ACTA ARITHMETICA
LVI (1990)

Eisenstein's theorem on power series expansions of algebraic functions

by

WOLFGANG M. SCHMIDT* (Boulder, Col.)

1. Introduction. A well-known theorem of Eisenstein asserts that if a formal series

$$y = \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \ldots \tag{1.1}$$

satisfies an equation $F(X, y) = 0$ where F is a nonzero polynomial with algebraic coefficients, then $\alpha_0, \alpha_1, \ldots$ lie in an algebraic number field, and there are natural numbers a_0, a such that

$$a_0 a^j \alpha_j \quad (j = 0, 1, \ldots) \tag{1.2}$$

are algebraic integers. It is our purpose to make this more explicit.

In the special case when the polynomial $F(X, Y)$ lies in $\boldsymbol{Z}[X, Y]$ and has no multiple factors, our results will imply that we may take a, a_0 with

$$a < c_1(N) H^{8N^3}, \quad a_0 = a^N,$$

where N is the total degree, and H is the maximum modulus of the coefficients of F. The only quantitative version of Eisenstein's Theorem that I could find in the literature** is due to Coates [2, Lemma 3], and implies a value

$$a = a_0 < c_2(N) H^{c_3}$$

with $c_3(N) = (2N)^{6N^2}$.

$F(X, Y)$ may be regarded as a polynomial in Y whose coefficients are polynomials in X. As such it has a discriminant $D(X)$ which is a polynomial in X. We will suppose throughout that $D(X) \neq 0$, i.e., that $F(X, Y)$ when regarded as a polynomial in Y has no multiple factors. We will assume that F is of degree $m > 0$ in X and of degree $n > 0$ in Y, and that the coefficients of F lie in an algebraic number field k of degree d. It is well known and easily seen that

---

* Supported in part by NSF grant DMS-8603093.

** Added in proof. D. L. Hilliker and E. G. Straus on p. 656 of their paper in Trans. Amer. Math. Soc. 280 (1983), 637–657 obtain a bound similar to Coates'.

if y as above satisfies $F(X, y) = 0$, then the coefficients $\alpha_0, \alpha_1, \ldots$ generate a field K over k of degree $[K:k] \leqslant n$. Thus K has degree $\delta = [K:\boldsymbol{Q}] \leqslant nd$. Let $\alpha \mapsto \alpha^{(i)}$ $(i = 1, \ldots, \delta)$ be the isomorphic embeddings of K into $\boldsymbol{C}$. It is known that there are positive reals A_0, A such that

$$(1.3) \qquad |\alpha_j^{(i)}| \leqslant A_0 A^j \quad (1 \leqslant i \leqslant \delta;\ j = 0, 1, \ldots).$$

This, together with the assertion on (1.2), implies that y is a *G-function* as defined by Siegel [7].

By an absolute value of k we will always understand an absolute value which is normalized so that it extends either the standard absolute value or a p-adic absolute value of $\boldsymbol{Q}$. Given such an absolute value $|\cdot|_w$ of k, let n_w be its local degree. Let $M(k)$ be a set of symbols v, such that with every $v \in M(k)$ there is associated an absolute value $|\cdot|_v$ of k, and moreover every absolute value $|\cdot|_w$ of k is obtained for precisely n_w elements of $M(k)$. In other words, $M(k)$ is the set of absolute values of k with multiplicities, so that a given $|\cdot|_w$ occurs n_w times. With this convention, we have the product formula

$$\prod_{v \in M(k)} |\alpha|_v = 1 \quad \text{for } \alpha \in k,\ \alpha \neq 0.$$

We will write $v | \infty$ if v extends the Archimedean absolute value of $\boldsymbol{Q}$, i.e., when v is Archimedean. There are precisely d such $v \in M(k)$. We will write $v | p$ if v extends the p-adic absolute value of $\boldsymbol{Q}$. Given a prime p, there are precisely d such $v \in M(k)$. We will set

$$M(k) = M_\infty(k) \cup M_1(k) \cup M_2(k),$$

where $M_\infty(k)$ consists of v with $v | \infty$, where $M_1(k)$ consists of v with $v | p$ where $p > n$, and $M_2(k)$ consists of v with $v | p$ where $p \leqslant n$.

Now let P be a polynomial in one or several variables and with coefficients in k. Given $v \in M(k)$, let $|P|_v$ be the maximum of $|\pi|_v$ over all the coefficients π of P. We define the *field height* $H_k(P)$ of P by

$$H_k(P) = \prod_{v \in M(k)} |P|_v,$$

and the *absolute height* by $H(P) = H_k(P)^{1/d}$. (Warning: sometimes, e.g. in [6], a different height is used.) We define $M(K)$ in complete analogy with $M(k)$. When $v \in M(k)$, $w \in M(K)$ and the restriction of $|\cdot|_w$ to k is $|\cdot|_v$, we write $w | v$. Given $v \in M(k)$, there are precisely $[K:k]$ elements $w \in M(K)$ with $w | v$.

THEOREM 1. *Let F, y be as above. There are real numbers $A_v \geqslant 1$, defined for $v \in M(k)$ and with $A_v = 1$ for all but finitely many v, such that*

$$(1.4) \qquad |\alpha_j|_w \leqslant A_v^{m+j} \quad (j = 0, 1, \ldots)$$

for every $v \in M(k)$, $w \in M(K)$ with $w | v$, and such that

$$(1.5) \qquad \prod_{v \in M_\infty(k) \cup M_1(k)} A_v \leqslant ((m+1)(n+1)\sqrt{n})^{(2n+1)d} H(F)^{2nd} = C,$$

say, and

$$(1.6) \qquad \prod_{v \in M_2(k)} A_v < (16m)^{11n^3 d} H(F)^{(2n^3+2n)d}.$$

It is likely that the bound in (1.6) is weak and should be replaced by a bound similar to (1.5). In order to obtain Eisenstein's Theorem we need a variation on Theorem 1. For $v \in M_\infty(k)$, let G_v be the group $\boldsymbol{R}^+$ of positive reals under multiplication. For

$$v \in M_0(k) := M_1(k) \cup M_2(k) = M(k) \backslash M_\infty(k),$$

let $G_v \subseteq \boldsymbol{R}^+$ be the subgroup consisting of values $|\alpha|_v$ with $\alpha \neq 0$ in k.

THEOREM 2. *Let F, y be as above. There are numbers $B_v \in G_v$ for each $v \in M(k)$, having $B_v \geqslant 1$, and $B_v = 1$ for all but finitely many v, such that*

$$(1.7) \qquad |\alpha_j|_w \leqslant B_v^{m+j} \quad (j = 0, 1, \ldots)$$

for every $v \in M(k)$, $w \in M(K)$ with $w | v$, and such that

$$(1.8) \qquad \prod_{v \in M(k)} B_v < (2^{14} m^3 n^3 H(F))^{4(n+m)n^2 d} = C_1, \quad \textit{say}.$$

It is an immediate consequence of Theorem 1 that

$$|\alpha_j^{(i)}| \leqslant C^{m+j} \quad (1 \leqslant i \leqslant \delta;\ j = 0, 1, \ldots),$$

so that (1.3) holds with $A = C$, $A_0 = C^m$. On the other hand, for $v \in M_0(k)$ let $\mathfrak{P}_v$ be the prime ideal in the ring of integers in k consisting of α with $|\alpha|_v < 1$. If $v | p_v$, then $(p_v) = \mathfrak{P}_v^{e_v} \mathfrak{P}_2^{e_2} \ldots \mathfrak{P}_l^{e_l}$ for prime ideals $\mathfrak{P}_v, \mathfrak{P}_2, \ldots, \mathfrak{P}_l$ and exponents $e_v, e_2, \ldots, e_l$. The value group G_v is generated by p_v^{1/e_v}. Every $\alpha \in \mathfrak{P}_v$ has $|\alpha|_v \leqslant p_v^{-1/e_v}$. The ideal $\mathfrak{P}_v$ generates an ideal in the ring of integers of K which we will also denote by $\mathfrak{P}_v$, and every $\alpha \in \mathfrak{P}_v$, $\alpha \in K$ has $|\alpha|_w \leqslant p_v^{-1/e_v}$ when $w | v$. Now if $B_v = p_v^{b_v/e_v}$ for $v \in M_0(k)$, let $\mathscr{A}$ be the ideal

$$\mathscr{A} = \prod_{v \in \mathbf{M}_0(k)} \mathfrak{P}_v^{b_v}.$$

where $\mathbf{M}_0(k)$ (in contrast to $M_0(k)$) indexes every absolute value just once. Then by (1.7),

$$(1.9) \qquad \mathscr{A}^{m+j}(\alpha_j) \quad (j = 0, 1, \ldots)$$

are integral ideals in the ring of integers of K. Moreover, $\mathfrak{P}_v$ has some norm $\mathscr{N}(\mathfrak{P}_v) = p_v^{f_v}$ with $e_v f_v \leqslant d$, and

$$\mathscr{N}(\mathscr{A}) = \prod_{v \in \mathbf{M}_0(k)} \mathscr{N}(\mathfrak{P}_v)^{b_v} = \prod_{v \in \mathbf{M}_0(k)} p_v^{f_v b_v} = \prod_{v \in \mathbf{M}_0(k)} B_v^{f_v e_v} = \prod_{v \in M_0(k)} B_v \leqslant C_1.$$

Setting $a = \mathscr{N}(\mathscr{A})$, we obtain the following quantitative version of Eisenstein's Theorem.

THEOREM 3. *There is an ideal $\mathscr{A}$ in the ring of integers of k with $\mathscr{N}(\mathscr{A}) \leqslant C_1$ such that the ideals (1.9) are integral. There is a natural number a with $a \leqslant C_1$ such that*

$$a^{m+j}\alpha_j \quad (j = 0, 1, \ldots)$$

are algebraic integers.

We remark that some precision is lost in going from the ideal $\mathscr{A}$ to the natural number a. In fact, the formulation in Theorem 1 may be best. For example, if $k = K = \mathbf{Q}$, and if 2 occurs in the denominator of α_j to the exponent $[j/2]$ where [ ] denotes integer parts, then in Theorem 1 we may take $A_2 = 2^{1/2}$, but in Theorem 2 we have to take $B_2 = 2$, and in Theorem 3 we need to take a divisible by 2.

The quantitative version of Eisenstein's Theorem due to Coates [2, Lemma 3], has $a_0 = a \leqslant c_4(n, m)H(F)^{c_5}$ and $c_5 = (4n^2 d)^{3nm}$.

The proofs of Theorems 1 and 2 will distinguish between elements v in $M_\infty(k)$, $M_1(k)$, $M_2(k)$. The argument for $v \in M_\infty(k)$ will follow classical lines. For $v \in M_1(k)$, a result of Dwork and Robba [3] on p-adic radii of convergence will be crucial. A conjectured variation (see Section 2, below Lemma 1) of this result for $v \in M_2(k)$ would lead to a great simplification and to better bounds. Since such a variation has not been proved, in order to deal with $v \in M_2(k)$ we have to derive a linear differential equation satisfied by y, and to use a paper of Clark [1] on p-adic convergence of solutions of such differential equations. I am grateful to Professor Dwork for drawing my attention to this work of Clark.

Eisenstein in [4] apparently supposes that the discriminant $D(X)$ does not vanish at $x = 0$. Under this assumption, his theorem becomes considerably easier, and our bounds could be much improved.

2. Quantities ϱ and σ. For $w \in M_\infty(K)$, let $\mathbf{C}_w$ be the algebraic closure of the completion of K under $|\cdot|_w$. Thus $\mathbf{C}_w \cong \mathbf{C}$. For $w \in M_0(K)$, let $\mathbf{C}_w$ be the completion of the algebraic closure of the completion of K under $|\cdot|_w$. There is a natural extension of $|\cdot|_w$ to $\mathbf{C}_w$. Similarly define $\mathbf{C}_v$ for $v \in M(k)$, and extend $|\cdot|_v$ to $\mathbf{C}_v$.

For $w \in M(K)$, let ϱ_w be the w-adic radius of convergence of y. Thus ϱ_w is the supremum of the numbers ϱ such that the series for y converges w-adically for every $x \in \mathbf{C}_w$ with $|x|_w \leqslant \varrho$. We will see in the course of our investigation that $\varrho_w > 0$ for each w.

Let $D(X)$ be the discriminant of $F(X, Y)$ when considered as a polynomial with coefficients in $k[X]$. Then $D(X) \in k[X]$, and $D(X) \neq 0$ by hypothesis. Write

$$F(X, Y) = A_n(X)Y^n + \ldots + A_0(X),$$

so that $A_n(X) \neq 0$. Put

$$R(X) = A_n(X)D(X); \tag{2.1}$$

then $\deg R(X) \leqslant (2n-1)m$. Write

$$R(X) = X^q R^*(X) \tag{2.2}$$

where R^* is a polynomial with $R^*(0) \neq 0$.

Now let $v \in M(k)$, and k_v the completion of k under $|\cdot|_v$, so that $k_v \subseteq \mathbf{C}_v$. In $k_v[X]$ we have a factorization $R^*(X) = R_1(X) \ldots R_t(X)$ into irreducible factors. Say $R_i(X) = (X - \beta_{i1}) \ldots (X - \beta_{i,s(i)})$ in $\mathbf{C}_v$. Then it is well known that $|\beta_{i1}|_v = \ldots = |\beta_{i,s(i)}|_v = \nu_i$, say $(i = 1, \ldots, t)$. Thus the set of v-adic absolute values of the roots of R^* is $\{\nu_1, \ldots, \nu_t\}$. Set

$$\sigma_v = \min(1, \nu_1, \ldots, \nu_t). \tag{2.3}$$

Suppose now that E is an algebraic extension of k in which $R^*(X)$ factors into linear factors, say $R^*(X) = c(X - \beta_1) \ldots (X - \beta_l)$, and let $|\cdot|_w$ be an extension of v to E. Then, since E can be embedded into $\mathbf{C}_v$, the set of absolute values $|\beta_i|_w$ $(i = 1, \ldots, l)$ is the same as $\{\nu_1, \ldots, \nu_t\}$. In other words, this set is independent of E and of w. Thus

$$\sigma_v = \min(1, |\beta_1|_w, \ldots, |\beta_l|_w). \tag{2.4}$$

LEMMA 1. *Suppose $w \mid v$ with $w \in M(K)$, $v \in M_\infty(k) \cup M_1(k)$. Then $\varrho_w \geqslant \sigma_v$.*

Proof. The case when $v \in M_\infty(k)$ is classical: We may suppose that K is embedded in $\mathbf{C}$ and that $|\cdot|_w$, $|\cdot|_v$ are the ordinary absolute value. The equation $F(X, y) = 0$ has n Puiseux series solutions $y_1(X), \ldots, y_n(X)$ at $x = 0$. Since $A_n(x) \neq 0$ and $F_Y(x, y) \neq 0$ for every x, y in $\mathbf{C}$ with $0 < |x| < \sigma_v$ and $F(x, y) = 0$, each of the series $y_1, \ldots, y_n$ can be continued analytically to $0 < |x| < \sigma_v$. Since there can be no more than n formal Puiseux series solutions to $F(X, y) = 0$, the given series y of (1.1) is among $y_1, \ldots, y_n$, hence is analytic in $|x| < \sigma_v$. Therefore its radius of convergence is $\geqslant \sigma_v$.

The case when $v \in M_1(k)$ is due to Dwork and Robba [3]. Again, at each x_0 in $\mathbf{C}_w$ with $0 < |x_0|_w < \sigma_v$, the equation $F(x, y) = 0$ has n distinct locally analytic solutions $y_1, \ldots, y_n$. Pick $\xi \in \mathbf{C}_w$ with $|\xi|_w = \sigma_v$, and set $G(X, Y) = F(\xi X, Y)$. Then at each $x_0 \in \mathbf{C}_w$ with $0 < |x_0|_w < 1$, the equation $G(x, y) = 0$ has n distinct locally analytic solutions. By Dwork and Robba's Theorem 2.1, $\hat{y}(x) := y(\xi x)$ is convergent for $|x|_w < 1$, so that $y(x)$ itself is convergent for $|x|_w < \sigma_v$. Thus $\varrho_w \geqslant \sigma_v$.

I conjecture that when $v \in M_2(k)$ and everything else is as above, then $\hat{y}(x)$ is convergent for $|x|_w < c(n)$, where $c(n)$ depends on n only.

In what follows, write

$$A_n(X) = a_r X^r + a_{r-1}X^{r-1} + \ldots + a_u X^u \tag{2.5}$$

with $a_r \neq 0$, $a_u \neq 0$. Theorems 1, 2 are invariant under multiplication of F by a nonzero element of k. We therefore may, and we will, suppose in the sequel that

$$a_u = 1. \tag{2.6}$$

LEMMA 2. (a) *Suppose that* $w|v$ *where* $w \in M(K)$ *and* $v \in M_\infty(k)$. *Then*

$$|\alpha_j|_w \leqslant 2n|F|_v(2/\sigma_v)^{m+j} \qquad (j = 0, 1, \ldots).$$

(b) *Suppose that* $w|v$ *with* $w \in M(K)$ *and* $v \in M_0(k)$. *Suppose that* $\tau_w > 0$, *where*

$$\tau_w = \min(\sigma_v, \varrho_w).$$

Then

$$|\alpha_j|_w \leqslant |F|_v(1/\tau_w)^{m+j} \qquad (j = 0, 1, \ldots).$$

Proof. (a) We may suppose that K is embedded in C and that $|\cdot|_w, |\cdot|_v$ are the ordinary absolute value. We factor

$$(2.7) \qquad A_n(X) = a_r X^u(X-\gamma_1) \ldots (X-\gamma_{r-u}).$$

(When $r = u$, we have $A_n(X) = a_r X^r$.) Since $\gamma_1, \ldots, \gamma_{r-u}$ are among the roots of R^*, we have $|\gamma_i|_w \geqslant \sigma_v$ $(i = 1, \ldots, r-u)$ by (2.4).

Let z be complex with $|z| = \sigma_v/2$. Then $|z-\gamma_i| \geqslant |\gamma_i|/2$ $(i = 1, \ldots, r-u)$ and

$$|A_n(z)| \geqslant |a_r|(\sigma_v/2)^u(|\gamma_1|/2) \ldots (|\gamma_{r-u}|/2) = \sigma_v^u 2^{-r}|a_r\gamma_1 \ldots \gamma_{r-u}|$$
$$= \sigma_v^u 2^{-r}|a_u| = \sigma_v^u 2^{-r} \geqslant (\sigma_v/2)^m.$$

On the other hand, since $|z| = \sigma_v/2 \leqslant 1/2$,

$$|A_i(z)| < 2|F|_v \qquad (i = 0, \ldots, n).$$

Since $y(z)$ satisfies $F(z, y(z)) = A_n(z)y(z)^n + \ldots + A_0(z) = 0$, we have

$$|y(z)| < 2n|F|_v(2/\sigma_v)^m.$$

By Cauchy's formula, the coefficient α_j in the expansion of $y(z)$ is given by

$$\alpha_j = \frac{1}{2\pi i}\int_C \frac{y(z)}{z^{j+1}}dz,$$

where C is, say, the circle $|z| = \sigma_v/2$. On this circle, $|y(z)/z^{j+1}| \leqslant 2n|F|_v(2/\sigma_v)^{m+j+1}$. The path of integration has length $2\pi(\sigma_v/2)$. We obtain

$$|\alpha_j|_w = |\alpha_j| \leqslant 2n|F|_v(2/\sigma_v)^{m+j} \qquad (j = 0, 1, \ldots).$$

(b) Let ϱ be a number in $0 < \varrho < \tau_w$, of the type $\varrho = p^t$ where $v|p$ and $t \in Q$. Since $\varrho < \varrho_w$, the series for $y(z)$ is w-adically convergent for $z \in C_w$ with $|z|_w = \varrho$. In C_w we again have a factorization (2.7), and $|\gamma_i|_w \geqslant \sigma_v \geqslant \tau_w > \varrho$ $(i = 1, \ldots, r-u)$. Therefore z with $|z|_w = \varrho$ has

$$|A_n(z)|_w = |a_r|_w \varrho^u|\gamma_1|_w \ldots |\gamma_{r-u}|_w = \varrho^u|a_u|_w = \varrho^u \geqslant \varrho^m.$$

On the other hand, since $|z|_w = \varrho < 1$,

$$|A_i(z)|_w \leqslant |F|_v \qquad (i = 0, \ldots, n).$$

The quotients have $|A_i(z)/A_n(z)|_w \leqslant |F|_v\varrho^{-m}$ $(i = 0, \ldots, n)$. Note that the right side here is > 1, since $\varrho < 1$ and since $|F|_v \geqslant 1$ by (2.6). Since $y(z)$ satisfies $A_n(z)y(z)^n + \ldots + A_0(z) = 0$, we have

$$|y(z)|_w \leqslant |F|_v\varrho^{-m}.$$

Pick $\xi \in C_w$ with $|\xi|_w = \varrho$, and set

$$\hat{y}(X) = y(\xi X) = \alpha_0 + \alpha_1\xi X + \alpha_2\xi^2X^2 + \ldots = \delta_0 + \delta_1 X + \delta_2 X^2 + \ldots,$$

say. Then $|\hat{y}(z)| \leqslant |F|_v\varrho^{-m}$ for every $z \in C_w$ having $|z|_w = 1$. Furthermore, since $\hat{y}(z)$ is w-adically convergent for such z, $|\delta_j|_w \to 0$ as $j \to \infty$. Put

$$B = \max_j |\delta_j|_w,$$

and when $B \neq 0$ pick t such that $|\delta_j|_w < B$ for $j > t$. There is a $z \in C_w$ with $|z|_w = 1$ and

$$|\delta_0 + \delta_1 z + \ldots + \delta_t z^t|_w = B;$$

then also $|\hat{y}(z)|_w = B$. This implies that $B \leqslant |F|_v\varrho^{-m}$, so that $|\delta_j|_w \leqslant |F|_v\varrho^{-m}$, i.e., $|\alpha_j\xi^j|_w \leqslant |F|_v\varrho^{-m}$, and therefore

$$|\alpha_j|_w \leqslant |F|_v\varrho^{-m}|\xi|_w^{-j} = |F|_v\varrho^{-m-j} \qquad (j = 0, 1, \ldots).$$

Since this is true for every $\varrho < \tau_w$ of the type specified above, assertion (b) follows.

3. On $R(X)$ and its roots. Given $\varepsilon \in E$ where E is an algebraic number field, define its field height to be

$$h_E(\varepsilon) = \prod_{w \in M(E)} \max(1, |\varepsilon|_w),$$

and its absolute height by $h(\varepsilon) = h_E(\varepsilon)^{1/e}$, where $e = [E:Q]$.

LEMMA 3. *Suppose* $P(X) = q(X-\varepsilon_1) \ldots (X-\varepsilon_l)$ *with* $q, \varepsilon_1, \ldots, \varepsilon_l$ *in* E. *Then*

$$h(\varepsilon_1) \ldots h(\varepsilon_l) \leqslant (l+1)H(P).$$

Proof. For $w \in M(E)$, put

$$\mathscr{M}_w = |q|_w \max(1, |\varepsilon_1|_w) \ldots \max(1, |\varepsilon_l|_w).$$

When $w \in M_0(E)$, so that $|\cdot|_w$ is non-Archimedean, Gauss' Lemma yields

$$\mathscr{M}_w = |P|_w.$$

Now suppose that w is Archimedean. After embedding E in a suitable way into C, we may suppose that $|\cdot|$ is the standard absolute value of C. Then $\mathscr{M}_w$ is the Mahler height of P, and therefore

$$\mathscr{M}_w = \exp\int_0^1 \log|P(e^{2\pi i x})|\,dx$$

(Mahler [5]). But $|P(e^{2\pi i x})| \leqslant (l+1)|P|_w$, so that

$$\mathcal{M}_w \leqslant (l+1)|P|_w$$

when $w \in M_\infty(E)$. Since $M_\infty(E)$ has cardinality e,

$$h_E(\varepsilon_1) \dots h_E(\varepsilon_l) = \prod_{w \in M(E)} \mathcal{M}_w \leqslant (l+1)^e H_E(P).$$

The lemma follows.

LEMMA 4. *Let $F(X, Y)$, $R(X)$ be as in Section 2. Then*

$$H(R) < ((m+1)(n+1)\sqrt{n})^{2n-1} H(F)^{2n-1}. \tag{3.1}$$

Proof.

$R(X) = A_n(X) D(X)$

$$= \left|\begin{array}{cccccc} A_n & A_{n-1} & \dots & A_0 & & \\ & A_n & A_{n-1} & \dots & A_0 & \\ \dots & \dots & \dots & \dots & \dots & \dots \\ & & A_n & A_{n-1} & \dots & A_0 \\ nA_n & (n-1)A_{n-1} & \dots & A_1 & & \\ & nA_n & (n-1)A_{n-1} & \dots & A_1 & \\ \dots & \dots & \dots & \dots & \dots & \dots \\ & & nA_n & (n-1)A_{n-1} & \dots & A_1 \end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\}{n-1} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\}{n} \end{array}$$

In particular, $R(X) = Q(A_n(X), \dots, A_0(X))$, where Q is a homogeneous polynomial of degree $2n-1$ and with coefficients in $\mathbf{Z}$.

Each coefficient of each $A_j(X)$ has v-adic absolute value $\leqslant |F|_v$. Therefore when v is non-Archimedean,

$$|R|_v \leqslant |F|_v^{2n-1}.$$

Suppose now that v is Archimedean. Let M be a monomial of degree $2n-1$ in $A_n(X), \dots, A_0(X)$. Since $\deg A_i(X) \leqslant m$ $(i = 0, \dots, n)$, every coefficient of $M(X)$ has v-adic absolute value $\leqslant (m+1)^{2n-1} |F|_v^{2n-1}$, i.e.,

$$|M|_v \leqslant (m+1)^{2n-1} |F|_v^{2n-1}.$$

The sum of the moduli of the coefficients of $Q(Y_n, \dots, Y_0)$ is

$$\leqslant (n+1)^{n-1}(1+2+ \dots +n)^n = (n+1)^{n-1}\left(\frac{n(n+1)}{2}\right)^n$$

$$= (n+1)^{2n-1} n^n 2^{-n} < (n+1)^{2n-1} n^{n-1/2} = ((n+1)\sqrt{n})^{2n-1}.$$

We may conclude that

$$|R|_v < ((m+1)(n+1)\sqrt{n}|F|_v)^{2n-1}.$$

We obtain

$$H_k(R) = \prod_{v \in M(k)} |R|_v < ((m+1)(n+1)\sqrt{n})^{(2n-1)d} H_k(F)^{2n-1},$$

where $d = [k:\mathbf{Q}]$. The lemma follows.

LEMMA 5.

$$\prod_{v \in M(k)} \sigma_v \geqslant ((m+1)(n+1)\sqrt{n})^{-2nd} H(F)^{-(2n-1)d}.$$

Proof. Let E be an extension in which $R^*(X)$ splits into linear factors, say

$$R^*(X) = c(X-\beta_1) \dots (X-\beta_l).$$

For $v \in M(k)$ and any extension $|\cdot|_w$ of $|\cdot|_v$ to E we have (2.4). Thus if $q = [E:k]$, then

$$\sigma_v^q = \prod_{\substack{w \in M(E) \\ w|v}} \min(1, |\beta_1|_w, \dots, |\beta_l|_w). \tag{3.2}$$

The quantities $\varepsilon_1 = 1/\beta_1, \dots, \varepsilon_l = 1/\beta_l$ are roots of the reciprocal polynomial $R_1(X) = X^l R^*(1/X)$. Since $H(R_1) = H(R^*) = H(R)$, Lemma 3 gives

$$h(\varepsilon_1) \dots h(\varepsilon_l) \leqslant (l+1) H(R) \leqslant 2nm\, H(R).$$

Therefore

$$\prod_{w \in M(E)} \max(1, |\varepsilon_1|_w, \dots, |\varepsilon_l|_w) \leqslant h_E(\varepsilon_1) \dots h_E(\varepsilon_l) \leqslant (2nm\, H(R))^{dq},$$

since $[E:\mathbf{Q}] = dq$. But now by (3.2)

$$\prod_{v \in M(k)} \sigma_v^q \geqslant (2nm\, H(R))^{-dq}.$$

The lemma now follows upon extracting qth roots, in view of (3.1) and of $2nm \leqslant (m+1)(n+1)\sqrt{n}$.

We now can do the part of Theorem 1 which is concerned with $v \in M_\infty(k) \cup M_1(k)$. Set

$$A_v = \begin{cases} 2n|F|_v(2/\sigma_v) & \text{for } v \in M_\infty(k), \\ |F|_v(1/\sigma_v) & \text{for } v \in M_1(k). \end{cases}$$

Since $|F|_v \geqslant 1$ by (2.6), and since each $\sigma_v \leqslant 1$, we have $A_v \geqslant 1$. We have $\sigma_v = 1$ for all but finitely many v, therefore $A_v = 1$ for all but finitely many v. It is not difficult to deduce from Lemma 2 that (1.4) is indeed true for $v \in M_\infty(k) \cup M_1(k)$: it is enough to observe that for such v and for $w|v$, we have $\tau_w = \sigma_v$ by Lemma 1. Furthermore,

$$\prod_{v\in M_\infty(k)\cup M_1(k)} A_v \leqslant (4n)^d H(F) \prod_{v\in M(k)} \sigma_v^{-1}$$
$$\leqslant \left((m+1)(n+1)\sqrt{n}\right)^{(2n+1)d} H(F)^{2nd} = C,$$

so that (1.5) is true.

Encouraged by this, let us do the part of Theorem 2 concerned with $v\in M_\infty(k)\cup M_1(k)$. Set

$$B_v = A_v = 2n|F|_v(2/\sigma_v) \quad \text{for } v\in M_\infty(k).$$

When $v\in M_1(k)$, we observe that $|F|_v\in G_v$, but not necessarily $\sigma_v\in G_v$. Each β_i in (2.4) generates a field over k of degree $\leqslant \deg R < 2nm$, and therefore for each i there is an $e_i < 2nm$ with $|\beta_i|_w^{e_i}\in G_v$. Therefore there is some e_v in $1\leqslant e_v < 2nm$ with $\sigma_v^{e_v}\in G_v$. Put

$$B_v = |F|_v(1/\sigma_v^{e_v}) \quad \text{for } v\in M_1(k).$$

Then (1.7) is certainly true, and

$$\prod_{v\in M_\infty(k)\cup M_1(k)} B_v \leqslant \Big(\prod_{v\in M_\infty(k)\cup M_1(k)} A_v\Big)^{2nm} = C^{2nm}. \tag{3.3}$$

4. A differential equation. It remains for us to deal with $v\in M_2(k)$. For this case we have to put in a lot of extra effort, but on the other hand, our auxiliary theorem on differential equations may be of independent interest.

Our solution y of $F(X, y) = 0$ generates a function field $\mathscr{K}$ over the field of rational functions $k(X)$; and $[\mathscr{K}: k(X)] \leqslant n$. It is well known (see also our arguments below) that all the derivatives $y', y'', \ldots$ lie in $\mathscr{K}$. Now $y, y', \ldots, y^{(n)}$ must be linearly dependent over $k(X)$, so that y satisfies an nth order linear differential equation with coefficients in $k(X)$, and in fact with coefficients in the polynomial ring $k[X]$. We will make this more precise.

Let $\mathscr{L}$ be a linear differential operator,

$$\mathscr{L} = L_n(X)\frac{d^n}{dX^n} + \ldots + L_1(X)\frac{d}{dX} + L_0(X)$$

with coefficients $L_i(X)\in k[X]$ $(i = 0, \ldots, n)$. We define

$$\deg\mathscr{L} = \max(\deg L_n, \ldots, \deg L_0).$$

We further define the height by

$$H_k(\mathscr{L}) = \prod_{v\in M(k)} |\mathscr{L}|_v,$$

where

$$|\mathscr{L}|_v = \max(|L_n|_v, \ldots, |L_0|_v).$$

The absolute height is $H(\mathscr{L}) = H_k(\mathscr{L})^{1/d}$.

THEOREM 4. *Let F, y be as above. Then y satisfies a nontrivial n-th order linear differential equation $\mathscr{L}y = 0$, where*

$$\deg\mathscr{L} \leqslant 2n^3 m, \tag{4.1}$$

$$H(\mathscr{L}) < (16m)^{9n^3} H(F)^{2n^3}. \tag{4.2}$$

We have to begin with a series of lemmas.

LEMMA 6. *We have*

$$A_n^j(X)y^j = B_{j0}(X) + B_{j1}(X)y + \ldots + B_{j,n-1}(X)y^{n-1} \quad (j = 1, 2, \ldots) \tag{4.3}$$

with certain polynomials $B_{jl}\in k[X]$ satisfying

$$\deg B_{jl} \leqslant jm, \tag{4.4}$$

$$|B_{jl}|_v < (2m+2)^j |F|_v^j \quad \text{when } v\in M_\infty(k), \tag{4.5}$$

$$|B_{jl}|_v \leqslant |F|_v^j \quad \text{when } v\in M_0(k). \tag{4.6}$$

Proof. When $j\leqslant n-1$ we set $B_{jj} = A_n^j$, and $B_{jl} = 0$ for $l\neq j$. Then (4.3), (4.4), (4.6) hold. In order to prove (4.5), it is enough to observe the fact, which will be used repeatedly, that if $S(X)$, $T(X)$ are polynomials with $\deg S = s$, $\deg T = t$, then

$$|ST|_v \leqslant (1+\min(s, t))\,|S|_v\,|T|_v. \tag{4.7}$$

Thus for $j\leqslant n-1$, (4.5) holds in the strengthened form that

$$|B_{jl}|_v \leqslant (m+1)^{j-1} |F|_v^j.$$

Suppose now that the assertion is true for some $j\geqslant n-1$. Then

$$A_n^{j+1} y^{j+1} = A_n B_{j0}\, y + A_n B_{j1}\, y^2 + \ldots + A_n B_{j,n-2}\, y^{n-1} + A_n B_{j,n-1}\, y^n$$

and

$$A_n B_{j,n-1}\, y^n = -A_0 B_{j,n-1} - A_1 B_{j,n-1}\, y - \ldots - A_{n-1} B_{j,n-1}\, y^{n-1}.$$

Therefore (4.3) holds for $j+1$ with

$$B_{j+1,0} = -A_0 B_{j,n-1},$$
$$B_{j+1,i} = A_n B_{j,i-1} - A_i B_{j,n-1} \quad (0 < i < n).$$

Now (4.4), (4.5), (4.6) follow by induction, where for (4.5) we use the observation (4.7).

In what follows, denote the partial derivatives of $F(X, Y)$ by $F_X, F_Y, F_{XX}, F_{XY}, \ldots$ Further $G_t = G_t(X, Y)$ will be a polynomial parametrized by $t = 1, 2, \ldots$, and with partial derivatives G_{tX}, G_{tY}.

LEMMA 7. *For $t = 1, 2, \ldots$ we have*

$$F_Y(X, y)^{2t-1} y^{(t)} = G_t(X, y) \tag{4.8}$$

where $G_t(X, Y) \in k[X, Y]$ *has*

$$\deg_X G_t \leqslant (2m-1)t-m, \tag{4.9}$$

$$\deg_Y G_t \leqslant (2n-2)t+2-n, \tag{4.10}$$

$$|G_t|_v < (20(m+1)^3 n^4)^t t! |F|_v^{2t-1} \quad \textit{when } v \in M_\infty(k), \tag{4.11}$$

$$|G_t|_v \leqslant |F|_v^{2t-1} \quad \textit{when } v \in M_0(k). \tag{4.12}$$

Proof. Differentiating $F(X, y) = 0$ we obtain $F_X + F_Y y' = 0$, so that (4.8) is true for $t = 1$ with $G_1 = -F_X$. Then also (4.9), (4.10) hold for $t = 1$. When v is Archimedean, $|F_X|_v \leqslant m|F|_v$, so that (4.11) is certainly true for $t = 1$. Similarly, we have (4.12).

We now proceed by induction on t. Differentiating (4.8) we obtain

$$(2t-1) F_Y^{2t-2}(F_{XY}+F_{YY} y') y^{(t)} + F_Y^{2t-1} y^{(t+1)} = G_{tX} + G_{tY} y'.$$

We multiply by F_Y^2 and note $F_Y^{2t-1} y^{(t)} = G_t$ and $F_Y y' = -F_X$ to obtain

$$(2t-1) G_t(F_Y F_{XY} - F_X F_{YY}) + F_Y^{2t+1} y^{(t+1)} = (F_Y G_{tX} - F_X G_{tY}) F_Y.$$

Thus (4.8) holds for $t+1$ with

$$G_{t+1} = (2t-1)\begin{vmatrix} F_X & F_Y \\ F_{XY} & F_{YY} \end{vmatrix} G_t - F_Y \begin{vmatrix} F_X & F_Y \\ G_{tX} & G_{tY} \end{vmatrix}. \tag{4.13}$$

Therefore

$$\deg_X G_{t+1} \leqslant 2m-1+\deg_X G_t,$$

$$\deg_Y G_{t+1} \leqslant 2n-2+\deg_Y G_t,$$

so that the truth of (4.9), (4.10) for t implies it for $t+1$.

In what follows, we will use the fact that if $S(X, Y)$, $T(X, Y)$ are in $k[X, Y]$ with $\deg_X S = s_X$, $\deg_Y S = s_Y$, $\deg_X T = t_X$, $\deg_Y T = t_Y$, then

$$|ST|_v \leqslant (1+\min(s_X, t_X))(1+\min(s_Y, t_Y))|S|_v |T|_v. \tag{4.14}$$

(Of course, much more is true when $v \in M_0(k)$.) We have

$$|F_X|_v \leqslant m|F|_v, \quad |F_Y|_v \leqslant n|F|_v, \quad |F_{XY}|_v \leqslant mn|F|_v, \quad |F_{YY}|_v \leqslant n^2|F|_v$$

and

$$|F_X F_{YY}|_v \leqslant m(n-1)|F_X|_v |F_{YY}|_v \leqslant m^2 n^3 |F|_v^2,$$

$$|F_Y F_{XY}|_v \leqslant mn|F_Y|_v |F_{XY}|_v \leqslant m^2 n^3 |F|_v^2,$$

so that

$$|F_X F_{YY} - F_Y F_{XY}|_v \leqslant 2m^2 n^3 |F|_v^2.$$

(Here and below, the $\leqslant$ may often be replaced by $<$ if $F \neq 0$.) We further obtain

$$|(F_X F_{YY} - F_Y F_{XY}) G_t|_v \leqslant (2m)(2n-1)|F_X F_{YY} - F_Y F_{XY}|_v |G_t|_v$$
$$\leqslant 8m^3 n^4 |F|_v^2 |G_t|_v.$$

On the other hand,

$$|F_X G_{tY}|_v \leqslant m(n+1)|F_X|_v |G_{tY}|_v$$
$$\leqslant m(n+1) m|F|_v((2n-2)t+2-n)|G_t|_v$$
$$\leqslant 2m^2 n^2 t |F|_v |G_t|_v,$$

$$|F_Y G_{tX}|_v \leqslant (m+1)n|F_Y|_v |G_{tX}|_v$$
$$\leqslant (m+1)n \cdot n|F|_v((2m-1)t-m)|G_t|_v$$
$$\leqslant 2(m+1)^2 n^2 t |F|_v |G_t|_v,$$

so that

$$|F_X G_{tY} - F_Y G_{tX}|_v \leqslant 4(m+1)^2 n^2 t |F|_v |G_t|_v.$$

We further obtain

$$|F_Y(F_X G_{tY} - F_Y G_{tX})|_v \leqslant (m+1)n^2 |F|_v |F_X G_{tY} - F_Y G_{tX}|_v$$
$$\leqslant 4(m+1)^3 n^4 t |F|_v^2 |G_t|_v.$$

Combining our estimates, we see that (4.13) yields

$$|G_{t+1}|_v \leqslant ((2t-1)\cdot 8m^3 n^4 + 4(m+1)^3 n^4 t)|F|_v^2 |G_t|_v$$
$$\leqslant 20(m+1)^3 n^4 t |F|_v^2 |G_t|_v.$$

Now (4.11) follows by induction on t. The proof of (4.12) is similar and simpler.

LEMMA 8. *For* $0 \leqslant t \leqslant n$ *we have*

$$F_Y(X, y)^{2n-1} y^{(t)} = N_t(X, y) \tag{4.15}$$

where $N_t(X, Y) \in k[X, Y]$ *with*

$$\deg_X N_t \leqslant 2nm-m-t, \tag{4.16}$$

$$\deg_Y N_t \leqslant 2n^2-3n+2, \tag{4.17}$$

$$|N_t|_v \leqslant (20(m+1)^3 n^5)^{n+1} |F|_v^{2n-1} \quad \textit{when } v \in M_\infty(k), \tag{4.18}$$

$$|N_t|_v \leqslant |F|_v^{2n-1} \quad \textit{when } v \in M_0(k). \tag{4.19}$$

Proof. When $t=0$ we set $N_0 = Y\cdot F_Y^{2n-1}$. Then (4.16), (4.17), (4.19) are clear. On the other hand

$$|F_Y|_v \leqslant n|F|_v \quad \text{and} \quad |F_Y^j|_v \leqslant ((m+1)n)^{j-1}|F_Y|_v^j$$

by (4.14) and induction on j for $j=1,2,\ldots$, so that

$$|F_Y^j|_v \leqslant ((m+1)n^2)^j |F|_v^j \quad (j=1,2,\ldots). \tag{4.20}$$

With $j=2n-1$ we obtain (4.18) for $t=0$.

When $0<t\leqslant n$, we take

$$N_t(X,Y) = G_t(X,Y)\cdot F_Y(X,Y)^{2n-2t}. \tag{4.21}$$

In view of (4.9), (4.10) we obtain

$$\deg_X N_t \leqslant (2m-1)t-m+(2n-2t)m = 2nm-m-t,$$

$$\deg_Y N_t \leqslant (2n-2)t+2-n+(2n-2t)(n-1) = 2n^2-3n+2,$$

i.e., (4.16), (4.17). Using (4.21), (4.14), (4.16), (4.17), (4.11), (4.20), we get

$$|N_t|_v \leqslant ((2m-1)t-m+1)((2n-2)t+3-n)|G_t|_v|F_Y^{2n-2t}|_v$$

$$\leqslant (2mt)(2nt)\big((20(m+1)^3n^4)^t\cdot t!\cdot((m+1)n^2)^{2n-2t}\big)|F|_v^{2n-1}.$$

Since $t\leqslant n$, we may conclude that

$$|N_t|_v \leqslant (2mn)(2n^2)(20(m+1)^3n^4)^n n^n |F|_v^{2n-1}$$

$$\leqslant (20(m+1)^3n^5)^{n+1}|F|_v^{2n-1},$$

i.e., (4.18). The proof of (4.19) is similar and simpler.

LEMMA 9. *For* $0\leqslant t\leqslant n$ *we have*

$$A_n(X)^{2n^2-3n+2}F_Y(X,y)^{2n-1}y^{(t)} = Q_t(X,y) \tag{4.22}$$

where

$$\deg_X Q_t \leqslant 2n^2m, \tag{4.23}$$

$$\deg_Y Q_t \leqslant n-1, \tag{4.24}$$

$$|Q_t|_v \leqslant 2^{2n+3}(2m+2)^{2n^2+7}n^{5n+11}|F|_v^{2n^2-n+1} \quad \textit{when } v\in M_\infty(k), \tag{4.25}$$

$$|Q_t|_v \leqslant |F|_v^{2n^2-n+1} \quad \textit{when } v\in M_0(k). \tag{4.26}$$

Proof. Write

$$N_t(X,Y) = N_{t0}(X)+N_{t1}(X)Y+\ldots+N_{ts}(X)Y^s$$

where $s=2n^2-3n+2$. Since by Lemma 6,

$$A_n^j y^j = B_{j0}+B_{j1}y+\ldots+B_{j,n-1}y^{n-1} = B_j(X,y),$$

say, (4.22) will hold with

$$Q_t(X,Y) = \sum_{j=0}^{s} A_n(X)^{s-j}N_{tj}(X)B_j(X,Y) \quad (0\leqslant t\leqslant n). \tag{4.27}$$

Then (4.24) is clear. On the other hand, by (4.16), (4.4), a typical summand in (4.27) has

$$\deg_X \leqslant (s-j)m+(2nm-m-t)+jm \leqslant (s+2n-1)m \leqslant 2n^2m,$$

so that (4.23) holds.

We have

$$|A_n^{s-j}|_v \leqslant (m+1)^{s-j}|F|_v^{s-j},$$

$$|N_{tj}|_v \leqslant q|F|_v^{2n-1} \quad \text{with } q=(20(m+1)^3n^5)^{n+1}$$

by (4.18),

$$|B_j|_v \leqslant (2m+2)^j|F|_v^j$$

by (4.5). A typical summand on the right hand side of (4.27) has v-adic absolute value

$$\leqslant ((s-j)m+1)((s-j)m+2nm-m+1)|A_n^{s-j}|_v|N_{tj}|_v|B_j|_v$$

$$\leqslant (2n^2m)(3n^2m)(m+1)^{s-j}q(2m+2)^j|F|_v^{s+2n-1}$$

$$\leqslant 6n^4m^2(2m+2)^s(20(m+1)^3n^5)^{n+1}|F|_v^{s+2n-1}$$

$$< 2^{2n+2}(2m+2)^{s+3n+5}n^{5n+9}|F|_v^{s+2n-1}$$

$$= 2^{2n+2}(2m+2)^{2n^2+7}n^{5n+9}|F|_v^{2n^2-n+1}.$$

After multiplying by the number $s+1\leqslant 2n^2$ of summands in (4.27), we obtain (4.25). The proof of (4.26) is similar and simpler.

Proof of Theorem 4. We may suppose that some coefficient of F is 1, so that

$$|F|_v \geqslant 1 \tag{4.28}$$

for each v. Since the discriminant $D(X)\neq 0$ by hypothesis, y with $F(X,y)=0$ has $F_Y(X,y)\neq 0$. Write

$$Q_t(X,Y) = Q_{t0}(X)+Q_{t1}(X)Y+\ldots+Q_{t,n-1}(X)Y^{n-1}.$$

In view of Lemma 9, it will suffice to choose the coefficients $L_n,\ldots,L_0$ of the desired linear differential operator $\mathscr{L}$ with

$$\sum_{t=0}^{n} Q_{tj}L_t = 0 \quad (j=0,\ldots,n-1).$$

This is a system of n linear equations in the $n+1$ unknowns $L_0, \ldots, L_n$. Say this system has rank r, and the equations with $j = 0, \ldots, r-1$ are independent, say the submatrix (Q_{tj}) with $0 \leqslant t, j \leqslant r-1$ is nonsingular. We set $L_{r+1} = \ldots = L_n = 0$ (there are no such when $r = n$), and for $L_0, \ldots, L_r$ we take certain obvious determinants of order r from (Q_{tj}) with $0 \leqslant t \leqslant r$, $0 \leqslant j \leqslant r-1$.

Then the L_i will be in $k[X]$, and (4.23) yields

$$\deg L_i(X) \leqslant 2n^2 mr \leqslant 2n^3 m \quad (i = 0, \ldots, n),$$

and therefore (4.1). The determinant for L_i has $r!$ summands, and each summand is (up to sign) a product of r factors Q_{tj}. Therefore by (4.14), (4.23), each summand has v-adic norm

$$\leqslant (2n^2 m+1)^{r-1} \max_{0 \leqslant t < n} |Q_t|^r,$$

and by (4.25) this is

$$< (4n^2 m)^{n-1}\, 2^{2n^2+3n} (2m+2)^{2n^3+7n}\, n^{5n^2+11n} |F|_v^{2n^3},$$

in view of (4.28). Since the determinant for each L_i has $r!$ summands, we obtain

$$|\mathcal{L}|_v < 2^{4n^3+2n^2+19n}\, n^{5n^2+14n}\, m^{2n^3+8n-1} |F|_v^{2n^3} < 2^{35n^3} m^{9n^3} |F|_v^{2n^3}.$$

This holds for $v \in M(k)$, whether Archimedean or not. For $v \in M_0(k)$, i.e., non-Archimedean, we obtain in a similar manner that

$$|\mathcal{L}|_v \leqslant |F|_v^{2n^3}.$$

Theorem 4 follows.

5. Application of Clark's Theorem. Let $\mathcal{L}$ be the differential operator of Theorem 4 and $l = \deg \mathcal{L}$, so that

$$l \leqslant 2n^3 m. \tag{5.1}$$

Let t be least such that each $X^{t-i} L_i(X)$ $(i = 0, \ldots, n)$ is a polynomial. After multiplying our differential operator by X^t, and denoting the new differential operator and its coefficients again by $\mathcal{L}$, $L_n, \ldots, L_0$, we have

$$L_i(X) = \sum_{j=0}^{l+t} \lambda_{ij} X^{i+j} \quad (i = 0, \ldots, n), \tag{5.2}$$

where the λ_{ij} lie in k, and $\lambda_{00}, \lambda_{10}, \ldots, \lambda_{n0}$ are not all 0. $\mathcal{L}$ applied to X^s is

$$\mathcal{L}(X^s) = \sum_{j=0}^{l+t} \Phi_j(s+j) X^{s+j} \quad (s = 0, 1, \ldots), \tag{5.3}$$

where Φ_j $(j = 0, \ldots, l+t)$ is the polynomial with

$$\Phi_j(s+j) = \sum_{i=0}^{n} \lambda_{ij} s(s-1) \ldots (s-i+1).$$

Then Φ_0 is the classical indicial polynomial of $\mathcal{L}$. We have

$$\Phi_j(X) = \sum_{i=0}^{n} \lambda_{ij} (X-j)(X-j-1) \ldots (X-j-i+1),$$

where the summand with $i = 0$ is to be interpreted as λ_{0j}. Therefore

$$|\Phi_j|_v \leqslant \big(1+(j+1)+(j+1)(j+2)+ \ldots +(j+1)\ldots(j+n)\big) |\mathcal{L}|_v,$$

and

$$|\Phi_j|_v \leqslant (1+j+n)^n |\mathcal{L}|_v \quad \text{when } v \in M_\infty(k). \tag{5.4}$$

On the other hand,

$$|\Phi_j|_v \leqslant |\mathcal{L}|_v \quad \text{when } v \in M_0(k). \tag{5.5}$$

Put

$$\psi_v = \max_{j=0,\ldots,l+t} (|\Phi_j|_v / |\Phi_0|_v)^{1/j}; \tag{5.6}$$

here and in (5.7) below, the term on the right for $j = 0$ is to mean 1.

LEMMA 10. *We have*

$$\prod_{v \in M(k)} \psi_v \leqslant (n+2)^{2nd} H_k(\mathcal{L}).$$

Proof. When $v \in M_\infty(k)$, we have from (5.4) (and the fact that $(1+j+n)^{1/j} \leqslant n+2$ when $j \geqslant 1$) that

$$\psi_v \leqslant (n+2)^n \max_{j=0,\ldots,l+t} (|\mathcal{L}|_v / |\Phi_0|_v)^{1/j} \leqslant (n+2)^n \max(|\mathcal{L}|_v, |\Phi_0|_v)/|\Phi_0|_v. \tag{5.7}$$

When $v \in M_0(k)$, then

$$\psi_v \leqslant \max(|\mathcal{L}|_v, |\Phi_0|_v)/|\Phi_0|_v.$$

Therefore, using (5.4), (5.5) again,

$$\prod_{v \in M(k)} \psi_v \leqslant (n+2)^{nd} \Big(\prod_{v \in M(k)} \max(|\mathcal{L}|_v, |\Phi_0|_v) \Big) H_k(\Phi_0)^{-1}$$
$$\leqslant (n+2)^{2nd} \prod_{v \in M(k)} |\mathcal{L}|_v = (n+2)^{2nd} H_k(\mathcal{L}).$$

When $v \in M_0(k)$ and $v \mid p$, put

$$\omega_v = p^{-n/(p-1)} \psi_v^{-1}. \tag{5.8}$$

LEMMA 11. *Suppose $v \in M_0(k)$, $w \in M(K)$ and $w \mid v$. Then $\varrho_w \geqslant \omega_v$.*

Proof. This follows from Clark's Theorem 3 in [1]. Clark uses the order function rather than our absolute value $|\cdot|_w$, so that his value group is additive rather than multiplicative. His $b_1(l)$ corresponds to our ψ_v^{-1}, his $b(l)$ corresponds to our ω_v. The zeros of our indicial polynomial Φ_0 are algebraic, so that they are non-Liouville as defined by Clark. His function $w(\alpha)$ (see Definition 2 in [1]) has $0 \leqslant w(\alpha) \leqslant 1/(p-1)$. Since Φ_0 is of degree $\leqslant n$, Clark's $w(\Phi_0) \leqslant n/(p-1)$, which explains the exponent in (5.8).

6. Conclusion. For $w \mid v$ with $w \in M(K)$, $v \in M_0(k)$, the quantity τ_w of Lemma 2 has $\tau_w \geqslant \min(\sigma_v, \omega_v)$ by Lemma 11. When $v \mid p$, let τ_v^* be the largest number of the type p^u with $u \in \mathbf{Z}$ having $\tau_v^* \leqslant \min(\sigma_v, \omega_v)$. Then $\tau_v^* \in G_v$,

$$\tau_v^* \geqslant p^{-1} \min(\sigma_v, \omega_v),$$

and

$$|\alpha_j|_w \leqslant |F|_v (1/\tau_v^*)^{m+j}$$

by Lemma 2.

For $v \in M_2(k)$ we set

$$A_v = B_v = |F|_v / \tau_v^*.$$

Then $B_v \in G_v$, and (1.4), (1.7) are true for $w \mid v$. We have

$$\prod_{v \in M_2(k)} A_v \leqslant H_k(F) \prod_{v \in M_2(k)} (p \max(\sigma_v^{-1}, \omega_v^{-1}))$$

where $p = p(v)$ with $v \mid p$. We obtain

$$\leqslant H_k(F) \prod_{v \in M_2(k)} (p^{1+(n/(p-1))} \sigma_v^{-1} \psi_v)$$

from (5.8), since $\sigma_v \leqslant 1$, $\psi_v \geqslant 1$. Given p, there are d elements $v \in M(k)$ with $v \mid p$, so that

$$\prod_{v \in M_2(k)} p^{1+(n/(p-1))} \leqslant \prod_{p \leqslant n} p^{2nd/(p-1)} \leqslant n^{2n^2 d}.$$

(We are very generous!) Combining this with Lemma 5 and 10, we get

$$\prod_{v \in M_2(k)} A_v \leqslant (n^n (m+1)(n+1)\sqrt{n}(n+2))^{2nd} H(\mathscr{L})^d H(F)^{2nd}.$$

With the help from Theorem 4 we finally obtain

$$\prod_{v \in M_2(k)} A_v < (16m)^{11n^3 d} H(F)^{(2n^3+2n)d}, \tag{6.1}$$

so that (1.6) holds. Theorem 1 is established.

For (1.8) and Theorem 2, we recall that $B_v = A_v$ when $v \in M_2(k)$, so that (3.3) in conjunction with (6.1) yields

$$\prod_{v \in M(k)} B_v < (16m)^{11n^3 d} H(F)^{(2n^3+2n)d} C^{2nm},$$

further by (1.5),

$$\prod_{v \in M(k)} B_v < (16m)^{11n^3 d} (4mn\sqrt{n})^{6n^2 md} H(F)^{(2n^3+2n+4n^2 m)d},$$

and therefore (1.8).

References

[1] D. N. Clark, *A note on the p-adic convergence of solutions of linear differential equations*, Proc. Amer. Math. Soc. 17 (1966), 262–269.

[2] J. Coates, *Construction of rational functions on a curve*, Proc. Camb. Phil. Soc. 68 (1970), 105–123.

[3] B. Dwork and B. Robba, *On natural radii of p-adic convergence*, Trans. Amer. Math. Soc. 256 (1979), 199–213.

[4] G. Eisenstein, *Über eine allgemeine Eigenschaft der Reihen-Entwicklungen aller algebraischen Funktionen*, Bericht Königl. Preuss. Akad. d. Wiss. zu Berlin (1852), 441–443.

[5] K. Mahler, *An application of Jensen's formula to polynomials*, Mathematika 7 (1960), 98–100.

[6] W. Schmidt, *The number of solutions of norm form equations*, Trans. Amer. Math. Soc. 317 (1990), 197–227.

[7] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss., Phys.-math. Klasse 1929, Nr. 1.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF COLORADO
Boulder
Colorado 80309-0426
U.S.A.

Received on 10.4.1989 (1923)