Pacific Journal of Mathematics

ON THE COMPLEXITY OF RATIONAL PUISEUX EXPANSIONS

P.G. Walsh

Volume 188 No. 2 April 1999

PACIFIC JOURNAL OF MATHEMATICS
Vol. 188, No. 2, 1999

ON THE COMPLEXITY OF RATIONAL PUISEUX EXPANSIONS

P.G. Walsh

Dedicated to the memory of Professor Bernard Dwork

Duval defined and studied rational Puiseux expansions. In this paper we first prove that the existence of rational Puiseux expansions follows from the structure of algebraic extensions of a completion of the rational function field. We then describe a canonical system of rational Puiseux expansions, which are constructed in terms of the coefficients of classical Puiseux expansions. Using recent effective results on algebraic functions, we use this construction to prove that a system of rational Puiseux expansions exists whose height can be bounded in terms of the degrees and height of the polynomial determining the rational Puiseux expansions.

1. Introduction.

The layout of the paper is as follows. In Section 2 we make some definitions and state the main results of the paper. In Section 3 we discuss some of the theory of algebraic extensions of complete fields. In Section 4 some preliminary results are proved. In Section 5 the main theorems on the existence of rational Puiseux expansions are proved. Finally, in Section 6 we present an explicit construction of a system of rational Puiseux expansions, and thereby provide an effective version of the existence theorem.

2. Statement of main results.

Throughout this paper $F \in \mathbf{Q}[x, y]$ will denote a polynomial of degree $n > 0$ in y and of degree m in x. We will assume that $disc_y F \neq 0$, where $disc_y F$ is the discriminant of F, and F is regarded as a polynomial in y. Puiseux's theorem (see for example p. 118 of [**7**]) asserts the existence of n distinct formal series

$$y_i(x) = \sum_{k=f_i}^{\infty} a_{k,i} \left(x^{1/e_i} \right)^k \qquad (i = 1, ..., n)$$

such that

$$F(x,y) = v(x)\prod_{i=1}^{n}(y - y_i(x)), \tag{2.1}$$

where $v(x)$ is the leading coefficient of F when F is regarded as a polynomial in y, the $a_{k,i}$ are complex numbers, and f_i are integers defined by the condition $a_{f_i,i} \neq 0$. These are the n *Puiseux expansions* at $x = 0$ of the algebraic function y defined by $F(x,y) = 0$. For $i = 1, ..., n$, the integer e_i is the *ramification index* of the series y_i, and is minimal in the sense that if d is any positive divisor of e_i, then there is an index k not divisible by d such that $a_{k,i} \neq 0$. Throughout this paper we will make reference to

$$y(x) = \sum_{k=f}^{\infty} a_k \left(x^{1/e}\right)^k, \tag{2.2}$$

which is one of the n series given above.

Let ζ_e denote a primitive e-th root of unity. The *branch* of the series $y(x)$ is the set of series

$$B(y(x)) = \left\{ \sum_{k=f}^{\infty} a_k \left(\zeta_e^j x^{1/e}\right)^k ;\ j = 0, \dots, e-1 \right\}.$$

Note that $B(y(x))$ contains precisely e distinct series. Let $L = \mathbf{Q}(a_f, a_{f+1}, \dots)$, $s = [L : \mathbf{Q}]$, and $\sigma_1, \sigma_2, ..., \sigma_s$ be the s embeddings of L into $\overline{\mathbf{Q}}$, where $\overline{\mathbf{Q}}$ is an algebraic closure of $\mathbf{Q}$. The *conjugacy class* of $y(x)$ is

$$C(y(x)) = \left\{ \sum_{k=f}^{\infty} \sigma_i(a_k) \left(\zeta_e^j x^{1/e}\right)^k ;\ i = 1, \dots, s\ ,\ j = 0, \dots, e-1 \right\}.$$

Note that $C(y(x))$, and hence $B(y(x))$, consist entirely of Puiseux expansions at $x = 0$ of the algebraic function y defined by $F(x,y) = 0$.

In what follows, for any field E, $E((x)) = \{\sum_{k=l}^{\infty} c_k x^k\ ;\ l \in \mathbf{Z}\ ,\ c_k \in E \text{ for } k \geq l\}$ is the field of Laurent series in x with coefficients in E. The following is a consequence of the fact that the n Puiseux expansions of y are distinct. The details can be found in Lemma 1 and Lemma 2 of [**16**].

Proposition 2.1.

1. *The product* $\prod_{B(y(x))}(y - y_i(x))$ *is irreducible in* $\overline{\mathbf{Q}}((x))[y]$*, of degree* e *in* y*.*

2. *The product* $\prod_{C(y(x))}(y - y_i(x))$ *is irreducible in* $\mathbf{Q}((x))[y]$ *of degree* $e(s/s_0)$ *in* y*, where*
$s_0 = \#\left\{\sigma : L \hookrightarrow \overline{\mathbf{Q}};\ \exists\, t \in \mathbf{Z}\ \text{ such that }\ \sigma(a_k) = a_k\zeta_e^{tk} \text{ for all } k \geq f\right\}$.

The above result illustrates that the classical Puiseux expansions of y determine information about the factorization of F in $\overline{\mathbf{Q}}((x))[y]$, but fail to

exhibit explicit information about the factorization of F in $\mathbf{Q}((x))[y]$. We will see that a rational Puiseux expansion associated to $y(x)$ has coefficients in a subfield of $L = \mathbf{Q}(a_f, a_{f+1}, \dots)$ which is of degree precisely s/s_0 over $\mathbf{Q}$. In this way, the rational Puiseux expansions not only contain all of the information of the classical Puiseux expansions, but also give information about the factorization of F in $\mathbf{Q}((x))[y]$ (see Theorem 2 of [**4**]).

We now proceed to define rational Puiseux expansions. A *parametrization* of the branch $B(y(x))$, determined by $y(x)$, with $y(x)$ as in (2.2), is the pair $(x, y) = (Z^e, \sum_{k=f}^{\infty} a_k Z^k)$. Parametrizations of $B(y(x))$ determined by two different elements in $B(y(x))$ are *equivalent parametrizations*. A *generalized parametrization* of $B(y(x))$, determined by $y(x)$, is $(x, y) = (\lambda Z^e, \sum_{k=f}^{\infty} \alpha_k Z^k)$, where $\lambda \in \overline{\mathbf{Q}}$, $\alpha_k = a_k(\lambda^{1/e})^k$ for $k \geq f$, and $\lambda^{1/e}$ is a fixed e-th root of λ. Two generalized parametrizations of $B(y(x))$ are *equivalent* if they are determined by two elements of $B(y(x))$. If $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then σ acts on a generalized parametrization by $\sigma(\lambda Z^e, \sum_{k=f}^{\infty} \alpha_k Z^k) = (\sigma(\lambda) Z^e, \sum_{k=f}^{\infty} \sigma(\alpha_k) Z^k)$.

Definition. Assume that the algebraic function y has g branches. A *system of rational Puiseux expansions* of the algebraic function y is a set of g pairwise inequivalent generalized parametrizations of the branches of y with the property of being invariant under the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Elements in such a system are called *rational Puiseux expansions*.

By invariance under the Galois action, we mean that under the action of any element in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, the images of two distinct generalized parametrizations are distinct.

For the sake of illustration we provide an example, given in [**4**]. Let

$$F(x, y) = (x^2 + y^2)^3 - 4x^2y^2.$$

In this case the algebraic function y has the 6 Puiseux expansions

$$\begin{aligned} y_1(x) &= 1/2x^2 + \cdots, \quad y_2(x) = -1/2x^2 + \cdots, \\ y_3(x) &= \sqrt{2}x^{1/2} + \cdots, \quad y_4(x) = i\sqrt{2}x^{1/2} + \cdots, \\ y_5(x) &= -\sqrt{2}x^{1/2} \cdots, \quad y_6(x) = -i\sqrt{2}x^{1/2} + \cdots. \end{aligned}$$

In this case the branches (and conjugacy classes) of the algebraic function y are

$$\{y_1(x)\}, \{y_2(x)\}, \{y_3(x), y_5(x)\}, \{y_4(x), y_6(x)\},$$

and a corresponding set of rational Puiseux expansions is the set of pairs

$$\{(T, 1/2T^2 + \cdots), (T, -1/2T^2 + \cdots), (1/2T^2, T + \cdots), (-1/2T^2, T + \cdots)\}.$$

In this example we see that the coefficients of the rational Puiseux expansions all lie in $\mathbf{Q}$. By Theorem 2.2 below this is not surprising since, for example for $y_3(x)$, $e = 2$, $s = 2$, and $s_0 = 2$, showing that the coefficients of the corresponding rational Puiseux expansion lie in an extension of $\mathbf{Q}$ of degree $s/s_0 = 2/2 = 1$. To see that $s_0 = 2$, we use the fact that all 6 of the Puiseux expansions have different leading terms, which, by the proof of Theorem 2.2, implies that the value l in Theorem 2.2 can be taken to be $f = 1$.

Note that rational Puiseux expansions are in one to one correspondence with the branches of the algebraic function y. Moreover, the classical Puiseux expansions are easily recovered from a system of rational Puiseux expansions. In particular, if $(\lambda Z^e, \sum_{k=f}^{\infty} \alpha_k Z^k)$ is a generalized parametrization representing a branch B, then B consists of the e series

$$\left\{ \sum_{k=f}^{\infty} \alpha_k (\lambda^{-1/e} \zeta^j)^k (x^{1/e})^k; \;\; j = 0, ..., e-1 \right\},$$

for some e-th root of unity ζ and some e-th root, $\lambda^{-1/e}$, of λ^{-1}.

The following result was proved in [**4**]. We provide an alternative proof based on the structure of algebraic extensions of complete fields.

Theorem 2.1. *Let $F(x, y) \in \mathbf{Q}[x, y]$ with $disc_y F \neq 0$, and let y denote the algebraic function defined by $F(x, y) = 0$. Then there exists a system of rational Puiseux expansions of y.*

The following result shows how a rational Puiseux expansion gives explicit information about the factorization of F in $\mathbf{Q}((x))[y]$.

Theorem 2.2. *Let $y(x)$ be as in* (2.2), *and let $(\lambda Z^e, \sum_{k=f}^{\infty} \alpha_k Z^k)$ be a rational Puiseux expansion parametrizing $B(y(x))$. Let $L = \mathbf{Q}(a_f, a_{f+1}, \cdots)$, $s = [L : \mathbf{Q}]$, and*

$$s_0 = \# \left\{ \sigma : L \hookrightarrow \overline{\mathbf{Q}};\ \exists\, t \in \mathbf{Z} \;\; \text{such that} \;\; \sigma(a_k) = a_k \zeta_e^{tk} \;\; \text{for all} \;\; k \geq f \right\}.$$

Then $\mathbf{Q}(\lambda, \alpha_f, \alpha_{f+1}, \cdots)$ is a subfield of L of degree s/s_0 over $\mathbf{Q}$, and hence

$$\#C(y(x)) = e \cdot [\mathbf{Q}(\lambda, \alpha_f, \alpha_{f+1}, \dots) : \mathbf{Q}].$$

Moreover, $\mathbf{Q}(\lambda, \alpha_f, \alpha_{f+1}, \dots) = \mathbf{Q}(\lambda, \alpha_f, \alpha_{f+1}, \dots, \alpha_l)$ for some $l \leq 4mn^2$.

It is noteworthy that these results can be extended to any base field K of characteristic zero, although for the sake of simplicity we will consider only the case that $K = \mathbf{Q}$.

By Proposition 2.1, $\#C(y(x))$ is the degree of the irreducible factor of F in $\mathbf{Q}((x))[y]$ with $y - y(x)$ as a factor. Thus, F is irreducible in $\mathbf{Q}((x))[y]$ precisely if $\#C(y(x)) = n$. In this way, along with Theorem 2.2, a system of rational Puiseux expansions gives information about the factorization of F in $\mathbf{Q}((x))[y]$.

In the final section of this paper we will describe an explicit system of rational Puiseux expansions. From this we deduce the following effective version of Theorem 2.1. We first require some definitions.

If $P \neq 0$ is a (possibly multivariate) polynomial with integer coefficients, the *content* of P is the greatest common divisor of the coefficients of P. If $P \neq 0$ has rational coefficients, the *denominator* of P is the unique positive integer $\text{denom}(P)$ such that $\text{denom}(P) \cdot P$ has integer coefficients and content equal to one. If P has integer coefficients, then the *height* of P, denoted $ht(P)$, is the maximum of the absolute values of the coefficients of P. More generally, if P has rational coefficients, then the height of P is the maximum of $\text{denom}(P)$ and $ht(\text{denom}(P) \cdot P)$. Given an algebraic number α, P_α will denote the defining polynomial of α, that is, the unique irreducible univariate polynomial $P(x)$, with integer coefficients and content equal to one, such that $P(\alpha) = 0$. The *height* of α, denoted $ht(\alpha)$, is defined to be $ht(P_\alpha)$.

Definition. Let $S = \left\{(\lambda_i Z^e, \sum_{k=f_i}^{\infty} \alpha_{i,k} Z^k);\ i = 1, \cdots, r\right\}$ be a system of rational Puiseux expansions. The *height* of S, denoted $ht(S)$, is the maximum of $ht(\lambda_1), ..., ht(\lambda_r)$.

Because of the fact that the classical Puiseux expansions are canonical, a system of rational Puiseux expansions is completely determined by the choice of the parameters $\lambda_1, ..., \lambda_r$. This remark not only provides justification for the previous definition, but also motivates the problem of determining a system of rational Puiseux expansions of small height.

Theorem 2.3. *Let $F(x, y) \in \mathbf{Q}[x, y]$ be of degree n in y, m in x, and let $h = ht(F)$. Assume that $disc_y F \neq 0$, and let y denote the algebraic function defined by $F(x, y) = 0$. Then there exists a positive constant C, with $C < 2500$, and a system S of rational Puiseux expansions of y with*

$$ht(S) < (2^n m n^{\log n} h)^{C m^2 n^{10}}. \tag{2.3}$$

It seems difficult to prove such an effective result directly from the construction described in [**4**]. From the point of view of a bit-complexity analysis, the system of rational Puiseux expansions in the proof of Theorem

2.3 would be easier to compute than the one described in [**4**]. In fact, using the main result of either [**2**] or [**15**], it can be shown that the system of rational Puiseux expansions described in this paper can be computed in polynomial-time in the bit complexity of F, which does not seem to be the case for the system described in [**4**]. More precisely, because of the potential for large coefficient growth, a theoretical bit-complexity analysis of the construction of rational Puiseux expansions by the method in [**4**] yields an exponential running time in the number of bit operations. On the other hand, the computation described therein would probably be more practical than computing the system described here because of the fact that all of the computations in the algorithm of [**4**] are done in the inertial subfield instead of the extension field generated by the coefficients of the classical Puiseux expansions, as is done here. Therefore, the main purpose of our result is to prove the existence of at least one parameter λ with 'small' height.

3. Algebraic extensions of $\mathbf{Q}((x))$.

The purpose of this section is to present some of the basic theory of algebraic extension of complete fields. No new results are presented here.

Throughout this section the field of Laurent series with rational coefficients

$$\mathbf{Q}((x)) = \left\{ \sum_{k=f}^{\infty} a_k x^k;\ f \in \mathbf{Z}, a_k \in \mathbf{Q} \right\}$$

will be the base field whose extensions we will be interested in studying. Let $v = |\ |_x$ denote the valuation on $\mathbf{Q}(x)$ at $x = 0$, given by $v(0) = 0$ and $v(G/H) = 2^{-f}$, where $G \neq 0$ and $G/H = x^f(G_1/H_1)$ with $G_1(0) \neq 0$, $H_1(0) \neq 0$. Then $\mathbf{Q}((x))$ is the completion of $\mathbf{Q}(x)$ with respect to v, and $v(\sum_{k=f}^{\infty} a_k x^k) = 2^{-f}$, where $a_f \neq 0$. The integer f is the *order* of $\sum_{k=f}^{\infty} a_k x^k$, written as $f = \mathrm{ord}_x \sum_{k=f}^{\infty} a_k x^k$.

Let E denote an algebraic extension of $\mathbf{Q}((x))$ of degree n. Then (for example, see Theorem 7 in Chapter 2 of [**1**]) there is precisely one extension v_1 of v to E, given by

$$v_1(\alpha) = v(\mathcal{N}(\alpha))^{1/n},$$

where $\mathcal{N}$ is the norm from E to $\mathbf{Q}((x))$. The function ord_x is similarly extended to E by

$$\mathrm{ord}_x(\alpha) = (1/n)\mathrm{ord}_x(\mathcal{N}(\alpha)),$$

for $\alpha \in E$. The *ring of integers* of E is the set

$$\mathcal{O} = \{\alpha \in E;\ v_1(\alpha) \leq 1\},$$

and the unique maximal ideal consisting of the nonunits of $\mathcal{O}$ is

$$\mathcal{P} = \{\alpha \in E;\ v_1(\alpha) < 1\}.$$

The field $\mathcal{O}/\mathcal{P}$ is the *residue class field* of E. We remind the reader here of some of the basic properties of the residue class field.

Let $E_1 \subseteq E_2$ be algebraic extensions of $\mathbf{Q}((x))$, then (for example see Theorem 3 in Chapter 3 of [**1**]) the residue class field of E_1 is isomorphic to a subfield of the residue class field of E_2.

If K is an algebraic extension of $\mathbf{Q}$, and $e \geq 1$ is a positive integer, then the residue class field of $K((x^{1/e}))$ is K.

We now turn our attention to the structure of E. More precisely, by Puiseux's theorem, we may assume that E is of the form

$$E = \mathbf{Q}((x))(y_0),$$

where $y_0 = y(x)$ is given in (2.2).

Let K denote the residue class field of E, then $\delta = \delta(E/\mathbf{Q}((x))) = [K : \mathbf{Q}]$ is the *inertia* of E, and $K((x))$ is the *inertial subfield of* E (the inertia is normally denoted by f which we reserve for the order of a Laurent series). $K((x))$ is the maximal subfield of E of the form $L((x))$, with L an algebraic number field. The ring of integers of $K((x))$ is denoted $K[[x]]$. Note that K is the residue class field of $K((x))$.

An algebraic extension E of $\mathbf{Q}((x))$ is called *unramified* if the inertia of E over $\mathbf{Q}((x))$ equals the degree of E over $\mathbf{Q}((x))$, that is, $\delta(E/\mathbf{Q}((x))) = [E : \mathbf{Q}((x))]$. It is easy to see that such extensions are of the form $L((x))$ for some algebraic number field L. Thus, in the notation of the preceding paragraph, we have that $K((x))$ is the *maximal unramified extension of* $\mathbf{Q}((x))$ in E.

Again let E denote an algebraic extension of $\mathbf{Q}((x))$, and let ord_x denote the order function on E defined in Section 2. The set $G_E = \{\mathrm{ord}_x(\alpha);\ \alpha \in E\}$ is called the *value group* of E, and it is easy to see that the index $[G_E : \mathbf{Z}]$ is an integer, called the *ramification index* of L over $\mathbf{Q}((x))$, and denoted $e(E/\mathbf{Q}((x)))$. By Theorem 10 in Chapter 3 of [**1**] we have the relation

$$[E : \mathbf{Q}((x))] = e(E/\mathbf{Q}((x))) \cdot \delta(E/\mathbf{Q}((x))).$$

Thus, E is unramified precisely when $e(E/\mathbf{Q}((x))) = 1$. On the other hand, E is said to be *totally ramified* if $e(E/\mathbf{Q}((x))) = [E : \mathbf{Q}((x))]$. It is evident from the definitions of ramification and inertia that if $\mathbf{Q}((x)) \subseteq E_1 \subseteq E_2$ are algebraic extensions, then

$$e(E_2/\mathbf{Q}((x))) = e(E_2/E_1) \cdot e(E_1/\mathbf{Q}((x))),$$
$$\delta(E_2/\mathbf{Q}((x))) = \delta(E_2/E_1) \cdot \delta(E_1/\mathbf{Q}((x))).$$

Thus, $E = \mathbf{Q}((x))(y_0)$ is a totally ramified extension of its inertial subfield $K((x))$. It follows (for example see Proposition 3.4.3 of [**18**]) that

$$E = K((x))(w),$$

where w is a solution of

$$x^{e_1} = \alpha,$$

where $\alpha \in K((x))$, and $e_1 = e(E/K((x))) = [E : K((x))]$. It will be shown that the integer e_1 is equal to the ramification index e of the series $y_0 = y(x)$, justifying the terminology.

4. Preliminary Results.

In this section we prove some results required for the proofs of the main theorems. The following result is well known, the reader is referred to p. 70 of [**1**].

Lemma 4.1. *Let L be an algebraic number field, and let*

$$\alpha = 1 + a_1 x + a_2 x^2 + \dots$$

be a nonzero element in $1 + xL[[x]]$. If $e \geq 1$ is a positive integer, then the equation

$$Z^e = \alpha \tag{4.1}$$

has a solution in $L((x))$.

We will assume henceforth that F is an irreducible element in $\mathbf{Q}((x))[y]$, and y_0 will denote a root of F, given by $y_0 = y(x)$ in (2.2). Let $E = \mathbf{Q}((x))(y_0)$, then by the remarks in the previous section,

$$E = K((x))(T),$$

where K is the residue class field of E, and $T^{e_1} \in K((x))$, with $e_1 = [E : K((x))]$.

Lemma 4.2. *Let e denote the ramification index of y_0, then $e = e_1$. Moreover, $E = K((x))(T)$ where T satisfies the relation $T^e = \mu x$ for some $\mu \in K$.*

Proof. Write $T^{e_1} \in K((x))$ as

$$T^{e_1} = \alpha_t x^t + \alpha_{t+1} x^{t+1} + \dots = \alpha_t x^t (1 + P(x)),$$

where $t \in \mathbf{Z}$, $P(x) \in xK[[x]]$, and $\alpha_i \in K$ for $i \geq t$. By Lemma 4.1, it follows that T can be chosen so that $T^{e_1} = \beta x^t$ for some $\beta \in K$.

If $d = gcd(t, e_1)$, then E is a field extension of $K(\beta^{1/d})((x))$ of degree e_1/d for some d-th root of β. Thus, by the remarks in the previous section about $K((x))$ being the maximal unramified extension of $\mathbf{Q}((x))$ in E, it follows that $\beta^{1/d} \in K$, and hence that $T^{e_1/d} \in K((x))$. Thus, $d = 1$ since T is of

degree e_1 over $K((x))$, and there are integers r and s such that $1 = rt - e_1 s$. By replacing T by T^r/x^s, it follows that $T^{e_1} = \mu x$, with $\mu = \beta^r$.

To see that $e = e_1$, first notice that $T = (\mu x)^{1/e_1} \in E$, while $E = \mathbf{Q}((x))(y_0)$ contains only elements which are a sum of terms involving the formal variable $x^{1/e}$. Therefore, $e_1 > e$ is impossible, and the result will follow by proving that e divides e_1. Let p be a prime dividing e, and let r be the power of p which properly divides e. By the definition of the ramification index of y_0, there is a positive integer k, not divisible by p, such that the coefficient a_k of $x^{k/e}$ in y_0 is nonzero. Since y_0 can be written in the form $\sum \alpha_k((\mu x)^{1/e_1})^k$, it follows that p^r must divide e_1. Since this holds for any prime dividing e, it follows that e divides e_1. □

Let all notation be as above: $y_0 = y(x)$ is as in (2.2), e is the ramification index of y_0, $f = \operatorname{ord}_x y_0$, $E = \mathbf{Q}((x))(y_0)$, K is the residue class field of E, and T is an element in E such that $E = K((x))(T)$ and $T^e = \mu x$ for some $\mu \in K$. Note that $E = K((T))$, a fact to be used later in this section. For $k \geq f$ define α_k by

$$\alpha_k = a_k(\mu^{-1/e})^k,$$

where $\mu^{1/e}$ is an e-th root of μ such that $\mu^{1/e}x^{1/e} \in E$ ($\mu^{1/e}x^{1/e} = T$, and T is defined by this). The author would like to express his gratitude to Professor Bernard Dwork for suggestions in [**5**] leading to the results of this section.

Lemma 4.3. *Let $L = \mathbf{Q}(a_f, a_{f+1}, \dots)$ and $K_0 = \mathbf{Q}(\mu, \alpha_f, \alpha_{f+1}, \dots)$. Then $K = K_0$, $L = K(\mu^{1/e})$, and $[K(\mu^{1/e}) : K] = s_0$.*

Proof. For brevity let $K_0 = \mathbf{Q}(\mu, \alpha_f, \alpha_{f+1}, \dots)$ and $K_1 = \mathbf{Q}(a_f, a_{f+1}, \dots)$. Since $y_0 \in E = K((x))(T)$, y_0 can be written in the form

$$y_0 = \sum_{k=f_1}^{\infty} \beta_k T^k,$$

where $\beta_k \in K$ for $k \geq f_1$. But, as Lemma 4.2 shows, $T = \mu^{1/e}x^{1/e}$, so that

$$y_0 = \sum_{k=f_1}^{\infty} \beta_k(\mu^{1/e})^k(x^{1/e})^k = \sum_{k=f}^{\infty} a_k(x^{1/e})^k.$$

Therefore $f = f_1$ and $\beta_k = \alpha_k$ for $k \geq f$. This shows that $K_0 \subseteq K$, and moreover that $y_0 \in K_0((x))(T)$, from which it follows that $K((x))(T) = K_0((x))(T)$. Also, $K_0 \subseteq K$ forces $[E : K_0((x))] \geq e$. On the other hand, $T^e \in K_0((x))$ and $E = K_0((x))(T)$, so that $[E : K_0((x))] \leq e$, and hence $[E : K_0((x))] = e$. But now this and $K_0 \subseteq K$ imply that $K((x)) = K_0((x))$, from which it follows that $K = K_0$.

To show that $K_1 = K(\mu^{1/e})$ it will be shown that they are both equal to the residue class field, say K_2, of the field $E_1 = E(x^{1/e})$. First observe that

$E_1 = \mathbf{Q}((x^{1/e}))(y_0)$, so that $a_k \in K_2$ for all $k \geq f$, and hence $K_1 \subseteq K_2$. Now $y_0 \in K_1(x^{1/e})$, therefore $E_1 = \mathbf{Q}((x^{1/e}))(y_0) \subseteq K_1(x^{1/e})$. By the remarks in the previous section it follows that $K_2 \subseteq K_1$, and hence K_1 is the residue class field of $E(x^{1/e})$. Now observe that $T = \mu^{1/e}x^{1/e} \in K(\mu^{1/e})((x))(x^{1/e})$, so that $E = K((x))(T) \subseteq K(\mu^{1/e})((x))(x^{1/e})$, and hence $E_1 \subseteq K(\mu^{1/e})((x^{1/e}))$. Since the residue class field of $K(\mu^{1/e})((x^{1/e}))$ is $K(\mu^{1/e})$, we have that $K_2 \subseteq K(\mu^{1/e})$. But $T = \mu^{1/e}x^{1/e} \in E$, so that $\mu^{1/e} \in E_1$, and hence $K(\mu^{1/e})(x^{1/e}) \subseteq E_1$. It follows that $K(\mu^{1/e}) \subseteq K_2$, and so $K(\mu^{1/e})$ is the residue class field of E_1, which is the required result.

By part 2 of Proposition 2.1, we have that y_0 is of degree es/s_0 over $\mathbf{Q}((x))$, and so $[E : \mathbf{Q}((x))] = es/s_0$. By Lemma 4.2, $[E : K((x))] = e$, and so $[K((x)) : \mathbf{Q}((x))] = [K : \mathbf{Q}] = s/s_0$. The last statement now follows from the fact that $[K(\mu^{1/e}) : \mathbf{Q}] = s$. □

5. Proof of Theorem 2.1 and 2.2.

Proof of Theorem 2.1. Assume that F factors into irreducibles in $\mathbf{Q}((x))[y]$ as $F = F_1F_2 \cdots F_r$, and that y_i is an algebraic function defined by $F_i(x, y_i) = 0$ for $i = 1, \ldots r$. If U_i is a system of rational Puiseux expansions of y_i for $i = 1, \ldots r$, then it follows that $U = \bigcup_{i=1}^{r} U_i$ is a system of rational Puiseux expansions of the algebraic function y. Thus, it is sufficient to consider the case that F is an irreducible element in $\mathbf{Q}((x))[y]$. By Proposition 2.1, the algebraic function y defined by $F(x, y) = 0$ has only one conjugacy class of Puiseux expansions at $x = 0$. Let $y_0 = y(x)$, given in (2.2), be one these expansions, and define E to be the algebraic extension $E = \mathbf{Q}((x))(y_0)$ of $\mathbf{Q}((x))$. By Lemma 4.2 there is an element $T \in \mathbf{Q}((x))(y_0)$ such that $E = K((x))(T)$, where K is the residue class field of E, and such that $T^e = \mu x$ for some $\mu \in K$. It follows that there are $\alpha_k \in K$ for $k \geq f$ such that $y_0 = \sum_{k=f}^{\infty} \alpha_k T^k$, and there is an e-th root, $\mu^{1/e}$ of μ, and corresponding e-th root, $\lambda^{1/e}$ of λ, such that $\alpha_k = a_k(\lambda^{1/e})^k$, for $k \geq f$, where $\lambda = \mu^{-1}$. Define

$$(x(T), y(T)) = \left(\lambda T^e, \sum_{k=f}^{\infty} \alpha_k T^k \right).$$

Then $(x(T), y(T))$ is a generalized parametrization of the branch containing y_0. Let $\mathcal{T}$ denote the orbit of $(x(T), y(T))$ under the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then $\mathcal{T}$ is a set of generalized parametrizations of the branches of Puiseux expansions in the conjugacy class of y_0, and is invariant under the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. It suffices to prove that no two elements of $\mathcal{T}$ are equivalent.

If two elements of $\mathcal{T}$ are equivalent, then there are embeddings $\sigma, \gamma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and an integer i, with $0 \leq i \leq e-1$, such that

$$\sigma(\alpha_k)(\sigma(\lambda^{-1})^{1/e})^k = \gamma(\alpha_k)(\gamma(\lambda^{-1})^{1/e})^k \zeta_e^{ik}$$

for all $k \geq f$, where ζ_e is an e-th root of unity.

Regard σ and γ as embeddings of $K((x))$ into an algebraic closure in the obvious way. Recall that T is defined by $T = (\lambda^{-1})^{1/e}x^{1/e}$. Since $e = [E : K((x))]$, for each of σ and γ there are e distinct and unique embeddings of E into this algebraic closure, defined by $\overline{\sigma_j}(T) = \sigma(\lambda^{-1})^{1/e}x^{1/e}\zeta_e^j$ and $\overline{\gamma_j}(T) = \gamma(\lambda^{-1})^{1/e}x^{1/e}\zeta_e^j$ for $j = 0, \dots, e-1$. Consider the action of $\overline{\sigma_{e-i}}$ on y_0, where i is as above. Then

$$\overline{\sigma_{e-i}}(y_0) = \sum_{k=f}^{\infty} \sigma(\alpha_k)\overline{\sigma_{e-i}}(T)^k = \sum_{k=f}^{\infty} \sigma(\alpha_k)(\sigma(\lambda^{-1})^{1/e})^k\zeta_e^{-ik}x^{k/e}$$

while

$$\overline{\gamma_0}(y_0) = \sum_{k=f}^{\infty} \gamma(\alpha_k)\overline{\gamma_0}(T)^k = \sum_{k=f}^{\infty} \gamma(\alpha_k)(\gamma(\lambda^{-1})^{1/e})^k x^{k/e}.$$

Since y_0 is a primitive element of E, it follows that $\overline{\sigma_{e-i}} = \overline{\gamma_0}$. But if σ and γ are not equal, then the two sets of embeddings $\{\overline{\sigma_j};\ j = 0, \dots, e-1\}$ and $\{\overline{\gamma_j};\ j = 0, \dots, e-1\}$ are disjoint. Therefore, $\sigma = \gamma$, and hence $i = 0$, showing that no two elements of $\mathcal{T}$ are equivalent. □

Proof of Theorem 2.2. In order to prove the first part of the theorem, it is enough to show that $\mathbf{Q}(\lambda, \alpha_f, \dots)$ is the residue class field K of $E = \mathbf{Q}((x))(y_0)$. Since $y_0 \in \mathbf{Q}(\lambda, \alpha_f, \dots)((x))(Z)$, it follows that $E \subset \mathbf{Q}(\lambda, \alpha_f, \dots)((x))(Z)$. Recall that E is of degree e over $K((x))$, where e is the ramification index of y_0. As $\mathbf{Q}(\lambda, \alpha_f, \dots)((x))(Z)$ is of degree e over $\mathbf{Q}(\lambda, \alpha_f, \dots)((x))$, it follows that $K \subset \mathbf{Q}(\lambda, \alpha_f, \dots)$. Recall that the order of the conjugacy class $C(y_0)$ of y_0 is $e(s/s_0)$, and so because $(\lambda Z^e, \sum_{k=f}^{\infty} \alpha_k Z^k)$ is a rational Puiseux expansion parametrizing $B(y_0)$, its orbit under $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ has s/s_0 elements. Therefore, $[\mathbf{Q}(\lambda, \alpha_f, \dots) : \mathbf{Q}] = s/s_0 = [K : \mathbf{Q}]$ and hence $K = \mathbf{Q}(\lambda, \alpha_f, \dots)$.

The proof of the last statement in Theorem 2.2 is somewhat more involved. Let $\overline{y_0}$ denote the *singular part* of y_0, defined as the initial partial sum

$$\overline{y_0} = \sum_{k=f}^{l} a_k(x^{1/e})^k \tag{5.1}$$

of y_0, where l is minimal with the property that $\overline{y_0}$ is not equal to an initial partial sum of any other Puiseux expansion of the algebraic function y at $x = 0$ defined by $F(x, y) = 0$. We will need an upper bound for l. Define $H(t, z) = t^r F(t^e, zt^f)$, where r is chosen so that H is a polynomial not divisible by t. Then the series

$$z(t) = \sum_{k=0}^{\infty} a_{k+f}t^k$$

is a root of $H(t,z)$. Moreover, it is easy to see that $\deg_z H = n$ and $\deg_t H \leq 2mn$. Therefore, by Lemma 3 of [**3**], it follows that

$$l \leq 2mn(2n-1), \tag{5.2}$$

and that

$$\mathbf{Q}(a_f, a_{f+1}, \cdots) = \mathbf{Q}(a_f, a_{f+1}, \cdots, a_l).$$

It is now enough to prove that

$$\mathbf{Q}((x))(y_0) = \mathbf{Q}((x))(\overline{y_0}),$$

for the result follows immediately from the fact, which is proved in a similar manner as Lemma 4.3, that the residue class field of $\mathbf{Q}((x))(\overline{y_0})$ is $\mathbf{Q}(\alpha_f, \alpha_{f+1}, \cdots, \alpha_l)$.

Let $K' = \mathbf{Q}(\alpha_f, \alpha_{f+1}, \cdots, \alpha_l)$, then

$$\mathbf{Q}((x))(\overline{y_0}) \subseteq K'((x))(T) \subseteq K((x))(T) = \mathbf{Q}((x))(y_0),$$

so it is enough to prove that $\overline{y_0}$ is of degree at least es/s_0 over $\mathbf{Q}((x))$.

Let $G(y)$ be the defining polynomial of $\overline{y_0}$ over $\mathbf{Q}((x))$. For $j = 0, 1, \ldots, e-1$ and an embedding σ of L into $\overline{\mathbf{Q}}$, define the series

$$\overline{y_0}(x, \sigma, j) = \sum_{k=f}^{l} \sigma(a_k)(\zeta_e^j x^{1/e})^k.$$

Then it is easy to see that each $\overline{y_0}(x, \sigma, j)$ is a root of $G(y) = 0$. By using the exact argument given in the proof of Lemma 2 of [**16**], applied to $\overline{y_0}$, it follows that the number of distinct $\overline{y_0}(x, \sigma, j)$ is precisely es/s_0, and the result follows. □

6. Proof of the Theorem 2.3.

In this section we prove Theorem 2.3 by constructing an explicit system of rational Puiseux expansions. The proof of the bound in (2.3) is enabled by a recent effective result on algebraic functions proved in [**6**]. The author would like to greatly thank Professor Hendrik Lenstra for his suggestions in [**11**] on this work.

Let $F(x,y) \in \mathbf{Q}[x,y]$ be as in (2.1), with $n = \deg_y F$, $m = \deg_x F$, and $h = ht(F)$, and let

$$y(x) = \sum_{i=1}^{\infty} A_i x^{f_i/e_i} \tag{6.1}$$

be a Puiseux expansion at $x = 0$ of the algebraic function y defined by $F(x,y) = 0$, where for each $i \geq 1$, $A_i \neq 0$ and the greatest common divisor of f_i and e_i is 1.

In order to construct a system of rational Puiseux expansions of F, it suffices to consider the case that F is irreducible in $\mathbf{Q}((x))[y]$, for in general one would construct one system for each irreducible factor of F in $\mathbf{Q}((x))[y]$ and then take the union of these as a system of rational Puiseux expansions for F. We also make the assumption that F has integer coefficients, for this causes no loss of generality since one may replace F by $\mathrm{denom}(F)\cdot F$.

Let

$$y_l(x) = \sum_{i=1}^{l} A_i x^{f_i/e_i} \tag{6.2}$$

denote the singular part of $y(x)$, as defined in the proof of Theorem 2.2. Note that by (5.2),

$$l \leq 4mn^2,$$

and that $\mathbf{Q}(A_1, A_2, \dots) = \mathbf{Q}(A_1, A_2, \dots, A_l)$. Let $e = lcm(e_1, \dots, e_l)$, which by Theorem 6.1 of [**9**], is the ramification index of $y(x)$. For $i \geq 1$, let $c_i = e/e_i$, then from the definition of e and the fact that $gcd(e_i, f_i) = 1$, it follows that $gcd(c_1 f_1, \dots, c_l f_l, e) = 1$. Hence, there exist integers $n_1, \dots, n_l$ such that $0 \leq n_i \leq e-1$ for each $i \geq 1$ and

$$\sum_{i=1}^{l} n_i c_i f_i \equiv -1 \pmod{e}.$$

Define algebraic numbers μ and λ by

$$\mu = \prod_{i=1}^{l} A_i^{n_i},$$

$$\lambda = \mu^e, \tag{6.3}$$

and for $i \geq 1$ put

$$\beta_i = A_i \mu^{c_i f_i}.$$

Let $K = \mathbf{Q}(\lambda, \beta_1, \beta_2, \dots)$, and $r = [K : \mathbf{Q}]$. Let $\sigma_1, \dots, \sigma_r$ denote the embeddings of K into $\overline{\mathbf{Q}}$. For $1 \leq j \leq r$ put

$$(x_{\sigma_j}(T), y_{\sigma_j}(T)) = \left(\sigma_j(\lambda) T^e, \sum_{i=1}^{\infty} \sigma_j(\beta_i T^{c_i f_i}) \right).$$

Lemma 6.1. *The set* $S = \left\{ (x_{\sigma_j}(T), y_{\sigma_j}(T)); \ \ j = 1, \dots, r \right\}$ *is a system of rational Puiseux expansions of the algebraic function* y *defined by* $F(x, y) = 0$.

Proof. It is clear that S consists of generalized parametrizations of the branches of the algebraic function y at $x = 0$, and that to each branch of y

there is at least one parametrization of that branch in S. It suffices to show that no two elements of S are equivalent, in other words, to show that no two elements of S represent the same branch.

For a fixed embedding σ_j of K into $\overline{\mathbf{Q}}$ let $E(\sigma_j)$ denote the set of σ_k such that $(x_{\sigma_j}(T), y_{\sigma_j}(T))$ and $(x_{\sigma_k}(T), y_{\sigma_k}(T))$ are equivalent. By an argument identical to that given in the proof of Lemma 2 of [**16**], it can be seen that there is an extension σ_j' of σ_j to $K(\mu)$ such that

$$E(\sigma_j) = \left\{\sigma_j' \circ \theta;\ \ \theta \in E(\mathbf{1}_K)\right\}.$$

Thus, it suffices to prove that $E(\mathbf{1}_K) = \{\mathbf{1}_K\}$. Assume that without loss of generality that $\sigma_1 \in E(\mathbf{1}_K)$, and let σ_1' denote an extension of σ_1 to $K(\mu)$. The result will follow by showing that σ_1' is the identity map on K.

We are assuming that $(\lambda T^e, \sum_{i=1}^{\infty} \beta_i T^{c_i f_i})$ and $(\sigma_1(\lambda) T^e, \sum_{i=1}^{\infty} \sigma_1(\beta_i) T^{c_i f_i})$ represent the same branch. This implies that there is an integer j with $0 \le j \le e-1$ such that for all $i \ge 1$

$$\sigma_1(\beta_i)\sigma_1'(\mu)^{-c_i f_i} = \beta_i \mu^{-c_i f_i} \zeta_e^{j c_i f_i}.$$

From the definition of β_i we deduce that for all $i \ge 1$

$$\sigma_1'(A_i) = A_i \zeta_e^{j c_i f_i}.$$

It follows from the choice of the integers $n_1, \dots, n_l$ that

$$\sigma_1'(\mu) = \prod_{i=1}^{l} \sigma_1'(A_i)^{n_i} = \prod_{i=1}^{l} A_i^{n_i} \zeta_e^{j n_i c_i f_i} = \mu \zeta_e^{-j},$$

and hence also that $\sigma_1(\lambda) = \lambda$. Moreover, for $i \ge 1$,

$$\sigma_1'(\beta_i) = \sigma_1'(A_i)\sigma_1'(\mu)^{c_i f_i} = A_i \zeta_e^{j c_i f_i} \mu^{c_i f_i} \zeta_e^{-j c_i f_i} = \beta_i.$$

Recall that $K = \mathbf{Q}(\lambda, \beta_1, \beta_2, \dots)$, and so σ_1' is the identity on K, which is what we needed to prove. □

To complete the proof of Theorem 2.3 we need to estimate the height of λ, where λ is given in (6.3). This is accomplished by proving a series of preliminary results.

We define quantities A and B which will be used frequently in what follows. Let

$$A = \max_{1 \le i \le l} \|A_i\|,$$

where for an algebraic number α with algebraic conjugates $\alpha = \alpha^{(1)}, \dots, \alpha^{(q)}$, the *house* of α is

$$\|\alpha\| = \max_{1 \le j \le q} |\alpha^{(j)}|.$$

Also, let

$$B = \max_{1 \le i \le l} \operatorname{denom}(A_i),$$

where for an algebraic number α, $\operatorname{denom}(\alpha)$ is the *denominator* of α, and is defined as the least positive integer v such that $v\alpha$ is an algebraic integer.

Lemma 6.2. *There is an algebraic integer α such that $\mathbf{Q}(\alpha) = \mathbf{Q}(A_1, A_2, \dots, A_l)$ and*

$$ht(\alpha) \le (8mn^4AB)^n.$$

Proof. Let $B_1, \dots, B_l$ be positive integers no larger than B such that for each $i = 1, \dots, l$, B_iA_i is an algebraic integer. Since $\deg(A_i) \le n$ for each $1 \le i \le l$, the proof on p. 139 of [14] shows that there are positive integers $t_1, \dots, t_{l-1}$, with $1 \le t_i \le n^2$ for each i, such that

$$\alpha = B_1A_1 + t_1B_2A_2 + \cdots + t_{l-1}B_lA_l$$

is a primitive element of $\mathbf{Q}(A_1, \dots, A_l)$. Moreover, α defined this way is an algebraic integer. We have then that

$$\|\alpha\| = \|B_1A_1 + t_1B_2A_2 + \cdots + t_{l-1}B_lA_l\| \le ln^2BA \le 4mn^4AB.$$

But since α is an algebraic integer, Lemma A.2 of [**13**] shows that

$$ht(\alpha) \le (2\|\alpha\|)^n,$$

from which the result follows. □

Lemma 6.3. *Let α be as in the previous result. For each i with $1 \le i \le l$ there exists a polynomial $P_i(x) \in \mathbf{Q}[x]$ of degree at most $n-1$ such that $A_i = P_i(\alpha)$ and*

$$ht(P_i) \le (8mn^4AB)^{2n^2}.$$

Proof. Fix i in the range $1 \le i \le l$. Define

$$A_i^* = \operatorname{denom}(A_i) \cdot A_i.$$

Then because A_i^* is an algebraic integer,

$$ht(P_{A_i^*}) \le ht\left(\prod_{j=1}^{n}(x + \operatorname{denom}(A_i) \cdot \|A_i\|)\right) \le (2BA)^n.$$

Also, because $A_i^* \in \mathbf{Q}(\alpha)$, we have that $A_i^* = p_i(\alpha)$, where $p_i(x) \in \mathbf{Q}[x]$ is some polynomial of degree no greater than $n-1$.

Let D denote a positive integer and let β denote an algebraic integer. For a polynomial $P \in (1/D)\mathbf{Z}[\beta][x]$, we define its *height* to be the largest of the absolute values of the rational integers appearing in $D \cdot Q$, and denote this height by $P_{\max}$, where it is understood that this height is dependent upon the fixed values D and β.

In the proof of Proposition 3.11 of [**10**], it was shown that a monic factor of degree m of a polynomial Q in $(1/D)\mathbf{Z}[\beta][x]$ has height bounded by

$$Q_{\max}\left(2(\deg(Q)+1)(c^3)(c-1)^{(c-1)}\left(\binom{2m}{m}\right)\right)^{1/2} ht(P_\beta)^{2(c-1)},$$

where c is the degree of β over $\mathbf{Q}$.

Using this together with the result of Lemma 6.2, it follows that $x-p_i(\alpha)$ is a factor of $P_{A_i^*}(x)$ in $\mathbf{Q}[\alpha][x]$ such that

$$\begin{aligned} ht(p_i(x)) &\leq ht(P_{A_i^*})[2(n+1)^2n^3n^n\cdot 2]^{1/2}(n+1)^{n-1}ht(P_\alpha)^{2n-2} \\ &\leq (2BA)^n(2n)^{\frac{n+5}{2}}(n+1)^{n-1}(8mn^4AB)^{2n^2-2n}\cdot B \\ &\leq (8mn^4AB)^{2n^2-n}. \end{aligned}$$

The result now follows by defining $P_i(x)=(1/\mathrm{denom}(A_i))p_i(x)$. □

Lemma 6.4. *There is a polynomial $P\in\mathbf{Q}[x]$ with $\deg P\leq n-1$ such that $\lambda=P(\alpha)$ and*

$$ht(P)\leq (8mn^4AB)^{8mn^6}.$$

Proof. From the definition of λ we have that

$$\lambda=\prod_{i=1}^{l}P_i(\alpha)^{n_ie},$$

where the P_i are as in Lemma 6.3. Let $P^*(x)=\prod_{i=1}^{l}P_i(x)^{n_ie}$, then $\lambda=P^*(\alpha)$ and $\deg P^*\leq 4mn^3(n-1)^2$. Since α is of degree at most n, then reducing the higher powers of α appearing in $P^*(\alpha)$ results in a representation $\lambda=P(\alpha)$ for some polynomial $P\in\mathbf{Q}[x]$ of degree at most $n-1$. Using the estimates obtained so far, we can deduce an upper bound for $ht(P)$. For an element $\beta\in\mathbf{Q}[\alpha]$, with $\beta=p(\alpha)$ and $p\in\mathbf{Q}[x]$ of degree less than n, let $(\beta)_{\max}=ht(p)$. By an inductive argument it is easy to see that $(\alpha^t)_{\max}\leq ht(\alpha)(ht(\alpha)+1)^{t-n}$ for all $t\geq n$. Therefore, since each $n_i\leq n-1$, we have by Lemma 6.3 that

$$\begin{aligned} ht(P) &\leq ht(P^*)\sum_{i=0}^{\deg P^*}(\alpha^i)_{\max} \\ &\leq (ht(P^*))(\deg P^*+1)\cdot\max_i\left((\alpha^i)_{\max}\right) \\ &\leq (4mn^5)\left(\max_{1\leq i\leq l}ht(P_i)\right)^{4mn^3(n-1)}ht((1+\cdots+x^{n-1})^{4mn^5})ht(P_\alpha)^{4mn^5} \\ &\leq (4mn^5)(8mn^4AB)^{8mn^5(n-1)}n^{4mn^5}ht(P_\alpha)^{4mn^5} \\ &\leq (8mn^4AB)^{8mn^6}. \end{aligned}$$

Completion of the proof of Theorem 2.3. We begin by computing an estimate for $\|\lambda\|$. Let $G = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. With P as in Lemma 6.4 we have

$$\begin{aligned}\|\lambda\| &= \max_{\sigma\in G}\|\sigma(P(\alpha))\| \\ &= \max_{\sigma\in G}\|P(\sigma(\alpha))\| \\ &\leq ht(P)\cdot n\cdot\|\alpha\|^n.\end{aligned}$$

Let

$$\lambda^* = \prod_{i=1}^{l}(B_iA_i)^{n_ie},$$

then λ^* is an algebraic integer and

$$\|\lambda^*\| = \prod_{i=1}^{l}B_i^{n_ie}\|\lambda\|.$$

By Lemma A.2 of [**13**],

$$ht(\lambda^*) \leq (2\|\lambda^*\|)^n.$$

Therefore,

$$ht(\lambda^*) \leq 2^nB^{4mn^5}ht(P)^nn^n\|\alpha\|^n.$$

We now remark that if β is an algebraic number and $\nu = \mathrm{denom}(\beta)$, then β is a root of the polynomial $P_{\nu\beta}(\nu x)$, which has integer coefficients, leading coefficient equal to $\nu^{\deg(\beta)}$, and the same degree as P_β. It follows that if $lc(P_\beta)$ represents the leading coefficient of P_β, then $lc(P_\beta) \leq \mathrm{denom}(\beta)^{\deg(\beta)}$. Therefore,

$$\begin{aligned}ht(P_\lambda) &\leq lc(P_\lambda)\cdot ht(P_{\lambda^*}) \\ &\leq (\mathrm{denom}(\lambda))^n\cdot ht(P_{\lambda^*}) \\ &\leq B^{4mn^5}2^nB^{4mn^5}ht(P)^nn^n\|\alpha\|^n \\ &\leq B^{8mn^5}(2n)^n(8mn^4AB)^{n^2}(8mn^4AB)^{8mn^7} \\ &\leq (8mn^4AB)^{9mn^7}.\end{aligned}$$

Regard $y(x)$ as in (2.2), and let

$$y_{l_1} = \sum_{k=f}^{l_1}a_k(x^{1/e})^k$$

denote the singular part of $y(x)$. Then by (5.2), $l_1 \leq 4mn^2$. By Lemma 2.a of [**12**], it follows that

$$\|a_k\| \leq 2(h+1)[(h(2mn+1)(n+1))^{2n}]^{2mn^2+k},$$

for $k \geq 0$. Since $A = \max_{f\leq k\leq l_1}\|a_k\|$, it follows that

$$A \leq 2(h+1)[(h(2mn+1)(n+1))]^{12mn^3}.$$

Since $y(x)$ satisfies $F(x, y(x)) = 0$, it follows that for $b_k = a_{k+f}$, the series $z(t) = \sum_{k=0}^{\infty} b_k t^k$, satisfies $H(t, z(t)) = 0$, where $H(t, z) = t^r F(t^e, zt^{-f})$, and r is chosen to be the positive integer so that $H(t, z)$ is a polynomial, and $H(0, z) \neq 0$. Note that $f \leq m$ and $r \leq 2mn$, from which it follows that $\deg_t H \leq 2mn$, $\deg_z H \leq n$ and $ht(H) = ht(F)$. Applying the main result of [**6**] to the series $z(t)$, we obtain

$$\mathrm{denom}(b_k) \leq h(4.8n^{4+2.74\log n}2^{2n}h^2(2mn+1)^2)^{n(k+2nm)},$$

for all $k \geq 0$. We recall that $B = \max_{f \leq k \leq l_1} \mathrm{denom}(a_k)$, and so from the definition of the b_k and the bound $l_1 \leq 4mn^2$, it follows that

$$B \leq (4.8n^{4+2.74\log n}2^{2n}h^2(2mn+1)^2)^{6mn^3},$$

from which Theorem 2.3 follows.

References

[1] E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1967.

[2] A.L. Chistov, *Polynomial complexity of the Newton-Puiseux algorithm*, Lecture Notes in Computer Science, **233** (1986), 247-255.

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

[4] D. Duval, *Rational Puiseux expansions*, Compositio Mathematica, **70** (1989), 119-154.

[5] B.M. Dwork, Personal communication, 1992.

[6] B.M. Dwork and A.J. van der Poorten, *The Eisenstein constant*, Duke Math. J., **65**(**1**) (1992), 23-43.

[7] M. Eichler, *Introduction to the Theory of Algebraic Numbers and Functions*, Academic Press, London, 1966.

[8] 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.

[9] H.T. Kung and J.F. Traub, *All algebraic functions can be computed fast*, J. Assoc. Comput. Mach., **25** (1978), 246-260.

[10] A. Lenstra, *Factoring polynomials over algebraic number fields*, Proc. EuroCal. 1983, Lecture Notes in Computer Science, **162** (1983), 245-254.

[11] H.W. Lenstra, Jr., Personal communication, 1994.

[12] W.M. Schmidt, *Eisenstein's theorem on power series expansions of algebraic functions*, Acta Arith., **56** (1990), 161-179.

[13] T.N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge, 1986.

[14] B.L. van der Waerden, *Modern Algebra*, Frederick Ungar, seventh edition, New York, 1970.

[15] P.G. Walsh, *A polynomial-time complexity bound for the computation of the singular part of an algebraic function*, Submitted to Mathematics of Computation, 1994.

[16] ———, *Irreducibility testing over local fields*, Submitted to Mathematics of Computation, 1994.

[17] ———, *The computation of Puiseux expansions and a quantitative version of Runge's theorem on diophantine equations*, Doctoral Thesis, University of Waterloo, 1994.

[18] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.

Received August 13, 1997 and revised May 20, 1998.

University of Ottawa
Ottawa, Ontario K1N-6N5
Canada
E-mail address: gwalsh@mathstat.uottawa.ca