Beiträge zur Algebra und Geometrie
8 (1979), 115–123

Der Cohensche Eliminationssatz in positiver Charakteristik

TADEUSZ MOSTOWSKI und GERHARD PFISTER

1. Einleitung

In diesem Artikel wollen wir den Cohenschen Eliminationssatz (vgl. [1]) für henselsche diskrete Bewertungsringe beliebiger Charakteristik beweisen. Der Beweis folgt der Idee von P. J. COHEN, der das entsprechende Resultat in Charakteristik 0 bewiesen hat.

Für analoge Betrachtungen im n-dimensionalen Fall verweisen wir auf [4] und [5]. Es sei I ein exzellenter henselscher diskreter Bewertungsring mit perfektem Restklassenkörper k, K der Quotientenkörper von I. Mit v wollen wir die Bewertung von I bezeichnen und mit p ein fest gewähltes Primelement (d. h. $v(p) = 1$) aus I. Es sei weiterhin $R_k = I/p^k$.

Wenn K die Charakteristik $t > 0$ hat, ist I ein endlicher I^t-Modul, da I exzellent ist und k perfekt (vgl. [6]). In diesem Fall ist $\hat{I} = k[[p]]$ und $1, p, \ldots, p^{t-1}$ eine Basis von $\hat{I}$ über $\hat{I}^t$. Damit ist auch $1, p, \ldots, p^{t-1}$ eine Basis von I über I^t und eine Basis von K über K^t.

Um den Satz von COHEN formulieren zu können, müssen wir auch einige Bezeichnungen aus der mathematischen Logik einführen: Wir führen unsere Untersuchungen in K, R_k und $\mathbf{Z}$ (dem Ring der ganzen Zahlen), deshalb führen wir K-Variable ein, die wir gewöhnlich mit $x, y, \ldots, u, v, \ldots$ bezeichnen und stets als Elemente von K interpretieren; wir führen analog R_k-Variable ein (mit den gleichen Bezeichnungen) und $\mathbf{Z}$-Variable, die wir gewöhnlich mit $n, m, \ldots$ bezeichnen. Wir werden nun die atomaren Formeln beschreiben, aus denen sich unter Benutzung der logischen Operationen &, $\vee$, $\sim$, $\Rightarrow$ und der Quantifikatoren $\forall$, $\exists$ die uns interessierenden Elementarformeln zusammensetzen lassen.

$x + y = z, \quad x \cdot y = z$	für K-Variable oder R_k-Variable x, y, z
$n + m = k, \quad n \leqq m$	für $\mathbf{Z}$-Variable n, m, k
$v(x) = n$	für eine K-Variable oder eine R_k-Variable x und eine $\mathbf{Z}$-Variable n

(Einer derartigen Formel wird stets eine Formel vorangestellt sein, aus der hervorgeht, daß $x \neq 0$ ist.)

$[x]_k = y$	für eine K-Variable oder eine R_l-Variable x und eine R_k-Variable y
$[x]_k = 0$	für eine K-Variable oder eine R_l-Variable x und eine $\mathbf{Z}$-Variable k

(hierbei bezeichnet $[x]_k$ die Klasse von x in R_k; Formeln dieser Art wird stets eine Formel vorangestellt sein, aus der hervorgeht, daß im Fall einer K-Variablen x stets $x \in I$ ist.)

$B_i(u) = u_i$ falls Char $(K) = t > 0$ ist

$i = 0, \ldots, t-1$ für K-Variable $u, u_0, \ldots, u_{t-1}$, wobei $u = \sum_{i=0}^{t-1} u_i p^i$, $u_i \in K^t$ ist.

Wir wollen mit $\mathbf{C}$ die Klasse der elementaren Formeln bezeichnen, die wir durch Zusammensetzen dieser atomaren Formeln unter Benutzung der logischen Operationen &, $\vee$, $\sim$, $\Rightarrow$ und der Quantifikatoren $\forall$, $\exists$ erhalten.
Unter einer gebundenen Variablen wollen wir im folgenden wie üblich solche Variable verstehen, die unter einem Quantifikator vorkommen; die übrigen nennen wir freie Variable.

1.1. **Satz von COHEN.** *Jede Formel Φ aus $\mathbf{C}$ ist äquivalent zu einer Formel Ψ aus $\mathbf{C}$, so daß in Ψ nur solche $\mathbf{Z}$- und K-Variable vorkommen wie auch in Φ und alle gebundenen Variablen von Ψ R_k-Variable sind.*

Mit Hilfe dieses Satzes kann jede elementare Aussage über K zu Aussagen über (endlich viele) Ringe R_k reduziert werden.

Beispiel. Es sei $F(U) = a_0 + a_1 U + \cdots + a_m U^m$ ein Polynom aus $I[U]$, dessen Diskriminannte δ nicht verschwindet; es sei $\Delta = \delta \cdot a_m$ und $r = v(\Delta)$. Dann folgt aus dem Newtonschen Lemma (vgl. [3]), daß $\exists\, u\, F(u) = 0\ \&\ v(u) \geqq 0$ äquivalent zur Formel

$$\exists\, w,\ [a_0]_{2r+1} + [a_1]_{2r+1}\, w + \cdots + [a_m]_{2r+1}\, w^m = 0$$

ist, wobei u eine K-Variable ist und w eine R_{2r+1}-Variable.
Für Polynome in mehreren Variablen kann man dieses Verfahren nicht so ohne weiteres anwenden. Wenn nämlich die Koeffizienten der obigen Gleichung von Parametern abhängen, hängt δ von Parametern ab, und wir würden als äquivalente Formel unendlich viele Bedingungen erhalten.

2. Beweis des Satzes von Cohen

2.1. **Definition.** Es sei $f(x_1, \ldots, x_r)$ eine Funktion (wobei die Variablen x_i K-, R_k- bzw. $\mathbf{Z}$-Variable sein können, die Werte von f in K, R_k oder $\mathbf{Z}$ liegen können). f heißt *effektiv*, wenn ein Algorithmus existiert, der jeder Formel $\Phi(t, y_1, \ldots, y_s)$ eine Formel $\Psi(x_1, \ldots, x_r, y_1, \ldots, y_s)$ zuordnet, so daß

(1) $\Phi(f(x_1, \ldots, x_r), y_1, \ldots, y_s) \Leftrightarrow \Psi(x_1, \ldots, x_r, y_1, \ldots, y_s)$

ist und

(2) Ψ dieselben freien K-Variablen und $\mathbf{Z}$-Variablen hat wie Φ.

Ein Beispiel soll den Begriff der effektiven Funktion veranschaulichen: Wenn wir über dem Körper der reellen Zahlen die Klasse der Formeln betrachten, die man aus den ersten beiden der zuvor angegebenen Atomformeln erhält, so ist die Funktion $f(x) = \sqrt{x}$ nicht in dieser Klasse. Aussagen über $f(x)$ können jedoch auf elementare Aussagen zurückgeführt werden (z. B. ist $a \geqq \sqrt{x}$ genau dann erfüllt, wenn $a \geqq 0$ und $a^2 \geqq x$ ist).
Ein wichtiges Beispiel für effektive Funktionen sind die Nullstellen eines gegebenen Polynoms als Funktion der Koeffizienten. Wir werden später darauf eingehen.

Ein weiterer wichtiger Begriff für die folgenden Untersuchungen ist der der Überdeckung von K durch Zellen:

2.2. Definition

(1) Eine *unendliche Zelle* ist eine Teilmenge von K der Form $\{x, v(x) \leqq \alpha\}$ für ein $\alpha \in \mathbf{Z}$.

(2) Eine *endliche Zelle* ist eine Teilmenge von K der Form

$\{x, x = x_0 + u, v(u) \geqq \alpha\}$

für ein $\alpha \in \mathbf{Z}$ und ein $x_0 \in K$.

(3) Die *Daten einer Zelle* sind die Zahl α und ein ausgewähltes Element x_0 (das natürlich nicht eindeutig bestimmt ist).

(4) Eine *Überdeckung von K* ist eine endliche Zahl von Zellen, unter denen genau eine unendliche Zelle ist und deren Vereinigung K ist.

(5) Es sei $\mathscr{C}$ eine Überdeckung von K, $C \in \mathscr{C}$ eine Zelle. Wir sagen, $x \in C$ *gehört echt zu C*, wenn $x \notin C'$ ist für alle von C verschiedenen Zellen $C' \in \mathscr{C}$.

Wir wollen nun für ein gegebenes Polynom eine spezielle Überdeckung von K konstruieren und sie als „Graphen" bezeichnen.

2.3. Definition. Es sei $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$. Ein *Graph von f* ist eine Überdeckung $\mathscr{C}$ von K mit folgenden Eigenschaften:

(1) Ist $\{x, v(x) \leqq \alpha\}$ die unendliche Zelle von $\mathscr{C}$, dann ist

$n\alpha + v(a_n) < i\alpha + v(a_i)$ für $i < n$

und somit $v(f(x)) = v(a_n x^n)$ für alle x aus dieser Zelle.

(2) Wenn $\{x, x = x_0 + u, v(u) \geqq \beta\}$ eine endliche Zelle aus $\mathscr{C}$ ist, dann tritt stets einer der beiden folgenden Fälle ein:

a) $v(f(x)) \leqq c$ für ein $c \in \mathbf{Z}$ und alle x, die zu dieser Zelle gehören.

b) Es sei $g(u) = f(x_0 + u) = b_0 + b_1 u + \cdots + b_n u^n$, dann existieren eine natürliche Zahl i und ein $\gamma \in \mathbf{Z}$, so daß für alle $j \neq i$ und alle s mit $\beta \leqq s < \gamma$

$v(b_i) + i \cdot s < v(b_j) + j \cdot s$

ist; die Elemente $x_0 + u$ mit $v(u) \geqq \gamma$ gehören nicht echt zu dieser Zelle. Es gilt also für Elemente $x = x_0 + u$, die echt zur Zelle gehören,

$v(f(x)) = v(b_i u^i)$.

Der Sinn einer solchen Überdeckung besteht darin, die Funktion $v(f(x))$ leicht beschreiben zu können. Wie wir gesehen haben, ist diese Funktion in den einzelnen Zellen beschränkt bzw. linear in $v(x - x_0)$.

Die *Daten eines Graphen* bestehen aus

(1) der Anzahl der Zellen in der Überdeckung, den Daten dieser Zellen und der Zuordnung a) oder b) zu jeder endlichen Zelle (je nachdem, welcher Fall eintritt);

(2) der Zahl c im Falle a);

(3) dem Element x_0 und den Zahlen i, γ und $v(b_i)$ im Falle b).

Die *Ordnung eines Graphen* ist das Maximum aus der Anzahl der Zellen und der Zahlen c.

Zum Beweis des Satzes von Cohen benötigen wir das folgende

2.4. Lemma. *Zu jedem Polynom $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$ existiert ein Graph, dessen Daten effektive Funktionen von $a_0, \ldots, a_n$ sind. Die Ordnung des Graphen ist durch eine Funktion beschränkt, die nur von n und den $v(a_j)$ abhängt.*

Beweis. Wir beweisen das Lemma durch Induktion nach n. Der Fall $n = 0$ ist trivial. Wir wollen nun zunächst voraussetzen, daß f separabel ist.
Nach Induktionsvoraussetzung hat $f'(X)$ einen Graphen mit den im Lemma geforderten Eigenschaften.
Nun betrachten wir die ganzen Teile der Zahlen $\dfrac{v(a_i) - v(a_j)}{i-j}$ für $i \neq j$ und ordnen sie der Größe nach an (gleiche Zahlen werden nur einmal aufgeführt): $\alpha_1 < \alpha_2 < \cdots < \alpha_s$. Damit gilt für alle x mit $v(x) \neq \alpha_i$, $i = 1, \ldots, s$, stets $v(a_j x^j) \neq v(a_k x^k)$ für $j \neq k$.
Wir konstruieren nun den Graphen für f wie folgt: Als unendliche Zelle wählen wir $\{x, v(x) \leqq \alpha_1 - 1\}$. Es ist klar, daß diese Zelle bezüglich f die Eigenschaft (1) hat. Nun sei $C_i = \{x, v(x) \geqq \alpha_i\}$ und $D_i = \{x, v(x) \geqq \alpha_i + 1\}$. Dann gilt, wie man sofort nachrechnet, für $i < s$ in $D_i - C_{i+1}$ stets $v(f(x)) = v(a_k x^k)$ für ein $k = k(i)$, d. h., der Fall b) tritt auf. In D_s tritt der Fall a) ein mit $c = v(a_0)$, falls $a_0 \neq 0$ ist, ansonsten der Fall b).
Damit haben wir eine Überdeckung von K gefunden $(\{x, v(x) \leqq \alpha_1 - 1\}, C_1, \ldots, C_s)$, die im wesentlichen schon die Eigenschaften eines Graphen von f hat. Wir müssen jetzt noch das Verhalten von f auf $C_i - D_i$ untersuchen und dabei die eben konstruierte Überdeckung gegebenenfalls verfeinern.
Nun kann man zunächst eine Überdeckung von K finden, so daß die Elemente von jedem $C_i - D_i$ echt zu einer Zelle dieser Überdeckung gehören: Es sei $x_0 = p^{\alpha_i}$, $x_1 = p^{\alpha_i + 1}$, dann ist

$$\begin{aligned} C_i - D_i &= \{x, v(x) = \alpha_i\} \\ &= \{x, x = x_0 + u, v(u) \geqq \alpha_i\} - \{x, x = x_1 + u, v(u) \geqq \alpha_i + 1\}. \end{aligned}$$

Damit können wir annehmen, wir hätten eine Überdeckung $\{A_j\}$ von K gefunden, so daß diese bis auf $\{x \in K, v(x) = \alpha_i\}$ die Eigenschaft eines Graphen hat. Die x mit $v(x) = \alpha_i$ gehören echt gewissen Zellen an.
Es sei nun $\{\Gamma_j\}$ ein Graph für f', dann ist $\{A_i \cap \Gamma_j\}_{i,j}$ eine Überdeckung von K. Wir wollen jetzt zeigen, daß dies ein Graph für f ist. Dazu genügt es jetzt, f in $\Gamma_j \cap \{x, v(x) = \alpha_i\}$ zu untersuchen. Es sei $\Gamma_1 = \{x, v(x) \leqq \beta\}$ die unendliche Zelle von $\{\Gamma_j\}$. Wenn $\alpha_i \leqq \beta$ ist für ein i, d. h. $\{x, v(x) = \alpha_i\} \subset \Gamma_1$, dann gilt für $x \in \Gamma_1$ und $v(x) = \alpha_i$

$$v(f'(x)) = v(h a_h) + (h-1)\,\alpha_i < \infty$$

(wobei $h \leqq n$ die größte Zahl ist, die nicht durch $t = \mathrm{Char}\,(K)$ teilbar ist, für die $a_h \neq 0$ ist; eine solche Zahl existiert, da f separabel ist).
Es sei nun $\varrho = \max\{-\min\{v(a_i), a_i \neq 0\}, 0\}$, dann hat $\bar f(X) = p^\varrho f(X)$ Koeffizienten aus I, $\bar f'(X) = p^\varrho f'(X)$ und $\bar f$ und f haben dieselben Nullstellen.
Jetzt ist $\bar f \in I[X]$, $v(\bar f'(x)) = v(h a_h) + (h-1)\,\alpha_i + \varrho := \lambda$ für $x \in \Gamma_1$ und $v(x) = \alpha_i$. Falls nun $v(\bar f(x)) \geqq 2\lambda + 1$ ist für ein solches x, folgt aus dem Newtonschen Lemma, daß eine Nullstelle $\xi \in I$ von $\bar f$ existiert mit $v(\xi - x) > \lambda$.
Damit ist die Frage nach der Existenz einer Nullstelle von $f(X)$ in $\{x, v(x) = \alpha_i\}$ reduziert auf eine Frage über das Verschwinden einer Bewertung in $R_{2\lambda+1}$.
Für jede Nullstelle ξ betrachten wir ihre Zelle

$$\{x, x = \xi + u, v(u) \geqq \lambda + 1\}.$$

Es gibt höchstens n solcher Zellen. Außerhalb dieser Zellen in $\{x, v(x) = \alpha_i\}$ ist $f(x)$ beschränkt:

$$f(x) < 2\lambda + 1 - \varrho$$

(wäre nämlich $f(x) \geqq 2\lambda + 1 - \varrho$, d. h. $\bar f(x) \geqq 2\lambda + 1$, so würde nach den obigen Überlegungen folgen, daß x in einer der „Nullstellenzellen" liegen würde). Es tritt also hier der Fall a) ein.

In den Zellen $\{x, x = \xi + u, v(u) \geqq \lambda + 1\}$ haben wir folgende Situation:

$$f(\xi) = 0, \quad v(f'(x)) = \lambda - \varrho, \quad v(f(x)) \geqq 2\lambda - \varrho + 1$$

für alle x aus dieser Zelle. Es sei $x = \xi + u$ aus dieser Zelle, $f(\xi + u) = g(u) = d_r u^r + \cdots + d_n u^n$, $r \geqq 1$ und $d_r \neq 0$; $v(f'(x)) = v(g'(u)) = \lambda - \varrho$. Es sei $\bar{f}(\xi + u) = \bar{d}_r u^r + \cdots + \bar{d}_n u^n$, $\bar{d}_j \in I$. Ist $v(u) > \max \{v(\bar{d}_r)/(j - r), j > r\}$, so ist $v(\bar{f}(x)) = v(\bar{d}_r u^r)$, also $v(f(x)) = v(d_r u^r)$. In den Zellen

$$\left\{x, x = \xi + u, v(u) > \max_{j>r} \{v(d_r)/(j - r)\} + 1\right\}$$

tritt der Fall b) ein. Außerhalb dieser Zellen in Γ_1 tritt der Fall a) ein. $v(d_r)$ läßt sich mittels der Eliminationstheorie aus den Koeffizienten von f berechnen.
Die bisherigen Untersuchungen mit der unendlichen Zelle von $\{\Gamma_j\}$ sind typisch. Wir wollen uns deshalb kurz fassen.
Wir untersuchen nun, wie sich f im Durchschnitt einer endlichen Zelle aus dem Graphen von f' mit $\{x, v(x) = \alpha_i\}$ verhält. Es sei Γ eine solche endliche Zelle von f'. Wir wollen zunächst annehmen, daß a) bezüglich f' in Γ gilt. Es sei

$$\Gamma = \{x, x = x_0 + u, v(u) \geqq \alpha\}$$

und $v(f'(x)) \leqq c$ für alle x, die echt zu Γ gehören. Analog zum vorigen Fall wählen wir ϱ, so daß $\bar{f}(x) = p^\varrho f(x)$ ganze Koeffizienten hat. Dann ist $v(\bar{f}'(x)) \leqq \varrho + c$ für echt zu Γ gehörige x. Nun wiederholen wir den vorigen Schluß, den wir bei der Untersuchung der unendlichen Zelle verwendet haben.
Nehmen wir jetzt an, b) gelte bezüglich f' in Γ. Es sei $g(u) = f'(x_0 + u)$. Dann können wir (analog zur Konstruktion der C_i) Γ durch endliche Zellen überdecken, so daß in diesen Zellen für $g(u)$ stets der Fall a) gilt, außer für endlich viele Mengen der Form $\{u, v(u) = \beta\}$ (deren Zahl $\frac{n}{2}(n + 1)$ nicht übersteigt). Auf diese endlich vielen Mengen wenden wir wieder die obige Schlußweise an.
Wir haben somit im Fall eines separablen Polynoms f induktiv mit Hilfe von f' einen Graphen von f konstruiert. Die Konstruktion ergab, daß in die Ordnung dieses Graphen nur n und die $v(a_i)$ eingehen, d. h., man erhält induktiv, daß seine Ordnung in der angegebenen Weise beschränkt ist.

In die Daten des Graphen gingen neben den Daten des Graphen von f' nur die Nullstellen von f, die Zahlen α_i, ϱ ein. Diese Zahlen sind offensichtlich effektive Funktionen der Koeffizienten von f. Um zu zeigen, daß der von uns konstruierte Graph von f als Daten effektive Funktionen von $a_0, \ldots, a_n$ hat, genügt es zu zeigen, daß die Nullstellen von f effektive Funktionen der Koeffizienten sind. Genauer gesagt, es genügt, folgendes zu beweisen:
Es sei $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in I[X]$ gegeben, und für ein x_0 sei

$$v(f(x_0)) \geqq 2\lambda + 1 \text{ und } v(f'(x_0)) \leqq \lambda.$$

Dann ist die durch $v(\xi - x_0) > \lambda$ eindeutig bestimmte Nullstelle ξ von f eine effektive Funktion.
Wir können dazu o. B. d. A. $x_0 = 0$ annehmen. Um die Effektivität nachzuweisen, müssen wir zeigen (vgl. Definition 2.1), wie

1. $v(g(\xi))$ für ein beliebiges Polynom g zu berechnen ist,
2. $[g(\xi)]_k$ zu bestimmen ist, falls $g(\xi) \in I$ ist,
3. $[B_i(g(\xi))]_k$ und $v(B_i(g(\xi)))$ zu berechnen ist für alle i.

Unter Benutzung des Euklidischen Algorithmus können wir uns darauf beschränken, daß $\deg(g) < \deg(f)$ ist. Damit hat g einen effektiven Graphen, d. h. einen Graphen mit effektiven Daten. Es genügt daher zu zeigen, wie $v(\xi - a)$ für alle $a \in K$ berechnet werden kann, weil die Funktion $v(g(\xi))$ entweder linear oder beschränkt in einer Zelle ist. Ähnliches gilt für $[g(\xi)]_k$ in R_k. Da $\xi - a$ eine Nullstelle von $h(x) = f(x + a)$ ist, können wir o. B. d. A. $a = 0$ setzen. Nun ist

$$f(x) = f(0) + f'(0)\,x + a_2 x^2 + \cdots + a_n x^n$$

und damit

$$-f(0) = f'(0)\,\xi + a_2\,\xi^2 + \cdots + a_n \xi^n .$$

Weiterhin ist nach Voraussetzung

$$v(f(0)) \geqq 2\lambda + 1\,, \quad v(f'(0)) \leqq \lambda\,, \quad v(\xi) > \lambda\,.$$

Daraus folgt

$$v(\xi) = v\left(\frac{f(0)}{f'(0)}\right).$$

Die Berechnung der Klasse von ξ in R_k nimmt man iterativ mit Hilfe des Verfahrens vor, das im Beweis des Newtonschen Lemmas verwendet wird (vgl. [3]).
Schließlich müssen wir noch zeigen, wie im Fall der Charakteristik $t > 0$ die $B_i(g(\xi))$ zu berechnen sind. Zunächst kann man mit Hilfe der Eliminationstheorie (vgl. [7]) $c_0, \ldots, c_k \in K$ finden, so daß $c_0 + c_1 g(\xi) + \cdots + c_k g(\xi)^k = 0$ ist. Dann ist nach Definition der B_i

$$c_i = \sum_{j=0}^{t-1} B_j(c_i)\,p^j\,, \qquad g(\xi) = \sum_{j=0}^{t-1} B_j(g(\xi))\,p^j\,.$$

Damit erhalten wir Gleichungen für die $B_i(g(\xi))$ und können damit $v(B_i(g(\xi)))$ und $[B_i(g(\xi))]_k$ ermitteln, da im Fall positiver Charakteristik $\hat{I} = k[[p]]$ ist (vgl. S. 115).
Wir setzen nun voraus, daß f ein inseparables Polynom ist. Es sei $f(X) = g(X^t)$, $t =$ Charakteristik von K. Nach Induktionsvoraussetzung hat g einen Graphen $\mathscr{C}_g$ mit effektiven Daten. Es sei $C \in \mathscr{C}_g$ eine Zelle, $C' =: \{x, x \in K, x^t \in C\}$. Dann ist $\{C', C \in \mathscr{C}_g\}$ ein Graph für f. Dazu müssen wir zeigen:

(1) C' ist eine Zelle, wenn C' nicht leer ist,

(2) $\bigcup_{C \in \mathscr{C}_g} C' = K$,

(3) wenn z echt zu C' gehört, gehört z^t echt zu C,

(4) ist $v(g(z)) \leqq c$ für echt zu C gehörige z, so ist $v(f(z)) \leqq c$ für echt zu C' gehörige z,

(5) wenn für $C \in \mathscr{C}_g$ bezüglich g der Fall b) gilt, dann existiert eine Überdeckung der Zelle C', so daß für die Elemente dieser Überdeckung bezüglich f entweder der Fall a) oder der Fall b) gilt,

(6) ist $C = \{x, v(x) \leqq \alpha\}$ die unendliche Zelle von $\mathscr{C}_g$, so ist
$C' = \left\{x, v(x) \leqq \left[\frac{\alpha}{t}\right]\right\}$ die unendliche Zelle von $\{C', C \in \mathscr{C}_g\}$.

Sind (1)—(6) bewiesen, so haben wir einen Graphen von f konstruiert, dessen Daten effektive Funktionen der Koeffizienten von f sind. (3), (4) und (6) sind trivial.

Zu (1): $C = \{x_0 + u, v(u) \geqq \alpha\}$ sei eine endliche Zelle von $\mathscr{C}_g$, und es sei $C' = \{x, x^t = x_0 + u, v(u) \geqq \alpha\} \neq \emptyset$. Nun ist in R_α $[x^t]_\alpha = [x_0]_\alpha$ und damit $C = \{x_1^t + u, v(u) \geqq \alpha\}$ für ein $x_1 \in C'$. Damit ist $C' = \left\{x_1 + u, v(u) \geqq \left[\frac{\alpha}{t}\right]\right\}$.
Zu (2): Für jedes $x \in K$ existiert ein $C \in \mathscr{C}_g$ mit $x^t \in C$, d. h. $x \in C'$.
Zu (5): Durch eine Überdeckung der Zelle C mit Zellen $C^{(i)}$ können wir erreichen,

daß für $g(x)$ auf $C^{(i)}$ entweder Fall a) eintritt und damit für $f(x)$ auf $C^{(i)}$, oder $g(X)$ auf $C^{(i)}$ eine effektive Nullstelle ξ besitzt, so daß $g(X) = \sum_{j=r}^{n/t} d_j(X-\xi)^j$ ist, $d_r \neq 0$, $r \geqq 1$ und $C^{(i)} = \left\{x, x = \xi + u, v(u) \geqq \max_{j>r} \{v(d_r)/(j-r) + 1\}\right\}$ ist. Mit Hilfe der Operation B_0 können wir effektiv entscheiden, ob $\sqrt[t]{\xi}$ aus K ist oder nicht. Ist $\sqrt[t]{\xi} \in K$, so liegt in $C^{(i)\prime}$ der Fall b) für $f(x)$ vor. Ist $\sqrt[t]{\xi} \notin K$, dann tritt der Fall a) für $f(x)$ in $C^{(i)\prime}$ ein (es ist $v(f(x)) \leqq v(\xi - B_0(\xi)) + v(d_r)$ für alle x, die echt zur Zelle $C^{(i)\prime}$ gehören). Damit ist das Lemma bewiesen.

Wir wollen nun aus dem Lemma COHENS Satz folgern. Der Beweis verläuft analog zu COHENS Arbeit [1].
Es sei $\Phi(u)$ eine Formel, die außer u eventuell noch andere Variable enthält, wobei u entweder eine K-Variable oder eine $\mathbf{Z}$-Variable ist. Wir müssen nun ein Ψ konstruieren, das u nicht enthält und höchstens diejenigen K- und $\mathbf{Z}$-Variablen hat, die auch Φ enthält, so daß $\exists\, u\, \Phi(u) \Leftrightarrow \Psi$ gilt.

1. Fall: *u ist eine K-Variable.*
Nun kann u in $\Phi(u)$ enthalten sein durch

(i) die Bewertung von einigen $p_j(u)$, p_j Polynome in u, deren Koeffizienten Polynome in anderen K-Variablen über $\mathbf{Z}$ bzw. dem Primkörper von K sind, die noch in Φ vorkommen (insbesondere kann $p_j(u) = 0$ vorkommen),
(ii) die Bewertung von einigen $p_j(B_i(u))$ (p_j wie in (i)),
(iii) die Klassen von $p_j(u)$ bzw. $p_j(B_i(u))$ in R_{k_j} (k_j eine feste ganze Zahl oder eine $\mathbf{Z}$-Variable, p_j wie in (i)).

Zu (i): Für jedes Polynom p_j betrachten wir seinen Graphen $\mathscr{C}_j$ mit effektiven Daten. Ist $C \in \mathscr{C}_j$ eine Zelle und gehört u echt zu C, dann ist $v(p_j(u))$ eine lineare Funktion von $v(u - \xi_j^{(C)})$, wobei $\xi_j^{(C)}$ ein geeignetes Element von C ist, oder $v(p_j(u))$ ist beschränkt in C. Wir können nun für jedes j diejenigen Zellen $C_{j,s} \in \mathscr{C}_j$ auswählen ($s = 1, \ldots, e_j$), in denen $v(p_j(u))$ die in Φ geforderten Bedingungen erfüllt. Damit muß jedes u, das $\Phi(u)$ erfüllt, in den C_{j,s_j} liegen für ein $s_j \leqq e_j$. Wenn wir aus Φ also die Variable u eliminieren wollen, so müssen wir über die Graphen $\mathscr{C}_j$ Bedingungen hinzunehmen, die garantieren, daß

$$\bigcap_j \bigcup_{s=1}^{e_j} C_{j,s} \neq \emptyset$$

ist. Da die $\mathscr{C}_j$ effektive Daten haben, ist eine solche Bedingung äquivalent zu einer Formel Ψ in den anderen K- und $\mathbf{Z}$-Variablen von Φ.
Zu (ii): Wenn $B_r(u)$ durch Bewertungen von Polynomen $q_j(B_r(u))$ (mit analogen Eigenschaften wie in (i)) in Φ vorkommt, betrachten wir effektive Graphen für die Polynome $q_j(W^t)$. Analog zu (i) können wir geeignete Durchschnitte $K_1, \ldots, K_a$ von Zellen dieser Graphen konstruieren, daß die Existenz eines w, so daß w^t die an $B_r(u)$ gestellten Bedingungen erfüllt, äquivalent dazu ist, daß $\bigcup_i K_i \neq \emptyset$ ist.

Zusammen mit den in (i) gefundenen Bedingungen erhalten wir: Die Existenz eines $u \in K$, das die Bedingungen bezüglich der Bewertung v der Formel Φ erfüllt, ist äquivalent zur Bedingung $Z = \bigcap_j \bigcup_{s=1}^{e_i} C_{j,s} \neq \emptyset$ und $\{B_r(x), x \in Z\} \cap \bigcup_i K_i^t \neq \emptyset$.
Wegen der Effektivität der K_i und $C_{i,j}$ läßt sich diese Bedingung wieder durch eine Formel Ψ, die nicht von u abhängt, ausdrücken.
Analog verfährt man bei (iii).

2. Fall: *u ist eine* **Z**-*Variable.*
Nun kann u in $\Phi(u)$ enthalten sein durch

(i) Ausdrücke, die nur durch die Atomformeln $n + m = k$, $n \leqq k$ zusammengesetzt sind und eventuell noch andere in Φ vorkommende **Z**-Variablen enthalten,

(ii) Bewertungen endlich vieler Elemente der Form $Q(w_1^{m_1(u)}, \ldots, w_r^{m_r(u)})$, wobei Q und $w_1, \ldots, w_r$ Polynome in den in Φ enthaltenen K-Variablen über dem Primkörper von K sind und $m_1(u), \ldots, m_r(u)$ Funktionen, die durch Formeln aus (i) definiert werden (d. h., $n = m_i(u)$ ist äquivalent zu einer Formel, wie sie in (i) charakterisiert wurde),

(iii) Gleichungen der Art $[w]_u = 0$ und Ungleichungen der Art $[w]_u \neq 0$, wobei w ein Polynom in den in Φ enthaltenen K-Variablen über dem Primkörper von K ist.

Um u aus Φ zu eliminieren, überlegen wir uns, daß die in (i) und (ii) vorkommenden Funktionen in u stückweise linear sind mit effektiven Daten, d. h. die Zerlegung des Primkörpers von K in endlich viele Intervalle, in denen die f_j und h_j jeweils linear sind und die Werte dieser Funktionen an den Endpunkten dieser Intervalle sind effektive Funktionen. In (i) ist das trivial; in (ii) muß man zeigen, daß $v\big(Q(w_1^{m_1(u)}, \ldots, w_r^{m_r(u)})\big)$ eine stückweise lineare Funktion ist. Das ist nicht schwierig (wir verweisen auf [1]), wir wollen es hier nicht ausführen. Wir können also für (i) und (ii) annehmen, daß die Variable u in $\Phi(u)$ durch die Gleichungen und Ungleichungen der Form

$$f_j(u) = 0, \qquad h_j(u) \geqq 0$$

vorkommt, wobei die f_j und h_j stückweise lineare Funktionen mit Werten in **Z** und effektiven Daten sind.
Jetzt können wir analog zum ersten Fall schließen. (iii) eliminiert man wie folgt:

$$\exists\, u[w]_u = 0 \Leftrightarrow [w]_{v(w)} = 0,$$
$$\forall\, u[w]_u = 0 \Leftrightarrow w = 0$$

und analog die entsprechenden Ungleichungen.
Damit ist der Satz von COHEN bewiesen.

2.5. Bemerkung. Es sei eine Formel der Gestalt $\exists\, l, \big(l \geqq 0 \,\&\, \Phi(l, u, v, \ldots)\big)$ gegeben, wobei l eine **Z**-Variable ist. Dann ist die Funktion, die den Variablen $u, v, \ldots$ das kleinste l zuordnet, so daß die obige Formel erfüllt ist, eine effektive Funktion in $u, v, \ldots$

Diese Bemerkung folgt sofort aus dem Satz von COHEN.

3. Eine Anwendung

Wir wollen jetzt als Anwendung einen anderen Beweis für den Greenbergschen Approximationssatz (vgl. [2]) geben:

Satz. *Es sei I ein exzellenter henselscher diskreter Bewertungsring mit perfektem Restklassenkörper; p sei ein Primelement von I. Weiterhin seien $F_1, \ldots, F_m \in I[Y_1, \ldots, Y_N]$ gegeben. Wenn das Gleichungssystem $F_i(Y) = 0$ für alle i eine formale Lösung $\bar{y} = (\bar{y}_1, \ldots, \bar{y}_N)$, $\bar{y}_i \in \hat{I}$ hat, dann existieren für alle natürlichen Zahlen c solche $y_{i,c} \in I$, daß $y_{i,c} \equiv \bar{y}_i$ mod p^c ist und $F_i(y_{1,c}, \ldots, y_{N,c}) = 0$.*

Beweis. Nach COHENS Satz (angewendet auf $Q(\hat{I})$) ist die Formel $\exists\, \bar{y}_1, \ldots, \bar{y}_N$ $F_1(\bar{y}) = 0 \,\&\, \ldots \,\&\, F_m(\bar{y}) = 0 \,\&\, [\bar{y}_i]_c = w_i$ äquivalent zu einer Formel Ψ aus $\mathscr{C}$, so daß in Ψ nur R_k-Variable als gebundene Variable vorkommen. Da $\hat{I}/p^k = I/p^k$ ist und wir davon ausgehen können, daß über I die Formel

$$\exists\, y_1, \ldots, y_N\ F_1(y) = 0 \;\&\; \ldots \;\&\; F_m(y) = 0 \;\&\; [y_i]_c = w_i$$

auch äquivalent zu Ψ ist (vgl. Beweis des Satzes von COHEN), folgt sofort die Behauptung.

LITERATUR

[1] COHEN, P. J.: Decision procedures of real and p-adic fields, Commun. Pure Appl. Math. *22* (1969), 131–151.

[2] GREENBERG, M. J.: Rational points in henselian discrete valuation rings. Publ. math. *31* IHES (1966), 59–64.

[3] KURKE, H., G. PFISTER und M. ROCZEN: Henselsche Ringe und algebraische Geometrie. VEB Deutscher Verlag der Wissenschaften, Berlin 1975.

[4] KURKE, H., T. MOSTOWSKI, G. PFISTER, D. POPESCU und M. ROCZEN: Die Approximationseigenschaft lokaler Ringe. Lecture Notes in Math. 634, Springer-Verlag, Berlin–Heidelberg–New York 1978.

[5] MOSTOWSKI, T.: A decision procedure for rings of power series of several variables and applications. Bull. Acad. Polon. Sc. *23* (12) (1975), 1229–1232.

[6] SEYDI, H.: Sur la théorie des anneaux excellents en characteristic p. Bull. Sc. math. 2e serie *96* (1972), 193–198.

[7] VAN DER WAERDEN, B. L.: Algebra I, II. Springer-Verlag, Berlin–Göttingen–Heidelberg 1955.

Manuskripteingang: 22. 5. 1977

VERFASSER:

TADEUSZ MOSTOWSKI, Mathematisches Institut der Universität Warschau
GERHARD PFISTER, Sektion Mathematik der Humboldt-Universität Berlin