and obtain

$$N(\sigma, T) \ll T^{\frac{48(1-\sigma)}{37(2\sigma-1)}+\varepsilon}. \tag{10.19}$$

The estimate (10.19) also holds in a short interval to the right of 75/89.

Since (10.16) was established in [4] for $\sigma \geqslant 5/6$, we have (10.16), a weak form of the density hypothesis, for $\sigma \geqslant 189/230$.

Added in proof. 1. To prove (6.6) $M^{-c}B(R, M, D)$ was assumed to be a decreasing function of $M$ for $c > 1$. This may be false for $M < D$. The difficulty may be resolved by redefining $B(R, M, D)$ or by moving the contour to the right, increasing $c$ to $1/\varepsilon$ and permitting an extra factor $M^{\varepsilon}$ in the upper bounds. The upper bounds substituted for $B(R, M, D)$ give decreasing functions, and the zero-density theorems are unaffected.

2. Jutila [*On a density theorem of H. L. Montgomery for L-functions*, Acta Acad. Sci. Fenn. Series AI 520] has new density theorems for $L$-functions, including the density hypothesis for $\sigma > 5/6$. Jutila's ideas will be discussed in the second part of this paper.

### References


[1] M. Forti and C. Viola, *Density estimates for the zeros of L-functions*, Acta Arith. 23 (1973), pp. 379–391.

[2] W. Haneke, *Verschärfung der Abschätzung von* $\zeta(\frac{1}{2}+it)$, Acta Arith. 8 (1963), pp. 357–430.

[3] M. N. Huxley, *The large sieve inequality for algebraic number fields II*, Proc. London Math. Soc. (3) 21 (1970), pp. 108–128.

[4] — *On the difference between consecutive primes*, Inventiones Math. 15 (1972), pp. 164–170.

[5] M. Jutila, *On the Dirichlet polynomial method in the theory of zeta and L-functions*, to appear.

[6] H. L. Montgomery, *Topics in multiplicative number theory*, Berlin–Heidelberg–New York 1971.


*Received on 28. 10. 1972* (342)

ACTA ARITHMETICA
XXIV (1973)

# Zur Methode von Stepanov

von

WOLFGANG M. SCHMIDT (Boulder, Colo.)

*Herrn Professor C. L. Siegel zum 75. Geburtstag gewidmet*

**1. Einleitung.** S. A. Stepanov hat mit seiner neuen Methode einen wichtigen Fall des Satzes von Hasse–Weil elementar bewiesen ([2], [3], [4]). Es sei $F_q$ der endliche Körper mit $q$ Elementen, und es sei $f(X)$ ein Polynom vom Grad $m$ mit Koeffizienten in $F_q$. Ist nun $n$ eine positive, zu $m$ relativ prime Zahl, und ist $q > 4m^2n(n-1)^2$, dann hat Stepanov gezeigt, daß die Anzahl $A$ der Lösungen der Gleichung

$$y^n = f(x)$$

in Elementen $x, y$ aus $F_q$ die Ungleichung

$$|A-q| < (3mn)^{3/2}q^{1/2}$$

befriedigt. Weiter hat er ein ähnliches Resultat für Gleichungen $y^p - y = f(x)$ hergeleitet [5], wobei $p$ die Charakteristik von $F_q$ ist(1).

In der vorliegenden Arbeit wollen wir allgemein Polynome $f(X, Y)$ zulassen, die absolut irreduzibel sind, die also in keinem algebraischen Erweiterungskörper reduzibel sind. Wir werden die Methode von Stepanov weiter führen und das folgende Ergebnis elementar beweisen.

SATZ. *Das Polynom $f(X, Y)$ mit Koeffizienten in $F_q$ sei absolut irreduzibel, und es habe Grad $m > 0$ in $X$ and Grad $n > 0$ in $Y$. Ist nun*

$$q > 9(m+1)^2(n+1)^2 \quad (2), \tag{1}$$

*dann gilt für die Anzahl $A$ der Lösungen der Gleichung*

$$f(x, y) = 0 \tag{2}$$

*in Elementen $x, y$ aus $F_q$ die Ungleichung*

$$|A-q| < 2\,\mathrm{Min}(m^2n, n^2m)q^{1/2}. \tag{3}$$

(1) In einem Brief vom 22.6.1972 hat mir Herr Stepanov mitgeteilt, daß er nunmehr Gleichungen $y^n + g_1(x)y^{n-1} + \ldots + g_n(x) = 0$ behandeln kann, für die der Grad $m$ von $g_n(X)$ zu $n$ relativ prim ist, und für die weiter der Grad von $g_i(X)$ kleiner ist als $(i/n)m$ $(1 \leqslant i \leqslant n-1)$.*

(2) Mit zusätzlichem Aufwand könnte diese Bedingung gemildert werden.

* Bemerkung bei der Korrektur. Dieses Ergebnis erschien in Izv. Akad. Nauk SSSR, Ser. Mat 36 (1972), S. 683–711.

A. Weil hat im Jahre 1948 [7] mit tiefliegenden Hilfsmitteln aus der algebraischen Geometrie die Beziehung $|A'-q-1| \leqslant 2gq^{1/2}$ bewiesen, wobei $A'$ die Anzahl der Primdivisoren vom ersten Grade von (2) ist, und wobei $g$ das Geschlecht der durch $f(X, Y) = 0$ definierten Kurve bedeutet. Zieht man Eigenschaften der Zetafunktion dieser Kurve heran (siehe etwa [1], Seite 319), dann kann man auch aus unserem Satz folgern, daß $|A'-q-1| \leqslant 2gq^{1/2}$ ist.

**2. Vorbereitungen.** Wir werden einige einfache Begriffe aus der Theorie der Körper benötigen. Mit $\overline{F}_q$ bezeichnen wir die maximale algebraische Erweiterung von $F_q$, also einen algebraisch abgeschlossenen algebraischen Erweiterungskörper von $F_q$.

Mit $X, Y, Z, W, \ldots, X_1, X_2, \ldots$ werden wir Variable, also über $F_q$ algebraisch unabhängige Größen, bezeichnen. Es werden $\mathfrak{X}, \mathfrak{Y}, \ldots$ Größen sein, die von einigen der $X, Y, \ldots$ algebraisch abhängen. Schließlich werden $x, y, \ldots$ Elemente von $\overline{F}_q$ sein.

Mit $a(X)$, $a(X, Y)$, $b(X), \ldots$ werden wir Polynome mit Koeffizienten aus $F_q$ bezeichnen. Gilt $a(X_1, \ldots, X_n) = 0$, dann verschwindet das Polynom identisch. Gilt aber $a(x_1, \ldots, x_n) = 0$, dann verschwindet das Polynom $a(X_1, \ldots, X_n)$ im „Punkt" $(x_1, \ldots, x_n)$. Wir schreiben

$$\mathrm{Grad}_{X_i} a(X_1, \ldots, X_n)$$

für den Grad eines Polynoms $a(X_1, \ldots, X_n)$ in der Variablen $X_i$ $(1 \leqslant i \leqslant n)$. Schließlich gebrauchen wir die Bezeichnung $r(X), r(X, Y), s(X), \ldots$ für rationale Funktionen mit Koeffizienten in $F_q$.

Ist $K'$ ein endlich algebraischer Erweiterungskörper des Körpers $K$, dann bedeute $[K' : K]$ den Grad der Erweiterung. Wir schreiben $K(X_1, \ldots, X_u, \mathfrak{X}_1, \ldots, \mathfrak{X}_v, x_1, \ldots, x_w)$ für den Körper, der aus dem Körper $K$ durch Adjunktion von $X_1, \ldots, X_u, \mathfrak{X}_1, \ldots, \mathfrak{X}_v, x_1, \ldots, x_w$ entsteht. So ist etwa $F_q(X_1, \ldots, X_u)$ der Körper der rationalen Funktionen in $u$ Variablen über $F_q$.

Mit $|\omega|$ bezeichnen wir die Anzahl der Elemente einer endlichen Menge $\omega$.

Wir bilden die elementaren symmetrischen Funktionen

$$l_1(U_1, \ldots, U_n) = -(U_1 + \ldots + U_n),\ l_2(U_1, \ldots, U_n) = U_1U_2 + \ldots + U_{n-1}U_n,$$
$$\ldots, l_n(U_1, \ldots, U_n) = (-1)^n U_1 \ldots U_n.$$

HILFSSATZ 1. *Das Polynom $a(U_1, \ldots, U_n)$ sei symmetrisch, also invariant unter Permutationen der Variablen $U_1, \ldots, U_n$. Dann gibt es ein Polynom $b(V_1, \ldots, V_n)$, sodaß*

$$a(U_1, \ldots, U_n) = b\big(l_1(U_1, \ldots, U_n), \ldots, l_n(U_1, \ldots, U_n)\big)$$

*ist. Falls weiter $a$ in jeder Variablen $U_i$ vom Grad $\delta$ ist, dann hat $b$ den Gesamtgrad $\delta$.*



Beweis. Zumindest die erste Behauptung ist wohlbekannt. Die zweite Behauptung ergibt sich unmittelbar aus dem Beweis, wie er etwa im Lehrbuch von Van der Waerden [6] gegeben wird.

Die Zahl $q$ ist von der Gestalt

$$q = p^\varkappa, \tag{4}$$

wobei $p$ die Charakteristik von $F_q$ ist. Die Abbildung $x \to x^p$ ist ein Isomorphismus von $F_q$ auf sich; durchläuft daher $x$ die Elemente von $F_q$, dann durchläuft auch $x^p$ die Elemente von $F_q$. Ist das gegebene Polynom $f(X, Y)$ von der Gestalt $f(X, Y) = g(X^p, Y)$ für ein Polynom $g$, dann ist die Anzahl der Lösungen von $f(x, y) = g(x^p, y) = 0$ mit $x, y \in F_q$ gleich der Anzahl der Lösungen von $g(x, y) = 0$ mit $x, y \in F_q$. Das Polynom $g(X, Y)$ ist wieder absolut irreduzibel. Indem man diese Reduktion endlich oft durchführt, gelangt man schließlich zu einem Polynom, das nicht als Polynom in $X^p, Y$ ausgedrückt werden kann. Daher dürfen wir ohne Beschränkung der Allgemeinheit annehmen, daß $f(X, Y)$ nicht von der Gestalt $g(X^p, Y)$ ist, daß also $f(X, Y)$ „separabel" in $X$ ist. Ebenso dürfen wir annehmen, daß $f(X, Y)$ separabel in $Y$ ist.

Ist $m = 1$ oder $n = 1$, dann ist $A = q$. Wir dürfen daher ohne Beschränkung der Allgemeinheit annehmen, es sei

$$2 \leqslant n \leqslant m. \tag{5}$$

Das Polynom $f(X, Y)$ ist von der Gestalt

$$f(X, Y) = g_0(X)\,Y^n + g_1(X)\,Y^{n-1} + \ldots + g_{n-1}(X)\,Y + g_n(X)$$

mit $g_0(X) \not\equiv 0$ und mit

$$\mathrm{Grad}\ g_i(X) \leqslant m \qquad (0 \leqslant i \leqslant n).$$

HILFSSATZ 2. *Es seien $X, Z$ Unbestimmte, und $\mathfrak{Y}, \mathfrak{U}$ mögen*

$$f(X, \mathfrak{Y}) = 0, \qquad f(Z, \mathfrak{U}) = 0$$

*erfüllen. Dann ist*

$$[F_q(X, Z, \mathfrak{Y}, \mathfrak{U}) : F_q(X, Z)] = n^2.$$

Beweis. Es wird genügen, die beiden Gleichungen

$$[F_q(X, Z, \mathfrak{Y}, \mathfrak{U}) : F_q(X, Z, \mathfrak{Y})] = n \tag{6}$$

und

$$[F_q(X, Z, \mathfrak{Y}) : F_q(X, Z)] = n \tag{7}$$

zu zeigen. Um (6) zu zeigen, haben wir nachzuweisen, daß $f(Z, U)$ über dem Körper $F_q(X, \mathfrak{Y})$ irreduzibel ist. Wäre das nicht der Fall, dann wäre

$$f(Z, U) = f_1(Z, U) f_2(Z, U),$$

wobei $f_1(Z, U), f_2(Z, U)$ Polynome mit Koeffizienten in $F_q(X, \mathfrak{Y})$ sind, deren Gesamtgrade kleiner sind als der Gesamtgrad von $f(Z, U)$. Es sei etwa

$$f_i(Z, U) = \sum_{j,k} c_{ijk} Z^j U^k \qquad (i = 1, 2)$$

mit

$$c_{ijk} = r_{ijk}^{(0)}(X)\mathfrak{Y}^{n-1} + \ldots + r_{ijk}^{(n-2)}(X)\mathfrak{Y} + r_{ijk}^{(n-1)}(X).$$

Nun sei $x \in \overline{F_q}$ derart, daß $g_0(x) \neq 0$ ist und daß der gemeinsame Nenner der rationalen Funktionen $r_{ijk}^{(l)}(X)$ in $x$ nicht verschwindet. Es sei $y \in \overline{F_q}$ mit $f(x, y) = 0$. Setzen wir

$$\overline{c_{ijk}} = r_{ijk}^{(0)}(x)y^{n-1} + \ldots + r_{ijk}^{(n-2)}(x)y + r_{ijk}^{(n-1)}(x),$$

dann gilt

$$f(Z, U) = \bar{f}_1(Z, U)\bar{f}_2(Z, U) \tag{8}$$

mit

$$\bar{f}_i(Z, U) = \sum_{j,k} \overline{c_{ijk}} Z^j U^k \qquad (i = 1, 2).$$

Der Gesamtgrad von $\bar{f}_i(Z, U)$ $(i = 1, 2)$ ist kleiner als der Gesamtgrad von $f(Z, U)$. Die Gleichung (8) widerspricht der totalen Irreduzibilität von $f(Z, U)$.

Damit ist (6) bewiesen. Der Beweis von (7) verläuft ähnlich und etwas einfacher.

**3. Ein Ergebnis über lineare Unabhängigkeit.** Durchwegs seien $\mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}$ Größen mit

$$f(X, \mathfrak{Y}) = 0, \quad \mathfrak{Z} = X^q, \quad \mathfrak{W} = \mathfrak{Y}^q. \tag{9}$$

Der folgende Hilfssatz ist wesentlich für alles weitere.

HILFSSATZ 3. *Es sei $a(X, Y, Z, W)$ ein nicht identisch verschwindendes Polynom der Gestalt*

$$a(X, Y, Z, W) = \sum_{i=0}^{n-1} \sum_{j=0}^{N} \sum_{k=0}^{n-1} b_{ijk}(X)\, Y^i Z^j W^k, \tag{10}$$

*mit Polynomen $b_{ijk}(X)$ vom Grad*

$$\leqslant (q/n) - mn.$$

*Dann ist*

$$a(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) \neq 0.$$



Beweis. Wir setzen

$$a(X, Y, Z; W_1, \ldots, W_n) = \prod_{t=1}^{n} a(X, Y, Z, W_t).$$

Dann ist nach Hilfssatz 1

$$a(X, Y, Z; W_1, \ldots, W_n) = b(X, Y, Z; l_1(W_1, \ldots, W_n), \ldots, l_n(W_1, \ldots, W_n)) \tag{11}$$

für ein gewisses Polynom $b(X, Y, Z; V_1, \ldots, V_n)$, dessen Gesamtgrad in den Variablen $V_1, \ldots, V_n$ höchstens $n-1$ ist. Wir bilden das neue Polynom

$$c(X, Y, Z; V_0, V_1, \ldots, V_n) = g_0(X)^{(n-1)^2} V_0^{n-1} b(X, Y, Z; V_1/V_0, \ldots, V_n/V_0). \tag{12}$$

Dieses Polynom $c$ ist homogen in den Variablen $V_0, \ldots, V_n$ vom Grad $n-1$.

Gemäß der Definition von $\mathfrak{Y}$ gilt

$$g_0(X)\mathfrak{Y}^n = -g_1(X)\mathfrak{Y}^{n-1} - \ldots - g_n(X),$$

wobei die Polynome $g_i(X)$ einen Grad $\leqslant m$ haben. Mittels Induktion nach $\delta$ erhalten wir hieraus

$$g_0(X)^\delta \mathfrak{Y}^{(n-1)+\delta} = g_1^{(\delta)}(X)\mathfrak{Y}^{n-1} + \ldots + g_n^{(\delta)}(X) \qquad (\delta = 1, 2, \ldots), \tag{13}$$

wobei die Polynome $g_i^{(\delta)}(X)$ $(1 \leqslant i \leqslant n)$ einen Grad $\leqslant m\delta$ haben. Da nun $a(X, Y, Z; W_1, \ldots, W_n)$ und daher auch die Polynome $b$ und $c$ vom Grad $\leqslant n(n-1) = (n-1) + (n-1)^2$ in $Y$ sind, und da weiter das Polynom $c$ durch $g_0(X)^{(n-1)^2}$ teilbar ist, gilt

$$c(X, \mathfrak{Y}, Z; V_0, \ldots, V_n) = d(X, \mathfrak{Y}, Z; V_0, \ldots, V_n), \tag{14}$$

wobei $d$ ein Polynom mit

$$\mathrm{Grad}_Y d(X, Y, Z; V_0, \ldots, V_n) \leqslant n-1 \tag{15}$$

und

$$\mathrm{Grad}_X d(X, Y, Z; V_0, \ldots, V_n) \leqslant \mathrm{Grad}_X b(X, Y, Z; V_1, \ldots, V_n) + m(n-1)^2 \leqslant n\{(q/n) - mn\} + m(n-1)^2 < q \tag{16}$$

ist.

Es seien $\mathfrak{Y}_1 = \mathfrak{Y}, \mathfrak{Y}_2, \ldots, \mathfrak{Y}_n$ die Wurzeln des Polynoms $f(X, Y)$ in $Y$, das heißt, es sei

$$f(X, Y) = g_0(X)(Y - \mathfrak{Y}_1) \ldots (Y - \mathfrak{Y}_n). \tag{17}$$

Wir bilden

$$\mathfrak{W}_1 = \mathfrak{W} = \mathfrak{Y}_1^q, \quad \mathfrak{W}_2 = \mathfrak{Y}_2^q, \quad \ldots, \quad \mathfrak{W}_n = \mathfrak{Y}_n^q. \tag{18}$$

Dann ist

$$f(X^q, Y^q) = f(X, Y)^q = g_0(X^q)(Y^q - \mathfrak{W}_1) \ldots (Y^q - \mathfrak{W}_n).$$

Da $Y^q$ von $X, \mathfrak{W}_1, \ldots, \mathfrak{W}_n$ algebraisch unabhängig ist, folgt hieraus

$$l_j(\mathfrak{W}_1, \ldots, \mathfrak{W}_n) = g_j(X^q)/g_0(X^q) = g_j(\mathfrak{Z})/g_0(\mathfrak{Z}) \quad (j = 1, \ldots, n). \tag{19}$$

Nun nehmen wir indirekt an, es sei $a(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) = 0$. Dann ist auch $a(X, \mathfrak{Y}, \mathfrak{Z}; \mathfrak{W}_1, \ldots, \mathfrak{W}_n) = 0$, folglich wegen (11) und (19), $b(X, \mathfrak{Y}, \mathfrak{Z}; g_1(\mathfrak{Z})/g_0(\mathfrak{Z}), \ldots, g_n(\mathfrak{Z})/g_0(\mathfrak{Z})) = 0$, daher weiter $c(X, \mathfrak{Y}, \mathfrak{Z}; g_0(\mathfrak{Z}), \ldots, g_n(\mathfrak{Z})) = 0$ und

$$d(X, \mathfrak{Y}, \mathfrak{Z}; g_0(\mathfrak{Z}), g_1(\mathfrak{Z}), \ldots, g_n(\mathfrak{Z})) = 0.$$

Nun gilt aber (15), und $\mathfrak{Y}$ ist algebraisch genau vom Grad $n$ über $F_q(X, \mathfrak{Z}) = F_q(X)$. Daher ist

$$d(X, Y, \mathfrak{Z}; g_0(\mathfrak{Z}), g_1(\mathfrak{Z}), \ldots, g_n(\mathfrak{Z})) = 0.$$

In dieser Identität substituieren wir $X_1 + X_2$ für $X$ und erhalten

$$d(X_1 + X_2, Y, X_1^q + X_2^q; g_0(X_1^q + X_2^q), \ldots, g_n(X_1^q + X_2^q)) = 0. \tag{20}$$

Die linke Seite von (20) ist gleich

$$d(X_1 + X_2, Y, X_1^q; g_0(X_1^q), \ldots, g_n(X_1^q)) + X_2^q e(X_1, X_2, Y)$$

mit einem Polynom $e(X_1, X_2, Y)$. Nun ist aber wegen (16)

$$\mathrm{Grad}_{X_2} d(X_1 + X_2, Y, X_1^q; g_0(X_1^q), \ldots, g_n(X_1^q)) < q.$$

Daher erhalten wir $d(X_1 + X_2, Y, X_1^q; g_0(X_1^q), \ldots, g_n(X_1^q)) = 0$, und da $X_1 + X_2, Y, X_1^q$ algebraisch unabhängig sind, die Identität

$$d(X, Y, Z; g_0(Z), \ldots, g_n(Z)) = 0.$$

Hieraus folgt $d(X, \mathfrak{Y}, Z; g_0(Z), \ldots, g_n(Z)) = 0$, weiter wegen (14), $c(X, \mathfrak{Y}, Z; g_0(Z), \ldots, g_n(Z)) = 0$. Da $g_0(X) \neq 0$, $g_0(Z) \neq 0$ ist, erhalten wir

$$b(X, \mathfrak{Y}, Z; g_1(Z)/g_0(Z), \ldots, g_n(Z)/g_0(Z)) = 0, \tag{21}$$

vermöge (12). Es seien $\mathfrak{U}_1, \ldots, \mathfrak{U}_n$ die Wurzeln von $f(Z, U)$ in $U$, also es sei

$$f(Z, U) = g_0(Z)(U - \mathfrak{U}_1) \ldots (U - \mathfrak{U}_n),$$



daher

$$l_j(\mathfrak{U}_1, \ldots, \mathfrak{U}_n) = g_j(Z)/g_0(Z) \quad (j = 1, \ldots, n).$$

Aus (11) und (21) folgt

$$a(X, \mathfrak{Y}, Z; \mathfrak{U}_1, \ldots, \mathfrak{U}_n) = 0.$$

Es gibt daher ein $t$, $1 \leqslant t \leqslant n$, sodaß $\mathfrak{U} = \mathfrak{U}_t$ der Gleichung

$$a(X, \mathfrak{Y}, Z, \mathfrak{U}) = 0 \tag{22}$$

genügt.

Es ist $f(X, \mathfrak{Y}) = 0$ und $f(Z, \mathfrak{U}) = 0$. Nach Hilfssatz 2 bilden die $n^2$ Elemente $\mathfrak{Y}^i \mathfrak{U}^k$ $(0 \leqslant i, k \leqslant n-1)$ eine Körperbasis von $F_q(X, \mathfrak{Y}, Z, \mathfrak{U})$ über $F_q(X, Z)$. Da $a(X, Y, Z, W)$ einen Grad $\leqslant n-1$ in $Y$ und einen Grad $\leqslant n-1$ in $W$ hat, ist (22) nur möglich, wenn $a(X, Y, Z, W) = 0$ ist. Diese letzte Gleichung steht aber im Widerspruch zur Voraussetzung.

**4. Die Ableitungen gewisser algebraischer Funktionen.** Da $f(X, Y)$ als Polynom in $Y$ separabel ist, ist $\mathfrak{Y}$ eine einfache Nullstelle, und die partielle Ableitung $f_Y(X, Y)$ hat

$$f_Y(X, \mathfrak{Y}) \neq 0.$$

Mit $D$ bezeichnen wir die Ableitung nach $X$ im Körper $F_q(X)$. Da $\mathfrak{Y}$ separabel über diesem Körper ist, kann $D$ auf genau eine Weise zu einer „Ableitung" in $F_q(X, \mathfrak{Y})$ fortgesetzt werden ([6], § 66). Offenbar ist $f_X(X, \mathfrak{Y}) + f_Y(X, \mathfrak{Y}) D\mathfrak{Y} = 0$, daher

$$D\mathfrak{Y} = -f_X(X, \mathfrak{Y})/f_Y(X, \mathfrak{Y}). \tag{23}$$

Im Folgenden sei

$$h(X, Y) = g_0(X)^{n-1} f_Y(X, Y).$$

Hilfssatz 4. *Die Größen $\mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}$ mögen (9) erfüllen, und $a(X, Y, Z, W)$ sei so wie in Hilfssatz 3. Dann gibt es Polynome $a^{(l)}(X, Y, Z, W)$ $(l = 0, 1, \ldots)$ mit folgenden Eigenschaften.*

(i)

$$a^{(l)}(X, Y, Z, W) = \sum_{i=0}^{n-1} \sum_{j=0}^{N} \sum_{k=0}^{n-1} b_{ijk}^{(l)}(X) Y^i Z^j W^k,$$

*wobei der Grad von $b_{ijk}^{(l)}(X)$ höchstens gleich $(q/n) - mn + 2lmn$ ist.*

(ii) *Die Koeffizienten der Polynome $b_{ijk}^{(l)}(X)$ sind lineare Kombinationen der Koeffizienten der Polynome $b_{ijk}(X)$ in (10).*

(iii) *Setzen wir*

$$s^{(l)}(X, Y) = a^{(l)}(X, Y, X^q, Y^q) h(X, Y)^{-2l}, \tag{24}$$

*dann gilt*

$$D^l a(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) = s^{(l)}(X, \mathfrak{Y}). \tag{25}$$

Beweis. Wir haben $D\mathfrak{Z} = D\mathfrak{W} = 0$, daher

$$\begin{aligned} Da(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) &= a_X(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) + a_Y(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W})\, D\mathfrak{Y} \\ &= b(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) f_Y(X, \mathfrak{Y})^{-1} \\ &= c(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) f_Y(X, \mathfrak{Y})^{-2} \end{aligned}$$

mit

$$b(X, Y, Z, W) = a_X(\ldots) f_Y(\ldots) - a_Y(\ldots) f_X(\ldots),$$

$$\mathrm{Grad}_X b \leqslant (q/n) - mn + m - 1, \quad \mathrm{Grad}_Y b \leqslant 2n - 2,$$

sowie mit

$$c(X, Y, Z, W) = b(X, Y, Z, W) f_Y(X, Y),$$

$$\mathrm{Grad}_X c \leqslant (q/n) - mn + 2m - 1, \quad \mathrm{Grad}_Y c \leqslant 3n - 3.$$

Nun sei für ein $l$ bereits

$$D^l a(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) = c^{(l)}(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) f_Y(X, \mathfrak{Y})^{-2l} \tag{26}$$

mit

$$\mathrm{Grad}_X c^{(l)} \leqslant (q/n) - mn + l(2m-1), \quad \mathrm{Grad}_Y c^{(l)} \leqslant (2l+1)(n-1)$$

gezeigt. Dann ist

$$Dc^{(l)}(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) = d^{(l)}(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) f_Y(X, \mathfrak{Y})^{-2}$$

mit

$$\mathrm{Grad}_X d^{(l)} \leqslant (q/n) - mn + (l+1)(2m-1), \quad \mathrm{Grad}_Y d^{(l)} \leqslant (2l+3)(n-1).$$

Weiter ist

$$D\left(f_Y(X, \mathfrak{Y})^{-2l}\right) = -2l f_Y(X, \mathfrak{Y})^{-2l-1} D f_Y(X, \mathfrak{Y}) = e^{(l)}(X, \mathfrak{Y}) f_Y(X, \mathfrak{Y})^{-2l-2}$$

mit

$$\mathrm{Grad}_X e^{(l)} \leqslant 2m - 1, \quad \mathrm{Grad}_Y e^{(l)} \leqslant 2n - 2.$$

Also ist

$$D^{l+1} a(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) = c^{(l+1)}(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) f_Y(X, \mathfrak{Y})^{-2l-2}$$

mit $c^{(l+1)} = d^{(l)} + c^{(l)} e^{(l)}$, daher mit

$$\mathrm{Grad}_X c^{(l+1)} \leqslant (q/n) - mn + (l+1)(2m-1), \quad \mathrm{Grad}_Y c^{(l+1)} \leqslant (2l+3)(n-1).$$

Somit gilt (26) auch für $l+1$, also für jedes $l$.

Indem wir (13) mit $\delta = 2l(n-1)$ anwenden, erhalten wir

$$c^{(l)}(X, \mathfrak{Y}, Z, W) = a^{(l)}(X, \mathfrak{Y}, Z, W) g_0(X)^{-2l(n-1)}$$

mit

$$\mathrm{Grad}_X a^{(l)} \leqslant (q/n) - mn + l(2m-1) + 2l(n-1)m, \quad \mathrm{Grad}_Y a^{(l)} \leqslant n - 1.$$

Das Polynom $a^{(l)}(X, Y, Z, W)$ hat die gewünschten Eigenschaften.



**5. Konstruktion zweier algebraischer Funktionen.** Es sei $d(X)$ die Diskriminante von $f(X, Y)$ als Polynom in $Y$. Da $f(X, Y)$ in $Y$ separabel ist, muß $d(X) \neq 0$ sein. Offenbar ist $d(X)$ vom Grad $\leqslant m(2n-2) < 2mn$. Es sei $\sigma$ die Menge der $x \in F_q$ mit $d(x) \neq 0$. Für die Anzahl $|\sigma|$ der Elemente von $\sigma$ gelten die Ungleichungen

$$q - 2mn < |\sigma| \leqslant q. \tag{27}$$

Ist $x \in \sigma$, dann sei $\nu(x)$ die Menge der $y \in \overline{F}_q$ mit $f(x, y) = 0$. Für $x \in \sigma$ hat das Polynom $f(x, Y)$ in $Y$ den Grad $n$ und hat $n$ verschiedene Wurzeln, woraus

$$|\nu(x)| = n$$

folgt. $\nu(x)$ ist die Vereinigungsmenge der beiden fremden Mengen $\nu_1(x)$ und $\nu_2(x)$, wobei $\nu_1(x)$ aus allen $y \in \nu(x)$ mit $y \in F_q$, und $\nu_2(x)$ aus allen $y \in \nu(x)$ mit $y \notin F_q$ besteht. Insbesonders ist

$$|\nu_1(x)| + |\nu_2(x)| = n \quad (x \in \sigma). \tag{28}$$

Bilden wir

$$e_1(X, Y, Y') = Y - Y',$$

$$e_2(X, Y, Y') = \sum_{j=1}^{n} y_{n-j}(X)(Y^{j-1} + Y^{j-2}Y' + \ldots + Y'^{j-1}),$$

dann gilt die Identität

$$f(X, Y) - f(X, Y') = e_1(X, Y, Y') e_2(X, Y, Y').$$

Ist $x \in \sigma$, $y \in \nu(x)$, also $f(x, y) = 0$, dann ist auch

$$f(x, y^q) = f(x^q, y^q) = f(x, y)^q = 0.$$

Daraus folgt

$$f(x, y) - f(x, y^q) = e_1(x, y, y^q) e_2(x, y, y^q) = (y - y^q) e_2(x, y, y^q) = 0.$$

Da nun $y$ eine einfache Wurzel von $f(x, Y)$ ist, haben wir $e_2(x, y, y) \neq 0$, und es gilt genau eine der beiden Gleichungen

$$e_1(x, y, y^q) = y - y^q = 0$$

und

$$e_2(x, y, y^q) = 0.$$

Die Elemente $y \in F_q$ sind durch $y^q = y$ charakterisiert; also gilt die erste der beiden Gleichungen genau dann, wenn $y \in \nu_1(x)$ ist. Daher ist

*$\nu_i(x)$ die Menge der $y \in \overline{F}_q$ mit $f(x, y) = 0$ und $e_i(x, y, y^q) = 0$ $(i = 1, 2)$.*

Wir setzen

$$\varepsilon_1 = 1, \quad \varepsilon_2 = n - 1. \tag{29}$$

Hilfssatz 5. *Es sei $M$ eine natürliche Zahl mit*

$$M^2(n^2+1) + (M+m)n^2 < q. \tag{30}$$

*Wir setzen*

$$N_i = [(\varepsilon_i/n)(M+m)] \qquad (i = 1, 2), \tag{31}$$

*wobei* [ ] *die nächst kleinere ganze Zahl bedeutet.*

*Dann gibt es Polynome* $a_i(X, Y, Z, W)$ *von der in Hilfssatz 3 betrachteten Gestalt mit* $N = N_i$ $(i = 1, 2)$, *sodaß für die in Hilfssatz 4 konstruierten rationalen Funktionen* $s_i^{(l)}(X, Y)$ $(i = 1, 2)$ *die Gleichungen*

$$s_i^{(l)}(x, y) = 0 \qquad (l = 0, 1, \ldots, M-1) \tag{32}$$

*für alle* $(x, y)$ *mit* $x \in \sigma$, $y \in \nu_i(x)$ *gelten.*

(Zur Interpretation ist zu sagen, daß $a_i(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W})$ eine algebraische Funktion ist, die auf den endlichen Punkten der Riemannschen Fläche von $f(X, Y) = 0$ eindeutig definiert ist. Infolge Hilfssatz 4 besagt (32), daß diese algebraische Funktion und viele Ableitungen derselben im Punkt $(x, y)$ der Riemannschen Fläche verschwinden.)

Beweis. Die Fälle $i = 1$ und $i = 2$ sind voneinander unabhängig und wurden nur der Bequemlichkeit halber in einen Hilfssatz zusammengefaßt. Im Beweis dürfen wir uns daher $i$ als fest gegeben denken. Ist $x \in \sigma$ und $y \in \nu(x)$, dann ist $g_0(x) \neq 0$, $f_Y(x, y) \neq 0$, und $h(x, y) \neq 0$. Auf Grund von (24) sind die Bedingungen (32) sicher erfüllt, falls $a_i^{(l)}(x, y, x^q, y^q) = 0$ ist für $l = 0, 1, \ldots, M-1$, also falls

$$a_i^{(l)}(x, y, x, y^q) = 0 \quad \text{ist für} \quad l = 0, 1, \ldots, M-1 \tag{33}$$

und für alle $(x, y)$ mit $x \in \sigma$, $y \in \nu_i(x)$.

Ist $i = 1$, so gilt $y^q = y$, und (33) ist gleichbedeutend mit

$$c_1^{(l)}(x, y, y^q) = 0 \qquad (l = 0, 1 \ldots, M-1),$$

wobei $c_1^{(l)}(X, Y, Y') = a_1^{(l)}(X, Y, X, Y)$ ist. Insbesonders ist $c_1^{(l)}(X, Y, Y')$ vom Grad $\leqslant (q/n) - mn + 2lmn + N_1$ in $X$, vom Grad $\leqslant 2n-2$ in $Y$, und vom Grad $0 = \varepsilon_1 - 1$ in $Y'$.

Ist $i = 2$, dann gilt $e_2(x, y, y^q) = 0$. Nun ist $e_2(X, Y, Y')$ ein Polynom vom Grad $\leqslant m$ in $X$ und vom Grad $n-1$ in $Y$ und in $Y'$. Der Koeffizient von $Y'^{n-1}$ ist $g_0(X)$. Wir haben also $g_0(x)y^{q(n-1)} = d(x, y, y^q)$, wo $d(X, Y, Y')$ ein von $x, y, y'$ unabhängiges Polynom vom Grad $\leqslant m$ in $X$, vom Grad $n-1$ in $Y$ und vom Grad $\leqslant n-2 = \varepsilon_2 - 1$ in $Y'$ ist. Es ist daher weiter $g_0(x)a_2^{(l)}(x, y, x, y^q) = c_2^{(l)}(x, y, y^q)$, wobei $c_2^{(l)}(X, Y, Y')$ vom Grad $\leqslant (q/n) - mn + 2lmn + m + N_2$ in $X$, vom Grad $\leqslant 2n-2$ in $Y$ und vom Grad $\leqslant \varepsilon_2 - 1$ in $Y'$ ist.

In beiden Fällen ist also (33) gleichbedeutend mit

$$c_i^{(l)}(x, y, y^q) = 0 \qquad (l = 0, 1, \ldots, M-1), \tag{34}$$

wobei $c_i^{(l)}(X, Y, Y')$ ein Polynom mit

$$\operatorname{Grad}_X c_i^{(l)}(X, Y, Y') \leqslant (q/n) - mn + 2lmn + m + N_i,$$
$$\operatorname{Grad}_Y c_i^{(l)}(X, Y, Y') \leqslant 2n-2, \qquad \operatorname{Grad}_{Y'} c_i^{(l)}(X, Y, Y') \leqslant \varepsilon_i - 1$$



ist. Da nun $f(x, y) = 0$ und $g_0(x) \neq 0$ ist, haben wir gemäß (13)

$$g_0(x)^\delta y^{n-1+\delta} = g_1^{(\delta)}(x)y^{n-1} + \ldots + g_n^{(\delta)}(x) \qquad (\delta = 1, 2, \ldots),$$

und hieraus folgt

$$g_0(x)^{n-1} c_i^{(l)}(x, y, y^q) = d_i^{(l)}(x, y, y^q),$$

wobei $d_i^{(l)}(X, Y, Y')$ ein Polynom mit

$$\operatorname{Grad}_X d_i^{(l)}(X, Y, Y') \leqslant (q/n) - mn + 2lmn + m + N_i + m(n-1)$$
$$= (q/n) + 2lmn + N_i,$$
$$\operatorname{Grad}_Y d_i^{(l)}(X, Y, Y') \leqslant n-1, \qquad \operatorname{Grad}_{Y'} d_i^{(l)}(X, Y, Y') \leqslant \varepsilon_i - 1$$

ist.

Die Bedingungen (34) sind sicher für alle $(x, y)$ mit $x \in \sigma$, $y \in \nu_i(x)$ erfüllt, falls die Polynome $d_i^{(l)}(X, Y, Y')$ $(l = 0, 1, \ldots, M-1)$ identisch verschwinden. Die Anzahl der Koeffizienten von $d_i^{(l)}$ ist

$$\leqslant n\varepsilon_i\big((q/n) + 2lmn + N_i + 1\big),$$

und die Anzahl $B_i$ der Koeffizienten aller Polynome $d_i^{(l)}$ mit $0 \leqslant l \leqslant M-1$ leistet

$$\begin{aligned} B_i &\leqslant n\varepsilon_i\big(M\big((q/n) + N_i + 1\big) + M(M-1)mn\big) \\ &\leqslant \varepsilon_i\big(Mq + M\big((n-1)(M+m) + n\big) + M(M-1)mn^2\big) \\ &= \varepsilon_i\big(Mq + M^2(mn^2 + n - 1) - M\big(mn^2 - m(n-1) - n\big)\big) \\ &\leqslant \varepsilon_i\big(Mq + M^2 m(n^2+1)\big), \end{aligned}$$

denn wegen (5), (29), (31) ist $nN_i \leqslant (n-1)(M+m)$, sowie

$$mn^2 + n - 1 \leqslant mn^2 + m = m(n^2+1) \qquad \text{und} \qquad mn^2 \geqslant m(n-1) + n.$$

Jeder dieser Koeffizienten ist eine lineare Kombination der Koeffizienten von $a_i(X, Y, Z, W)$. Die Anzahl $C_i$ der Koeffizienten von $a_i(X, Y, Z, W)$ leistet

$$\begin{aligned} C_i &\geqslant n^2(N_i+1)\big((q/n) - mn\big) \geqslant n^2(\varepsilon_i/n)(M+m)\big((q/n) - mn\big) \\ &= \varepsilon_i(M+m)(q - mn^2) > B_i \end{aligned}$$

wegen (30). Wir haben $B_i$ lineare homogene Gleichungen in den $C_i$ Koeffizienten von $a_i(X, Y, Z, W)$. Da nun $C_i > B_i$ ist, hat dieses Gleichungssystem eine nicht triviale Lösung.

### 6. Konstruktion zweier Polynome.

Hilfssatz 6. *Die natürliche Zahl* $M$ *möge* (30) *befriedigen. Dann gibt es nicht identisch verschwindende Polynome* $h_i(X)$ $(i = 1, 2)$ *mit*

$$\operatorname{Grad} h_i(X) \leqslant q(\varepsilon_i M + 2mn - 2m + 1), \tag{35}$$

*sodaß*

$$D^l h_i(x) = 0 \qquad (0 \leqslant l < M\,|v_i(x)|) \tag{36}$$

*für jedes* $x \in \sigma$ *gilt.*

Beweis. Die beiden Fälle $i = 1$ und $i = 2$ sind wieder unabhängig, sodaß wir $i$ als fest ansehen dürfen. So wie schon früher seien $\mathfrak{Y}_1 = \mathfrak{Y}$, $\mathfrak{Y}_2, \ldots, \mathfrak{Y}_n$ die Wurzeln in $Y$ von $f(X, Y)$, also es gelte (17). Ist $a_i(X, Y, Z, W)$ das in Hilfssatz 5 konstruierte Polynom, dann setzen wir

$$\begin{aligned} h_i(X) &= g_0(X)^{(n-1)(q+1)}\,\mathfrak{N}\big(a_i(X, \mathfrak{Y}, 3, \mathfrak{W})\big) \\ &= g_0(X)^{(n-1)(q+1)} \prod_{t=1}^{n} a_i(X, \mathfrak{Y}_t, X^q, \mathfrak{Y}_t^q), \end{aligned} \tag{37}$$

wo $\mathfrak{N}$ die Norm von $F_q(X, \mathfrak{Y})$ nach $F_q(X)$ bedeutet.

Nun ist

$$\prod_{t=1}^{n} a_i(X, Y_t, X^q, Y_t^q)$$

vom Grad $\leqslant n\big(qN_i + (q/n) - mn\big)$ in $X$ und vom Grad $\leqslant (n-1)(q+1)$ in $Y_t$ $(1 \leqslant t \leqslant n)$. Infolge von Hilfssatz 1 und wegen

$$l_j(\mathfrak{Y}_1, \ldots, \mathfrak{Y}_n) = g_j(X)/g_0(X) \qquad (j = 1, \ldots, n)$$

ist daher

$$h_i(X) = k_i\big(X, g_0(X), \ldots, g_n(X)\big),$$

wobei $k_i(X, U_0, \ldots, U_n)$ ein Polynom ist, das vom Grad $\leqslant n\big(qN_i + (q/n) - mn\big)$ in $X$ ist, und das homogen vom Grad $(n-1)(q+1)$ in $U_0, \ldots, U_n$ ist. Daher ist $h_i(X)$ ein Polynom vom Grad

$$\begin{aligned} &\leqslant nqN_i + q - mn^2 + m(n-1)(q+1) \\ &< q\big(nN_i + m(n-1) + 1\big) \\ &\leqslant q\big(n(\varepsilon_i/n)(M+m) + m(n-1) + 1\big) \\ &\leqslant q\big(\varepsilon_i M + 2m(n-1) + 1\big) \end{aligned}$$

wegen (31) und (29). Infolge Hilfssatz 3 ist $h_i(X) \not\equiv 0$.

Wir haben $D^u a_i(X, \mathfrak{Y}_t, X^q, \mathfrak{Y}_t^q) = s_i^{(u)}(X, \mathfrak{Y}_t)$ $(u = 0, 1, \ldots)$ und daher

$$D^l h_i(X) = \sum_{u_0+u_1+\ldots+u_n=l} \left(\frac{l!}{u_0!\,u_1!\ldots u_n!}\right)^{(3)} \big(D^{u_0} g_0(X)^{(n-1)(q+1)}\big) \times \times \prod_{t=1}^{n} s_i^{(u_t)}(X, \mathfrak{Y}_t), \tag{38}$$

(3) Dieser Bruch soll die Restklasse modulo $p$ der ganzen Zahl $l!\,(u_0!\ldots u_n!)^{-1}$ bedeuten.



wobei die Summe über nicht-negative ganze Zahlen $u_0, u_1, \ldots, u_n$ erstreckt ist. Wir können kurz schreiben

$$D^l h_i(X) = p_i^{(l)}(X, \mathfrak{Y}_1, \ldots, \mathfrak{Y}_n),$$

wobei $p_i^{(l)}(X, Y_1, \ldots, Y_n)$ eine in $Y_1, \ldots, Y_n$ symmetrische rationale Funktion ist. Daher gibt es eine rationale Funktion

$$q_i^{(l)}(X, U_1, \ldots, U_n)$$

mit

$$p_i^{(l)}(X, Y_1, \ldots, Y_n) = q_i^{(l)}\big(X, l_1(Y_1, \ldots, Y_n), \ldots, l_n(Y_1, \ldots, Y_n)\big),$$

und daher mit

$$\begin{aligned} D^l h_i(X) &= q_i^{(l)}\big(X, l_1(\mathfrak{Y}_1, \ldots, \mathfrak{Y}_n), \ldots, l_n(\mathfrak{Y}_1, \ldots, \mathfrak{Y}_n)\big) \\ &= q_i^{(l)}\big(X, g_1(X)/g_0(X), \ldots, g_n(X)/g_0(X)\big). \end{aligned}$$

Nun sei $x \in \sigma$, und $y_1, \ldots, y_n$ seien die Elemente von $v(x)$. Dann ist $f(x, y_t) = 0$ $(t = 1, \ldots, n)$ und $l_j(y_1, \ldots, y_n) = g_j(x)/g_0(x)$ $(1 \leqslant j \leqslant n)$, folglich

$$\begin{aligned} D^l h_i(x) &= q_i^{(l)}\big(x, g_1(x)/g_0(x), \ldots, g_n(x)/g_0(x)\big) \\ &= q_i^{(l)}\big(x, l_1(y_1, \ldots, y_n), \ldots, l_n(y_1, \ldots, y_n)\big) \\ &= p_i^{(l)}(x, y_1, \ldots, y_n). \end{aligned}$$

Nun möge $v_i(x)$ ohne Beschränkung der Allgemeinheit aus $y_1, \ldots, y_{|v_i|}$ bestehen(4). Es sei $0 \leqslant l < M\,|v_i(x)|$. Jeder Summand von $p_i^{(l)}(x, y_1, \ldots, y_n)$ hat einen Faktor $s_i^{(u_t)}(x, y_t)$ mit $1 \leqslant t \leqslant |v_i| = |v_i(x)|$ und $u_t \leqslant l/|v_i(x)|$, daher mit $u_t < M$. Nach Hilfssatz 5 ist $s_i^{(u_t)}(x, y_t) = 0$, und Hilfssatz 6 folgt.

**7. Beweis des Satzes für den Fall eines Primkörpers.** Es sei jetzt $F_q$ ein Primkörper, also es sei

$$q = p.$$

Ist $h(X)$ ein Polynom und ist

$$0 = h(c) = Dh(c) = \ldots = D^{L-1}h(c)$$

mit $L \leqslant q = p$, dann ist $h(X)$ durch $(X-c)^L$ teilbar. Ist nun

$$Mn \leqslant q, \tag{39}$$

dann ist $M\,|v_i(x)| \leqslant q$, und das Polynom $h_i(X)$ von Hilfssatz 6 ist durch $(X-x)^{M|v_i(x)|}$ teilbar $(i = 1, 2)$. Das gilt für jedes $x \in \sigma$. Setzen wir jetzt

$$Z_i = \sum_{x \in \sigma} |v_i(x)| \qquad (i = 1, 2),$$

(4) Man kann das nicht zugleich für $i = 1$ und $i = 2$ verlangen, doch ist $i$ im Augenblick ja fest.

dann ist der Grad von $h_i(X)$ mindestens gleich $MZ_i$. In Verbindung mit (35) gibt das

$$Z_i \leqslant q(\varepsilon_i + (2mn-2m+1)M^{-1}) \quad (i = 1, 2).$$

Die Anzahl $A$ der Lösungen der gegebenen Gleichung (2) befriedigt wegen (27), (28) und (29) die Ungleichungen

$$A \leqslant Z_1 + n(q-|\sigma|) < Z_1 + 2mn^2 \leqslant q + (2mn-2m+1)(q/M) + 2mn^2$$

und

$$\begin{aligned} A &\geqslant Z_1 = (Z_1+Z_2) - Z_2 = n|\sigma| - Z_2 \geqslant n(q-2mn) - Z_2 \\ &\geqslant q - (2mn-2m+1)(q/M) - 2mn^2, \end{aligned}$$

daher

$$|A-q| \leqslant (2mn-2m+1)(q/M) + 2mn^2. \tag{40}$$

All das gilt, falls $M$ die Bedingungen (30) und (39) erfüllt. Das ist jedenfalls so, wenn

$$M \geqslant m \quad \text{und} \quad (n^2+1)(M+1)^2 \leqslant q$$

ist. Setzen wir

$$M = \left[\left(\frac{q}{n^2+1}\right)^{1/2}\right] - 1,$$

dann ist

$$M > \left(q/(n^2+1)\right)^{1/2} - 2 \geqslant q^{1/2}/(n+1) \geqslant m,$$

denn es ist

$$q^{1/2}\left((n^2+1)^{-1/2} - (n^2+2n+1)^{-1/2}\right) \geqslant q^{1/2}\,\tfrac{1}{2}\frac{2n}{(n+1)^3} \geqslant 2$$

wegen (1) und (5). Setzt man diesen Wert von $M$ in (40) ein, dann erhält man

$$\begin{aligned} |A-q| &< (2mn-2m+1)q^{1/2}(n+1) + 2mn^2 \\ &= (2mn^2-2m+n+1)q^{1/2} + 2mn^2. \end{aligned}$$

Wegen (1) und (5) ist $(m-1)(m+1)(n+1) = m^2n + m^2 - n - 1 \geqslant m^2n \geqslant mn^2$, weiter

$$(2m-n-1)q^{1/2} \geqslant (m-1)q^{1/2} \geqslant 3(m-1)(m+1)(n+1) \geqslant 2mn^2,$$

daher schließlich

$$|A-q| < 2mn^2q^{1/2} = 2\,\mathrm{Min}\,(m^2n, n^2m)\,q^{1/2}.$$



**8. Höhere Differentiale.** Ist $q = p^\varkappa$ mit $\varkappa > 1$ und ist $h(X)$ ein Polynom mit Koeffizienten in $F_q$, dann kann man aus

$$0 = h(c) = Dh(c) = \ldots = D^{L-1}h(c)$$

mit $L \leqslant q$ nicht schließen, daß $h(X)$ durch $(X-c)^L$ teilbar ist. (Das geht nur für $L \leqslant p$.)

Ist $S$ ein Ring, dann sei $S[X]$ der Ring der Polynome in $X$ mit Koeffizienten in $S$. Es sei $\varphi$ der Homomorphismus von den ganzen Zahlen auf den Primkörper $F_p$. Weiter seien $E^{(l)}$ $(l = 0, 1, \ldots)$ die durch

$$E^{(l)}(c_0 + c_1X + \ldots + c_jX^j) = c_l + c_{l+1}\varphi\left(\binom{l+1}{l}\right)X + \ldots + c_j\varphi\left(\binom{j}{l}\right)X^{j-l}$$

definierten linearen Operatoren auf $F_q[X]$. Man kann leicht zeigen, daß

$$E^{(l)}(X-c)^j = \varphi\left(\binom{j}{l}\right)(X-c)^{j-l}$$

ist. Aus der Bedingung

$$0 = E^{(0)}h(c) = E^{(1)}h(c) = \ldots = E^{(L-1)}h(c)$$

für ein Polynom $h(X)$ folgt daher, daß $h(X)$ durch $(X-c)^L$ teilbar ist. Man kann aber $E^{(l+1)}h(X)$ nicht rekursiv aus $E^{(l)}h(X)$ berechnen. Um diese Schwierigkeit zu überwinden, müssen wir im Folgenden gewisse algebraische Hilfsmittel einführen. Wir werden dabei ganz elementar vorgehen.

Wir werden einige Ringe und Körper der Charakteristik Null konstruieren. Die Elemente dieser Ringe und Körper werden mit $\hat{a}, \hat{b}, \hat{a}(X), \ldots$ bezeichnet werden, mit Ausnahme der Primzahl $p$. Ist $\hat{a} = p^\nu\hat{b}/\hat{c}$ eine rationale Zahl mit nicht durch $p$ teilbaren ganzen Zahlen $\hat{b}, \hat{c}$, dann setzen wir $\nu(\hat{a}) = \nu$. Weiter setzen wir $\nu(0) = +\infty$. Für rationale Zahlen $\hat{a}, \hat{a}'$ gilt offenbar

$$\nu(\hat{a}+\hat{a}') \geqslant \mathrm{Min}\left(\nu(\hat{a}), \nu(\hat{a}')\right), \qquad \nu(\hat{a}\hat{a}') = \nu(\hat{a}) + \nu(\hat{a}'),$$

und daher ist $\nu$ eine „Exponentenbewertung" der rationalen Zahlen. Es sei $\boldsymbol{Q}_0$ der Ring der rationalen Zahlen $\hat{a}$ mit $\nu(\hat{a}) \geqslant 0$. Dann kann $\varphi$ auf genau eine Weise zu einem Homomorphismus von $\boldsymbol{Q}_0$ auf $F_p$ fortgesetzt werden; dieser neue Homomorphismus werde ebenfalls mit $\varphi$ bezeichnet. Schließlich kann $\varphi$ zu einem Homomorphismus von $\boldsymbol{Q}_0[X]$ auf $F_p[X]$ mit $\varphi(X) = X$ fortgesetzt werden.

Der Körper $F_q$ entstehe aus dem Primkörper $F_p$ durch Adjunktion des Elementes $z$. Es sei $a(X) = X^\varkappa + a_1X^{\varkappa-1} + \ldots + a_\varkappa$ das Minimalpolynom von $z$ über $F_p$. Es sei $\hat{a}(X) = X^\varkappa + \hat{a}_1X^{\varkappa-1} + \ldots + \hat{a}_\varkappa$ ein Polynom in $\boldsymbol{Q}_0[X]$ mit $\varphi(\hat{a}(X)) = a(X)$. Dann ist $\hat{a}(X)$ irreduzibel. Es sei $\hat{z}$ eine Wurzel von $\hat{a}(X)$, und $K$ sei der algebraische Zahlkörper vom Grad $\varkappa$, der aus den rationalen Zahlen durch Adjunktion von $\hat{z}$ entsteht. (Es

macht uns nichts aus, daß $K$ von $z$ und von $\hat{a}(X)$ abhängt). Das allgemeine Element von $K$ ist von der Gestalt

$$\hat{u} = \hat{b}_1\hat{z}^{\varkappa-1} + \hat{b}_2\hat{z}^{\varkappa-2} + \ldots + \hat{b}_\varkappa$$

mit rationalen Koeffizienten $\hat{b}_1, \ldots, \hat{b}_\varkappa$. Wir setzen

$$v(\hat{u}) = \mathrm{Min}\big(v(\hat{b}_1), \ldots, v(\hat{b}_\varkappa)\big).$$

Da $\hat{z}^\varkappa = -\hat{a}_1\hat{z}^{\varkappa-1} - \ldots - \hat{a}_\varkappa$ ist mit $\hat{a}_i \in \boldsymbol{Q}_0$, bilden die Elemente $u$ mit $v(\hat{u}) \geqq 0$ einen Teilring $K_0$ von $K$. Die Abbildung $\psi$ mit

$$\psi(\hat{b}_1\hat{z}^{\varkappa-1} + \ldots + \hat{b}_\varkappa) = \varphi(\hat{b}_1)z^{\varkappa-1} + \ldots + \varphi(\hat{b}_\varkappa)$$

ist ein Homomorphismus von $K_0$ auf $F_q$, dessen Kern $K_1$ aus den Elementen $\hat{u}$ mit $v(\hat{u}) \geqq 1$ besteht. Für beliebige Elemente $\hat{u}$, $\hat{u}'$ von $K$ ist wieder

$$v(\hat{u}+\hat{u}') \geqq \mathrm{Min}\big(v(\hat{u}), v(\hat{u}')\big), \qquad v(\hat{u}\hat{u}') = v(\hat{u}) + v(\hat{u}'). \tag{41}$$

Die Erste dieser beiden Relationen ist trivial. Was die Zweite betrifft, so kann man ihren Beweis sofort auf den Spezialfall mit $v(\hat{u}) = v(\hat{u}') = 0$ zurückführen. Dann ist $\hat{u}, \hat{u}' \in K_0$, daher $\hat{u}\hat{u}' \in K_0$, daher schließlich $v(\hat{u}\hat{u}') \geqq 0$. Wäre $v(\hat{u}\hat{u}') \geqq 1$, dann wäre $\hat{u}\hat{u}' \in K_1$, daher $\psi(\hat{u})\psi(\hat{u}') = \psi(\hat{u}\hat{u}') = 0$, also entweder $\psi(\hat{u}) = 0$ oder $\psi(\hat{u}') = 0$, also entweder $v(\hat{u}) \geqq 1$ oder $v(\hat{u}') \geqq 1$, entgegen der Voraussetzung.

Für ein Polynom

$$\hat{c}(X) = \hat{c}_0 + \hat{c}_1 X + \ldots + \hat{c}_l X^l$$

aus $K[X]$ setzen wir

$$v\big(\hat{c}(X)\big) = \mathrm{Min}\big(v(\hat{c}_0), \ldots, v(\hat{c}_l)\big).$$

Die Elemente $\hat{c}(X)$ mit $v\big(\hat{c}(X)\big) \geqq 0$ bilden den Teilring $K_0[X]$ von $K[X]$. Der Homomorphismus $\psi$ kann zu einem Homomorphismus von $K_0[X]$ auf $F_q[X]$ mit $\psi(X) = X$ fortgesetzt werden. Für beliebige Polynome $\hat{c}(X)$, $\hat{c}'(X)$ von $K[X]$ ist

$$\begin{aligned} v\big(\hat{c}(X)+\hat{c}'(X)\big) &\geqq \mathrm{Min}\big(v\big(\hat{c}(X)\big), v\big(\hat{c}'(X)\big)\big), \\ v\big(\hat{c}(X)\hat{c}'(X)\big) &= v\big(\hat{c}(X)\big) + v\big(\hat{c}'(X)\big). \end{aligned} \tag{42}$$

Der Beweis erfolgt so wie für (41).

Ist $\hat{c}(X) = \hat{c}_1(X)/\hat{c}_2(X) \in K(X)$ mit $\hat{c}_1(X), \hat{c}_2(X) \in K[X]$, dann setzen wir $v\big(\hat{c}(X)\big) = v\big(\hat{c}_1(X)\big) - v\big(\hat{c}_2(X)\big)$. Dann gilt (42) für alle Elemente $\hat{c}(X)$ von $K(X)$. Die Elemente $\hat{c}(X)$ von $K(X)$ mit $v\big(\hat{c}(X)\big) \geqq 0$ bilden einen Teilring, den wir mit $K(X)_0$ bezeichnen. Die Abbildung $\psi$ kann auf genau eine Weise zu einem Homomorphismus von $K(X)_0$ auf $F_q(X)$ fortgesetzt werden.



Es sei

$$f(X, Y) = g_0(X)Y^n + \ldots + g_n(X)$$

das gegebene Polynom in $F_q[X, Y]$. Es seien $\hat{g}_0(X), \ldots, \hat{g}_n(X)$ Polynome in $K_0[X]$ mit $\psi\big(\hat{g}_i(X)\big) = g_i(X)$ und $\mathrm{Grad}\,\hat{g}_i(X) = \mathrm{Grad}\,g_i(X)$ $(i = 0, 1, \ldots, n)$. Wir bilden

$$\hat{f}(X, Y) = \hat{g}_0(X)Y^n + \ldots + \hat{g}_n(X).$$

Es sei $\hat{\mathfrak{Y}}$ ein über $K(X)$ algebraisches Element mit $\hat{f}(X, \hat{\mathfrak{Y}}) = 0$. Nun ist $g_0(X) \neq 0$, daher $v\big(\hat{g}_0(X)\big) = 0$, daher

$$\hat{\mathfrak{Y}}^n = \hat{r}_1(X)\hat{\mathfrak{Y}}^{n-1} + \ldots + \hat{r}_n(X) \tag{43}$$

mit $\hat{r}_i(X) \in K(X)_0$. Ist

$$\hat{\mathfrak{U}} = \hat{s}_1(X)\hat{\mathfrak{Y}}^{n-1} + \ldots + \hat{s}_n(X)$$

ein beliebiges Element von $K(X, \hat{\mathfrak{Y}})$, dann setzen wir

$$v(\hat{\mathfrak{U}}) = \mathrm{Min}\big(v\big(\hat{s}_1(X)\big), \ldots, v\big(\hat{s}_n(X)\big)\big).$$

Infolge (43) bilden die Elemente $\hat{\mathfrak{U}}$ mit $v(\hat{\mathfrak{U}}) \geqq 0$ einen Teilring $K(X, \hat{\mathfrak{Y}})_0$ von $K(X, \hat{\mathfrak{Y}})$. Es kann $\psi$ durch die Formel

$$\psi\big(\hat{s}_1(X)\hat{\mathfrak{Y}}^{n-1} + \ldots + \hat{s}_n(X)\big) = \psi\big(\hat{s}_1(X)\big)\mathfrak{Y}^{n-1} + \ldots + \psi\big(\hat{s}_n(X)\big)$$

zu einem Homomorphismus von $K(X, \hat{\mathfrak{Y}})_0$ auf $F_q(X, \mathfrak{Y})$ fortgesetzt werden. Man sieht ebenso wie in (41), daß für beliebige $\hat{\mathfrak{U}}, \hat{\mathfrak{U}}'$ aus $K(X, \hat{\mathfrak{Y}})$ die Beziehungen

$$v(\hat{\mathfrak{U}}+\hat{\mathfrak{U}}') \geqq \mathrm{Min}\big(v(\mathfrak{U}), v(\mathfrak{U}')\big), \qquad v(\mathfrak{U}\mathfrak{U}') = v(\hat{\mathfrak{U}}) + v(\hat{\mathfrak{U}}') \tag{44}$$

gelten.

Wir hoffen, ein etwaiger Leser hat nach diesen ziemlich pedantischen Ausführungen nicht die Geduld verloren. Es sei jetzt $\hat{D}$ die Ableitung nach $X$ im Körper $K(X)$. Da $\hat{\mathfrak{Y}}$ separabel über $K(X)$ ist, kann $\hat{D}$ auf eindeutige Weise zu einer Ableitung in $K(X, \hat{\mathfrak{Y}})$ fortgesetzt werden. Wir setzen

$$\hat{E}^{(l)}(\hat{\mathfrak{U}}) = \frac{1}{l!}D^l\hat{\mathfrak{U}} \qquad (l = 0, 1, \ldots) \tag{45}$$

für $\hat{\mathfrak{U}} \in K(X, \hat{\mathfrak{Y}})$. Dann gilt für beliebige $\hat{\mathfrak{U}}, \hat{\mathfrak{B}}$

$$\hat{E}^{(l)}(\hat{\mathfrak{U}}\hat{\mathfrak{B}}) = \sum_{i=0}^{l} \hat{E}^{(i)}(\hat{\mathfrak{U}})\hat{E}^{(l-i)}(\hat{\mathfrak{B}}). \tag{46}$$

HILFSSATZ 7. *Für jedes* $\hat{\mathfrak{U}} \neq 0$ *in* $K(X, \hat{\mathfrak{Y}})$ *ist*

$$v(\hat{E}^{(l)}\hat{\mathfrak{U}}) \geqslant v(\hat{\mathfrak{U}}) \qquad (l = 0, 1, \ldots).$$

Beweis. Nur $l = 0$ ist die Behauptung richtig. Ist sie für $0, 1, \ldots, l-1$ schon gezeigt, dann schließen wir für den Fall $l$ wie folgt.

(i) Die Behauptung ist richtig, falls $\hat{\mathfrak{U}} = X^t$ mit $t \geqslant 0$ ist, und daher gilt sie allgemeiner für $\hat{\mathfrak{U}} \in K[X]$.

(ii) Nun sei $\hat{\mathfrak{U}} \in K(X)$. Es sei zunächst $v(\hat{\mathfrak{U}}) = 0$. Dann gibt es $\hat{\mathfrak{B}}_0$, $\hat{\mathfrak{B}}_1 \in K[X]$ mit $\hat{\mathfrak{B}}_0\hat{\mathfrak{U}} = \hat{\mathfrak{B}}_1$ und mit $v(\hat{\mathfrak{B}}_0) = v(\hat{\mathfrak{B}}_1) = 0$. Wegen (i) ist $v(\hat{E}^{(l)}\hat{\mathfrak{B}}_1) \geqslant 0$, daher $v\big(\hat{E}^{(l)}(\hat{\mathfrak{B}}_0\hat{\mathfrak{U}})\big) \geqslant 0$. Nun ist aber

$$\hat{E}^{(l)}(\hat{\mathfrak{B}}_0\hat{\mathfrak{U}}) = \sum_{i=0}^{l} \hat{E}^{(l-i)}(\hat{\mathfrak{B}}_0)\,\hat{E}^{(i)}(\hat{\mathfrak{U}}).$$

Wegen (i) und nach Induktionsannahme ist

$$v\big(\hat{E}^{(l-i)}(\hat{\mathfrak{B}}_0)\hat{E}^{(i)}(\hat{\mathfrak{U}})\big) = v(\hat{E}^{(l-i)}\hat{\mathfrak{B}}_0) + v(\hat{E}^{(i)}\hat{\mathfrak{U}}) \geqslant 0 \quad \text{für} \quad i < l,$$

und daher ist auch

$$v\big(\hat{E}^{(0)}(\hat{\mathfrak{B}}_0)\hat{E}^{(l)}(\hat{\mathfrak{U}})\big) \geqslant 0.$$

Aus $v(\hat{E}^{(0)}\hat{\mathfrak{B}}_0) = v(\hat{\mathfrak{B}}_0) = 0$ folgt $v(\hat{E}^{(l)}\hat{\mathfrak{U}}) \geqslant 0 = v(\hat{\mathfrak{U}})$, und die Behauptung stimmt für $\hat{\mathfrak{U}}$. Jedes $\hat{\mathfrak{U}} \neq 0$ aus $K(X)$ ist von der Gestalt $\hat{\mathfrak{U}} = p^r\hat{\mathfrak{U}}'$ mit $v(\hat{\mathfrak{U}}') = 0$, und daher gilt die Behauptung allgemein für $\hat{\mathfrak{U}} \in K(X)$.

(iii) Wegen (46), und da der Hilfssatz für $\hat{\mathfrak{U}} \in K(X)$ schon bewiesen ist, wird es für den allgemeinen Fall genügen, wenn wir noch zeigen, daß

$$v(\hat{E}^{(l)}\hat{\mathfrak{Y}}) \geqslant 0$$

ist. Es gilt

$$\hat{f}(X, \hat{\mathfrak{Y}}) = \hat{g}_0(X)\hat{\mathfrak{Y}}^n + \ldots + \hat{g}_n(X) = 0.$$

Nun ist

$$\hat{E}^{(l)}\big(\hat{g}_{n-i}(X)\hat{\mathfrak{Y}}^i\big) = \hat{E}^{(l)}\big(\hat{g}_{n-i}(X)\hat{\mathfrak{Y}}\ldots\hat{\mathfrak{Y}}\big) = \sum_{\substack{u_0, u_1, \ldots, u_i \geqslant 0 \\ u_0+u_1+\ldots+u_i = l}} \hat{E}^{(u_0)}\big(\hat{g}_{n-i}(X)\big)\,\hat{E}^{(u_1)}(\hat{\mathfrak{Y}})\ldots\hat{E}^{(u_i)}(\hat{\mathfrak{Y}}).$$

Die Summanden $\hat{\mathfrak{S}}(u_0, u_1, \ldots, u_i)$ mit $u_1 < l, \ldots, u_i < l$ haben $v\big(\hat{\mathfrak{S}}(u_0, u_1, \ldots, u_i)\big) \geqslant 0$ wegen (i) und wegen unserer Induktionsannahme. Die Summe der übrigen Summanden ist $i\hat{g}_{n-i}(X)\hat{\mathfrak{Y}}^{i-1}\hat{E}^{(l)}(\hat{\mathfrak{Y}})$. Aus der Gleichung $\hat{E}^{(l)}\big(\hat{f}(X, \hat{\mathfrak{Y}})\big) = 0$ folgt daher die Relation

$$v\big(\hat{f}_Y(X, \hat{\mathfrak{Y}})\hat{E}^{(l)}\hat{\mathfrak{Y}}\big) = v\Big(\sum_{i=0}^{l} i\hat{g}_{n-i}(X)\hat{\mathfrak{Y}}^{i-1}\hat{E}^{(l)}\hat{\mathfrak{Y}}\Big) \geqslant 0.$$



Die Koeffizienten von $\hat{f}(X, Y)$ liegen in $K_0$, sodaß $\hat{f}_Y(X, \hat{\mathfrak{Y}}) \in K(X, \hat{\mathfrak{Y}})_0$ ist und $v\big(\hat{f}_Y(X, \hat{\mathfrak{Y}})\big) \geqslant 0$ ist. Weiter ist $\psi\big(\hat{f}_Y(X, \hat{\mathfrak{Y}})\big) = f_Y(X, \mathfrak{Y}) \neq 0$, daher $v\big(\hat{f}_Y(X, \hat{\mathfrak{Y}})\big) = 0$ und schließlich $v(\hat{E}^{(l)}\hat{\mathfrak{Y}}) \geqslant 0$.

HILFSSATZ 8. *Es sei* $\hat{a}(X, Y, Z, W)$ *ein Polynom mit Koeffizienten in* $K_0$. *Es sei*

$$l < q.$$

*Dann ist*

$$\psi\big(\hat{E}^{(l)}\hat{a}(X, \hat{\mathfrak{Y}}, X^q, \hat{\mathfrak{Y}}^q)\big) = \psi\big(\hat{E}^{(l)}\hat{a}(X, \hat{\mathfrak{Y}}, Z, W)_{Z=X^q, W=\hat{\mathfrak{Y}}^q}\big).$$

Beweis. Der Hilfssatz besagt, daß die „Differentiationen" nach $X^q$ und nach $\hat{\mathfrak{Y}}^q$ nicht durchgeführt werden brauchen. Es wird genügen, ihn für $\hat{a}(X, Y, Z, W) = X^e Y^i Z^j W^k$ zu zeigen. Dann ist

$$\hat{E}^{(l)}(X^e\hat{\mathfrak{Y}}^i X^{qj}\hat{\mathfrak{Y}}^{qk}) = \sum_{u_1+\ldots+u_4=l} \hat{E}^{(u_1)}(X^e)\,\hat{E}^{(u_2)}(\hat{\mathfrak{Y}}^i)\,\hat{E}^{(u_3)}(X^{qj})\,\hat{E}^{(u_4)}(\hat{\mathfrak{Y}}^{qk}).$$

Jeder der vier Faktoren jedes Summanden liegt in $K(X, \hat{\mathfrak{Y}})_0$. Es genügt, nachzuweisen, daß $v(\hat{E}^{(u_3)}X^{qj}) > 0$ ist für $0 < u_3 \leqslant l$, und daß $v(\hat{E}^{(u_4)}\hat{\mathfrak{Y}}^{qk}) > 0$ ist für $0 < u_4 \leqslant l$. Es gilt sogar allgemein

$$v(\hat{E}^{(u)}\hat{\mathfrak{U}}^q) > 0 \quad \text{für} \quad \mathfrak{U} \in K(X, \hat{\mathfrak{Y}})_0 \quad \text{und} \quad 0 < u < q.$$

Es ist nämlich $\hat{E}^{(u)}\hat{\mathfrak{U}}^q = (q/u)E^{(u-1)}(\hat{\mathfrak{U}}^{q-1}\hat{D}\hat{\mathfrak{U}})$, und dabei ist $v(q/u) = v(p^\varkappa/u) = \varkappa - v(u) > 0$ wegen $u < q = p^\varkappa$.

Jetzt sei $h(X) \in F_q[X]$. Es sei $\hat{h}(X) \in K_0[X]$ mit $\psi\big(\hat{h}(X)\big) = h(X)$. Dann ist offenbar

$$E^{(l)}h(X) = \psi\big(\hat{E}^{(l)}\hat{h}(X)\big). \tag{47}$$

Allgemeiner sei jetzt $\mathfrak{U} \in F_q(X, \mathfrak{Y})$. Es sei $\hat{\mathfrak{U}} \in K(X, \hat{\mathfrak{Y}})_0$ mit $\psi(\hat{\mathfrak{U}}) = \mathfrak{U}$. Dann ist $\hat{E}^{(l)}\hat{\mathfrak{U}}$ wieder in $K(X, \mathfrak{Y})_0$, und wir setzen

$$E^{(l)}\mathfrak{U} = \psi(\hat{E}^{(l)}\hat{\mathfrak{U}}). \tag{48}$$

Diese Definition ist von der Wahl von $\hat{\mathfrak{U}}$ unabhängig, denn ist $\psi(\hat{\mathfrak{U}}_1) = \psi(\hat{\mathfrak{U}}_2)$, dann ist $v(\hat{\mathfrak{U}}_1 - \hat{\mathfrak{U}}_2) > 0$, daher $v\big(\hat{E}^{(l)}(\hat{\mathfrak{U}}_1) - \hat{E}^{(l)}(\hat{\mathfrak{U}}_2)\big) > 0$ und $\psi(\hat{E}^{(l)}\hat{\mathfrak{U}}_1) = \psi(\hat{E}^{(l)}\hat{\mathfrak{U}}_2)$. Die Operatoren $E^{(l)}$ können als „höhere Differentiale" in $F_q(X, \mathfrak{Y})$ angesehen werden.

**9. Beweis des Satzes im allgemeinen Fall.** Die Exponentenbewertung $v$ von $K(X)$ kann zu einer Exponentenbewertung $v_2$ von $K(X, Y)$ fortgesetzt werden, ebenso zu einer Exponentenbewertung $v_3$ von $K(X, Y, Z)$, usw. Analog zu $K(X)_0$ definiert man Ringe $K(X, Y)_0$, $K(X, Y, Z)_0, \ldots$ Der Homomorphismus $\psi$ von $K(X)_0$ nach $F_q(X)$ kann auf natürliche Weise zu einem Homomorphismus $\psi_2$ von $K(X, Y)_0$ nach $F_q(X, Y)$ fortgesetzt

werden, ebenso zu einem Homomorphismus $\psi_3$ von $K(X, Y, Z)_0$ nach $F_q(X, Y, Z)$, usw. Der Zusammenhang von $\psi_2$ mit dem früher definierten Homomorphismus $\psi$ von $K(X, \mathfrak{Y})_0$ nach $F_q(X, \hat{\mathfrak{Y}})$ besteht darin, daß aus $\psi_2(\hat{u}(X, Y)) = u(X, Y)$ die Gleichung $\psi(\hat{u}(X, \hat{\mathfrak{Y}})) = u(X, \mathfrak{Y})$ folgt.

Wir werden zwei Varianten zu Hilfssatz 4 angeben. Die erste Variante behandelt Polynome $\hat{a}(X, Y, Z, W)$ mit Koeffizienten in $K_0$. Es sei

$$\hat{a}(X, Y, Z, W) = \sum_{i=0}^{n-1} \sum_{j=0}^{N} \sum_{k=0}^{n-1} \hat{b}_{ijk}(X)\, Y^i Z^j W^k, \tag{49}$$

wobei die $\hat{b}_{ijk}(X)$ Polynome in $K_0[X]$ vom Grad $\leqslant (q/n) - mn$ seien. Wir setzen

$$\hat{F}^{(l)}\hat{a}(X, \hat{\mathfrak{Y}}, X^q, \hat{\mathfrak{Y}}^q) = \hat{E}^{(l)}\hat{a}(X, \hat{\mathfrak{Y}}, Z, W)_{Z=X^q, W=\hat{\mathfrak{Y}}^q}. \tag{50}$$

Wir bilden $\hat{h}(X, Y) = \hat{g}_0(X)^{n-1}\hat{f}_Y(X, Y)$. Dann gilt das Analogon zu Hilfssatz 4: Es gibt Polynome $\hat{a}^{(l)}(X, Y, Z, W)$ mit Koeffizienten in $K_0$, sodaß (i) und (ii) gelten, und daß (iii) mit

$$\hat{F}^{(l)}\hat{a}(X, \hat{\mathfrak{Y}}, X^q, \hat{\mathfrak{Y}}^q) = \hat{s}^{(l)}(X, \hat{\mathfrak{Y}})$$

an Stelle von (25) gilt.

Zunächst ist nur klar, daß $\hat{a}^{(l)}$ Koeffizienten in $K$ hat. Nun ist aber $\nu(\hat{s}^{(l)}(X, \hat{\mathfrak{Y}})) \geqslant 0$, außerdem $\nu(\hat{h}(X, \hat{\mathfrak{Y}})) = 0$ wegen $h(X, \mathfrak{Y}) \neq 0$, daher $\nu(\hat{a}^{(l)}(X, \hat{\mathfrak{Y}}, \mathfrak{Z}, \hat{\mathfrak{W}})) \geqslant 0$. Ist

$$\hat{a}^{(l)}(X, Y, Z, W) = \sum \hat{a}_{ij}^{(l)}(X, Y) Z^i W^j,$$

dann ist sogar $\nu(\hat{a}_{ij}^{(l)}(X, \hat{\mathfrak{Y}})) \geqslant 0$, denn die Variablen $Z$, $W$ werden durch $\hat{F}^{(l)}$ nicht berührt. Da $\hat{a}_{ij}^{(l)}(X, Y)$ ein Polynom vom Grad $\leqslant n-1$ in $Y$ ist, folgt aus der Definition von $\nu$ auf $K(X, \hat{\mathfrak{Y}})$ und von $\nu_2$ auf $K(X, Y)$, daß $\nu_2(\hat{a}_{ij}^{(l)}(X, Y)) \geqslant 0$ ist. Also hat $\hat{a}_{ij}^{(l)}(X, Y)$, daher $\hat{a}^{(l)}(X, Y, Z, W)$ Koeffizienten in $K_0$.

Die zweite Variante behandelt Polynome $a(X, Y, Z, W)$ mit Koeffizienten in $F_q$, von der in Hilfssatz 3 betrachteten Art. Es sei $a(X, Y, Z, W)$ ein solches Polynom. Wir wählen Polynome $\hat{b}_{ijk}(X) \in K_0[X]$ mit $\psi(\hat{b}_{ijk}(X)) = b_{ijk}(X)$ und $\operatorname{Grad}\hat{b}_{ijk}(X) = \operatorname{Grad} b_{ijk}(X)$ $(0 \leqslant i, k \leqslant n-1;\ 0 \leqslant j \leqslant N)$, und bilden $\hat{a}(X, Y, Z, W)$ gemäß (49). Wir bestimmen $\hat{a}^{(l)}(X, Y, Z, W)$ so, daß die erste Variante von Hilfssatz 4 gilt. Nun setzen wir

$$a^{(l)}(X, Y, Z, W) = \psi_4(\hat{a}^{(l)}(X, Y, Z, W)).$$

Wegen Hilfssatz 8 und der Definition (50) gilt nun Hilfssatz 4 für $a(X, Y, Z, W)$ und für

$$l < q,$$



wobei aber (25) durch

$$E^{(l)}a(X, \mathfrak{Y}, \mathfrak{Z}, \mathfrak{W}) = s^{(l)}(X, \mathfrak{Y}) \tag{51}$$

zu ersetzen ist.

Hilfssatz 5 bleibt für die Funktionen $s^{(l)}(X, Y)$ aus (51) richtig. Ebenso bleibt Hilfssatz 6 richtig, wenn (36) durch

$$E^{(l)}h_i(x) = 0 \qquad (0 < l < M\,|\nu_i(x)|)$$

ersetzt wird. Der Rest des Beweises verläuft so wie früher.

## Literatur


[1] M. Eichler, *Einführung in die Theorie der algebraischen Zahlen und Funktionen*, Basel und Stuttgart 1963.

[2] S. A. Stepanov, *Die Anzahl der Punkte einer hyperelliptischen Kurve über einem Primkörper* (Russisch), Izv. Akad. Nauk SSSR, Ser. Mat. 33 (1969), S. 1171–1181.

[3] — *Elementary method in the theory of congruences for a prime modulus*, Acta Arith. 17 (1970), S. 231–247.

[4] — *An elementary proof of the Hasse–Weil Theorem for hyperelliptic curves*, J. Number Theory 4 (1972), S. 118–143.

[5] — *Abschätzungen von rationalen trigonometrischen Summen mit Primnennern* (Russisch), Trudy Mat. Inst. Steklov 112 (1971), S. 346–371.

[6] B. L. Van der Waerden, *Algebra I*, 4. Aufl., Berlin, Göttingen, Heidelberg 1955.

[7] A. Weil, *Sur les courbes algébriques et les variétes qui s'en déduisent*, Act. Sci. Ind. 1041, Paris 1948.



UNIVERSITY OF COLORADO
Boulder, Colorado
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
Bombay, India


*Eingegangen 15. 11. 1972* (354)