[3] F. Hirzebruch, *Über vierdimensionale Riemannsche Flächen mehrdeutiger analytischer Funktionen von zwei komplexen Veränderlichen*, Math. Ann. 126 (1953), pp. 1–22.

[4] — *The Hilbert modular group, resolution of the singularities at the cusps and related problems*, Sem. Bourbaki # 396 (1971/2), pp. 1–14.

[5] C. L. Siegel, *Einführung in die Theorie der Modulfunktionen n-ten Grades*, Math. Ann. 116 (1939), pp. 617–657.

[6] — *Symplectic geometry*, Amer. Journ. Math. 65 (1943), pp. 1–86.

[7] — *Geometry of Numbers*, Lecture notes by B. Friedman, New York University, 1945.

MATHEMATICS DEPARTMENT
CITY COLLEGE OF NEW YORK
New York, N. Y.

Received on 18. 10. 1972 (338)

ACTA ARITHMETICA
XXIV (1973)

Specialization of quadratic and symmetric bilinear forms, and a norm theorem

by

MANFRED KNEBUSCH (Saarbrücken)

Dedicated to Carl Ludwig Siegel on his 75 birthday

Introduction. In the first part of this paper (§ 1–§ 3) we study the specialization of a symmetric bilinear or quadratic form over a field K with respect to a place $\lambda: K \to L \cup \infty$, provided the form has "good reduction". We have to distinguish between symmetric bilinear and quadratic forms since we do not exclude fields of characteristic 2. A typical result obtained by this theory is the following: We denote a symmetric bilinear form by the corresponding symmetric matrix of its coefficients. Let $k(t)$ be the field of rational functions in independent variables $t_1, \ldots, t_r$ over a field k. Consider symmetric bilinear forms $(f_{ij}(t))$, $(g_{kl}(t))$ over $k(t)$ whose coefficients $f_{ij}(t)$, $g_{kl}(t)$ are polynomials. Assume that the form $(g_{kl}(t))$ is represented by $(f_{ij}(t))$. Assume further that c is an r-tupel in k^r such that the form $(f_{ij}(c))$ over k is non singular. If $\operatorname{char} k \neq 2$ the following holds true:

(i) If also $(g_{kl}(c))$ is non singular, then this form is represented by $(f_{ij}(c))$ over k (see § 2).

(ii) If $(g_{kl}(t))$ is a diagonal matrix with m rows and columns and if c is a non singular zero of each polynomial $g_{kk}(t)$, then the form $(f_{ij}(c))$ has Witt index $\geqslant m/2$ if m is even and $\geqslant (m+1)/2$ if m is odd (see § 3).

The assertion (i) may be considered as a generalization of the principle of substitution of Cassels and Pfister ([15], p. 365; [10], p. 20). At the end of Section 3 (Proposition 3.6) we shall also generalize the subform theorem of Cassels and Pfister ([15], p. 366; [10], p. 20).

Using the result quoted above and a similar result for $\operatorname{char} k = 2$ we prove in the last section § 4 a theorem about the polynomials in $k[t]$ which can occur as norms of similarity over $k(t)$ for a fixed symmetric bilinear form defined over k. Special cases of this norm theorem have been used in a crucial way by Arason and Pfister in [1] and by Elman and Lam in [5].

In general our results about quadratic forms are much less complete than those about bilinear forms.

Although the language of forms is quite natural to describe the main results of this paper, we use in the body of the paper the geometric language of quadratic and bilinear spaces, since the geometric language seems to be more suitable to understand the proofs.

The theory developed here will be applied in a subsequent paper about the behavior of quadratic forms in transcendental field extensions [9].

§ 1. Preliminaries about bilinear and quadratic spaces. We recall some standard notations and well-known facts about symmetric bilinear and quadratic forms over a (not necessarily noetherian) local ring A. For proofs of statements given here without further reference and moreover for the basic theory over arbitrary commutative rings the reader may consult Chapter V of [3], [13], [7] and § 1 of [8]. In the present paper essentially only the case that A is a field or a valuation ring will play a rôle.

A free (symmetric) *bilinear module* (E, B) over A is a finitely generated free A-module E equipped with a symmetric bilinear form $B: E \times E \to A$. We often denote (E, B) by a symmetric matrix (a_{ij}) with $a_{ij} = B(x_i, x_j)$ for some basis $x_1, \ldots, x_n$ of E over A. We say that (E, B) — or B — is *non singular*, or that (E, B) is a *bilinear space*, if $\det(a_{ij})$ lies in the unit group A^* of A, i.e. if $x \mapsto B(-, x)$ is a bijection from E to the dual module $\mathrm{Hom}_A(E, A)$. A free *quadratic module* (E, q) over A is a finitely generated free A-module E equipped with a quadratic form q, i.e. with a mapping $q: E \to A$ such that $q(cx) = c^2 q(x)$ and $B(x, y) := q(x+y) - q(x) - q(y)$ is bilinear in x and y, for c in A, x and y in E. We say that (E, q) — or q — is *non singular* or that (E, q) is a *quadratic space* if the associated bilinear form B is non singular. A quadratic module (E, q) will often be denoted by a symmetric matrix $[a_{ij}]$ in square bracket with $a_{ii} = q(x_i)$, $a_{ij} = B(x_i, x_j)$ if $i \neq j$, for some basis $x_1, \ldots, x_n$ of E. If 2 is a unit in A there is no essential difference between quadratic and bilinear modules, since then any bilinear form B corresponds to a unique quadratic form $q(x) = \frac{1}{2}B(x, x)$.

For a free quadratic module we always denote the quadratic form by the letter q and the associated bilinear form by B as far as no confusion is possible, and we often write E instead of (E, q). Similarly we denote the bilinear form of a free bilinear module usually by the letter B, and we often write E instead of (E, B). If we use the word "space" without further specification we regard bilinear and quadratic spaces at the same time. The rank of a free finitely generated A-module V will be denoted by $\dim V$.

Let $\varphi: A \to A'$ be a homomorphism between (local) rings (of course $\varphi(1) = 1$). For any free bilinear or quadratic module E we denote by $\varphi_*(E)$ the A'-module $E \otimes_\varphi A'$ equipped with the bilinear resp. quadratic form which is deduced from the form on E by base extension ([4], § 1 no 4, § 3 no 4). We often write $E \otimes_A A'$ or $E \otimes A'$ instead of $\varphi_*(E)$ if it is clear which map φ is considered.

Let E be a free quadratic or bilinear module over A. We call a submodule V of the A-module E a *direct submodule* if $E = V \oplus W$ with some other submodule W ($\oplus$ means the module sum, without regarding forms). If A is a valuation ring then for any submodule V of E the module $V^\perp$ consisting of all x in E such that $B(V, x) = 0$ is a direct submodule, for $E/V^\perp$ is torsion free and finitely generated and hence free.

We call the bilinear or quadratic module E *isotropic* if E has a direct submodule $V \neq 0$ which is *totally isotropic*, i.e. $q(V) = 0$ in the quadratic case and $B(V \times V) = 0$ in the bilinear case. If E is not isotropic, we say E is *anisotropic*. Notice that if A is a field any anisotropic bilinear module over A must be a space, but that in case $\mathrm{char} A = 2$ there exist anisotropic quadratic modules which are not spaces.

A quadratic space E over A is called *hyperbolic*, if E contains a totally isotropic direct submodule V such that $V^\perp = V$. Then E is isomorphic to the orthogonal sum $t \times H$ of $t = \frac{1}{2}\dim E$ copies of the *hyperbolic plane* $H = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Similarly a bilinear space E is called *metabolic*, if E contains a direct submodule $V = V^\perp$. A metabolic bilinear space is isomorphic to the orthogonal sum of spaces $\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$ with some a in A.

Every quadratic resp. bilinear space E has an orthogonal decomposition

$$(*) \qquad E = E_0 \perp M$$

with E_0 anisotropic and M hyperbolic resp. metabolic. Now in the quadratic case Witt's cancellation law is true, since A is local [6], i.e.

$$(1.0) \qquad F_1 \perp G \cong F_2 \perp G \Rightarrow F_1 \cong F_2$$

for quadratic spaces F_1, F_2, G over A ("$\cong$" means "isomorphic"). Furthermore $M \cong t \times H$ with some $t > 0$. Thus in the decomposition $(*)$ the number $t = \frac{1}{2}\dim M$ and up to isomorphism the space E_0 are uniquely determined by E. We call t the *index* of E and E_0 a *kernel space* of E and write $t = \mathrm{ind} E$, $E_0 = \mathrm{Ker}(E)$. If A is a *field* of char 2 then in the bilinear case the cancellation law fails, but the space E_0 in $(*)$ is up to isomorphism still uniquely determined by E ([7], § 8.2, [11]). We again call E_0 a kernel space of E and $t := \frac{1}{2}\dim M$ the index of E and write $E_0 = \mathrm{Ker}(E)$, $t = \mathrm{ind} E$.

We call two bilinear resp. quadratic spaces E and F over A *equivalent*, and write $E \sim F$, if there exist metabolic resp. hyperbolic spaces M and N such that $E \perp M \cong F \perp N$. If well-defined kernel spaces exist, this means $\mathrm{Ker}(E) \cong \mathrm{Ker}(F)$. The equivalence class of a space E will be denoted by $\{E\}$. For any space E we denote by $-E$ the module E equipped with the form $-B$ resp. $-q$, where B resp. q denotes the form of the original space. The space $E \perp (-E)$ is always metabolic resp. hyperbolic. Thus the equivalence classes of bilinear or quadratic spaces form an abelian group under the addition $\{E\} + \{F\} = \{E \perp F\}$, and the inverse of a class $\{E\}$ is $\{-E\}$. This group is called the *Witt group* $W(A)$ of bilinear spaces resp. the Witt group $Wq(A)$ of quadratic spaces over A. In fact, $W(A)$ is even a commutative ring under the multiplication $\{E\} \cdot \{F\} = \{E \otimes F\}$. Here $E \otimes F$ denotes the tensor product of the A-modules E and F equipped with the tensor product of the bilinear forms of E and F ([4], § 1 no 9). (Furthermore $Wq(A)$ is a $W(A)$-module; we shall not need this fact.) Clearly a ring homomorphism $\varphi\colon A \to A'$ (with $\varphi(1) = 1$ of course) induces homomorphisms $W(\varphi)\colon W(A) \to W(A')$ and $Wq(\varphi)\colon Wq(A) \to Wq(A')$ which map the class $\{E\}$ of a space E to the class $\{\varphi_*(E)\}$.

We now give a description of the ring $W(A)$ by generators and relations. Any bilinear space E over A which contains an element x with $B(x, x)$ in A^* has an orthogonal basis, i.e.

$$E \cong (a_1) \perp \ldots \perp (a_n)$$

with some a_i in A^*. As usual we denote the right hand side also by $(a_1, \ldots, a_n)$. Notice that if 2 is a unit of A every bilinear space $E \neq 0$ contains some x with $B(x, x)$ in A^*. Anyway for an arbitrary local ring A the ring $W(A)$ is additively generated by the classes $\{(a)\}$ of spaces of rank one. We write $\{a\}$ instead of $\{(a)\}$. Let G denote the group A^*/A^{*2} of square classes $\langle a \rangle = aA^{*2}$. We have a ring homomorphism Φ from the group ring $\mathbb{Z}[G]$ onto $W(A)$ mapping $\langle a \rangle$ to $\{a\}$. Let $\mathfrak{m}$ denote the maximal ideal of A. The following well known theorem will be used in this paper only for $\mathfrak{m} = 0$.

Theorem 1.1 ([19], Satz 7, [7], § 5, [8], § 1). *Assume $A/\mathfrak{m}$ contains more than two elements. Then the kernel of Φ is additively generated by the elements $\langle a \rangle + \langle -a \rangle$ and the elements $\langle a_1 \rangle + \langle a_2 \rangle - \langle b_1 \rangle - \langle b_2 \rangle$ such that $(a_1, a_2) \cong (b_1, b_2)$, which is the case if and only if $\langle a_1 a_2 \rangle = \langle b_1 b_2 \rangle$ and $b_1 = c^2 a_1 + d^2 a_2$ with c and d in A.*

We close this section with some remarks on quadratic modules. The following generalization of Witt's cancellation theorem is an immediate consequence of Satz 0.1 in [6].

Proposition 1.2. *Let M and N be free quadratic modules over a local ring A and let G be a quadratic space over A. If $G \perp N$ represents $G \perp M$ then N represents M.*

For any quadratic module E over a field K we call the submodule consisting of all x in E with $B(x, E) = 0$ the *quasilinear part* of E. We say that E is *non degenerate* if the quasilinear part of E is anisotropic (in difference to the terminology in [6]). Notice that in the case $\mathrm{char}\, K \neq 2$ the quasilinear part of a non degenerate module E must be zero and thus E must be a space. Any non degenerate quadratic module E over K has a decomposition

$$E \cong r \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \perp E_0$$

with some $r \geqslant 0$ and E_0 anisotropic (cf. [2], p. 160). By Proposition 1.2 the number r and up to isomorphy the quadratic module E_0 are uniquely determined by E ([2]). We call r the index of E and E_0 a kernel module of E. Any maximal totally isotropic submodule V of E has rank r. Indeed, V has intersection zero with the quasilinear part R of E. Thus $E = R \oplus \oplus V \oplus W$ with some other module W. The module $U = V \oplus W$ must be a space. Thus V is contained in a hyperbolic space $M \subset U$ of rank $2\dim V$ (e.g. [7], Satz 3.2.1). We have $E = M \perp M^\perp$ and $M^\perp$ must be anisotropic due to the maximality of V.

§ 2. Good reduction of spaces. We consider a fixed place $\lambda\colon K \to L \cup \infty$ with K and L fields of arbitrary characteristic. We denote by $\mathfrak{o}$ the valuation ring of λ, by $\mathfrak{m}$ the maximal ideal of $\mathfrak{o}$ and by μ the restriction $\mathfrak{o} \to L$ of λ.

Lemma 2.1. *Assume M_1 and M_2 are (quadratic or bilinear) spaces over $\mathfrak{o}$ such that $M_1 \otimes_{\mathfrak{o}} K \cong M_2 \otimes_{\mathfrak{o}} K$. Then $M_1 \sim M_2$. In the quadratic case even $M_1 \cong M_2$.*

If $\mathrm{char}\, L \neq 2$ there is of course no distinction between the quadratic and the bilinear case.

Proof of Lemma 2.1. Since $\mathfrak{o}$ is a Prüfer ring the maps $Wq(\mathfrak{o}) \to Wq(K)$ and $W(\mathfrak{o}) \to W(K)$ induced by the inclusion $\mathfrak{o} \to K$ are injective. This is proved in [7], § 11, or [13], p. 93, in the bilinear case. (In [13] only Dedekind rings are considered, but the proof holds for Prüfer rings.) The quadratic case can be settled in the same way. Thus $M_1 \sim M_2$. Since M_1 and M_2 have the same rank we obtain in the quadratic case $M_1 \cong M_2$ (see § 1). q.e.d.

We say that a quadratic or bilinear space E over K has *good reduction* with respect to λ, if E contains a quadratic resp. bilinear space over $\mathfrak{o}$ of full rank, in other words, if $E \cong M \otimes_{\mathfrak{o}} K$ with some space M over $\mathfrak{o}$. By Lemma 2.1 the space $\mu_*(M)$ is up to Witt-equivalence uniquely determined by E. We denote the class $\{\mu_*(M)\}$ in $W(L)$ by $\lambda_*\{E\}$. It clearly depends only of the class $\{E\}$ in $W(K)$. In the quadratic case by Lemma 2.1 even the space $\mu_*(M)$ over L is up to isomorphism uniquely determined

by E, and will be denoted by $\lambda_*(E)$. We call $\lambda_*(E)$ the *reduction* or *specialization* of E with respect to λ. Assume now that $\operatorname{char} L = 2$ and E is bilinear. We say that E has *very good reduction*, if E contains a bilinear space M over $\mathfrak{o}$ of full rank such that the space $M/\mathfrak{m}M = M \otimes \mathfrak{o}/\mathfrak{m}$ over $\mathfrak{o}/\mathfrak{m}$ is anisotropic. Then for any other space M' over $\mathfrak{o}$ of full rank contained in E we obtain from $M'/\mathfrak{m}M' \sim M/\mathfrak{m}M$ that $M/\mathfrak{m}M$ is isomorphic to a kernel space of $M'/\mathfrak{m}M'$ (see § 1) and thus $M'/\mathfrak{m}M' \cong M/\mathfrak{m}M$, since the ranks are equal. Thus also $M'/\mathfrak{m}M'$ is anisotropic and $\mu_*(M) \cong \mu_*(M')$. We again call $\mu_*(M)$ the reduction or specialization $\lambda_*(E)$ of E.

The later Example 2.6 (i) shows that in the bilinear case with $\operatorname{char} L = 2$ "good reduction" is not enough to ensure the uniqueness of $\lambda_*(E)$.

PROPOSITION 2.2. *Let $E = F \perp G$ be an orthogonal decomposition of a space E over K.*

(i) *If E and F have good reduction, then also G has good reduction and*

$$\lambda_*\{E\} = \lambda_*\{F\} + \lambda_*\{G\}.$$

In the quadratic case even

$$\lambda_*(E) \cong \lambda_*(F) \perp \lambda_*(G).$$

(ii) *Assume E is bilinear and* $\operatorname{char} L = 2$. *If E has very good reduction and F has good reduction, then F and G both have very good reduction and again*

$$\lambda_*(E) \cong \lambda_*(F) \perp \lambda_*(G).$$

Remark. We shall see in § 3 (Proposition 3.2) that in assertion (ii) the assumption that F has good reduction can be dropped.

Proof. We chose a decomposition $G = G_0 \perp G_1$ with G_0 anisotropic and G_1 hyperbolic resp. metabolic. It is easy to find a space R_1 over $\mathfrak{o}$ of full rank in G_1. It remains to find such a space in G_0. Clearly G_0 is a kernel space of $E \perp (-F)$. We chose spaces M, N over $\mathfrak{o}$ of full rank in E and F. We further chose a decomposition $M \perp (-N) \cong R_0 \perp S$ into an anisotropic space R_0 and a hyperbolic resp. metabolic space S. The space $R_0 \otimes_{\mathfrak{o}} K$ is again anisotropic (see [7], § 11.1), hence

$$R_0 \otimes_{\mathfrak{o}} K \cong \operatorname{Ker}\big(E \perp (-F)\big) \cong G_0,$$

and $G \cong R \otimes_{\mathfrak{o}} K$ with $R := R_0 \perp R_1$. We see that G has good reduction, and obtain from $E \cong (N \perp R) \otimes_{\mathfrak{o}} K$, that $\lambda_*\{E\} = \lambda_*\{F\} + \lambda_*\{G\}$ and in the quadratic case $\lambda_*(E) \cong \lambda_*(F) \perp \lambda_*(G)$.

Assume now that $\operatorname{char} L = 2$ and E is a bilinear space with very good reduction. Then $N/\mathfrak{m}N \perp R/\mathfrak{m}R$ is anisotropic. Thus both summands are anisotropic and assertion (ii) follows. q.e.d.

If M and N are quadratic or bilinear free modules over a local ring A, we say that M is *represented* by N and write $M < N$, if N contains a direct submodule $M' \cong M$ (isomorphism respecting the forms). If M is a space this implies $N \cong M \perp T$ with a suitable quadratic resp. bilinear module T. Of course if N and M are both spaces also T is a space. Up to the last part of this section we shall only deal with representations of spaces by spaces.

COROLLARY 2.3. *Assume A is a regular local ring with quotient field K and maximal ideal $\mathfrak{M}$ and that M and N are spaces over A.*

(i) *In the quadratic case $M \otimes_A K < N \otimes_A K$ implies $M/\mathfrak{M}M < N/\mathfrak{M}N$.*

(ii) *If $2 \in \mathfrak{M}$ the same holds true in the bilinear case, if in addition $N/\mathfrak{M}N$ is anisotropic.*

Proof. It is easy to construct a place $\lambda: K \to A/\mathfrak{M} \cup \infty$ which on A coincides with the evident map $A \to A/\mathfrak{M}$. In fact, let $t_1, \ldots, t_r$ denote a regular system of parameters of A. We show the existence of λ by induction on r. If $r = 1$ take the canonical place associated with the valuation ring A. Assume now $r > 1$ and let $\mathfrak{p}$ denote the prime ideal At_r. Clearly $A_{\mathfrak{p}}$ is a valuation ring and $L := A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ may be regarded as the quotient field of the ring $A/\mathfrak{p}$, which is again regular. By induction hypothesis there is a place $\alpha: L \to A/\mathfrak{M} \cup \infty$ which coincides on $A/\mathfrak{p}$ with the evident map from $A/\mathfrak{p}$ to $A/\mathfrak{M}$. Let $\beta: K \to L \cup \infty$ denote the canonical place associated with $A_{\mathfrak{p}}$. The place $\lambda = \alpha \circ \beta$ fullfills our requirements.

We now obtain the assertions of Corollary 2.3 applying Proposition 2.2 with $E := N \otimes_A K$, $F := M \otimes_A K$ and G a space over K such that $E \cong F \perp G$. q.e.d.

Remarks 2.4. (a) If in part (ii) of Corollary 2.3 we do not assume that $N/\mathfrak{M}N$ is anisotropic, then it still can be shown that $M/\mathfrak{M}M$ is "stably represented" by $N/\mathfrak{M}N$, i.e. $M/\mathfrak{M}M \perp S$ is represented by $N/\mathfrak{M}N \perp S$ for some space S over $A/\mathfrak{M}$.

(b) It is unknown whether for a regular local ring A with quotient field K the canonical maps $W(A) \to W(K)$ and $Wq(A) \to Wq(K)$ are injective. Corollary 2.3 gives a small hint that this might be true.

As a special case of Corollary 2.3 we obtain

COROLLARY 2.5 (Principle of substitution). *Let $(f_{ij}(t))_{1 \leqslant i,j \leqslant n}$ and $(g_{kl}(t))_{1 \leqslant k,l \leqslant m}$ be symmetric matrices of polynomials in an arbitrary number r of variables $t = (t_1, \ldots, t_r)$ over an arbitrary field k. Let further $c = (c_1, \ldots, c_r)$ be an r-tuple with coordinates c_i in a field extension L of k.*

(i) *If the quadratic modules $[g_{kl}(c)]$ and $[f_{ij}(c)]$ over L are nonsingular and if the module $[g_{kl}(t)]$ over $k(t)$ is represented by $[f_{ij}(t)]$, then $[g_{kl}(c)]$ is represented by $[f_{ij}(c)]$.*

(ii) *The analogous statement holds for the bilinear modules $(g_{kl}(t))$, $(f_{ij}(t))$, $(g_{kl}(c))$, $(f_{ij}(c))$ if we assume in the case $\operatorname{char} k = 2$ in addition that $(f_{ij}(c))$ is anisotropic.*

Proof. $[g_{kl}(t)]$ resp. $(g_{kl}(t))$ is a fortiori represented by $[f_{ij}(t)]$ resp. $(f_{ij}(t))$ over $L(t)$. Thus it suffices to consider the case $L = k$. Now apply Corollary 2.3 with $A = k[t]_{\mathfrak{p}}$, where $\mathfrak{p}$ denotes the ideal of $k[t]$ generated by $t_1 - c_1, \ldots, t_r - c_r$. q.e.d.

Remark. Corollary 2.5 (ii) is in the case $m = 1$ and all $f_{ij}(t)$ constant the well known principle of substitution of Cassels and Pfister ([15], p. 365, [10], p. 20). In this case no additional assumption is needed if $\operatorname{char} k = 2$. In fact, we may assume again that $L = k$. Let E denote the space (f_{ij}) over k. We consider a decomposition

$$E = E_0 \perp \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \perp \cdots \perp \begin{pmatrix} a_r & 1 \\ 1 & 0 \end{pmatrix} \perp s \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

with E_0 anisotropic and minimal r. Then the subspace

$$\tilde{E} = E_0 \perp (a_1, \ldots, a_r)$$

is anisotropic. $(g_{11}(t))$ is already represented by $\tilde{E} \otimes k(t)$, and our Corollary 2.5 shows that $(g_{11}(c))$ is represented by $\tilde{E}$, hence by E.

Examples 2.6. (i) Assume k is a field of characteristik 2 which is not perfect, and let a be an element of k which is not a square. Then with one variable t the spaces $(1, 1 + at^2)$ and $(a, a(1 + at^2))$ over $k(t)$ are isomorphic. Substituting $t = 0$ we obtain the spaces $(1, 1)$ and (a, a) over k, which are not isomorphic. $(1, 1 + at^2)$ represents (a) over $k(t)$ but $(1, 1)$ does not represent (a) over k. This shows that even for $m = 1$ an additional assumption is needed in Corollary 2.5 (ii) if $\operatorname{char} k = 2$ and the $f_{ij}(t)$ are not constant.

(ii) For $m = 2$ and $\operatorname{char} k = 2$ already an additional assumption is needed if all f_{ij} are constant. For example with the element a from above the spaces $(1, 1, a)$ and $(a + t^2, a + t^2, a)$ over $k(t)$ are isomorphic (see [11], Theorem 3, or [7], Satz 8.3.1). Thus $(1, 1, a)$ represents the anisotropic space $(a, a + t^2)$ over $k(t)$. But $(1, 1, a)$ does not represent (a, a) over k. Indeed, otherwise $(1, 1, a)$ would be isomorphic to (a, a, a) which is absurd, since (a, a, a) does not represent (1).

We now want to prove a generalization of Proposition 2.2 in the quadratic case. As above let $\lambda\colon K \to L \cup \infty$ denote a fixed place with valuation ring $\mathfrak{o}$. We tacitly assume up to the end of this section that $\operatorname{char} L = 2$, since otherwise Lemma 2.8 and Proposition 2.9 below are already proved.

Lemma 2.7. *Let N be a free quadratic module over $\mathfrak{o}$ such that $N/\mathfrak{m}N$ is non degenerate. Then N is maximal among the lattices N' over $\mathfrak{o}$ in $N \otimes K$ with $q(N') \subset \mathfrak{o}$.*

Proof. There exists some decomposition

$$N/\mathfrak{m}N = \bar{N}_1 \perp \bar{N}_2$$

with $\bar{N}_1$ a space over $\mathfrak{o}/\mathfrak{m}$ and $\bar{N}_2$ the quasilinear part of $N/\mathfrak{m}N$. This decomposition can be lifted to a decomposition $N = N_1 \perp N_2$ (e.g. [6], p. 259). Since $\bar{N}_2$ is anisotropic it is easily seen that N_2 is the set of all z in the submodule $N_2 \otimes K$ of E with $q(z) \in \mathfrak{o}$. Now assume that x is a vector in E such that $q(N + \mathfrak{o}x)$ is still contained in $\mathfrak{o}$. We have $x = x_1 + x_2$ with x_i in $N_i \otimes K$. Clearly $B(x, N_1) = B(x_1, N_1) \subset \mathfrak{o}$. This implies $x_1 \in N_1$, since N_1 is a space. Thus $N + \mathfrak{o}x = N + \mathfrak{o}x_2$. In particular $q(x_2) \in \mathfrak{o}$, which implies $x_2 \in N_2$, as states above. This completes the proof. q.e.d.

Lemma 2.8. *Let M and N be free quadratic modules over $\mathfrak{o}$ such that $M/\mathfrak{m}M$ and $N/\mathfrak{m}N$ are non degenerate. Assume that $N \otimes K$ represents $M \otimes K$. Then $N/\mathfrak{m}N$ represents $M/\mathfrak{m}M$. If M is a space over $\mathfrak{o}$ or if $N/\mathfrak{m}N$ is anisotropic, then even N represents M.*

Proof. (a) We shortly write $\bar{M}$ for $M/\mathfrak{m}M$, $\bar{N}$ for $N/\mathfrak{m}N$, and k for $\mathfrak{o}/\mathfrak{m}$. We first consider the special case that M is a space over $\mathfrak{o}$ and have to show $M < N$. By Proposition 1.2 it suffices to prove $M \perp (-M) < N \perp \perp (-M)$. Now

$$M \perp (-M) \cong r \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

for some $r \geqslant 0$. Thus we see again by Proposition 1.2 that it suffices to prove our assertion in the special case $M \cong \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, which we consider now.

We regard N as a lattice of $E := N \otimes K$. Since E represents a hyperbolic plane, there exists some x in N with $q(x) = 0$ and $\mathfrak{o}x$ a direct summand of the $\mathfrak{o}$-module N. The ideal $B(x, N)$ of $\mathfrak{o}$ is finitely generated, thus $B(x, N) = a\mathfrak{o}$ with some $a \neq 0$ in $\mathfrak{o}$. Assume $a \in \mathfrak{m}$. Then one immediately sees, that q takes on $N + a^{-1}x\mathfrak{o}$ only values in $\mathfrak{o}$. This contradicts Lemma 2.7. Thus $a \in \mathfrak{o}^*$ and there exists some y in N with $B(x, y) = 1$. (This is a very classical argument, see e.g. [14], p. 235). The submodule $\mathfrak{o}x + \mathfrak{o}y$ of N is non singular and in particular a direct summand of N. Furthermore $\mathfrak{o}x + \mathfrak{o}y$ is isotropic and thus hyperbolic.

(b) We now consider the general case. As explained in the proof of Lemma 2.7, we have a decomposition $M = M_1 \perp M_2$ with M_1 a space over $\mathfrak{o}$ and $B(M_2 \times M_2) \subset \mathfrak{m}$. We know by part (a) of the proof that $M_1 < N$, and thus $N \cong M_1 \perp N_2$ with some quadratic module N_2. By Proposition 1.2 we obtain from $M \otimes K < N \otimes K$ that $M_2 \otimes K < N_2 \otimes K$. It suffices to show that $M_2/\mathfrak{m}M_2$ is represented by $N_2/\mathfrak{m}N_2$. We thus have reduced the proof to the special case that $B(M \times M) \subset \mathfrak{m}$ in addition to the assumptions of the proposition.

We again regard N as a lattice in $E: = N\otimes K$ and regard M as a lattice in $F: = M\otimes K$. We assume without loss of generality that F is a submodule of E over K. Now the intersection $N_1: = N\cap F$ is contained in M since M is the set of all z in F with $q(z)$ in $\mathfrak{o}$. By the elementary divisor theorem there exists a basis $x_1, \ldots, x_m$ of M and a basis $y_1, \ldots, y_m$ of N_1 such that $y_i = a_i x_i$ with a_i in $\mathfrak{o}$. We may assume that there is some s in $[0, m]$ such that $a_i = 1$ for $1 \leqslant i \leqslant s$ and $a_i \in \mathfrak{m}$ for $s < i \leqslant m$. If $s = m$, then $N_1 = M$ and thus $M < N$. Certainly $s = m$ if $\bar{N}$ is anisotropic. Since now we assume $s < m$. Let V denote the image of the direct summand N_1 of N in $\bar{N}$. Since $B(M\times M) \subset \mathfrak{m}$ we have $B(N_1 \times N_1) \subset \mathfrak{m}$ and thus $B(V\times V) = 0$. Let a_i denote the image of $q(x_i)$ in k. Then

$$(*) \qquad \bar{M} \cong [a_1]\perp\ldots\perp[a_m],$$

and

$$V \cong [a_1]\perp\ldots\perp[a_s]\perp(m-s)\times[0].$$

Let further V_0 denote the intersection of V with the quasilinear part R of $\bar{N}$. Since V_0 is an anisotropic submodule of V, clearly V_0 is represented by $[a_1]\perp\ldots\perp[a_s]$, i.e.

$$(**) \qquad [a_1]\perp\ldots\perp[a_s] \cong V_0\perp[c_1]\perp\ldots\perp[c_{s-t}]$$

with $t = \dim V_0$ and suitable elements $c_1, \ldots, c_{s-t}$ in k^*. (Read V_0 for the right hand side if $t = s$.) Thus we have a decomposition $V = V_0 \perp U$ where U is a submodule of V with

$$U \cong [c_1]\perp\ldots\perp[c_{s-t}]\perp(m-s)\times[0].$$

(The $[c_i]$ have to be omitted if $t = s$.) Now we choose a submodule W of $\bar{N}$ such that

$$\bar{N} = R\oplus U\oplus W = R\perp(U\oplus W).$$

The submodule $P: = U\oplus W$ must be a space. Let $u_1, \ldots, u_{m-t}$ denote a basis of U with $q(u_i) = c_i$ for $1 \leqslant i \leqslant s-t$ and $q(u_i) = 0$ for $s-t < i \leqslant m-t$. Since $B(U\times U) = 0$, we can find elements $z_1, \ldots, z_{m-t}$ in P such that $B(z_i, z_j) = 0$ and $B(z_i, z_j) = \delta_{ij}$ for i and j in $[1, m-t]$ (e.g. [7], Satz 3.2.1). Thus we finally obtain a decomposition

$$\bar{N} = R\perp(ku_1+kz_1)\perp\ldots\perp(ku_{m-t}+kz_{m-t})\perp Q$$

with some space Q. Now R represents V_0 and ku_i+kz_i represents $[c_i]$ for $1 \leqslant i \leqslant s-t$. For $s-t < i \leqslant m-t$ the space ku_i+kz_i is hyperbolic and certainly represents $[a_{t+i}]$. We see that $\bar{N}$ indeed represents $\bar{M}$, since by $(*)$ and $(**)$

$$\bar{M} \cong V_0\perp[c_1]\perp\ldots\perp[c_{s-t}]\perp[a_{s+1}]\perp\ldots\perp[a_m].$$

q.e.d.

We say that a quadratic module E over K has *nearly good reduction* with respect to $\lambda: K\to L\cup\infty$, if E contains a quadratic $\mathfrak{o}$-module M of full rank with $M/\mathfrak{m}M$ non degenerate. We then denote by $\lambda_*(E)$ the quadratic module $\mu_*(M)$ over L with $\mu: \mathfrak{o}\to L$ the restriction of λ. By the just proved Lemma 2.8 the quadratic module $\lambda_*(E)$ depends up to isomorphy only on E and λ.

We now obtain from Lemma 2.8 the following generalization of Proposition 2.2 for quadratic modules:

PROPOSITION 2.9. *If E and F are quadratic modules over K with nearly good reduction with respect to $\lambda: K\to L\cup\infty$, and if $F < E$, then $\lambda_*(F) < \lambda_*(E)$.*

COROLLARY 2.10. *The assertion* (i) *of Corollary* 2.3 *remains true if for the quadratic modules M and N occurring there we only assume that $M/\mathfrak{M}M$ and $N/\mathfrak{M}N$ are non degenerate. The assertion* (i) *of Corollary* 2.5 *remains true if the word "non singular" there is replaced by "non degenerate".*

§ 3. Subspaces with bad reduction. As in § 2 we consider a fixed place $\lambda: K\to L\cup\infty$. The following theorem is well-known in the special case that the valuation ring $\mathfrak{o}$ of λ has rank 1, see [7], § 12, and for $\mathfrak{o}$ discrete also [17] and [13], Chapter IV, § 1. We shall prove it by generalizing the argument given in [13].

THEOREM 3.1. *There exists a unique additive map $\lambda_*: W(K)\to W(L)$ with $\lambda_*\{a\} = \{\lambda(a)\}$ for every a in K^* such that $\lambda(a) \neq 0, \infty$, and with $\lambda_*\{a\} = 0$ for every a in K^* such that $\lambda(ac^2) = 0$ or ∞ for every c in K^*.*

Proof. We may assume without loss of generality that $L = \mathfrak{o}/\mathfrak{m}$ and $\lambda: K\to L\cup\infty$ is the canonical place associated with $\mathfrak{o}$. We may further assume $\mathfrak{m} \neq 0$, since else the theorem is trivial. Then certainly K is infinite and we can apply Theorem 1.1 with $A = K$. The image of an element a of $\mathfrak{o}$ in L will be denoted by $\bar{a}$. We have a well defined additive map Λ from the group ring $\mathbf{Z}[G]$, $G: = K^*/K^{*2}$, to $W(L)$ with $\Lambda\langle a\rangle = \{\bar{a}\}$ if a in $\mathfrak{o}^*$, and $\Lambda\langle a\rangle = 0$ if the square class $\langle a\rangle$ does not contain a unit of $\mathfrak{o}$. Clearly this map Λ vanishes on all elements $\langle a\rangle + \langle -a\rangle$ with a in K^*. According to Theorem 1.1 our theorem will be proved if we show that Λ vanishes on an arbitrary element

$$z = \langle a_1\rangle + \langle a_2\rangle - \langle a_3\rangle - \langle a_4\rangle$$

with $(a_1, a_2) \cong (a_3, a_4)$. If none of the square classes $\langle a_i\rangle$ contains a unit of $\mathfrak{o}$, this is evident. Thus we assume without loss of generality $a_1 \in \mathfrak{o}^*$. Then $z = \langle a_1\rangle y$ with an element

$$y = 1 + \langle c\rangle - \langle b\rangle - \langle bc\rangle$$

such that $(1, c) \cong (b, bc)$, which means $b = u^2+v^2c$ with suitable elements u, v of K. For arbitrary elements a in $\mathfrak{o}^*$ and x in $\mathbf{Z}[G]$ we clearly

have $\Lambda(\langle a\rangle x) = \{\bar{a}\}\Lambda(x)$. Thus it suffices to prove $\Lambda(y) = 0$. We assume that both u and v are $\neq 0$, since otherwise already $y = 0$.

We first consider the case that c lies in $\mathfrak{o}^*$. Then

$$\Lambda(y) = (1+\{\bar{c}\})\Lambda(1-\langle b\rangle).$$

We have nothing to prove if $\{\bar{c}\} = \{-1\}$. Thus we assume in addition $\{\bar{c}\} \neq \{-1\}$, which means that the space $(1, \bar{c})$ over L is anisotropic. Changing b by a square we further assume that u and v both lie in $\mathfrak{o}$ but not both in $\mathfrak{m}$. Since $(1, c)$ is anisotropic, we have $\bar{b} = \bar{u}^2+\bar{c}\bar{v}^2 \neq 0$ and

$$\Lambda(y) = (1+\{\bar{c}\})(1-\{\bar{u}^2+\bar{c}\bar{v}^2\}) = 0.$$

We now consider the remaining case that $\langle c\rangle$ does not contain a unit of $\mathfrak{o}$. Then $u^{-2}v^2c$ is not a unit and thus either $b = u^2(1+d)$ or $b = v^2c(1+d)$ with some d in $\mathfrak{m}$. Hence $\Lambda(1-\langle b\rangle) = 0$ or $= 1-\{\bar{c}\}$ and $\Lambda(y) = 0$ in both subcases. q.e.d.

Remark. For a bilinear space E over K with good reduction the element $\lambda_*\{E\}$ constructed in § 2 is the same element as the image of $\{E\}$ under the map λ_* constructed now. This follows easily from the fact, that for every space M over $\mathfrak{o}$ at least the space $M\perp(1)$ has the form $(a_1, \ldots, a_r)$ with a_i in $\mathfrak{o}^*$ (cf. § 1).

The map $\lambda_*: W(K)\to W(L)$ gives some information about spaces with good reduction which contain subspaces with bad reduction, i.e. not good reduction.

Proposition 3.2. *Let E be a bilinear space over K with good reduction.*

(i) *Assume* $\operatorname{char} L \neq 2$. *If E represents a space $(b_1, \ldots, b_m)$ such that $\lambda(b_ic^2) = 0$ or ∞ for each b_i and every c in K^*, then $\lambda_*(E)$ has index $\geqslant \{m/2\}$.* (*As usual $\{m/2\}$ denotes the least integer $\geqslant m/2$.*)

(ii) *If* $\operatorname{char} L = 2$ *and E has very good reduction, then each subspace of E also has very good reduction.*

Proof. (i) $E \cong (b_1, \ldots, b_m, c_1, \ldots, c_{n-m})$ with some c_i in K^*. Thus $\lambda_*\{E\} = \lambda_*\{(c_1, \ldots, c_{n-m})\}$. From the definition of λ_* it is clear that the equivalence class of $\lambda_*(E)$ contains a space of rank $\leqslant n-m$. This means that $\lambda_*(E)$ has an index $\geqslant \{m/2\}$.

(ii) E must be anisotropic since E has very good reduction. Thus certainly every subspace of E has an orthogonal basis. If E would contain a subspace with bad reduction, then E would contain a space (b) of rank one such that $\lambda(bc^2) = 0$ or ∞ for all c in K^*. But then we see again, that $\lambda_*(E)$ is equivalent to a space of lower rank. This contradicts the assumption that $\lambda_*(E)$ is anisotropic. Now the assertion follows from Proposition 2.2 (ii). q.e.d.

Proposition 3.3. *Let $(f_{ij}(t))$ be a symmetric (n, n)-matrix of polynomials $f_{ij}(t) \in k[t_1, \ldots, t_r]$ over an arbitrary field k, and $g_1(t), \ldots, g_m(t)$ be m*

further polynomials in $k[t]$. Assume $c = (c_1, \ldots, c_r)$ is an r-tuple with coordinates in a field extension L of k such that $\det(f_{ij}(c)) \neq 0$, and that c is a non singular zero of each g_p, i.e. $g_p(c) = 0$, $(\partial g_p/\partial t_q)(c) \neq 0$ with some q depending on p. Then if the space $(f_{ij}(t))$ over $k(t)$ represents the space $(g_1(t), \ldots, g_m(t))$, the space $(f_{ij}(c))$ over L has an index $\geqslant \{m/2\}$.

Proof. As in the proof of Corollary 2.5 we may assume $L = k$. If $r = 1$, then our proposition follows immediately from Proposition 3.2 by use of the place $\lambda: k(t_1)\to k\cup\infty$ over k (i.e. λ is the identity on k) with $\lambda(t_1) = c_1$. Assume now $r > 1$. We first consider the case that k is infinite. Then there exists an r-tuple $(a_1, \ldots, a_r)$ in k^r such that

$$\sum_{q=1}^{r} a_q(\partial g_p/\partial t_q)(c) \neq 0$$

for $1 \leqslant p \leqslant m$. Thus performing a suitable linear transformation of coordinates with coefficients in k we may assume $(\partial g_p/\partial t_1)(c) \neq 0$ for $1 \leqslant p \leqslant m$. Let c' denote the $(r-1)$-tuple $(c_2, \ldots, c_r)$. There exists a place $\alpha: k(t)\to k(t_1)\cup\infty$ over $k(t_1)$ with $\alpha(t_i) = c_i$ for $2 \leqslant i \leqslant r$. (Cf. the proof of Corollary 2.3 with A the local ring of $k(t_1)[t_2, \ldots, t_r]$ corresponding to c'.) Using the map $\lambda_*: W(k(t))\to W(k(t_1))$ we see that the space $(f_{ij}(t_1, c'))$ over $k(t_1)$ is equivalent to a space

$$(g_1(t_1, c'), \ldots, g_m(t_1, c'), h_1(t_1), \ldots, h_s(t_1))$$

with some polynomials $h_p(t_1)$ and $m+s \leqslant n$. (If $m = n$, omit the h_p.) Let $\lambda: k(t_1)\to k\cup\infty$ denote the place over k with $\lambda(t_1) = c_1$. Then using $\lambda_*: W(k(t_1))\to W(k)$ we see that, since all $\lambda_*\{g_i(t_1, c')\}$, $1 \leqslant i \leqslant m$, are zero, the space $(f_{ij}(c))$ over k is equivalent to a space of rank $\leqslant n-m$. This means that the index of this space is $\geqslant \{m/2\}$.

Assume now that k is finite. Let u denote an indeterminate over k. By what has been proved the space $(f_{ij}(c))$ is equivalent over $k(u)$ to a space of rank $\leqslant n-m$. Applying $\beta_*: W(k(u))\to W(k)$ with some place $\beta: k(u)\to k\cup\infty$ over k, we see that $(f_{ij}(c))$ is over k equivalent to a space of rank $\leqslant n-m$. q.e.d.

Remark. If $\operatorname{char} k \neq 2$ the proof could have been shortened by applying first the principle of substitution and then Proposition 3.2 (i).

Proposition 3.4. *Assume E is a quadratic module over K which has nearly good reduction with respect to $\lambda: K\to L\cup\infty$. Further assume that F is a submodule of E with $\lambda(q(x)) = 0$ or ∞ for every x in F. Then $\lambda_*(E)$ has an index $\geqslant \dim F$.*

Proof. Let N denote a module over $\mathfrak{o}$ of full rank in E with $N/\mathfrak{m}N$ non degenerate and let M denote the intersection $N\cap F$. Then $N = M\oplus M'$ with some other submodule M' of N. The image $\bar{M}$ of M in $N/\mathfrak{m}N$ is

a submodule of the same rank as F with $q(\bar{M}) = 0$, since $q(x) \in \mathfrak{m}$ for all x in M. This implies the assertion (see § 1). q.e.d.

PROPOSITION 3.5. *Let $(f_{ij}(t))$ be a symmetric matrix of polynomials $f_{ij}(t)$ in $k[t] = k[t_1, \ldots, t_r]$ and $g_1(t), \ldots, g_m(t)$ be m further polynomials in $k[t]$. Assume that $c = (c_1, \ldots, c_r)$ is an r-tuple with coordinates c_i in a field extension L of k, such that the quadratic module $[f_{ij}(c)]$ over L is non degenerate, all $g_p(c) = 0$, and the matrix $(\partial g_p/\partial t_q)(c)$ has rank m. Assume further that the module $[f_{ij}(t)]$ over $k(t)$ represents $[g_1(t)] \perp \ldots \perp [g_m(t)]$. Then the module $[f_{ij}(c)]$ over L has index $\geqslant m$.*

Proof. We may assume $k = L$. Further replacing the variables t_i by $t_i - c_i$ we assume $c = 0$. Finally subjecting the t_i to a suitable linear transformation with coefficients in k we assume

$$(*) \qquad (\partial g_p/\partial t_q)(0) = \delta_{pq},$$

for $1 \leqslant p \leqslant m$, $1 \leqslant q \leqslant r$. We consider the field $K = k(t, s)$ with an indeterminate s over $k(t)$, and the subfield $k(u) = k(u_1, \ldots, u_r)$ of K with $u_i = t_i s^{-1}$. Let λ denote the place from $K = k(u, s)$ to $k(u)$ over $k(u)$ which maps s to 0. Regarding the module

$$F = [g_1(t)] \perp \ldots \perp [g_m(t)]$$

over K, we shall prove below:

$$(**) \qquad \lambda(q(x)) = 0 \text{ or } \infty \quad \text{for all } x \text{ in } F.$$

Since the module $[f_{ij}(t)]$ over K represents F, and $\lambda(t_i) = 0$ for $1 \leqslant i \leqslant r$, it then follows by Proposition 3.4, that the module $[f_{ij}(0)]$ over $k(u)$ has index $\geqslant m$. By Corollary 2.10 also the module $[f_{ij}(0)]$ over k has index $\geqslant m$.

We now prove (**). For any $x \neq 0$ in F the value $q(x)$ has the form ZN^{-1} with

$$N = h(u, s)^2, \quad Z = \sum_{i=1}^{m} a_i(u, s)^2 g_i(u_1 s, \ldots, u_r s),$$

$h(u, s)$ and $a_i(u, s)$ denoting polynomials in $k[u, s]$ such that $h(u, s) \neq 0$ and not all $a_i(u, s) = 0$. We now regard the $a_i(u, s)$ as polynomials in s with coefficients in $k[u]$. For some $l \geqslant 0$ we may write for $1 \leqslant i \leqslant r$

$$a_i(u, s) = b_i(u) s^l + \text{higher terms},$$

with at least one $b_i(u) \neq 0$. By (*) the lowest term of $g_i(u_1 s, \ldots, u_r s)$ with respect to s is $u_i s$. Thus the lowest term of Z is $c(u) s^{2l+1}$ with

$$c(u) = \sum_{i=1}^{m} b_i(u)^2 u_i,$$

provided $c(u) \neq 0$. But a glance on the term of lowest (or highest) total degree in the polynomial $c(u)$ makes evident, that indeed $c(u) \neq 0$. Thus the lowest degree with respect to s occurring in the polynomial Z is $2l+1$. On the other hand the lowest degree of N is an even number. Clearly $\lambda(ZN^{-1}) = 0$ or $= \infty$. q.e.d.

We now consider the following situation: $(f_{ij}(t))$ is a bilinear space over $k(t) = k(t_1, \ldots, t_r)$ with indeterminates t_i and the $f_{ij}(t)$ polynomials in $k[t]$. Further $g(t)$ is a polynomial in $k[t]$, which is represented by the space $(f_{ij}(t))$ over $k(t)$. Finally c is an r-tupel with coordinates in a field extension L of k such that the bilinear module $(f_{ij}(c))$ over L is non singular and $g(c) = 0$. If the zero c of g is non singular, then by Proposition 3.3 the space $(f_{ij}(c))$ over L must be isotropic. But if c is a singular zero then it may very well happen that $(f_{ij}(c))$ is anisotropic. The following Proposition 3.6 deals with this case. Recall that any bilinear module E over L has a decomposition

$$E \cong F \perp r \times (0)$$

with F a non singular bilinear module, which up to isomorphism is uniquely determined by E. We call F the *non singular part* of E.

PROPOSITION 3.6. *Assume* Char $k \neq 2$ *and that in the situation described above $(f_{ij}(c))$ is an anisotropic space over L and in particular c is a singular zero of g. Then the space $(f_{ij}(c))$ over L represents the non singular part of the bilinear module (a_{pq}), $1 \leqslant p, q \leqslant r$, over L with*

$$a_{pq} = \tfrac{1}{2}(\partial^2 g/\partial t_p \partial t_q)(c).$$

Remark. In the special case that all $f_{ij}(t)$ are constant, $g(t)$ is a quadratic form, and $c = 0$, Proposition 3.6 is the well known subform theorem of Cassels and Pfister ([10], p. 20). In fact, the theorem of Cassels and Pfister provides the main step in the proof of Proposition 3.6, which now follows.

Proof. We proceed on a similar way as in the proof of Proposition 3.5. Without loss of generality we assume $k = L$ and $c = 0$. Let

$$h(t) = \sum_{p,q} a_{pq} t_p t_q$$

denote the Hessian form of $g(t)$, with the a_{pq} from above. We have

$$g(t) = h(t) + c(t)$$

with a polynomial $c(t)$ which only contains monomials of total degree $\geqslant 3$. If $h(t) = 0$, there is nothing to prove. Thus we assume after a suitable linear transformation of coordinates that for some index m in $[1, r]$ all a_{pq} with $p > m$ or $q > m$ are zero and the matrix (a_{pq}), $1 \leqslant p, q \leqslant m$

has determinant $\neq 0$. If $m < r$ we obtain by the principle of substitution 2.5, that the space $\langle f_{ij}(t_1, \ldots, t_m, 0, \ldots, 0)\rangle$ over $k(t_1, \ldots, t_m)$ represents $g(t_1, \ldots, t_m, 0, \ldots, 0)$. Thus we may assume without loss of generality from the beginning, that the space (a_{pq}) over k is non singular.

We again consider the fields $K = k(t, s) = k(u, s)$ and $k(u)$ constructed in the proof of Proposition 3.5. The space $\langle f_{ij}(u_1 s, \ldots, u_r s)\rangle$ over K represents the element

$$s^{-2} g(t) = h(u) + s\tilde{c}(u, s)$$

with $\tilde{c}(u, s)$ a polynomial in $k[u, s]$. Substituting the value 0 for s we see by 2.5, that the space $\langle f_{ij}(0)\rangle$ over $k(u)$ represents $h(u)$. Now the subform theorem of Cassels and Pfister yields that the space $\langle f_{ij}(0)\rangle$ over k represents the space (a_{pq}) over k. q.e.d.

§ 4. The norm theorem. We consider a fixed bilinear or quadratic module E over an arbitrary field k. We call an element a of k^* a *norm* of E, if $(a)\otimes E \cong E$, i.e. if a is the norm of a similarity transformation of E. (If E is quadratic with associated quadratic form q then $(a)\otimes E$ denotes the module E with the quadratic form aq.) The set of norms of E is a group $N(E)$ which contains all squares in k^*.

The main goal of this section is to prove the Theorem 4.2 below about the norms of $E\otimes k(t)$ with $k(t) = k(t_1, \ldots, t_r)$ the field of rational functions in an arbitrary number r of variables $t_1, \ldots, t_r$ over k. For any polynomial $f(t) \in k[t]$ we denote by f^* the coefficient of the highest monomial occurring in $f(t)$ with respect to the lexigraphical ordering. ($t_1^{a_1} \ldots t_r^{a_r} > t_1^{b_1} \ldots t_r^{b_r}$ if and only if the first difference $a_i - b_i \neq 0$ is > 0.) We say that f is *normed* if $f^* = 1$. Notice that this notion depends on the chosen ordering $t_1 > t_2 > \ldots > t_r$ of the variables. We further fix the following notations for this section if $r > 1$: K denotes the field $k(t')$ with $t' = (t_2, \ldots, t_r)$, $\deg_1 f$ denotes the degree of f as a polynomial of $K[t_1]$.

We shall need the following

LEMMA 4.1. *Assume that E is an anisotropic bilinear or quadratic module $\neq 0$. If a polynomial $f(t) \in k[t]$ is a norm of $E\otimes k(t)$ then the highest monomial occurring in $f(t)$ has the form $t_1^{m_1} \ldots t_r^{m_r}$ with even exponents m_i. Furthermore f^* is a norm of E.*

We prove the lemma by induction on r. Assume first $r = 1$ and write t instead of t_1. We consider the place $\lambda\colon k(t) \to k \cup \infty$ over k with $\lambda(t) = \infty$. Clearly $E\otimes k(t)$ represents an element $af(t)$ with a in k^*. If $\deg f$ would be odd, then the Propositions 3.2 and 3.4 would imply that E is isotropic. Thus $\deg f$ is an even number m, and hence

$$(*) \qquad E\otimes k(t) \cong \langle t^{-m} f(t)\rangle \otimes (E\otimes k(t)).$$

Furthermore $\lambda(t^{-m} f(t)) = f^*$. Thus by computing $\lambda_*(E\otimes k(t)) = E$ using the right hand side of $(*)$ we obtain $E \cong (f^*)\otimes E$.

Assume now $r > 1$, and let $h \in k[t']$ denote the highest coefficient of f as a polynomial of $K[t_1]$. From the case $r = 1$ we obtain that $\deg_1 f$ is even and h is a norm of $E\otimes K$. Now apply the induction hypothesis to h. q.e.d.

For any irreducible polynomial $p(t)$ in $k[t]$ we denote by $k(p)$ the function field over k of the variety of zeros of $p(t)$, i.e. the quotient field of $k[t]/(p(t))$.

THEOREM 4.2. *Assume that E is an anisotropic bilinear space $\neq 0$ over k and that $p(t)$ is a normed irreducible polynomial in $k[t_1, \ldots, t_r]$. Then the following are equivalent:*

(i) *$p(t)$ is a norm of $E\otimes k(t)$.*

(ii) *$p(t)$ divides a square free polynomial $f(t)$* {i.e. $g^2(t) \mid f(t) \Rightarrow g(t) = \text{const}$}, *which is a norm of $E\otimes k(t)$.*

(iii) *$E\otimes k(p) \sim 0$.*

If $\operatorname{char} k \neq 2$ we may replace in this theorem — and similarly in Lemma 4.1 — the assumption "E anisotropic" by "E not hyperbolic", since $E\otimes k(t)$ and $\operatorname{Ker}(E)\otimes k(t) = \operatorname{Ker}(E\otimes k(t))$ have the same norm group.

Clearly Theorem 4.2 and Lemma 4.1 imply

COROLLARY 4.3. *Assume E is an anisotropic bilinear space $\neq 0$ over k. Then a polynomial $f(t) \in k[t_1, \ldots, t_r]$ is a norm of $E\otimes k(t)$ if and only if f^* is a norm of E and $E\otimes k(p) \sim 0$ for all normed irreducible $p \in k[t]$ which divide f with an odd power.*

We shall prove Theorem 4.2 by induction on r and consider first the case $r = 1$. Write t instead of t_1. The assertion (i) $\Rightarrow$ (ii) is trivial. To prove (ii) $\Rightarrow$ (iii) we consider the canonical place $\lambda_p\colon k(t) \to k(p) \cup \infty$ over k associated to p. Applying the map $(\lambda_p)_*$ from $W(k(t))$ to $W(k(p))$ to the equation

$$\{(1, -f)\} \cdot \{E\otimes k(t)\} = 0$$

we obtain $\{E\otimes k(p)\} = 0$, as desired. To prove (iii) $\Rightarrow$ (i) we consider for every normed polynomial π in $k[t]$ the map

$$\partial_\pi\colon W(k(t)) \to W(k(\pi))$$

defined by

$$\partial_\pi(x) = (\lambda_\pi)_*(\{\pi\} x).$$

As is well known ([12], Theorem 5.3) the sequence

$$(A) \qquad 0 \to W(k) \to W((kt)) \xrightarrow{(\partial_\pi)} \coprod_\pi W(k(\pi)) \to 0$$

is exact. (We shall not need the surjectivity of (∂_π).) Furthermore it is evident that a splitting of this sequence is given (for example) by the map $(\lambda_\infty)_*\colon W\big(k(t)\big)\to W(k)$ which comes from the place $\lambda_\infty\colon k(t)\to k\cup\infty$ over k with $t\mapsto\infty$. We consider the element

$$z := \{(1, -p)\}\cdot\{E\otimes k(t)\}$$

of $W\big(k(t)\big)$. Clearly $\partial_\pi(z) = 0$ for all $\pi \neq p$ and by assumption also $\partial_p(z) = -\{E\otimes k(p)\} = 0$. Finally we want to show $(\lambda_\infty)_*(z) = 0$. Then it is clear that $z = 0$, which means, that p is a norm of $E\otimes k(t)$, as desired.

By a theorem of Springer E remains anisotropic over any finite field extension of k of odd degree. ([16], Springer's argument is also valid if $\operatorname{char} k = 2$, both for the quadratic and bilinear case.) Thus p must have even degree. Since p is normed we obtain $(\lambda_\infty)_*\{p\} = \{1\}$ which implies $(\lambda_\infty)_*(z) = 0$. This completes the proof of Theorem 4.2 for $r = 1$.

Assume now $r > 1$ and that Theorem 4.2 is true for $r-1$. This time we prove first (i)$\Leftrightarrow$(ii) and then (i)$\Leftrightarrow$(iii) for r variables. We use the notations introduced before Lemma 4.1. We further denote by F the space $E\otimes K$ and by n the degree of p as a polynomial of $K[t_1]$. Of course (i)$\Rightarrow$(ii) is again trivial.

(ii) $\Rightarrow$ (i): We first assume that k has infinitely many elements. We consider the cases $n = 0$ and $n > 0$ separately. Assume first $n = 0$. We have a decomposition $f(t) = p(t')h(t)$ in $k[t]$. We choose an element c in k such that $p(t')$ does not divide $h(c, t')$ in $k[t']$. This is possible since k is infinite. (Regard the image of $h(t)$ in $\big(k[t']/(p)\big)[t_1]$.) Since $p(t')h(t)$ is a norm of $F\otimes K(t_1)$ we obtain by the principle of substitution (Corollary 2.5 (ii)) that $p(t')h(c, t')$ is a norm of F. Since by induction hypothesis also Corollary 4.3 is true for $(r-1)$ variables, we obtain that $p(t')$ is a norm of F and a fortiori of $F\otimes K(t_1)$.

Assume now $n > 0$. We denote by $a(t')\in k[t']$ the highest coefficient of p as a polynomial in $K[t_1]$ and by $\tilde p(t_1)$ the normed polynomial $a^{-1}p$ of $K[t_1]$. By the settled case $r = 1$ we know that $\tilde p(t_1)$ is a norm of $F\otimes K(t_1)$, hence

$$(B)\qquad (p)\otimes\big(F\otimes K(t_1)\big) \cong (a)\otimes\big(F\otimes K(t_1)\big).$$

Thus it suffices to show that $a(t')$ is a norm of F. Let $\pi(t')$ be an arbitrary irreducible normed polynomial in $k[t']$, which divide $a(t')$ with an odd power (if there is any such π). We shall show $\pi(t')\in N(F)$. Since $a(t')$ is normed it then will be clear that $a(t')\in N(F)$.

π does not divide all coefficients of $p(t)$ considered as a polynomial in t_1 over $k[t']$. Thus, since k is infinite, we find an element c in k such that π does not divide the polynomial $p(c, t')$ in $k[t']$. By the principle of substitution we obtain from (B)

$$(C)\qquad \big(p(c, t')\big)\otimes F \cong \big(a(t')\big)\otimes F,$$

i.e. $a(t')p(c, t')\in N(F)$. Since $\pi(t')$ divides this polynomial with an odd power we obtain by induction hypothesis that π is a norm of F. This completes the proof of (ii)$\Rightarrow$(i) if k is infinite.

If now k is finite we consider the field $L = k(u)$ with one indeterminate u. Applying (ii)$\Rightarrow$(i) to the space $E\otimes L$ and p, f as polynomials in $L[t]$ we obtain that p is a norm of $E\otimes L$. Then we see by the principle of substitution, e.g. specializing u to 0, that p is also a norm of E.

We now prove (i)$\Leftrightarrow$(iii) for r variables. If p does not depend on the variable t_1 we are through by induction hypothesis, since the field $k(p)$ corresponding to p as a polynomial in $k[t]$ is a purely transcendental extension of the field $k(p)'$ corresponding to p as a polynomial in $k[t']$. Thus we may assume $\deg_1 p > 0$. We use the letters K, F, a, p in the same meaning as in the proof of (i)$\Leftrightarrow$(ii).

(i) $\Rightarrow$(iii): By Lemma 4.1 $a(t')$ is a norm of F. Thus $\tilde p = a^{-1}p$ is a norm of $F\otimes K(t_1)$. From the case $r = 1$ we obtain $F\otimes K(\tilde p)\sim 0$. Notice that $K(\tilde p) = k(p)$ and $F\otimes K(\tilde p) = E\otimes k(p)$.

(iii) $\Rightarrow$(i): We know from the case $r = 1$ that $\tilde p$ is a norm of $F\otimes K(t_1) = E\otimes k(t)$. Thus $a(t')p(t)\in N\big(E\otimes k(t)\big)$. By the implication (ii)$\Rightarrow$(i) already proved for r variables we obtain $p(t)\in N\big(E\otimes k(t)\big)$. This finishes the proof of Theorem 4.2.

Remark. In the case that $\operatorname{char} k \neq 2$ and p is a quadratic form the implication (iii)$\Rightarrow$(i) of Theorem 4.2 has been used as a fundamental trick by Arason–Pfister [1] and Elman–Lam [5]. Arason and Pfister give in this case a proof of (iii)$\Rightarrow$(i) entirely different from our methods.

It would be interesting to prove a statement similar to Theorem 4.2 for quadratic spaces or modules if $\operatorname{char} k = 2$. The main obstacle seems to be, that no theorem analogous to the exact sequence (A) above is known. I only can state

Proposition 4.4. *Assume E is a quadratic module over k and $f(t)$ is a square free polynomial in $k[t]$ which is a norm of $E\otimes k(t)$. Then for every irreducible polynomial $p(t)\in k[t]$ which divides $f(t)$ and is separable, i.e. $\partial p/\partial t_i \neq 0$ for at least one variable t_i, we have*

$$E\otimes k(p) \cong l\times\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\perp s\times[0]$$

with some $l\geqslant 0$ and $s\geqslant 0$.

Proof. Let τ_j denote the image of t_j in $k(p)$. If $\partial p/\partial t_i \neq 0$ then certainly p does not divide $\partial p/\partial t_i$, thus $(\partial p/\partial t_i)(\tau) \neq 0$ for $\tau = (\tau_1, \dots, \tau_r)$. Since f is square free we obtain $f(\tau) = 0$ and $(\partial f/\partial t_i)(\tau) \neq 0$. We have

a decomposition

$$E\otimes k(p)\cong l\times\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\perp s\times[0]\perp G$$

with some anisotropic module G over $k(p)$ which up to isomorphy is uniquely determined by E. Assume $G\neq 0$. Let $u=(u_1,\dots,u_r)$ denote a set of r indeterminates over $k(p)$. Clearly $f(u)$ is a norm of $E\otimes k(p)(u)$ and thus also of $G\otimes k(p)(u)$. Applying Proposition 3.5 in the special case $m=1$ we easily obtain a contradiction. Thus $G=0$. q.e.d.

Theorem 4.2 gives for an anisotropic bilinear space E a characterization of the irreducible normed polynomials $p(t)$ such that $E\otimes k(p)\sim 0$. The reader might ask for a similar characterization of those normed irreducible $p(t)$ such that $E\otimes k(p)$ is isotropic. This has been given by Witt [19]. I want to recall his result in a way similar to Theorem 4.2.

Let $q(X_1,\dots,X_n)\in k[X_1,\dots,X_n]$ denote an anisotropic quadratic form in an arbitrary number n of variables X_i over an arbitrary field k. Let $t=(t_1,\dots,t_r)$ be another set of variables. We consider the subgroup $G_t(q)$ of $k(t)$ which is generated by all polynomials $g(t)\in k[t]$ such that $g(t)=q\big(f_1(t),\dots,f_n(t)\big)$ with polynomials $f_i(t)$ whose greatest common divisor is 1.

THEOREM 4.5. *For a normed irreducible polynomial $p(t)$ in $k[t]$ the following are equivalent:*

(i) $p(t)\in G_t(q)$.

(ii) *There exists a polynomial $f(t)$ in $G_t(q)$ which is divided by $p(t)$.*

(iii) $q\otimes k(p)$ *is isotropic.*

In fact, Witt states the equivalence of (i) and (iii) only for $r=1$, but his argument is valid for arbitrary r.

References

[1] J. K. Arason und A. Pfister, *Beweis des Krullschen Durchschnittsatzes für den Wittring*, Invent. Math. 12 (1971), pp. 173–176.

[2] C. Arf, *Untersuchungen über quadratische Formen in Körpern der Charakteristik 2* (Teil I), J. Reine Angew. Math. 183 (1941), pp. 148–167.

[3] H. Bass, *Lectures on Topics in Algebraic K-Theory*, Bombay 1967.

[4] N. Bourbaki, *Algèbre*, Chap. 9, *Formes sesquilinéaires et formes quadratiques*, Paris 1959.

[5] R. Elman and T. Y. Lam, *Pfister forms and K-theory of fields*, J. Algebra 23(1972), pp. 181–213.

[6] M. Knebusch, *Isometrien über semilokalen Ringen*, Math. Zeitschr. 108 (1969), pp. 255–268.

[7] — *Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen*, S. -B. Heidelberger Akad. Wiss. Math.-Natur. Kl. 1969/70, 3. Abhandelung, pp. 93–157 (also obtainable as separate volume).

[8] M. Knebusch, A. Rosenberg and R. Ware, *Structure of Wittrings and quotients of abelian group rings*, Amer. J. Math. 94 (1972), pp. 119–155.

[9] — *Generic zero fields and splitting towers of quadratic forms*, in preparation.

[10] F. Lorenz, *Quadratische Formen über Körpern*, Lecture Notes in Mathematics 130, Berlin 1970.

[11] J. Milnor, *Symmetric inner product spaces in characteristic 2*, Prospects in Mathematics, pp. 59–75, Ann. of Math. Studies 70 (1971). Princeton Univ. Press.

[12] — *Algebraic K-theory and quadratic forms*, Invent. Math. 9 (1970), pp. 318–344.

[13] J. Milnor and D. Husemoller, *Symmetric bilinear forms*, Berlin, Heidelberg, New York 1973.

[14] O. T. O'Meara, *Introduction to Quadratic Forms*, Berlin, Göttingen, Heidelberg 1963.

[15] A. Pfister, *Multiplikative quadratische Formen*, Arch. Math. 16 (1965), pp. 363–370.

[16] T. A. Springer, *Sur les formes quadratiques d'indice zéro*, C. R. Acad. Sci. (Paris) 234 (1952), pp. 1517–1519.

[17] — *Quadratic forms over fields with a discrete valuation I*, Indag. Math. 17 (1955), pp. 352–362.

[18] E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. 176 (1937), pp. 31–44.

[19] — *Verschiedene Bemerkungen zur Theorie der quadratischen Formen über einem Körper*, Colloque d'Algèbre supérieure, Bruxelles 1956, pp. 245–250.

MATHEMATISCHES INSTITUT
DER UNIVERSITÄT DES SAARLANDES
BRD, 66-Saarbrücken 15

Received on 28. 10. 1972 (339)