J. Aust. Math. Soc. **94** (2013), 158–180
doi:10.1017/S144678871300013X

REMARKS ON EISENSTEIN

YURI BILU[✉] and ALEXANDER BORICHEV

(Received 13 December 2011; accepted 3 December 2012; first published online 14 August 2013)

Communicated by I. Shparlinski

Dedicated to the memory of Alf van der Poorten

Abstract

We obtain a fully explicit quantitative version of the Eisenstein theorem on algebraic power series which is more suitable for certain applications than the existing version due to Dwork, Robba, Schmidt and van der Poorten. We also treat ramified series and Laurent series, and we demonstrate some applications; for instance, we estimate the discriminant of the number field generated by the coefficients.

1. Introduction

Let $f(z) = a_0 + a_1 z + a_2 z^2 + \cdots \in \bar{\mathbb{Q}}[[z]]$ be an algebraic power series. 'Algebraic' means here that f is algebraic over the field of rational functions $\bar{\mathbb{Q}}(z)$. It is well known (and easy to see) that the coefficients of an algebraic power series belong to a finite extension of $\mathbb{Q}$. The classical theorem attributed to Eisenstein asserts that there exists a nonzero rational integer T such that $T^{k+1}a_k$ is an algebraic integer for all k.

Since $f(z)$ is algebraic, there exists a nonzero polynomial $P(z, w) \in \bar{\mathbb{Q}}[z, w]$ such that $P(z, f(z)) = 0$. Eisenstein himself made his observation in [10] assuming the nonvanishing condition $P'_w(0, 0) \neq 0$ (the 'implicit function theorem' condition). In this case the proof is simpler and one can have a good estimate for the 'Eisenstein constant' T. The first proof in the general case was, probably, due to Heine [12, pages 50–53], who observed that for sufficiently large N the 'tail series' $\sum_{k=N}^{\infty} a_k z^{N-k}$ satisfies a polynomial equation with nonvanishing w-derivative at the origin.

Assume that the coefficients of the series $f(z)$ belong to a number field K. Denote by M_K the set of absolute values of K (normalized to extend the standard absolute values of $\mathbb{Q}$). The Eisenstein theorem is essentially equivalent to the following statement: for every $v \in M_K$ the v-adic norms $|a_k|_v$ grow at most exponentially in k, and for all but finitely many v we have $|a_k|_v \leq 1$ for all k. (Strictly speaking, the classical

Yuri Bilu was supported by the ANR project HAMOT, and by the Swiss National Foundation *Ambizione* fund PZ00P2_121962.

Eisenstein theorem refers only to finite absolute values, but it is natural to include infinite absolute values as well.)

It will be convenient to use the notion of M_K-divisor. By an *M_K-divisor* we mean associating to every $v \in M_K$ a positive real number A_v with the following property: for all but finitely many v we have $A_v = 1$. Then Eisenstein theorem simply means that there exists an M_K-divisor such that $|a_k|_v \le A_v^{k+1}$ for every $v \in M_K$.

The Eisenstein theorem has many applications, most notably in Diophantine analysis [1–4, 6, 7, 11, 13, 14, 16, 19], to mention only some of them. For these applications one often needs a quantitative version of the theorem in terms of the polynomial $P(z, w)$ above. For instance, in the Diophantine analysis one often needs to construct explicitly rational functions on algebraic curves with prescribed poles and zeros, see [6, 18]. The Eisenstein theorem is an indispensable tool for such constructions, and to make them explicit one needs a quantitative version of the qualitative statement above. First such versions were given by Coates [6] and Hilliker–Straus [13], who used the 'tail series' trick described above.

Schmidt [17] suggested a much more efficient approach: to estimate the v-adic norms of the coefficients in terms of the v-adic convergence radius. Using the previous work of Dwork and Robba [8], Schmidt obtained optimal estimates when the underlying prime p_v satisfies $n < p_v \le \infty$, where $n = \deg_w P(z, w)$. Schmidt conjectured that the same was possible for $p_v \le n$ as well (his own estimates in this case were not optimal). This was confirmed by Dwork and van der Poorten [9].

The following theorem is a compilation of the results from [8, 9, 17], made in [3, Theorem 2.2]. We define the *height* of an M_K-divisor $\mathcal{A} = (A_v)_{v \in M_K}$ by

$$\mathrm{h}(\mathcal{A}) = d^{-1} \sum_{v \in M_K} d_v \log^+ A_v, \qquad \log^+ = \max\{\log, 0\},$$

where $d = [K : \mathbb{Q}]$ is the absolute degree of K and $d_v = [K_v : \mathbb{Q}_v]$ is the absolute local degree of v. An M_K-divisor $\mathcal{A} = (A_v)_{v \in M_K}$ will be called *effective* if $A_v \ge 1$ for all v. For an effective M_K-divisor, $\log^+$ in the definition of the height can be replaced by log.

Theorem 1.1 (Dwork, Robba, Schmidt, van der Poorten). *Let K be a number field and $P(z, w) \in K[z, w]$ an irreducible polynomial of degrees $\deg_z P = m$ and $\deg_w P = n$. Further, let $f(z) = \sum_{k=0}^{\infty} a_k z^k \in \bar{K}[[z]]$ be a power series satisfying $P(z, f(z)) = 0$. Then there exist M_K-divisors $\mathcal{A}' = (A'_v)_{v \in M_K}$ and $\mathcal{A} = (A_v)_{v \in M_K}$ such that*

$$|a_k|_v \le A'_v A_v^{m+k} \quad (k = 0, 1, 2, \ldots)$$

for any $v \in M_K$ anyhow extended to $\bar{K}$, and such that

$$\mathrm{h}(\mathcal{A}') \le \mathrm{h}_{\mathrm{p}}(P) + O(\log n), \qquad \mathrm{h}(\mathcal{A}) \le (2n - 1)\mathrm{h}_{\mathrm{p}}(P) + O(n \log(2mn)), \tag{1.1}$$

the constants implied by $O(\cdot)$ being absolute.

Here $\mathrm{h}_{\mathrm{p}}(P)$ is the usual projective height of the polynomial P, see Section 2.

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

As Dwork and van der Poorten explain in the introduction to their article [9], one cannot improve on the term $(2n-1)\mathrm{h}_{\mathrm{p}}(P)$. So, the bound for $\mathrm{h}(\mathcal{A})$ in (1.1) is the best possible. Still, there is one unsatisfactory point in Theorem 1.1: the term m in the estimate $|a_k|_v \le A'_v A_v^{m+k}$. This term originates from Schmidt's Lemma 2 in [17]. It is implicit in Schmidt's article and indicated in [3] that m can be replaced by $\mathrm{ord}_z p_n(z)$, where $p_n(z)$ is the leading coefficient of $P(z,w)$ viewed as a polynomial in w over $K[z]$. Still, one expects, and for certain applications one needs, a bound $|a_k|_v \le A'_v A_v^k$ with divisors $\mathcal{A}'$ and $\mathcal{A}$ satisfying (1.1) or similar.

The principal purpose of this article is obtaining such a bound. The price we have to pay here is a slightly weaker estimate for the height of $\mathcal{A}$, with $2n-1$ replaced by $3n-1$. The following theorem is proved in Section 6.

THEOREM 1.2. *Assume the set-up of Theorem 1.1. Then there exist effective M_K-divisors $\mathcal{A}' = (A'_v)_{v\in M_K}$ and $\mathcal{A} = (A_v)_{v\in M_K}$ such that*

$$|a_k|_v \le A'_v A_v^k \quad (k = 0, 1, 2, \ldots)$$

for any $v \in M_K$ anyhow extended to $\bar{K}$, and such that

$$\mathrm{h}(\mathcal{A}') \le \mathrm{h}_{\mathrm{p}}(P) + \log 3, \quad \mathrm{h}(\mathcal{A}) \le (3n-1)\mathrm{h}_{\mathrm{p}}(P) + 3n\log(mn) + 7n.$$

We also obtain more general results, on ramified series and Laurent series (they cannot be reduced to Theorem 1.2 by a simple variable change).

1.1. Plan of the article. In Section 2 we introduce some (mainly standard) terminology. In Section 3 we collect various auxiliary results to be used in the main body of the article.

Section 4 is the technical heart of the article. We obtain therein a required version of the already mentioned Schmidt's Lemma 2 from [17], and deduce a v-adic upper bound for the coefficients of the series. In Section 5 we extend the results of the previous section to general ramified Laurent series.

Theorem 1.2, as well as its ramified Laurent generalization, are deduced in Section 6 more or less straightforwardly from the results of Sections 4 and 5. Some immediate applications are given as well.

In Section 7 we obtain a slightly different type of the Eisenstein theorem, where the estimate involves the initial coefficient a_0. Finally, in Section 8 we give an explicit upper bound for the discriminant of the number field generated by the coefficients.

2. Notation and conventions

In this section we make general definitions and state some conventions assumed throughout the article.

Let P be a polynomial over some field. For any nonzero element α of the field, the polynomial αP will be called a *normalization* of P. A normalization will be called *moderate* if one of its coefficients is 1.

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

Let P be a polynomial over a field equipped with an absolute value $|\cdot|$. We denote by $|P|$ the maximal absolute value of the coefficients of P.

We denote by $\bar{K}$ the algebraic closure of the field K.

Let K be a number field of degree $d = [K : \mathbb{Q}]$. We denote by M_K the set of absolute values of K, normalized to extend the standard absolute values of $\mathbb{Q}$. That is, for $v \in M_K$ we have $|p|_v = p^{-1}$ if $v \mid p < \infty$, and $|2012|_v = 2012$ if $v \mid \infty$. With this convention the product formula reads

$$\prod_{v \in M_K} |\alpha|_v^{d_v} = 1 \quad (\alpha \in K^*),$$

where $d_v = [K_v : \mathbb{Q}_v]$ is the local degree of v.

Given a vector $\mathbf{a} = (a_1, \dots, a_m)$ with algebraic entries, we define its *projective height* and its *affine height* as

$$\mathrm{h_p}(\mathbf{a}) = d^{-1} \sum_{v \in M_K} d_v \log \max_{1 \le k \le m} |a_k|_v, \quad \mathrm{h_a}(\mathbf{a}) = d^{-1} \sum_{v \in M_K} d_v \log^+ \max_{1 \le k \le m} |a_k|_v,$$

where $\log^+ = \max\{\log, 0\}$ and K is a number field containing the entries of $\mathbf{a}$, the degrees d and d_v being as above. It is well known (and very easy to see) that both $\mathrm{h_p}(\mathbf{a})$ and $\mathrm{h_a}(\mathbf{a})$ depend only on the vector $\mathbf{a}$, but not on the particular choice of the field K.

Given a polynomial P with algebraic coefficients, we define its heights $\mathrm{h_p}(P)$ and $\mathrm{h_a}(P)$ as the corresponding heights of the vector of its nonzero coefficients. If the polynomial P has 1 as one of its coefficients (that is, P is *moderately normalized* in the terminology introduced above), then $\mathrm{h_p}(P) = \mathrm{h_a}(P)$.

Finally, in this article the letter e is used exclusively for ramification indices; it never denotes the constant 2.718 . . . .

3. Some estimates

In this section we collect some very simple estimates which will be used in the article.

3.1. Local estimates. In this subsection K is an algebraically closed field equipped with an absolute value $|\cdot|$. For a polynomial P over K we denote by $|P|$ the maximum of the absolute values of the coefficients of P.

Proposition 3.1.

(1) *Let $P(w_1, \dots, w_\ell)$ be a polynomial over K. Put $n_i = \deg_{w_i} P$. Then at any point $(w_1, \dots, w_\ell) \in K^\ell$*

$$|P(w_1, \dots, w_\ell)| \le A|P| \prod_{i=1}^{\ell} \max\{1, |w_i|\}^{n_i},$$

where $A = (n_1 + 1) \cdots (n_\ell + 1)$ in the Archimedean case, and $A = 1$ in the non-Archimedean case.

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

(2) *Let* $P(z_1, \dots, z_k, w_1, \dots, w_\ell)$ *be a polynomial over* K. *Put* $n_i = \deg_{w_i} P$. *Then at any point* $(z_1, \dots, z_k, w_1, \dots, w_\ell) \in K^{k+\ell}$ *such that* $|z_1|, \dots, |z_k| < 1$ *and* $|w_1|, \dots, |w_\ell| > 1$

$$|P(z_1, \dots, z_k, w_1, \dots, w_\ell)| \le \begin{cases} |P| \prod_{i=1}^{k} \frac{1}{1-|z_i|} \prod_{i=1}^{\ell} \frac{|w_i|^{n_i}}{1-|w_i|^{-1}} & \text{if } |\cdot| \text{ is Archimedean,} \\ |P| \prod_{i=1}^{\ell} |w_i|^{n_i} & \text{if } |\cdot| \text{ is non-Archimedean.} \end{cases}$$

Proof. Item (1) and the non-Archimedean case of item (2) are obvious. In the Archimedean case of item (2), denoting $m_i = \deg_{z_i} P$,

$$|P(z_1, \dots, z_k, w_1, \dots, w_\ell)| \le |P| \prod_{i=1}^{\ell} |w_i|^{n_i} \prod_{i=1}^{k} (1 + |z_i| + \dots + |z_i|^{m_i}) \times \prod_{i=1}^{\ell} (1 + |w_i|^{-1} + \dots + |w_i|^{-n_i}).$$

Replacing finite sums by infinite sums, the result follows. □

Proposition 3.2. *Let* α *be a nonzero root of* $P(z) = a_n z^n + \dots + a_0 \in K[z]$ *(with* $a_n \ne 0$*) and let* m *be the order of* 0 *as a root of* P. *Then*

$$\frac{|a_m|}{2|P|} \le |\alpha| \le \frac{2|P|}{|a_n|} \quad \text{if } |\cdot| \text{ is Archimedean,}$$

$$\frac{|a_m|}{|P|} \le |\alpha| \le \frac{|P|}{|a_n|} \quad \text{if } |\cdot| \text{ is non-Archimedean.}$$

Proof. For the upper estimates we may assume that $|\alpha| \ge 2$ in the Archimedean case and $|\alpha| > 1$ in the non-Archimedean case. Using item (2) of Proposition 3.1,

$$|\alpha|^n = \left| \frac{a_{n-1}}{a_n} \alpha^{n-1} + \dots + \frac{a_0}{a_n} \right| \le \begin{cases} \frac{|P|}{|a_n|} \frac{|\alpha|^{n-1}}{1-|\alpha|} \le \frac{2|P|}{|a_n|} |\alpha|^{n-1} & \text{if } |\cdot| \text{ is Archimedean,} \\ \frac{|P|}{|a_n|} |\alpha|^{n-1} & \text{if } |\cdot| \text{ is non-Archimedean,} \end{cases}$$

which proves the upper estimates. The lower estimates follow upon replacing α by α^{-1}. □

The following proposition will be used only in the case $k = \ell = 1$, but we prefer to state it in the general case for the sake of further applications.

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

Proposition 3.3.

(1) *Let $P(w_1, \dots, w_\ell)$ be a polynomial over K. Put $n_i = \deg_{w_i} P$. For a multi-index $\mathbf{j} = (j_1, \dots, j_\ell)$ denote by $D_\mathbf{j}$ the differential operator*

$$D_\mathbf{j} = \frac{1}{j_1! \cdots j_\ell!} \frac{\partial^{j_1+\cdots+j_\ell}}{\partial w_1^{j_1} \cdots \partial w_\ell^{j_\ell}}.$$

Then $|D_\mathbf{j} P| \le 2^{n_1+\cdots+n_\ell}|P|$ in the Archimedean case, and $\left|D_\mathbf{j} P\right| \le |P|$ in the non-Archimedean case.

(2) *Let $P(z_1, \dots, z_k, w_1, \dots, w_\ell)$ be a polynomial over K, and $\alpha_1, \dots, \alpha_\ell \in K$. Put $n_i = \deg_{w_i} P$. Then the polynomial*

$$Q(z_1, \dots, z_k, w_1, \dots, w_\ell) = P(z_1, \dots, z_k, w_1 + \alpha_1, \dots, w_\ell + \alpha_\ell)$$

satisfies

$$|Q| \le A|P| \prod_{i=1}^{\ell} \max\{1, |\alpha_i|\}^{n_i},$$

where $A = (n_1 + 1) \cdots (n_\ell + 1)2^{n_1+\cdots+n_\ell}$ in the Archimedean case, and $A = 1$ in the non-Archimedean case.

Proof. In item (1) each coefficient of the polynomial $D_\mathbf{j} P$ is equal to a coefficient of P multiplied by a product of binomial coefficients $\binom{\nu_1}{j_1} \cdots \binom{\nu_\ell}{j_\ell}$, where $\nu_i \le n_i$. The absolute value of this product does not exceed $2^{n_1+\cdots+n_\ell}$ in the Archimedean case, and 1 in the non-Archimedean case. This proves item (1).

In item (2) every coefficient of Q is of the form $D_\mathbf{j} P(0, \dots, 0, \alpha_1, \dots, \alpha_\ell)$. Hence item (2) is a consequence of item (1) of this proposition and item (1) of Proposition 3.1. □

3.2. Global estimates.

Proposition 3.4. *Let $P(z_1, \dots, z_k, w_1, \dots, w_\ell)$ be a polynomial with algebraic coefficients, and $\alpha_1, \dots, \alpha_\ell$ are algebraic numbers. Put $n_i = \deg_{w_i} P$. Then the polynomial*

$$Q(z_1, \dots, z_k, w_1, \dots, w_\ell) = P(z_1, \dots, z_k, w_1 + \alpha_1, \dots, w_\ell + \alpha_\ell)$$

satisfies

$$\mathrm{h_p}(Q) \le \mathrm{h_p}(P) + \sum_{i=1}^{\ell} (n_i \mathrm{h_a}(\alpha) + n_i \log 2 + \log(n_i + 1)).$$

Proof. The coefficients of P and the numbers $\alpha_1, \dots, \alpha_\ell$ belong to some number field K. Then the desired statement is an immediate consequence of item (2) of Proposition 3.3. □

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

Given a polynomial $P(z, w)$, we denote by $R_P(z)$ the w-resultant of P and P'_w, the w-derivative of P.

PROPOSITION 3.5. *Let $P(z, w)$ be a polynomial with algebraic coefficients of z-degree m and w-degree n. Then*

$$\mathrm{h_p}(R_P) \le (2n-1)\mathrm{h_p}(P) + (2n-1)\log((m+1)(n+1)\sqrt{n}).$$

For the proof see Schmidt [17, Lemma 4].

PROPOSITION 3.6. *Let $P(z)$ be a polynomial with algebraic coefficients of degree m.*

(1) *Let α be a root of P. Then $\mathrm{h_a}(\alpha) \le \mathrm{h_p}(P) + \log 2$.*
(2) *Let $\alpha_1, \dots, \alpha_m$ be the roots of P counted with multiplicities. Then*

$$\mathrm{h_a}(\alpha_1) + \cdots + \mathrm{h_a}(\alpha_m) \le \mathrm{h_p}(P) + \log(m+1).$$

PROOF. Item (1) is an immediate consequence of Proposition 3.2. Item (2) is a classical result of Mahler; see, for instance, [17, Lemma 3]. □

4. Local Eisenstein theorem: the regular case

In this section p is a prime number or $p = \infty$, and $\mathbb{C}_p$ is the completion of the algebraic closure of $\mathbb{Q}_p$; in particular, $\mathbb{C}_\infty = \mathbb{C}$. Since p is fixed, we may write $|\cdot|$ instead of $|\cdot|_p$.

Let ρ be a positive real number and let

$$f(z) = a_0 + a_1 z + a_2 z^2 + \cdots \in \mathbb{C}_p[[z]] \tag{4.1}$$

be a power series converging in the disk $|z| < \rho$ and satisfying the equation $P(z, f(z)) = 0$, where $P(z, w) \in \mathbb{C}_p[z, w]$ is a nonzero polynomial. The purpose of this section is to estimate the coefficients a_k in terms of the polynomial P. First of all let us estimate $f(z)$ in some disk contained in the disk of convergence. The principal novelty of our estimate, as compared with that of Schmidt [17, Lemma 2], is that it does not depend on the z-degree of $P(z, w)$.

Recall that we denote by $|P|$ the maximum of the absolute values of the coefficients of P.

PROPOSITION 4.1. *In the above set-up, assume that the polynomial $P(z, w)$ is not divisible by z, so that the polynomial $q(w) := P(0, w)$ is nonzero. Assume further that the polynomial $q(w)$ is monic:*

$$q(w) = w^{\deg q} + \textit{terms of lower degree}.$$

Put $n = \deg_w P$ and

$$\varrho = \begin{cases} \min\{\rho, (6|P|)^{-n}\} & \text{if } p = \infty, \\ \min\{\rho, |P|^{-n}\} & \text{if } p < \infty. \end{cases}$$

Then for $|z| < \varrho$ we have $|f(z)| \le 3|P|$ if $p = \infty$, and $|f(z)| \le |P|$ if $p < \infty$.

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

The non-Archimedean part of the proof requires a lemma, that may be viewed as a p-adic analogue of the 'Bolzano–Cauchy theorem' from elementary analysis. Recall that for $p < \infty$ the possible absolute values of nonzero elements of $\mathbb{C}_p$ are exactly the rational powers of p:

$$\{|z| : z \in \mathbb{C}_p^*\} = p^{\mathbb{Q}},$$

where $p^{\mathbb{Q}} = \{p^a : a \in \mathbb{Q}\}$.

LEMMA 4.2. *Assume that $p < \infty$, and let f be defined by the series (4.1) convergent in the disk $|z| < \rho$. Let $s_1, s_2 \in p^{\mathbb{Q}}$ be such that $s_1 < s_2$ and there exist z_1, z_2 in the disk with $|f(z_i)| = s_i$. Then for any $s \in [s_1, s_2] \cap p^{\mathbb{Q}}$ there exists z in the same disk such that $|f(z)| = s$.*

PROOF. Shifting the variable we may assume that $z_1 = 0$. Convergence of the series (4.1) implies that for any nonnegative $r < \rho$ we have $\lim_{k\to\infty} |a_k| r^k = 0$. Hence the quantity

$$\mathrm{M}(r) = \max\{|a_k| r^k : k = 0, 1, \ldots\}$$

is well defined for $r \in [0, \rho)$ and continuous[1] on this interval. Let us show that for $r \in [0, \rho) \cap p^{\mathbb{Q}}$,

$$\max\{|f(z)| : |z| \le r\} = \mathrm{M}(r). \tag{4.2}$$

Denote by ℓ the biggest k with $|a_k| r^k = \mathrm{M}(r)$, and by $f_\ell(z)$ the ℓth partial sum of the series (4.1):

$$f_\ell(z) = a_0 + a_1 z + \cdots + a_\ell z^\ell.$$

The '$\le$'-inequality in (4.2) is obvious, and to prove the opposite inequality, we must find z with $|z| = r$ for which $|f_\ell(z)| = \mathrm{M}(r)$. Putting $g(z) = \mathrm{M}(r)^{-1} f_\ell(rz)$, we must find z with $|z| = 1$ for which $|g(z)| = 1$. By the definition of $\mathrm{M}(r)$, the polynomial $g(z)$ has coefficients in the local ring of $\mathbb{C}_p$, and its reduction $\bar{g}(z)$ modulo the maximal ideal is a nonzero polynomial over the residue field of $\mathbb{C}_p$. We are left with the following task: find a nonzero element of the residue field which is not a root of $\bar{g}(z)$. And this is always possible, because the residue field is infinite. This proves (4.2).

Since $\mathrm{M}(r)$ is a continuous real function on the interval $[0, \rho)$, satisfying $\mathrm{M}(0) = s_1$ and $\mathrm{M}(|z_2|) \ge s_2$, for any $s \in [s_1, s_2]$ there exists $r \in [0, \rho)$ with $\mathrm{M}(r) = s$. If s is a rational power of p, then so is r, and (4.2) implies that $f(z) = s$ for some z in the disk. □

(We owe this elegant proof of Lemma 4.2 to Michel Matignon.)

PROOF OF PROPOSITION 4.1 To simplify the notation, put $A = |P|$. It might be worth noticing that $A \ge 1$ (because $P(z, w)$ has 1 as one of its coefficients) and that $\varrho \le 1$. Both inequalities will be repeatedly used in the proof.

The argument splits into two cases, $p = \infty$ and $p < \infty$, the proofs being similar, but not identical.

[1] Because for every $\rho' \in [0, \rho)$ there exists n such that $M(r) = \max\{|a_k| r^k : k = 0, 1, \ldots, n\}$ on the interval $[0, \rho']$.

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

Assume first that $p = \infty$. Then $|f(0)| \le 2A$ by Proposition 3.2, because $f(0)$ is a root of the monic polynomial $q(w)$. Now assume that there exists z' in the disk $|z| < \varrho$ such that $|f(z')| > 3A$. By continuity, $|f(z)|$ takes in this disk all values in the interval $[3A, |f(z')|]$. In particular, there exists z in the disk $|z| < \varrho$ such that $3A < |f(z)| \le 4A$. Writing

$$P(z, w) = q(w) + zQ(z, w) \tag{4.3}$$

and using item (2) of Proposition 3.1, we obtain for such z the estimates

$$|q(f(z))| \ge |f(z)|^{\deg q} - A\frac{|f(z)|^{\deg q-1}}{1 - |f(z)|^{-1}} \ge |f(z)|^{\deg q} - \frac{3}{2}A|f(z)|^{\deg q-1} > \frac{3}{2}A$$

and

$$|Q(z, f(z))| \le A\frac{1}{1 - |z|}\frac{|f(z)|^n}{1 - |f(z)|^{-1}} < 2A(4A)^n.$$

Hence

$$|P(z, f(z))| > \tfrac{3}{2}A - 2A(4A)^n(6A)^{-n} > 0,$$

a contradiction. This proves the statement for $p = \infty$.

In the case $p < \infty$, Proposition 3.2 gives $|f(0)| \le A$. If our statement is not true, then there exists z' with $|z'| < \varrho$ such that $|f(z')| > A$. Pick r such that $|z'| < r < \varrho$; notice that $r < A^{-n}$. Lemma 4.2 (with r instead of ρ) implies the existence of z with $|z| < r$ and $A < |f(z)| < (rA)^{-1/(n-1)}$. Since $|f(z)| > A \ge 1$,

$$|q(f(z)) - f(z)^{\deg q}| \le A|f(z)|^{\deg q-1} < |f(z)|^{\deg q},$$

which implies that

$$|q(f(z))| = |f(z)|^{\deg q} \ge |f(z)| > |rAf(z)^n| > |zQ(z, f(z))|,$$

whence $P(z, f(z)) \ne 0$, a contradiction. This completes the proof for $p < \infty$ as well. □

Corollary 4.3. *In the set-up of Proposition 4.1, the coefficients of the series (4.1) satisfy*

$$|a_k| \le \begin{cases} 3|P|\varrho^{-k} & \text{if } p = \infty, \\ |P|\varrho^{-k} & \text{if } p < \infty. \end{cases}$$

Proof. It suffices to show that for any positive $r < \rho$,

$$|a_k| \le r^{-k} \sup\{|f(z)| : |z| = r\}. \tag{4.4}$$

In the case $p = \infty$, this follows from

$$a_k = \frac{1}{2\pi i}\int_{|z|=r} f(z)z^{-k-1}\,dz.$$

In the case $p < \infty$, this follows from (4.2). □

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

To make all this work, we need a lower estimate for the convergence radius ρ in terms of the polynomial P. This can be found in the work of Dwork, Robba, Schmidt and van der Poorten [8, 9, 17]. Given a polynomial $F(z) \in \mathbb{C}_p(z)$, we denote by $\sigma(F)$ the smallest absolute value of a nonzero root of $F(z)$:

$$\sigma(F) = \min\{|\alpha| : F(\alpha) = 0, \alpha \neq 0\}.$$

Call a polynomial $P(z, w)$ *w-separable* if it is not divisible by a square of a polynomial of positive w-degree, and denote by $R_P(z)$ the w-resultant of $P(z, w)$ and $P'_w(z, w)$; the latter is a nonzero polynomial if $P(z, w)$ is w-separable.

THEOREM 4.4 (Dwork, Robba, Schmidt, van der Poorten). *Assume that P is w-separable. Then the series (4.1) converges for $|z| < \sigma(R_P)$ if $n < p \leq \infty$, and for $|z| < (np^{1/(p-1)})^{-1}\sigma(R_P)$ if $p \leq n$.*

PROOF. For the case $n < p \leq \infty$, see Schmidt [17, Lemma 1]. As indicated by Schmidt, the case $n < p < \infty$ is a direct consequence of a result of Dwork and Robba [8]. The case $p \leq n$ is due to Dwork and van der Poorten [9, Theorem 3], who confirmed a conjecture of Schmidt. □

Thus, assuming P to be w-separable, everywhere above one can take $\rho = c(p, n)^{-1}\sigma(R_P)$, where

$$c(p, n) = \begin{cases} 1 & \text{if } n < p \leq \infty, \\ np & \text{if } p \leq n. \end{cases} \tag{4.5}$$

Put

$$\Sigma = \begin{cases} \max\{\sigma(R_P)^{-1}, (6|P|)^n\} & \text{if } p = \infty, \\ \max\{c(p, n)\sigma(R_P)^{-1}, |P|^n\} & \text{if } p < \infty. \end{cases} \tag{4.6}$$

The following theorem is now immediate.

THEOREM 4.5 (Local Eisenstein theorem, regular case). *Let $f(z) \in \mathbb{C}_p[[z]]$ written as in (4.1) satisfy the polynomial equation $P(z, f(z)) = 0$, where the polynomial $P(z, w) \in \mathbb{C}_p[z, w]$ is not divisible by z and w-separable. We normalize P so the polynomial $P(0, w) \in \mathbb{C}_p[w]$ is monic. Then for $k = 0, 1, 2, \ldots$ we have $|a_k| \leq 3|P|\Sigma^k$ when $p = \infty$, and $|a_k| \leq |P|\Sigma^k$ when $p < \infty$.*

For applications it is convenient to replace $\sigma(R_P)$, which is defined in terms of the roots of R_P, by a quantity defined in terms of its coefficients. Let μ be the order of 0 as the root of $R_P(z)$ and γ its lowest nonzero coefficient, so that

$$R_P(z) = \gamma z^\mu + \text{higher powers of } z. \tag{4.7}$$

Proposition 3.2 implies that

$$\sigma(R_P)^{-1} \leq \begin{cases} 2|R_P/\gamma| & \text{if } p = \infty, \\ |R_P/\gamma| & \text{if } p < \infty. \end{cases}$$

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

We obtain the following statement.

COROLLARY 4.6. *Let $f(z) \in \mathbb{C}_p[[z]]$ written as in (4.1) satisfy the polynomial equation $P(z, f(z)) = 0$, where the polynomial $P(z, w) \in \mathbb{C}_p[z, w]$ is not divisible by z and w-separable. We normalize P so the polynomial $P(0, w) \in \mathbb{C}_p[w]$ is monic. Put*

$$\Xi = \begin{cases} \max\{2|R_P/\gamma|, (6|P|)^n\} & \text{if } p = \infty, \\ \max\{c(p,n)|R_P/\gamma|, |P|^n\} & \text{if } p < \infty. \end{cases}$$

Then for $k = 0, 1, 2, \ldots$ we have $|a_k| \le 3|P|\Xi^k$ when $p = \infty$, and $|a_k| \le |P|\Xi^k$ when $p < \infty$.

5. Local Eisenstein theorem: the general case

We now allow the series f to admit a finite pole at 0 and finite ramification,

$$f(z) = \sum_{k=\kappa}^{\infty} a_k z^{k/e} \in \mathbb{C}_p((z^{1/e})), \tag{5.1}$$

where e is a positive integer and κ is an integer which may be positive, negative or zero. At the moment we do not assume that κ is maximal and that e is minimal (that is, it may well happen that $a_\kappa = 0$ and/or that $f \in \mathbb{C}_p((z^{1/e'}))$ for some $e' < e$).

We need to introduce one technical notion. Let $P(z, w)$ be a nonzero polynomial over some field, and k an integer (which may be negative). Then there exists a unique integer N such that

$$P_k(z, w) := z^N P(z, z^k w)$$

is a polynomial not divisible by z. The polynomial P will be called *k-normalized* if the polynomial $P_k(0, w)$ is monic. This is a *moderate normalization*, as defined in Section 2. The normalization hypothesis of Theorem 4.5 means exactly that P is 0-normalized.

It might be worth remarking that the polynomial P_k has the same set of nonzero coefficients as P; in particular, $|P_k| = |P|$. Also, the w-resultant of P_k is equal to the w-resultant of P times a power of z. In particular, the quantity Σ defined in (4.6), as well as the quantity Σ_e defined in (5.2) below, are the same for P and P_k.

Now let f be as in the beginning of this section, $P(z, w) \in \mathbb{C}_p[z, w]$ a w-separable polynomial of w-degree n such that $P(z, f(z)) = 0$, and $R_P(z)$ the w-resultant of $P(z, w)$ and $P'_w(z, w)$. Put

$$\Sigma_e = \begin{cases} \max\{\sigma(R_P)^{-1}, (6|P|)^n\} & \text{if } p = \infty, \\ \max\{c(p,n)^e \sigma(R_P)^{-1}, |P|^n\} & \text{if } p < \infty, \end{cases} \tag{5.2}$$

where $\sigma(\cdot)$ is defined in the paragraph before Theorem 4.4. If $e = 1$ (no ramification) and P is κ-normalized, then we have the estimates $|a_k| \le 3|P|\Sigma_1^{k-\kappa}$ when $p = \infty$,

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

and $|a_k| \le |P|\Sigma_1^{k-\kappa}$ when $p < \infty$. This follows by applying Theorem 4.5 to the series $z^{-\kappa} f(z)$ and the polynomial $P_\kappa(z, w)$.

We believe that in the general case, after a suitable moderate normalization of P, the estimates $|a_k| \le 3|P|\Sigma_e^{(k-\kappa)/e}$ when $p = \infty$, and $|a_k| \le |P|\Sigma_e^{(k-\kappa)/e}$ when $p < \infty$ must hold. Unfortunately, we can prove only a slightly weaker result.

THEOREM 5.1 (Local Eisenstein theorem, general case). *Let $f(z)$ as in (5.1) satisfy the polynomial equation $P(z, f(z)) = 0$, where the polynomial $P(z, w) \in \mathbb{C}_p[z, w]$ is w-separable and $\lfloor \kappa/e \rfloor$-normalized. Then for $k \ge \kappa$ we have the estimates $|a_k| \le 3|P|\Sigma_e^{k/e-\lfloor \kappa/e \rfloor}$ when $p = \infty$, and $|a_k| \le |P|\Sigma_e^{k/e-\lfloor \kappa/e \rfloor}$ when $p < \infty$.*

Replacing $f(z)$ and $P(z, w)$ by $z^{-\lfloor \kappa/e \rfloor} f(z)$ and $P_{\lfloor \kappa/e \rfloor}(z, w)$, respectively (as indicated above, this does affect the quantity Σ_e), we may assume that $\lfloor \kappa/e \rfloor = 0$; in particular, $\kappa \ge 0$. Defining $a_k = 0$ for $0 \le k < \kappa$, we reduce the theorem to the special case $\kappa = 0$. Thus, we have to prove the following proposition.

PROPOSITION 5.2. *In the set-up of Theorem 5.1 assume that $\kappa = 0$. Then for $k \ge 0$ we have the estimates $|a_k| \le 3|P|\Sigma_e^{k/e}$ when $p = \infty$, and $|a_k| \le |P|\Sigma_e^{k/e}$ when $p < \infty$.*

PROOF. The proof is quite analogous to that of Theorem 4.5. Put $\tilde{f}(z) = f(z^e)$ and $\widetilde{P}(z, w) = P(z^e, w)$, so that $\widetilde{P}(z, \tilde{f}(z)) = 0$. We have $|\widetilde{P}| = |P|$ and $\sigma(R_{\widetilde{P}}) = \sigma(R_P)^{1/e}$. Theorem 4.4 implies now that $\tilde{f}(z)$ converges in the disk $|z| < \tilde{\rho} := c(p, n)^{-1}\sigma(R_P)^{1/e}$. Put

$$\tilde{\varrho} = \begin{cases} \min\{\tilde{\rho}, (6|P|)^{-n/e}\} & \text{if } p = \infty, \\ \min\{\tilde{\rho}, |P|^{-n/e}\} & \text{if } p < \infty. \end{cases}$$

The polynomial $q(w) := P(0, w)$ is monic by assumption, and, in the notation of (4.3),

$$\widetilde{P}(z, w) = q(w) + z^e Q(z^e, w).$$

Arguing exactly as in the proof of Proposition 4.1, we obtain that for $|z| < \tilde{\varrho}$ we have $|f(z)| \le 3|P|$ if $p = \infty$, and $|f(z)| \le |P|$ if $p < \infty$. Now Corollary 4.3 implies

$$|a_k| \le \begin{cases} 3|P|\tilde{\varrho}^{-k} & \text{if } p = \infty, \\ |P|\tilde{\varrho}^{-k} & \text{if } p < \infty. \end{cases}$$

Since $\tilde{\varrho}^{-1} = \Sigma_e^{1/e}$, this completes the proof. □

We also state an analogue of Corollary 4.6, with $\sigma(R_P)^{-1}$ replaced by $|R_P/\gamma|$.

COROLLARY 5.3. *Let $f(z)$ as in (5.1) satisfy the polynomial equation $P(z, f(z)) = 0$, where the polynomial $P(z, w) \in \mathbb{C}_p[z, w]$ is w-separable and $\lfloor \kappa/e \rfloor$-normalized. Put*

$$\Xi_e = \begin{cases} \max\{2|R_P/\gamma|, (6|P|)^n\} & \text{if } p = \infty, \\ \max\{c(p, n)^e|R_P/\gamma|, |P|^n\} & \text{if } p < \infty. \end{cases}$$

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

Then for $k \geq \kappa$ we have the estimate

$$|a_k| \leq \begin{cases} 3|P|\Xi_e^{k/e-\lfloor \kappa/e \rfloor} & \text{if } p = \infty, \\ |P|\Xi_e^{k/e-\lfloor \kappa/e \rfloor} & \text{if } p < \infty. \end{cases}$$

6. Global Eisenstein theorem

In this section K is a number field of degree $d = [K : \mathbb{Q}]$ and M_K is the set of its absolute values normalized as indicated in Section 2.

Recall that by an *M_K-divisor* we mean associating to every $v \in M_K$ a positive real number A_v with the following property: for all but finitely many v we have $A_v = 1$. The M_K-divisor is *effective* if $A_v \geq 1$ for all v. The *height* of an M_K-divisor $\mathcal{A} = (A_v)_{v \in M_K}$ is defined as

$$\mathrm{h}(\mathcal{A}) = d^{-1} \sum_{v \in M_K} d_v \log^+ A_v,$$

where $d_v = [K_v : \mathbb{Q}_v]$ is the absolute local degree of v. For an effective divisor, $\log^+$ can be replaced by log.

Theorem 6.1 (Global Eisenstein theorem, regular case). *Let $P(z, w) \in K[z, w]$ be a w-separable polynomial of degrees $\deg_z P = m$ and $\deg_w P = n$. Further, let $f(z) = \sum_{k=0}^{\infty} a_k z^k \in \bar{K}[[z]]$ be a power series satisfying $P(z, f(z)) = 0$. Then there exist effective M_K-divisors $\mathcal{A}' = (A'_v)_{v \in M_K}$ and $\mathcal{A} = (A_v)_{v \in M_K}$ such that*

$$|a_k|_v \leq A'_v A_v^k \quad (k = 0, 1, 2, \ldots)$$

for any $v \in M_K$ anyhow extended to $\bar{K}$, and such that

$$\mathrm{h}(\mathcal{A}') \leq \mathrm{h}_{\mathrm{p}}(P) + \log 3, \quad \mathrm{h}(\mathcal{A}) \leq (3n-1)\mathrm{h}_{\mathrm{p}}(P) + 3n \log(mn) + 7n. \tag{6.1}$$

Notice that this is (a slight generalization of) Theorem 1.2 from the introduction.

Remark 6.2. The w-separability assumption can be dropped for the price of slightly increasing the estimates (6.1). Indeed, the classical 'Gauss–Mahler–Gelfond' lemma (see, for instance, [5, Theorem 1.6.13]) implies that if f, g are polynomials in r variables $x_1, \ldots, x_r$ with algebraic coefficients, and $g \mid f$, then $\mathrm{h}_{\mathrm{p}}(g) \leq \mathrm{h}_{\mathrm{p}}(f) + n_1 + \cdots + n_r$, where $n_i = \deg_{x_i} f$. Hence, if the polynomial P is not w-separable, then we may replace it by its square free part, which is w-separable and whose height is at most $\mathrm{h}_{\mathrm{p}}(P) + m + n$.

Proof. We may assume that the polynomial P is not divisible by z and is normalized in such a way that the w-polynomial $P(0, w)$ is monic (0-normalized in the terminology of Section 5). For every $v \in M_K$ we define A'_v and A_v as Corollary 4.6 suggests:

$$A_v = \begin{cases} \max\{2|R_P/\gamma|_v, (6|P|_v)^n\} & \text{if } v \mid \infty, \\ \max\{c(p,n)|R_P/\gamma|_v, |P|_v^n\} & \text{if } v \mid p < \infty, \end{cases} \qquad A'_v = \begin{cases} 3|P|_v & \text{if } v \mid \infty, \\ |P|_v & \text{if } v \mid p < \infty, \end{cases}$$

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

where $R_P(z)$ is the w-resultant of $P(z, w)$ and $P'_w(z, w)$, written as in (4.7), and $c(p, n)$ is defined in (4.5). Since the polynomial P has a coefficient equal to 1, both divisors $\mathcal{A}'$ and $\mathcal{A}$ are effective. Theorem 4.5 implies that $|a_k|_v \le A'_v A_v^k$, whichever way v is extended to $\bar{K}$.

Clearly $\mathrm{h}(\mathcal{A}') \le \mathrm{h}_{\mathrm{p}}(P) + \log 3$. Now,

$$\log A_v \le \begin{cases} \log |R_P/\gamma|_v + n \log |P| + n \log 6 & \text{if } v \mid \infty, \\ \log |R_P/\gamma|_v + n \log |P| + \log c(p, n) & \text{if } v \mid p < \infty. \end{cases}$$

It follows that

$$\mathrm{h}(\mathcal{A}) \le \mathrm{h}_{\mathrm{p}}(R_P) + \log 2 + n\mathrm{h}_{\mathrm{p}}(P) + n \log 6 + \sum_{p<\infty} \log c(p, n). \tag{6.2}$$

For the latter sum,

$$\sum_{p<\infty} \log c(p, n) = \pi(n) \log n + \sum_{p \le n} \log p \le 2.3n,$$

where we use inequalities (3.6) and (3.32) from [15, pages 69–71]. Combining all this with Proposition 3.5, we obtain, after a little calculation, the estimate

$$\mathrm{h}(\mathcal{A}) \le (3n - 1)\mathrm{h}_{\mathrm{p}}(P) + 3n \log(mn) + 7n,$$

as required. □

Theorem 6.3 (Global Eisenstein theorem, general case). *Let*

$$f(z) = \sum_{k=\kappa}^{\infty} a_k z^{k/e} \in \bar{K}((z^{1/e}))$$

be a power series over K satisfying $P(z, f(z)) = 0$. Then there exist effective M_K-divisors $\mathcal{A}' = (A'_v)_{v \in M_K}$ and $\mathcal{A} = (A_v)_{v \in M_K}$ such that $|a_k|_v \le A'_v A_v^{k/e - \lfloor \kappa/e \rfloor}$ for $v \in M_K$ anyhow extended to $\bar{K}$ and $k \ge \kappa$, and

$$\mathrm{h}(\mathcal{A}') \le \mathrm{h}_{\mathrm{p}}(P) + \log 3, \quad \mathrm{h}(\mathcal{A}) \le (3n - 1)\mathrm{h}_{\mathrm{p}}(P) + 3n \log(mn) + 7en.$$

Proof. The proof is identical to that of Theorem 6.1, but now instead of Corollary 4.6 one should use Corollary 5.3; in particular, we define

$$A_v = \begin{cases} \max\{2|R_P/\gamma|_v, (6|P|_v)^n\} & \text{if } v \mid \infty, \\ \max\{c(p, n)^e |R_P/\gamma|_v, |P|_v^n\} & \text{if } v \mid p < \infty, \end{cases} \quad A'_v = \begin{cases} 3|P|_v & \text{if } v \mid \infty, \\ |P|_v & \text{if } v \mid p < \infty, \end{cases} \tag{6.3}$$

where P is assumed to be $\lfloor \kappa/e \rfloor$-normalized. We leave the further details to the reader. □

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

We conclude this section with one application of Theorem 6.3, which is used in [4]. The Eisenstein theorem implies that for all but finitely many $v \in M_K$ the v-adic norms of all the coefficients of an algebraic power series are bounded by 1. We want to estimate the size of the finite set of exceptional v for which this fails.

Let us make some definitions. We define the *absolute norm* $\mathcal{N}v$ of $v \in M_K$ as the absolute norm of the corresponding prime ideal if $v \mid p < \infty$; for $v \mid \infty$ we set $\mathcal{N}v = 1$.

We define the *height* of a finite subset $S \subset M_K$ as $\mathrm{h}(S) = d^{-1} \sum_{v \in S} \log \mathcal{N}v$. (Recall that $d = [K : \mathbb{Q}]$.)

So far we dealt with an individual series f. However, if the polynomial $P(z, w) \in K[z, w]$ is w-separable, then the Puiseux theorem implies existence of $n = \deg_w P$ distinct series $f_1, \dots, f_n$, which can be written as

$$f_i(z) = \sum_{k=\kappa_i}^{\infty} a_{ik} z^{k/e_i} \quad (i = 1, \dots, n), \tag{6.4}$$

and which satisfy $P(z, f_i(z)) = 0$.

THEOREM 6.4. *Let $P(z, w) \in K[z, w]$ be a w-separable polynomial with $m = \deg_z P$ and $n = \deg_w P$, and let $f_1, \dots, f_n$ be the n distinct series, written as in (6.4) and satisfying $P(z, f_i(z)) = 0$. Let S be the (finite) set of $v \in M_K$ such that $|a_{ik}|_v > 1$ for some coefficient a_{ik} and some extension of v to $\bar{K}$. Then*

$$\mathrm{h}(S) \le 3n(\mathrm{h}_{\mathrm{p}}(P) + \log(mn) + 1).$$

PROOF. For a non-Archimedean $v \in M_K$ let π_v be a primitive element of v (a generator of the maximal ideal of the local ring of v). Any $\alpha \in K^\times$ can be written as $\alpha = \pi_v^\ell \eta$ with $\ell \in \mathbb{Z}$ and η a v-adic unit. One verifies immediately that $\ell = d_v \log |\alpha|_v / \log \mathcal{N}v$ (where $d_v = [K_v : \mathbb{Q}_v]$ is the local degree), which shows that for $\alpha \in K^\times$ the quotient $d_v \log |\alpha|_v / \log \mathcal{N}v$ is an integer. In particular, if $|\alpha|_v > 1$ then $d_v \log |\alpha|_v \ge \log \mathcal{N}v$.

Denote by $P_i(z, w)$ the $\lfloor \kappa_i / e_i \rfloor$-normalization of P. As follows from Theorem 6.3 together with definitions (6.3), we may have $|a_{ik}|_v > 1$ (for some extension of v to $\bar{K}$) only if either $|P_i|_v > 1$, or $|R_P/\gamma|_v > 1$, or $v \mid p \le n$ or $v \mid \infty$. Since each of the numbers $|P_i|_v$, $|R_P/\gamma|_v$ and $|p^{-1}|_v$ is equal to $|\alpha|_v$ for some $\alpha \in K$,

$$\log \mathcal{N}v \le \begin{cases} d_v \log |P_i|_v & \text{if } |P_i|_v > 1, \\ d_v \log |R_P/\gamma|_v & \text{if } |R_P/\gamma|_v > 1, \\ d_v \log p & \text{if } v \mid p. \end{cases}$$

It follows that

$$\begin{aligned} \mathrm{h}(S) &\le \mathrm{h}_{\mathrm{p}}(R_P/\gamma) + \mathrm{h}_{\mathrm{p}}(P_1) + \cdots + \mathrm{h}_{\mathrm{p}}(P_n) + \sum_{p \le n} \log p \\ &= \mathrm{h}_{\mathrm{p}}(R_P) + n\mathrm{h}_{\mathrm{p}}(P) + \sum_{p \le n} \log p \\ &\le 3n(\mathrm{h}_{\mathrm{p}}(P) + \log(mn) + 1), \end{aligned}$$

where we use Proposition 3.5 and estimate (3.32) in [15, page 71]. □

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

7. Estimates involving the initial coefficient

For certain types of applications one needs a result slightly subtler than Theorem 6.1. More precisely, we want to express the divisor $\mathcal{A}'$ not in terms of the polynomial P, but in terms of the initial coefficient a_0. We prove the following theorem.

THEOREM 7.1. *Assume the set-up of Theorem 6.1. Then there exists an effective M_K-divisor $\mathcal{A} = (A_v)_{v\in M_K}$ such that*

$$|a_k|_v \le \max\{1, |a_0|_v\}A_v^k \quad (k = 0, 1, 2, \ldots)$$

for any $v \in M_K$ anyhow extended to $\bar{K}$, and such that

$$\mathrm{h}(\mathcal{A}) \le 3n\mathrm{h}_{\mathrm{p}}(P) + 3n\log(mn) + 10n.$$

For the proof, we shall use the following modification of Corollary 4.3.

PROPOSITION 7.2. *In the set-up of Proposition 4.1, the coefficients of the series (4.1) satisfy*

$$|a_k| \le \begin{cases} \max\{1, |a_0|\}(8|P|\varrho^{-1})^k & \text{if } p = \infty, \\ \max\{1, |a_0|\}(|P|\varrho^{-1})^k & \text{if } p < \infty \end{cases} \quad (k = 0, 1, 2, \ldots).$$

PROOF. Using Corollary 4.3, we find that for $|z| < \varrho$

$$|f(z) - a_0| \le \begin{cases} \dfrac{3|P||z|}{\varrho - |z|} & \text{if } p = \infty, \\ |P||z|/\varrho & \text{if } p < \infty. \end{cases}$$

It follows that in the Archimedean case for $|z| \le (1/2)\varrho|P|^{-1}$ we have $|f(z) - a_0| \le 3$. Hence

$$|f(z)| \le 4\max\{1, |a_0|\},$$

and applying (4.4) with $r = (1/2)\varrho|P|^{-1}$, we obtain $|a_k| \le 4\max\{1, |a_0|\}(2|P|\varrho^{-1})^k$, which implies that $|a_k| \le \max\{1, |a_0|\}(8|P|\varrho^{-1})^k$. Similarly, in the non-Archimedean case for $|z| < \varrho|P|^{-1}$ we have $|f(z) - a_0| < 1$. Hence $|f(z)| \le \max\{1, |a_0|\}$, and applying (4.4) with arbitrary $r < \varrho|P|^{-1}$, we obtain $|a_k| \le \max\{1, |a_0|\}(|P|\varrho^{-1})^k$. □

Now we have the following analog of Corollary 4.6.

COROLLARY 7.3. *In the set-up of Corollary 4.6 put*

$$\Sigma = \begin{cases} 8|P|\max\{2|R_P/\gamma|, (6|P|)^n\} & \text{if } p = \infty, \\ |P|\max\{c(p, n)|R_P/\gamma|, |P|^n\} & \text{if } p < \infty. \end{cases}$$

Then $|a_k| \le \max\{1, |a_0|\}\Sigma^k$ for $k = 0, 1, 2, \ldots$.

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

Proof of Theorem 7.1 Same as the proof of Theorem 6.1, but now, as Corollary 7.3 suggests, we put

$$A_v = \begin{cases} 8|P|_v \max\{2|R_P/\gamma|_v, (6|P|_v)^n\} & \text{if } v \mid \infty, \\ |P|_v \max\{c(p,n)|R_P/\gamma|_v, |P|_v^n\} & \text{if } v \mid p < \infty. \end{cases}$$

Instead of (6.2),

$$\mathrm{h}(\mathcal{A}) \le \mathrm{h}_{\mathrm{p}}(R_P) + \log 2 + (n+1)\mathrm{h}_{\mathrm{p}}(P) + n\log 48 + \sum_{p<\infty} \log c(p,n). \tag{7.1}$$

Arguing as in the end of the proof of Theorem 6.1, we find that the right-hand side of (7.1) does not exceed $3n\mathrm{h}_{\mathrm{p}}(P) + 3n\log(mn) + 10n$. □

Similar results hold true in the general case as well. Here are the analogues of Corollary 5.3 and Theorem 6.3. We omit the details which are routine.

Corollary 7.4. *In the set-up of Corollary 5.3 put*

$$\Xi_e = \begin{cases} (8|P|)^e \max\{2|R_P/\gamma|, (6|P|)^n\} & \text{if } p = \infty, \\ |P|^e \max\{c(p,n)^e|R_P/\gamma|, |P|^n\} & \text{if } p < \infty. \end{cases}$$

Then for $k \ge \kappa$ we have the estimate $|a_k| \le \max\{1, |a_{e\lfloor \kappa/e \rfloor}|\}\Xi_e^{k/e-\lfloor \kappa/e \rfloor}$.

Here we tacitly define $a_k = 0$ for $k < \kappa$. In particular, $\max\{1, |a_{e\lfloor \kappa/e \rfloor}|\} = 1$ if $e \nmid \kappa$.

Theorem 7.5. *Assume the set-up of Theorem 6.3. Then there exists an effective M_K-divisor $\mathcal{A} = (A_v)_{v\in M_K}$ such that $|a_k|_v \le \max\{1, |a_{e\lfloor \kappa/e \rfloor}|_v\}A_v^{k/e-\lfloor \kappa/e \rfloor}$ for $v \in M_K$ anyhow extended to $\bar{K}$ and any $k \ge \kappa$, and*

$$\mathrm{h}(\mathcal{A}) \le (3n + e - 1)\mathrm{h}_{\mathrm{p}}(P) + 3n\log(mn) + 10en. \tag{7.2}$$

8. Fields generated by the coefficients

If the polynomial $P(z,w)$ has coefficients in a field K (of characteristic zero), then any power series $f(z)$ satisfying $P(z, f(z)) = 0$ has coefficients in a finite extension L of K of degree at most $n = \deg_w P$; this follows from the fact that there can be at most n distinct series $g(z)$ satisfying $P(z, g(z)) = 0$, and they include all the series obtained from f by the Galois conjugation over K.

For applications one needs to estimate the discriminant or some other invariants of the field L in the case when K is a number field; see, for instance, [2, 3, 6, 19], where such estimates are crucial for Baker's method. In fact, Schmidt's interest in the Eisenstein theorem was largely motivated by applications in Diophantine analysis [19], in particular, through estimating in [18] the number fields generated by coefficients of certain algebraic power series.

The standard approach used in the articles quoted above was to estimate the number of the coefficients of the series f needed to generate L, and then to estimate the field L

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

itself, in the form of estimating one of its generators, as in [2, 18], or its discriminant, as in [3, Lemma 2.4.2].

Here we follow a similar approach, but introduce one technical novelty (see Lemma 8.2 below) which allows us to obtain results looking best possible for the method up to a constant factor. Surprisingly, it turns out to be more efficient to generate the field L coefficient by coefficient, passing through the subfields, rather than by all the coefficients at once, as in [3, Lemma 2.4.2]. In particular, we use item (4) of Proposition 8.1 below only in the case when $\mathbf{a}$ is a singleton.

Let us introduce some notation. Given an extension L/K of number fields, we denote by $\partial_{L/K}$ the *normalized logarithmic relative discriminant*:

$$\partial_{L/K} = \frac{\log \mathcal{N}_{K/\mathbb{Q}} \mathcal{D}_{L/K}}{[L:\mathbb{Q}]},$$

where $\mathcal{D}_{L/K}$ is the usual relative discriminant and $\mathcal{N}_{K/\mathbb{Q}}$ is the norm map. The properties of this quantity are summarized in the following proposition, which will be used in the following without special reference.

Proposition 8.1.

(1) *(additivity in towers) If $K \subset L \subset M$ is a tower of number fields, then $\partial_{M/K} = \partial_{L/K} + \partial_{M/L}$.*
(2) *(base extension) If K' is a finite extension of K and $L' = LK'$ then $\partial_{L'/K'} \le \partial_{L/K}$.*
(3) *(triangle inequality) If L_1 and L_2 are extensions of K, then $\partial_{L_1L_2/K} \le \partial_{L_1/K} + \partial_{L_2/K}$.*
(4) *(bounding in terms of the generators) Let $\mathbf{a} = (a_1, \dots, a_k)$ be a point in $\bar{K}^k$. Put $L = K(\mathbf{a})$ and $\nu = [L:K]$. Then*

$$\partial_{L/K} \le 2(\nu - 1)\mathrm{h}_{\mathrm{a}}(\mathbf{a}) + \log \nu.$$

Proof. Items (1) and (2) follow from the definition of the discriminant as the norm of the different, and the multiplicativity of the different in towers. Item (3) is a direct consequence of the previous two. Item (4) is due to Silverman [20, Theorem 2]. □

In the following K is a number field,

$$P(z, w) = p_n(z)w^n + p_{n-1}(z)w^{n-1} + \cdots + p_0(z) \in K[z, w]$$

is a w-separable polynomial with

$$m = \deg_z P, \quad n = \deg_w P,$$

and $f(z) \in \bar{K}((z^{1/e}))$ is a power series satisfying $P(z, f(z)) = 0$.

More generally, since the polynomial $P(z, w)$ is w-separable, there are n distinct series $f_1 = f, f_2, \dots, f_n$ satisfying $P(z, f_i(z)) = 0$, with $f_i(z) \in \bar{K}((z^{1/e_i}))$ for some natural e_i.

We denote by L the number field generated over K by the coefficients of f; more generally, we denote by $L_1, \dots, L_n$ the number fields generated by the coefficients of $f_1, \dots, f_n$, respectively.

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

8.1. Integral case. In this subsection we consider the *integral case*, that is, we assume that

$$p_n(0) \neq 0.$$

This latter condition is equivalent to saying that the series $f_1, \dots, f_n$ have no negative part: $f_i(z) \in \bar{K}[[z^{1/e_i}]]$. In particular, for $f = f_1$,

$$f(z) = \sum_{k=0}^{\infty} a_k z^{k/e} \in \bar{K}[[z^{1/e}]].$$

Our main tool is Lemma 8.2 below. To state it, we need some more definitions. We denote by Λ_k the field generated over K by the first k coefficients of f; more precisely,

$$\Lambda_0 = K, \quad \Lambda_k = K(a_0, \dots, a_{k-1}) \quad (k = 1, 2, 3, \dots).$$

Clearly, $\Lambda_k = L$ for sufficiently large k. Further, put $\lambda_k = [L : \Lambda_k]$, so that all but finitely many of the λ_k are 1.

Lemma 8.2. *In the set-up above,*

$$\sum_{k=0}^{\infty} \frac{k}{e}(\lambda_k - \lambda_{k+1}) \leq \operatorname{ord}_z P'_w(z, f(z)).$$

Proof. We may assume that $f = f_1, f_2, \dots, f_\nu$ are the series obtained from f by Galois conjugation over K. By the definition of the degrees λ_k, there are exactly $\lambda_k - \lambda_{k+1}$ indices $i \in \{2, \dots, \nu\}$ satisfying $\operatorname{ord}_z(f - f_i) = k/e$. Hence

$$\sum_{k=0}^{\infty} \frac{k}{e}(\lambda_k - \lambda_{k+1}) = \operatorname{ord}_z \prod_{i=2}^{\nu}(f(z) - f_i(z)). \tag{8.1}$$

Since the series $f_1, \dots, f_n$ have no negative part, the product in the right-hand side of (8.1) divides

$$P'_w(z, f(z)) = p_n(z) \prod_{i=2}^{n}(f(z) - f_i(z))$$

in the ring $L[[z]]$. This completes the proof. □

Now we may state and prove the principal result of this section in the integral case. Let $D(z) = D_P(z)$ be the w-discriminant of $P(z, w)$; it is not identically zero because P is w-separable.

Theorem 8.3. *Assume that $p_n(0) \neq 0$.*

(1) *The field L, generated by the coefficients of f, satisfies*

$$\partial_{L/K} \leq 2(\nu - 1)\mathrm{h_a}(a_0) + (8n - 1)\operatorname{ord}_z P'_w(z, f(z))(\mathrm{h_p}(P) + \log(mn) + 3e),$$

where $\nu = [L : K]$.

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

(2) *Put* $E = \max\{e_1, \dots, e_n\}$. *Then the number fields* $L_1, \dots, L_n$, *generated over* K *by the coefficients of* $f_1, \dots, f_n$, *respectively, satisfy*

$$\sum_{i=1}^{n} \partial_{L_i/K} \le 2(n-1)(\mathrm{h_p}(P) + \log(n+1)) + (8n-1)\mathrm{ord}_z D(z)(\mathrm{h_p}(P) + \log(mn) + 3E). \tag{8.2}$$

Proof. Write $\mu_k = [\Lambda_{k+1} : \Lambda_k] = \lambda_k/\lambda_{k+1}$. Items (1) and (4) of Proposition 8.1 imply that

$$\partial_{L/K} \le \sum_{k=0}^{\infty} (2(\mu_k - 1)\mathrm{h_a}(a_k) + \log \mu_k). \tag{8.3}$$

Theorem 7.5 gives an M_L-divisor $\mathcal{A}$, satisfying (7.2), and such that $\mathrm{h_a}(a_k) \le \mathrm{h_a}(a_0) + \mathrm{h}(\mathcal{A})k/e$. Substituting this to (8.3),

$$\partial_{L/K} \le 2\mathrm{h_a}(a_0) \sum_{k=0}^{\infty} (\mu_k - 1) + 2\mathrm{h}(\mathcal{A}) \sum_{k=0}^{\infty} \frac{k}{e}(\mu_k - 1) + \log \nu.$$

Lemma 8.2 implies that

$$\sum_{k=0}^{\infty} \frac{k}{e}(\mu_k - 1) = \sum_{k=0}^{\infty} \frac{k}{e} \frac{\lambda_k - \lambda_{k+1}}{\lambda_{k+1}} \le \sum_{k=0}^{\infty} \frac{k}{e}(\lambda_k - \lambda_{k+1}) \le \mathrm{ord}_z P'_w(z, f(z)).$$

Similarly,

$$\sum_{k=0}^{\infty} (\mu_k - 1) = \sum_{k=0}^{\infty} \frac{\lambda_k - \lambda_{k+1}}{\lambda_{k+1}} \le \sum_{k=0}^{\infty} (\lambda_k - \lambda_{k+1}) = \nu - 1.$$

We obtain

$$\partial_{L/K} \le 2(\nu - 1)\mathrm{h_a}(a_0) + 2\,\mathrm{ord}_z P'_w(z, f(z))\mathrm{h}(\mathcal{A}) + \log \nu.$$

Combining this with (7.2), item (1) follows after a simplification.

Analogous inequalities hold for every field L_i. Since $\nu_i = [L_i : K] \le n$ and

$$D(z) = \prod_{i=1}^{n} P'_w(z, f_i(z)),$$

summing up these n inequalities gives

$$\sum_{i=1}^{n} \partial_{L_i/K} \le 2(n-1)(\mathrm{h_a}(a_{1,0}) + \cdots + \mathrm{h_a}(a_{n,0})) + (8n-1)\mathrm{ord}_z D(z)(\mathrm{h_p}(P) + \log(mn) + 3E),$$

where $a_{i,0}$ is the initial coefficient of f_i. It remains to notice that $a_{1,0}, \dots, a_{n,0}$ are the roots of the polynomial $q(w) = P(0, w)$, and item (2) of Proposition 3.6 gives

$$\mathrm{h_a}(a_{1,0}) + \cdots + \mathrm{h_a}(a_{n,0}) \le \mathrm{h_p}(q) + \log(n+1) \le \mathrm{h_p}(P) + \log(n+1).$$

This proves item (2). □

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

The estimates in Theorem 8.3 involve orders of vanishing, which is practical for certain applications, but not convenient to be used directly. Therefore, we give below a 'prêt à porter' version, ready to be used; it also gives a good idea of the quality of our estimates.

COROLLARY 8.4. *Assume that* $p_n(0) \neq 0$.

(1) *We have*

$$\sum_{i=1}^{n} \partial_{L_i/K} \leq 16mn(n-1)(\mathrm{h_p}(P) + \log(mn) + 3E). \tag{8.4}$$

(2) *Assume that the field* $L = L_1$ *is of degree* ν *over* K. *Then*

$$\partial_{L/K} \leq \frac{1}{\nu} 16mn(n-1)(\mathrm{h_p}(P) + \log(mn) + 3E). \tag{8.5}$$

PROOF. Since $\mathrm{ord}_z D(z) \leq \deg D(z) \leq 2m(n-1)$, estimate (8.4) follows from (8.2) after easy transformations. Next, if $[L : K] = \nu$ then among the fields L_i there are ν fields conjugate to L over K. If L_i is conjugate to L then $\partial_{L_i/K} = \partial_{L/K}$. Hence, the left-hand side of (8.4) is at least $\nu\partial_{L/K}$, which proves (8.5). □

We believe that the order of magnitude in the estimates (8.4) and (8.5) is best possible, but the numerical constant 16 can probably be replaced by 8.

8.2. General case. In this subsection we consider the general case; that is, we no longer assume that $p_n(0) \neq 0$. One can treat it similarly, using the general version of the Eisenstein theorem. But it turns out to be more practical to reduce it to the integral case treated above.

THEOREM 8.5. *The number fields* $L_1, \ldots, L_n$, *generated over* K *by the coefficients of* $f_1, \ldots, f_n$, *respectively, satisfy*

$$\sum_{i=1}^{n} \partial_{L_i/K} \leq 2(n-1)(\mathrm{h_p}(P) + 4n) + (8n-1)\mathrm{ord}_z D(z)(\mathrm{h_p}(P) + 5n + \log m). \tag{8.6}$$

PROOF. We may assume that the polynomial $P(z, w)$ is not divisible by z. There exists an algebraic number ζ, which is either zero or an nth root of unity, and which is distinct from any root of the polynomial $P(0, w)$. Writing the polynomial $Q(z, w) = w^n P(z, w^{-1} + \zeta)$ as

$$Q(z, w) = q_n(z)w^n + q_{n-1}(z)w^{n-1} + \cdots + q_0(z),$$

we find $q_n(z) = P(z, \zeta)$, and, in particular, $q_n(0) \neq 0$. The series $g_i(z) = (f_i(z) - \zeta)^{-1}$ satisfies $Q(z, g_i(z)) = 0$, and its coefficients generate the field $L_i(\zeta)$ over $K(\zeta)$. We may also notice that the polynomials P and Q have the same w-discriminant (up to the sign); as before, we denote this discriminant by $D(z)$.

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

We may now apply item (2) of Theorem 8.3 to the polynomial $Q(z, w)$, the series $g_i(z)$ and the fields $L_i(\zeta)/K(\zeta)$. We obtain

$$\sum_{i=1}^{n} \partial_{L_i(\zeta)/K(\zeta)} \le 2(n-1)(\mathrm{h_p}(Q) + \log(n+1)) + (8n-1)\mathrm{ord}_z D(z)(\mathrm{h_p}(Q) + \log(mn) + 3E).$$

By the choice of ζ we have $\mathrm{h_a}(\zeta) = 0$ and $[K(\zeta) : K] \le n - 1$. Proposition 3.4 implies that

$$\mathrm{h_p}(Q) \le \mathrm{h_p}(P) + n \log 2 + \log(n+1),$$

and Proposition 8.1 implies that

$$\partial_{L_i/K} \le \partial_{L_i(\zeta)/K(\zeta)} + \partial_{K(\zeta)/K} \le \partial_{L_i(\zeta)/K(\zeta)} + \log(n-1).$$

Combining the last three inequalities, we obtain (8.6) after an obvious transformation. □

We again give a 'prêt à porter' version; the proof is the same as for Corollary 8.4 and is left out.

Corollary 8.6.

(1) *We have*

$$\sum_{i=1}^{n} \partial_{L_i/K} \le 16mn(n-1)(\mathrm{h_p}(P) + 5n + \log m).$$

(2) *Assume that the field $L = L_1$ is of degree ν over K. Then*

$$\partial_{L/K} \le \frac{2}{\nu} 16mn(n-1)(\mathrm{h_p}(P) + 5n + \log m).$$

Acknowledgements

We thank Michel Matignon for suggesting an elegant proof of Lemma 4.2, and Andrea Surroca for valuable discussions. He thanks the University of Basel and Andrea Surroca for hospitality in November–December 2011, when a substantial part of this work was done.

References

[1] M. Abouzaid, 'Heights and logarithmic gcd on algebraic curves', *Int. J. Number Theory* **4** (2008), 177–197.

[2] A. Baker and J. Coates, 'Integer points on curves of genus 1', *Proc. Cambridge Philos. Soc.* **67** (1970), 592–602.

[3] Yu. Bilu, 'Quantitative Siegel's theorem for Galois coverings', *Compositio Math.* **106**(2) (1997), 125–158.

[4] Yu. Bilu, M. Strambi and A. Surroca, 'Quantitative Chevalley–Weil theorem for curves', arXiv:0908.1233, December 2011.

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press

[5] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, New Math. Monographs, 4 (Cambridge University Press, Cambridge, 2006).
[6] J. Coates, 'Construction of rational functions on a curve', *Proc. Cambridge Philos. Soc.* **67** (1970), 105–123.
[7] P. Corvaja and U. Zannier, 'On the number of integral points on algebraic curves', *J. reine angew. Math.* **565** (2003), 27–42.
[8] B. Dwork and P. Robba, 'On natural radii of p-adic convergence', *Trans. Amer. Math. Soc.* **256** (1979), 199–213.
[9] B. M. Dwork and A. J. van der Poorten, 'The Eisenstein constant', *Duke Math. J.* **65**(1) (1992), 23–43.
[10] G. Eisenstein, 'Über eine allgemeine Eigenschaft der Reihen-Entwicklungen aller algebraischen Funktionen', *Bericht Königl. Preuss. Akad. Wiss. Berlin* (1852), 441–443.
[11] C. Fuchs, 'Polynomial–exponential equations and linear recurrences', *Glas. Mat. Ser.* III **38**(58) (2003), 233–252.
[12] E. Heine, *Theorie der Kugelfunktionen*, 2. Aufl. (Reimer, Berlin, 1878).
[13] D. L. Hilliker and E. G. Straus, 'Determination of bounds for the solutions to those binary Diophantine equations that satisfy the hypotheses of Runge's theorem', *Trans. Amer. Math. Soc.* **280** (1983), 637–657.
[14] M. Laurent and D. Poulakis, 'On the global distance between two algebraic points on a curve', *J. Number Theory* **104** (2004), 210–254.
[15] J. B. Rosser and L. Schoenfeld, 'Approximate formulas for some functions of prime numbers', *Illinois J. Math.* **6** (1962), 64–94.
[16] A. Sankaranarayanan and N. Saradha, 'Estimates for the solutions of certain Diophantine equations by Runge's method. (English summary)', *Int. J. Number Theory* **4** (2008), 475–493.
[17] W. M. Schmidt, 'Eisenstein's theorem on power series expansions of algebraic functions', *Acta Arith.* **56**(2) (1990), 161–179.
[18] W. M. Schmidt, 'Construction and estimation of bases in function fields', *J. Number Theory* **39** (1991), 181–224.
[19] W. M. Schmidt, 'Integer points on curves of genus 1', *Compositio Math.* **81** (1992), 33–59.
[20] J. H. Silverman, 'Lower bounds for height functions', *Duke Math. J.* **51** (1984), 395–403.

YURI BILU, IMB, Université Bordeaux 1,
351 cours de la Libération,
33405 Talence CEDEX, France
e-mail: bilu.yuri@gmail.com

ALEXANDER BORICHEV, LATP, CMI,
Aix-Marseille Université,
39 rue F. Joliot Curie,
13453 Marseille Cedex 13, France

https://doi.org/10.1017/S144678871300013X Published online by Cambridge University Press