 + \cdots + A\mu_s = A.$$

Then the hermitian space $E := (a_1, \ldots, a_r, b_1, \ldots, b_s)$ over A is isotropic and hence equivalent to a space F of smaller rank. But $\sigma(E) = \dim E$. This is a contradiction, since $\sigma(F) \leqq \dim F$, as is easily seen, cf. [15], Lemma 5. 11.

Since now we assume for some time that A has trivial involution.

Lemma B. 2. *Every z in Q has a presentation*

$$z = a_1 + \lambda_2^2 a_2 + \cdots + \lambda_n^2 a_n$$

with a_i in P and λ_i in A.

Proof. We choose a presentation

$$z = \lambda_1^2 a_1 + \lambda_2^2 a_2 + \cdots + \lambda_n^2 a_n$$

such that $\lambda_1 \in A \setminus \mathfrak{m}$ for as many as possible maximal ideals $\mathfrak{m}$ of A. If these are all maximal ideals of A, then λ_1 is a unit, hence $\lambda_1^2 a_1 \in P$, and the lemma is proved. Suppose there exists some maximal ideal $\mathfrak{m}$ of A with $\lambda_1 \in \mathfrak{m}$. Then we number the maximal ideals of A in such a way that λ_1 does not lie in $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$, but does lie in the remaining maximal ideals $\mathfrak{m}_{s+1}, \ldots, \mathfrak{m}_t$. Among the coefficients $\lambda_2, \ldots, \lambda_n$ at least one does not lie in $\mathfrak{m}_{s+1}$, and we assume without loss of generality that λ_2 does not lie in $\mathfrak{m}_{s+1}$. We now choose elements ξ and η in A such that

$$\xi \equiv 1, \ \eta \equiv 0 \bmod \mathfrak{m}_i \quad \text{for} \quad i \neq s+1, \qquad \xi \equiv 0, \ \eta \equiv 1 \bmod \mathfrak{m}_{s+1}.$$

The element $c := \xi^2 + \eta^2 b_2$ with $b_2 := a_1^{-1} a_2$ lies in P, and we have the identity

$$(\lambda_1^2 a_1 + \lambda_2^2 a_2)c = (\lambda_1\xi - \lambda_2\eta b_2)^2 a_1 + (\lambda_1\eta + \lambda_2\xi)^2 a_2.$$

Thus

$$z = \mu_1^2 c^{-1} a_1 + \mu_2^2 c^{-1} a_2 + \lambda_3^2 a_3 + \cdots + \lambda_n^2 a_n,$$

with

$$\mu_1 = \lambda_1\xi - \lambda_2\eta b_2, \ \mu_2 = \lambda_1\eta + \lambda_2\xi.$$

Now μ_1 apparently does not lie in $\mathfrak{m}_1, \ldots, \mathfrak{m}_{s+1}$. This is a contradiction to the maximality of s. Thus in our original presentation of z the coefficient λ_1 is indeed a unit.

Lemma B. 3 (cf. Lemma 4. 4). *Let x and y be elements of A with $x+y$ lying in Q. Then at least one of the elements x and y lies in Q.*

Proof. By the previous lemma we have a presentation

$$x + y = a_1 + \lambda_2^2 a_2 + \cdots + \lambda_n^2 a_n$$

with a_i in P and λ_i in A. Replacing x by $a_1^{-1}x$ and y by $a_1^{-1}y$ we assume without loss of generality $a_1 = 1$. Now choose elements ξ and η in A such that for every maximal ideal $\mathfrak{m}$ of A the following holds true: If $y \not\equiv 1 \bmod \mathfrak{m}$ then $\xi \equiv 1$ and $\eta \equiv 0 \bmod \mathfrak{m}$, and otherwise $\xi \equiv 0$ and $\eta \equiv 1 \bmod \mathfrak{m}$. The element $c := \xi^2 + \eta^2$ lies in P, and we have

$$x + y = \xi^2 c^{-1} + \eta^2 c^{-1} + \lambda_2^2 a_2 + \cdots + \lambda_n^2 a_n.$$

Now $cy - \xi^2 = \xi^2(y-1) + \eta^2 y$ is apparently a unit, and hence also the element $z := y - \xi^2 c^{-1}$ is a unit. Thus either $z \in P$ or $z \in -P$. In the first case $y = z + \xi^2 c^{-1}$ lies in Q. In the second case

$$x = -z + \eta^2 c^{-1} + \lambda_2^2 a_2 + \cdots + \lambda_n^2 a_n$$

lies in Q.

Let $\mathfrak{p}$ denote the complement of $Q \cup (-Q)$ in A. Then we see as in § 4 in the local case that $\mathfrak{p}$ is an additive subgroup of A with $Q + \mathfrak{p} = Q$.

We now want to prove $Q\mathfrak{p} < \mathfrak{p}$. Since for a in P we have $aQ = Q$, $a(-Q) = -Q$, and thus $a\mathfrak{p} = \mathfrak{p}$, it suffices to show $\lambda^2\mathfrak{p} < \mathfrak{p}$ for an arbitrary element λ of A.

Given some λ in A we choose an element μ in A such that $\lambda^2 + \mu^2$ is a unit. This is always possible. Let x be an element of $\mathfrak{p}$. We have $\lambda^2 x + \mu^2 x \in \mathfrak{p}$, since $\lambda^2 + \mu^2$ lies in P and $P\mathfrak{p} = \mathfrak{p}$. Suppose $\lambda^2 x$ lies in $-Q$. Then $\mu^2 x$ lies in $Q + \mathfrak{p} = Q$, and we have presentations

$$-\lambda^2 x = \sum_{i=1}^{r} \gamma_i^2 a_i, \qquad \mu^2 x = \sum_{j=1}^{s} \delta_j^2 b_j$$

with a_i, b_j in P, and

$$\sum_{i=1}^{r} \gamma_i A = \sum_{j=1}^{s} \delta_j A = A.$$

This implies

$$\sum_{i=1}^{r} \gamma_i^2 \mu^2 a_i + \sum_{j=1}^{s} \delta_j^2 \lambda^2 b_j = 0,$$

and proves that 0 lies in Q. But this is a contradiction already to Lemma B. 1. Thus $\lambda^2 x$ does not lie in $-Q$. Replacing x by $-x$ we see that $\lambda^2 x$ does not lie in Q either. Thus $\lambda^2 x \in \mathfrak{p}$, and $Q\mathfrak{p} = \mathfrak{p}$ is proved.

We now obtain as in the local case $A\mathfrak{p} = \mathfrak{p}$. Since $A \setminus \mathfrak{p}$ is closed under multiplication, $\mathfrak{p}$ is a prime ideal. The first part of Theorem 4. 8 is proved. We call $\mathfrak{p}$ the prime ideal associated with σ.

We finally consider the case that A has non trivial involution. Let σ_0 denote the restriction $\sigma | A_0$, and let $\mathfrak{p}_0$ denote the prime ideal of A_0 associated with σ_0. We know already from the proof of Lemma B. 1 that for every x in A the norm $N(x)$ does not lie in $-Q(\sigma_0)$. Now the reader may check that the parts b) and c) of the proof Theorem 4. 6 remain valid word by word in our more general situation. Thus all statements of Theorem 4. 6 remain true in the semi-local case, and the proof of Theorem 4. 8 is complete.

We mention the following consequence of Theorem 4. 8.

Proposition B. 4. $Q(\sigma) = Q(\sigma_0)$.

Proof. Clearly $Q(\sigma_0) < Q(\sigma)$. Let now x be an element of $Q(\sigma)$,

$$x = N(\lambda_1)a_1 + \cdots + N(\lambda_n)a_n$$

with a_i in P and $\lambda_1 A + \cdots + \lambda_n A = A$. If a coefficient λ_i lies in $A \setminus \mathfrak{p}$, then $N(\lambda_i)a_i$ lies in $Q(\sigma_0)$. Otherwise $N(\lambda_i)a_i$ lies in $\mathfrak{p}_0$. Since not all λ_i lie in $\mathfrak{p}$, we obtain $x \in Q(\sigma_0)$.

Under mild restrictions on A we have a very simple description of $Q(\sigma)$.

Proposition B. 5. *Assume A_0 has no residue class field $A_0/\mathfrak{m}$ with less then four elements. Then the elements of $Q(\sigma)$ are the sums $a + b$ with a and b in $\Gamma(\sigma)$.*

Proof. i) By the preceding Proposition B. 4 we may assume that A has trivial involution. Let z be an arbitrary element of $Q := Q(\sigma)$. We first show that we have a presentation

$$(*) \qquad z = a_1 + \cdots + a_r$$

with $r \geqq 2$ elements a_i of $P := \Gamma(\sigma)$. According to Lemma B. 2 we have an equation

$$z = b_1 + \lambda_2^2 b_2 + \cdots + \lambda_s^2 b_s$$

with $s \geqq 2$ elements b_i of P and elements $\lambda_2, \ldots, \lambda_s$ of A. It suffices to find a presentation (*) in the case $s = 2$. Then we immediately obtain such a presentation in the general case by induction on s. Replacing z by $b_1^{-1}z$ we further may assume $b_1 = 1$. Thus we are reduced to the case $z = 1 + \lambda^2 b$ with b in P and λ in A. We choose an element η of A such that $\eta \not\equiv 0$, $\eta^2 b \not\equiv -1 \mod \mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ with $\lambda \in \mathfrak{m}$, and $\eta \equiv 0 \mod \mathfrak{m}$ for the remaining $\mathfrak{m}$. Then $c := 1 + \eta^2 b$ lies in P and

$$z = (1 - b\eta\lambda)^2 c^{-1} + (\lambda + \eta)^2 b c^{-1}$$

is a presentation of z as a sum of two elements of P.

ii) Starting from the presentation (*) we now show that z is a sum of two elements of P. It suffices to consider the case $r = 3$. Then our assertion will follow for arbitrary r by induction. We shall choose elements α, β in A such that the elements

$$c := \alpha^2 + \beta^2, \quad \alpha^2(a_1 + a_3) + \beta^2 a_1, \quad \alpha^2 a_2 + \beta^2(a_2 + a_3)$$

are units. If this is done, $z = (a_1 + \alpha^2 a_3 c^{-1}) + (a_2 + \beta^2 a_3 c^{-1})$ will be a presentation of z as a sum of two elements of P. To obtain the elements α, β with the desired properties we prescribe the images of α, β in the fields $A/\mathfrak{m}$ with $\mathfrak{m}$ running through the maximal ideals of A in the following way: If $a_1 + a_3 \not\equiv 0 \mod \mathfrak{m}$, then $\alpha \equiv 1$, $\beta \equiv 0 \mod \mathfrak{m}$. If $a_2 + a_3 \not\equiv 0 \mod \mathfrak{m}$, then $\alpha \equiv 0$, $\beta \equiv 1 \mod \mathfrak{m}$. Finally if $a_1 + a_3$ and $a_2 + a_3$ both lie in $\mathfrak{m}$, we impose the conditions $\alpha \equiv 1$, $\beta \not\equiv 0$, $\beta^2 \not\equiv -1 \mod \mathfrak{m}$. All these conditions can be fulfilled simultaneously, since A is semi-local and all residue class fields $A/\mathfrak{m}$ contain more than two elements.

Remark B. 6. If A_0 is a local ring with maximal ideal $\mathfrak{m}$, then without any further restriction on A every element z of $Q(\sigma)$ is an element of $\Gamma(\sigma)$ or a sum of two elements of $\Gamma(\sigma)$, as is easily seen, cf. Remark 4. 2. If $A_0/\mathfrak{m}$ contains at least three elements, then z can always be written as a sum of two elements of $\Gamma(\sigma)$, since there exist units α and β of A_0 such that $\alpha^2 + \beta^2$ is again a unit.

References

[1] *E. Artin*, Theory of Algebraic Numbers, Lecture Notes, Göttingen 1959.

[2] *E. Artin* and *O. Schreier*, Algebraische Konstruktion reeller Körper, Hamb. Abh. **5** (1926), 85—99.

[3] *E. Artin* and *O. Schreier*, Eine Kennzeichnung der reell abgeschlossenen Körper, Hamb. Abh. **5** (1927), 225—231.

[4] *N. Bourbaki*, Algèbre commutative, Chap. 5, Actualités Sci. Indust., no 1308, Paris 1964.

[5] *S. U. Chase, D. K. Harrison* and *A. Rosenberg*, Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc. No. **52** (1965), 15—33.

[6] *A. Dress*, Contributions to the theory of induced representations, Proceedings of the Seattle conference on algebraic K-theory 1972, vol. 2; Lecture Notes Math. **342**, Berlin-Heidelberg-New York 1973.

[7] *A. Dress*, The Witt ring as Mackey functor, Notes on the theory of representations of finite groups I, Chap. 2, Appendix A, Univ. Bielefeld 1971.

[8] *F. DeMeyer* and *E. Ingraham*, Separable algebras over commutative rings, Lecture Notes Math. **181**, Berlin-Heidelberg-New York 1971.

[9] *A. Grothendieck*, Éléments de géométrie algébrique, IV, 4, Inst. Hautes Et. Sci., Publ. Math. No. **32** (1967).

[10] *D. K. Harrison*, Wittrings, Lecture Notes, Dept. Math. Univ. Kentucky, Lexington, Kentucky 1970.

[11] *T. Kanzaki* and *K. Kitamura*, On prime ideals of a Wittring over a local ring, Osaka J.Math. **9** (1972), 225—229.

[12] *M. Knebusch*, Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen, Sitzber. Heidelberg. Akad. Wiss. Math.-naturw. Kl. 1969/70, 3 Abh. (also obtainable as single volume from Springer Verlag).

[13] *M. Knebusch*, Real closures of semi-local rings, and extension of real places, Bull. Amer. Math. Soc. **79** (1973), 78—81.

[14] *M. Knebusch*, On the uniqueness of real closures and the existence of real places, Comment. Math. Helv. **47** (1972), 260—269.

[15] *M. Knebusch*, Generalization of a theorem of Artin-Pfister to arbitrary semi-local rings, and related topics. J. of Algebra, to appear.

[16] *M. Knebusch, A. Rosenberg* and *R. Ware*, Structure of Wittrings and quotients of abelian group rings, Amer. J. Math. **43** (1972), 657—673.

[17] *M. Knebusch, A. Rosenberg, R. Ware*, Signatures on semilocal rings, J. Algebra **26** (1973), 208—250.

[18] *M. Knebusch, A. Rosenberg, R. Ware*, Grothendieck and Wittrings of hermitian forms over Dedekind rings, Pacific J. Math. **43** (1972), 657—673.

[19] *J. Leicht* and *F. Lorenz*, Die Primideale des Wittschen Ringes, Invent. math. **10** (1970), 82—88.

[20] *J. Milnor* and *D. Husemoller*, Symmetric bilinear forms, Ergebnisse Math. 73, Berlin-Heidelberg-New York 1973.

Fachbereich Mathematik der Universität, 8400 Regensburg, Universitätsstr. 31

Eingegangen 2. Juli 1973