On Algebraic Curves over Real Closed Fields. II

Manfred Knebusch

Fachbereich Mathematik der Universität, Universitätsstr. 31, D-8400 Regensburg,
Federal Republic of Germany

The contents of this second part of our study on smooth algebraic curves over a real closed field K have roughly been indicated in part I [K_3] at the end of the introduction. Throughout we use the terminology, notations, and results developed in part I.

§7. A Closer Look at the Topology of γ

Again we assume that the set γ of real points of our smooth curve X is not empty. As always let $\gamma_1, \ldots, \gamma_r$ denote the components of γ.

(7.1) **Definition.** A *generalized open interval* on γ is either an interval $]P, Q[$ or a component γ_i or a set $\gamma_i \smallsetminus \{P\}$ obtained by omission of one point P from a component γ_i.

Our first goal is to prove

(7.2) **Theorem.** i) *For every real function $f \neq 0$ on γ the set $f^{-1}(]\infty, 0[)$ is a disjoint union of generalized open intervals.*

ii) *For any disjoint union A of generalized open intervals there exists a real function f on γ with $f^{-1}(]\infty, 0[) = A$ and without poles on γ.*

The first assertion in this theorem is an easy consequence of the results in the preceding Section 6. Indeed, let f be a real function $\neq 0$ on γ. It suffices to show that the intersection A_1 of $f^{-1}(]\infty, 0[)$ with the component γ_1 is a disjoint union of generalized open intervals. If f is positive definite on γ_1 the set A_1 is empty. If f is negative definite on γ_1 the set A_1 arises from γ_1 by omission of the finitely many poles and zeros of f on this component, and by Corollary (6.7) A_1 is certainly a disjoint union of open intervals or a generalized open interval. Let now f be indefinite on γ_1. By Theorem (6.8) the set

$$A_1' := \{P \in \gamma_1 \mid \tau_P(f) = -1\}$$

is a disjoint union of open intervals. A_1 arises from A_1' by omission of the poles and zeros of f contained in A_1'. Now omitting a point R in an interval $]P, Q[$ we obtain the disjoint union of the intervals $]P, R[$ and $]R, Q[$ (Prop. (6.5)). Thus A_1 again is a disjoint union of open intervals.

This proves part i) of Theorem (7.2). For the proof of part ii) we make use of the previous Lemma (2.14) on definite functions with prescribed poles and zeros on γ. Let $\mathfrak{A}$ be a finite family of disjoint generalized open intervals on γ and A their union. Let T denote the finite set of points P with either $P \in \gamma_i$ and $\gamma_i \smallsetminus \{P\}$ in $\mathfrak{A}$ or with P a common endpoint of two open intervals in $\mathfrak{A}$. Then $B := A \cup T$ is a disjoint union of sets $I_1, \ldots, I_s$ which are full components of γ or open intervals without any common endpoints. For every I_j we choose a real function h_j as follows. If I_j is a component γ_i, then h_j is a function f_i negative definite on γ_i and positive definite on $\gamma \smallsetminus \gamma_i$. If I_j is an open interval, then h_j is a interval function for I_j. Let h denote the product $h_1 \ldots h_s$. Clearly

$$B = \{P \in \gamma \mid \tau_P(h) = -1\}.$$

Using Lemma (2.14) we easily find a positive definite real function g such that $f := gh$ has no poles on γ and has zeros in B precisely at the points of T. {We do not need the full content of Lemma (2.14) for this.} Obviously $f^{-1}(]\infty, 0[) = A$, and our Theorem (7.2) is proved.

We now want to prove that the set of open intervals is a basis of the topology of γ.

(7.3) **Lemma.** *Let A and B be generalized open intervals on γ_1 which are not disjoint. Then $A \cup B$ is again a generalized open interval, and the intersection $A \cap B$ is either a generalized open interval or the disjoint union of two intervals.*

Proof. We assume that A and B are open intervals, $A =]P, Q[$, $B =]R, S[$, since otherwise the statements of the lemma are evident. We first consider the case $A \cup B \neq \gamma_1$. We choose a point P_0 on γ_1 outside $A \cup B$, and we equip $\gamma_1 \smallsetminus \{P_0\}$ with the total ordering introduced in § 6. Then $P < Q$ and $R < S$. If $Q \leq R$ then the intervals A and B would be disjoint. Thus $Q > R$, and $A \cup B =]P, S[$, $A \cap B =]R, Q[$ {Apply Prop. (6.6)}.

Assume now $A \cup B = \gamma_1$. In this case we will not need the assumption that A and B are not disjoint. The four points P, Q, R, S certainly all are different. We equip $\gamma_1 \smallsetminus \{P\}$ with the ordering introduced in § 6 and apply again Proposition (6.6). Since P lies in B we have $S < R$, and since R lies in A we have $R < Q$. From the relation $S < R < Q$ we see that $A \cap B$ is the union of the intervals $]P, S[$ and $]R, Q[$. This finishes the proof of the lemma.

Let $\mathfrak{J}$ denote the set of all subsets of γ which are disjoint unions of finitely many generalized open intervals. From the Lemma (7.3) just proved and part i) of Theorem (7.2) we obtain easily

(7.4) **Theorem.** *The union and the intersection of finitely many elements of $\mathfrak{J}$ again lie in $\mathfrak{J}$. The set of open intervals of γ is a basis of the topology of γ.*

Now we have no difficulty to prove

(7.5) **Proposition.** *The closure of an open interval $]P, Q[$ is the closed interval $[P, Q] =]P, Q[\cup \{P, Q\}$.*

Proof. Assume that $]P, Q[$ is contained in γ_1. We have seen in § 6 that $[P, Q]$ is indeed a closed set. To prove that P is adherent to $]P, Q[$ it suffices by the preceding theorem to show that for every interval $]R, S[$ containing P the intersection $]P, Q[\cap]R, S[$ is not empty. This is clear from the proof of Lemma (7.3) in the case that $]P, Q[\cup]R, S[= \gamma_1$. Otherwise introduce the ordering of $\gamma_1 \smallsetminus \{P_0\}$ with respect to a point P_0 not lying in $]P, Q[\cup]R, S[$ and apply Proposition (6.6). In the same way we see that Q is adherent to $]P, Q[$.

(7.6) *Remark.* Using Theorem (7.4) we immediately see that the closure of a generalized open interval $\gamma_i \smallsetminus \{P\}$ is γ_i. More generally every set obtained from γ_i by omission of finitely many points is dense in γ_i.

§ 8. Analysis of Real Functions

We study the behaviour of a real function f on a closed interval $[P, Q]$ on which f has no poles.

Let $[P, Q]$ be contained in the component γ_1. We equip $[P, Q]$ with the total ordering induced by the ordering of $\gamma_1 \smallsetminus \{P_0\}$ defined in § 6. Here P_0 denotes an arbitrary point of γ_1 not contained in $[P, Q]$. The ordering of $[P, Q]$ does not depend on the choice of P_0. Indeed, for every point R in $]P, Q[$ we have $P < R < Q$, and for two points R, S in $]P, Q[$ we have $R \leq S$ if and only if $[P, R]$ is contained in $[P, S]$ (cf. Prop. (6.6)).

Without essential loss of generality we always assume that our function f is not constant, i.e. $f \notin K$. We choose once and for all a definite differential ω_0 representing the orientation of γ (cf. § 5). Let g denote the *differential quotient* df/ω_0. By this we mean the unique function g in F^* with $df = g\omega_0$.

(8.1) **Lemma.** *Let R be a point of γ which is not a pole of f. Then with $c := f(R)$*

$$\tau_R(g) = \partial_R(f - c), \quad \partial_R(g) = \tau_R(f - c).$$

N.B. τ_R and ∂_R have been defined in § 2 and § 5.

Proof. Replacing f by $f - c$ we assume $c = 0$. We choose a uniformizing parameter t of X at R. The function field F embeds in a natural way into the quotient field $K((t))$ of the ring $K[[t]]$ of formal power series in the variable t over K. Using this embedding we may write

$$f = t^n(a_0 + a_1 t + \cdots)$$
$$\omega_0 = t^{2m}(b_0 + b_1 t + \cdots)dt$$

with $n \geq 1$, m an integer, and $a_0 \neq 0$, $b_0 \neq 0$. We have

$$df = t^{n-1}(na_0 + \cdots)dt,$$

hence

$$g = t^{n-1-2m}(na_0 b_0^{-1} + \cdots).$$

If n is odd we get

$$\partial_R(g) = \tau_R(f) = 0,$$

$$\partial_R(f) = \operatorname{res}_R \langle f \omega_0 \rangle = \operatorname{sign}(a_0 b_0) = \tau_R(g).$$

If n is even we get

$$\tau_R(g) = \partial_R(f) = 0,$$

$$\partial_R(g) = \operatorname{res}_R \langle df \rangle = \operatorname{sign}(a_0) = \tau_R(f).$$

Thus the assertions of the lemma hold true in both cases.

We recall that we always assume that f has no poles in $[P, Q]$ and is not a constant.

(8.2) **Theorem.** (Intermediate value theorem.) *If $f(P) < f(Q)$ and c is an element of K with $f(P) < c < f(Q)$ then $]P, Q[$ contains a point R with $f(R) = c$ and $\tau_R(g) = +1$. If $f(P) > f(Q)$ and again c lies between $f(P)$ and $f(Q)$ then $]P, Q[$ contains a point R with $f(R) = c$ and $\tau_R(g) = -1$.*

Proof. Again replacing f by $f - c$ we assume $c = 0$. In the first case $f(P) < 0$ and $f(Q) > 0$, in the second $f(P) > 0$ and $f(Q) < 0$. The assertions immediately follow from Theorem (6.8) and the Lemma (8.1) just proved.

(8.3) **Theorem.** ("Rolle's theorem".) *Assume $f(P) = f(Q)$. If there is a pont P' in $]P, Q[$ with $f(P') > f(P)$ then there exists in $]P, Q[$ a zero R of g with $\partial_R(g) = -1$. If there is a point P' in $]P, Q[$ with $f(P') < f(P)$ then there exists in $]P, Q[$ a zero R of g with $\partial_R(g) = +1$.*

Proof. We may assume $f(P) = f(Q) = 0$. Moreover we may assume that f has no zero in $]P, Q[$, since otherwise we just pass to a smaller closed interval. By the intermediate value Theorem (8.2) we than have either $f(R) > 0$ for all R in $]P, Q[$ or $f(R) < 0$ for all these R. Eventually replacing f by $-f$ we assume $f(R) > 0$ for all R in $]P, Q[$. If f has even order at P then $\tau_P(f) = +1$. {Multiply f by the square of some real function such that the zero P disappears.} Thus $\partial_P(g) = +1$ by Lemma (8.1). If f has odd order at P then by Theorem (6.8) $\partial_P(f) = +1$, hence $\tau_P(g) = +1$. In the same way we see that either $\partial_Q(g) = +1$ or $\tau_Q(g) = -1$. Thus only the following four cases are possible:

1) $\partial_P(g) = \partial_Q(g) = +1$;
2) $\partial_P(g) = +1, \quad \tau_Q(g) = -1$;
3) $\tau_P(g) = +1, \quad \partial_Q(g) = +1$;
4) $\tau_P(g) = +1, \quad \tau_Q(g) = -1$.

In all these cases Theorem (6.8) tells us that there exists a point R in $]P, Q[$ with $\partial_R(g) = -1$.   q.e.d.

Theorems (8.2) and (8.3) imply

(8.4) **Corollary.** (Monotone functions.) *Assume $\tau_R(g) = +1$ for all R in $]P, Q[$. Then f is strictly increasing on $[P, Q]$, i.e. for points R and S in $[P, Q]$ with $R < S$ we always have $f(R) < f(S)$.*

Proof. Let R and S be points in $[P, Q]$ with $R < S$. If $f(R) > f(S)$ then by Theorem (8.2) there would exist (infinitely many) points T in $]R, S[$ with $\tau_T(g) = -1$. If $f(R) = f(S)$ then by Theorem (8.3) the interval $]R, S[$ would contain a zero of g of odd order. By assumption such a zero does not exist. Thus $f(R) < f(S)$.

Now we are able to show that f "attains its maximum and its minimum" on $[P, Q]$.

(8.5) Theorem. $f([P, Q])$ *is a closed interval* $[a, b]$ *of* K. *For every point* R *in* $]P, Q[$ *with* $f(R) = a$ *we have* $\partial_R(g) = +1$, *and for every point* S *in* $]P, Q[$ *with* $f(S) = b$ *we have* $\partial_S(g) = -1$.

Proof. If g has no zeros of odd order in $]P, Q[$ then the assertions follow immediately from the preceding Corollary (8.4), since then $\tau_R(g)$ has the same value for all R in $]P, Q[$ (cf. Cor. (6.9)). Assume now that g has in $]P, Q[$ the zeros $P_1 < \cdots < P_t$ of odd order. Eventually replacing g by $-g$ we further assume $\partial_{P_1}(g) = -1$. Then by Theorem (6.8)

$$\partial_{P_i}(g) = (-1)^i \quad (1 \leq i \leq t),$$

and $\tau_R(g)$ has constant value $(-1)^i$ for R in $]P_i, P_{i+1}[$, $1 \leq i \leq t-1$, and constant values $+1$ in $]P, P_1[$ and -1 in $]P_t, Q[$. Thus we know from Corollary (8.4) that

$$f(P) < f(P_1), f(P_1) > f(P_2), \dots$$

and

$$f([P, P_1]) = [f(P), f(P_1)],$$
$$f([P_1, P_2]) = [f(P_2), f(P_1)],$$

etc. Moreover f is in each of the intervals $[P, P_1]$, $[P_1, P_2]$, ..., $[P_t, Q]$ strictly increasing or strictly decreasing. The assertions of the theorem are now obvious.

Remark. A theorem similar to Theorem (8.5) clearly holds true for real functions on a component γ_i which have no poles in γ_i.

(8.6) Corollary. (Local extrema.) *Let* P *be a point of* γ *at which* f *has no pole. The following statements are equivalent:*

i) $\partial_P(g) = +1$.

ii) *There exists a closed interval* $[R, S]$ *with* P *in* $]R, S[$ *and* $f(P') > f(P)$ *for all points* P' *in* $[R, S]$ *which are different from* P.

Proof. The implication ii) $\Rightarrow$ i) is evident from the preceding Theorem (8.5). Assume now that $\partial_P(g) = +1$. We choose a neighbourhood $[R, S]$ of P in which g has no zero of odd order except P. This is certainly possible since the set of open intervals is a basis of the topology of γ (Th. (7.5)). Again by the preceding theorem $f(P') > f(P)$ for all $P' \neq P$ in $[R, S]$.

§ 9. Quadratic Forms over the Function Field

Since now we do not exclude the case $r = 0$, i.e. γ may be empty. But many statements will be void if $r = 0$.

We first want to generalize the previous Theorem (6.8) about the sign behaviour of real functions to quadratic forms.

(9.1) **Lemma.** *Let φ be a quadratic form over F, and assume $\partial_R(\varphi)=0$ for all R in some open interval $]P, Q[$. Then the function $R \mapsto \tau_R(\varphi)$ is contant in $]P, Q[$.*

Proof. We choose a diagonalisation

$$\varphi \cong \langle f_1, \ldots, f_n \rangle.$$

If none of the functions f_i has odd order at any point in $]P, Q[$, then the f_i all have constant sign in $]P, Q[$ (Cor. (6.9)) and

$$\tau_R(\varphi) = \sum_{i=1}^{n} \tau_R(f_i)$$

has constant value in $]P, Q[$. Assume now there are points in $]P, Q[$ at which at least one of the functions f_i has odd order, and let

$$P_1 < \cdots < P_t$$

be these points. Put $P_0 := P$ and $P_{t+1} := Q$. We know from above that $R \mapsto \tau_R(\varphi)$ has on each interval $]P_i, P_{i+1}[$, $0 \leq i \leq t$, a constant value n_i. We fix a point P_i, $1 \leq i \leq t$, and choose a diagonalisation

$$\varphi \cong \langle u_1, \ldots, u_n \rangle$$

with functions u_i which have no pole or zero at P_i. This is possible since $\partial_{P_i}(\varphi)=0$, cf. [MH, p. 92]. There exist points P' in $]P_{i-1}, P_i[$ and Q' in $]P_i, P_{i+1}[$ such that $u_1, \ldots, u_n$ all have no zeros or poles in $]P', Q'[$, since the open intervals are a basis of the topology of γ (Th. (7.4)). Thus $\tau_R(\varphi)$ is constant in $]P', Q'[$. This interval has the non empty intersection $]P', P_i[$ with $]P_{i-1}, P_i[$ and also a non empty intersection with $]P_i, P_{i+1}[$. Thus $n_{i-1} = n_i$ and our lemma is proved.

(9.2) **Theorem.** *Assume $\gamma \neq \varnothing$. Let φ be a quadratic form over F, and let t denote the number of points P on the component γ_1 with $\partial_P(\varphi) \neq 0$.*

   i) *If $t=0$, then the function $P \mapsto \tau_P(\varphi)$ is constant on γ_1 (clear by the preceding Lemma (9.1)).*

   ii) *If $t \neq 0$, then $t \geq 2$. Let $P_0, \ldots, P_{t-1}$ be then points P of γ_1 with $\partial_P(\varphi) \neq 0$, and assume*

$$P_1 < \cdots < P_{t-1}$$

with respect to the ordering of $\gamma_1 \smallsetminus \{P_0\}$ (cf. §6). In each open interval $]P_i, P_{i+1}[$, $0 \leq i \leq t-1$, the function $P \mapsto \tau_P(\varphi)$ has a constant value n_i, according to the preceding Lemma (9.1) {Read $P_t = P_0$}. We have

$$\tau_{P_i}(\varphi) = \tfrac{1}{2}(n_i + n_{i+1})$$
$$\partial_{P_i}(\varphi) = \tfrac{1}{2}(n_{i+1} - n_i)$$

for $0 \leq i \leq t-1$ {Read $n_t = n_0$}.

Proof. We only have to consider the case $t > 0$. Clearly $t \geq 2$ by the sum formula (5.6). Let $Q := P_i$ for some fixed i, $0 \leq i \leq t - 1$. We choose a real function u which is negative definite in $]P_{i-1}, P_i[$ and positive definite in $]P_i, P_{i+1}[$. {Read $P_{-1} = P_{t-1}$.} In particular u has odd order at $Q = P_i$, cf. Theorem (6.8). We choose a decomposition

$$\varphi \cong \psi \perp u \chi$$

with $\partial_Q(\psi) = \partial_Q(\chi) = 0$. Then for suitable points R in $]P_{i-1}, P_i[$ and S in $]P_i, P_{i+1}[$ both $\tau_P(\psi)$ and $\tau_P(\chi)$ have constant values $\tau_P(\psi) = m_i$, $\tau_P(\chi) = \delta_i$ if P runs in $[R, S]$. We compute (read $n_{-1} = n_{t-1}$):

$$n_{i-1} = m_i - \delta_i, \qquad n_i = m_i + \delta_i,$$

since $\tau_R(u) = -1$ and $\tau_S(u) = +1$ (cf. Th. (6.8)). On the other hand we have

$$\tau_Q(\varphi) = m_i, \qquad \partial_Q(\varphi) = \delta_i,$$

since $\partial_Q(u) = +1$ by Theorem (6.8). Thus indeed the formulas for $\tau_Q(\varphi)$ and $\partial_Q(\varphi)$ stated in the theorem are true.

(9.3) **Definition.** Let P be a point of γ and φ be a quadratic form over F. We say φ is *positive definite* (*negative definite*) at P if $\tau_P(\varphi) = \dim \varphi$ (resp. $\tau_P(\varphi) = -\dim \varphi$). If φ is neither positive nor negative definite at P we call φ *indefinite* at P.

φ is positive definite at P if and only if either $\varphi = 0$ or φ has a diagonalization

$$\varphi \cong \langle f_1, \ldots, f_n \rangle$$

with all f_i positive definite at P. This then is true for every diagonalisation of φ. Clearly an isotropic form φ is indefinite everywhere on γ.

(9.4) **Theorem.** *Assume φ is indefinite at almost all real points of X and $\dim \varphi \geq 3$. Then φ is isotropic.*

This important theorem is in the case $K = \mathbb{R}$ due to Witt [W₁, Satz 22], and in the general case to Elman-Lam-Prestel [ELP, p. 298]. Elman, Lam, and Prestel use quite another method then Witt. Our work in § 2 − § 7 allows us to give a proof of the theorem along precisely the same lines as Witt's proof. We give this proof in detail, since in [W₁] the geometric facts needed for the proof are only faintly indicated.

We first consider the case that φ is a quaternion form $\langle 1, -f \rangle \otimes \langle 1, -g \rangle$. Then we can write (cf. Lemma (2.11))

$$\varphi \cong 2 \times \langle 1, -u \rangle$$

with some real function u. For almost all P in γ we have

$$\tau_P(\varphi) = 2(1 - \tau_P(u)) < 4.$$

Thus $\tau_P(u) = +1$ for almost all P and u is positive definite (Th. (2.3)). By Theorem (4.1) u is a sum of two squares in F, hence

$$\varphi \cong 2 \times \langle 1, -1 \rangle.$$

We now consider the case dim $\varphi = 3$. Multiplying φ by a constant we may assume that φ is the pure part $\langle -f, -g, fg \rangle$ of a quaternion form $\psi = \langle 1, f \rangle \otimes \langle 1, -g \rangle$. Since $\psi = \langle 1 \rangle \perp \varphi$, certainly $\tau_P(\psi) < 4$ for almost all P. Thus ψ is hyperbolic as shown above. This implies that φ is isotropic.

We finally prove the theorem for dim $\varphi = n \geq 4$ by induction on n. We choose some decomposition

$$\varphi \cong \psi_1 \perp (-\psi_2)$$

with dim $\psi_1 = n - 2$, dim $\psi_2 = 2$. By Theorem (9.2) the set A_i of all P in γ with ψ_i positive definite at P is the disjoint union of open intervals and whole components. Thus by Theorem (7.4) the union $A := A_1 \cup A_2$ is certainly a disjoint union of generalized open intervals, and by Theorem (7.2) there exists a real function f on γ with $f^{-1}(]0, \infty[) = A$. The quadratic forms

$$\tilde{\psi}_i := \psi_i \perp \langle -f \rangle, \quad i = 1, 2$$

are clearly both indefinite at almost all points of γ. By the induction hypothesis they are isotropic. Thus ψ_1 and ψ_2 both represent $\langle f \rangle$, and φ is isotropic.

We denote the signed determinant of φ [L, p. 38] by $d(\varphi)$. Theorem (9.4) implies the following – in fact much weaker – statement:

(9.5) **Theorem** (cf. [W_1, Satz 23]). *Let φ and ψ be forms over F with dim $\varphi =$ dim ψ, $d(\varphi) = d(\psi)$, and $\tau_P(\varphi) = \tau_P(\psi)$ for almost all P in γ. Then $\varphi \cong \psi$.*

Proof. Let χ denote the kernel form of $\varphi \perp (-\psi)$. We have $\tau_P(\chi) = 0$ for almost all P in γ, hence by the preceding theorem dim $(\chi) \leq 2$. Since χ has even dimension and $d(\chi) = 1$ we have $\chi = 0$. This implies $\varphi \cong \psi$.

By $\nu(\varphi)$ we denote the "dimension index" of φ, i.e. the element dim φ mod 2 of $\mathbf{Z}/2\mathbf{Z}$. Another way to state Theorem (9.5) is as follows:

(9.6) **Corollary.** *Let φ and ψ be quadratic forms over F with $\nu(\varphi) = \nu(\psi)$, $d(\varphi) = d(\psi)$, and $\tau_P(\varphi) = \tau_P(\psi)$ for almost all P in γ. Then $\varphi \sim \psi$.*

In this corollary the condition $\nu(\varphi) = \nu(\psi)$ can be omitted if $r > 0$, since clearly

$$\nu(\varphi) = \tau_P(\varphi) \bmod 2$$

for every P in γ with $\partial_P(\varphi) = 0$. It also should be noticed that already by Theorem (9.2) the equality $\tau_P(\varphi) = \tau_P(\psi)$ for almost all P in γ implies this equality for all P in γ.

§ 10. Witt Rings of Curves

We want to compute the Witt ring $W(Z)$ of a Zariski open subset Z of X. We first give the definition of this ring. Let A denote the Grothendieck ring of "*bilinear spaces*" over Z, i.e. of pairs (E, B) with E a locally free $\mathcal{O}_Z$-module of finite rank and $B: E \times E \to \mathcal{O}_Z$ a non degenerate symmetric bilinear form on E (cf. [K]; in [K] this ring is denoted by $K(Z)$). A "Lagrangian subspace" V of E is an $\mathcal{O}_Z$-submodule

V of E which is locally a direct summand of the $\mathcal{O}_Z$-module E and has the property $V = V^{\perp}$ with respect to B. Let $\mathfrak{a}$ denote the set of all elements $[(E_1, B_1)] - [(E_2, B_2)]$ in A such that both E_1 and E_2 have Lagrangian subspaces. It is easily seen that $\mathfrak{a}$ is an ideal of A, and we define

(10.1) $W(Z) := A/\mathfrak{a}.$

Remark. If $Z \neq X$, hence Z affine, this definition coincides with the definition of Witt rings given in [K]. Indeed, if V is a Lagrangian subspace of (E, B) there exists a decomposition $E = V \oplus G$ with G a suitable submodule of E, and thus (E, B) is "hyperbolic" in this case [K, 3.3.1]. If $Z = X$, the definition (10.1) usually yields a coarser object than the Witt ring defined in [K]. There exist strong reasons to adopt (10.1) instead of the definition of $W(Z)$ in [K], but we do not have space here to discuss these matters.

We have a natural homomorphism from $W(Z)$ to $W(F)$ mapping a class $[(E, B)]$ to the class $[(\tilde{E}, \tilde{B})]$ in $W(F)$ with $\tilde{E}$ the F-vectorspace of rational sections of E and $\tilde{B}$ the bilinear form induced by B on $\tilde{E}$. The argument at the beginning of § 13 in [K] shows (cf. [MH, p. 93] for Z affine):

(10.2)   **Proposition.** *The natural homomorphism from $W(Z)$ to $W(F)$ is injective.*

Since now we always regard $W(Z)$ as a subring of $W(F)$. We want to describe this subring. For every complex point $\mathfrak{p}$ of X we define an additive map

$\partial_{\mathfrak{p}}: W(F) \to \mathbb{Z}/2\mathbb{Z}$

by

$\partial_{\mathfrak{p}}(\varphi) := \mathrm{ord}_{\mathfrak{p}}(d(\varphi)) \bmod 2$

using an obvious notation. This definition coincides with the general definition of a "second residue class form map" in [MH, p. 85] or [K, 13.3.5], since the residue class field $K(\sqrt{-1})$ at $\mathfrak{p}$ has the Witt ring $\mathbb{Z}/2\mathbb{Z}$. {In particular different choices of a local uniformizing parameter at $\mathfrak{p}$ yield the same map $\partial_{\mathfrak{p}}$.}

As a special case of [K, Satz 13.3.6] we have (cf. [MH, p. 91] for Z affine)

(10.3)   **Proposition.** $W(Z)$ *is the set of elements ξ in $W(F)$ with $\partial_{\mathfrak{p}}(\xi) = 0$ for all real and all complex points $\mathfrak{p}$ of Z.*

In particular the intersection of $W(Z)$ with the subgroup $Q(F)$ of classes of one dimensional forms in $W(F)$ is the group $Q(Z)$ introduced in § 2.

Let $\beta_1, \ldots, \beta_t$ be the components of the set β of real points of Z ($t = 0$ if β empty). These β_i are generalized open intervals, explicitly described in Theorem (6.10). Let φ be a form over F with class $[\varphi]$ in $W(Z)$. Then according to Lemma (9.1) and the preceding Proposition (10.3) the function $P \mapsto \tau_P(\varphi)$ has on each β_i a constant value, which we call $\tau_i(\varphi)$. In this way we obtain t ring homomorphisms

$\tau_i: W(Z) \to \mathbb{Z}, \quad 1 \leq i \leq t.$

We choose elements $\langle f_1 \rangle, \ldots, \langle f_t \rangle$ in $Q(Z)$ such that f_i has sign -1 on β_i and $+1$ on $\beta \setminus \beta_i$. This is possible by Theorem (2.10) and Proposition (2.4). We further denote by $Q^+(Z)$ the group of all square classes $\langle f \rangle$ in $Q(Z)$ with $\tau_i(\langle f \rangle) = +1$

for $1 \leq i \leq t$. These functions f are the real functions which are positive definite on β, hence on γ, and have even order also at all complex points of Z.

We finally denote by $I(Z)$ the ideal of all classes $[\varphi]$ in $W(Z)$ of dimension index $v(\varphi) = 0$, and by $I^n(Z)$ the n-th power of this ideal $(n \geq 1)$. We have the following description of $W(Z)$:

(10.4) Theorem. i) *Every element ξ of $W(Z)$ is uniquely determined by the values $v(\xi), d(\xi), \tau_1(\xi), \ldots, \tau_t(\xi)$. In case $t \geq 1$ the value $v(\xi)$ can be omitted.*

ii) *The torsion part $I(Z)_t$ of $I(Z)$ as abelian group consists of the elements $1 - \langle f \rangle$ with $\langle f \rangle$ in $Q^+(Z)$. We have $I^2(Z)_t = 0$ and in particular $2 I(Z)_t = 0$. The ideal $I(Z)_t$ is the nil radical of $W(Z)$.*

iii) *$I(Z)$ has the direct decomposition*

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

The product of any two different components in this decomposition is zero.

iv) *If $t \geq 1$ the ring homomorphism*

$$(\tau_1, \ldots, \tau_t) : W(Z) \to \mathbb{Z}^t$$

maps $W(Z)$ onto the subring of $\mathbb{Z}^t$ consisting of all t-tupels $(n_1, \ldots, n_t)$ with all n_i even or all n_i odd.

This theorem follows from Corollary (9.6) at the end of §9 in precisely the same way as indicated in $[K_2, II, §11]$ in the special case $K = \mathbb{R}$, Z affine (cf. Proof of Th. 11.7 in $[K_2]$).

The reader may check now that it is also possible to develop a theory of "real closures" of the curve Z along the same lines as is done in $[K_2]$ in the special case $K = \mathbb{R}$, Z affine.

We write down some immediate consequences of Theorem (10.4).

(10.5) Corollary. i) *The map $\langle f \rangle \mapsto 1 - \langle f \rangle$ from the group $Q^+(Z)$ to the additive group $I(Z)_t$ is an isomorphism.*

ii) *If $t = 0$, then $I(Z)_t = I(Z)$ and $I^2(Z) = 0$.*

iii) *Assume $t > 0$. The homomorphism $(\tau_1, \ldots, \tau_t)$ from $W(Z)$ to $\mathbb{Z}^t$ has the kernel $I(Z)_t$. The induced homomorphisms*

$$I^n(Z) \to (2^n \mathbb{Z})^t$$

are surjective for $n = 1$ and bijective for $n \geq 2$. Thus for $n \geq 2$ the group $I^n(Z)$ is torsion free, and $I^n(Z) = 2^{n-1} I(Z)$.

(10.6) Remark. It is also possible now to calculate the Brauer group $\mathrm{Br}(Z)$ of Z (cf. [Gr]), since $\mathrm{Br}(Z)$ injects into the Brauer group $\mathrm{Br}(F)$ of F [Gr, II, Cor. 1.10] and $\mathrm{Br}(F)$ consists entirely of quaternion algebras as a consequence of Tsen's theorem that $\mathrm{Br}(F(\sqrt{-1})) = 0$. The result is as follows: If $t = 0$ then $\mathrm{Br}(Z) = 0$. If $t \geq 1$, then there exist Azumaya algebras $\mathfrak{A}_1, \ldots, \mathfrak{A}_t$ such that the norm form of $\mathfrak{A}_i$ over the generic point of Z is $2 \times \langle 1, -f_i \rangle$. The Brauer group $\mathrm{Br}(Z)$ is the free $\mathbb{Z}/2\mathbb{Z}$-module over the classes $[\mathfrak{A}_1], \ldots, [\mathfrak{A}_t]$ of these algebras.

To finish the calculation of $W(Z)$ we have to determine the order of the group $Q^+(Z)$ of exponent 2, which by Proposition (2.5) is finite. We do this here for $Z = X$. As always we denote the components of γ by $\gamma_1, \ldots, \gamma_r$, if the number r of these components is not zero. $Q(X)$ is generated by $Q^+(X)$ and by the square classes $\langle f_i \rangle$, $1 \leq i \leq r$, introduced above. Thus

$$|Q(X)| = 2^r |Q^+(X)|.$$

Taking into account the exact sequence (2.6) we obtain

(10.7) $|Q^+(X)| = 2^{-r+1} |\text{Pic}(X)_2|,$

with $\text{Pic}(X)_2$ the group of elements of order ≤ 2 in the divisor class group $\text{Pic}(X)$.

In the case $r > 0$ we identified in §2 the group $\text{Pic}_0(X)$ of divisor classes of degree zero, which contains $\text{Pic}(X)_2$, with the group J^G of fixed points of the Jacobian J under the Galois group $G = \{1, \rho\}$ of $K(\sqrt{-1})/K$. Thus in this case $\text{Pic}(X)_2$ coincides with the group $(J_2)^G$ of G-invariant elements of order ≤ 2 in J.

We need a similar interpretation of $\text{Pic}(X)_2$ in the case $r = 0$. We use the notations of §2. As in the case $r > 0$ we see that the canonical maps from $\mathfrak{H}(X)$ to $\mathfrak{H}(\bar{X})^G$ and from $\text{Div}(X)$ to $\text{Div}(\bar{X})^G$ are bijective. Furthermore the G-module $\text{Div}(\bar{X})$ is now induced. Thus we get from the canonical sequence

(*) $1 \to \mathfrak{H}(\bar{X}) \to \text{Div}(\bar{X}) \to \text{Pic}(\bar{X}) \to 1$

an exact sequence

$$1 \to \mathfrak{H}(X) \to \text{Div}(X) \to \text{Pic}(\bar{X})^G \to H^1(\mathfrak{H}(\bar{X})) \to 1$$

hence a canonical exact sequence

$$1 \to \text{Pic}(X) \to \text{Pic}(\bar{X})^G \to H^1(\mathfrak{H}(\bar{X})) \to 1$$

Now it is easily checked that the whole §2 of Geyer's paper $[G_1]$ remains true in our more general setting. {Notice that the central fact, the triviality of the Herbrand quotient of J, remains valid, cf. Th. (4.2).} In particular the sequence (*) induces an isomorphism

$$H^0(\text{Pic}(\bar{X})) \overset{\sim}{\longrightarrow} H^1(\mathfrak{H}(\bar{X}))$$

$[G_1, \text{p. } 90]$. Furthermore $H^1(\mathfrak{H}(\bar{X}))$ has order 2 $[G_1, \text{p. } 89]$. Looking at our exact sequence above starting with $\text{Pic}(X)$ we learn:

(10.8) **Lemma.** *In the case $r = 0$ the canonical map from $\text{Pic}(X)$ to $\text{Pic}(\bar{X})^G$ maps $\text{Pic}(X)$ bijectively onto the norm group $N(\text{Pic}(\bar{X}))$. This norm group has index 2 in $\text{Pic}(\bar{X})^G$.*

In order to relate $\text{Pic}(X)_2$ to $(J_2)^G$ it turns out that we need a precise description of $\text{Pic}(X)/2\,\text{Pic}(X)$, as has been given for $r > 0$ in §5. The degree function on the divisors of X induces in the case $r = 0$ a homomorphism

$$\overline{\text{deg}}: \text{Pic}(X)/2\,\text{Pic}(X) \to 2\mathbb{Z}/4\mathbb{Z}.$$

(10.9) **Theorem.** *Assume $r = 0$. Then $\overline{\text{deg}}$ is an isomorphism from $\text{Pic}(X)/2\,\text{Pic}(X)$ onto $2\mathbb{Z}/4\mathbb{Z}$.*

Proof. The surjectivity is trivial. To prove the injectivity we have to consider a divisor $\mathfrak{a}$ on X of degree divisible by 4 and must show that $\mathfrak{a}$ is linearly equivalent to the square of a divisor on X. Since there exists a divisor of degree 2 on X we may multiply $\mathfrak{a}$ by an even power of this divisor and retreat to the case $\deg(\mathfrak{a}) = 0$. Now by the preceding Lemma (10.8) the divisor $\mathfrak{a}$ is linearly equivalent to the norm $N(\mathfrak{b})$ of a divisor $\mathfrak{b}$ on $\bar{X}$, which clearly again has degree zero. But the Jacobian J is 2-divisible. Thus $\mathfrak{b} \sim \mathfrak{c}^2$ with $\mathfrak{c}$ some divisor on $\bar{X}$, and $\mathfrak{a} \sim N(\mathfrak{c})^2$.   q.e.d.

(10.10) **Proposition.** *The subgroup* $\mathrm{Pic}(X)_2$ *of* J_2^G *coincides with* J_2^G *if* $r > 0$ *and also if* $r = 0$ *and the genus* g *of* X *is even. If* $r = 0$ *and* g *is odd, the group* $\mathrm{Pic}(X)_2$ *has index 2 in* J_2^G.

Proof. We only have to consider the case $r = 0$. According to Lemma (10.8) we have

$$\mathrm{Pic}(\bar{X})^G = \mathrm{Pic}(X) \cup \mathrm{Pic}(X)\alpha$$

with α the class of a divisor $\mathfrak{a}$ on $\bar{X}$ such that $\rho(\mathfrak{a}) \sim \mathfrak{a}$ but $\rho(\mathfrak{a}) \neq \mathfrak{a}$. Thus the index μ of $\mathrm{Pic}(X)_2$ in $\mathrm{Pic}(\bar{X})_2^G = J_2^G$ is at most 2, and $\mu = 2$ if and only if there exists some β in $\mathrm{Pic}(X)$ with $(\alpha\beta^{-1})^2 = 1$, i.e. $\alpha^2 = \beta^2$. From Theorem (10.9) we know that this happens if and only if the degree of α^2 is divisible by 4, which means that the degree of α is even. But according to Geyer [G_1, p. 91]

$$\deg \mathfrak{a} \equiv g - 1 \bmod 2.$$

This proves our proposition.

Thus our calculation of $|\mathrm{Pic}(X)_2|$ boils down to a computation of $|J_2^G|$ also in the case $r = 0$. For any G-module M with finite cohomology we denote the orders of the cohomology groups $H^i(M)$ by $h^i(M)$ ($i = 0, 1$). We have the following general

(10.11) **Proposition.** *Let* A *be an abelian variety defined over* K, *let* s *denote the number* ≥ 0 *with*

$$2^s = h^0(A) = h^1(A)   (\textit{cf. Th. (4.2)}),$$

and let g *denote the dimension of* A. *Then* A *has precisely* 2^{g+s} *real points of order* ≤ 2. *{N.B. We identify* A *with its group of points rational over* $K(\sqrt{-1})$.*}*

The proof will be given below. For $A = J$ we have seen in §4 that $s = r - 1$ in the case $r > 0$. In the case $r = 0$ we have according to Geyer [G_1, p. 92] $s = 0$ if g is even and $s = 1$ if g is odd. Thus we obtain from (10.7), Proposition (10.10), and Proposition (10.11) the following final result:

(10.12) **Theorem.** *The group* $Q^+(X)$ *has order* 2^g *if* γ *is not empty, and order* 2^{g+1} *if* γ *is empty.*

Using Corollary (10.5) we can also state

(10.13) **Corollary.** *If* γ *is empty the Witt ring* $W(X)$ *has cardinality* 2^{g+2}.

It remains to prove Proposition (10.11). Let $A(2)$ denote the 2-primary torsion part of A. Since in $A/A(2)$ unique divisibility by 2 holds true we have natural iso-

morphisms

$$H^i(A(2)) \xrightarrow{\sim} H^i(A) \quad (i=0,1).$$

Let W denote the dyadic Tate group $T_2(A)$ and V denote the extended Tate group $E_2(A)$ [e.g. Lg$_2$, Chap. VII]. V is a vector space of rank $2g$ over the field $\mathbb{Q}_2$ of dyadic numbers, on which G acts, and W is a G-invariant lattice in V of rank $2g$ over the ring $\mathbb{Z}_2$ of integral dyadic numbers. We have an evident exact sequence of G-modules [loc. cit.]

$$0 \to W \to V \to A(2) \to 0.$$

Since V is uniquely divisible by 2 we see that $H^i(W)$ has finite order for both $i=0, 1$, and

$$h^0(W) = h^1(W) = 2^s.$$

W contains the direct sum $W_{1-\sigma} \oplus W_{1+\sigma}$ (notations from §2), and this lattice is a subgroup of finite index in W. Denoting by q the Herbrand quotient h^0/h^1, we thus have

(∗) $1 = q(W) = q(W_{1-\sigma})q(W_{1+\sigma}).$

Denoting the rank of $W_{1-\sigma}$ by g_0 and the rank of $W_{1+\sigma}$ by g_1 we clearly have

$$h^0(W_{1-\sigma}) = (W_{1-\sigma} : 2W_{1-\sigma}) = 2^{g_0},$$
$$h^1(W_{1+\sigma}) = (W_{1+\sigma} : 2W_{1+\sigma}) = 2^{g_1},$$
$$h^1(W_{1-\sigma}) = h^0(W_{1+\sigma}) = 0.$$

Thus we deduce from (∗) that $g_0 = g_1$. Since $g_0 + g_1 = 2g$ we see that $W_{1-\sigma}$ and $W_{1+\sigma}$ both have rank g.

Remark. Thus the eigenvalues ± 1 of ρ on the vector space $V = E_2(A)$ both have the same multiplicity g. This is just another way to state Geyer's Theorem 4.2.

It is now possible by the same arguments as in [G$_1$, § 1] to find bases $r_1, \ldots, r_g$ of $V_{1-\sigma}$ and $i_1, \ldots, i_g$ of $V_{1+\sigma}$ over $\mathbb{Q}_2$ such that

$$r_1, \ldots, r_s, \quad r_{s+1}, \ldots, r_g$$

$$i_1, \ldots, i_s, \quad i_{s+1} + \frac{r_{s+1}}{2}, \ldots, i_g + \frac{r_g}{2}$$

is a basis of W over $\mathbb{Z}_2$. From this basis we immediately read off that $W/2W$ contains precisely 2^{g+s} elements invariant under G. Now by the sequence

$$0 \to W \to V \to A(2) \to 0$$

we have a natural isomorphism from $2^{-1}W/W$ onto A_2 compatible with the actions of G. Thus also A_2 contains precisely 2^{g+s} elements invariant under G. This completes the proof of Proposition (10.11) and of Theorem (10.12).

In the case $K = \mathbb{R}$, $r > 0$, Theorem (10.12) had been proved before by Alling [Al, Th. 5.9] using analytic techniques.

§ 11. Witt Rings of Function Fields

We shall give a description of the Witt ring $W(F)$ by inserting $W(F)$ into an exact sequence all whose other terms are explicitly known. This sequence will neglect the multiplicative structure of $W(F)$. To remedy this a little we shall also write down exact sequences for the powers of the fundamental ideal $I(F)$. Similar exact sequences are known for the rational function field in one variable over an arbitrary field [L, p. 265 and p. 270] and for arbitrary function fields in one variable over a finite field (cf. the computations [KS]).

We first consider the case that γ is not empty and as always denote the components of γ by $\gamma_1, \ldots, \gamma_r$. The most natural idea seems to be to study the sequence

$$(11.1) \quad 0 \to W(X) \to W(F) \xrightarrow{\partial} \mathbf{Z}^{(\gamma)} \times (\mathbf{Z}/2\,\mathbf{Z})^{(X \smallsetminus \gamma)} \xrightarrow{\sigma} \mathbf{Z}^r \to 0$$

with the following notations. $\mathbf{Z}^{(\gamma)}$ is the free $\mathbf{Z}$-module over γ, and $(\mathbf{Z}/2\,\mathbf{Z})^{(X \smallsetminus \gamma)}$ is the free $(\mathbf{Z}/2\,\mathbf{Z})$-module over the set $X \smallsetminus \gamma$ of complex points of X. We think of the elements of $\mathbf{Z}^{(\gamma)} \times (\mathbf{Z}/2\,\mathbf{Z})^{(X \smallsetminus \gamma)}$ as families $(n_\mathfrak{p} \mid \mathfrak{p} \in X)$ with $n_\mathfrak{p}$ in $\mathbf{Z}$ for $\mathfrak{p}$ real and in $\mathbf{Z}/2\,\mathbf{Z}$ for $\mathfrak{p}$ complex, and with almost all $n_\mathfrak{p} = 0$. The map from $W(X)$ to $W(F)$ is the canonical map. ∂ assigns to every ξ in $W(F)$ the family $(\partial_\mathfrak{p}(\xi) \mid \mathfrak{p} \in X)$. Finally σ assigns to a family $(n_\mathfrak{p} \mid \mathfrak{p} \in X)$ in case $r > 0$ the r-tupel $(n_1, \ldots, n_r)$ with

$$n_i = \sum_{P \in \gamma_i} n_P.$$

In case $r = 0$ we read $\mathbf{Z}^{(\gamma)} = \mathbf{Z}^r = 0$. We know already that this sequence (10.1) is exact at the places $W(X)$ and $W(F)$ (Prop. 10.2 and 10.3). It clearly is also exact at the last place $\mathbf{Z}^r$. According to the sum formula (5.6) we have $\sigma \circ \partial = 0$.

We also know from Corollary (10.5) for every Zariski open subset Z of X that $I^n(Z) = 2^{n-1} I(Z)$ for $n \geq 2$. Since $W(F)$ is the union and direct limit of the subrings $W(Z)$ this implies $I^n(F) = 2^{n-1} I(F)$. {This follows also from Lemma (2.11).} Thus ∂ maps $I^n(F)$ into the subgroup $(2^{n-1} \mathbf{Z})^{(\gamma)}$ of $\mathbf{Z}^{(\gamma)} \times (\mathbf{Z}/2\,\mathbf{Z})^{(X \smallsetminus \gamma)}$, cf. also [MH, p. 86].

(11.2) Theorem $(r > 0)$. *The sequence* (11.1) *is exact. The following sequences* S_n, $n \geq 1$, *induced by* (11.1) *are also exact:*

$$S_1: 0 \to I(X) \to I(F) \xrightarrow{\partial} \mathbf{Z}^{(\gamma)} \times (\mathbf{Z}/2\,\mathbf{Z})^{(X \smallsetminus \gamma)}$$
$$\longrightarrow \mathbf{Z}^r \to 0.$$

$n \geq 2$:

$$S_n: 0 \to I^n(X) \to I^n(F) \xrightarrow{\partial} (2^{n-1} \mathbf{Z})^{(\gamma)} \xrightarrow{\partial} (2^{n-1} \mathbf{Z})^r \to 0.$$

N.B. An explicit description of $W(X)$ and the powers $I^n(X)$ has been given in § 10 (Th. (10.4), Cor. (10.5), Th. (10.12)).

We know from Corollary (10.5) for every Zariski open subset Z of X that $I^2(Z)$ is torsion free and $I^n(Z) = 2^{n-2} I^2(Z)$ for $n \geq 3$. Thus also $I^2(F)$ is torsion free and $I^n(F) = 2^{n-2} I^2(F)$, and we observe that the exactness of the sequence S_n for $n \geq 3$ is an immediate consequence of the exactness of S_2. We further observe that the exactness of (11.1) immediately follows from the exactness of S_1, since $W(X)$ is additively generated by $I(X)$ and the element $\langle 1 \rangle$, and $W(F)$ is additively generated by $I(F)$ and $\langle 1 \rangle$.

Thus it suffices to prove the exactness of the complexes S_1 and S_2. We first consider S_2. The exactness at $I^2(F)$ means

(11.3) $I^2(F) \cap I(X) = I^2(X)$,

since we already know that S_1 is exact at $I(F)$. Now $I^2(F)$ is the set of all elements ξ of $I(F)$ with $d(\xi) = 1$ [L, p. 39], and we have no difficulty to conclude from Theorem (10.4) that $I^2(X)$ is the set of all elements ξ of $I(X)$ with $d(\xi) = 1$. Thus (11.3) is evident, and S_2 is exact at $I^2(X)$. The only place where the exactness of S_2 now is not yet clear is the third one. The kernel of σ on $(2\mathbf{Z})^{(\gamma)}$ is generated by the elements $\varepsilon(P_1, P_2)$ which have coordinate $+2$ at a point P_1, -2 at a point P_2, and zero at all other points, and with P_1 and P_2 lying on the same component of γ. We choose an interval function f for (P_2, P_1). The quadratic form $2 \times \langle 1, -f \rangle$ then maps under ∂ onto $\varepsilon(P_1, P_2)$ and lies in $I^2(F)$. This finishes the proof of the exactness of S_2.

The complex S_2 injects into S_1. To prove the exactness of S_1 it suffices to show that the cokernel complex S_1/S_2 is exact. Now the signed determinant d induces an isomorphism from the group $I(F)/I^2(F)$ onto the group $Q(F)$ of square classes [loc. cit.]. Furthermore d maps $I(X)$ onto the group $Q(X)$ defined in §2, as follows again from Theorem 10.5. {A more intrinsic proof is easily obtained from the description of the signed determinant on $W(X)$ by associating to a space (E, B) of rank n over X the n-th exterior power of E, cf. [K, §4].} By (11.3) d induces an isomorphism from $I(X)/I^2(X)$ onto $Q(X)$. Therefore S_2/S_1 is isomorphic to the complex

$$0 \to Q(X) \to Q(F) \xrightarrow{\bar{\partial}} (\mathbf{Z}/2\mathbf{Z})^{(X)} \xrightarrow{\bar{\sigma}} (\mathbf{Z}/2\mathbf{Z})^r \to 0$$

with the following notations: $Q(X) \to Q(F)$ is the inclusion map, $\bar{\partial}$ associates to a square class $\langle \bar{f} \rangle$ the element

$$(\text{ord}_{\mathfrak{p}}(f) \bmod 2 \mid \mathfrak{p} \in X),$$

$\bar{\sigma}$ means summation over the coordinates at the points in γ_i for $1 \leq i \leq r$.

The exactness of this complex is non trivial only at the third place. Let $(\varepsilon_{\mathfrak{p}} \mid \mathfrak{p} \in X)$ be a family with all $\varepsilon_{\mathfrak{p}} = 0$ or $= 1$, almost all $\varepsilon_{\mathfrak{p}} = 0$, and

$$\sum_{P \in \gamma_i} \varepsilon_P \equiv 0 \bmod 2$$

for $1 \leq i \leq r$. By Theorem (5.1) there exists a real function $f \neq 0$ and a divisor $\mathfrak{a}$ on X such that

$$\text{div}(f) = \mathfrak{a}^2 \cdot \prod_{\mathfrak{p} \in X} \mathfrak{p}^{\varepsilon_{\mathfrak{p}}}.$$

The square class $\langle f \rangle$ has under $\bar{\partial}$ the image $(\varepsilon_{\mathfrak{p}} \mid \mathfrak{p} \in X)$. This finishes the proof of the exactness of S_1, and of Theorem (11.2).

The case $r = 0$ is easier. We consider the sequence

(11.4) $0 \to W(X) \to W(F) \xrightarrow{\partial} (\mathbf{Z}/2\mathbf{Z})^{(X)} \xrightarrow{\sigma} \mathbf{Z}/2\mathbf{Z} \to 0$,

the first two maps being defined in the same way as in the case $r > 0$ and σ denoting summation over all coordinates.

(11.5) **Theorem.** *The sequence* (11.4) *and the induced sequence*

$$0 \to I(X) \to I(F) \xrightarrow{\partial} (\mathbb{Z}/2\mathbb{Z})^{(X)} \xrightarrow{\sigma} \mathbb{Z}/2\mathbb{Z} \to 0$$

both are exact $(r=0)$.

Proof. Again the exactness of one of these sequences implies the exactness of the other one. Thus we only study the sequence starting with $I(X)$. Now according to Corrollary (9.5) or Corollary (10.5) we have $I^2(F)=0$ and $I^2(X)=0$. Thus we can identify $I(F)$ with $Q(F)$ and $I(X)$ with $Q(X)$ by use of the signed determinant. Our sequence then reads

$$0 \to Q(X) \to Q(F) \xrightarrow{\bar{\partial}} (Z/2\mathbb{Z})^{(X)} \xrightarrow{\sigma} (Z/2\mathbb{Z}) \to 0$$

with $\bar{\partial}$ having the same meaning as in the case $r>0$. We verify the exactness of this sequence in the same way as for the analogous sequence in the case $r>0$, using Theorem (10.9) instead of (5.1).   q.e.d.

In the case $r>0$ we can replace (11.1) by an exact sequence which is nearly a presentation of $W(F)$ as a direct sum with elementary summands. We choose on each component γ_i a point P_i and denote the set consisting of these r points by S. We introduce the homomorphism

$$\alpha: Q^+(X) \to W(F)$$

mapping a square class $\langle f \rangle$ in $Q^+(X)$ onto $1 - \langle f \rangle$, further the homomorphism

$$\beta: W(F) \to \mathbb{Z}^{(\gamma)} \times (Z/2\mathbb{Z})^{(X \smallsetminus \gamma)}$$

with component $\partial_\mathfrak{p}$ at every $\mathfrak{p}$ in $X \smallsetminus S$ and component $\partial_P + \tau_P$ (a ring homomorphism!) at every P in S.

(11.6) **Theorem.** *The sequence*

$$0 \to Q^+(X) \xrightarrow{\alpha} W(F) \xrightarrow{\beta} \mathbb{Z}^{(\gamma)} \times (\mathbb{Z}/2\mathbb{Z})^{(X \smallsetminus \gamma)} \to 0$$

is exact $(r>0)$.

This follows easily from the exactness of these sequence (111) and the description of $W(X)$ in Theorem (10.4) and Corollary (10.5). Details are left to the reader. As shown in §10 the group $Q^+(X)$ has order 2^s (Th. (10.12)).

References

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

AL.   Alling, N.L.: Analytic geometry on real algebraic curves. Math. Ann. **207**, 23–46 (1974)

ELP.   Elman, R., Lam, T.Y., Prestel, A.: On some Hasse principles over formally real fields. Math. Z. **134**, 291–301 (1973)

G_1.   Geyer, W.D.: Ein algebraischer Beweis des Satzes von Weichold über reelle algebraische Funktionenkörper. In: Algebraische Zahlentheorie (Oberwolfach 1964), pp. 83–98. Mannheim: Bibliographisches Institut 1967

Gr.   Grothendieck, A.: Le groupe de Brauer I, II. In: Séminaire Bombaki. 1964/65 fasc. 3. Exposé 290. Paris: Secrétariat mathematique 1966 and Seminaire Bombaki 1965/1966. Exposé 297. New York-Amsterdam: Benjamin 1966

K.   Knebusch, M.: Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinear-
         formen. S.-ber. Heidelberg. Akad. Wiss. math.-naturw. Kl. 1969/70, 3. Abhdl., 96 pp. (1970)
K_2.   Knebusch, M.: Real closures of commutative rings, I: J. reine angew. Math. 274/275, 61–89
         (1975), II: J. reine angew. Math., to appear
K_3.   Knebusch, M.: On algebraic curves over real closed fields, I. Math. Z. **150**, 49–70 (1976)
KS.   Knebusch, M., Scharlau, W.: Quadratische Formen und quadratische Reziprozitätsgesetze
         über algebraischen Zahlkörpern. Math. Z. **121**, 346–368 (1971)
L.   Lam, T. Y.: The algebraic theory of quadratic forms. Reading: Benjamin 1973
Lg_2. Lang, S.: Abelian varieties. New York: Interscience 1959
MH.   Milnor, J., Husemoller, D.: Symmetric bilinear forms. New York-Heidelberg-Berlin: Springer
         1973
W_1.   Witt, E.: Theorie der quadratischen Formen in beliebigen Körpern. J. reine angew. Math. **176**,
         31–44 (1937)