Real closures of commutative rings II.

Manfred Knebusch

Journal für die reine und angewandte Mathematik
Band 286/287

This is the second and final part of a paper [K_o] dedicated to Helmut Hasse on his 75. birthday. The emphasis will be on local studies, and the central result is the main theorem 10.12 at the end of § 10. This is a theorem about semi-local rings with involution, which in the special case of trivial involution tells us, that the signatures of the semi-local ring A correspond uniquely to the conjugacy classes of elements of order 2 in the Galois group $G(\overline{A}|A)$.

In § 9 we present some applications of our results about real closures to the structure theory of Witt rings, partially announced already in [K_1]. In particular we try to obtain some information about the subring N(A) of a Witt ring W(A) generated by the "natural forms" over A, i.e. the forms $Tr_{B/A}(x\overline{y})$ with B running through the finite etale extensions of A. This section is not needed for the proof of the main theorem and thus may be skipped by readers interested only in this theorem.

In § 11 we discuss the perhaps easiest global situation of interest, namely real closures of affine curves over the field of real numbers. Our results support the hope that here a theorem completely analogous to Theorem 10.12 holds true, cf. Question 11.11.

The terminology and notations developed in part I of the paper [K_o] will be used throughout without further explanation.

Contents.

§ 6 The involution of a real closure

We need - also for later sections - some more terminology. Let A be a π-ring with trivial involution.

Definitions 6.1. i) We call A strictly simply connected, if A is simply connected in the category of rings without involution.
ii) Let A be connected. Then we call a covering $\varphi : A \to T$ of A a strict universal covering, if T has trivial involution and T is strictly simply connected.

In § 5 we introduced the notation $\overline{A}$ for the unique subring of $\tilde{A}$ containing A which is a strict universal covering of A.

We now consider an arbitrary real closed pair (R,ρ). We denote by ρ_o the restriction of ρ to the fixed ring R_o of the involution J_R. We know from Prop. 3.17 that (R_o,ρ_o) is strictly real closed. In § 5 we have seen that $[\overline{R}_o:R_o] \leq 2$, and in fact $[\overline{R}_o:R_o] = 2$ if there exists a rational prime number p which is a unit in R.

The goal of the present small section is to prove

Theorem 6.2. Assume that R_o is not strictly simply connected (e.g. $p \in R^*$ for some prime number p). Then the involution of R is non degenerate.

This theorem clearly implies

Corollary 6.3. Let (R,ρ) be an arbitrary real closed pair. Then (R_o,ρ_o) is strictly real closed and (R,ρ) is the real closure of (R_o,ρ_o).

To prove Theorem 6.2 we consider a real closure (S,σ) of the strictly real closed pair (R_o,ρ_o). According to § 5 the ring $|S|$ is

simply connected. Thus by our assumption S is a covering of R_o of degree 2. Clearly the involution J_S is non degenerate and the fixed ring of J_S is R_o. By Th.3.9 there exists a morphism

$$\beta : (S,\sigma) \to (R,\rho)$$

which is the identity on R_o. We want to show that β is an isomorphism, which will prove our theorem.

The R_o-module R bears the hermitian form

$$b : R \times R \to R_o, \quad b(x,y) = x\bar{y} + \bar{x}y,$$

and S bears an hermitian form b' defined in the same way. Our map β is isometric with respect to b' and b, since β is π-equivariant. Now the form b' on S is non singular. {Indeed, the class of (S,b') in $W(R_o)$ is the element $Tr^*_{S/R_o}(1)$ studied already in § 3.} Thus β is certainly injective. Since now we regard S as a subring of R and β as the inclusion map.

We have to show S = R. We pick an arbitrary maximal ideal $\mathfrak{m}$ of R_o and denote by A,B,C the localized rings $R_{o\mathfrak{m}}$, $R_{\mathfrak{m}}$, $S_{\mathfrak{m}}$ respectively. It suffices to prove B = C. We use again the letter b for the hermitian form induced on B by the form b above on R. Let W be the set of all x in B with b(x,C) = 0. Since C is a non singular submodule of B, we have the orthogonal decomposition

$$(*) \qquad B = C \perp W.$$

Moreover

$$(**) \qquad CW \subset W,$$

since C is stable under J_B and

$$b(x\bar{y},z) = b(x,yz)$$

for x,y,z in B. Now the A-module C has a free basis $1,\omega$ with the relation $\omega^2-\omega = a$ for some a in A, such that $1+4a$ is a unit of A, cf. [KRW_2, 5.13] or [Sm]. The involution of C is given by $\bar{\omega} = 1 - \omega$. We consider the element $u := 1 - 2\omega$ of C, which is a unit of B since $u^2 = 1+4a$. By (**) we have $uW \subset W$. But on the other hand $\bar{u} = -u$, and also $\bar{w} = -w$ for every w in W since $b(w,1) = 0$. Thus uW is contained in the fixed ring A of the involution of B, and a fortiori $uW \subset B$. From (*) we obtain $uW = 0$ and then $W = 0$, since u is a unit. Thus $B = C$, and our theorem is proved.

Example 6.4. Let R be the ring $\mathbb{Z}[\sqrt{-1}]$ equipped with the involution $\sqrt{-1} \mapsto -\sqrt{-1}$. The ring $|R|$ is simply connected, as can be deduced from Minkowski's lower estimate for the discriminants of algebraic number fields as in the previous examples 5.2. The π-ring $\mathbb{Q} \otimes_{\mathbb{Z}} R$, i.e. the quotient field of R with the involution induced by J_R, has a unique signature, and thus by Cor. 4.11 also R has a unique signature ρ. The pair (R,ρ) is real closed, but J_R is degenerate.

§ 7 Real closures of semi-local rings.

We first derive a general result on the extension of signatures.

Definition 7.1. Let A be an arbitrary commutative ring (without π-action). A ring extension $B \supset A$ is called a quadratic etale extension of A, if B is etale over A and for every maximal ideal $\mathfrak{m}$ of A the $A_{\mathfrak{m}}$-module $B_{\mathfrak{m}}$ is free of rank 2.

If A is weakly semi-local (cf.§ 5), then every quadratic etale extension of A is an Artin-Schreier extension $A[\frac{1}{f}a]$ with some a in A such that 1+4a is a unit, as defined in § 5, cf. [KRW_2, 5.13] or [Sm].

In general we have for every quadratic etale extension B/A a unique automorphism α of B such that A is the fixed ring of α [Sm]. Indeed, by a standard argument it suffices to show this for the localizations $B_{\mathfrak{m}}/A_{\mathfrak{m}}$ with $\mathfrak{m}$ running through the maximal ideals of A, i.e. we may assume that A is local. Then $B = A + A\omega$ with an Artin-Schreier generator ω. One immediately checks that there exists precisely one automorphism α of B over A different from the identity, defined by $\alpha(\omega) = 1-\omega$, and that indeed α has the fixed ring A.

We have $\alpha^2 = 1$, and we call α the canonical involution of B/A. We now regard A and B as π-rings with trivial involution, and we denote by B' the ring B equipped with the involution α.

Proposition 7.2. Let B be a quadratic etale extension of A. Every signature σ of A can be extended to precisely one of the π-rings B and B'. If B is an Artin-Schreier extension $A[\frac{1}{f}a]$ then σ extends to B if and only if $\sigma(1+4a) = 1$ (cf.[KRW_2, 5.15]).

Proof. Let $\alpha : (A,\sigma) \to (K,\tau)$ be a morphism into a strictly real closed pair (K,τ) with K a field. Such a morphism exists by § 4. Further let $B \otimes_A K$ denote the tensor product of B and K over A constructed by use of α. Then $B \otimes_A K$ is a quadratic etale extension of K and $(B \otimes K)' = B' \otimes K$. Now by Th. 3.15 the signature σ can be extended to B {resp. B'} if and only if τ can be extended to $B \otimes K$ {resp. $B' \otimes K$}. Thus we see that it suffices to prove both assertions in the case that A is a field and (A,σ) is real closed. Assume a is an element of A with $B = A[\frac{1}{p}a]$. Then $B = A[\sqrt{c}]$ with $c = 1+4a$.

1. Case: $\sigma(c) = 1$. Then c is a square in A, and $B \cong A \times A$, the inclusion map from A to B corresponding to the diagonal embedding. σ has two extensions to B, but no extension to B', since $W(B') = 0$.

2. Case: $\sigma(c) = -1$. Then $B \cong \overline{A}$. We have $W(A) = W(B') = \mathbb{Z}$ and $W(B) = \mathbb{Z}/2\mathbb{Z}$. Thus σ has no extension to B and one extension to B'.

q.e.d.

Let now (R,ρ) be a real closed and weakly semi-local pair, and let ρ_o denote the restriction of ρ to R_o. By Prop. 3.17 the pair (R_o,ρ_o) is strictly real closed. We have seen in § 6 that the involution of R is non degenerate. Thus R is a quadratic etale extension of R_o. Choosing a natural number $h \geq 1$ with $4h-1$ a unit in R_o we have according to § 5 the following explicit description of R over R_o. (Notice that $|R|$ is the ~~strict~~ universal covering of $|R_o|$, and apply Cor. 5.4.)

(7.3) $\quad R = R_o + R_o\omega,\ \omega^2 - \omega = -h,\ \overline{\omega} = 1 - \omega.$

We want to prove

Theorem 7.4. $W(R) \cong \mathbf{Z}$. In particular ρ is the unique signature of R.

To prove this theorem we need three lemmata.

Lemma 7.5. Assume a is an element of R_o with $1+4a \in R_o^*$ and $\rho_o(1+4a) = 1$. Then $a = b^2 - b$ with some b in R_o, and thus $1+4a = (1-2b)^2$.

Proof. By Prop. 7.2 the signature ρ_o can be extended to the Artin-Schreier extension $R_o[\sqrt{a}]$, equipped with the trivial involution. Since (R_o, ρ_o) is strictly real closed, this implies that $R_o[\sqrt{a}]$ is not connected, and then

$$R_o[\sqrt{a}] = R_o e + R_o(1-e)$$

with an idempotent e. We thus have elements b,c in R_o such that

$$z := be + c(1-e)$$

fulfills the equation $z^2 - z = a$. This means $b^2 - b = c^2 - c = a$.

q.e.d.

Lemma 7.6. Let B be a ring with trivial involution which is strictly simply connected and weakly semi-local. Then for every maximal ideal $\mathfrak{M}$ of B the field $B/\mathfrak{M}$ is separably closed.

Proof. Assume $\mathfrak{M}_o$ is a maximal ideal of B such that $B/\mathfrak{M}_o$ is not separably closed, and let

$$p_o(t) = t^n + a_1 t^{n-1} + \ldots + a_n$$

be an irreducible separable polynomial of degree $n > 1$ over $B/\mathfrak{M}_o$.

We choose a semi-local subring B' of B such that B is integral over B' and the subfield $B'/\mathfrak{M}_o \cap B'$ of $B/\mathfrak{M}_o$ contains all coefficients a_i of $p_o(t)$. Let $m_o = \mathfrak{M}_o \cap B'$, $m_1, \ldots, m_r$ denote the finitely many maximal ideals of B'. We choose for every i with $1 \leqslant i \leqslant t$ a separable polynomial

$$p_i(t) = t^n + a_1^{(i)} t^{n-1} + \ldots + a_n^{(i)}$$

of degree n over B'/m_i. Indeed, if B'/m_i is finite we may choose $p_i(t)$ as an irreducible polynomial, and if B'/m_i is infinite we may choose $p_i(t)$ as a product of different linear polynomials. By the "Chinese remainder theorem" we find a polynomial

$$p(t) = t^n + \alpha_1 t^{n-1} + \ldots + \alpha_n$$

in $B'[t]$, whose image in $(B'/m_i)[t]$ is $p_i(t)$ for $0 \leqslant i \leqslant r$. Clearly the ring $C := B[t]/(p(t))$ is a finite etale extension of B. If C would not be connected then also $C/\mathfrak{M}_o C$ would not be connected, which contradicts the irreducibility of $p_o(t)$. Thus C is a covering of B of degree $n > 1$. This is a contradiction, since B is strictly simply connected. Thus $B/\mathfrak{M}_o$ must be separably closed.

q.e.d.

Returning to our real closed pair (R,ρ) we obtain from Lemma 7.6 the following

Corollary 7.7. Let $\mathfrak{m}$ be a maximal ideal of R_o. If $\mathfrak{m}R$ is not a maximal ideal of R, then the field $R_o/\mathfrak{m}$ is separably closed. If $\mathfrak{m}R$ is maximal, then the field $R_o/\mathfrak{m}$ is strictly real closed (= real closed in classical terminology).

Proof. In the first case

$$R/\mathfrak{m}R \cong R_o/\mathfrak{m} \times R_o/\mathfrak{m}$$

(with the involution at the right hand side interchanging the factors), and thus $R_o/\mathfrak{m}$ is separably closed by the previous lemma. In the second case $R/\mathfrak{m}R$ is a separably closed field, again by the previous lemma, and this field has degree 2 over $R_o/\mathfrak{m}$. Thus by a well known theorem of Artin and Schreier [AS_2] the field $R_o/\mathfrak{m}$ is strictly real closed.

q.e.d.

Lemma 7.8. Let a be a unit of R_o. Then $\rho(a) = 1$ if and only if a is the norm $N(\varepsilon) = \varepsilon\bar{\varepsilon}$ of some unit ε of R.

Proof. For every ε in R^* the spaces (1) and $(N(\varepsilon))$ over R are isometric and thus $\rho(N(\varepsilon)) = 1$. Assume now that a is a unit of R_o with $\rho(a) = 1$. We choose the number h occuring in the description (7.3) of R/R_o as an odd number such that $h \not\equiv 0 \bmod p$ and $4h \not\equiv 1 \bmod p$ for all the finitely many odd prime numbers which may occur as the characteristics of some residue class field $R_o/\mathfrak{m}$ of R_o. Then both h and 4h-1 are units in R_o. We have to solve the equation

$$a = N(x+y\omega) = x^2 + xy + hy^2$$

with x and y in R_o. Since by Cor. 7.7 all fields $R_o/\mathfrak{m}$ have infinitely many elements there exists a unit c of R_o such that for $b := ac^2$ the three elements

$$1-bh,\ 4+b(1-4h),\ 4h^2b+(1-4h)$$

are units in R_o. Indeed such a unit c can be found in any semi-local

subring A of R_o containing a, such that R_o is integral over A and all residue class fields of A contain more then 7 elements.

Having fixed such a unit c we first consider the case that $\rho(1-bh) = 1$. Since also $\rho(b) = 1$, we have $\rho(b^{-1}-h) = 1$. Now also

$$1+4(b^{-1}-h) = b^{-1}\{4+b(1-4h)\}$$

is a unit, and according to a general rule about signatures [KRW_2, 2.3] we obtain

$$\rho(1+4(b^{-1}-h)) = 1.$$

By Lemma 7.5 there exists some x in R_o with

$$b^{-1}-h = x^2-x.$$

Thus

$$b^{-1} = x^2-x+h$$

is a norm, and also $a = b^{-1}b^2c^{-2}$ is a norm.

We now consider the remaining case that $\rho(1-bh) = -1$. Then $\rho(bh^2-h) = 1$, and hence also the unit

$$1+4(bh^2-h) = 4h^2b+(1-4h)$$

has value +1 under ρ. Again by Lemma 7.5 there exists some x in R_o with

$$bh^2-h = x^2-x.$$

Thus bh^2 is a norm, which implies that a is norm.

q.e.d.

Theorem 7.4 is now an immediate consequence of Lemma 7.8. The ring $W(R)$ is generated by the elements $[(a)]$ with a in R_o^*. According to Lemma 7.6 we have $(a) \cong (1)$ if $\sigma(a) = 1$, and thus also $(a) \cong (-1)$ if $\sigma(a) = -1$. Therefore $W(R) = \mathbb{Z}[(1)]$. Since R is real, $[(1)]$ is not a torsion element, and $W(R) \cong \mathbb{Z}$.

We state a consequence of Theorem 7.4.

Corollary 7.9. Let (T,τ) be a weakly semi-local pair with trivial involution, and assume that (T,τ) is strictly real closed. Then τ is the only signature of T and

$$W(T) = \mathbb{Z} \oplus \mathfrak{N}$$

with $\mathfrak{N}$ the nilradical of $W(T)$.

Proof. Let h denote a natural number ≥ 1 with $1-4h$ a unit in T. Then the strict universal covering $\overline{T}$ of T has according to Cor. 5.4 the form

$$\overline{T} = T\left[\tfrac{1}{\beta}(-h)\right].$$

Let R denote the π-ring $(\overline{T})'$, i.e. the strict universal covering of T equipped with the automorphism $\alpha \neq id$ of $\overline{T}/T$ as involution. Let σ be an arbitrary signature of T. The π-ring $\overline{T}$ (with trivial involution) is non real, since $-(4h-1)$ is a square in $\overline{T}$. Thus σ certainly cannot be extended to $\overline{T}$. By Prop. 7.2 the signature σ extends to a signature ρ of R. Since $|R|$ is simply connected in the category of rings without involution, the pair (R,ρ) must be real closed. Now Theorem 7.4 tells us that ρ is the only signature of R. This implies that σ is the only signature of T, and we have $\sigma = \tau$. Clearly

$$W(T) = \mathbb{Z} \oplus \mathrm{Ker}(\tau).$$

Since τ is the only signature of T, the ideal $\mathrm{Ker}(\tau)$ is the only minimal prime ideal of T, cf. Th. 2.3, and thus $\mathrm{Ker}(\tau) = \mathfrak{N}$.

q.e.d.

Definitions 7.10. i) Let R be a weakly semi-local π-ring. We call R real closed if R possesses a signature ρ such that (R,ρ) is real closed, and we call R strictly real closed if R has trivial involution and possesses a signature ρ such that (R,ρ) is strictly real closed. These definitions are natural, since by Th. 7.4 and its Corollary 7.9 in both cases ρ is the only signature of R. ii) Further let A be a connected weakly semi-local π-ring, and σ be a signature of A. Then we call a covering $\varphi : A \to R$ a real closure of A with respect to σ, or a real closure of (A,σ), if R is real closed and the unique signature ρ of R extends σ. In the same way we use the notion of a strict real closure $\psi : A \to T$ of A with respect to σ in the case that A has trivial involution.

If $\varphi : A \to R$ is a real closure of A with respect to σ, then by Th. 7.4 the induced map $\varphi_* : W(A) \to W(R)$ may be identified with σ.

In the case that 2 is a unit we can simplify Corollary 7.9.

Proposition 7.11. Let T be a strictly real closed weakly semi-local ring, and assume that 2 is a unit in T. Then $W(T) \cong \mathbb{Z}$.

Proof. $W(T)$ is generated by the elements $[(a)]$ with a in T^*. Since a can be written in the form $1+4b$ with b in T, we see from Lemma 7.5 that $(a) \cong (1)$ if $\sigma(a) = 1$ and then $(a) \cong (-1)$ if $\sigma(a) = -1$. Thus

$$W(T) = \mathbb{Z}\,(1) \cong \mathbb{Z}.$$

q.e.d.

The assumption that 2 is a unit is essential in Prop. 7.11, as shows the following

Example 7.12. Let A be the localization of the ring $\mathbb{Z}$ with respect to the prime ideal $2\mathbb{Z}$, and let σ be the restriction of the signature of $\mathbb{Q}$ to the subring A, which by Cor. 4.11 is the unique signature of A. Let T be a strict real closure of A with respect to σ. Finally let n be a square free natural number with $n \equiv 3 \bmod 4$. Then n is not a square in T. Indeed, otherwise T would contain the ring $B := A[\sqrt{n}]$. Since both rings are integrally closed we would obtain from the Galois theory of fields, applied to the quotient fields of T and B, that B coincides with the fixed ring of T with respect to the group H of all automorphisms of T over B. Thus B would be a covering of A, which is not true. A fortiori $\sqrt{n}$ is not a square in T, and thus the element $z := [(1,-n)]$ of W(T) is not zero. But z has value zero under the unique signature of T. Thus W(T) is not isomorphic to $\mathbb{Z}$.

The following proposition improves the previous Cor. 7.7.

Proposition 7.13. Let T be a connected weakly semi-local ring with trivial involution, which is strictly real closed. Let $\mathfrak{p}$ denote the prime ideal of T associated with the unique signature τ of T (cf. Th. 4.8 and Appendix B).

i) For every maximal ideal $\mathfrak{m}$ of T with $\mathfrak{m} \neq \mathfrak{p}$ the field $T/\mathfrak{m}$ is separably closed.

ii) If $\mathfrak{p}$ is a maximal ideal, then $T/\mathfrak{p}$ is strictly real closed (i.e. a real closed field in classical terminology).

N.B. The ideal $\mathfrak{p}$ may be maximal or may be not maximal.

Proof. Assume $\mathfrak{m}$ is a maximal ideal and the field $T/\mathfrak{m}$ is real. Then T has a signature which can be extended to $T/\mathfrak{m}$. This signature must be the only signature τ, and thus $\mathfrak{m}$ is contained in $\mathfrak{p}$, which implies

$\mathfrak{m} = \mathfrak{p}$. Now Prop. 7.13 follows from Cor. 7.7.

q.e.d.

Corollary 7.14. Let R be a connected weakly semi-local π-ring which is real closed. Let $\mathfrak{P}$ denote the prime ideal of R associated with the unique signature ρ of R.

i) For every maximal ideal $\mathfrak{M}$ of R the field $R/\mathfrak{M}$ is separably closed.

ii) The ideal $\mathfrak{P}$ is stable under the involution of R, and the induced involution on the field $R(\mathfrak{P})$ is not trivial.

iii) If $\mathfrak{M}$ is a maximal ideal of R and $\mathfrak{M} \neq \mathfrak{P}$, then $\mathfrak{M}$ is not stable under the involution of R.

Proof. The first assertion follows from Lemma 7.6 and the fact that $|R|$ is simply connected in the category of rings without involution, which has been proved in § 5. Clearly $\mathfrak{P}$ is stable under J_R, since J_R is an automorphism of the pair (R,ρ). Let w denote the Artin-Schreier generator of R over R_o occuring in (7.3). We have $w + \bar{w} = 1$. Suppose the image w' of w in $R(\mathfrak{P})$ would be fixed under the involution of $R(\mathfrak{P})$. Then $w' = \frac{1}{2}$, and

$$h = w' - w'^2 = \frac{1}{4}$$

in $R(\mathfrak{P})$. But 1-4h is not zero in $R(\mathfrak{P})$. Thus w' is moved by the involution of $R(\mathfrak{P})$, and this involution is certainly not the identity. Now let $\mathfrak{M}$ be a maximal ideal of R different from $\mathfrak{P}$, and let $\mathfrak{m}$ denote the intersection $\mathfrak{M} \cap R_o$. By § 4 the ideal $\mathfrak{p} := \mathfrak{P} \cap R_o$ is the prime ideal associated with the unique signature $\rho_o = \rho|R_o$ of the strictly real closed ring R_o, and $\mathfrak{P}$ is the only prime ideal of R lying over $\mathfrak{p}$. Thus certainly $\mathfrak{m} \neq \mathfrak{p}$, and by Prop. 7.13 the field $R_o/\mathfrak{m}$ is separably

closed. Therefore the quadratic etale extension $R/\mathfrak{m}R$ of $R_o/\mathfrak{m}$ is not connected. This means $\mathfrak{m} \neq J_R(\mathfrak{m})$.

q.e.d.

We close this section with an application of our result, that a strict real closure of a connected semi-local ring with trivial involution has only one signature (Cor.7.9).

Proposition 7.15. Let K be an algebraic number field, not necessarily of finite degree over $\mathbb{Q}$, and let S be a finite set of non archimedian spots of K. Let K_{nr} denote the maximal subfield of the algebraic closure $\overline{K}$ which is unramified with respect to all spots in S. Further let γ_1 and γ_2 be two elements of order 2 in the Galois group $G(\overline{K}|K)$. Assume that the restrictions $\gamma_1|K_{nr}$ and $\gamma_2|K_{nr}$ are conjugate elements in $G(K_{nr}|K)$. Then γ_1 and γ_2 are conjugate in $G(\overline{K}|K)$.

Proof. There exists some α in $G(\overline{K}|K)$ such that γ_1 and $\alpha\gamma_2\alpha^{-1}$ coincide on K_{nr}. Replacing γ_2 by $\alpha\gamma_2\alpha^{-1}$ we assume that γ_1 and γ_2 have the same restriction to K_{nr}.

Let R_1, R_2 denote the subfields of fixed elements of γ_1, γ_2 in $\overline{K}$. Due to our assumption the intersections $R_1 \cap K_{nr}$ and $R_2 \cap K_{nr}$ are equal. The fields R_1 and R_2, equipped with the trivial involution, are strictly real closed [AS_2]. We denote by ρ_i the unique signature of R_i. By the uniqueness theorem for strict real closures the conjugacy of γ_1 and γ_2 is equivalent to the assertion that the restrictions $\rho_1|K$ and $\rho_2|K$ are equal. Let A denote the semi-local subring of K consisting of all elements which are integral with respect to all spots in S. It suffices to prove that the restrictions $\sigma_1 := \rho_1|A$ and $\sigma_2 := \rho_2|A$ are equal, since every signature of A can be extended in only one way

to a signature of K [KRW_2, Prop. 2.14].

The integral closure $\overline{A}$ of A in K_{nr} is a strict universal covering of A. Let B denote the integral closure of A in the field $R_1 \cap K_{nr} = R_2 \cap K_{nr}$ equipped with the trivial involution, and let τ_i denote the restriction $\rho_i | B$. Then (B,τ_i) is a covering of (A,σ_i), and (B,τ_i) is strictly real closed since the only non trivial covering $\overline{A}$ of B is non real. Since B has only one signature (Cor. 7.9), we have $\tau_1 = \tau_2$, hence $\sigma_1 = \sigma_2$.

q.e.d.

§ 8 The multiplicities $n(\tau,A)$ in the semi-local case.

Let (A,σ) be a connected weakly semi-local pair and let (B,τ) be a covering of (A,σ), which then again is weakly semi-local. We shall study the automorphisms of (B,τ) over (A,σ), and thereafter we shall compute the multiplicity $n(\tau,A)$ introduced in § 3 in the case $[B:A] < \infty$.

For any weakly semi-local ring C and signature ρ of C we denote by $\mathfrak{p}(\rho)$ the prime ideal associated with ρ, cf. Theorem 4.8, and by $\overline{\rho}$ the signature induced on the quotient field $C(\mathfrak{p}(\rho))$ of $C/\mathfrak{p}(\rho)$. We further denote by $Q(\rho)$ the set of all finite sums $N(x_1)a_1 + \ldots + N(x_r)a_r$ with x_i in C, a_i in C_0^*, $\rho(a_i) = 1$, and $x_1C + \ldots + x_rC = C$. As explained in Appendix B this set $Q(\rho)$ coincides with the set $Q(\rho|C_0)$ introduced already in § 4.

We return to our covering (B,τ) of (A,σ). We denote by σ_0 and τ_0 the restrictions $\sigma|A_0$ and $\tau|B_0$ respectively, and we use the following abbreviations: $\mathfrak{p} := \mathfrak{p}(\sigma)$, $\mathfrak{q} := \mathfrak{p}(\tau)$, $\mathfrak{p}_0 := \mathfrak{p}(\sigma_0)$, $\mathfrak{q}_0 := \mathfrak{p}(\tau_0)$. By Th. 4.8 we have $\mathfrak{p}_0 = \mathfrak{p} \cap A_0$ and $\mathfrak{q}_0 = \mathfrak{q} \cap B_0$.

Before coming to the main subject of this section we prove

Proposition 8.1. $\mathfrak{q} \cap A = \mathfrak{p}$, and $\mathfrak{q}_0 \cap A_0 = \mathfrak{p}_0$. Further $Q(\tau) \cap A_0 = Q(\sigma)$.

Proof. Denoting the intersection $\mathfrak{q} \cap A$ by $\mathfrak{p}'$ we have a natural commutative diagram

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow & & \downarrow \\ A(\mathfrak{p}') & \longrightarrow & B(\mathfrak{q}). \end{array}$$

The signature σ of A can be extended to the signature $\overline{\tau}$ of $B(q)$, and thus σ can also be extended to a signature of $A(\mathfrak{p}')$. This implies $\mathfrak{p}' \subset \mathfrak{p}$.

Let now $\alpha : (A,\sigma) \to (R,\rho)$ be a morphism into a real closed pair (R,ρ) whose kernel is the prime ideal $\mathfrak{p}$. We obtain such a morphism for example by composing the natural map from (A,σ) to $(A(\mathfrak{p}),\overline{\sigma})$ with a real closure of $(A(\mathfrak{p}),\overline{\sigma})$. By Th. 3.9 α can be extended to a morphism β from (B,τ) to (R,ρ). Let $\mathfrak{r}$ denote the kernel of β. Then we have a commutative diagram

$$\begin{array}{ccc} A & \hookrightarrow & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\gamma} \\ R & \xleftarrow{\ \overline{\beta}\ } & B(\mathfrak{r}) \end{array}$$

with γ the canonical map from B to $B(\mathfrak{r})$ and $\overline{\beta} \circ \gamma = \beta$. The signature τ can be extended to R by ρ, and thus τ can also be extended to $B(\mathfrak{r})$. This implies $\mathfrak{r} \subset \mathfrak{q}$ and then $\mathfrak{p} = \mathfrak{r} \cap A \subset \mathfrak{p}'$. Thus we have proved $\mathfrak{p} = \mathfrak{p}'$, i.e. $\mathfrak{p} = \mathfrak{q} \cap A$. We also have

$$\mathfrak{p}_o = \mathfrak{p} \cap A_o = \mathfrak{q} \cap A_o = \mathfrak{q}_o \cap A_o .$$

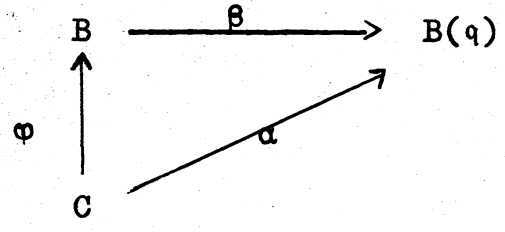
It follows from the definition of $Q(\sigma)$ and $Q(\tau)$, that $Q(\sigma)$ is contained in $Q(\tau) \cap A_o$. Let now z be an element of $Q(\tau) \cap A_o$. Then z is neither an element of $-Q(\sigma)$ nor of $\mathfrak{p}$, since $-Q(\sigma)$ is contained in $-Q(\tau)$ and $\mathfrak{p}$ is contained in $\mathfrak{q}$. Thus z must lie in $Q(\sigma)$. This proves $Q(\sigma) = Q(\tau) \cap A_o$.

q.e.d.

Proposition 8.2. The group G of automorphisms of (B,τ) over (A,σ) contains at most 2 elements. If the involution of $B(\mathfrak{q})$ is trivial or if the involution of $A(\mathfrak{p})$ is non trivial, then $G = 1$. On the other hand if $G \neq 1$, then the element $\neq$ id of G induces the (nontrivial) involution of $B(\mathfrak{q})$.

Proof. For every automorphism g of (B,τ) over (A,σ) we denote by g' the induced automorphism of $(B(\mathfrak{q}),\overline{\tau})$ over $(A(\mathfrak{p}),\overline{\sigma})$. Now $\overline{\tau}$ corresponds to an ordering of $B(\mathfrak{q})_0$, and g' yields an automorphism of $B(\mathfrak{q})_0$ preserving this ordering. Furthermore g' is the identity on the subfield $A(\mathfrak{p})_0$, and $B(\mathfrak{q})_0$ is algebraic over $A(\mathfrak{p})_0$. Thus g' must be the identity on $B(\mathfrak{q})_0$. Indeed, g' cannot permute the finitely many conjugates of an element x of $B(\mathfrak{q})_0$ over $A(\mathfrak{p})_0$, since g' preserves the ordering relations between them, and thus $g'(x) = x$. Denoting by j the involution $J_{B(\mathfrak{q})}$ we obtain ~~that~~ $g' = id$ or $g' = j$.

Let C denote the subring B^G of B. By § 1 we know that B is a galois covering of C. We consider the commutative diagram



with φ the inclusion map, β the canonical map from B to $B(\mathfrak{q})$, and α the restriction of β to C. For every g in G we have $\beta \circ g = g' \circ \beta$. Hence by Cor.1.16 any two elements g_1, g_2 of G with $g_1' = g_2'$ must coincide themselves. Thus G has at most 2 elements, and if G contains an element $g \neq id$, then

$$g' = j \neq id.$$

Certainly such an element g does not exist if j = id or if j is not the identity on $A(\mathfrak{p})$.

q.e.d.

Examples 8.3. If B has trivial involution then (B,τ) has no automorphism over (A,σ) except the identity. The same holds true if A has a non degenerate involution. A proof of the first statement, completely different from our proof of Prop. 8.2, is already contained in [KRW_2,§ 5]. If A has trivial involution but B has non trivial involution, then J_B is an automorphism of (B,τ) over (A,σ), cf. Lemma 3.11. By Prop. 8.2 this is the only automorphism except the identity. In particular a strict real closure T of a weakly semi-local ring A with trivial involution has no automorphism except the identity, and a real closure R has only the automorphisms id and J_R over A. {Recall from § 7 that both R and T have only one signature.}

We now come to the definition of the numbers $n(\tau,A)$ for infinite coverings. Let (A,σ) be an arbitrary connected pair and let $\alpha : (A,\sigma) \to (S,\gamma)$ be a morphism into a real closed pair (S,γ). For every finite covering (B,τ) of (A,σ) we denoted in § 3 by $n(\tau,A)$ the number of morphisms from (B,τ) to (S,γ) extending α. As we have seen in § 3 this number $n(\tau,A)$ is ≥ 1 and does not depend on the choice of α. Furthermore if C/A is a subcovering of B/A then clearly

$$n(\tau,A) = n(\tau,C)\, n(\tau|C,A). \tag{8.4}$$

If now (B,τ) is an infinite covering of (A,σ) then we define $n(\tau,A)$ as the supernatural number [cf.S, Chap.I,§ 1]

$$n(\tau,A) = \sup_{B'} n(\tau|B',A)$$

with B' running through all finite subcoverings of B/A. {$n(\tau,A)$ is a formal product $\prod p^{\alpha_p}$ with p running through all prime numbers and $0 \leqslant \alpha_p \leqslant \infty$ }. It is then easily seen that (8.4) remains true for arbitrary coverings. Again $n(\tau,A)$ may be interpreted as the number of morphisms from (B,τ) to (S,γ) extending the morphism α above. In general $n(\tau,A)$ may well be infinite, cf. the end of § 11, but if A is weakly semi-local this does not occur. Indeed, let (R,ρ) denote a real closure of (B,τ). Then $n(\tau,A)$ divides $n(\rho,A)$ and $n(\rho,A)$ is the number of automorphisms of (R,ρ) over (A,σ). Thus if A is weakly semi-local we know from Prop. 8.2 that $n(\tau,A)$ is 1 or 2. More precisely the following holds true:

Theorem 8.5. Let (B,τ) be a covering of a weakly semi-local connected pair (A,σ) and let $\mathfrak{p},\mathfrak{q}$ denote the prime ideals of A and B associated with σ and τ respectively. If $A(\mathfrak{p})$ has trivial involution but $B(\mathfrak{q})$ has non trivial involution, then $n(\tau,A) = 2$. In the other cases $n(\tau,A) = 1$.

Before proving this we restate Th. 8.4 in the special case $(B,\tau) = (R,\rho)$ in other terms. Recall from Cor. 7.14 that the involution of the field $R(\mathfrak{r})$ with $\mathfrak{r}$ the prime ideal associated with ρ is non trivial.

Corollary 8.6. Let R be a real closure of (A,σ). If $A(\mathfrak{p})$ has trivial involution then R has precisely two automorphisms over A. Otherwise the identity is the only automorphism of R over A.

We now prove Theorem 8.5. As above let (R,ρ) denote a real closure of (B,τ). If $A(\mathfrak{p})$ has non trivial involution, then we know

already from Prop. 8.2 that R has no automorphism over A except the identity and thus

$$n(\tau,A) = n(\rho,A) = 1.$$

We assume since now that $A(\mathfrak{p})$ has trivial involution. Consider the morphism

$$\lambda : (A,\sigma) \to (A(\mathfrak{p}),\overline{\sigma}) \to (B(\mathfrak{q}),\overline{\tau}) \xrightarrow{\kappa} (S,\gamma)$$

with the first two arrows the canonical maps occuring already in the proof of Prop. 8.2, and the morphism κ being a real closure of $(B(\mathfrak{q}),\overline{\tau})$. Clearly λ has the extension

$$\mu : (B,\tau) \to (B(\mathfrak{q}),\overline{\tau}) \xrightarrow{\kappa} (S,\gamma)$$

to (B,τ), with the first arrow again the canonical map. Assume now that $B(\mathfrak{q})$ has non trivial involution. Then also $J_S \circ \mu$ is an extension of λ which is different from μ. Thus $n(\tau,A) = 2$ in this case. Applying this to (R,ρ) instead of (B,τ) we have already proved Corollary 8.6 completely. To finish the proof of Th. 8.5 it remains to consider the case that $B(\mathfrak{q})$ has trivial involution. We have

$$n(\rho,A) = n(\rho,B)n(\tau,A)$$

and we know already

$$n(\rho,A) = n(\rho,B) = 2.$$

Thus $n(\tau,A) = 1$, and Th. 8.5 is completely proved.

Remark 8.7. If (A,σ) is a weakly semi-local pair but not necessarily connected, and (B,τ) is a finite étale extension of (A,σ), then the reader may check that Prop. 8.1 and its proof remain valid. Further-

more Theorem 8.5 can be extended verbatim to the present situation. Indeed, one easily retreats to the case that A and B are semi-local. Then one uses the fact, that A and B are finite cartesian products of connected π-rings, and that τ is induced by a unique signature of one of the factors of B, cf. [KRW_2,§ 2].

§ 9 Applications to the theory of Witt rings.

Our results on signatures and real closures obtained up to now imply some consequences for the structure of Witt rings. Of course these applications have a modest range, since signatures are insensitive to the torsion part and the nilradical of a Witt ring.

Let A be a real ring with involution, and let X denote the set of all signatures of A. This set can be identified with the set of all minimal prime ideals of W(A) and then also with the set $\mathrm{Spec}(\mathbb{Q} \otimes W(A))$ of all prime ideals of $\mathbb{Q} \otimes_{\mathbb{Z}} W(A)$, associating with a signature σ of A the kernel of the corresponding homomorphism from $\mathbb{Q} \otimes W(A)$ to $\mathbb{Q}$, cf. Th. 2.3. Since $\mathbb{Q} \otimes W(A)$ has Krull dimension zero, $\mathrm{Spec}(\mathbb{Q} \otimes W(A))$ is with respect to the Zariski topology a Boolean space, i.e. a totally disconnected compact Hausdorff space [B_1,§ 4 Exercise 16, p.173]. Thus by the above identification also X is a Boolean space. Without referring to prime ideals this topology of X can be described as the coarsest topology such that all functions

$$\tilde{z} : X \to \mathbb{Z}, \quad \sigma \mapsto \sigma(z) \tag{9.0}$$

with z running through W(A) are continuous, as is immediately checked. Of course $\mathbb{Z}$ here bears the discrete topology. Clearly the sets $\{\sigma \in X \mid \sigma(z) = a\}$ with fixed z in W(A) and a in $\mathbb{Z}$ are clopen (= closed and open) in X and form a basis of X. For a more thorough description of this topology in the case that A is semi-local cf.[KRW_2,§ 3].

Let $\overline{W}(A)$ denote the reduced Witt ring of A, i.e. the quotient of W(A) by its nilradical $\mathfrak{N}$. The ring $\overline{W}(A)$ is torsion free and thus will be regarded as a subring of $\mathbb{Q} \otimes_{\mathbb{Z}} \overline{W}(A)$. Indeed, if A is semi-local then $\mathfrak{N}$ coincides with the torsion part of W(A), as has been shown in

[KRW_1], and thus by Dress' theorem 2.4 the torsion part of $W(A)$ will be contained in $\mathfrak{N}$ in the general case.

The ring $\mathbb{Q} \otimes \overline{W}(A)$ is von Neumann regular [B_1, Exc.17, p.64; Exc.16, p.173]. Every signature σ of A induces maps from $\overline{W}(A)$ to $\mathbb{Z}$ and from $\mathbb{Q} \otimes \overline{W}(A)$ to $\mathbb{Q}$, which we again denote by σ. Due to the correspondence of the signatures with the prime ideals of $\mathbb{Q} \otimes \overline{W}(A)$ we have a natural ring isomorphism

$$\alpha_A : \mathbb{Q} \otimes \overline{W}(A) \xrightarrow{\sim} C(X,\mathbb{Q}) \tag{9.1}$$

from $\mathbb{Q} \otimes \overline{W}(A)$ onto the ring $C(X,\mathbb{Q})$ of all continuous $\mathbb{Q}$-valued functions on X, assigning to each element z of $\mathbb{Q} \otimes \overline{W}(A)$ the function $\tilde{z} : \sigma \mapsto \sigma(z)$, cf.[A-K,Th.2.3]. {Of course $\mathbb{Q}$ bears the discrete topology.}

By this "Gelfand isomorphism" α_A the subring $\overline{W}(A)$ of $\mathbb{Q} \otimes \overline{W}(A)$ is mapped onto a subring of $C(X,\mathbb{Z})$. Let $\tilde{W}(A)$ denote the integral closure of $\overline{W}(A)$ in $\mathbb{Q} \otimes \overline{W}(A)$. The ring $C(X,\mathbb{Z})$ is integrally closed and integral over $\mathbb{Z}$, since $C(X,\mathbb{Z})$ is generated as a module over $\mathbb{Z}$ by the characteristic functions χ_U of the clopen subsets U of X. {$\chi_U = 1$ on U and $= 0$ on $X \setminus U$}. A fortiori $C(X,\mathbb{Z})$ is integral over the ring $\alpha_A(\overline{W}(A))$, and thus α_A maps $\tilde{W}(A)$ isomorphically onto $C(X,\mathbb{Z})$. By the way we learn that $\overline{W}(A)$ is integral over $\mathbb{Z}$ and thus $W(A)$ is integral over $\mathbb{Z}$. (This remains true if A is non real.)

The Gelfand isomorphism α_A depends on A in a functorial way. Indeed, let $\varphi : A \to B$ be a homomorphism from A into another real ring B with involution. φ induces a ring homomorphism φ_* from $W(A)$ to $W(B)$ and thus also a homomorphism from $\mathbb{Q} \otimes \overline{W}(A)$ to $\mathbb{Q} \otimes \overline{W}(B)$ which we again denote by φ_*. On the other hand we have a continuous map p from the Boolean space Y of signatures of B to X, assigning to a signature

τ of Y its restriction $\tau|A = \tau \circ \varphi_*$. The diagram

$$\begin{array}{ccc} Q \otimes W(A) & \xrightarrow[\alpha_A]{\sim} & C(X,Q) \\ \downarrow{\scriptstyle \varphi_*} & & \downarrow{\scriptstyle p^*} \\ Q \otimes W(B) & \xrightarrow[\alpha_B]{\sim} & C(Y,Q) \end{array} \tag{9.2}$$

with p^* denoting the map $f \mapsto f \circ p$ clearly commutes.

The continuous map p just defined is closed since X is compact and Y is Hausdorff. As a first application of the trace formula developed in § 3 we obtain

Proposition 9.3. If φ is finite etale, then p is also open.

Proof. Let U be a clopen subset of Y and let χ_U denote its characteristic function. Then we can find some element z in W(B) and some natural number $m \geq 1$ such that the function $\tilde{z}$ (cf.9.0) coincides with $m\chi_U$, since α_B is an isomorphism from $Q \otimes W(B)$ to $C(Y,Q)$. Using the trace formula

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

we see that the function $(\mathrm{Tr}^*_{B/A}(z))^{\sim}$ on X has the support p(U). Thus p(U) is clopen in X.

q.e.d.

Since now $\varphi : A \to B$ always denotes a finite etale homomorphism. We study the function $\tau \mapsto n(\tau,A)$ on Y associated with φ.

Proposition 9.4. The function $\tau \mapsto n(\tau,A)$ is lower semi-continuous, i.e. for every natural number $m \geqslant 1$ the set of all τ in Y with $n(\tau,A) \leqslant m$ is open.

Proof. Let τ_o be a point in Y. We want to show $n(\tau,A) \leqslant n(\tau_o,A)$ for all τ in some neighbourhood of τ_o. Let $\sigma_o = p(\tau_o)$ and let $p^{-1}(\sigma_o) = \{\tau_o,\ldots,\tau_r\}$ be the fibre of p through τ_o $\{r \geqslant 0\}$. There exists some x in W(B) with $\tau_o(x) \neq 0$ and $\tau_i(x) = 0$ for $1 \leqslant i \leqslant r$. Let z denote the element x^2. We have $\tau(z) \geqslant 0$ for every τ in Y and furthermore

$$\tau_o(z) > 0,\ \tau_i(z) = 0 \text{ for } 1 \leqslant i \leqslant r.$$

Let further w denote the element $Tr^*_{B/A}(z)$ of W(A). We introduce the clopen sets

$$U := \{\tau \in Y \mid \tau(z) = \tau_o(z)\},$$

$$V := \{\sigma \in X \mid \sigma(w) = \sigma_o(w)\},$$

$$W := U \cap p^{-1}(V).$$

W is a clopen neighbourhood of τ_o, and the trace formula yields for τ in W and $\sigma = p(\tau)$, that

$$\sigma(w) \geqslant n(\tau,A)\tau(z) = n(\tau,A)\tau_o(z).$$

On the other hand, again by the trace formula

$$\sigma(w) = \sigma_o(w) = n(\tau_o,A)\tau_o(z).$$

Since $\tau_o(z) \neq 0$ this implies $n(\tau,A) \leqslant n(\tau_o A)$ for all τ in W.

q.e.d.

Lemma 9.5. i) The function $\tau \mapsto n(\tau,A)$ on Y is locally constant if and only if the function

$$f : \sigma \mapsto \text{Card } p^{-1}(\sigma)$$

on X, assigning to each σ in X the number of points in its fibre, is locally constant. ii) Assume that f is locally constant and let r denote the maximum of f on X. Then the ring extension $\varphi_* : \tilde{W}(A) \to \tilde{W}(B)$ is finite etale. More precisely we can find r idempotents $e_1,\ldots,e_r$ in $\tilde{W}(A)$ such that as an algebra over $\tilde{W}(A)$

$$\tilde{W}(B) \cong \Lambda_1 \times \ldots \times \Lambda_r$$

with $\Lambda_i := \tilde{W}(A)e_i$.

Proof. i) Let σ_o a point of X. If $f(\sigma_o) = 0$ then $f(\sigma) = 0$ for all σ in some neighbourhood of σ_o, since $p(Y)$ is a closed subset of X. Assume since now $f(\sigma_o) = s \geq 1$ and let $\tau_1,\ldots,\tau_s$ denote the points of $p^{-1}(\sigma_o)$. We choose mutually disjoint clopen neighbourhoods U_i' of the τ_i such that $n(\tau,A) \leq n(\tau_i,A)$ for every τ in U_i'. This is possible by the preceding Prop. 9.4. Then we choose a clopen neighbourhood

$$V \subset p(U_1') \cap \ldots \cap p(U_s')$$

of σ_o such that the function $(\mathrm{Tr}^*_{B/A}(1))^{\sim}$ is constant on V and furthermore

$$p^{-1}(V) \subset U_1' \sqcup \ldots \sqcup U_s' ,$$

which again is possible since the image of $Y \setminus (U_1' \cup \ldots \cup U_s')$ in X is closed and does not contain σ_o. Let U_i denote the clopen neighbourhood $p^{-1}(V) \cap U_i'$ of τ_i. Then p maps each U_i onto V and

$$p^{-1}(V) = U_1 \sqcup \ldots \sqcup U_s.$$

For every σ in V we have

$$\sigma(\mathrm{Tr}^*(1)) = \sigma_o(\mathrm{Tr}^*(1))$$

and thus by the trace formula

$$\sum_{p(\tau)=\sigma} n(\tau,A) = \sum_{i=1}^{s} n(\tau_i,A)$$

On the other hand $n(\tau,A) \leqslant n(\tau_i A)$ for τ in U_i. Thus we see that in each U_i there lies precisely one point over σ, i.e. $f(\sigma) = s$, if and only if $n(\tau,A) = n(\tau_i A)$ for every i in $[1,s]$ and τ in $p^{-1}(\sigma) \cap U_i$. Now the first assertion of the lemma is evident.

ii) Assume that f is locally constant. Then we may assume that on the clopen neighbourhood V of σ_o constructed above in addition f is constant, and we see that every U_i, $1 \leqslant i \leqslant s$, is mapped bijectively onto V.

We now cover p(Y) by finitely many clopen sets $V_1,\ldots,V_n$ such that

$$p^{-1}(V_j) = U_{j1} \sqcup U_{j2} \sqcup \ldots \sqcup U_{js_j}$$

for every j, with clopen sets U_{ji} which are mapped bijectively onto V_j. Replacing V_j by $V_j \setminus (V_1 \cup \ldots \cup V_{j-1})$ for $j > 1$ we assume in addition that the V_j are mutually disjoint. Clearly f has the constant value s_j on V_j, hence

$$r = \mathrm{Max}(s_1,\ldots,s_n).$$

For every i in $[1,r]$ we denote by Z_i the union of all sets U_{ji} with $1 \leqslant j \leqslant n$ and $s_j \geqslant i$. Then

$$Y = Z_1 \sqcup \ldots \sqcup Z_r,$$

and each Z_i is a clopen subset of Y which under p is mapped bijectively and thus homeomorphically onto its image $X_i := p(Z_i)$. We have

$$C(Y,\mathbb{Z}) \cong \prod_{i=1}^{r} C(Z_i,\mathbb{Z})$$

and

$$C(Z_i,\mathbb{Z}) \cong C(X_i,\mathbb{Z}) \cong C(X,\mathbb{Z})\chi_{X_i}.$$

Here all isomorphisms are compatible with the action of $C(X,\mathbb{Z})$ on the corresponding rings. Now the second assertion of our lemma follows from the diagram (9.2), since $C(X,\mathbb{Z})$ and $C(Y,\mathbb{Z})$ correspond to the rings $\tilde{W}(A)$ and $\tilde{W}(B)$ under the Gelfand isomorphisms α_A and α_B.

q.e.d.

We now state the first main result of this section, essentially announced already in [K_1]. By $2^{-\infty}$ we denote localization with respect to the powers of 2.

Theorem 9.6. Let A,B be weakly semi-local rings with involution and let $\varphi : A \to B$ be a finite etale homomorphism. Assume that the involution J_A is either trivial or non degenerate. Put $s := 1$ if J_A is non degenerate or if $J_B = id$ and $s := 2$ in the remaining case $J_A = id$ and J_B non degenerate. Let further t denote the natural number $s^{-1}\,\mathrm{Max}[B_m:A_m]$ with m running through all maximal ideals of A. Then the homomorphism

$$\varphi_* : 2^{-\infty}W(A) \to 2^{-\infty}W(B)$$

is finite etale. More precisely there exist $r \leq t$ idempotents $e_1,\dots,e_r$ of $2^{-\infty}W(A)$ such that as algebra over $2^{-\infty}W(A)$

$$2^{-\infty}W(B) \cong \Lambda_1 \times \dots \times \Lambda_r$$

with $\Lambda_i := 2^{-\infty}W(A)e_i$.

Proof. There is nothing to prove if A or B is non real in view of Th. 2.3. Assume now that A and B are both real. By Remark 8.7 we have $n(\tau,A) = s$ for every signature τ of B. Thus we can apply the preceding Lemma 9.5, and we clearly have $r \leq t$ for the natural number r occuring there. The nilradical of W(A) is the torsion part of W(A) and this torsion part is 2-primary [KRW_1]. Thus we can identify $2^{-\infty}W(A)$ with the subring $2^{-\infty}\overline{W}(A)$ of $\mathbb{Q} \otimes \overline{W}(A)$. Furthermore $\widetilde{W}(A)/\overline{W}(A)$ is again a 2-torsion group [KRW_1, Prop. 3.17]. Thus $2^{-\infty}W(A) = 2^{-\infty}\widetilde{W}(A)$. In the same way we can identify $2^{-\infty}W(B)$ with $2^{-\infty}\widetilde{W}(B)$, and we obtain the theorem from the preceding Lemma 9.5.

q.e.d.

Assume now that $\varphi : A \to B$ is a finite etale homomorphism and $\alpha : A \to A'$ is an arbitrary homomorphism between rings with involution. As in previous sections we denote for any ring C with involution by Sign(C) the set of signatures of C which is a Boolean space. We have a commutative diagram

$$\begin{array}{ccc} B & \xrightarrow{1 \otimes \alpha} & B \otimes_A A' \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi \otimes 1} \\ A & \xrightarrow{\alpha} & A' \end{array}$$

from which we obtain a continuous map

$$\Phi : \mathrm{Sign}(B \otimes_A A') \to \mathrm{Sign}(B) \times_{\mathrm{Sign}(A)} \mathrm{Sign}(A')$$

between Boolean spaces, mapping a signature τ' of $B \otimes_A A'$ to the pair

$(\tau'|B, \tau'|A')$ consisting of the restrictions $\tau'|B = \tau' \circ (1 \otimes \alpha)_*$ and $\tau'|A' = \tau' \circ (\varphi \otimes 1)_*$. By Th. 3.15 this map Φ is surjective and thus identifying.

Theorem 9.8. We assume A to be weakly semi-local.

i) Every fibre of Φ contains at most 2 elements.
ii) Assume in addition that either B has trivial involution or A has a non degenerate involution. Alternatively assume that A' has trivial involution and $B \otimes_A A'$ has a non degenerate involution. Then Φ is bijective and thus a homeomorphism.
iii) In addition to one of the assumptions made in ii) we also assume that A' is weakly semi-local. Then the kernel and the cokernel of the map

$$W(B) \otimes_{W(A)} W(A') \longrightarrow W(B \otimes_A A')$$

induced by the diagram (9.7) above are 2-torsion groups.

Proof. We assume that A,B,A' are all real, since otherwise the assertions are trivial. Let (τ, σ') be an element of the fibre product $\mathrm{Sign}\, B \times_{\mathrm{Sign}\, A} \mathrm{Sign}\, A'$ and let σ denote the common restriction $\tau|A = \sigma'|A$ of the signatures τ of B and σ' of A'. We have to count the signatures τ' of $B \otimes A'$ with $\tau'|B = \tau$ and $\tau'|A' = \sigma'$. For this reason we choose some morphism λ from (A', σ') into a real closed pair (S, γ). Then the morphisms μ from (B, τ) to (S, γ) with $\mu \circ \varphi = \lambda \circ \alpha$ correspond bijectively to the morphisms μ' from $(B \otimes A', \tau')$ to (S, γ) with $\mu' \circ (\varphi \otimes 1) = \lambda$ and τ' running through the fibre $\Phi^{-1}(\tau, \sigma')$. Thus we obtain by our description of the multiplicities $n(\tau, A)$ in Th. 3.4

$$n(\tau, A) = \sum_{\tau'} n(\tau', A)$$

with τ' running through $\Phi^{-1}(\tau,\sigma')$. From this relation the assertions i) and ii) follow immediately: We have $n(\tau,A) \leq 2$ by Remark 8.7, since we assume A to be weakly semi-local. Thus $\Phi^{-1}(\tau,\sigma')$ contains at most 2 points. If J_A is non degenerate or J_B is trivial then by the same theorem $n(\tau,A) = 1$ and thus $\Phi^{-1}(\tau,\sigma')$ contains only one point. The same holds true if A' has trivial involution and $B \otimes_A A'$ has non degenerate involution, since then a priori $n(\tau',A') \geq 2$ for every signature τ' of $B \otimes A'$ (Prop. 3.12 and 8.4). The third assertion now follows from an interpretation of $2^{-\infty}W(B \otimes A')$ as the ring of continuous functions on $\mathrm{Sign}(B \otimes A')$ with values in $2^{-\infty}\mathbb{Z}$ and of $2^{-\infty}W(B) \otimes_{W(A)} W(A')$ as the ring of continuous functions on $\mathrm{Sign}(B) \times_{\mathrm{Sign}(A)} \mathrm{Sign}(A')$ with values in $2^{-\infty}\mathbb{Z}$.

q.e.d.

We now switch over to another topic, which over fields of Char $\neq 2$ has been discovered by A.Dress, cf. [D_2] and [D_3,Prop.2]. If B is a finite etale extension of A, then we obtain from B the non singular bilinear space $\mathrm{Tr}^*_{B/A}(1)$, consisting of the projective A-module B equipped with the form $\mathrm{Tr}_{B/A}(x\bar{y})$. For shortness this space will be denoted by $\{B/A\}$ or simply by $\{B\}$. We call these spaces the natural spaces over A, and we denote by N(A) the subring of W(A) generated by the natural spaces. From the evident rules

(9.9a) $$\{B_1\} \perp \{B_2\} \cong \{B_1 \times B_2\}$$

and

(9.9b) $$\{B_1\} \otimes \{B_2\} \cong \{B_1 \otimes_A B_2\}$$

we see that every element of N(A) is a difference $\{B\} - \{C\}$ of two

spaces. (If no confusion is to be feared we denote the image of $\{B\}$ in $W(A)$ again by $\{B\}$.)

We want to obtain some information about the ring $N(A)$ of natural spaces. For this reason we introduce the Burnside ring $\Omega(A)$ of A, which by definition is the Grothendieck ring of finite etale algebras B over A. Let $[B]$ denote the stable isomorphy class of such an algebra B $\{[B] = [B']$ if $B \times D \cong B' \times D$ for some finite etale algebra $D.\}$ The elements of $\Omega(A)$ are differences $[B_1] - [B_2]$ of these stable isomorphy classes, and the addition and multiplication in $\Omega(A)$ is given by

$$[B_1] + [B_2] = [B_1 \times B_2],$$

$$[B_1] \cdot [B_2] = [B_1 \otimes_A B_2].$$

Clearly $\Omega(A)$ has the unit element $[A]$.

Let C be a completely arbitrary commutative algebra (with 1) over A. Then C yields a ring homomorphism

$$\gamma_C : \Omega(A) \to \mathbb{Z}$$

mapping the class $[B]$ of a finite etale A-algebra B to the number of A-homomorphisms from B to C. We have the following theorem of Burnside - Dress [D_2]:

Theorem 9.10. Assume A is connected.

i) If B_1 and B_2 are two finite algebras over A with $\gamma_C[B_1] = \gamma_C[B_2]$ for every covering C of A, then $B_1 \cong B_2$.

ii) The isomorphy classes of coverings C of A correspond uniquely to the homomorphisms λ from $\Omega(A)$ to $\mathbb{Z}$ by the relation $\lambda = \gamma_C$.

iii) The minimal prime ideals of $\Omega(A)$ are the kernels of these homomorphisms λ.

Of course in this theorem our ring A with involution can be replaced by a connected ω-ring for an arbitrary finite group ω.

Corollary 9.11. Let A be an arbitrary ring with involution (or ω-ring).
i) Every two stable isomorphic finite etale algebras over A are actually isomorphic.
ii) The minimal prime ideals of $\Omega(A)$ are the kernels of the homomorphisms from $\Omega(A)$ to $\mathbb{Z}$.
iii) $\Omega(A)$ has no nilpotent elements $\neq 0$.

Proof. All this is clear from Th. 9.10 if A is connected and then also for a finite product $A = A_1 \times \ldots \times A_r$ of connected rings A_i with involution, i.e. for a ring A with involution, which has only finitely many idempotents. The assertions then can be deduced for arbitrary A by observing that A is an inductive limit of noetherian subrings stable under the involution.

According to the formulas (9.9) we have a well defined homomorphism

$$Sc : \Omega(A) \to W(A)$$

mapping an isomorphy class $[B]$ to the element $\{B\}$ of W(A). Following $[D_2]$ we call Sc the Scharlau map over A. Clearly Sc has the image N(A).

Lemma 9.12. Let $\sigma : W(A) \to \mathbb{Z}$ be a signature of A, and let $\alpha : (A,\sigma) \to (R,\rho)$ be a morphism into a real closed pair (R,ρ). Then the function $\sigma \circ Sc$ on $\Omega(A)$ coincides with γ_R. {Of course R is regarded as algebra over A by α.}

Proof. For an arbitrary finite etale algebra B over A the trace formula yields

$$\sigma \circ \mathrm{Sc}[B] = \sigma\{B\} = \sum_{\tau|\sigma} n(\tau, A)$$

with τ running through the signatures of B extending σ. According to the description of the $n(\tau,A)$ in Th. 3.4 this sum is the number $\gamma_R[B]$ of homomorphisms from B to R over A.

q.e.d.

For any ring Λ we denote the localization $\mathbb{Q} \otimes_{\mathbb{Z}} \Lambda$ briefly by $\mathbb{Q} \otimes \Lambda$. The ring $\mathbb{Q} \otimes \Omega(A)$ is von Neumann regular (cf. the discussion of $\mathbb{Q} \otimes \overline{W}(A)$ above). Thus also the homomorphic image $\mathbb{Q} \otimes N(A)$ of $\mathbb{Q} \otimes \Omega(A)$ is von Neumann regular. In particular $\mathbb{Q} \otimes N(A)$ has no nilpotent elements, hence we may regard $\mathbb{Q} \otimes N(A)$ as a subring of $\mathbb{Q} \otimes \overline{W}(A)$.

Theorem 9.13. Assume A is connected. The following statements are equivalent:

(i) $\mathbb{Q} \otimes N(A) = \mathbb{Q} \otimes \overline{W}(A)$.

(ii) If σ_1 and σ_2 are signatures of A with $\sigma_1 \circ \mathrm{Sc} = \sigma_2 \circ \mathrm{Sc}$, then $\sigma_1 = \sigma_2$.

(iii) If R is a covering of A which is real closed with respect to some signature then the group of automorphisms of R over A acts transitively on the set Sign R of signatures of R.

Proof. (i) $\Leftrightarrow$ (ii): Let Y denote the set of ring homomorphisms from $\mathbb{Q} \otimes N(A)$ to $\mathbb{Q}$. The kernels of these homomorphisms are the prime ideals of $\mathbb{Q} \otimes N(A)$. This follows either from Th. 9.10.iii or from the fact that $\mathbb{Q} \otimes \overline{W}(A)$ is integral over $\mathbb{Q} \otimes N(A)$. Thus we may identify Y with

the Boolean space Spec($\mathbb{Q} \otimes N(A)$). Let further X denote the Boolean space of signatures of A which we interpret as the homomorphisms from $\mathbb{Q} \otimes \overline{W}(A)$ to $\mathbb{Q}$. The map $f : X \to Y$ assigning to a signature σ its restriction to $\mathbb{Q} \otimes N(A)$ is continuous. We have a commutative diagram

$$(*) \qquad \begin{array}{ccc} \mathbb{Q} \otimes N(A) & \xrightarrow{\sim} & C(Y,\mathbb{Q}) \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle f^*} \\ \mathbb{Q} \otimes \overline{W}(A) & \xrightarrow{\sim} & C(X,\mathbb{Q}) \end{array}$$

with Gelfand isomorphisms as horizontal maps, i the inclusion map, and f^* the map between the function rings induced by f, cf. the discussion leading to the diagram (9.2) above. In particular f^* is injective, hence f is surjective. Statement (ii) means that f is injective and thus bijective. This in turn is equivalent to the statement that f^* is bijective. Now the equivalence (i) $\Leftrightarrow$ (ii) is clear from the diagram (*).

(ii) $\Rightarrow$ (iii): Let $\alpha : A \to R$ be the map which makes R a covering of A. Let ρ_1, ρ_2 be two signatures of R, and let $\sigma_1 = \rho_1 \circ \alpha_*$, $\sigma_2 = \rho_2 \circ \alpha_*$ denote their restrictions to A. We know from Th. 5.1, that $[\tilde{A}:R] = 2$. Thus R has no real covering of degree >1 and the pairs (R,ρ_1), (R,ρ_2) both are real closed. By Lemma 9.12 we have

$$\sigma_1 \circ Sc = \sigma_2 \circ Sc = \gamma_R.$$

Under the assumption (ii) this implies $\sigma_1 = \sigma_2$, and then, by the uniqueness theorem 3.5 for real closures, that (R,ρ_1) is isomorphic to (R,ρ_2) over A.

(iii) $\Rightarrow$ (ii): Assume that σ_1 and σ_2 are signatures of A with $\sigma_1 \circ Sc = \sigma_2 \circ Sc$, and let (R_i,ρ_i) denote a real closure of (A,σ_i).

Es folgt Seite 38a.

Then by Lemma 9.12

$$\gamma_{R_1} = \sigma_1 \circ Sc = \sigma_2 \circ Sc = \gamma_{R_2}.$$

Thus by Burnside's theorem 9.10 the coverings R_1 and R_2 over A are isomorphic. We choose an isomorphism β from R_1 to R_2 over A and we denote by ρ_2' the signature $\rho_2 \circ \beta_*$ on R_1. By our assumption there exists an automorphism λ of R_1 over A with $\rho_2' = \rho_1 \circ \lambda_*$, and then $\beta \circ \lambda$ is an isomorphism from (R_1,ρ_1) to (R_2,ρ_2) over A. Clearly the restrictions σ_1 and σ_2 of ρ_1,ρ_2 to A must coincide.

q.e.d.

Of course we obtain analogous results by working only in the category of rings with trivial involution. Let A be a ring with trivial involution, and let $\Omega_o(A)$ denote the subring of $\Omega(A)$ generated by the finite etale algebras with trivial involution. Further let

$$Sc_o : \Omega_o(A) \longrightarrow W(A)$$

denote the restriction of the Scharlau map to $\Omega_o(A)$ and let $N_o(A)$ denote the image of Sc_o. Finally we denote for an arbitrary A-algebra C with trivial involution by γ_C^o the restriction of the $\mathbb{Z}$-valued function γ_C to $\Omega_o(A)$. Then we have

Lemma 9.12a. Let σ be a signature of A and let $\alpha : (A,\sigma) \to (T,\tau)$ be a morphism into a strictly real closed pair (T,τ). Then $\sigma \circ Sc_o$ coincides with γ_T^o.

In proving the analogous result to Th. 9.13 we have to be slightly careful, since for a strictly real closed pair (T,τ) we do not know in general, whether T is also strictly real closed with

respect to all other signatures of T. {We know this if there exists a prime number which is not a unit in T, cf. proof of Prop. 5.5}. We obtain

Theorem 9.13a. Assume A is connected and has trivial involution. Then the following are equivalent:

(i) $\mathbb{Q} \otimes N_0(A) = \mathbb{Q} \otimes \overline{W}(A)$.

(ii) If σ_1 and σ_2 are signatures of A with $\sigma_1 \circ Sc_0 = \sigma_2 \circ Sc_0$, then $\sigma_1 = \sigma_2$.

(iii) If T is a covering of A with trivial involution which is strictly real closed with respect to some signature, then the automorphism group of T over A acts transitively on the set of all signatures τ of T such that (T,τ) is strictly real closed.

These theorems 9.13 and 9.13a imply the following concrete results.

Examples 9.14. a) Assume A is a weakly semi-local ring with involution. Then $W(A)/N(A)$ is a torsion group. Indeed, this holds true if A is connected by the preceding theorem 9.13 since then according to § 7 every real closure of A has only one signature. By the usual standard argument we then see that $W(A)/N(A)$ is a torsion group also if A is not connected (cf. proof of Cor. 9.11). Question: For which prime numbers p is the p-component of $W(A)/N(A)$ not zero? If A has trivial involution then we obtain by the same method the stronger result that $W(A)/N_0(A)$ is a torsion group. Moreover $W(A) = N_0(A)$ if in addition 2 is a unit in A. This has been observed by Dress in the case that A is a field [D_2], and follows in our more general situation by the same argument as in [D_2]. This argument also shows $W(A) = N(A)$ if A has arbitrary involution and 2 is a unit.

b) Let A be the ring $R[X]$ of regular algebraic functions on a

smooth affine curve X over the field R of real numbers equipped with an involution. Let R be a covering of A which is real closed with respect to some signature. We shall prove in § 11 that then $W(R) = \mathbb{Z}$, and hence R has only one signature. Thus by the preceding theorem 9.13 $\mathbb{Q} \otimes N(A) = \mathbb{Q} \otimes \overline{W}(A)$. Furthermore every nilpotent element of W(A) is a torsion element, since A is a Dedekind domain [KRW_3]. Thus $\mathbb{Q} \otimes \overline{W}(A) = \mathbb{Q} \otimes W(A)$, and $W(A)/N(A)$ is again a torsion group. If A has trivial involution then even $W(A)/N_o(A)$ is a torsion group.

§ 10 The main theorem for semi-local rings.

In this section we mostly regard rings which are not equipped with an involution. Thus we slightly change our notation for the present section: A ring B equipped with an involution J will be denoted by (B,J) instead of a single letter.

Let A be a connected weakly semi-local ring, and let G denote the Galois group of the universal covering $\overline{A}$ over A. For every signature σ of (A,id) we choose a strict real closure T of A with respect to σ (cf. Def. 7.10). We know from § 5 that $[\overline{A}:T] = 2$. Thus we have a unique element γ of order 2 in G whose fixed ring in $\overline{A}$ is T. If we choose another strict real closure of σ, then by the uniqueness theorem for strict real closures (Cor. 3.10) γ changes to $\alpha\gamma\alpha^{-1}$ for some α in G. Associating with σ the conjugacy class of γ we thus obtain a well defined map Φ from the set Sign(A) of signatures of (A,id) to the set of conjugacy classes of elements of order 2 in G. This map Φ is injective, since the fixed ring T of γ has only one signature from which we obtain σ back by restriction to A. We shall prove

Theorem 10.1. Φ is bijective. Thus the signatures of A correspond uniquely to the conjugacy classes of elements of order 2 in G.

A generalization of this theorem to rings with involution (Th. 10.12) will be the "main theorem" to which the title of this section alludes.

Notice that we did not exclude the case that A is non real. In this case Th. 10.1 tells us the still remarkable fact, that G contains no elements of order 2.

Theorem 10.1 will follow immediately from

Proposition 10.2. Let A be a connected weakly semi-local ring. Assume $[\overline{A}:A] = 2$. Then A is real with respect to the trivial involution.

Indeed, to prove Th. 10.1 it only remains to show that Φ is surjective. Thus let γ be a given element of order 2 in G, and let T denote the fixed ring of γ. By Prop. 10.2 the ring T has at least one signature τ. Certainly (T,τ) is strictly real closed, since the only non trivial covering $\overline{A}$ of T (with trivial involution) is non real. Thus the conjugacy class of γ is the image of $\tau|A$ under Φ.

Most space of the present section will be occupied by the proof of Prop. 10.2. We first will be concerned with the construction of cyclic coverings of degree 4. Then we shall prove Prop.10.2 by observing that the ring A there does not possess any cyclic coverings of degree 4.

For our study of cyclic coverings of degree 4 we do not need the hypothesis that A is weakly semi-local. Thus A is now an arbitrary commutative ring with 1. We introduce on A compositions $\circ$ and $*$ (cf. [Sm]), defined by

$$a \circ b = a + b + 4ab = a(1+4b) + b,$$

$$a * b = a + b - 2b = a(1-2b) + b.$$

Notice that

$$1 - 2(a * b) = (1-2a)(1-2b), \tag{10.3}$$

$$1 + 4(a \circ b) = (1+4a)(1+4b).$$

Both compositions $\circ$ and $*$ are associative and commutative and have the neutral element 0. Moreover we have the map

$$\wp : A \to A,\ x \mapsto x^2-x$$

which satisfies the identity

$$\wp(a * b) = \wp(a) \circ \wp(b).$$

We denote by $\Gamma(A)$ the set of elements x in A with $1-2x$ a unit and by $\Delta(A)$ the set of elements y in A with $1+4y$ a unit. $\Gamma(A)$ is a group with respect to the composition $*$, the inverse of an element x of $\Gamma(A)$ being the element $-x(1-2x)^{-1}$, and $\Delta(A)$ is a group with respect to $\circ$, the inverse of y in $\Delta(A)$ being the element $-y(1+4y)^{-1}$. The restriction of $\wp$ to $\Gamma(A)$ is a group homomorphism from $\Gamma(A)$ to $\Delta(A)$. We call two elements y and z of A equivalent, and write $y \sim z$, if there exists some x in $\Gamma(A)$ with

$$y_2 = y_1 \circ (x^2-x).$$

The relevance of $\Delta(A)$ and of this equivalence relation stems from the fact, used already in § 5 and § 6, that the elements of $\Delta(A)$ yield quadratic etale extensions (cf. Def. 7.1) of A. For every a in A we have an extension $B = A + A\omega$ of A with free basis 1, ω and the relation $\omega^2-\omega = a$. We denote this "Artin-Schreier generator" ω by $\wp^{-1}a$. The algebra $B = A[\wp^{-1}a]$ is etale over A if and only if a lies in $\Delta(A)$ (cf.[KRW_2,pp 241 ff] and [Sm]). The other Artin-Schreier generators of this algebra $B = A + A\omega$ are precisely the elements

$$\omega' = (1-2\lambda)\omega + \lambda$$

with λ in $\Gamma(A)$, as is immediately checked. This implies that for a

and b in A the algebras $A[\wp^{-1}a]$ and $A[\wp^{-1}b]$ are isomorphic over A if and only if $a \sim b$.

As stated in § 7 all quadratic etale extensions of A have Artin-Schreier generators if A is weakly semi-local. Thus in this case the set of isomorphy classes of quadratic etale extensions of A can be identified with the cokernel of $\wp: \Gamma(A) \to \Delta(A)$. More general results can be found in [Sm].

In general, if A is connected then for a in $\Delta(A)$ the ring $B = A[\wp^{-1}a]$ is not connected if and only if

$$B \cong A \times A \cong A[\wp^{-1}0].$$

Thus every a in $\Delta(A)$ which is not equivalent zero yields a covering of degree 2 over A (cf. proof of Lemma 7.5).

We fix some a in A and consider the extension

$$B = A[\wp^{-1}a] = A + A\omega, \quad \omega^2-\omega = a$$

of A. We denote the canonical involution of B over A, i.e. the automorphism mapping ω to $1-\omega$, by $z \mapsto \overline{z}$. This involution does not depend on the choice of the Artin-Schreier generator and has the fixed ring A. We further denote the norm map $z \mapsto z\overline{z}$ from B to A by N. We now define maps μ and ν from B to A by

$$\mu(x) = x * \overline{x}\ , \quad \nu(x) = x \circ \overline{x}.$$

We then have

$$N(1-2x) = 1 - 2\mu(x), \quad N(1+4y) = 1 + 4\nu(y). \tag{10.4}$$

Thus μ and ν yield homomorphisms from $\Gamma(B)$ to $\Gamma(A)$ and $\Delta(B)$ to $\Delta(A)$ respectively. Clearly

$$\rho(\mu(x)) = \nu(\rho(x))$$

for every x in B. Thus we have a commutative diagram

(10.5)

$$\begin{array}{ccc} \Gamma(B) & \xrightarrow{\mu} & \Gamma(A) \\ \rho \downarrow & & \downarrow \rho \\ \Delta(B) & \xrightarrow{\nu} & \Delta(A) \end{array}$$

of group homomorphisms.

We shall need the following complicated identities.

Lemma 10.6. Assume $a = b^2$ for some b in A with $1 + 2b + 4b^2$ a unit. Then

$$\rho(-b-2b^2) \circ \nu(-b\omega(1+2b+4b^2)^{-1}) = b^2.$$

Furthermore

$$1 + 4\rho(-b-2b^2) = (1+2b+4b^2)^2$$

is a unit. Thus

$$\nu(-b\omega(1+2b+4b^2)^{-1}) \sim b^2.$$

Proof. The second identity is immediately verified. To prove the first one it suffices to consider the case $A = \mathbb{Z}[t,(1+2t+4t^2)^{-1}]$, $b = t$, with t an indeterminate. Thus we may assume that A is an integral domain and $2 \neq 0$ in A. Then by (10.3) and (10.4) it suffices to prove

$$1 + 4b^2 = (1+2b+4b^2)^2 \, N(1-4b\omega(1+2b+4b^2)^{-1})$$

or more simply

$$1 + 4b^2 = N(1+4b^2+2b(1-2\omega)).$$

This is easily done.

q.e.d.

Now we are prepared to prove

Theorem 10.7. Let A be a connected commutative ring and let b an element of A such that $1 + 4b^2$ and $1 + 2b + 4b^2$ are units of A, but b^2 is not equivalent to zero. Then the commutative algebra $E := A[\omega, \zeta]$ over A with the defining relations

$$\omega^2 - \omega = b^2, \quad \zeta^2 - \zeta = -b\omega(1+2b+4b^2)^{-1}$$

is a galois covering of A whose Galois group $G(E|A)$ is cyclic of order 4.

Remark 10.8. Assume that also b itself is a unit. Then E is generated over A by ζ alone. Assume in addition that 2 is a unit in A. Then introducing the elements

$$\alpha := (2b)^{-1}(1-2\omega), \quad \beta := 1 - 2\zeta$$

we have the defining relations

$$\alpha^2 = 1 + (2b)^{-2}$$

and

$$\beta^2 = (1+2b+4b^2)^{-1}4b^2(\alpha^2+\alpha).$$

Thus E can be written in the form

$$E = A\left[\sqrt{d(1+c^2+\sqrt{1+c^2})}\right]$$

with units c and d of A. This is the typical form of cyclic coverings of degree 4 in the case that A is a field of Char $\neq 2$, cf. [A1, Chap. IX] and [DD].

Proof of Th. 10.7. The subring $B := A[\omega]$ of E has the defining relation $\omega^2 - \omega = b^2$, hence B is a quadratic covering of A since

b^2 lies in $\Delta(A)$ and is not equivalent zero. We introduce the element

$$\gamma := -b\omega(1+2b+4b^2)^{-1}$$

of B. By Lemma 10.6 the element $\nu(\gamma)$ is equivalent to b^2 and thus lies in $\Delta(A)$. By (10.4) this implies that γ itself lies in $\Delta(B)$. But γ is not equivalent to zero over B, since $\nu(\gamma)$ is not equivalent to zero over A {recall (10.5)}. Therefore $E = B[\zeta]$ is a covering of B of degree 2 due to the defining relation

$$\zeta^2 - \zeta = \gamma,$$

and E is a covering of A of degree 4.

The three elements $\zeta, \omega, -b-2b^2$ all lie in the group $\Gamma(E)$, since their images under the map $\rho : E \to E$ lie in $\Delta(E)$ (cf. Lemma 10.6 for $-b-2b^2$). Thus there exists a unique element η in $\Gamma(E)$ with

$$\zeta * \eta * (-b-2b^2) = \omega.$$

Applying ρ to this equation we obtain

$$\gamma \circ \rho(\eta) \circ \rho(-b-2b^2) = b^2.$$

On the other hand, denoting by δ the conjugate of γ in B,

$$\delta := -b(1-\omega)(1+2b+4b^2)^{-1},$$

we have by Lemma 10.6

$$\gamma \circ \delta \circ \rho(-b-2b^2) = b^2.$$

Thus we see $\delta = \rho(\eta)$, or more explicitly

$$\eta^2 - \eta = \delta.$$

Using our defining relations of E over A we now can write down explicitly 4 different homomorphisms from E to $\overline{A}$ over A, namely except the identity

$$\omega \mapsto \omega, \quad \zeta \mapsto 1 - \zeta;$$
$$\omega \mapsto 1 - \omega, \quad \zeta \mapsto \eta;$$
$$\omega \mapsto 1 - \omega, \quad \zeta \mapsto 1 - \eta.$$

Since $[E:A] = 4$ this must be all homomorphisms from E to $\overline{A}$ over A (cf. Prop. 1.6). They all map E into E. Thus E is galois over A. Recall that every homomorphism from E to E over A is an automorphism of E (cf. Lemma 1.1). Thus we have listed above the full Galois group of E over A. This group apparently is cyclic of order 4.

q.e.d.

Assume now that A is connected and weakly semi-local and that $[\overline{A}:A] = 2$. We want to prove the assertion of Prop. 10.2 that A is real. For every maximal ideal $\mathfrak{M}$ of $\overline{A}$ the field $\overline{A}/\mathfrak{M}$ is separably closed by Lemma 7.6. Now $\overline{A}/\mathfrak{M}$ has degree ≤ 2 over the subfield $A/\mathfrak{M} \cap A$. If this degree is precisely 2, then $A/\mathfrak{M} \cap A$ is real, since Prop. 10.2 is known to hold true over fields $[AS_2]$, and thus A certainly is also real. Thus we assume since now that for every maximal ideal $\mathfrak{m}$ of A the field $A/\mathfrak{m}$ is separably closed. (This assumption is not substantial for the arguments below.) We denote by $\mathfrak{S}$ the set of all maximal ideals $\mathfrak{m}$ of A such that $A/\mathfrak{m}$ has <u>not</u> characteristic 2. This set may of course be empty. We need a technical lemma.

<u>Lemma 10.9.</u> Let $a_1, \ldots, a_n$ be a finite sequence of elements of A. Then there exists a semi-local subring B of A and a family $\{M(\mathfrak{m}) \mid \mathfrak{m} \in \mathfrak{S}\}$ of subsets $M(\mathfrak{m})$ of the fields $A/\mathfrak{m}$ with the following four properties:

(i) Every set $M(\mathfrak{m})$ has cardinality $|M(\mathfrak{m})| \leq 2^{3n-1}$.

(ii) If x is an element of A such that $x \bmod \mathfrak{m}$ does not lie in $M(\mathfrak{m})$ for every $\mathfrak{m}$ in $\mathfrak{S}$, then the element $(a_1^2 + \ldots + a_n^2)x^2$ lies in $\Delta(A)$ and is equivalent zero.

(iii) A is integral over B. Every set $M(\mathfrak{m})$ is contained in the subfield $B/\mathfrak{m} \cap B$ of $A/\mathfrak{m}$.

(iv) If two maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2$ in $\mathfrak{S}$ have the same intersection $\mathfrak{m}_1 \cap B = \mathfrak{m}_2 \cap B$ with B, then $M(\mathfrak{m}_1) = M(\mathfrak{m}_2)$ {both sets regarded as subsets of $B/\mathfrak{m}_1 \cap B = B/\mathfrak{m}_2 \cap B$}.

Proof. We proceed by induction on n. n = 1: For every $\mathfrak{m}$ in $\mathfrak{S}$ we define $M(\mathfrak{m})$ as the set of all elements in $A/\mathfrak{m}$ which are zeros of at least one of the following two separable polynomials over $A/\mathfrak{m}$:

$$1 + 4\bar{a}_1^2 T^2, \quad 1 + 2\bar{a}_1 T + 4\bar{a}_1^2 T^2.$$

Here $\bar{a}_1$ denotes the image of a_1 in $A/\mathfrak{m}$. All these sets $M(\mathfrak{m})$ contain at most 4 elements. If x is an element of A such that $x \bmod \mathfrak{m}$ does not lie in $A/\mathfrak{m}$ for every $\mathfrak{m}$ in $\mathfrak{S}$, then clearly $1 + 4a_1^2x^2$ is a unit, i.e. $a_1^2x^2$ lies in $\Delta(A)$. Furthermore $1 + 2a_1x + 4a_1^2x^2$ is a unit. Since A has no cyclic coverings of degree 4 we now obtain from Th. 10.7 that $a_1^2x^2 \sim 0$. Thus the conditions (i),(ii) of our lemma are fulfilled. We choose a semi-local subring B' of A containing a_1 such that A is integral over B'. Then by the method used in the proof of Lemma 7.6 one easily constructs an overring B of B' in A such that for every $\mathfrak{m}$ in $\mathfrak{S}$ the zeros of the two separable polynomials listed above lie in the subfield $B/\mathfrak{m} \cap B$ of $A/\mathfrak{m}$. With this ring B the conditions (iii), (iv) are also fulfilled.

(n-1) ⇒ n: We choose a family $\{N(\mathfrak{m}) \mid \mathfrak{m} \in \mathfrak{S}\}$ of subsets $N(\mathfrak{m})$ of the fields $A/\mathfrak{m}$ and a semi-local subring C of A, for which the properties

(i) - (iv) hold true with respect to the sequence $a_1,\dots,a_{n-1}$. For every m in $\mathfrak{S}$ we denote by $U(m)$ the set of all z in A/m which are zeros of one of the polynomials

$$(*) \qquad 1 + 4\bar{a}_n^2T^2, \quad 1 + 2\bar{a}_nT + 4\bar{a}_n^2T^2$$

over A/m. Let x be an element of A such $x \bmod m$ does not lie in $U(m)$ for every m in $\mathfrak{S}$. As we have seen above $a_n^2x^2$ lies in $\Delta(A)$ and is equivalent zero. Thus there exists an element b in A such that

$$a_n^2x^2 = b^2 - b$$

and $1-2b$ is a unit. Introducing the element

$$y := x(1-2b)^{-1}$$

we have

$$(a_1^2 + \dots + a_n^2)x^2 = [(a_1^2 + \dots + a_{n-1}^2)y^2] \circ (a_n^2x^2),$$

hence

$$(a_1^2 + \dots + a_n^2)x^2 \sim (a_1^2 + \dots + a_{n-1}^2)y^2.$$

Thus if $y \bmod m$ does not lie in $N(m)$ for every m in $\mathfrak{S}$, then

$$(a_1^2 + \dots + a_n^2)x^2 \sim 0.$$

Let us analyse the situation, that $y \bmod m$ lies in $N(m)$ for some m. We have an equation

$$\bar{x} = (1-2\bar{b})c$$

in A/m with some element c of $N(m)$. Squaring this equation we obtain

$$\bar{x}^2 = (1+4\bar{a}_n^2\bar{x}^2)c^2$$

and then

$$(1 - 4\bar{a}_n^2 c^2)\bar{x}^2 - c^2 = 0.$$

We now introduce the set $V(\mathfrak{m})$ of all z in $A/\mathfrak{m}$ which are zeros of one of the polynomials

$$(**) \qquad (1 - 4\bar{a}_n^2 c^2)T^2 - c^2$$

over $A/\mathfrak{m}$ with c running through $N(\mathfrak{m})$, and we define

$$M(\mathfrak{m}) := U(\mathfrak{m}) \cup V(\mathfrak{m}).$$

By the consideration above this family $\{M(\mathfrak{m}) \mid \mathfrak{m} \in \mathfrak{S}\}$ fulfills property (ii). Furthermore

$$|V(\mathfrak{m})| \leq 2|N(\mathfrak{m})| \leq 2 \cdot 2^{3n-4} = 2^{3n-3}$$

and

$$|M(\mathfrak{m})| \leq 2^{3n-3} + 4 < 2^{3n-1},$$

since $n \geq 2$. Now again by the method used in the proof of Lemma 7.6 it is possible to construct an overring B of C in A containing $a_1, \ldots, a_n$ such that for every $\mathfrak{m}$ in $\mathfrak{S}$ the separable polynomials listed above under (*) and (**) have all their zeros in the subfield $B/\mathfrak{m} \cap B$ of $A/\mathfrak{m}$. Then also the conditions (iii) and (iv) are fulfilled.

q.e.d.

Now we are able to prove Proposition 10.2. We suppose that our ring A with $[\bar{A}:A] = 2$ is non real with respect to the trivial involution, and we want to deduce from this supposition a contradiction. Since A is weakly semi-local, we have

$$\bar{A} = A[\wp^{-1}a]$$

with some a in $\Delta(A)$ which is not equivalent zero. The element -1 of A is a sum of squares in A, since A is assumed to be non real [K_3,Cor.2.7]. Thus also

$$1 + 4a = (1+2a)^2 - 4a^2$$

is a sum of squares,

$$1 + 4a = a_1^2 + \ldots + a_n^2$$

with a_i in A. From this equation we shall deduce the contradiction $a \sim 0$. We take some element b of $\Gamma(A)$ and we study the element

$$c := a \circ (b^2-b)$$

of $\Delta(A)$. We have

$$1 + 4c = (1+4a)(1-2b)^2.$$

Introducing the element

$$d := c(1-2b)^{-1}(1+4a)^{-1}$$

we obtain

$$c^2(1+4c)^{-1} = d^2(a_1^2 + \ldots + a_n^2).$$

Starting from the sequence $a_1,\ldots,a_n$ we now choose a family $\{M(m) \mid m \in \mathfrak{S}\}$ of subsets of those fields A/m, which have Char $\neq 2$, and a semi-local subring B of A as indicated in the preceding Lemma 10.9. Suppose we can choose the element b of A above in such a way, that for every m in $\mathfrak{S}$

1) the element $1 - 2\bar{b}$ of A/m is $\neq 0$,
2) the element $\bar{d}$ of A/m does not lie in M(m).

Then b lies in $\Gamma(A)$, $c^2(1+4c)^{-1}$ lies in $\Delta(A)$ and is equivalent zero,

and

$$a \sim c \sim [c^2(1+4c)^{-1}] \circ c = c^2 + c \sim 0,$$

which is the desired contradiction.

We want to see that such a choice of b is indeed possible. Assume that b fulfills the condition 1) but that d mod m lies in M(m) for some m. Then we obtain in A/m an equation

$$\overline{b}^2 - \overline{b}(1-2g) - g + \overline{f} = 0$$

with some g in M(m) and

$$f := a(1+4a)^{-1}.$$

Let S(m) denote the set of elements of A/m which are zeros of 1 - 2T or of one of the separable polynomials

$$T^2 - T(1-2g) - g + \overline{f}$$

with g running through M(m). Clearly both conditions 1) and 2) are fulfilled for b, if $\overline{b}$ does not lie in S(m) for every m in $\mathfrak{S}$. Now

$$|S(m)| \leq 1 + 2|M(m)| \leq 1 + 2^{3n}.$$

By the method used in the proof of Lemma 7.6 we can find some semi-local overring D of B in A such that for every m in $\mathfrak{S}$ the set S(m) is contained in the subfield D/m ∩ D of A/m, and moreover all these finitely many fields D/m ∩ D contain at least $2^{3n}+2$ elements. By our construction of the S(m) we have $S(m_1) = S(m_2)$ for maximal ideals m_1, m_2 in $\mathfrak{S}$ with $m_1 \cap D = m_2 \cap D$, both sets $S(m_i)$ regarded as subsets of $D/m_1 \cap D = D/m_2 \cap D$. By the "Chinese remainder theorem" we can find an element b of D such that b mod m ∩ D does not lie in the proper subset S(m) of D/m ∩ D for every m in $\mathfrak{S}$. This element b has

the desired properties 1),2) above. Prop. 10.2 and Theorem 10.1 are now proved.

As an immediate consequence of Th. 10.1 we obtain

Corollary 10.10. Let A be a connected weakly semi-local ring. Then the Galois group $G(\overline{A}|A)$ contains no element of order 4.

Proof. Suppose α is an element of order 4 in $G(\overline{A}|A)$. By Th. 10.1 the fixed ring B of α^2 is strictly real closed. But α induces a non trivial automorphism of B over A. This is impossible by the results of § 8 (cf. Ex. 8.3).

q.e.d.

Conjecture 10.11. If A is connected and weakly semi-local, then $G(\overline{A}|A)$ does not contain elements of finite order except involutions.

To prove this conjecture it suffices by Cor. 10.10 to show for every prime number $p \neq 2$ that $G(\overline{A}|A)$ contains no element of order p. This is certainly true if p is a unit in A or if $p = 0$ in A. Indeed, let B be any connected weakly semi-local ring. Assume that p is a unit in B and that B contains roots of unity of order p. Then the cyclic coverings of B of degree p are up to isomorphy the extensions $B[T]/(T^p-a)$ with units a in B which are not p-powers in B. If $p = 0$ in B then the cyclic coverings are the extensions $B[T]/(T^p-T-a)$ with a in B but not $a = b^p-b$ for some b in B. These facts can be proved along the same lines as in the field case, cf. e.g. [La,p.213 ff]. Now our assertion follows immediately by the arguments of J.B.Leicht in his simplification of Artin-Schreier's proof [L]. By the way, if only $p^n=0$ in A for some $n \geq 1$, then still $G(\overline{A}|A)$ contains no elements of order p, since the group $G(\overline{A}|A)$ does not alter if A is replaced by

its reduction modulo the nilradical [G_1, Exp.1, Th.8.3].

Thus our conjecture certainly holds true if A contains a field, and also if 2 lies in the Jacobson radical of A.

The following theorem is a condensation of most of our efforts for semi-local rings.

Main theorem 10.12. Assume A is connected and weakly semi-local. Let J be an arbitrary involution on A. For every signature σ of (A,J) we choose a real closure $(\overline{A},\alpha)$ of (A,J) with respect to σ. Then the conjugacy class $[\alpha]$ of α with respect to the group $G(\overline{A}|A)$ is uniquely determined by σ. The map $\sigma \mapsto [\alpha]$ is a bijection from the set of signatures of (A,J) to the set of conjugacy classes of non degenerate involutions α on $\overline{A}$ which extend J.

Notice that in the case J = id this theorem coincides with Th. 10.1.

Proof. We know from § 5 that indeed every real closure of (A,J) with respect to some signature σ is of the form $(\overline{A},\alpha)$ with an involution α, and from § 6 that α is non degenerate. Furthermore by § 3 the pair $(\overline{A},\alpha)$ is up to isomorphy uniquely determined by σ, which means that the conjugacy class of α is uniquely determined by σ. Furthermore σ is the restriction of the unique signature of $(\overline{A},\alpha)$ (cf.§ 7) to A, and thus different signatures yield different conjugacy classes of involutions. Finally let α be a non degenerate involution of $\overline{A}$ extending J. Then the fixed ring T of α is strictly real closed by Prop. 10.2, and thus bears a unique signature τ. By Prop. 7.2 τ can be extended to a signature ρ of $(\overline{A},\alpha)$. Clearly $(\overline{A},\alpha)$ is the real closure of the restriction σ of ρ to (A,J). Thus every conjugacy class of non degenerate involutions on $\overline{A}$ extending J originates from a signature of (A,J).

q.e.d.

Involutions on semi-local rings occur in abundance in algebraic geometry. Whenever J is an involution on a scheme $(X,\mathcal{O}_X)$ and x is a fixed point of J in X, then J induces an involution on $\mathcal{O}_x$. If x is a point moved under J then J induces an involution on the semi-local ring A of local sections of $\mathcal{O}_X$ defined in a neighbourhood of $\{x,J(x)\}$.

To the authors opinion Th. 10.12 might serve as a comfort to those readers who dislike the complications and dragging passages in this paper due to our study of rings with involution instead of rings without involution.

§ 11 Real curves.

Real affine curves provide an extremely beautiful illustration of our theory of real closures, and thus will be discussed here although everything done in this section is only an exercise on Witt's results about real function fields in [W] and [W_1].

In this section X always denotes a smooth irreducible affine curve over the field $\mathbb{R}$ of real numbers {curve = scheme of dimension 1}, and A denotes the ring $\mathbb{R}[X]$ of algebraic functions defined on X. We assume that $\mathbb{R}$ is the precise field of constants of X, i.e. that A does not contain $\sqrt{-1}$. By A' we denote the ring $A[\sqrt{-1}]$.

We equip A with the trivial involution and A' with the involution $\sqrt{-1} \mapsto -\sqrt{-1}$ over A, and we want to describe explicitly the Witt rings W(A) and W(A'). For this we shall first recall the results of Witt mentioned above.

Let F denote the field of fractions $\mathbb{R}(X)$ of A, i.e. the field of rational functions on X. Let Y denote the - up to isomorphy unique - smooth projective irreducible curve over $\mathbb{R}$ which contains X as an open subset. The local rings $\mathfrak{o}_\mathfrak{p}$ of the closed points $\mathfrak{p}$ of Y are precisely all discrete valuation rings of F containing $\mathbb{R}$ which have F as field of fractions.

Further notations:

$m_\mathfrak{p}$: = maximal ideal of $\mathfrak{o}_\mathfrak{p}$.

$t_\mathfrak{p}$: = an arbitrarily chosen generator of $m_\mathfrak{p}$.

$Y(\mathbb{R})$: = set of real points of Y, i.e. closed points $\mathfrak{p}$ with $\mathfrak{o}_\mathfrak{p}/m_\mathfrak{p} \cong \mathbb{R}$.

$X(\mathbb{R})$: = $X \cap Y(\mathbb{R})$ = set of real points of X.

S : = $Y(\mathbb{R}) \setminus X(\mathbb{R})$, a finite set.

$F' := F(\sqrt{-1})$, equipped with the involution $\sqrt{-1} \mapsto -\sqrt{-1}$ over F.

$Y' :=$ normalization of Y in F'.

$Q(F) :=$ group F^*/F^{*2} of square classes $(f) = fF^{*2}$ of F.

$Q^+(F) :=$ subgroup of all (f) in $Q(F)$ with f positive definite, i.e. $f(\mathfrak{p}) \geq 0$ for all $\mathfrak{p}$ in $Y(\mathbb{R})$ where f is defined.

$Q(F') :=$ group $F^*/N(F'^*)$ of norm classes $\langle f \rangle = fN(F'^*)$ of F'.

$Q(A) :=$ subgroup of all (f) in $Q(F)$ with f of even order at all closed points of X.

$Q^+(A) := Q(A) \cap Q^+(F)$.

$Q(A') :=$ subgroup of all $\langle f \rangle$ in $Q(F')$ with f of even order at all $\mathfrak{p}$ in $X(\mathbb{R})$.

We need a more geometric interpretation of the groups Q(F), Q(F'), Q(A), Q(A'). We regard Q(F) as a subgroup of the unit group of W(F), namely as the set of classes of bilinear spaces (f) of rank one over F. Similary we regard Q(F') as the set of classes of hermitian spaces of rank one in W(F'). It is known that $Q^+(F)$ is the set of all square classes (f) with f a sum of two squares, i.e. a norm of F'/F, cf. [W,Ge]. Thus

$$Q(F') = Q(F)/Q^+(F). \tag{11.1}$$

The Witt rings W(A) and W(A') inject into W(F) and W(F') respectively [KRW_3, Lemma 1.1], and we regard since now W(A) as a subring of W(F) and W(A') as a subring of W(F'). Then Q(A) coincides with the set of classes of bilinear spaces of rank one over A [K, 13.3.2], and similarly Q(A') coincides with the set of classes of hermitian spaces of rank one over A'. The canonical map from Q(F) to

$Q(F')$ induces a map from $Q(A)$ to $Q(A')$ with kernel $Q^+(A)$. We now show that this map is onto, i.e.

(11.2) $$Q(A') = Q(A)/Q^+(A).$$

Indeed, let $\langle f \rangle$ be a norm class in $Q(A')$. If S is not empty we write the divisor $\mathrm{div}(f)$ of f in Y in the form

$$\mathrm{div}(f) = \mathfrak{a} + N(\mathfrak{b})$$

with $\mathfrak{a}$ a divisor with support in S and $N(\mathfrak{b})$ the norm of a divisor $\mathfrak{b}$ of Y' of degree zero. Now the group $\mathrm{Pic}_0(Y')$ of divisor classes of degree zero over Y' is an abelian variety over $\mathbb{C}$ and thus certainly a 2-divisible group. Hence we can find some function g in F' and a divisor $\mathfrak{c}$ in Y' of degree zero such that

$$\mathfrak{b} = 2\mathfrak{c} + \mathrm{div}(g).$$

We obtain

$$\mathrm{div}(fN(g)^{-1}) = \mathfrak{a} + 2N(\mathfrak{c})$$

which implies that the square class $(fN(g)^{-1})$ lies in $Q(A)$. If S is empty we proceed similarly starting with a decomposition

$$\mathrm{div}(f) = n\mathfrak{p}_0 + N(\mathfrak{b})$$

with $\mathfrak{b}$ a divisor of Y' of degree zero and a multiple of a prime divisor $\mathfrak{p}_0$ not contained in X.

The structure of the group $Q(A')$ has been completely determined by Witt in [W], cf. also [Ge]. We introduce on $X(\mathbb{R})$ the "strong topology", i.e. the coarsest topolgy such that the f in A yield continuous real valued functions on $X(\mathbb{R})$. We have a decomposition

$$X(R) = Z_1 \sqcup Z_2 \sqcup \ldots \sqcup Z_r$$

into $r \geqslant 0$ connected components {$r = 0$ if $X(R)$ is empty}, and each Z_i is homeomorphic either to a circle or to an open interval of R. The group $Q(A')$ consists of the norm classes $\langle f \rangle$ of definite functions, i.e. those f in F^* which have on each Z_i a constant sign. In view of (11.2) Witt's theorem III in [W] can be stated in the following way:

Theorem 11.3. For every choice of signs $\varepsilon_i = \pm 1$ for $1 \leqslant i \leqslant r$ there exists a square class (f) in $Q(A)$ such that f has on each Z_i the sign ε_i. The group $Q(A')$ is isomorphic to $(\mathbb{Z}/2)^r$.

For every $\mathfrak{p}$ in $Y(R)$ we have an additive map

$$\partial_{\mathfrak{p}} : W(F) \longrightarrow W(R) \xrightarrow{\sim} \mathbb{Z}$$

defined on the set $Q(F)$ of generators of $W(F)$ in the following way, cf. [MH, p.85]: If $f = ut_{\mathfrak{p}}^i$ with u in $O_{\mathfrak{p}}^*$, i in $\mathbb{Z}$, then $\partial_{\mathfrak{p}}(f) = 0$ if i is odd, $\partial_{\mathfrak{p}}(f) = 1$ if i even and $u(\mathfrak{p}) > 0$, $\partial_{\mathfrak{p}}(f) = -1$ if i even and $u(\mathfrak{p}) < 0$.

The natural map from $W(F)$ to $W(F')$ is surjective, since it maps $Q(F)$ onto the set $Q(F')$ of generators of $W(F')$. The kernel of this map is the ideal generated by the elements $1 - (f)$ with (f) in $Q^+(F)$, cf. [KRW_2, Prop.2.5]. But the elements f occuring here are the sums of squares in F^*, and hence our ideal coincides with the nilradical of $W(F)$ [Pf, Satz 22]. Thus we may interpret $W(F')$ as the reduction of $W(F)$ by the nilradical,

$$W(F') = W(F)_{red}. \tag{11.4}$$

Since the nilradical of $W(F)$ consists of torsion elements [Pf], every map $\partial_{\mathfrak{p}}$ above factors through an additive map

$$\psi'_{\mathfrak{p}} : W(F') \longrightarrow \mathbb{Z} \qquad (\mathfrak{p} \in Y(R)).$$

We also have determinant maps from W(F) to Q(F) and from W(F') to Q(F'), cf. [Pf, p.121]. {We use the word "determinant" instead of "discriminant", since we consider hermitian forms instead of quadratic forms.} The determinant of some element z in W(F) or in W(F') will be denoted by d(z). If z lies in W(A) then d(z) lies in Q(A), and if z lies in W(A') then d(z) lies in Q(A'). Now we can state Witt's result on real function fields in [W_1]:

Theorem 11.5. Let z, w be elements of W(F) with same dimension index $\nu(z) = \nu(w)$, same determinant $d(z) = d(w)$, and $\psi_{\mathfrak{p}}(z) = \psi_{\mathfrak{p}}(w)$ for almost all $\mathfrak{p}$ in Y(R). Then $z = w$.

Notice that the condition $\nu(z) = \nu(w)$ is superfluous if $Y(R) \neq \emptyset$.

If $Y(R) = \emptyset$ then by this theorem, or by the description of $Q^+(F)$ above, $4W(F) = 0$ and F is non real. Furthermore then W(F') is the field $\mathbb{F}_2$ of two elements according to (11.4).

If $Y(R) \neq \emptyset$ then a norm class $\langle f \rangle$ is uniquely determined by the signs of the values $f(\mathfrak{p})$ at the points $\mathfrak{p}$ in Y(R) where f is defined, cf. (11.1). Thus for z in W(F') the values $\psi'_{\mathfrak{p}}(z)$ for almost all $\mathfrak{p}$ in Y(R) determine beside $\nu(z)$ also the determinant d(z), and we obtain from Th. 11.5 the following

Corollary 11.6. Assume $Y(R) \neq \emptyset$. Let z,w be elements of W(F') with $\psi'_{\mathfrak{p}}(z) = \psi'_{\mathfrak{p}}(w)$ for almost all $\mathfrak{p}$ in Y(R). Then $z = w$.

We now are prepared to describe W(A) and W(A') explicitly. We interpret the closed points $\mathfrak{p}$ in X as the maximal ideals of A. For every component Z_i of X(R) we have signatures

$$\sigma_i : W(A) \longrightarrow W(A/\mathfrak{p}) \xrightarrow{\sim} \mathbb{Z}$$

and

$$\sigma_i' : W(A') \longrightarrow W(A'/\mathfrak{p}A') \xrightarrow{\sim} \mathbb{Z}$$

with $\mathfrak{p}$ arbitrarily chosen in Z_i, cf. Example 4.9. {Notice that $A'/\mathfrak{p}A' \cong C$, equipped with the complex conjugation as involution.} We know from Prop. 3.12 that σ_i' is the unique extension of σ_i to A'. According to Th. 11.3 we choose for every component Z_i an element (f_i) of $Q(A)$ with $\sigma_i(f_i) = -1$ and $\sigma_j(f_i) = +1$ for $j \neq i$. Recall that we denoted by $I(A)$, $I(A')$ the ideals of elements with dimension index zero in $W(A)$ and $W(A')$.

Theorem 11.7. i) Every element z of $W(A)$ is uniquely determined by the values $\nu(z), d(z), \sigma_1(z), \ldots, \sigma_r(z)$. In case $r \geq 1$ the value $\nu(z)$ can be omitted.

ii) The torsion part $I(A)_t$ of $I(A)$ consists of the elements $1-(f)$ with f in $Q^+(A)$ and is the nilradical of $W(A)$.

iii) $I(A)$ has the direct decomposition

$$I(A) = \bigoplus_{i=1}^{r} \mathbb{Z}[1-(f_i)] \oplus I(A)_t.$$

The product of any two different elements $1-(f_i)$, $1-(f_j)$ lies in $I(A)_t$.

iv) The homomorphism

$$(\sigma_1, \ldots, \sigma_r) : W(A) \longrightarrow \mathbb{Z}^r$$

maps $W(A)$ onto the subring of $\mathbb{Z}^r$ consisting of all r-tuples $(n_1, \ldots, n_r)$ with all n_i even or all n_i odd.

v) $\sigma_1, \ldots, \sigma_r$ are the only signatures of A.

Proof. Clearly $I(A)_t$ is the nilradical of $W(A)$ since $I(F)_t$ is the

nilradical of W(F). Assertion i) follows immediately from Th. 11.5 and the fact that for z in W(A) and $\mathfrak{p}$ in Z_i we have $\sigma_i(z) = \psi_{\mathfrak{p}}(z)$. Let z be an element of $I(A)_t$. Then d(z) is contained in Q(A) and also in $Q^+(F)$, since the ideal $I(F)_t$ is generated by the elements 1-(f) with f in $Q^+(F)$. Thus d(z) lies in $Q^+(A)$, and we obtain from Th. 11.5 that the elements z and 1-d(z) are equal. This proves (ii). Let now be z an element of I(A). Every $\sigma_i(z)$ is an even number $2n_i$. Consider the element

$$w := z - \sum_{i=1}^{r} n_i[1-(f_i)].$$

By use of Th. 11.5 we see $2w = 0$, and thus w lies in $I(A)_t$. Conversely if

$$z = \sum_{i=1}^{r} n_i'[1-(f_i)] + w'$$

with n_i' in $\mathbb{Z}$ and w' in $I(A)_t$, then $\sigma_i(z) = 2n_i'$, hence $n_i = n_i'$ and $w = w'$. Again by use of Th. 11.5 we obtain

$$[1-(f_i)][1-(f_j)] = 2\delta_{ij}[1-(f_i)].$$

Thus statement (iii) is proved. From this description of I(A) the statement (iv) is evident, and by (iv) the σ_i yield an isomorphism from $\mathbb{Q} \otimes_{\mathbb{Z}} W(A)$ to the ring $\mathbb{Q}^r$. Thus $\sigma_1, \ldots, \sigma_r$ must be the only signatures of A.

q.e.d.

Remark 11.8. By this theorem W(A) is generated by Q(A). This fact had been overlooked in [K, § 14].

Theorem 11.9. The canonical map from W(A) to W(A') is surjective, and its kernel is the nilradical $I(A)_t$ of I(A). Thus

$$W(A') = W(A)_{red}.$$

Proof. Since $W(F') = W(F)_{red}$ (cf. 11.4) clearly $W(A')$ has no nilpotent elements $\neq 0$, and the kernel of our map is indeed $I(A)_t$. If $r = 0$ then $Y(R) = \emptyset$ and $W(F') = \mathbb{F}_2$, as stated above. This forces $W(A') = \mathbb{F}_2$, and our map is certainly surjective. Assume now $r > 0$. Starting from Cor. 11.6 we see as in the proof of Th. 11.7 that $I(A')$ is generated by the elements $1 - \langle f_i \rangle$ with $1 \leq i \leq r$. The image of $W(A)$ contains 1 and $I(A')$ and thus must be the whole ring $W(A')$.

q.e.d.

Now we are able to prove the main result of this section.

Theorem 11.10. Let (R,ρ) be a real closed pair with R an integrally closed domain containing the field $\mathbb{R}$ of real numbers. Assume that the field of fractions of R has transcendency degree 1 over $\mathbb{R}$. Then $R = R_o[\sqrt{-1}]$ and

$$W(R_o) \cong W(R) \cong \mathbb{Z}.$$

Proof. Let ρ_o denote the restriction of ρ to R_o. According to Cor.6.3 the pair (R_o,ρ_o) is strictly real closed and (R,ρ) is the real closure of (R_o,ρ_o). Moreover $R = R_o[\sqrt{-1}]$ by Cor. 5.3. Now R_o is a filtered union of Dedekind domains A_α which are finitely generated over $\mathbb{R}$ and thus are the function rings $\mathbb{R}[X_\alpha]$ of smooth irreducible affine curves X_α over $\mathbb{R}$, having $\mathbb{R}$ as precise field of constants. Let (S_α,ρ_α) denote a strict real closure of A_α with respect to $\rho|A_\alpha$. There exists a morphism from (S_α,ρ_α) to (R_o,ρ_o) over A_α, cf.§ 3. The kernel of this homomorphism from S_α to R_o has intersection zero with A_α and hence must be zero itself. Thus we may choose from the beginning S_α as an overring of A_α in R_o and ρ_α as the restriction $\rho|S_\alpha$. Since R_o is the filtered union of the S_α and R is the filtered union of the

rings $S'_\alpha := S_\alpha[\sqrt{-1}]$ it suffices to prove that

$$W(S_\alpha) \cong W(S'_\alpha) \cong \mathbb{Z} .$$

From Th. 11.9 we learn that $W(S'_\alpha)$ is isomorphic to the reduction of $W(S_\alpha)$ by its nilradical. Thus we only need to show $W(S_\alpha) \cong \mathbb{Z}$, and we fall back upon the following problem:

Let A be a function ring $R[X]$ as introduced at the beginning of our section, equipped with the trivial involution. Let σ be a signature of A and (T,τ) be a strict real closure of (A,σ). Prove that $W(T) \cong \mathbb{Z}$!

We first show that W(T) has no torsion elements $\neq 0$. Thus let z be a torsion element of W(T). There exists a finite subcovering B of A in T such that z is the image of a torsion element w in W(B). By Th. 11.7 there exists some (f) in $Q^+(B)$ with $w = 1 - (f)$. We assume without loss of generality that $w \neq 0$, and we regard the normalization C of B in the extension $K(\sqrt{f})$ of the field of fractions K of B, equipped with the trivial involution. C is a covering of degree 2 of B. The kernel of the canonical map from W(K) to $W(K(\sqrt{f}))$ is generated by $1 - (f)$ in W(K) and hence is nilpotent. Thus also the kernel of the canonical map from W(B) to W(C) is nilpotent, and the signature $\tau|B$ of B can certainly be extended to C. This implies that C can be embedded into T over B by Cor. 3.10. Since the image of w in W(C) is zero, also the image z of w in W(T) must be zero. Thus W(T) contains no nilpotent elements $\neq 0$.

It now suffices to prove that τ is the only signature of T, cf. proof of Cor. 7.7. Suppose there exists another signature γ on T. We choose a finite subcovering B of A in T such that the signatures

$\tau_1 := \tau|B$ and $\gamma_1 := \gamma|B$ are still different. By Th. 11.7 there exists some (f) in Q(B) with $\tau_1(f) = +1$ and $\gamma_1(f) = -1$. We again consider the normalization C of B in the extension $K(\sqrt{f})$ of the field of fractions K of B. Let X_1 be the real curve corresponding to B and X_2 the real curve corresponding to C. We immediately see that there lies a connected component of $X_2(R)$ over the component of $X_1(R)$ belonging to τ_1 (cf. Th. 11.7) but no component of $X_2(R)$ lies over the component of $X_1(R)$ belonging to γ_1. Thus τ_1 can be extended to the covering C of B, while γ_1 can not be extended to C. This is the desired contradiction: We can imbed C over B into T, since τ_1 extends to C, and then $\gamma|C$ will be an extension of γ_1 to C. Thus τ must be the only signature of T.

q.e.d.

Question 11.11. Let B be a covering with trivial involution of our ring $A = R[X]$. Assume that $[\overline{A}:B] = 2$. Is B always real?

If this question has an affirmative answer then we shall have a theorem completely analogous to our main theorem 10.12 for Dedekind domains which contain R and have a field of fractions of transcendency degree 1 over R.

On the other hand a strict real closure of A may have a very big group of automorphisms over A in contrast to the semi-local case. As an example we choose A as the ring $R[x,y]$ with the defining relation

$$x^2 + y^2 = 1.$$

Then A' is the ring $C[z,z^{-1}]$ of Laurent polynomials in the variable $z := x + iy$ ($i := \sqrt{-1}$). The involution of A' extends the complex conjugation of C and maps z to

$$z^{-1} = x - iy.$$

{Keep in mind the formula $e^{i\varphi} = \cos\varphi + i \sin\varphi$.} For every natural number $n \geq 1$ we choose in the algebraic closure L of the field of fractions F' of A' an n-th root z_n of z such that

$$z_n^d = z_m$$

if n is a multiple md of m. We consider the subrings

$$A_n' := A[z_n] = C[z_n, z_n^{-1}]$$

of L, equipped with the involutions mapping z_n to z_n^{-1} and extending the complex conjugation of C. Then A_m' is a π-subring of A_n' if m divides n, and all A_n' are coverings of A'. This implies that the fixed rings $A_n := (A_n')_o$ are coverings of A. We have $A_n = R[x_n, y_n]$ with generators

$$x_n := \tfrac{1}{2}(z_n + z_n^{-1}), \quad y_n := \tfrac{1}{2i}(z_n - z_n^{-1}),$$

subject to the relation

$$x_n^2 + y_n^2 = 1.$$

We finally regard the infinite coverings

$$R := \bigcup_{n=1}^{\infty} A_n' , \quad T := \bigcup_{n=1}^{\infty} A_n$$

of A' and A respectively. According to the theorems 11.7 and 11.9 every A_n' has a unique signature σ_n' and every A_n has a unique signature σ_n. If m divides n then σ_n' must extend σ_m' and σ_n must extend σ_m. Thus R and T have unique signatures ρ and τ.

We want to prove that (T, τ) is a strict real closure of A with respect to the unique signature $\sigma := \sigma_1$, and that at the same time T is galois over A.

We have an automorphism

$$\alpha_n' : z_n \longmapsto \zeta_n z_n, \quad \zeta_n := e^{\frac{2\pi i}{n}},$$

of the ring A_n' over A', which is compatible with the involution of A_n' since $\overline{\zeta}_n = \zeta_n^{-1}$. This automorphism has order n. Since $[A_n' : A'] = n$, we see that A_n' is a galois covering of A' with Galois group generated by α_n'. If m divides n then α_n' clearly extends α_m', hence the α_n' yield an automorphism α' of R over A' and by restriction an automorphism α of $R_o = T$ over A. Clearly R is galois over A' and

$$G(R|A') \cong \hat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}$$

is generated by α'. This implies that T is galois over A with

$$G(T|A) \cong G(R|A') \cong \hat{\mathbb{Z}}$$

generated by α.

Now the Riemann surface

$$C^* = \mathbb{P}^1(C) \setminus \{0, \infty\}$$

corresponding to the curve Spec(A') over C is homotopy equivalent to the circle S^1 and hence has a topological fundamental group isomorphic to $\mathbb{Z}$. Thus there exists up to topological and hence analytical isomorphy only one covering of C^* of degree n for every $n \geq 1$. Since the isomorphy classes of finite coverings of C^* correspond uniquely to the isomorphy classes of finite coverings of $|A'|$, cf. e.g. [P, p.15], we learn that up to isomorphy $|A_n'|$ is the only covering of $|A'|$ of degree n. Thus $|R|$ is simply connected and (R,ρ) is certainly real closed. This implies that (T,τ) is strictly real closed.

References

References occuring already in part I are denoted here by the same symbol.

[AK] R.Ahrens, I.Kaplansky, Topological representations of algebras, Trans. Amer. Math. Soc. 63 (1948), 457 - 481.

[Al] A.A.Albert, "Modern higher algebra", Univ. Chicago Press, Chicago 1937.

[AS_2] E.Artin, O.Schreier, Eine Kennzeichnung der reell abgeschlossenen Körper, Hamb. Abh. 5 (1927), 225 - 231.

[B_1] N.Bourbaki, "Algèbre commutative", Chap. 1 - 2, Hermann, Paris 1961.

[DD] J.Diller, A.Dress, Zur Galoistheorie pythagoräischer Körper, Arch. Math. 16 (1965), 148 - 152.

[D_2] A.Dress, A connection between Burnside- and Wittrings, Notes on the theory of representations of finite groups I, Chap. 2, Appendix B, University of Bielefeld 1971.

[D_3] A.Dress, A note on Witt rings, Bull. Amer. Math. Soc. 79 (1973), 738 - 740.

[Ge] W.D.Geyer, Ein algebraischer Beweis des Satzes von Weichold über reelle algebraische Funktionenkörper, Bericht Tagung Algebr. Zahlentheorie Oberwolfach 1964, Bibliographisches Institut, Mannheim 1966.

[G_1] A.Grothendieck, Revêtements étales et groupe fondamental, Séminaire de géometrie algébrique du Bois Marie 1960-61, Springer, Lecture Notes in Math. 224 (1970).

[K] M.Knebusch, Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen, Sitz.ber. Heidelberg, Akad. Wiss. Math. - naturw. Kl. 1969/70, 3. Abh.

[K_0] M.Knebusch, Real closures of commutative rings I, J. reine angew. Math.

[K_1] M.Knebusch, Real closures of semi-local rings, and extension of real places, Bull. Amer. Math. Soc. 79 (1973), 78 - 81.

[K_3] M.Knebusch, Generalization of a theorem of Artin-Pfister to arbitrary semi-local rings, and related topics, J. of Algebra, to appear.

[KRW_2] M.Knebusch, A.Rosenberg, R.Ware, Signatures on semi-local rings, J. Algebra 26 (1973), 208 - 250.

[KRW_3] M.Knebusch, A.Rosenberg, R.Ware, Grothendieck and Wittrings of hermitian forms over Dedekind rings, Pacific J. Math. 43 (1972), 657 - 673.

[La] S.Lang, "Algebra", Addison-Wesley, Reading, Mass. 1965.

[L] J.B.Leicht, Zur Charakterisierung reell abgeschlossener Körper, Monatshefte f. Math. 70 (1966), 452 - 453.

[MH] J.Milnor, D.Husemoller, "Symmetric bilinear forms", Ergebnisse Math. 73, Springer, Berlin-Heidelberg-New York 1973.

[Pf] A.Pfister, Quadratische Formen in beliebigen Körpern, Invent. Math. 1 (1966), 116 - 132.

[P] H.Popp, "Fundamentalgruppen algebraischer Mannigfaltigkeiten", Springer, Lecture Notes in Math. 176, (1970).

[S] J.P.Serre, "Cohomologie galoisienne", Springer, Lecture Notes in Math. 5 (1964).

[Sm] C.Small, The group of quadratic extensions, J. pure appl. Algebra 2 (1972), 83 - 105.

[W] E.Witt, Zerlegung reeller algebraischer Funktionen in Quadrate, Schiefkörper über reellem Funktionenkörper, J. reine angew. Math. 171 (1934), 4 - 11.

[W_1] E.Witt, Theorie der quadratischen Formen in beliebigen Körpern, J. reine angew. Math. 176 (1937), 31 - 44.

Address: Manfred Knebusch
Fachbereich Mathematik der
Universität Regensburg

D-84 R e g e n s b u r g
Universitätsstraße 31