MÉMOIRES DE LA S. M. F.

F. LORENZ

Quadratische Formen und die Artin-Schreiersche Theorie der formal reellen Körper

Mémoires de la S. M. F., tome 48 (1976), p. 61-73

<http://www.numdam.org/item?id=MSMF_1976__48__61_0>

Col. sur les Formes Quadratiques (1975, Montpellier)
Bull. Soc. Math. France
Mémoire 48, 1976, p. 61-73

QUADRATISCHE FORMEN UND DIE ARTIN - SCHREIERSCHE THEORIE DER FORMAL REELLEN KÖRPER

par

F. LORENZ

In der Theorie der formal reellen Körper treten quadratische Formen in natürlicher Weise auf. Man kann sogar behaupten, dass - etwas metaphorisch gesprochen - die Artin-Schreiersche Theorie der formal reellen Körper in der Theorie der quadratischen Formen eine 'analytische Fortsetzung' besitzt. Im folgenden soll dabei besonders betont werden, dass in diesem Zusammenhang Wesentliches bereits auf sehr elementarem Niveau diskutiert werden kann.

1. Im folgenden bezeichne k stets einen Körper der Charakteristik $\neq 2$. Der Gegenstand der Artin-Schreierschen Theorie sind (total) geordnete Körper $(k,\leqslant)$. Eine Ordnung $\leqslant$ von k ist durch die Angabe ihres Positivbereiches $P = \{a \in k \mid a \geqslant 0\}$ gekennzeichnet. P besitzt die Eigenschaften

$$\begin{aligned} P + P &\subseteq P & P\,P &\subseteq P \\ P \cap -P &= \{0\} & P \cup -P &= k \end{aligned} \tag{1}$$

Jede Teilmenge P von k mit diesen Eigenschaften definiert umgekehrt eine Ordnung von k mit dem Positivbereich P. Wir nennen daher auch eine solche Teilmenge P von k eine Ordnung von k und bezeichnen einen geordneten Körper auch mit (k,P). Die erste wesentliche Feststellung, die man über diesen Begriff treffen kann, ist die, dass Quadrate in k positiv sind. Bezeichnen wir mit

$$QS(k) \tag{2}$$

die Gesamtheit aller Quadratsummen eines Körpers k, so gilt somit für einen geordneten Körper (k,P)

$$QS(k) \subseteq P \tag{3}$$

Die Menge $T = QS(k)$ ist daher der Grundkeim jeder möglichen Ordnung eines Körpers k. Sie besitzt die folgenden Eigenschaften

$$T + T \subseteq T \quad , \quad T\,T \subseteq T \tag{4}$$

2. Im folgenden wollen wir einige Grundlagen in einem allgemeinen Rahmen formulieren. Es sei A ein kommutativer Ring mit $1 \neq 0$. Mit $QS(A)$ bezeichnen wir die Gesamtheit aller Quadratsummen in A. Eine Teilmenge T von A mit den Eigenschaften

$$T + T \subseteq T \quad , \quad T\,T \subseteq T \quad , \quad QS(A) \subseteq T \tag{5}$$

wollen wir eine quadratische Präordnung des Ringes A nennen. Ist T eine quadra-

tische Präordnung von A, so ist $T + aT$ für jedes a aus A eine quadratische Präordnung, die a enthält.

Lemma 1. Sei T eine quadratische Präordnung von A mit $-1 \notin T$. Seien a,b Elemente aus A und gelte $ab \in T$. Dann ist $T + aT$ oder $T - bT$ eine quadratische Präordnung T' mit $-1 \notin T'$.

Beweis. Gelte im Widerspruch zur Behauptung $-1 = t_1 + at_2 = t_3 - bt_4$ mit $t_1, t_2, t_3, t_4 \in T$. Es folgt $-at_2 = 1 + t_1$, $bt_4 = 1 + t_3$. Multiplikation dieser beiden Gleichungen ergibt $-abt_2t_4 = 1 + t_5$ mit $t_5 \in T$. Somit $-1 = t_5 + abt_2t_4 \in T$ im Widerspruch zur Voraussetzung $-1 \notin T$.

Lemma 2. Sei T unter den quadratischen Präordnungen mit $-1 \notin T$ maximal. Dann besitzt T die folgenden beiden Eigenschaften :
(i) $T \cup -T = A$ (d. h. T ist eine totale quadratische Präordnung)
(ii) $T \cap -T$ ist ein Primideal von A.

Beweis. (i) Sei $a \in A$. Anwendung von Lemma 1 mit $a = b$ ergibt wegen der Maximalität von T, dass a oder $-a$ in T enthalten ist. (ii) Wegen (i) ist $T \cap -T$ ein Ideal von A. Aus (i) und Lemma 1 folgt, dass es ein Primideal sein muss.

Lemma 3. Sei T eine quadratische Präordnung von A mit $-1 \notin T$. Dann existiert eine quadratische Präordnung T' von A mit den folgenden Eigenschaften :

$$T \subseteq T' \quad , \quad T' \cup -T' = A \quad , \quad T' \cap -T' \text{ ist ein Primideal von } A$$

Beweis. Zorn's Lemma und Lemma 2.

3. Sei jetzt k wieder ein Körper der Charakteristik $\neq 2$. Für eine quadratische Präordnung T von k gilt dann

$$-1 \notin T \iff T \cap -T = 0 \iff T \neq k \quad .$$

Grundlage der Artin-Schreierschen Theorie ist der folgende

Satz 1. Für jede quadratische Präordnung T von k gilt

$$T = \bigcap_{T \subseteq P} P \tag{6}$$

wobei P sämtliche Ordnungen des Körpers k mit $T \subseteq P$ durchläuft. Ist insbesondere $-1 \notin T$, so gibt es eine Ordnung P des Körpers k mit $T \subseteq P$.

Beweis. Für $T = k$ ist nichts zu zeigen. Sei also $T \neq k$ und folglich $-1 \notin T$. Sei a ein Element von k mit $a \notin T$. Dann ist $T' = T - aT$ eine quadratische Präordnung von k mit $-1 \notin T'$. Nach Lemma 3 existiert eine Ordnung P des Körpers k mit $P \supseteq T' \supseteq T$. Es ist $-a \in P$, folglich $a \notin P$.

Damit kommen wir bereits zu dem folgenden

Satz 2. Seien (k,P) ein geordneter Körper und K/k eine Körpererweiterung. Wir setzen

$$QS_P(K) = \{ \sum a_i b_i^2 \mid a_i \in P, b_i \in K\} \tag{7}$$

Es gilt dann

$$QS_P(K) = \{b \in K \mid b \in P' \text{ für alle Ordnungen } P' \text{ von } K \text{ mit } P' \supseteq P\} \tag{8}$$

Beweis. Offenbar ist $T = QS_P(K)$ eine quadratische Präordnung von K mit $P \subseteq T$. Daher folgt die Behauptung aus Satz 1.

Als unmittelbare Folgerungen aus Satz 2 erhält man

Korollar 1 (Artin-Schreier, vgl. [1]). Sei (k,P) ein geordneter Körper. Dann sind für eine Körpererweiterung K/k die folgenden Aussagen gleichwertig : (i) Es gibt eine Ordnung P' von K mit $P' \supseteq P$. (ii) $-1 \notin QS_P(K)$. (iii) Für beliebige $a_1 > 0, \ldots, a_n > 0$ aus k ist die quadratische Form $a_1X_1^2 + \ldots + a_nX_n^2$ anisotrop über K.

Korollar 2 (A-S). Für einen beliebigen Körper K (der Charakteristik $\neq 2$) gilt :

$$QS(K) = \{b \in K \mid b \in P \text{ für alle Ordnungen } P \text{ von } K\} \tag{9}$$

Korollar 3 (A-S). Für einen beliebigen Körper K gilt : Genau dann ist K reell, d. h. $-1 \notin QS(K)$, wenn es eine Ordnung P von K gibt.

Zum Beweis der Korollare 2 und 3 hat man in Satz 2 nur $k = \mathbb{Q}$ zu setzen.

4. Der vorausgegangene Abschnitt zeigt bereits deutlich, dass quadratische Formen in der Theorie der formal reellen Körper in natürlicher Weise auftreten ; vgl. insbesondere die Formulierung von (iii) in Korollar 1. Der folgende Satz, der die erste spezifische Aussage der Artin-Schreierschen Theorie darstellt, ist nun sogar ein Spezialfall eines Satzes über quadratische Formen.

Satz 3 (A-S). Sei (k,P) ein geordneter Körper. Ist dann K/k eine endliche Körpererweiterung von ungeradem Grad, so gibt es eine Ordnung P' von K mit $P' \supseteq P$.

In der Tat ist Satz 3 im Hinblick auf Korollar 1 ein Spezialfall des folgenden Satzes.

Satz 3' (Springer [10]). Ist K/k eine endliche Körpererweiterung von ungeradem Grad, so ist jede anisotrope Form über k auch anisotrop über K.

Beweis. Man kann den Beweis von Artin und Schreier für Satz 3 unmittelbar übertragen : Wir nehmen im Widerspruch zur Behauptung an, die Gleichung

$$-1 = \sum_1^n a_i X_i^2 \qquad \text{mit} \qquad a_i \in k \tag{10}$$

sei lösbar in K, aber nicht in k. Ferner sei der Körpergrad K : k minimal. Es ist $K = k[X]/_f$ mit einem irreduziblen Polynom $f \in k[X]$. Nach (10) existieren dann in k[X] Polynome $g_i(X)$, h(X) mit

$$1 + \sum_1^n a_i \, g_i(X)^2 = h(X) \, f(x) \qquad (11)$$

Dabei kann man noch voraussetzen, dass die g_i alle einen Grad $< K : k$ haben. Es ergibt sich dann aus (11), dass der Grad von h ungerade und echt kleiner als K : k ist. Somit besitzt h einen irreduziblen Teiler f' von ungeradem Grade $< k : k$. Setzt man daher eine Nullstelle von f' in (11), ein, so erhält man einen Widerspruch zur Minimalität von K : k.

Satz 4 (A-S). Sei (k,P) ein geordneter Körper. Dann ist die Ordnung P von k fortsetzbar zu einer Ordnung P' des Erweiterungskörpers $K = k(\sqrt{a} \mid a \in P)$.

Wir übergehen an dieser Stelle den Beweis von Satz 4, der sich mittels Kor. 1 leicht führen lässt.

Nach Artin-Schreier heisst ein reeller Körper R reell abgeschlossen, wenn für jede algebraische Körpererweiterung E/R gilt : Ist E reell, so ist E = R. Ist R ein reell abgeschlossener Körper, so folgt aus Satz 4, dass die Menge $P = \{a^2 \mid a \in R\}$ der Quadrate in R eine Ordnung von R ist und somit R nur diese einzige Ordnung besitzt. Ferner folgt aus Satz 3 und Satz 4 mit etwas Körpertheorie der Satz von Euler-Lagrange : Ist C die algebraische abgeschlossene Hülle des reell abgeschlossenen Körpers R, so ist $C = R(i)$ mit $i^2 + 1 = 0$.

Lemma 4. (i) Sei k ein reeller Körper. Dann existiert ein reell algeschlossener Erweiterungskörper R von k, so dass R/k algebraisch ist. R heisst eine reelle Hülle des reellen Körpers k.

(ii) Sei (k,P) ein geordneter Körper. Dann existiert eine reelle Hülle R von k, deren Ordnung eine Fortsetzung von P ist. R heisst eine reelle Hülle des geordneten Körpers (k,P).

Beweis. (i) Lemma von Zorn. (ii) Nehme reelle Hülle des reellen Körpers $k(\sqrt{a} \mid a \in P)$.

5. Eine wesentliche, nicht ganz unmittelbar zugängliche Aussage ist nun

Satz 5 (A-S). Sind R_1, R_2 reelle Hüllen des geordneten Körpers (k,P), so gibt es (genau) einen k-Isomorphismus von R_1 auf R_2, und dieser ist ordnungstreu.

Für den Beweis ist im wesentlichen nur zu zeigen : Hat eine Polynom $f \in k[X]$ eine Nullstelle in R_1, so besitzt es auch eine Nullstelle in R_2. Dies folgt nun aus dem folgenden.

Satz 6 (Sylvester, et al.). Sei $(k;P)$ ein geordnter Körper. Zu f aus $k[X]$ gibt es dann eine quadratische Form $b_{f/k}$ mit folgender Eigenschaft : Für jede reelle Hülle R von (k,P) ist die Anzahl der Nullstellen von f in R gleich der Signatur (= Sylvesterscher Trägheitsindex) der Form $b_{f/k}$ bzgl. der Ordnung P von k :

$$|\{a \in R \mid f(a) = 0\}| = \mathrm{sgn}_P(b_{f/k}) \tag{12}$$

Beweis. Sei A eine endlich-dimensionale Algebra über einem Körper k. Mit $\mathrm{Tr}_{A/k} : A \to k$ bezeichnen wir die zugehörige Spur (der regulären Darstellung von A). Ist q eine symmetrische Bilinearform über A ; so ist

$$\mathrm{Tr}_{A/k}(q) := \mathrm{Tr}_{A/k} \circ q \tag{13}$$

eine symmetrische Bilinearform über k. Die Artikulation dieser einfachen, aber wichtigen Tatsache verdankt man Scharlau [9].

In der Situation von Satz 6 betrachten wir nun speziell $A = k[X]/f$ und setzen

$$b_{f/k} = \mathrm{Tr}_{A/k}(\langle 1\rangle) \tag{14}$$

wobei $\langle 1\rangle$ die Einsform auf A, d. h. die Multiplikation von A bezeichnet. Nun ist offenbar :

$$\mathrm{sgn}\,(b_{f/k}) = \mathrm{sgn}\,(b_{f/k} \otimes R) = \mathrm{sgn}\,(b_{f/R}) \tag{15}$$

Lediglich aus Bequemlichkeitsgründen nehmen wir im weiteren an, f sei irreduzibel über k. Sei dann

$$f = f_1 f_2 \ldots f_r \tag{16}$$

die Primfaktorzerlegung von f über R. Es ist

$$R[X]/f \cong R[X]/f_1 \times \ldots \times R[X]/f_r \tag{17}$$

(Isomorphie von R-algebren). Daher ist

$$b_{f/R} = b_{f_1/R} \oplus \ldots \oplus b_{f_r/R} \tag{18}$$

die orthogonale Summe der $b_{f_i/R}$. Folglich

$$\mathrm{sgn}(b_{f/R}) = \sum_1^r \mathrm{sgn}(b_{f_i/R}) \tag{19}$$

Nun ist aber offenbar $b_{f_i/R} \cong \langle 1\rangle$ bzw. $\langle 1\rangle \oplus \langle -1\rangle$, je nachdem ob $\mathrm{grad}\, f_i = 1$ bzw. $\mathrm{grad}\, f_i = 2$ ist. Hiermit ergibt sich aus (19) und (15) di Behauptung (12). Die erste Publikation einer solchen Beweisidee für Satz 5 findet man m. W. bei Knebusch [5] ; vgl. auch Becker und Spitzlay [2].

Auf der Grundlage von Satz 5 kann man mit der im Beweis von Satz 6 verwandten Methode leicht einige Folgerungen ziehen :

Satz 7. Seien (k,P) ein geordneter Körper und K/k eine endliche Körpererweiterung. Dann gilt

$$|\{Q \mid Q \text{ Ordnung von } K \text{ mit } Q \supseteq P\}| = \mathrm{sgn}_P(\mathrm{Tr}_{K\,k}(\langle 1\rangle))$$

Beweis. Satz 6 und Satz 5.

Allgemein gilt

Satz 8 (Knebusch [5]). Voraussetzunden wie in Satz 7. Dann gilt für jede quadratische Form q über K die Formel

$$\operatorname{sgn}_P(\operatorname{Tr}_{K/k}(q)) = \sum_{Q \geq P} \operatorname{sgn}_Q(q) \qquad (20)$$

wobei über alle Ordnungen Q von K, welche P fortsetzen, summiert wird.

Beweis. Zunächst können wir o. E. voraussetzen, dass q eindimensional ist : $q = \langle a \rangle$, $a \in K^*$. Unter Verwendung von Satz 7 erkennt man leicht, dass man darüberhinaus $K = k(a)$ annehmen darf. Sei f das Minimalpolynom von a über k, und sei R eine reelle Hülle von (k,P). Nun kann man genauso wie im Beweis von Satz 6 vorgehen : Es ist $K = k[X]/f$ und daher entsteht die R-Algebra $A' = R[X]/f$ durch Konstantenerweiterung aus der k-Algebra K. Folglich ist $\operatorname{sgn}_P \operatorname{Tr}_{K/k}(\langle a \rangle) = \operatorname{sgn} \operatorname{Tr}_{A'/R}(\langle a \rangle)$. Mittels (17) verifiziert man dann, dass dies gleich $\sum_1^s \operatorname{sgn}(a_i)$ ist, wobei $a_1, \ldots, a_s$ die verschiedenen Nullstellen von f in R sind. Im Hinblick auf Satz 5 ist diese Summe aber gleich dem Ausdruck auf der rechten Seite von (20).

Die Formel (20) ist eine gewiss bemerkenswerte Formel. Welche Bedeutung ihr zukommt, ist nicht ohne weiteres auszumachen. Jedenfalls scheint sei einen 'Archetyp' mathematischer Formeln zu vertreten ähnlich der Formel $\sum e_i f_i = n$ in der Bewertungstheorie.

6. In diesem Abschnitt soll auf das 17. Hilbertsche Problem eingegangen werden, dem die Theorie der formal reellen Körper ihre Entstehung verdankt, und welches Artin mittels derselben im positiven Sinne gelöst hat :

Satz 9 (Artin). Sei k ein reeller Körper, der genau eine Ordnung besitzt, und sei R eine reelle Hülle von k. Ist dann $f \in k[X_1,\ldots,X_n]$ ein Polynom in n Variablen über k, für welches $f(a_1,\ldots,a_n) \geqslant 0$ für alle $a_1,\ldots,a_n$ aus R gilt, so ist f Summe von Quadraten rationaler Funktionen aus $k(X_1,\ldots,X_n)$. Allgemeiner formuliert (vgl. auch [4]) : Sei V eine (über k definierte) irreduzible algebraische Varietät $\neq \emptyset$ von R^n mit dem Verschwindungsideal $I(V)$ von V in $k[X_1,\ldots,X_n]$. Die Elemente f von $k[V] := k[X_1,\ldots,X_n]/I(V)$ können wir dann als Funktionen auf V mit Werten in R auffassen. Es gilt dann : Ist $f(\underline{a}) \geqslant 0$ für alle $\underline{a} = (a_1,\ldots,a_n) \in V$, so ist f Summe von Quadraten im Quotientenkörper $k(V)$ von $k[V]$.

Beweisansatz. Sei $F = k(V)$. Wir nehmen im Widerspruch zur Behauptung an, dass $f \notin QS(F)$ ist. Nach Korollar 2 zu Satz 2 gibt es dann eine Ordnung $\leqslant$ des Körpers F mit

$$f < 0 \tag{21}$$

Es genügt dann zu zeigen, dass aus (21) die Existenz eines $a = (a_1,\ldots,a_n)$ aus V folgt mit

$$f(a) < 0 \tag{22}$$

Dies wird sich aus dem folgenden Satz ergeben.

Satz 9'. Sei k ein reell abgeschlossener Körper, und sei $K = k(x_1,\ldots,x_m)$ ein von den endlich vielen Elementen $x_1,\ldots,x_m$ erzeugter Erweiterungskörper von k. Ist dann K reell, so existiert ein Homomorphismus

$$k[x_1,\ldots,x_n] \to k$$

von k-Algebren.

Beweis von Satz 9 mittels Satz 9'. Wir übernehmen die obigen Bezeichnungen. Seien $x_1,\ldots,x_n$ der Reihe nach die kanonischen Bilder von $X_1,\ldots,X_n$ in $k[V]$. Somit hat man $k[V] = k[x_1,\ldots,x_n]$ und $F = k(x_1,\ldots,x_n)$. Sei R_F eine reelle Hülle des geordneten Körpers $(F,\leqslant)$. In R_F gilt $f < 0$, also gibt es ein h in R_F mit $f = -h^2$. Wir betrachten den algebraischen Abschluss R' von k in R_F. Man erkennt leicht, dass R' reell algeschlossen und somit ein reeller Abschluss des geordneten Körpers k ist. Aufgrund von Satz 5 sind wir berechtigt, $R' = R$ vorauszusetzen. Wir wenden nun Satz 9' auf den Erweiterungskörper $R(x_1,\ldots,x_n,h)$ von R an, der als Teilkörper von R_F reell ist. Wir erhalten die Existenz eines k-Algebrenhomomorphismus

$$\phi : k[x_1,\ldots,x_n,h,\tfrac{1}{h}] \to R$$

Seien $a_1,\ldots,a_n$ der Reihe nach die Bilder von $x_1,\ldots,x_n$ unter ϕ. Dann ist einerseits $(a_1,\ldots,a_n) \in V$, andererseits ist in der Tat $f(a_1,\ldots,a_n) = -h(a_1,\ldots,a_n)^2 < 0$.

Somit läuft alles auf den Beweis von Satz 9' hinaus. Man erkennt leicht, dass man sich dabei auf den Fall

$$\mathrm{Trgd}(K/k) = 1$$

beschränken kann. Sei nämlich K' ein Zwischenkörper von K/k mit $\mathrm{Trgd}(K/K') = 1$ (o. E. sei $\mathrm{Trgd}(K/k) \geqslant 1$, sonst ist $K = k$ und nichts zu beweisen). Sei R' eine reelle Hülle von K' innerhalb einer reellen Hülle R von K. Wenn unsere Behauptung für Erweiterungen vom Transzendenzgrad 1 richtig ist, erhalten wir einen Homomorphismus

$$\phi : R'[x_1,\ldots,x_m] \to R'$$

von R'-Algebren. Nun ist aber $\mathrm{Trgd}(k(\phi\, x_1,\ldots,\phi\, x_m)/k) \leqslant \mathrm{Trgd}(K/k) - 1$. Per Induktion sind wir fertig.

Sei jetzt also $K = k(x,y_1,\ldots,y_r)$, wobei x transzendent über k und die y_i algebraisch über $k(x)$ sind. Gesucht ist ein k-Algebrenhomomorphismus

$$k[x,y_1,\ldots,y_r] \to k$$

Nun gibt es nach dem Satz vom primitiven Element ein y aus K mit $K = k(x,y) = k(x)[y]$, wobei man y noch ganz über $k[x]$ annehmen darf. Für die y_i gilt dann

$$y_i = \frac{g_i(x,y)}{h_i(x)}$$

mit Polynomen $g_i(X,Y) \in k[X,Y]$, $0 \neq h_i(X) \in k[X]$. Wir erkennen somit, dass es genügt, die Existenz von unendlich vielen k-Algebrenhomomorphismen

$$\phi : k[x,y] \to k$$

sicherzustellen. Sei

$$f = f(x,Y) = Y^n + c_1(x)\,Y^{n-1} + \ldots + c_n(x)$$

das Minimalpolynom von y über $k(x)$. Wegen der Ganzheit von y über $k[x]$ liegen sämtliche $c_i(x)$ in $k[x]$. Es kommt daher darauf an, zu zeigen, dass es unendlich viele a aus k gibt, zu denen ein $b \in k$ existiert mit

$$f(a,b) = 0$$

Zu $a \in k$ betrachte man das Polynom

$$f_a(Y) = f(a,Y)$$

Nach Voraussetzung ist der Körper $K = k(x,y)$ reell, besitzt also eine Ordnung P. Sei R eine reelle Hülle des geordneten Körpers (K,P). Wir wissen, dass das Polynom

$$f = f(x,Y) \in k(x)[Y]$$

eine Nullstelle in R besitzt, nämlich $y \in K \subseteq R$. Folglich ist nach Satz 6

$$\operatorname{sgn}(b_{f/k(x)}) > 0 \ .$$

Sei die symmetrische Bilinearform $b_{f/k(x)}$ über $k(x)$ äquivalent zur Diagonalform

$$\langle h_1(x),\ldots,h_n(x)\rangle \quad \text{mit} \quad h_i(x) \in k[x] \tag{23}$$

Es gilt nun das folgende

Lemma. Sei k ein reell abgeschlossener Körper, und seien $h_1(X),\ldots,h_n(X) \in k[X]$ endlich viele Polynome einer Variablen über k. Sei $\leqslant$ eine Ordnung des Körpers $k(X)$ und werde mit $\operatorname{sgn} h$ das Vorzeichen eines Elementes h aus $k(X)$ bzgl. dieser Ordnung bezeichnet. Es gibt dann unendlich viele a aus k mit

$$\operatorname{sgn} h_i(a) = \operatorname{sgn} h_i(X) \quad \text{für} \quad i = 1,2,\ldots,n \tag{24}$$

Beweis. Weil k reell abgeschlossen ist, genügt es, die Behauptung für endlich viele Polynome der Gestalt $X - a_i$, $a_i \in k$ zu zeigen. Dies aber ist trivial.

Aus dem Lemma folgt nun, dass für unendlich viele a aus k die quadratische Form

$$\langle h_1(a),\ldots,h_n(a)\rangle \tag{25}$$

die gleiche Signatur hat wie die Form unter (23). Man kann sich aber leicht davon überzeugen, dass für fast alle a aus k die quadratische Form unter (25) äqui-

valent zu $b_{f_a/k}$ ist. Folglich ist für unendlich viele a aus k

$$\operatorname{sgn} b_{f_a/k} > 0 \ ,$$

und es existiert daher zu jedem dieser a ein b aus k mit $f_a(b) = f(a,b) = 0$. Dies beweist Satz 9' und damit auch Satz 9.

Nebenbei sei noch bemerkt, dass Satz 9' u.a. den folgenden Satz nach sich zieht (aus dem umgekehrt Satz 9' sofort folgt) :

Satz 9''. Sei k ein reell abgeschlossener Körper, und sei K ein Funktionenkörper einer Variablen über k. Ist dann K reell, so gibt es ein Element x aus K, für welches $K : k(x)$ ungerade ist.

Beweis. Mittels Satz 9' folgt in der Tat aus dem Satz von Riemann-Roch, dass ein x aus K existiert mit $K : k(x) = 2g+1$, wobei g das Geschlecht von K/k bezeichnet.

7. Es sei k ein reell abgeschlossener Körper und $B = k[X_1,\ldots,X_n]$ der Polynomring in n Variablen über k. Für ein Ideal $\mathfrak{a}$ von B sei $N(\mathfrak{a}) = N_k(\mathfrak{a})$ die Gesamtheit der Nullstellen $\underline{a} = (a_1,\ldots,a_n)$ von $\mathfrak{a}$ in k^n. Ein Primideal $\mathfrak{p}$ von B nennen wir reell, wenn der Quotientenkörper von $B/\mathfrak{p}$ reell ist. Wir können dann Satz 9' folgendermassen formulieren :

Satz 9'. Sei k reell abgeschlossen und $\mathfrak{p}$ ein reelles Primideal von $k[X_1,\ldots,X_n]$. Dann ist $N(\mathfrak{p}) \neq \emptyset$.

Diesen Satz können wir nach den im Beweis von Satz 9 mittels Satz 9' gemachten Überlegungen folgendermassen verschärfen. :

Satz 9'''. Sei k reell abgeschlossen und $\mathfrak{p}$ ein reelles Primideal von $k[X_1,\ldots,X_n]$ mit Restklassenring $k[x_1,\ldots,x_n]$. Sei $\leqslant$ eine Ordnung des Quotientenkörpers K von $k[x_1,\ldots,x_n]$. Ist dann $g < 0$ für ein g aus $k[x_1,\ldots,x_n]$, so gibt es ein $\underline{a} \in N(\mathfrak{p})$ mit $g(\underline{a}) < 0$.

Man kann aber Satz 9' noch in anderer Weise erweitern. Sei $\mathfrak{a}$ ein Ideal von B. Mit $r\text{-Rad}(\mathfrak{a})$ bezeichnen wir das reelle Radikal von $\mathfrak{a}$, d. h. das Ideal von B, welches aus allen f aus B besteht, zu denen es jeweils eine ganze Zahl $n \geqslant 0$ sowie eine Quadratsumme q aus $QS(B)$ gibt mit

$$f^{2^n} + q \in \mathfrak{a} \qquad (26)$$

Mit $IN(\mathfrak{a})$ bezeichnen wir das Verschwindungsideal von $N(\mathfrak{a})$, d. h. die Menge aller f aus B, die auf $N(\mathfrak{a})$ verschwinden. Dann gilt

Satz 10 ("Reeller Nullstellensatz", vgl. [8]). Es ist

$$IN(\mathfrak{a}) = r\text{-Rad}(\mathfrak{a}) \qquad (27)$$

für jedes Ideal $\mathfrak{a}$ von B.

Für den Beweis ist im wesentlichen nur der folgende Spezialfall von (27) zu zeigen :

Aus Aus $N(\mathfrak{a}) = \emptyset$ folgt $1 \in r\text{-Rad}(\mathfrak{a})$ (28)

Dann ergibt sich die allgemeine Aussage (27) aus (28) mit dem "Trick von Rabinowitsch" analog wie im Fall des Hilbertschen Nullstellensatzes für algebraisch abgeschlossene Grundkörper. Den Nachweis für die Gültigkeit von (28) aber kann man nach einer Idee von A. Prestel (Mitteilung in Oberwolfach 1975) erbringen, in dem man folgende Ergänzung zu Satz 9 beweist :

Zusatz zu Satz 9. Es gelten dieselben Bezeichnungen und Voraussetzungen wie in Satz 9. Sei $f \in k[V]$. Ist dann $f(a) > 0$ für alle a aus V, so gibt es Quadratsummen q und q' im Ring $k[V]$, so dass sich f in der Gestalt

$$f = \frac{1 + q'}{q} \tag{29}$$

darstellen lässt.

Beweis von (28) mittels des Zusatzes zu Satz 9. Sei $\mathfrak{a}$ von $f_1,\ldots,f_r$ erzeugt. Ist $N(\mathfrak{a}) = \emptyset$, so kann man den Zusatz zu Satz 9 auf $V = k^n$ und $f = f_1^2 + \ldots + f_r^2$ anwenden. Es gibt dann $q,q' \in QS(B)$ mit $1+q' = q\,f \in \mathfrak{a}$. Folglich ist $1 \in r\text{-Rad}\,\mathfrak{a}$, womit (28) bewiesen ist.

Zum Beweis des Zusatzes zu Satz 9 ergänzen wir Abschnitt 2 durch das folgende

Lemma 5. Sei A ein kommutativer Ring mit $1 \neq 0$. Sei a ein Element von A und gelte $q\,a \neq 1+q'$ für alle q,q' aus $QS(A)$. Dann gibt es ein Primideal $\mathfrak{p}$ von A und eine Ordnung $\leqslant$ des Quotientenkörpers K von $A/\mathfrak{p}$, so dass $\bar{a} \leqslant 0$ gilt (wobei $\bar{a}$ das Bild von a in $A/\mathfrak{p}$ bezeichnet).

Beweis. Die Voraussetzung bedeutet, dass die quadratische Präordnung $T = QS(A) - aQS(A)$ das Element -1 nicht enthält. Die Behauptung folgt dann unmittelbar aus dem Lemma 3 in Abschnitt 2.

Beweis des Zusatzes zu Satz 9. Wir nehmen an, die Behauptung gelte nicht. Weil $k(V)$ reell ist, können wir dann Lemma 5 auf $A = k[V]$ und $a = f$ anwenden. Wir erhalten ein Primideal $\mathfrak{p}$ von $k[X_1,\ldots,X_n]$ mit $\mathfrak{p} \supseteq I(V)$ sowie eine Ordnung $\leqslant$ des Quotientenkörpers K von $k[X_1,\ldots,X_n]/\mathfrak{p}$ Mskr. Nach Satz 9''' gibt es dann aber ein $\underline{a} \in N(\mathfrak{a}) \subseteq V$ mit $g(\underline{a}) = f(\underline{a}) \leqslant 0$. Widerspruch.

8. Nach den vorangegangenen Erörterungen kehren wir jetzt stärker zu unserem Thema zurück und zeigen in der Tat, dass die Theorie der formal reellen Körper im Prinzip ganz in der Theorie der quadratischen Formen aufgeht. Zuvor die folgende

Definition. Jeder Ringhomomorphismus $W(k) \to Z$ des Witt'schen Ringes $W(k)$ von k in den Ring Z der ganz-rationalen Zahlen heisst eine Signatur von k.

Diese Definition erhält ihre Berechtigung aus

Satz 11 ([7]). Für einen Körper k gilt : Ordnet man jeder Ordnung P von k die zugehörige Signaturabbildung sgn_P von $W(k)$ in Z zu, so erhält man eine umkehrbar eindeutige Entsprechung zwischen der Menge aller Ordnungen von k und der Menge $Sign(k)$ aller Signaturen von k.

Ausserdem gilt

Satz 12 ([7]). Ist k reell, so vermittelt die Zuordnung $s \mapsto \text{Kern } s$ eine umkehrbar eindeutige Entsprechung zwischen der Menge $Sign(k)$ aller Signaturen von k und der Menge aller minimalen Primideale von $W(k)$. Ist k nicht reell, so ist das Fundamentalideal $I(k)$ der Formen gerader Dimension das einzige Primideal von $W(k)$.

Die Sätze 11 und 12 ergeben sich gemeinsam fast unmittelbar aus den folgenden beiden in $W(k)$ gültigen Relationen, nämlich erstens der trivialen Beziehung

$$(1 + \langle a\rangle)(1 - \langle a\rangle) = 0 \quad \text{für alle} \quad a \in k^*$$

und zweitens der Witt'schen Relation

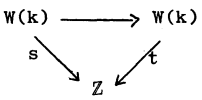
$$\langle a\rangle + \langle b\rangle = \langle a+b\rangle (1 + \langle ab\rangle) \quad \text{für alle} \quad a,b \in k^* \quad \text{mit} \quad a+b \neq 0 \tag{31}$$

Für einen detaillierten Beweis (sowie etwas über die Sätze 11 und 12 hinausgehende Information vgl. die Arbeit [7]).

Aufgrund von Satz 11 kann man statt Ordnungen von Körpern Signaturen von Körpern betrachten. Wir wollen diese Formulierungsmöglichkeit an einigen Beispielen demonstrieren. An die Stelle von Korollar 3 zu Satz 2 etwa tritt die Aussage :

$$k \text{ reell} \iff \text{Sing}(k) \neq \emptyset \tag{32}$$

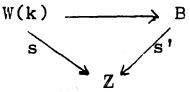
Sei K/k eine Erweiterung. Dann erscheint die Frage, unter welchen Umständen eine Ordnung von k zu einer solchen von K fortgesetzt werden kann, in einem neuen Licht. Eine Signatur t von K ist nämlich die Fortsetzung einer Signatur s von k, wenn das Diagramm



kommutativ ist. Wir schreiben dann $t|s$. An die Seite von Korollar 2 tritt dann die folgende

Feststellung. Sei K/k eine Erweiterung, $s \in \mathrm{Sign}(k)$. Dann existiert genau dann ein $t \in \mathrm{Sign}(K)$ mit $t|s$, wenn $\mathrm{Kern}(W(k) \to W(K)) \subseteq \mathrm{Kern}\, s$.

Beweis. Sei $B = \mathrm{Bild}(W(k) \to W(K))$, und sei s' der nach Voraussetzung existierende Ringhomomorphismus $B \to \mathbb{Z}$, so dass



kommutativ ist. Nun ist Kern s' eine minimales Primideal, also existiert ein minimales Primideal $\mathfrak{P}$ von $W(K)$ über Kern s'. Sei $t \in \mathrm{Sign}(K)$ die dazugehörige Signatur mit Kern $t = \mathfrak{P}$. Dann ist leicht zu sehen, dass $t|s$ gilt.

Als weiteres Beispiel erhalten wir einen zweiten

Beweis von Satz 3. Sei $s = \mathrm{sgn}_p$. Wegen Satz 7 genügt es zu zeigen, dass

$$s\, \mathrm{Tr}_{K/k}\langle 1\rangle \neq 0$$

ist. Sei $q = \mathrm{Tr}_{K/k}\langle 1\rangle$. Dann gilt $s(q) = \dim q = K : k \bmod 2$, somit $s(q) \neq 0$.

Schiesslich geben wir noch einen

Beweis von Satz 4. Im Hinblick auf die obige Feststellung ist folgendes zu zeigen: Ist $q \in \mathrm{Kern}(W(k) \to W(K))$, so folgt $\mathrm{sgn}_p(q) = 0$. Man erkennt dann, dass man dies nur für $K = k(\sqrt{a})$ mit $a \in P$ nachzuweisen braucht. Es folgt dann bekanntlich (vgl. [7]), dass q in $(\langle 1\rangle + \langle -a\rangle)\, W(k)$ liegt. Somit ist in der Tat $\mathrm{sgn}_p(q) = 0$.

In [7] wurden die Primideale des Witt'schen Ringes ursprünglich auch deshalb studiert, um eine Aussage über die Nullteiler des Witt'schen Ringes machen zu können. Das Ergebnis immerhin soll hier erwähnt und folgendermassen formuliert werden:

Satz 13 ([7]). Sei N die Menge der Nullteiler von $W(k)$. Dann gelten die folgenden Aussagen: (i) Genau dann ist $N = I(k)$, wenn $1+1$ in N liegt. (ii) Genau dann ist $1+1 \notin N$, wenn k reell und pythagoräisch ist. (iii) k ist genau dann reell und pythagoräisch, wenn N aus allen q aus $W(k)$ besteht, zu denen jeweils ein $s \in \mathrm{Sign}(K)$ mit $s(q) = 0$ existiert.

9. Der Grund dafür, dass wir den durch die Sätze 11 und 12 des vorigen Abschnittes ausgedrückten Sachverhalt in zwei getrennten Sätzen formuliert haben, ist der folgende: Es zeigt sich nämlich, dass Satz 12 für sich weitestgehender Verallgemeinerung fähig ist:

Satz 12'. Die Aussage von Satz 12 gilt für einen beliebigen zusammenhängenden kommutativen Ring A (statt k) mit $1 \neq 0$.

Dabei heisst natürlich ein kommutativer Ring A reell, wenn $\mathrm{Sign}(A) \neq \emptyset$, d.h. wenn es einen Ringhomomorphismus $W(A) \to \mathbb{Z}$ gibt (vgl. (32)). Der Beweis von Satz 12' folgt direkt aus einem (selbst allerdings nicht besonders leicht zugänglichen) Prinzip von Dress [3] in der K-Theorie. Der Satz 12' ist eine wichtige Grundlage für eine mögliche Verallgemeinerung der Artin-Schreierschen Theorie auf beliebige (zusammenhängende) kommutative Ringe (vgl. [6]). Was die Nullteiler in beliebigen Witt'schen Ringen betrifft, so kann man aufgrund von Satz 12' wenigstens soviel sagen :

Satz 13'. Sei A ein zusammenhängender kommutativer Ring mit $1 \neq 0$, und sei N die Menge der Nullteiler in $W(A)$. Mit $W(A)_t$ bezeichnen wir die Torsionsuntergruppe von $W(A)$. Dann gelten die folgenden Aussagen : (i) Genau dann ist $N = I(A)$, wenn $W(A)_t$ 2-primär und nicht-trivial ist. (ii) Genau dann ist $W(A)_t = 0$, wenn N aus allen q in $W(A)$ besteht, zu denen jeweils ein $s \in \mathrm{Sign}(A)$ mit $s(q) = 0$ existiert.

Literatur

[1] E. ARTIN und O. SCHREIER - Algebraische Konstruktion reeller Körper, Hamb. Abh. 5 (1926), 85-99.

[2] E. BECKER und K.J. SPITZLAY - Zum Satz von Artin-Schreier über die Eindeutigkeit des reellen Abschlusses eines angeordneten Körpers, Comment. Math. Helv. 50 (1975) 81-87.

[3] A. DRESS - The weak local-global principle in algebraic K-theory, Communications in Algebra 3 (1975).

[4] D. GONDARD et P. RIBENBOIM - Fonctions définies positives sur les variétés réelles, Bull. Sc. Math., 2è série, 98 (1974), 39-47.

[5] M. KNEBUSCH - On the uniqueness of real closures and the existence of real places, Comment. Math. Helv. 47 (1972) 260-269.

[6] M. KNEBUSCH - Real closures of commutative rings I, Jour. reine und angew. Math. 274/275 (1975) 61-89.

[7] F. LORENZ und J. LEICHT - Die Primideale des Wittschen Ringes, Invent. Math. 10 (1970) 82-88.

[8] P. RIBENBOIM - Le théorème de zéros pour les corps ordonnés, Séminaire d'Algèbre et théorie des nombres, Dubreil - Pisot (1970-71), Exp. 17.

[9] W. SCHARLAU - Zur Pfisterschen Theorie der quadratischen Formen, Invent. Math. 6 (1969), 307-328.

[10] T.A. SPRINGER - Sur les formes quadratiques d'indice zéro, C.R.Acad. Sci. 234 (1952) 1517-1519.

Mathematisches Institut
Westfälische Wilhelms Universität
Roxeler Strasse 64

44 MÜNSTER / WESTF.
ALLEMAGNE