EINIGE UNENTSCHEIDBARE KÖRPERTHEORIEN

Autor(en): **Ziegler, Martin**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **28 (1982)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-52241

EINIGE UNENTSCHEIDBARE KÖRPERTHEORIEN *

von Martin ZIEGLER

Professor E. Specker zum sechzigsten Geburtstag

0) EINLEITUNG

Wir konstruieren in dieser Arbeit eine Reihe von Körpern, in denen sich der Ring der ganzen Zahlen interpretieren läßt. Als Folgerung ergibt sich:

Eine endlich axiomatisierte Theorie, die einen algebraisch abgeschlossenen Körper, **R** (den Körper der reellen Zahlen) oder einen der p-adischen Körper $\mathbf{Q}_p$ als Modell hat, ist erblich unentscheidbar.

Insbesondere haben wir: (Fall **R**)

Die Theorie der euklidischen Körper ist erblich unentscheidbar.

Die Theorie der pythagoräischen Körper ist erblich unentscheidbar.

(Ein formal-reeller Körper ist *euklidisch*, wenn jedes Element Quadrat oder Negatives eines Quadrates ist, und *pythagoräisch*, wenn jede Quadratsumme Quadrat ist.)

Die Frage nach der Entscheidbarkeit der euklidischen Körper wurde 1959 von Tarski gestellt ([T]). Der Fall **R** unseres oben angegebenen Satzes wurde in [T] vermutet.

Tarskis Problem wurde bisher nur von K. Hauschild behandelt ([H 1], [H 2]). Sein Beweis für die Unentscheidbarkeit der pythagoräischen Körper ist jedoch fehlerhaft und irreparabel (siehe [C], [F]). Unsere Konstruktion verwendet einige grundsätzliche Ideen Hauschilds: „q-te Wurzeln", „Bewertungen", „schrittweise Konstruktion".

Ich danke A. Prestel und U. Henschel für ihre Unterstützung.

1) DISKUSSION DES RESULTATS

F_p sei der Körper mit p Elementen. L_p der algebraische Abschluß des rationalen Funktionenkörpers $F_p(t)$.

---

* This article has already been published in *Logic and Algorithmic*, an international Symposium in honour of Ernst Specker, Zürich, February 1980. Monographie de L'Enseignement Mathématique N° 30, Genève 1982.

Wir zeigen in den Abschnitten 2)—5) den

SATZ. q sei eine Primzahl, A eine abzählbare Struktur, L sei einer der Körper L_p $(p \neq q)$, $\mathbf{C}$, $\mathbf{R}$, $\mathbf{Q}_p$
Dann gibt es einen Körper $K \subset L$ mit

(1) A läßt sich in K interpretieren;

(2) Wenn der Zwischenkörper $H \subset L$ endlich über K ist, ist der Grad $[H : K]$ gleich 1 oder durch q teilbar.

Wenn L die Charakteristik o hat und $A = (\mathbf{Z}, +, \cdot)$, ist $\mathbf{Z}$ als Teilmenge von K definierbar.

Wir zeigen den in o) angegebenen Satz:

FOLGERUNG. Jede endliche Teiltheorie der Theorie von L ist erblich unentscheidbar.

Beweis: T sei eine endliche Teiltheorie von $Th(L)$. P sei die Menge aller von der Charakteristik von L verschiedenen Primzahlen. Zu jedem $q \in P$ wählen wir einen Körper K_q, für den (2) gilt und in dem $(\mathbf{Z}, +, \cdot)$ interpretierbar ist. Wir wählen einen Nicht-Hauptultrafilter U auf P.

$$K = \prod_{q \in P} K_q / U$$

ist dann relativ algebraisch abgeschlossen in $L^p/_U$. Daraus folgt nun $K \equiv L$. (Die hier gebrauchte (Modell-) Theorie der algebraisch-, reell- und p-adisch abgeschlossenen Körper findet man in [CK], [M], [K], [AK].)

K ist somit ein Modell von T, folglich ist auch einer der Körper K_q ein Modell von T (denn T ist endlich). T hat also ein Modell, in dem der Ring der ganzen Zahlen interpretierbar ist. Damit folgt die Behauptung aus [TMR].

Um weitergehende Folgerungen aus unserem Satz zu gewinnen, definieren wir eine Reihe von elementaren Theorien. Den Nachweis, daß diese Theorien wirklich „elementar" sind überlassen wir dem Leser. (Man beachte, daß die „p-Bewertung" in Modellen von $T^H_{p,q}$ elementar definierbar ist.)

$T^A_{p,q}$ = die Theorie der Körper der Charakteristik p, in denen der Grad jedes irreduziblen Polynoms = 1 oder durch q teilbar ist. (p prim oder = o);

T^R_2 = die Theorie der formal reellen Körper, in denen der Grad jedes irreduziblen Polynoms = 1 oder gerade ist;

T_q^R = die Theorie der formal reellen Körper mit:

a) der Grad jedes irreduziblen Polynoms, das in einer formal reellen Erweiterung eine Nullstelle hat, ist = 1 oder durch q teilbar;

b) der Körper liegt dicht in seinem reellen Abschluß. ($q \neq 2$);

$T_{p,q}^H$ = die Theorie der formal p-adischen Körper mit:

a) der Grad jedes irreduziblen Polynoms, das in einer formal p-adischen Erweiterung eine Nullstelle hat, ist = 1 oder durch q teilbar;

b) der Körper liegt dicht in seinem p-adischen Abschluß.

Man kann sich leicht überlegen, daß alle diese Theorien (wobei noch für $T_{p,q}^A$ $p \neq q$ gefordert sei), einen der im Satz angegebenen Körper K als Modell haben. Also gilt die

FOLGERUNG. — Die Theorien $T_{p,q}^A$ ($p \neq q$), T_q^R, $T_{p,q}^H$ sind erblich unentscheidbar.

Ohne Beweis sei noch eine Reihe von Bemerkungen angefügt:

Jede endliche Theorie, die einen der betrachteten Körper L als Modell hat, ist für genügend großes q Teiltheorie einer der Theorien $T_{p,q}^A$, T_q^R, T_q^H. Die Theorie der euklidischen Körper ist für $q \neq 2$ in T_q^R enthalten.

Ein Körper K der Charakteristik p ist ein Modell von $T_{p,q}^A$ *gdw.* jedes Polynom aus $K[X]$, dessen Grad nicht durch q teilbar ist, eine Nullstelle in K hat *gdw.* der Grad jeder endlichen Erweiterung von K eine q-Potenz ist.

Ein formal reeller Körper ist ein Modell von T_2^R *gdw.* jedes Polynom ungeraden Grades eine Nullstelle hat *gdw.* der Grad jeder endlichen formal reellen Erweiterung eine 2-Potenz ist.

$(R, <)$ sei dicht im reell abgeschlossenen Körper $(L, <)$. Dann ist R genau dann ein Modell von T_q^R, wenn der Grad jedes irreduziblen Polynoms, welches das Vorzeichen wechselt, = 1 oder durch q teilbar ist.

Der bewertete Körper (H, w) sei dicht im p-adisch abgeschlossenen Körper (L, v), $w \subset v$. Dann ist H genau dann ein Modell von $T_{p,q}^H$, wenn der Grad jedes irreduziblen Polynoms, dass die Voraussetzung von Hensels Lemma erfüllt, = 1 oder durch q teilbar ist.

Offene Fragen:

$T_{q,q}^A$ ist Untertheorie der (entscheidbaren) Theorie der separabel abgeschlossenen Körper der Charakteristik q (siehe [E]). Ist $T_{q,q}^A$ oder $T_{q,q}^A + \forall x \exists y \;\; y^q = x$ entscheidbar?

Für $q_1 \neq q_2$ ist $T^A_{p,q_1} + T^A_{p,q_2}$ die Theorie der algebraisch abgeschlossenen Körper der Charakteristik p. Für $q \neq 2$ ist $T^R_2 + T^R_q$ die Theorie der reell abgeschlossenen Körper. Sind für verschiedene q_i, $n \geqslant 1$, die Theorien $T^H_{p,q_o} + \ldots + T^H_{p,q_n}$ und $(q_i \neq 2)$ $T^R_{q_o} + \ldots + T^R_{q_n}$ entscheidbar?

K ist erblich quadratisch abgeschlossen, wenn jede algebraische Erweiterung von K quadratisch abgeschlossen ist. Die Theorie der erblich quadratisch abgeschlossenen Körper der Charakteristik p ist als Untertheorie von $T^A_{p,q}$, $q \neq 2$, erblich unentscheidbar. Ist die Theorie der erblich euklidischen Körper entscheidbar?

2) Konstruktion von M

Wir halten ab jetzt q, A und L wie in der Voraussetzung des Satzes fest. F sei der relative algebraische Abschluß des Primkörpers von L.

Lemma. Es gibt eine Teilmenge M von F, so daß sich A in (F, M) interpretieren läßt und

(3) $o \in M$; der Index der von M erzeugten additiven Untergruppe von F ist unendlich.

Beweis: Zunächst bemerken wir daß F unendliche Erweiterung des Primkörpers ist.

Im Fall $(\mathbf{Z}, +, \cdot) = A$, o = Charakteristik von L, setzen wir $M = \mathbf{Z}$.

Sonst können wir annehmen, daß $A = (A, R)$, R symmetrisch und irreflexiv. Denn jede Struktur läßt sich in einem Graphen interpretieren. A sei durch $a_0, a_1, \ldots$ ohne Wiederholung aufgezählt. Wir fassen F als Vektorraum über seinem Primkörper auf. $B = \{b_0, b_1, \ldots\}$ sei Basis eines unendlichdimensionalen Untervektorraums von unendlicher Kodimension. Wir übertragen R auf B: $S(b_i, b_j)$ gdw. $R(a_i, a_j)$, also $(A, R) \cong (B, S)$. c_1, c_2 seien linear unabhängig über B.

Wir setzen jetzt

$$M = \{o\} \cup B \cup \{c_1 + b_i \mid i \in \mathbf{N}\}$$
$$\cup \{c_2 + b_i \mid i \in \mathbf{N}\} \cup \{b_i + b_j \mid S(b_i, b_j)\}$$

Dann können wir B und S (mit Parametern c_1, c_2) definieren:

$$B = \{b \in M \mid c_1 + b \in M,\ c_2 + b \in M\}$$
$$S = \{(b, c) \mid b \in B,\ c \in B,\ b + c \in M,\ b \neq c\}$$

3) KONSTRUKTION VON K

$t \in L$ sei transzendent über F.

Wir wollen $K \subset L$ als algebraische Erweiterung von $F(t)$ so konstruieren, daß neben (2)

$$F = \{a \in K \mid \forall\, b \in L^q (1 + b \in K^q \,\&\, a^q + b^{-1} \in K^q) \to b \in K^q\}$$

und

$$M = \{r \in F \mid \forall\, r_1,\ r_2 \in F (r_1 \neq r_2 \,\&\, r_1 + r_2 = r \Rightarrow (t^q - r_1 \in F^* \cdot K^q \text{ oder } t^q - r_2 \in F^* \cdot K^q))\}$$

$(F^* = F \setminus \{o\})$

K gewinnen wir als Vereinigung einer Folge

$$F(t) = E_0 \subset E_1 \subset E_2 \subset \ldots \subset L$$

von endlichen Erweiterungen von $F(t)$. Um die q-ten Potenzen zu kontrollieren, wählen wir gleichzeitig eine Folge

$$\phi = S_0 \subset S_1 \subset S_2 \ldots$$

von endlichen Teilmengen $S_i \subset E_i \cap L^q$ mit dem Ziel, daß

$$(K \cap L^q) \setminus K^q = \left(\bigcup_{i \in \mathbf{N}} S_i \right)$$

Um die gewünschten Darstellungen von M und $(K \cap L^q) \setminus K^q$ nicht schon durch falsche Wahl von (E_i, S_i) unmöglich zu machen, fordern wir für alle i

(4) Es gibt eine Familie $(v_s)_{s \in S_i}$ von Bewertungen $v_s : E_i \to G_{v_s}$, v_s trivial auf F, mit:

(4.1) (in G_{v_s}) ist $v_s(s)$ nicht durch q teilbar, $(s \in S_i)$

(4.2) für alle $r_1,\ r_2 \in F,\ r_1 + r_2 \in M,\ r_1 \neq r_2$:

$\forall s \in S_i$ q teilt $v_s(t^q - r_1)$

oder

$\forall s \in S_i$ q teilt $v_s(t^q - r_2)$

Wir beginnen mit einer Aufzählung $a_0, a_1, \ldots$ aller $a \in L$, die algebraisch über $F(t)$ sind. Jedes Element der Folge soll unendlich oft vorkommen.

Sei (E_i, S_i) schon konstruiert. Wir unterscheiden vier Fälle:

$i = 4n$. Es gibt zwei Fälle

a) q teilt $[E_i(a_n): E_i]$. Wir setzen dann $(E_{i+1}, S_{i+1}) = (E_i, S_i)$

b) q teilt $[E_i(a_n): E_i]$ nicht. Dann setzen wir

$$(E_{i+1}, S_{i+1}) = (E_i(a_n), S_i).$$

Zum Nachweis von (4) verwenden wir

LEMMA 1. H_2 sei eine endliche Erweiterung des Körpers H_1, $q \nmid [H_2: H_1]$ $v_1: H_1 \to G_{v_1}$ sei eine diskrete Bewertung. Dann gibt es auf H_2 eine Fortsetzung v_2 von v_1 mit $q \nmid (G_{v_2}: G_{v_1})$.

Beweis: Wir können annehmen, daß H_2 separabel oder rein inseparabel über H_1 ist. Im separablen Fall gilt

$$[H_2: H_1] = \sum_i (G_{v_2^i}: G_{v_1}) f_i$$

wobei die v_2^i alle Fortsetzungen von v_1 auf H_2 durchlaufen und f_i der Grad der jeweiligen Restklassenkörpererweiterung ist. q kann also nicht alle $(G_{v_2^i}: G_{v_1})$ teilen.
Wenn H_2 rein inseparabel über H_1 ist, gibt es genau eine Fortsetzung v_2. $(G_{v_2}: G_{v_1})$ ist eine p-Potenz, $p \neq q$.

Wenn nun die $v_s: E_i \to G_{v_s}$, $s \in S_i$, (4.1) und (4.2) erfüllen, wählen wir Fortsetzungen $\bar{v}_s: E_{i+1} \to G_{\bar{v}_s}$ mit $q \nmid (G_{\bar{v}_s}: G_{v_s})$. Die $\bar{v}_s$, $s \in S_i$ erfüllen wieder (4.1) und (4.2).

$i = 4n+1$. Es gibt drei Fälle

a) $a_n \notin E_i$ oder $a_n \notin L^q$. Wir setzen dann $(E_{i+1}, S_{i+1}) = (E_i, S_i)$.
Wenn $a_n \in E_i \cap L^q$, wählen wir $v_s: E_i \to G_{v_s}$, $s \in S_i$ mit (4).

b) Es gibt ein $s \in S_i$, für das q nicht $v_s(a_n)$ teilt. Setze in diesem Fall

$$(E_{i+1}, S_{i+1}) = (E_i, S_i \cup \{a_n\}).$$

(4) gilt, wenn wir v_s für v_{a_n} nehmen.

c) q teilt alle $v_s(a_n)$, $s \in S_i$. Wir setzen

$$(E_{i+1}, S_{i+1}) = (E_i(\sqrt[q]{a_n}), S_i), \text{ wobei } \sqrt[q]{a_n} \in E_i, \text{ falls } a_n \in E_i^q$$

Daß (4) gilt, folgt aus

LEMMA 2. q sei verschieden von der Charakteristik des Restklassenkörpers des bewerteten Körpers (H, v); es sei $a \in H \setminus H^q$ und $v(a)$ durch q teilbar. Dann gibt es eine Fortsetzung w von v auf $H(\sqrt[q]{a})$ mit $G_v = G_w$.

Beweis: Zunächst bemerken wir, daß $q = [H(\sqrt[q]{a}): H]$. Es gibt ein $c \in H$ mit $v(c^q) = v(a)$. Wenn die Restklasse von $c^q a^{-1}$ im Restklassenkörper keine q-Potenz ist, ist $G_w = G_v$ für alle Fortsetzungen w von v (Gradungleichung). Sonst liegt die q-te Wurzel von $c^q a^{-1}$ in der henselschen Hülle von (H, v). Wir gewinnen w durch Einbettung von $H(\sqrt[q]{a})$ in die henselsche Hülle.

$i = 4n+2$. Es gibt zwei Fälle

a) $a_n \notin E_i$ oder $a_n \in F$. Wir setzen $(E_{i+1}, S_{i+1}) = (E_i, S_i)$

b) $a_n \in E_i \setminus F$.

Es gibt dann eine auf F triviale Bewertung v von E_i, für die $v(a_n)$ negativ ist. (4) möge von $(v_s)_{s \in S_i}$ erfüllt sein. Zuerst erweitern wir E_i zu einem Körper E, für den (4.2) für $v, v_s, (s \in S_i)$ gilt:
Wenn (4.2) schon in E_i für $v, v_s, (s \in S_i)$ gilt, bleiben wir bei $E = E_i$. Sonst muß es ein $r \in F$ geben mit

$$q \text{ teilt nicht } v(t^q - r)$$
$$\forall\, s \in S_i \; q \text{ teilt } v_s(t^q - \mathrm{r}).$$

(Man beachte: Es gibt höchstens ein $r \in F$, für das q $v(t^q - r)$ nicht teilt.) Wir brauchen noch

LEMMA 3. $L = L^q \cdot F$

Beweis: Sei $a \in L$. Wir suchen ein $b \in F^*$ mit $ab^{-1} \in L^{\varphi}$. Wenn L algebraisch- oder reell abgeschlossen ist, finden wir $b \in \{1, -1\}$. Im Fall $L = \mathbf{Q}_p$ bemerken wir, daß c in $\mathbf{Q}_p$ eine q-te Potenz ist, wenn $w(c - d^q) \geqslant w(c) + 3$ (Hensels Lemma, w ist die p-adische Bewertung von $\mathbf{Q}_p$). Wir wählen also $b \in F$ so, daß $w(a-b) \geqslant w(a) + 3$. Dann ist $w(ab^{-1} - 1) \geqslant w(ab^{-1}) + 3$.

Das Lemma liefert nun ein $d \in F^*$ mit $d(t^q - r) \in L^q$. Wir setzen $E = E_i(\sqrt[q]{d(t^q - r)})$. $\bar{v}$ sei irgendeine Fortsetzung von v auf E, die Fortsetzungen $\bar{v}_s$ der v_s seien nach Lemma 2 gewählt. (E, S_i) erfüllt also (4) und (4.2) gilt sogar für $\bar{v}, \bar{v}_s, (s \in S_i)$.

Schließlich bestimmen wir ein $b \in E$ mit

$b,\ 1+b,\ a_n^q + b^{-1} \in L^q$

c teilt $\bar{v}(1+b),\ \bar{v}(a_n^q+b^{-1}),\ \bar{v}_s(1+b),\ \bar{v}_s(a_n^q+b^{-1}),\ (s \in S_i)$

$\bar{v}(b)$ ist das kleinste positive Element von $G_{\bar{v}}$,

und setzen

$$(E_{i+1}, S_{i+1}) = \left(E\left(\sqrt[q]{1+b}, \sqrt[q]{a_n^q+b^{-1}}\right), S_i \cup \{b\}\right).$$

Wenn wir $\bar{v}$, $\bar{v}_s$ nach Lemma 2 fortsetzen, sehen wir, daß (4) gilt. ((4.2) ist wegen der Wahl von E erfüllt.)

Es bleibt noch b zu finden.

Die Bewertungen $\bar{v}, \bar{v}_s$ sind unabhängig. Der Approximationssatz liefert uns also ein $b \in E$ mit

$$q \text{ teilt } \bar{v}_s(b),\ \bar{v}_s(b) < o,\ -\bar{v}_s(a_n^q);\ (s \in S_i, \bar{v} \neq \bar{v}_s)$$
$$\bar{v}(b) = \text{kleinstes positives Element von } G_{\bar{v}}.$$

Man rechnet jetzt leicht nach, daß alle Werte $\bar{v}(1+b)$, $\bar{v}(a_n^q+b^{-1})$, $\bar{v}_s(1+b)$, $\bar{v}_s(a_n^q+b^{-1})$ durch q teilbar sind. Wenn $L = L_p$, $\mathbf{C}$ oder $q \neq 2$ und $L = \mathbf{R}$ ist auch klar, daß $b, 1+b, a_n^q+b^{-1} \in L^q$. In den anderen Fällen müssen wir b noch genauer bestimmen:

$L = \mathbf{R}$, $q = 2$: Wir wählen b so, daß zusätzlich $b > 0$.

$L = \mathbf{Q}_p$: w sei die p-adische Bewertung von L, $d \in \mathbf{Q}^q$ mit $w(d) \geqslant 3$ und $w(a_n^q d) \geqslant 3$. Mit dem Approximationssatz wählen wir nun b so, daß zusätzlich $w(d-b) \geqslant w(d) + 3$. Dann ist.

$w(b-d) \geqslant w(b) + 3 \Rightarrow b \in L^q$,

$w\big((1+b)-1\big) = w(d) \geqslant 3 \Rightarrow 1 + b \in L^q$,

$w\big((a_n^q+b^{-1})-b^{-1}\big) \geqslant w(b^{-1}) + 3 = w(a_n^q+b^{-1}) + 3$
$\Rightarrow a_n^q + b^{-1} \in L^q$.

$i = 4n+3$. Wir unterscheiden zwei Fälle

a) $a_n \in M$ oder $a_n \notin F$. Hier setzen wir $(E_{i+1}, S_{i+1}) = (E_i, S_i)$

b) $a_n \in F \setminus M$.

(4) sei durch $(v_s)_{s \in S_i}$ erfüllt. Wir beachten, daß

$$B = \left\{r \in F \mid \exists\, s \in S_i \quad q \text{ teilt nicht } v_s(t^q - r)\right\}$$

endlich ist.

Für $r \in F^*$ hat $t^q - r$ keine mehrfachen Faktoren (in $F[t]$). Es gibt also eine auf F triviale Bewertung $\bar{v}_r$ von $F(t)$, für die $\bar{v}_r(t^q - r)$ das kleinste positive Element von $G_{\bar{v}_r}$ ist. Wir wählen für jedes r eine Fortsetzung w_r von $\bar{v}_r$ auf E_i. Dann ist $G_{\bar{v}_r} = G_{w_r}$ für fast alle r. Die Menge

$$C = \{r \in F^* \mid q \text{ teilt } w_r(t^q - r)\}$$

ist also endlich. Wir bemerken noch, daß $w_r(t^q - r') = 0$, wenn $r \neq r'$.
Wir wählen jetzt $r_1 \in F$ so, daß $r_1 \neq 0$, a_n, $2r_1 \neq a_n$ und r_1 in keiner der Mengen

$$C,\ a_n - C,\ M - B,\ a_n - (M - B)$$

liegt. Es sei $r_2 = a_n - r_1$. Lemma 3 liefert uns $s_i \in F^*$ mit $s_i(t^q - r_i) \in L^q$. Wir setzen

$$(E_{i+1}, S_{i+1}) = \left(E_i, S_i \cup \{s_1(t^q - r_1), s_2(t^q - r_2)\}\right).$$

Es muß noch (4) gezeigt werden.
Weil q $w_{r_1}(t^q - r_1)$ und $w_{r_2}(t^q - r_2)$ nicht teilt, gilt zunächst (4.1) für die Bewertungen w_{r_1}, w_{r_2}, v_s, $(s \in S_i)$. Um (4.2) zu zeigen, seien $\bar{r}_1 \neq \bar{r}_2 \in F$, $\bar{r}_1 + \bar{r}_2 \in M$ gegeben. Es ist dann z.B. für alle $s \in S_i$ $v_s(t^q - \bar{r}_1)$ durch q teilbar. Wenn auch $w_{r_1}(t^q - \bar{r}_1)$ und $w_{r_2}(t^q - \bar{r}_1)$ durch q teilbar sind, sind wir fertig. Sei also z.B. $w_{r_1}(t^q - \bar{r}_1)$ nicht q-teilbar. Dann ist $r_1 = \bar{r}_1$, $r_i \neq \bar{r}_2$ und $\bar{r}_2 \in M - r_1$. Folglich ist $w_{r_i}(t^q - \bar{r}_2) = 0$, und alle $v_s(t^q - \bar{r}_2)$, $(s \in S_i)$, sind durch q teilbar.
Damit ist die Konstruktion von K abgeschlossen.

4) Die Eigenschaften von K

Wir zeigen in diesem Abschnitt (2) und

(5) $(K \cap L^q) \setminus K^q = \left(\bigcup_{i \in \mathbf{N}} S_i\right)$

(5'). $K \setminus F^* \cdot K^q = F^* \cdot \left(\bigcup_{i \in \mathbf{N}} S_i\right)$

(6) $F = \{a \in K \mid \forall\, b \in L^q \quad (1 + b \in K^q \,\&\, a^q + b^{-1} \in K^q) \Rightarrow b \in K^q\}$

(6') $F = \{a \in K \mid \forall\, b \in K \quad (1 + b \in K^q \,\&\, a^q + b^{-1} \in K^q) \Rightarrow b \in F^* \cdot K^q\}$

(7) $M = \{r \in F \mid \forall\, r_1, r_2 \in F\ (r_1 \neq r_2 \,\&\, r_1 + r_2 = r) \Rightarrow (t^q - r_1 \in F^* \cdot K^q$ oder $t^q - r_2 \in F^* \cdot K^q)\}$

Beweis von (2): Sei $K \subset H \subset L$ und H endlich über K. Wir wollen zeigen, daß q den Grad $[H : K]$ teilt. Wir können $H = K(a)$ annehmen. Für beliebig große n ist $a = a_n$. Wir wählen n so groß, daß

$$[E_{4n}(a) : E_{4n}] = [K(a) : K].$$

In der Konstruktion tritt bei $i = 4n$ der Fall a) ein. Also teilt q

$$[E_{4n}(a) : E_{4n}].$$

Beweis von (5) und (5'):

„$\supset$" Sei $a \in F^* \cdot K^q$. Für alle genügend großen i ist dann $a \in F^* \cdot E_i^q$ und $v(a)$ für alle auf F trivialen v durch q teilbar. Nach (4.1) liegt a nicht in $F^* \cdot S_i$.

„$\subset$" Sei $a \in K \setminus F^* \cdot K^q$. Nach Lemma 3 wählen wir $f \in F^*$ mit $\bar{a} = af \in L^q$. Wir haben jetzt $\bar{a} \in (K \cap L^q) \setminus K^q$.

Es sei $a_n = \bar{a}$ und n so groß, daß $\bar{a} \in E_{4n+1}$. In der Konstruktion tritt bei $i = 4n+1$ der Fall b) ein. Also ist $\bar{a} \in S_{i+1}$. Daraus folgt $a \in F^* \cdot S_{i+1}$.

Beweis von (6) und (6'):

„$\subset$" Sei $a \in F$. Für ein $b \in K$ sei $1 + b \in K^q$ und $a^q + b^{-1} \in K^q$. i sei so groß daß $1 + b \in E_i^q$ und $a^q + b^{-1} \in E_i^q$. v sei eine auf F triviale Bewertung von E_i. Wenn $v(b) > 0$, ist $v(b) = -v(a^q + b^{-1})$ durch q teilbar. Wenn $v(b) < 0$, ist $v(b) = v(1+b)$ durch q teilbar. Weil also $v(b)$ immer durch q teilbar ist, ist nach (4) $b \notin F^* \cdot S_i$. (5') ergibt $b \in F^* \cdot K^q$. Wenn $b \in L^q$, folgt aus (5), daß $b \in K^q$.

„$\supset$" Sei $a \in K \setminus F$. n sei so groß, daß $a \in E_{4n+2}$, und es sei $a = a_n$. In der Konstruktion tritt bei $i = 4n+2$ der Fall b) ein. In S_{i+1} gibt es dann ein b mit $1 + b$, $a^q + b^{-1} \in E_{i+1}^q$. Wir haben also

$$b \in L^q,\ 1 + b \in K^q,\ a^q + b^{-1} \in K^q,\ b \notin F^* \cdot K^q.$$

Beweis von (7):

„$\subset$" Sei $r_1 + r_2 \in M$, $r_1 \neq r_2$. Wenn die $t^q - r_1$ beide nicht in $F^* \cdot K^q$ sind, ist nach (5') $t^q - r_1$, $t^q - r_2 \in F^* \cdot S_i$ für genügend großes i. Das widerspricht aber (4).

„$\supset$" Sei $r = a_n \in F \setminus M$. In der Konstruktion tritt bei $i = 4n + 3$ der Fall b) ein. Es gibt dann $r_1 \neq r_2 \in F$, $r_1 + r_2 = r$ und $s_i \in F^*$, für die $s_1(t^q - r_1)$, $s_2(t^q - r_2) \in S_{i+1}$. Also nach (5') $t^q - r_1$, $t^q - r_2 \notin F^* \cdot K^q$.

5) Beweis des Satzes

Wir haben noch zu zeigen, daß A in K interpretierbar ist. Wegen (7), genügt es zu zeigen, daß F in K definierbar ist. Wir unterscheiden drei Fälle:

$$L = L_p, \mathbf{C} \text{ oder } q \neq 2 \text{ und } L = \mathbf{R}\,.$$

Dann ist $K \subset L^p$ und wir haben nach (6)

$$F = \{a \in K \mid \forall\, b \in K\,(1 + b \in K^q \,\&\, a_q + b^{-1} \in K^q) \Rightarrow b \in K^q\}$$

$L = \mathbf{R}$, $q = 2$.

Dann ist $F^* \cdot K^q = K^q \cup -K^q$. Und wir haben mit (6′)

$$F = \{a \in K \mid \forall\, b \in K\,(1 + b \in K^q \,\&\, a^q + b^{-1} \in K^q) \Rightarrow b \in K^q \cup -K^q\}$$

$L = \mathbf{Q}_p$.

Wir erhalten aus (6) eine Definition von F, wenn wir $K \cap L^q$ in K definieren können. Weil aber $\mathbf{Q}$ dicht in $\mathbf{Q}_p$ ist, ist nach Hensels Lemma

$$c \in L^q \text{ gdw. es gibt } d \in K \text{ (oder: } \mathbf{Q}\text{) mit } w\,(c - d^q) \geqslant w\,(c) + 3\,.$$

Es genügt also die p-adische Bewertung w in K elementar zu beschreiben: Wenn r relativ prim zu p ist, ist für alle $c \in L$

$$w\,(c) \geqslant o \quad \text{gdw.} \quad 1 + pc^r \in L^r\,.$$

Wenn r eine von q und p verschiedene Primzahl ist, gewinnen wir daraus mit (2) für alle $c \in K$

$$w\,(c) \geqslant o \quad \text{gdw.} \quad 1 + pc^r \in K^r\,.$$

LITERATUR

[AK] Ax, Kochen. Diophantine problems over local fields, I, II, III. *Amer. J. of Math. 87, 88* (1965, 1966).

[C] Cherlin, G. *Mathematical reviews 50* (1975), 9567. (Resprechung von H1).

[CK] Chang-Keisler. *Model Theory*. Alsterdam (1973).

[E] Ersov, Ju. L. Fields with a solvable theory. *Doklady Akademii Nauk SSSR 174* (1967), 19-20, (englische Übersetzung: *Soviet math. 8* (1967), 575-576.

[F] Ficht, H. *Zur Theorie der pythagoräischen Körper*. Diplomarbeit, Konstanz (1979).

[H1] HAUSCHILD, K. Rekursive Unentscheidbarkeit der Theorie der pythagoräischen Körper. *Fundamenta M.82* (1974), 191-197.

[H2] —— Addendum, betreffend die rekursive Unentscheidbarkeit der Theorie der pythagoräischen Körper. *Preprint*, Berlin (1977).

[K] KOCHEN, S. Integer valued rational functions over the p-adic numbers. A p-adic analogue of the theory of real fields. *Proc. Symp. pure Math. XII* (Number theory) (1969), 57-73.

[L] LANG, S. *Algebra.* Reading (1965).

[TMR] TARSKI, MOSTOWSKI, ROBINSON. *Undecidable Theories.* Amsterdam (1953).

[T] TARSKI. What is elementary geometry ? *Symp. axiomatic method*, Amsterdam (1959), 16-29.

[M] MACINTYRE, A. Definable subsets of p-adic fields. *Journal of Symbolic Logic 41* (1976).

(Reçu le 9 février 1981)

Martin Ziegler

Universität Bonn
Mathematisches Institut
Beringstrasse 4
D-5300 Bonn