Vol. 65, No. 1 DUKE MATHEMATICAL JOURNAL © January 1992

THE EISENSTEIN CONSTANT

BERNARD M. DWORK AND ALFRED J. VAN DER POORTEN

Introduction. Let $f(X, Y) \in \mathbb{Z}[X, Y]$ be of degree n in the variable Y and have coefficients bounded by H. A remark of Eisenstein [Eis] points out that, if y is a formal series

$$y = \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \cdots$$

which satisfies $f(X, y) = 0$, then there are natural numbers a_0 and a so that

$$a_0 a^i \alpha_i \qquad (i = 0, 1, \ldots)$$

are algebraic integers. (See [Die], p. 327 ff. for an old-fashioned proof.) We assert that the Eisenstein constant a is bounded by $c(n)H^{2n-1}$, where

$$c(n) = n^n(2n-1)!\mu_n\lambda_n^n,$$

$$\mu_n = \prod_{p \leqslant n} p \leqslant n!,$$

$$\lambda_n = \exp(\tau_n + \psi(n)),$$

$$\tau_n = \sum_{p \leqslant n} \frac{1}{p-1} \log p \leqslant \log 2 + 0.5 \log^2 n,$$

$$\psi(n) = \sum_{p \leqslant n} \left[\frac{\log n}{\log p}\right] \log p \leqslant 1.22n + 2.24 \log^2 n.$$

(For this estimate for ψ see [Sh, p. 389].) Thus,

$$c(n) \leqslant 4.8(8e^{-3}n^{4+2.74 \log n}e^{1.22n})^n.$$

The factor H^{2n-1} appears for the following reason: Suppose we write the discriminant $R(f, f_Y)$ of f in the form

$$D(X) = X^l(D_0 X^\mu + D_1 X^{\mu-1} + \cdots + D_\mu), \qquad D_\mu \neq 0, \quad D_j \in \mathbb{Z}.$$

Received 17 December 1990. Revision received 4 May 1991.
Dwork supported in part by an NSF Grant.
Van der Poorten's work supported in part by grants from the Australian Research Council.

For each prime p let r_p be the p-adic magnitude in the valuation of $\mathbb{C}_p$ normalised by $|p|_p = 1/p$ of the zero of D closest to the origin. We estimate

$$\prod_p r_p.$$

We know

$$r_p \geqslant |D_\mu|_p \quad \text{and so} \quad \prod_p r_p \geqslant \prod_p |D_\mu|_p = \frac{1}{|D_\mu|_\infty}.$$

Therefore,

$$\prod_p \frac{1}{r_p} \leqslant |D_\mu|_\infty \leqslant n^n(2n-1)!H^{2n-1}.$$

The last inequality follows from the determinant formula for D: We recall that, if $f(X, Y) = A_0 Y^n + A_1 Y^{n-1} \cdots + A_n$, then D is the determinant of an element of $\mathscr{M}_{2n-1}(\mathbb{Z}[X])$, $n-1$ of whose rows have entries lying in the set $\{A_0, A_1, \ldots, A_n\}$ and n of whose rows have entries lying in the set $\{nA_0, (n-1)A_1, \ldots, A_{n-1}\}$. Set $\delta = Xd/dX$. Our method is to consider the differential equation $\delta V = GV$ satisfied by the Vandermonde matrix constructed with the powers of the roots, $z_1, \ldots, z_n$ of f; i.e.,

$$V = (z_j^i)_{1 \leqslant j \leqslant n, 0 \leqslant i \leqslant n-1}.$$

The solution matrix is of the form $Y(X)X^A$ where $Y \in \mathrm{Gl}(n, \mathbb{Q}(X))$ and A is a diagonal matrix with coefficients in $\frac{1}{n!}\mathbb{Z}$. We may assume $Y \in \mathscr{M}_n(\mathbb{Q}[[X]])$. For each prime p let ρ_p be the p-adic radius of convergence of Y. Then ρ_p is a (possibly nonintegral) power of $1/p$. We choose $\sigma_p \leqslant \rho_p$ so that σ_p is bounded above by an integral power of $1/p$ which is again bounded from above by ρ_p. Then

$$a \leqslant \prod_p \frac{1}{\sigma_p}.$$

We know (see §6) that $\rho_p \geqslant r_p$ if $p > n$. Furthermore, $|D_\mu|_p$ is an integral power of $1/p$, and so we may take $\sigma_p = |D_\mu|_p$ for $p > n$. In this article we verify a conjecture of W. M. Schmidt [Schm] and show that, for all p, $\rho_p \geqslant c(n, p)r_p$, and in particular for $p \leqslant n$, we may choose $\sigma_p = p^{-1}c(n, p)r_p$. Thus,

$$a \leqslant c'(n) \prod_p \frac{1}{r_p} \leqslant c(n)H^{2n-1}$$

where

$$c(n) = n^n(2n-1)! \prod_{p \leqslant n} c(n,p)^{-1} \cdot \prod_{p \leqslant n} p.$$

By homothety the calculation of $c(n, p)$ may be reduced to the case $r_p = 1$. As usual, set π a fixed $(p-1)$-st root of $-p$. (We will only be interested in its p-adic value.)

In §2 we show that, if f is irreducible as an element of $E[Y]$ (E = completion of $\mathbb{Q}_p(X)$ under the p-adic gauss norm), then the solutions of $f(X, Y)$ at the generic unit t converge in the disk $D(t, |n\pi|^-)$; weaker estimates requiring less computation are given in §1. Dropping the irreducibility hypothesis, the solutions of $f(X, Y)$ at t converge in $D(t, |\pi p^{\log n/\log p}|_p^-)$.

In §3 we give a weak transfer theorem which shows that, if $r_p = 1$, then $\rho_p \geqslant |\pi|^n |p|_p^{n \log n/\log p}$, and so

$$\prod_p c(n,p)^{-1} = \left(\prod_{p \leqslant n} p^{1/(p-1)+\log n/\log p} \right)^n = \lambda_n^n.$$

Thus,

$$c(n) = n^n(2n-1)!\lambda_n^n \mu_n.$$

Schmidt [Schm] first employs [DwRo] to give sharp estimates in terms of f for the Eisenstein constant at primes greater than n. However, in his analysis the contribution from the small primes $p \leqslant n$ leads to a bound of the shape

$$a < c''(N)H^{8N^3}$$

where N is the total degree of f. Schmidt's conjecture immediately entails our exponent for H. He guesses $c(n) = n^{l(n)}$ where l is linear in n. This surmise cannot be checked by our methods without more precise information concerning the variation with p (for $p \leqslant n$) of the degrees of the factors of $f(x, y)$ over the completion of $Q(x)$ under the p-adic gauss norm.

We are indebted to Wolfgang Schmidt for making his manuscript available to us. We have been guided by his conjectures. We are indebted to Francesco Baldassarri for his assistance in the proof of Theorem 3.

The estimate for $c(n)$ could be improved by means of the bound [RS, Theorem 6]

$$\psi(n) < 1.0012(n + \sqrt{n}) + 3n^{1/3}.$$

We have received helpful advice from Brian Conrey.

1. Fields of analytic elements. (Cf. [DwRo, §1].) Let Ω be an algebraically closed field of characteristic zero complete under a rank-one nonarchimedean valuation with residue class field of characteristic p.

Let t be a unit of Ω to be chosen later. For $r \in (0, 1]$ let W_r be the ring of bounded analytic functions on $D(t, r^-)$ taking values in Ω. We may view W_r as a subring of $\mathcal{O}_t$, the ring of germs of analytic functions at t. Let $\| \ \|_r$ denote the sup norm on W_r. For $r_1 < r_2$ we have $W_{r_1} \supset W_{r_2}$ and for $v \in W_{r_2}$

$$\|v\|_{r_2} \geqslant \|v\|_{r_1}.$$

Certainly, $\partial = d/dX$ defines a continuous endomorphism of W_r. The operator norm is given by

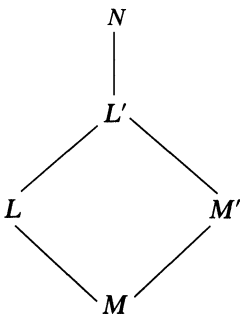
$$\|\partial\|_r = 1/r.$$

Let M be a subfield of W_r. For $v \in M$, $v \neq 0$, v can have neither zero nor pole in $D(t, r^-)$, and hence $|v(t)| = |v(x)|$ for all $x \in D(t, r^-)$; so $|v(t)| = \|v\|_r$. Thus, for fields there is no need to specify the value of r; accordingly, we write $|v|$ instead of $\|v\|_r$. But $|\partial|$ does depend on r. Let $\mathfrak{I}$ be the ring of integers of M.

THEOREM 1. *There exists a mapping c: $\mathbb{N} \to (0, 1)$ such that, if L is an extension of M of degree n, then $L \subset W_{rc(n)}$. This function depends upon p but not upon M.*

Proof. The proof consists of several reduction steps. Let ord $n = l$. We commence by reduction to the case in which L/M is a tower of l cyclic extensions of degree p.

We follow a reduction step similar to that in the proof of the second inequality of classfield theory [Ar, p. 133]. Let N be the galois closure of L over M. Let H be the galois group of N/L and let G be the galois group of N/M. Let P be a p-Sylow subgroup of H and P' a p-Sylow subgroup of G which contains P. Let L' be the fixed field of P and M' be the fixed field of P'. Now deg L'/L and deg M/M' are prime to p while deg L'/M' is a power of p. Since deg $L/M \cdot$ deg $L'/L =$ deg $L'/M =$ deg $M'/M \cdot$ deg L'/M', we conclude that deg $L'/M' = p^l$. Because P' is a p-group, it



follows that L'/M' is a tower of l cyclic extensions of degree p. Since the degree of M'/M is prime to p, we now know from [DwRo, Lemma 1.2] (see also §6 for the

case in which $r < 1$) that $M' \subset W_r$. This completes the proof of the reduction step. □

We have reduced to the following lemma.

LEMMA 1.1. *There exists a constant μ_p such that, if M is a complete subfield of W_r, then each cyclic extension M' of degree p lies in $W_{r\mu_p}$.*

We will need a few propositions:

For $z \in M', z \notin M$, let $z_1, \ldots, z_p$ be the conjugates of z and let $\Delta(z)$ be the associated polynomial discriminant

$$\Delta(z) = \prod_{i \neq j} (z_i - z_j)^2.$$

PROPOSITION 1.1. *Let M'/M be cyclic of degree p. Then there exists $z \in \mathcal{O}_{M'}$, $z \notin M$, such that* ord $\Delta(z) < 2v_0$ *where* $v_0 = p^2 - p$.

Proof. We may assume that ord $\Delta(z) = v > v_0$. Let $|z_1 - z_2| = \lambda$ be the minimal distance between conjugates of z. We may choose $\sigma \in \mathrm{Gal}(M'/M)$ such that $\sigma z_1 = z_2$ and then label the conjugates so that $\sigma z_i = z_{i+1}$. Then $\lambda = |z_2 - z_3| = \cdots = |z_{p-1} - z_p|$ so that $\lambda \geqslant |z_1 - z_j|$ for all j, which implies $\lambda \geqslant |z_i - z_j|$ for all $i \neq j$. Hence, by minimality, $|z_i - z_j| = \lambda$. Thus, $\lambda^{v_0} = |p|^v$, and so

$$z_j - z_1 = q_j \qquad (2 \leqslant j \leqslant p), \qquad \text{ord } q_j = v/v_0.$$

We conclude that

$$M \ni A = \sum_{j=1}^{p} z_j = pz_i + ph_i \qquad \text{ord } h_i \geqslant -1 + v/v_0.$$

We choose $\gamma \in \mathbb{Q}_p$ such that ord $\gamma = \lfloor v/v_0 \rfloor - 1$ and write

$$\frac{A}{p} = z_i + \gamma\eta_i, \qquad \text{ord } \eta_i \geqslant 0.$$

Clearly, $\eta_1, \ldots, \eta_p$ are conjugates of $\eta \in \mathcal{O}_{M'}$, $\eta \notin M$, and $\gamma^{v_0}\Delta(\eta) = \Delta(z)$; thus,

$$\text{ord } \Delta(\eta) = v - v_0(\lfloor v/v_0 \rfloor - 1) < 2v_0$$

as asserted.

Remark. This estimate is quite crude. Under the hypothesis of discrete valuation better estimates will be obtained.

PROPOSITION 1.2. *Let M' be a cyclic extension of degree p of M, a complete subfield of W_r. Let $z \in \mathcal{O}_{M'}$, $z \notin M$. Take V to be the Vandermonde matrix*

$$V = \begin{bmatrix} 1 & \cdots & 1 \\ z_1 & \cdots & z_p \\ \vdots & \vdots & \vdots \\ z_1^{p-1} & \cdots & z_p^{p-1} \end{bmatrix}$$

and set $\lambda = |z_1 - z_2|$.

Then

$$\frac{dV}{dX} = GV$$

where $G \in \mathcal{M}_p(M)$ and $|G| \leqslant \dfrac{1}{r\lambda^{2(p-1)}}$.

Proof. The automorphisms of M'/M commute with $\partial = d/dX$, and hence $G \in \mathcal{M}_p(M)$. (See the appendix for a more general result of this type.)

Let $f(X, Y) = Y^p + A_1 Y^{p-1} + \cdots + A_p$ be the monic polynomial for z over M. Then

$$|f_X(X, z_1)| \leqslant 1/r$$

$$|f_Y(X, z_1)| = \left| \prod_{j=2}^{p} (z_j - z_1) \right| = \lambda^{p-1}.$$

Thus,

$$|\partial z_1^j| \leqslant |\partial z_1| = |f_X(X, z_1)/f_Y(X, z_1)| \leqslant 1/r\lambda^{p-1},$$

and so $|\partial V| \leqslant (r\lambda^{p-1})^{-1}$.

The minor of z_p^j in the matrix V is a polynomial in $\mathbb{Z}[z_1, \ldots, z_{p-1}]$ divisible by

$$\prod_{1 \leqslant i < j \leqslant p-1} (z_i - z_j),$$

and hence

$$|\text{adj } V| \leqslant \lambda \binom{p-1}{2}.$$

Thus,

$$|V^{-1}| = |\det V|^{-1} \cdot |\text{adj } V| \leqslant \lambda \binom{p-1}{2} - \binom{p}{2} = (\lambda^{p-1})^{-1}.$$

So

$$|G| = |\partial V \cdot V^{-1}| \leqslant (r\lambda^{2(p-1)})^{-1}. \quad \square$$

PROPOSITION 1.3. *Let M be a complete subfield of W_r. If $G \in \mathcal{M}_n(M)$ with $|G| \leqslant 1/\mu r$ and $\mu \leqslant 1$, then the solution matrix at t of the equation*

$$\partial \mathbf{y} = G\mathbf{y}$$

converges in $D(t, |\pi|\mu r^-)$.

These solutions need not lie in $W_{|\pi|\mu r}$ as they need not be bounded.

Proof. The solution matrix is by Taylor's theorem given by

$$Y(x) = I_n + G(t)(x - t) + G_2(t)(x - t)/2! + \cdots$$

where $G_0 = I, G_1, G_2, \ldots$ are given inductively by

$$G_{s+1} = \partial G_s + G_s G$$

(so that $\partial^s \mathbf{y} = G_s \mathbf{y}$ for all solutions $\mathbf{y}$).

Clearly,

$$|G_{s+1}| \leqslant |G_s| \sup\left(\frac{1}{r}, \frac{1}{r\mu}\right) = |G_s|\frac{1}{r\mu}.$$

Thus, $|G_s| \leqslant (r\mu)^{-s}$, and the assertion follows from $|\pi^s/s!| \leqslant 1$. $\square$

This completes the proof of the lemma. Putting together our estimates, we have by Proposition 1.1 $|\lambda| > |p|^2$; so in Proposition 1.2 $|G| < r^{-1}p^{4(p-1)}$, and so Proposition 1.3 gives solutions in

$$W_{r|\pi|p^{-4(p-1)}}.$$

Starting with $r = 1$ and executing l steps ($p^l = n$), we find that our solutions lie in $W_{c(n,p)}$ with

$$c(n, p) = |n|_p^{4(p-1)+1/(p-1)}.$$

In the next section we shall give precise estimates in the discrete valuation case. We first consider a less computational point of view for that case.

For each subfield M of W_r, let $\overline{M}$ denote the residue class field.

LEMMA 1.4. *Let M be a complete subfield of W_r of absolute ramification e and let M' be an extension of M of degree n with $\mathcal{O}_{M'} = \mathcal{O}_M[z]$.*

Then $M' \subset W_{|\pi||\mathfrak{D}|\mu r}$ *where* $\mathfrak{D} = \mathfrak{D}_{M'/M}$ *is the different of* M'/M *and where* $\mu \geqslant |z|^{n-1}$ *in all cases but* $\mu = 1$ *if either* $\overline{M} = \overline{M}'$ *or if* $\deg \overline{M}'/\overline{M} = n$.

Proof. Let f be the irreducible monic polynomial for z over M. Then $|f_X(x, z)| \leqslant v/r$ where $v \leqslant 1$ in all cases and $v = |p|^{1/e}$ if f is an Eisenstein polynomial.

On the other hand, $|f_Y(x, z)| = |\mathfrak{D}|$. We write

$$\partial z^i = \sum_{j=0}^{n-1} G_{i,j} z^j \qquad (n = p^l)$$

and deduce

$$|G_{i,j} z^j| \leqslant v/r|\mathfrak{D}|.$$

If $\deg \overline{M}'/\overline{M} = n$, then $|z| = 1$ while, if $|z| = |p|^{1/en}$, then $|z^j| \geqslant |p|^{(n-1)/en}$. We conclude that in any case

$$|G| \leqslant 1/\mu r|\mathfrak{D}|$$

where in general $\mu = |z|^{n-1}$, but is 1 in the cases indicated. □

The different for extensions of degree p^l can be estimated as follows.

PROPOSITION 1.5. *Let* M'/M *be a totally ramified extension of degree* $n = p^l$. *Then*

$$|\mathfrak{D}_{M'/M}| \geqslant |p^l||p|^{(n-1)/ne}.$$

Proof. The Eisenstein polynomial $Y^n + A_1 Y^{n-1} + \cdots + A_n$ has derivative

$$f'(z) = nz^{n-1} + (n-1)A_1 z^{n-1} + \cdots + A_{n-1},$$

each of whose terms has distinct valuation. The result follows from $|z| = |p|^{1/ne}$. □

PROPOSITION 1.6. *If* M'/M *is a tower of* l *extensions of degree* p *with inseparable residue class fields, then* $|\mathfrak{D}_{M'/M}| \geqslant |p^l|$.

Proof. This follows from the case $l = 1$. If $\overline{M}' = \overline{M}(\bar{z})$ and $\deg \overline{M}'/\overline{M} = p = \deg M'/M$, then $M' = M(z)$ and z is a root of a polynomial $f(Y) = Y^p + A_1 Y^{p-1} + \cdots + A_{p-1} Y + A_p$, where $|A_p| = 1 > |A_j|$ for $j = 1, 2, \ldots, p-1$.

Then $f'(z) = pz^{p-1} + (p-1)A_1 z^{p-2} + \cdots + A_{p-1}$. Since $\bar{z}$ cannot satisfy a polynomial of degree less than p over $\overline{M}$, we conclude that $|f'(z)| \geqslant |p|$. □

Remark. Propositions 1.5 and 1.6 do give good estimates for the different and by a constant field extension one could eliminate the need for ramified extensions [Epp]. However, for $\overline{M}'/\overline{M}$ inseparable of degree $n = p^l$ there is no reason to expect $\overline{M}'$ to be a simple extension of $\overline{M}$, and hence the hypotheses of Lemma 1.4 need not hold.

2. Sharper estimates. We follow the method of [DwRo, §6, 7]. We replace the multiplicative notation W_r of §1 by an additive notation with a further condition: Recall ord $x = -\log|x|_p/\log p$, $|p|_p = 1/p$.

For $c \geqslant 0$ let U_c be the set of all functions θ analytic on the set

$$\operatorname{ord}(x-t) > c + \frac{1}{p-1} \qquad (|x-t| < |p|^{c+1/(p-1)})$$

together with the further condition that, for x in this disc,

$$\operatorname{ord}\frac{\theta(x)-\theta(t)}{\theta(t)} \geqslant \operatorname{ord}(x-t) - c \quad (>0).$$

Note that this condition automatically holds if θ is holomorphic for $\operatorname{ord}(x-t) > c$, that is,

$$W_{|p|^c} \subset U_c.$$

Note that, if $c' > c$, then $U_{c'} \supset U_c$.

PROPOSITION 2.1. *If θ_1, θ_2 lie in U_c, then*
(a) *$\theta_1\theta_2 \in U_c$, and*
(b) *$\theta_1 + \theta_2 \in U_c$ if* $\operatorname{ord}(\theta_1(t) + \theta_2(t)) = \inf(\operatorname{ord}\theta_1(t), \operatorname{ord}\theta_2(t))$.

Proof. If $\theta \in U_c$, then $|\theta(x)| = |\theta(t)|$ for all x in the disc.

Thus, for assertion (a) we use

$$\left|\frac{\theta_1(x)\theta_2(x) - \theta_1(t)\theta_2(t)}{\theta_1(t)\theta_2(t)}\right| = \left|\frac{\theta_2(x)}{\theta_2(t)}\,\frac{\theta_1(x)-\theta_1(t)}{\theta_1(t)} + \frac{\theta_2(x)-\theta_2(t)}{\theta_2(t)}\right|$$

$$\leqslant \sup_{i=1,2}\left|\frac{\theta_i(x)-\theta_i(t)}{\theta_i(t)}\right| \leqslant \frac{|x-t|}{|p|^c}$$

while for assertion (b) we may assume

$$\operatorname{ord}(\theta_1(t) + \theta_2(t)) = \operatorname{ord}\theta_1(t) \leqslant \operatorname{ord}\theta_2(t),$$

and so

$$\left|\frac{\theta_1(x) - \theta_1(t) + \theta_2(x) - \theta_2(t)}{\theta_1(t) + \theta_2(t)}\right| \leqslant \sup\left(\left|\frac{\theta_1(x)-\theta_1(t)}{\theta_1(t)}\right|, \left|\frac{\theta_2(x)-\theta_2(t)}{\theta_1(t)}\right|\right)$$

$$\leqslant \sup\left(\left|\frac{\theta_1(x)-\theta_1(t)}{\theta_1(t)}\right|, \left|\frac{\theta_2(x)-\theta_2(t)}{\theta_2(t)}\right|\right). \qquad \square$$

Remark. The basic example of an element in U_1 is $\theta(x) = x^{-1/p}$. Putting $x = t(1 + \tau)$, we find for ord $\tau > 1 + \dfrac{1}{p-1}$

$$\left|\frac{\theta(x) - \theta(t)}{\theta(t)}\right| = \left|\sum_{n=1}^{\infty} \left(\frac{1}{p}\right)_n \tau^n/n!\right| = \left|\frac{\tau}{p}\right| \left|\sum_{n=1}^{\infty} \left(\left(\frac{1}{p}\right)_n p^n\right)\left(\frac{\tau}{p\pi}\right)^{n-1}\left(\frac{\pi^{n-1}}{n!}\right)\right|$$

$$\leqslant \left|\frac{\tau}{p}\right|,$$

the point being that $|\pi^{n-1}/n!| \leqslant 1$ for $n \geqslant 1$.

LEMMA 2.1. *Let M be a complete subfield of U_c with discrete valuation and let M' be an extension of degree p. Then M' lies in U_{c+1}.*

Proof. If M'/M is ramified, let $z\mathcal{O}_{M'}$ be the prime ideal of $\mathcal{O}_{M'}$. In the contrary case let z be a representative of $\bar{z}$ where $\overline{M}' = \overline{M}(\bar{z})$.

In either case each element θ of M' is a sum

$$\theta = \sum_{j=0}^{p-1} a_j z^j \qquad (a_j \in M, 0 \leqslant j < p),$$

and $|\theta| = \sup_j |a_j z^j|$.

Hence, by the proposition, θ certainly lies in U_{c+1} if both a_j and z lie in U_{c+1}. By hypothesis $a_j \in U_c$. Hence, it is enough to show that $z \in U_{c+1}$.

Denote by $f(X, Y) = Y^p + A_1(X)Y^{p-1} + \cdots + A_p(X) \in M[Y]$ the irreducible polynomial for z. Let $\xi = z(t)$ so that $f(t, \xi) = 0$ and set $z = u + \xi$.

Then u satisfies the relation

$$0 = f(x, u + \xi) - f(t, \xi),$$

which we write in the form

$$u^p + B_{p-1}u^{p-1} + \cdots + B_1 u + B_0 = 0.$$

Here,

$$B_0 = A_p(x) - A_p(t) + \sum_{i=1}^{p-1} \xi^i (A_{p-i}(x) - A_{p-i}(t)),$$

$$B_1 = p\xi^{p-1} + \sum_{i=1}^{p-1} iA_{p-i}(x)\xi^{i-1},$$

$$B_i = \binom{p}{i}\xi^{p-i} + \sum_{s=i}^{p-1} \binom{s}{i} A_{p-s}(x)\xi^{s-i}, \quad 2 \leqslant i \leqslant p.$$

Note that the B_i lie in W_r ($r = |p^c\pi|$) but need not lie in a subfield of W_r. Since the valuation is discrete, M' is not an immediate extension of M. That is, either the ramification or the residue class degree is p ([Sch, p. 37]). To fix ideas we consider three cases.

(i) *M'/M is unramified ($\overline{M}'/\overline{M}$ separable).* Then $B_1(t) = f_Y(t, \xi)$ is a unit, and hence the same holds for $B_1(x)$ for $\operatorname{ord}(x - t) > c + 1/(p - 1)$. Clearly, $|B_i(x)| \leqslant 1$ for $i \geqslant 1$ while by the hypothesis on M

$$\operatorname{ord} B_0 \geqslant \operatorname{ord}(x - t) - c$$

for $\operatorname{ord}(x - t) > c + 1/(p - 1)$.

It follows that there exists a unique solution for u such that

$$\operatorname{ord} u(x) = \operatorname{ord} B_0(x) \geqslant \operatorname{ord}(x - t) - c.$$

Thus, $z \in U_c \subset U_{c+1}$.

(ii) *M'/M is ramified.* Let e be the absolute ramification of M. Let Π be a constant, $\Pi^{pe} = p$, and set $z/\Pi = w$. It is enough to show $w \in U_{c+1}$. So we replace M (respectively M') by $M(\Pi)$ (respectively $M'(\Pi)$) and, letting f denote the polynomial satisfied by w (instead of z), we have, by transforming the Eisenstein polynomial satisfied by z,

$$\operatorname{ord} A_p = 0$$

$$\operatorname{ord} A_j > 0 \qquad 1 \leqslant j \leqslant p - 1$$

$$pe \operatorname{ord}(p - j)A_j \equiv -j \pmod{p\mathbb{Z}} \qquad 0 \leqslant j \leqslant p.$$

We assert that for $\operatorname{ord}(x - t) > c + 1 + 1/(p - 1)$

(α) $$\operatorname{ord} B_0(x) - \operatorname{ord} B_1(x) \geqslant \operatorname{ord}(x - t) - (c + 1),$$

(β) $$\operatorname{ord} B_i(x) - \operatorname{ord} B_0(x) > i(\operatorname{ord} B_1(x) - \operatorname{ord} B_0(x)) \qquad 2 \leqslant i \leqslant p.$$

Statement (β) implies analyticity in the disc $D(t, |\pi p^{c+1}|^-)$ while (α) implies that w satisfies the special growth conditions.

We note that $\xi = w(t)$ is a unit and, using the formula for B_0 and the estimate for $\operatorname{ord} A_j$, we deduce that on our open disc

(γ) $$\operatorname{ord} B_0(x) \geqslant \operatorname{ord}(x - t) - c > 1 + \frac{1}{p - 1}.$$

A classical argument using the distinctness of the quantities $\operatorname{ord}(p - j)A_j$ shows that

(**) $$\operatorname{ord} B_1(x) = \inf\left(1, \inf_{1 \leqslant i \leqslant p-1} \operatorname{ord} A_{p-i}\right);$$

in particular,

$$(*) \qquad \operatorname{ord} B_1(x) \leqslant 1.$$

So now (α) follows ($*$) and the nonstrict part of (γ).

By the strict inequality (γ), the strict inequality (β) is implied by the nonstrict inequality

$$(\delta_i) \qquad \operatorname{ord} B_i(x) \geqslant i \operatorname{ord} B_1(x) - (i-1)\left(1 + \frac{1}{p-1}\right) \qquad (2 \leqslant i \leqslant p).$$

Certainly, (δ_p) is implied by ($*$) since $B_p = 1$.

For $2 \leqslant i \leqslant p-1$ we use

$$\operatorname{ord} B_i(x) \geqslant \inf\left(1, \inf_{i \leqslant s \leqslant p-1} \operatorname{ord} A_{p-s}\right),$$

and so (δ_i) is implied by the pair of inequalities

$$(\eta_i) \qquad 1 \geqslant i \operatorname{ord} B_1(x) - (i-1)\left(1 + \frac{1}{p-1}\right),$$

$$(\eta_{i,s}) \quad \operatorname{ord} A_{p-s} \geqslant i \operatorname{ord} B_1(x) - (i-1)\left(1 + \frac{1}{p-1}\right) \qquad (2 \leqslant i \leqslant s \leqslant p-1).$$

Now (η_i) is implied by ($*$) while $(\eta_{i,s})$ is reduced by the estimate

$$\operatorname{ord} B_1(x) \leqslant \operatorname{ord} A_{p-s}$$

to the sufficient condition

$$\operatorname{ord} B_1(x) \geqslant i \operatorname{ord} B_1(x) - (i-1)\left(1 + \frac{1}{p-1}\right),$$

and this is implied by ($*$). This completes the proof of (ii).

(iii) $\overline{M}'/\overline{M}$ *is inseparable.* We again have ord $A_p = 0$, ord $A_i \geqslant 0$ $(i \leqslant i \leqslant p-1)$.

The proof is a step-by-step repetition of case (ii), except for the verification of ($**$) which we now carry out.

The formula for B_1 shows that

$$B_1(x) = p\xi^{p-1} + \sum_{i=1}^{p-1} iA_{p-i}(t)\xi^{i-1} + q,$$

where ord $q \geqslant \operatorname{ord}(x-t) - c > 1$.

Thus, if (**) fails to hold, then

$$\operatorname{ord}\left(p\xi^{p-1} + \sum_{i=1}^{p-1} iA_{p-i}(t)\xi^{i-1}\right) > \lambda$$

where λ is the right side of (**). It follows that in the valuation ring of M'

$$pz^{p-1} + \sum_{i=1}^{p-1} iA_{p-i}(x)z^{i-1} \equiv 0 \mod p^{\lambda}\mathcal{O}_{M'}.$$

There exists $\alpha \in M$ such that ord $\alpha = \lambda$, and, dividing by α and reducing modulo the prime ideal of $\mathcal{O}_{M'}$, we obtain a nontrivial polynomial relation over $\overline{M}$ of degree $< p$ satisfied by $\bar{z}$, contrary to hypothesis.

THEOREM 2. *Let M be a subfield of W_1 with discrete valuation. Let L be an extension of degree n. Then $L \subset W_{|n\pi|}$.*

Proof. This follows from the reduction step of the proof of Theorem 1.

3. Transfer to the origin. Let k be a finite extension of $\mathbb{Q}_p$ and let z be algebraic of degree n over $k(x)$. Let V denote the Vandermonde matrix and with $\delta = Xd/dX$ define $G \in \mathcal{M}_n(k(x))$ by

$$(*) \qquad \delta V = GV.$$

Let $r_p = 1$ in the notation of the introduction. Thus, G has no singularity in the punctured disc $D(0, 1^-) - \{0\}$. We view k as a subfield of a field Ω as in §1, but we now insist that there exists $t \in \Omega$ with image $\bar{t}$ in the residue class field with $\bar{t}$ transcendental over the residue class field $\bar{k}$ of k. Then $k(X) \in W_1$. Let E be the completion of $k(x)$ under the norm of W_1. We note that imbeddings of z into the algebraic closure of E have degrees whose sum is n but which are otherwise unknown to us. Then by §2 we know that the solutions of (*) at t lie in W_R with $R = |\pi p^{\log n/\log p}|$.

Hence, $U_{G,t}$, the solution matrix at t of (*), converges in $D(t, R^-)$. Since (*) has a regular singular point at the origin, there is a solution matrix $Y \cdot x^A$ for some constant matrix A with rational eigenvalues and $Y \in \mathrm{Gl}(n, k((x)))$. In the present situation A can be diagonalised, and also we may assume $Y \in \mathcal{M}_n(k[[X]])$. Our object is to prove the following theorem.

THEOREM 3. *Y is analytic in $D(0, (R^n)^-)$.*

The result remains valid without the hypothesis that the differential equation has a solution matrix whose coefficients are algebraic over $k(x)$. We shall assume only that

(1) the origin is a regular singular point, and there is no other singular point in $D(0, 1^-)$;

(2) the monodromy about the origin is finite; and
(3) $R \leqslant |\pi|$.

Stronger results for $1 \geqslant R > |\pi|$ may be found in [Chr]; see also [ChrDw1, 2].

The proof requires a number of reduction steps. We set $G_{[H]} = \delta H \cdot H^{-1} + HGH^{-1}$.

Step 1. We first choose $H \in \mathrm{Gl}(n, k(x))$ such that

$$G_{[H]} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & 1 \\ c_n & \cdots & \cdots & \cdots & c_1 \end{bmatrix}$$

so that $\delta - G_{[H]}$ has the form of a scalar equation. By Fuchs $G_{[H]}$ is analytic at $x = 0$.

By the theorem of "Dwork-Frobenius" Proposition 7.1, [ChrDw1],

$$|c_j| \leqslant \frac{1}{R^j};$$

in fact, this can be sharpened [ChrDw2] to

$$|c_j| \leqslant \sup\left(1, \frac{|\pi|}{R}\right)^j = (|\pi|/R)^j.$$

Step 2. Extending the field of constants (if necessary), we choose $\beta \in k$ such that $\sup_j |c_j/\beta^j| = 1$, put

$$H_1 = \begin{bmatrix} 1 & & & \\ & \beta & & \\ & & \ddots & \\ & & & \beta^{n-1} \end{bmatrix}^{-1},$$

and conclude that

$$G_{[H_1 H]} = \begin{bmatrix} 0 & \beta & 0 & \cdots & 0 \\ 0 & 0 & \beta & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \beta \\ \dfrac{c_n}{\beta^{n-1}} & \cdots & \cdots & \cdots & c_1 \end{bmatrix},$$

which shows that

$$|G_{[H_1 H]}| \leqslant \sup(1, |\beta|) \leqslant |\pi|/R.$$

Step 3 ([ChrDw1, Prop. 2.4]). Again extending the field of constants, there exists $H_2 \in \mathrm{Gl}(n, k(x))$, $|H_2| = 1 = |H_2^{-1}|$, such that $G_{[H_2H_1H]}$ is analytic in $D(0, 1^-)$.

Step 4 ([ChrDw1, Prop. 2.3]). There exists $H_3 \in \mathrm{Gl}\left(n, k\left[x, \frac{1}{x}\right]\right)$, $|H_3| = 1 = |H_3^{-1}|$, such that $T = G_{[H_3H_2H_1H]}$ has the properties that

(i) T is analytic in $D(0, 1^-)$;

(ii) $T(0)$ is upper-diagonal with rational eigenvalues in $[0, 1)$, and $T(0)$ is diagonalisable; and

(iii) $|T| \leqslant |\pi|/R$.

Step 5. Again extending the field of constants (if necessary), we choose $\beta \in k$ such that $|\beta| = R/|\pi|$. Let

$$\Delta = \begin{bmatrix} 1 & & & \\ & \beta & & \\ & & \ddots & \\ & & & \beta^{n-1} \end{bmatrix}^{-1}$$

and put $S = T_{[\Delta]}$. So now

(i) S is analytic in $D(0, 1^-)$;

(ii) $S(0)$ is upper-triangular, has eigenvalues $\{\lambda_1, \ldots, \lambda_n\}$ in $\mathbb{Q} \cap [0, 1)$, and has off-diagonal terms bounded by unity;

(iii) $S(0)$ can be diagonalised; and

(iv) $|S| \leqslant (|\pi|/R)^n$.

Step 6. Let $\lambda\ (= \lambda_j)$ be one of the eigenvalues of $S(0)$. Let $\theta_m = (m + \lambda)I_n - S(0)$. The off-diagonal terms of θ_m are bounded by unity, and the diagonal terms are of the form $m + \lambda - \lambda_i$ which is bounded by $\sup(1, |\lambda - \lambda_i|)$. Thus, the adjoint of θ_m is bounded by $\prod_{i=1}^n \sup(1, |\lambda - \lambda_i|) = \prod_{i \in J'} |\lambda - \lambda_i|$, where J' is the set of all i such that $\lambda - \lambda_i \notin \mathbb{Z}_p$.

The determinant of θ_m is $\prod_{i=1}^n (m + \lambda - \lambda_i)$, and so

$$|\theta_m^{-1}| \leqslant 1/|P(m)|$$

where

$$P(s) = \prod_{i \in J} (s + \lambda - \lambda_i)$$

and J is the set of all i such that $\lambda_i - \lambda \in \mathbb{Z}_p$.

The equation $\delta - S$ has a solution matrix $\tilde{Y} \cdot x^{S(0)}$, where $\tilde{Y} \in \mathrm{Gl}(n, k[[x]])$, $\tilde{Y}(0) = I_n$. By hypothesis there exists $A \in \mathrm{Gl}(n, k)$ such that $A^{-1}S(0)A = \Lambda$, a diagonal matrix with entries $\lambda_1, \ldots, \lambda_n$. We choose $|A| \leqslant 1$ but make no effort to estimate $|A^{-1}|$. Then $\tilde{Y}Ax^{\Lambda}$ is also a solution matrix of $\delta - S$. Let $Z = \tilde{Y}A$ and let $\vec{z}$ be the jth column of Z. Thus, $\vec{z} \in (k[[x]])^n$, $|\vec{z}(0)| \leqslant 1$, and $\vec{z}x^{\lambda}$ is a solution of $\delta - S$; that is,

$$\delta\vec{z} + \lambda\vec{z} = S\vec{z}.$$

Writing $\vec{z} = \sum_{m=0}^{\infty} \vec{z}_m x^m$, $\vec{z}_m \in k^m$,

$$S = S(0) + S_1 x + \cdots, S_m \in \mathcal{M}_n(k),$$

we have the recursion formula

$$\theta_m \vec{z}_m = S_1 \vec{z}_{m-1} + \cdots + S_m \vec{z}_0 .$$

The estimate for $|S|$ implies $|S_i| \leqslant (|\pi|/R)^n$ for $i \geqslant 0$. Hence, by induction

$$|\vec{z}_m| \leqslant (|\pi|/R)^{nm} \Big/ \prod_{s=1}^{m} |P(s)|.$$

Let d be an upper bound for the denominator of $\lambda - \lambda_i$. Let b be an upper bound for $|1 + \lambda - \lambda_i|_\infty$. Since the λ_i all lie in $\mathbb{Q}$,

$$\prod_{s=1}^{m} |\lambda - \lambda_i + s| \geqslant |\pi|^m \frac{1}{d(m+b)}.$$

Thus,

$$\prod_{s=1}^{m} |P(s)| \geqslant |\pi|^{nm}/(d(m+b))^n,$$

and so

$$|\vec{z}_m| \leqslant \frac{1}{R^{nm}} (d(m+b))^n.$$

This estimate depends upon $\lambda_1, \ldots, \lambda_n$ but shows that $\vec{z}$ converges in $D(0, (R^n)^-)$. Hence, the same holds for Z and for $\tilde{Y}$.

So now the Vandermonde matrix at the origin may be written

$$V = H \tilde{Y} x^{S(0)}$$

for some $H \in \mathrm{Gl}(n, k(x))$. Putting $Y = H\tilde{Y}$, we conclude that Y is meromorphic everywhere in $D(0, (R^n)^-)$. Hence, ([ChrDw1, Prop. 2.9]) Y is analytic in the punctured disc as asserted.

4. Calculation of a_0. We use the notation of the introduction. Let $f(X, Y) = A_0 Y^n + \cdots + A_n \in \mathbb{Z}[X, Y]$. We may transform this equation by the substitution $Y = X^{-\tau} Z$ where $\tau \geqslant 0$ is the order of zero of A_0 at $X = 0$. This eliminates the zero of A_0 at $X = 0$ and does not change H, the bound for the coefficients of f. We now

have

$$Z = X^{\tau} y(X) = \alpha_0 X^{\tau} + \alpha_1 X^{\tau+1} + \cdots .$$

We have chosen $a \in \mathbb{Z}$ such that, for all p and for each imbedding in $\mathbb{C}_p$ of $\mathbb{Q}(\alpha_0, \alpha_1, \ldots)$, $y(aX)$ converges in $\mathbb{C}_p$ for $|X| < 1$. Furthermore, we have chosen a so that each zero γ of $D(X)$ satisfies $|\gamma/a|_p \geqslant 1$ for each imbedding of the zeros of D in $\mathbb{C}_p$.

We will choose $b_0 \in \mathbb{Z}$ such that $b_0 Z(aX)$ is bounded by unity on $D(0, 1^-)$ for each imbedding in $\mathbb{C}_p$. For the equation satisfied by Z we have

$$A_0(aX) = \lambda \prod_{i=1}^{l} (1 + \beta_i X)$$

where $\lambda \in \mathbb{Z}$ and $\beta_1, \ldots, \beta_l$ are algebraic integers. For $X \in D(0, 1^-)$ in $\mathbb{C}_p$ we know that $|A_j(aX)| \leqslant 1$ while $|A_0(aX)| = |\lambda|_p$. It follows that

$$|Z(aX)| \leqslant 1/|\lambda|_p .$$

This shows that $\lambda Z(aX)$ is bounded by 1 on $D(0, 1^-)$ for each imbedding into $\mathbb{C}_p$. Thus, we may take $a_0 = \lambda a^{\tau}$. Hence, if in the original equation, the coefficient of the leading term is $A_0(X) = A_{0,\tau} X^{\tau} + A_{0,\tau+1} X^{\tau+1} + \cdots$, $A_{0,\tau} \neq 0$, we have $a_0 \leqslant A_{0,\tau} a^{\tau} \leqslant H a^m$, where m is the degree of f in X.

5. Algebraic base field. Suppose now that f is given in $\mathcal{O}_k[X, Y]$, where $\mathcal{O}_k$ is the ring of integers of k, an algebraic number field of degree d over $\mathbb{Q}$. We could reduce to the preceding case by considering the polynomial $\mathrm{Norm}_{k/\mathbb{Q}} f(X, Y)$.

We adopt a more efficient procedure. Let $D \in \mathcal{O}_k[X]$ be the discriminant of f and let μ be the order of zero of D at $X = 0$; so again

$$D(X) = D_\mu X^{\mu} + D_{\mu+1} X^{\mu+1} + \cdots \qquad D_\mu \neq 0 .$$

The main point in the calculation of the Eisenstein constant $a \in \mathbb{Z}$ is to determine

$$\beta = \prod_p \beta_p , \qquad \beta_p = \inf_{\mathfrak{p}|p} |D_\mu|_{\mathfrak{p}} .$$

Here, the product is over all the rational primes p while $\mathfrak{p}|p$ refers to the various imbeddings of $\mathbb{Q}(D_\mu)$ in $\mathbb{C}_p$ (normalised so that $|p|_{\mathfrak{p}} = 1/p$).

Thus, in terms of the standard valuation of $\mathbb{Q}_p$

$$|D_\mu|_{\mathfrak{p}} = |\mathrm{Norm}_{k_{\mathfrak{p}}/\mathbb{Q}_p} D_\mu|_p^{1/d_{\mathfrak{p}}}$$

where $d_{\mathfrak{p}}$ is the local degree at $\mathfrak{p}$ of k over $\mathbb{Q}$.

Since we insist that $a \in \mathbb{Z}$, it is best to adjust β_p to be an integral power of $1/p$. This is automatic if $p \nmid \mathfrak{D}_k$, the discriminant of k, and so we set

$$\beta_p' = \begin{cases} \beta_p & \text{if } p \nmid \mathfrak{D}_k \\ \dfrac{1}{p}\beta_p & \text{if } p \mid \mathfrak{D}_k . \end{cases}$$

Having done this, we know that we need no extra factor if $n < p$ while for $n \geqslant p$ we need an additional factor

$$c(n, p) = (|p|_p^{1/(p-1)+\log n/\log p})^n \cdot |p|_p ,$$

the last $|p|_p$ again to adjust for nonintegrality of exponents. We thus find

$$a \leqslant \frac{1}{\beta}\mu_n \lambda_n^n |\mathfrak{D}_k|_\infty .$$

We use a rough bound for β:

$$\beta \geqslant \prod_p |\mathrm{Norm}_{k/\mathbb{Q}} D_\mu|_p = \frac{1}{|\mathrm{Norm}_{k/\mathbb{Q}} D_\mu|_\infty} ,$$

and so

$$\frac{1}{\beta} \leqslant |\mathrm{Norm}_{k/\mathbb{Q}} D_\mu|_\infty \leqslant \prod_{v|\infty} |D_\mu|_v$$

where $|\ |$ is the normalised valuation in $\mathbb{R}$ and $\mathbb{C}$. (So the latter is the square of the standard one in $\mathbb{C}$.)

Using the standard valuation v' in $\mathbb{C}$, we have

$$|D_\mu|_{v'} \leqslant (2n-1)! n^n |f|_{v'}^{2n-1} .$$

Hence, for the normalised valuation we obtain

$$|D_\mu|_v \leqslant |(2n-1)! n^n|_v |f|_v^{2n-1} ,$$

and so

$$\frac{1}{\beta} \leqslant \left(\prod_{v|\infty} |f|_v\right)^{2n-1} ((2n-1)! n^n)^d \leqslant H_k(f)^{2n-1} (n^n (2n-1)!)^d$$

where $H_k(f)$ is the field height of f ($= H(f)^d$, where $H(f)$ is the absolute height).

Thus,

$$a \leqslant \mathfrak{D}_k H_k(f)^{2n-1} \mu_n \lambda_n^n ((2n-1)! n^n)^d \qquad \text{for} \quad n \geqslant 2.$$

6. Newton's lemma. In this section we correct an error in §4 of [DwRo] but use the method to provide yet another proof of our Lemma 1.1. It was stated in that article that, if $f \in \mathbb{Z}[X, Y]$,

$$f(x, y) = 0, \qquad y = a_0 + a_1 x + \cdots \in \mathbb{Q}[[x]],$$

if

$$f_Y(x, y) \equiv b_0 x^s \mod x^{s+1}, \qquad b_0 \neq 0,$$

and if $a_0, a_1, \ldots, a_{2s} \in \mathbb{Z}$, then $b_0 \in \mathbb{Z}$ and

(i) for each $j \in \mathbb{N}$ there exists $m(j) \in \mathbb{N}$ such that $a_j b_0^{m(j)} \in \mathbb{Z}$, and

(ii) $a_{s+j} b_0^j \in \mathbb{Z}$.

The first statement is correct, the second is false. A counterexample is given by

$$f = Y^p - 1 - X, \qquad Y = \sum \binom{1/p}{j} X^j.$$

Here,

$$f_Y(x, y) = p y^{p-1} \equiv p \mod x.$$

So $s = 0$, $b_0 = p$, but $\operatorname{ord}_p a_p = -p - 1 < -p$.

PROPOSITION. *Let $\dot{W}_r$ be the set of elements of W_r which are bounded by unity on $D(t, r^-)$. Let $f(X, Y) \in \dot{W}_r[Y]$, $f(t, \xi) = 0$, $f_Y(t, \xi) = b \neq 0$ for some $\xi \in \Omega$, $|\xi| \leqslant 1$. Then there exists a unique germ*

$$y = \xi + a_1(x - t) + a_2(x - t)^2 + \cdots$$

of an analytic function at t such that $f(x, y) = 0$ and $y \in W_{r|b|^2}$.

Proof. Let $R < |b|^2$ and let U be the set of all $u \in W_{rR}$ such that $\|u - \xi\|_{rR} \leqslant R/|b|$. Certainly, U is complete under the topology induced by that of W_{rR}. The proof is completed by standard arguments which show that

$$\phi: u \mapsto u - \frac{f(x, u)}{f_Y(x, u)}$$

is a contractive map on U. □

Note. The method gives no improvement on Lemma 1.4. It does eliminate the factor $|\pi|$ but replaces the different by its square.

The lemma is useful in the case of tame ramification as follows.

COROLLARY. *Let M' be a tamely ramified extension of a complete subfield M of W_r. Then $M' \subset W_r$.*

Proof. We may reduce to two cases.

Case I. M'/M is unramified. (That is, $\overline{M}'/\overline{M}$ is separable of the same degree as M'/M.) Then $\overline{M}' = \overline{M}(\bar{z})$. Let z be a lifting of $\bar{z}$ to M'. Then $M' = M(z)$. Let $f(X, Y)$ be the irreducible monic polynomial for z over M. Then by separability $\bar{f}_Y(\bar{x}, \bar{z}) \neq 0$, and hence $f_Y(x, z)$ is a unit in M'; that is,

$$1 = |f_Y(x, z)|_{M'} = |f_Y(t, z(t))|.$$

The assertion follows from the proposition.

Case II. M'/M is purely ramified of degree n prime to p. If M had a discrete valuation, we could use the Eisenstein polynomial, but in the nondiscrete case the factor group $|M'|/|M|$ of the valuation groups need not be cyclic. Thus, in the nondiscrete case we use the fact that M' is a sequence of radical extensions of M. Thus, we reduce to the case in which $M' = M(z)$, the irreducible monic polynomial for z over M being $Y^n - A_0 = f(X, Y)$. If z is not a unit, then, adjoining $\alpha \in \Omega$ to M, $|\alpha| = |z|$, we reduce to the case in which z is a unit. So now

$$|f_Y(x, z)| = nz^{n-1}$$

is a unit of M' since $(n, p) = 1$. Thus, finally, $|f_Y(t, z(t))| = 1$; so again the assertion follows from the proposition. □

7. Final remarks. We give a more intrinsic formulation. Let k be an algebraic number field, $f \in k[X, Y]$, $n = \deg_Y f$. Let $\mathcal{O}$ be the ring of integers of K, the algebraic closure of k. Let $z = \sum \alpha_j X^j \in K[[X]]$ be a solution of $f(X, z) = 0$. Note that λ_n as defined in the introduction lies in K. Let $R(f, f_Y) = X^l(D_\mu + D_{\mu-1}X + \cdots + D_0 X^\mu)$. Let $\mathfrak{U}$ be the finitely generated $\mathcal{O}$-module

$$\mathfrak{U} = \frac{1}{(\lambda_n)^n} \sum_{i=0}^{\mu-1} \left(\frac{D_j}{D_\mu}\right)^{1/\mu - i} \mathcal{O}.$$

Then there exists $a \in K$ such that $a\alpha_j \in \mathfrak{U}^j$ for all j.

APPENDIX

Let $\mathcal{F}$ be a field with derivative δ. If $\mathcal{F}'$ is a separable extension of $\mathcal{F}$ of finite degree, then δ has a unique extension δ' to $\mathcal{F}'$. Let $\mathcal{F}'$ be the splitting field over $\mathcal{F}$

of $g \in \mathscr{F}[Y]$, a polynomial without multiple roots. Let $z_1, \ldots, z_n$ be the roots of g and let

$$V = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ z_1 & z_2 & \cdots & z_n \\ \cdot & \cdot & \cdots & \cdot \\ z_1^{n-1} & z_2^{n-1} & \cdots & z_n^{n-1} \end{bmatrix}$$

be the corresponding Vandermonde matrix.

PROPOSITION (classical).

$$\delta' V \cdot V^{-1} \in \mathscr{M}_n(\mathscr{F}).$$

Proof. By uniqueness of the extension, $\delta' \circ \sigma = \sigma \circ \delta'$ for all $\sigma \in \mathrm{Gal}(\mathscr{F}'/\mathscr{F})$. Of course, $\sigma V = VA_\sigma$, where A_σ is a permutation matrix. Since $\delta A_\sigma = 0$, $\sigma(\delta' V \cdot V^{-1}) = (\delta' \sigma V) \cdot (\sigma V)^{-1} = \delta(VA_\sigma) \cdot (VA_\sigma)^{-1} = \delta V \cdot V^{-1}$, which completes the proof.

REFERENCES

[Ar] EMIL ARTIN, *Algebraic Numbers and Algebraic Functions*, Nelson, London, 1968.

[Chr] G. CHRISTOL, *Un théorème de transfert pour les disques singuliers réguliers*, Astérisque **119–120** (1984), 151–168.

[ChrDw1] G. CHRISTOL AND B. DWORK, *Effective p-adic bounds at regular singular points*, Duke Math. J. **62** (1991), 689–720.

[ChrDw2] ———, *Differential Modules of Bounded Spectral Norm*, Contemp. Math., to appear.

[DwRo] B. DWORK AND P. ROBBA, *On natural radii of p-adic convergence*, Trans. Amer. Math. Soc. **256** (1979), 199–213.

[Die] P. DIENES, *The Taylor Series*, Dover, New York, 1957.

[Eis] G. EISENSTEIN, *Über eine allgemeine Eigenschaft der Reihen-Entwicklungen aller algebraischen Funktionen*, Bericht Königl. Preuß. Akad. Wiss. Berlin (1852), 411–443; *Mathmatische Werke, Band II*, Chelsea, New York, 1975, 765–767.

[Epp] HELMUT P. EPP, *Eliminating wild ramification*, Invent. Math. **19** (1973), 235–249.

[RS] J. ROSSER AND L. SCHOENFELD, *Sharper bounds for the Chebyshev functions $\theta(X)$ and $\varphi(X)$*, Math. Comp. **29** (1975), 243–269.

[Sch] O.F.G. SCHILLING, *The Theory of Valuations*, Math. Surveys **4**, Amer. Math. Soc., New York, 1950.

[Schm] WOLFGANG M. SCHMIDT, *Eisenstein's theorem on power series expansions of algebraic functions*, Acta Arith. **56** (1990), 161–179.

[Sh] H. SHAPIRO, *Introduction to the Theory of Numbers*, Wiley, New York, 1983.

DWORK: DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NEW JERSEY 08540; bmdwork@pucc.princeton.edu

VAN DER POORTEN: SCHOOL OF MATHEMATICS, PHYSICS, COMPUTING, AND ELECTRONICS, MACQUARIE UNIVERSITY NSW 2109, AUSTRALIA; alf@mqcomp.mqcs.mq.oz.au