ISRAEL JOURNAL OF MATHEMATICS **124** (2001), 93–114

GOOD REDUCTION OF CERTAIN COVERS $\mathbf{P}^1 \to \mathbf{P}^1$

BY

UMBERTO ZANNIER

Ist. Univ. Arch. D.C.A.
S. Croce, 191, 30135 Venezia, Italy
e-mail: zannier@iuav.unive.it

ABSTRACT

We investigate the existence of distinct polynomials F, G having roots of prescribed multiplicities and $\deg(F-G)$ as small as predicted by Mason's *abc* theorem. The case of characteristic zero has been treated completely in a previous paper, but those methods do not apply in positive characteristic. Here we study this problem through reduction; it turns out that what we require amounts to proving good reduction for certain covers of the projective line, unramified except above $0, 1, \infty$. We shall give sufficient conditions for good reduction of those covers, which sometimes go beyond known criteria due to Grothendieck, Fulton and Beckmann. The methods are completely different from those used by such authors and rely on results by Dwork and Robba on p-adic analytic continuation of Puiseux series.

1. Introduction

In [15, Thm. 1] we proved the existence of distinct polynomials $F, G \in \mathbf{C}[t]$ having roots of prescribed multiplicities and $\deg(F-G)$ as small as possible, which is consistent with R. C. Mason's *abc* inequality in the case of genus zero.* We are interested here in the analogous existence problem in positive characteristic. The same methods of [15] do not work in this case, and in fact the corresponding result is false without appropriate supplementary assumptions. In the case of characteristic zero our proof was roughly as follows: using an observation appearing already in [14], our existence problem was first reduced to the existence of certain covers of the projective line, unramified outside $0, 1, \infty$. (These covers were defined by the rational functions F/G associated to the sought examples.) After

* Some of the results had in fact been proved in [12], as acknowledged in [16].
Received December 1, 1999 and in revised form June 12, 2000

this reduction step, Riemann's Existence Theorem completed the arguments; just the lack of a corresponding weapon in positive characteristic prevents the same proof going through.

The only method I know of, which deals with such an existence problem in characteristic $p > 0$, is through reduction modulo a prime above p of some valued field containing the coefficients of the polynomials obtained by Riemann's Theorem. This approach leads to the problem of establishing sufficient conditions for good reduction of the relevant covers. Now, as recalled, e.g., in the paper by B. Birch in [9], some such condition was established by A. Grothendieck, and later reproved by W. Fulton and, more recently, by S. Beckmann [1] (we shall refer throughout to her fairly recent paper). The results of those authors (which concern covers of general curves), applied in our special case, state that the relevant covers have good reduction modulo all primes not dividing the order of the monodromy group. This implies in particular the existence of polynomials as above (i.e., the analogue of Thm. 1 of [15]), when the characteristic p is larger than the degree.

Apart from the mentioned existence question, which was our original motivation, criteria for good reduction are useful also because, as shown, e.g., in [1], no such prime may ramify in a minimal field containing the coefficients of polynomials with the desired properties. Therefore, knowledge of the primes of good reduction provides information about the minimal field of definition.

The purpose of the present paper is to investigate good reduction with entirely new methods, namely, using p-adic analytic continuation of Puiseux series, as in B. Dwork and P. Robba's paper [4]. (A different instance of how these results may be useful in the context of good reduction appears in [17].) In contrast to [1] we treat here only the special cases of the covers of genus zero mentioned above and considered in [15]. The method may certainly be generalized, but to what extent isn't clear to us at present. We point out that sometimes the method yields a sufficient condition for good reduction which is not covered by [1]; namely, such a condition may work for certain primes which divide the order of the monodromy group.* We also point out in Corollary 2 an implication (not concerning ramification) that small primes of good reduction may have on the structure of the field of definition.

NOTATIONS AND STATEMENTS. Throughout the paper we follow the language

* New criteria for good reduction were announced by Raynaud at the Lille conference (June 1996); the criteria and corresponding methods of proof appear to be unrelated to our results.

used in [15] and we now recall its basic points. We consider two finite sequences $\boldsymbol{\mu} := (\mu_1, \ldots, \mu_h)$, $\boldsymbol{\nu} := (\nu_1, \ldots, \nu_k)$ of positive integers with equal sum n,

$$n = \sum_{i=1}^{h} \mu_i = \sum_{j=1}^{k} \nu_j.$$

Let $F(t) = \prod_{i=1}^{h}(t-\xi_i)^{\mu_i}$, $G(t) = \prod_{j=1}^{k}(t-\eta_j)^{\nu_j}$ be distinct monic polynomials of degree n, with complex coefficients. We restrict for simplicity to the case when no integer > 1 divides all numbers μ_i, ν_j. We proved in [15], as a simple consequence of Mason's *abc* theorem, that the difference $F-G$ has degree $\geq n-h-k+1 = n-e$, say. We also proved that, provided $n \geq e := h + k - 1$, as we shall assume throughout, the bound is best possible over the complex numbers and that the examples of attained bound fall into finitely many *families* (or, *classes*), where the *solution* $a^{-n}F(at+b), a^{-n}G(at+b)$ ($a, b \in \mathbf{C}$, $a \neq 0$) is considered in the same family (or class) of F, G. (We say that the pair F, G is a *solution* to our existence question if the bound is attained, i.e. if $\deg(F-G) = n-e$.) We say that the solutions belong to the same family *over a field* K if a, b can be chosen in K. For each solution it was shown that F, G are coprime.

We had observed in [15] that F, G provide a solution iff the function $s(t) := F(t)/G(t)$ is a *Belyi function*, namely, it defines a cover of $\mathbf{P}^1$ unramified except above $0, 1, \infty$, the corresponding ramification indices being given by the sequence $\boldsymbol{\mu}$ (above 0), by $\boldsymbol{\nu}$ (above ∞), and by the sequence $h+k-1, 1, \ldots, 1$ (above 1). We shall refer to some such family as a (μ, ν)-cover. We also say that F, G is an *example*. If F, G have coefficients in a field K, we say that the example is defined over K.

As pointed out above, we are interested in proving analogous existence theorems in positive characteristic. These will follow from potential good reduction (see §2). Our main result is the following

THEOREM 1: *Let K be a field of characteristic zero, with discrete valuation v having residue field K_0 of characteristic $p > 0$. Let $s := F/G \in K(t)$ represent a (μ, ν)-cover which does not have potential good reduction at v. Then p divides the order of the monodromy group and also some nonzero integer of the form $\sum_{i \in A} \mu_i - \sum_{j \in B} \nu_j$, where $A \subset \{1, \ldots, h\}$, $B \subset \{1, \ldots, k\}$.*

The conclusion about the monodromy group follows from [1], but here it is obtained by the present method. The second conclusion, which sometimes allows one to prove good reduction even for primes dividing the mentioned group order, represents the main point. (The property *nonzero* is crucial; see Remark (7.3).)

This conclusion might look artificial, and we mention a couple of facts which may help to motivate its relevance.

Firstly, it is well known that *a prime of good reduction cannot divide any ramification index* (=multiplicity) above $0, 1, \infty$, but this is not a sufficient condition (see §6). Now, roughly speaking, when we reduce the rational function F/G, some of the zeros/poles may collapse, giving rise to new multiplicities. Well, these new integers which may arise are exactly of the shape $\pm(\sum_{i\in A}\mu_i - \sum_{j\in B}\nu_j)$. Therefore, in a "new sense", it becomes true that *the primes of bad reduction must divide some multiplicity.* (See also Lemma 3.6 below and its proof, for support towards this point of view.)

Secondly, a fact related to our result is mentioned in Birch's article in [9]; Birch verifies an observation by A. Zvonkin that the discriminant of the field of moduli of certain covers (those whose dessin is a so-called Shabat tree, i.e., the case $\boldsymbol{\nu} = \{n\}$ of our covers) must be a product of factors of the form $\sum_{i\in A}\mu_i$.* Now, observe that our Theorem 1, applied in this case, predicts that primes of bad reduction must divide precisely some integer of that form! Since, however, only primes of bad reduction can be ramified in the field of moduli (see [1], [15] and §2 below), we recover the conclusion that the discriminant in question in fact contains only prime factors dividing $\prod_A(\sum_{i\in A}\mu_i)$. Theorem 1 immediately provides a corresponding conclusion also when the sequence $\boldsymbol{\nu}$ is arbitrary; namely, the primes dividing the discriminant must divide some *nonzero* integer of the form $\sum_{i\in A}\mu_i - \sum_{j\in B}\nu_j$.

From Theorem 1 we derive, for instance, the following immediate

COROLLARY 1: *The number of primes not of potential good reduction is* $\leq 2^{h+k}\log n$.

It is easy to construct examples with $h + k$ small and monodromy group containing A_n; in those cases the result improves on what follows from [1]. When the indices μ_i, ν_j satisfy suitable congruence conditions, we get other implications which do not follow from [1]. A particular instance is provided, for example, by the family of covers defined by a Belyi function of the form $s(t) = h(t)^3 r(t)^8$, for some homography $h(t) \in \mathrm{Aut}(\mathbf{P}^1)$ and some rational function $r(t)$ without double zeros or poles. We have in fact:

COROLLARY 2: *Let* $h = k > 1$, $\mu_i = \nu_i$ *for all* i *and* $\mu_1 = 3$, $\mu_i = 8$ *for* $i \geq 2$. *Then the monodromy group contains* A_n. *If* $p > n/3$ *is a prime,* $p \equiv 1 \pmod 8$,

* Birch sketches an elegant argument using [1] and certain results about prime factors of values of polynomials at integers. No hint is given, however, about the proof of the crucial fact that the discriminant must be a polynomial in the relevant data.

then p is of potential good reduction. As a consequence we have the following conclusion about the fiber above a rational point of a (μ, ν)-cover defined by the rational function $s(t) = F(t)/G(t)$. Let L be any number field and $z \in L \smallsetminus \{0, 1\}$. Then, if n is sufficiently large, not all solutions of $s(t) = z$ will lie in L.

This statement too improves on [1], and one can obviously construct more general examples. The last conclusion of this corollary shows that the field generated by the fiber above any given point becomes large as n grows. Together with ramification, this shows how the (small) primes with good reduction may provide information about the field of definition. The result may be considered as a small step towards the problem of *bounding below* the degree of a field of definition of certain covers; up to now, to the best of my knowledge, only the opposite bound has been studied systematically, probably because of its relation with the inverse Galois problem ([9], [11, Ch. 8]).

Further notation: We shall be concerned with fields K of zero characteristic equipped with a discrete valuation v. We shall denote by K_0 the residue field, always assumed perfect, of characteristic $p > 0$, by $\mathcal{O} = \mathcal{O}_K$ the valuation ring and by $\hat{K}$ the completion of K at v. Usually we shall denote reduction with a bar. We shall often work with the *Gauss valuation* (or *Gauss norm*) on $K(x)$, where x is transcendental over K. This is the unique extension of v to $K(x)$ such that $\bar{x}$, i.e., the reduction of x, is transcendental over K_0 (see [5, Chs. I, IV] for properties of this norm). For $a \in K$, we shall denote by $|a|_v$ the absolute value of a normalized such that $|p|_v = 1/p$.

The paper will be organized in several (short) sections. In §2 we shall introduce simple notions of good reduction and discuss them. In §3 we shall analyze how the Gauss norm on $K(s)$ may be extended to a function field $K(t) \supset K(s)$. In §4 we shall recall a certain theorem of Dwork and Robba [4], which is at the basis of our method. Actually, we shall need a result which has not been stated explicitly in [4], but follows from the arguments given there. We shall indicate the few necessary modifications. In §5 we shall prove the above-stated results. In §6 we shall construct examples of bad reduction when p does not divide any ramification index. Finally, the last section will be devoted to several remarks.

ACKNOWLEDGEMENT: I wish to thank F. Baldassarri and C. Deninger for helpful discussions. Also, I wish to thank the Mathematics Department of the University of Muenster for hospitality and support.

2. Good reduction

We will need the notion of good reduction only for the above-defined (μ, ν)-covers and for this purpose we can take the naïve point of view of [15]. Namely, given a (μ, ν)-cover $s = F/G \in K(t)$ defined over a field K with a discrete valuation v having perfect residue field K_0 of characteristic $p > 0$, we say it has good reduction at v (over K) if there exists a cover F^*/G^* over K, in the same class of F/G over K,† such that the reduction $\bar{F}^*/\bar{G}^*$ mod v is defined, has the same degree as F/G and does not lie in $K_0(t^p)$, namely it defines a separable extension of function fields over K_0,†† of genus zero. We say that the cover has *potential good reduction* if it has good reduction over a finite extension of K. This notion is stable under base change, namely, if we consider F/G to be in $L(t)$, for L an extension of K.

Let $c \in \mathcal{O} \setminus \{0, 1\}$, and consider the zeros and poles $\zeta_1, \ldots, \zeta_n, \ldots, \zeta_{n+k}$ of $s(t) - c$ (necessarily distinct). Assume the valuation v has been extended to the field generated over K by such elements. We claim that there is good reduction over K if and only if there exist $a, b \in K$ such that

$$v(\zeta_i - b) \geq v(a) \quad \forall i, \qquad v(\zeta_i - \zeta_j) = v(a) \quad \forall i \neq j. \tag{2.1}$$

In fact, if (2.1) holds, the function

$$s(at + b) - c = \frac{\prod_{i=1}^{n}(t - \frac{\zeta_i - b}{a})}{\prod_{j=1}^{k}(t - \frac{\zeta_{j+n} - b}{a})^{\nu_j}} \cdot$$

has roots which are v-integral (by the first of (2.1)) and have distinct reductions (by the second of (2.1)), so the reduction of $s(at + b) - c$ has degree n and is not a p-th power. Conversely, assume $s(at + b) = F^*/G^*$ is an example with good reduction. Then $F^*, G^* \in \mathcal{O}_K[t]$, so the roots of $F^* - cG^*, G^*$ are v-integral for any extension of the valuation v. Reduction of a factorization of $s(at + b) - c$ then leads to (2.1). In particular, if we have potential good reduction, this occurs over the field generated by any two among the zeros and poles of $s(t) - c$.

By saying that p *is of good reduction* (for a certain cover) we mean that there is potential good reduction for the cover in question, no matter the valued field K with perfect residue field of characteristic p.

We also recall M. Deuring's approach (see, e.g., [3], [6] or the more recent paper [7]) to good reduction, which will play a role in the next sections. Let

† It may be easily shown that if two examples over K are in the same class over the algebraic closure, they are in the same class over K.

†† The condition guarantees, in particular, that also the reduced cover is unramified outside $0, 1, \infty$.

$s \in K(t)$ define a cover of $\mathbf{P}^1$. We can extend v to $K(s)$ by the Gauss valuation on $K(s)$, i.e., the reduction of s is transcendental over K_0. We now extend v to $K(t)$. We say that s has good reduction iff there exists precisely one such extension, unramified, which moreover defines an extension of residue fields that is separable and regular over K_0. Equivalently, it is required that the residue field extension is separable, of degree $[K(t) : K(s)]$, and that K_0 is algebraically closed in the residue field of $K(t)$.

The classical theory of extensions of valuations (see, e.g., [8], VI, §1 or [10], II, §3) establishes a $1-1$ correspondence between the extensions of v and the irreducible factors of $F(t) - sG(t)$ over $\widehat{K(s)}$, the completion of $K(s)$ with respect to the Gauss valuation (here $s = F/G$ with coprime $F, G \in K[t]$).

In view of the above definitions, we see that in testing good reduction it is enough to replace K with its completion of K at v.

It is easy to see that the definitions are in fact equivalent. In one direction, assume that the Gauss valuation on $K(s)$ may be uniquely extended to $K(t)$, so to be unramified and with separable and regular residue field extension. Let π be a uniformizer of K; it is also a uniformizer of $K(s)$, whence of $K(t)$, by the assumption on ramification. By replacing t with at, some $a \in K^*$, we may assume that $v(t) \geq 0$. If the reduction of t is not transcendental over K_0 we have, by the regularity assumption, $t = c_0 + \pi t'$, with $c_0 \in \mathcal{O}_K$, $K(t) = K(t')$ and $v(t') \geq 0$. We may repeat the procedure with t' in place of t. If the procedure does not stop, we see that $t \in \hat{K}$, whence $s \in \hat{K}$, a contradiction. So the procedure stops and we may assume that t itself has reduction transcendental over K_0. Now we see at once that, if $F^*(t)/G^*(t) = s$, then the example given by F^*, G^* has good reduction in the first sense (observe that F^*, G^* lies in the same family of F, G). The converse implication is even shorter and straightforward, and we omit it.

We remark that our definitions are essentially equivalent to Beckmann's more modern ones.

We conclude this section with a brief remark about ramified primes in a field of definition. Let K be complete (with perfect residue field K_0) and let L be the field generated over K by all the roots of F, G. Then L_0 is perfect so, by [10, Th. 4, p. 46], L contains a domain isomorphic to the Witt vector ring $W(L_0)$. Let L' be the field of fractions of this ring. Then L' is absolutely unramified and L/L' is totally ramified. We recall from [15] that, if F/G has good reduction, then we may find a cover F^*/G^*, in the same class of F/G, such that $F^*, G^*, F^* - G^*$ have all their roots in L'. This may be proved by lifting the reduction with a recursive method (see [15], Prop. 4 and Remark 5, where a slightly different notation and

language are used). In particular, if the cover has good reduction, one may find a cover map $s^* = F^*/G^*$ such that s^* and the fibers above $0, 1, \infty$ are defined over an absolutely unramified field. This somewhat strengthens the result (see [1]) that the field of moduli is unramified above primes of good reduction.

3. Extensions of the Gauss norm

In this section, as above, we let K denote a field of characteristic 0, with a discrete valuation v and perfect residue field K_0 of characteristic $p > 0$.

LEMMA 3.1: *Let x, z be transcendental over K and suppose that $K(z) \subset K(x)$. Suppose further that v has been extended to $K(x)$ so as to induce the Gauss valuation on $K(z)$. Then there exist a finite extension L of K, an extension of v to $L(x)$ and an element $y \in L(x)$ such that $L(y) = L(x)$, v is the Gauss norm on $L(y)$ and $L(x) = L(y)$ is unramified over $L(z)$.*

Proof: The last assertion follows from the preceding one, since if v induces the Gauss norm on $L(t)$, the value group on $L(t)$ equals the value group on L.

We may assume that $v(x) \geq 0$. Write

$$z = \frac{r(x)}{s(x)} \quad \text{where } r, s \in K[T].$$

We may replace K with a finite extension and assume that it contains all the roots of r, s. (Observe that, since the reduction of z is transcendental over K_0, every extension of v to $L(z)$, L finite over K, will equal the Gauss valuation.) We may thus write

$$\prod_{i=1}^{n}(\lambda_i x - \alpha_i) = cz \prod_{j=1}^{m}(\eta_j x - \beta_j),$$

where all the $\lambda_i, \alpha_i, \eta_j, \beta_j$ lie in $\mathcal{O}$ and $c \in K^*$.

We also assume, as we may, that $\min(v(\lambda_i), v(\alpha_i)) = \min(v(\eta_j), v(\beta_j)) = 0$ for all i, j.

We may renumber indices and assume that λ_i is a unit precisely for $i \leq n_1$ and η_j is a unit precisely for $j \leq m_1$. In those cases we may plainly replace λ_i, η_j by 1 without altering the shape of the equation. In conclusion, the equation takes the form

$$\Phi \prod_{i=1}^{n_1}(x - \alpha_i) = cz\Psi \prod_{j=1}^{m_1}(x - \beta_j) \tag{3.2}$$

where Φ and Ψ are products of factors of the form $(\lambda x - \alpha)$, where $v(\lambda) > 0$, $v(\alpha) = 0$.

We argue by induction on the integer $N := n_1 + m_1$.

Suppose first that $N = 0$. Then we conclude that c is a unit. Reducing the equation shows that the reduction of z lies in K_0, a contradiction, since v induces the Gauss valuation on $K(z)$. So we may assume $N > 0$ and the lemma true up to $N - 1$.

Observe that, replacing if necessary c (resp. z) with $1/c$ (resp. $1/z$), we may assume that $v(c) \geq 0$.

Suppose that $v(x - \alpha_i) = 0$ for all $i \leq n_1$. Then $v(c) = 0 = v(x - \beta_j)$ for all $j \leq m_1$. Reducing the equation we get, denoting reduction with a bar,

$$\prod_{i \leq n_1} (\bar{x} - \bar{\alpha}_i) = c_0 \bar{c} \bar{z} \prod_{j \leq m_1} (\bar{x} - \bar{\beta}_j)$$

for some $c_0 \in K_0^*$. Since no factor vanishes we may divide and express $\bar{z}$ as an element of $K_0(\bar{x})$. So $\bar{x}$ must be transcendental over K_0, proving what we want.

So we may assume that some factor $x - \alpha_i$ has zero reduction. Say this happens for $i = 1$. After a translation we may assume $\alpha_1 = 0$. Let ζ be an element of some finite extension K' of K such that $v(\zeta) = v(x) > 0$. Put then $x = \zeta x'$, where $x' \in K'(x)$ satisfies $v(x') = 0$. (Plainly K' and a suitable extension of v to $K'(x)$ exist: in fact v is discrete on $K(x)$, since it is discrete on $K(z)$, and it suffices to take K' a suitable radical extension of K.) Substituting for x in (3.2) we get

$$\Phi^* \prod_{i=1}^{n_1} (\zeta x' - \alpha_i) = cz\Psi^* \prod_{j=1}^{m_1} (\zeta x' - \beta_j),$$

where Φ^*, Ψ^* are of the same form as Φ, Ψ, but with x' in place of x.

We try to write this equation in the same shape as (3.2) by writing each factor involving x' in the form $\xi(\rho x' - \gamma)$ where ξ, ρ and γ lie in the valuation ring and at least one between ρ and γ is a unit. If in some factor $\zeta x' - \alpha_i$ or $\zeta x' - \beta_j$ the corresponding ρ has positive valuation, then the corresponding number N becomes decreased and induction applies. If this does not happen, it means that $v(\zeta) \leq \min_{i \leq n_1, j \leq m_1} (v(\alpha_i), v(\beta_j))$.

If the inequality is strict we may write $\alpha_i = \zeta \alpha_i^*$, $\beta_j = \zeta \beta_j^*$ where α_i^* and β_j^* lie in the maximal ideal of K'. Then the equation becomes, for some $c^* \in K^*$,

$$\Phi^* \prod_{i=1}^{n_1} (x' - \alpha_i^*) = c^* z \Psi^* \prod_{j=1}^{m_1} (x' - \beta_j^*).$$

Now, however, each factor $x' - \alpha_i^*$ or $x' - \beta_j^*$ has nonzero reduction and we reduce to a previously discussed case. Hence we may assume that $v(\zeta)$ equals some $v(\alpha_i)$

or some $v(\beta_j)$. In particular, $v(\zeta)$ lies in the value group of K and we may assume $K' = K$.

We have proved that, if the lemma is not true, then $x = \alpha + \zeta x'$ with $\alpha, \zeta \in \mathcal{O}$, $v(\zeta) > 0$ and $v(x') = 0$. We may then iterate the procedure replacing x with x'. If it eventually stops we are done. Otherwise, we see that x lies in the completion of K at v and the same must hold for z. But then v would not induce the Gauss norm on $K(z)$. ∎

Remark 3.3: The existence of a finite extension L of K such that $L(x)$ is unramified over $L(z)$ (a fact which easily implies the rest of the lemma) follows immediately from *Abhyankar's lemma* (see, e.g., [8], Corollary 4, p. 236) in case $K(x)/K(z)$ is tamely ramified.

Even though we shall not need it, we prove an extension of part of the lemma to function fields in one variable over K. Again, the result follows from Abhyankar's lemma in special cases.

PROPOSITION 3.4: *Assume K is complete. Let $\boldsymbol{\Phi}$ be a function field in one variable regular over K and assume v has been extended to $\boldsymbol{\Phi}$ so to induce the Gauss valuation on $K(z)$, for some $z \in \boldsymbol{\Phi}$. Then there exist a finite extension L of K and an extension of v to $L\boldsymbol{\Phi}$ ($:= L \otimes_K \boldsymbol{\Phi}$) such that $L\boldsymbol{\Phi}/L(z)$ is unramified.*

Proof: Let $x \in \boldsymbol{\Phi}$ be such that $v(x)$ generates the value group on $\boldsymbol{\Phi}$. (Observe that since $\boldsymbol{\Phi}$ has finite degree over $K(z)$, v is discrete on $\boldsymbol{\Phi}$.) If x is algebraic over K, then it lies in K (since $\boldsymbol{\Phi}$ is regular) and $\boldsymbol{\Phi}/K(z)$ is unramified. Hence we may assume that x is transcendental over K, so z satisfies an irreducible equation

$$a_0(x)z^n + a_1(x)z^{n-1} + \cdots + a_n(x) = 0$$

where $a_j \in K[T]$ are not all zero. Let i be an index such that $v(a_i(x)) = \min_{j \le n}\{v(a_j(x))\}$. Then

$$\frac{a_0(x)}{a_i(x)}z^n + \frac{a_1(x)}{a_i(x)}z^{n-1} + \cdots + \frac{a_n(x)}{a_i(x)} = 0$$

is an equation for z where all the coefficients have nonnegative valuation and some coefficient is 1. Consequently, we may reduce the equation to obtain a nontrivial equation for $\bar{z}$ over the residue field of $K(x)$. Since $\bar{z}$ is transcendental over K_0, we see that at least one coefficient of the reduced equation (say the reduction of $w := a_m(x)/a_i(x)$) will be transcendental over K_0. This means that v induces the Gauss valuation on $K(w) \subset K(x)$. By the previous lemma there exists a

finite extension L of K such that $L(x)$ is unramified over $L(w)$. Observe that $\boldsymbol{\Phi}$ is unramified over $K(x)$, so $L\boldsymbol{\Phi}$ is unramified over $L(x)$, whence over $L(w)$. So the value group on $L\boldsymbol{\Phi}$ equals the value group on $L(w)$, i.e., the value group on L which in turn is the value group on $L(z)$. ∎

Remark 3.5: The element y in Lemma 3.1 will plainly satisfy $x = \gamma(y)$ with $\gamma \in \mathrm{PGL}_2(L)$, namely,

$$x = \frac{ay+b}{cy+d} \quad \text{for some } a,b,c,d \in L \text{ with } ad-bc \neq 0.$$

We may also assume that $a,b,c,d \in \mathcal{O}_L$. Suppose that $v(x) \geq 0$. Then a,b,c,d may be chosen so that one at least among c,d is a unit. Put

$$w := \frac{Ay+B}{cy+d}$$

where $A,B \in \mathcal{O}_L$ are such that $v(Ad-Bc)=0$; such A,B exist since either c or d is a unit. Then $L(w)=L(y)$ and v induces the Gauss valuation also on $L(w)$. Also, we have that $x = \alpha w + \beta$ for some $\alpha \in L^*$, $\beta \in L$. In conclusion, when $v(x) \geq 0$, in the lemma we may choose y as a linear polynomial in x.

LEMMA 3.6: *With assumptions as in Lemma 3.1, let*

$$z = \frac{r(x)}{s(x)}$$

where $r,s \in K[T]$ are coprime polynomials. Let $\mu_1,\ldots,\mu_h$ (resp. $\nu_1,\ldots,\nu_k$) be the sequence of multiplicities of the roots of $r(T)$ (resp. $s(T)$) in an algebraic closure of K. Define D_r as the set of sums of the form $\sum_{i\in A}\mu_i$, where $A \subset \{1,\ldots,h\}$ and similarly for D_s. Then there exist a finite extension L of K and an extension of v to $L(x)$ such that (i) *$L(x)/L(z)$ is unramified and* (ii) *the residue class degree $f(L(x)/L(z))$ is of the form $\pm(\delta_r - \delta_s)$, where $\delta_r \in D_r$, $\delta_s \in D_s$.*

Proof: Replacing x by ax for suitable $a \in K$ we may assume that $v(x) \geq 0$, since the sets D_r, D_s do not change with this operation. Let L, y be as in the conclusion of Lemma 3.1. By Remark 3.5 above we may assume that x is a linear polynomial in y. Since a linear substitution in x does not modify the sets D_r, D_s we may assume at once that $y = x$, namely, that v induces the Gauss norm on $L(x)$. We may assume that L contains the roots of both r,s and, renumbering indices, we may write, similarly to the proof of Lemma 3.1,

$$\Phi \prod_{i=1}^{n_1}(x-\alpha_i)^{\mu_i} = cz\Psi \prod_{j=1}^{m_1}(x-\beta_j)^{\nu_j}$$

where $c \in L$, $\alpha_i, \beta_j \in \mathcal{O}_L$ and where Φ and Ψ are products of factors of the form $\rho x - \sigma$, with $v(\rho) > 0$, $v(\sigma) = 0$. Since no factor on the left has zero reduction, we see that c is a unit. Reducing the equation we have, for some $c_0 \in L_0^*$,

$$\prod_{i=1}^{n_1}(\bar{x} - \bar{\alpha}_i)^{\mu_i} = c_0 \bar{z} \prod_{j=1}^{m_1}(\bar{x} - \bar{\beta}_j)^{\nu_j}.$$

Observe that no factor on either side vanishes. So we may divide by the g.c.d. of the polynomials in $\bar{x}$ which appear on the left and right side, to obtain a nontrivial equation

$$\tilde{r}(\bar{x}) - \bar{z}\tilde{s}(\bar{x}) = 0$$

where the degrees of both $\tilde{r}$, $\tilde{s}$ are of the desired form. This is an irreducible equation for $\bar{x}$ over $L_0(\bar{z})$, proving what we want. ∎

4. A theorem of Dwork and Robba

We recall a result by Dwork and Robba about p-adic analytic continuation of Puiseux series. In fact, at the same time we briefly point out how the proof in [4] gives in certain cases the slightly more precise result stated below, which will turn out to be useful in our context. To state it, let K be as above and imbed it (as we may) in a complete algebraically closed field Ω containing an element t whose residue class is transcendental over K_0. Denote by $D(c, \rho^-)$ the disk $\{x \in \Omega : |x - c|_v < \rho\}$. As in §2 we denote by $\widehat{K(z)}$ the completion of $K(z)$ with respect to the Gauss norm.

PROPOSITION 4.1: *Let $f(x) = A_0(z)x^n + \cdots + A_n(z) \in K[x, z]$ be absolutely irreducible and suppose that at each $z_0 \in D(0, 1^-)$ (except possibly at $z_0 = 0$) the equation $f(x) = 0$ has n distinct locally analytic solutions.*

Factor f over $\widehat{K(z)}$ and consider the finite extensions of $\widehat{K(z)}$ corresponding to the various irreducible factors. Assume that each such extension is tamely ramified and that the corresponding residue field extension is separable. Then the solutions of $f(x) = 0$ at $z = 0$ are of the form

$$x = z^{-m/e}\xi(z^{1/e}), \tag{4.2}$$

where $m \in \mathbf{N}$, e is some ramification index at $z = 0$ of the function field extension of $K(z)$ defined by f and ξ is a power series with coefficients algebraic over K and radius of convergence at least 1.

Essentially, this statement is derived from Theorem 1.1 of [4], except that the various conditions concerning the factorisation of f are there replaced by the (stronger) condition $p > n$.

We briefly comment on how the proof of [4] can be easily modified to obtain the stated result. First, there is the field M_0 appearing in the proof of [4, Theorem 1.1] as the completion of the field generated by $A_0, \ldots, A_n$ over $\mathbf{Q}$. M_0 may be enlarged, so in our situation we may take $M_0 = \widehat{K(z)}$. The proof of the theorem then continues with an application of [4, Lemma 1.2] to each extension of M_0 defined by an irreducible factor of f over M_0. For the proof of that lemma to work, it is in fact sufficient that the relevant extension of M_0 is tamely ramified and that the residue field extension is separable.

The rest of the proof of [4, Theorem 1.1] does not need any modification.

As remarked in §2, we note that the factors of f over $\widehat{K(z)}$ correspond to the extensions of the Gauss norm on $K(z)$ to the function field $K(z,x)$ defined by $f(x) = 0$.

5. Proof of main results

We begin by proving Theorem 1. As noted in §2, we can replace K with its completion at v and so we can assume that K is complete.

Notations being as in the statement, assume either that p does not divide the order of the monodromy group or that it does not divide any nonzero integer of the form $\sum_{i\in A} \mu_i - \sum_{j\in B} \nu_j$. We must show that the cover has potential good reduction. We first enlarge K to a finite extension and assume it contains all the roots of $F, G, H := F - G$ and that it is algebraically closed in the splitting field of $F(x) - zG(t)$ over $K(z)$.

We let v denote the Gauss valuation on $K(z)$ and denote with the same letter any extension to that valuation to any of the involved fields. As above, we denote by $\widehat{K(z)}$ the v-completion of $K(z)$.

We consider the extensions of v to $K(x)$. We may enlarge K to a finite extension field to ensure that the conclusions of Lemma 3.6 hold with K in place of L for any extension of v to $K(x)$. In particular, we may assume that any such extension is unramified over $K(z)$.

As in the statement of Proposition 4.1, factor $F(x) - zG(x)$ over $\widehat{K(z)}$ and consider the finite extension fields of $\widehat{K(z)}$ corresponding to the various irreducible factors. By the preceding condition and the remark that such extension fields correspond to the extensions of v to $K(x)$ (see §2), each such extension is tamely ramified (in fact unramified), so one of the assumptions of Proposition 4.1 concerning the field extension is satisfied.

We contend that the second such assumption is satisfied too, namely, *we contend that each of the corresponding residue field extension is separable.*

In fact, since the various extensions are unramified, the residue class degrees equal respectively the degrees of the extensions themselves. On the other hand, these degrees divide the order of the monodromy group, since this group is the Galois group of the splitting field of $F(x) - zG(x)$ over $K(z)$. Hence our contention is proved if p does not divide this order.

In case p divides the order of the monodromy group we apply Lemma 3.6 (ii), stating that each residue class degree is of the form $\sum_{i\in A}\mu_i - \sum_{j\in B}\nu_j$; by our assumptions no such integer can be a multiple of p, completing the proof of the claim.

We are going to apply Proposition 4.1 above, but before doing that we normalize F, G conveniently. Namely, we may replace $F(t), G(t)$ resp. with $a^n F(t/a), a^n G(t/a)$, $a \in K$ an element with sufficiently large order at v, and assume that F, G have roots which are v-integers. We write

$$F(t) - G(t) = cH_1(t), \tag{5.1}$$

where $c \in \mathcal{O}$, $H_1 \in \mathcal{O}[t]$ and not all the coefficients of H_1 have positive order at v. We consider these equations for all couples of polynomials F^*, G^* lying in the same family (over K) of F, G (i.e., $F^*(t) = a^{-n}F(at+b)$, $G^*(t) = a^{-n}G(at+b)$, $a \in K^*, b \in K$), and having moreover v-integral roots. Among such equations we choose one of them with $v(c)$ minimal and suppose it is (5.1) above. We show that necessarily $v(c) = 0$.

We are going to apply Proposition 4.1 to the polynomial

$$f(X, z) := zF(X) - cH_1(X) = zF(X) - H(X).$$

The assumptions are verified for this polynomial. In fact we have

$$f(X, z) = zF(X) - (F(X) - G(X)) = (z-1)F(X) + G(X).$$

If we let x satisfy $(z-1)F(x) + G(x) = 0$, then the Gauss valuation on $K(s)$, where $s = F(x)/G(x)$, coincides with the Gauss valuation on $K(z)(= K(s))$, since $s = 1/(1-z)$ and

$$\det \begin{pmatrix} 0, 1 \\ -1, 1 \end{pmatrix} = 1$$

is a v-unit.* It follows that the assumptions concerning the relevant field extensions are verified.

* The underlying determinant criterion, stated explicitly in [3], is rather easy to prove.

We have now to verify that the solutions of $f(X,z)=0$ at each $z_0 \in D(0,1^-)$ (except possibly at $z_0=0$) are locally analytic. For this, it suffices to show that the equation $f(X,z_0)=0$ has $n=\deg_X f$ distinct solutions: in that case such solutions constitute the constant terms of n distinct power series solutions of $f(X,z)=0$ which necessarily have a nonzero radius of convergence (both in the classical and p-adic sense; see, e.g., [6], Ch. III, §1.4, pp. 115–116 or the beginning of the proof of Thm. 3.1 in [4]). Hence we have to show that $f(X,z)$ does not have double roots in X at any $z_0 \in D(0,1^-)\setminus\{0\}$ (of course, here we use that the cover defined by F/G is unramified outside $0,1,\infty$). We state the result in a short lemma.

LEMMA 5.2: *If $f(X,z_0)$ has a double root, then $z_0=1$.*

Proof: Let z_0 be such that $f(X,z_0)$ has a double root t_0, say. Then $z_0F(t_0)-H(t_0)=z_0F'(t_0)-H'(t_0)=0$. We find $F(t_0)H'(t_0)-F'(t_0)H(t_0)=0$, i.e., the Wronskian of F,H is zero at t_0. This Wronskian has degree $\le 2n-h-k$ and it is divisible by $(F,F')(G,G')$; this product of g.c.d. has degree $\ge 2n-h-k$ by our assumptions on the factorizations of F,G. So the Wronskian actually equals $(F,F')(G,G')$ (up to a nonzero constant multiple) and we conclude that $F(t_0)G(t_0)=0$. If $G(t_0)=0$ we would have $F(t_0)=H(t_0)$, whence $z_0=1$. If $F(t_0)=0$ we have $H(t_0)=0$, which contradicts the fact that F,H are coprime. ∎

We have completed the verification of the assumptions of Proposition 4.1 for the polynomial in question. So the conclusion holds for the Puiseux expansions $\theta=\theta(z)$ of the algebraic function solutions of $f(\theta,z)=0$ around $z=0$. Putting, as above, $e=h+k-1>0$ we find easily a first family of series

$$\theta_i(z)=a_{-1}\zeta^i z^{-1/e}+a_0+a_1\zeta^{-i}z^{1/e}+\cdots, \quad i=0,1,\dots,e-1, \tag{5.3}$$

where ζ is a given primitive e-th root of 1 and where a_{-1}^e is the leading coefficient of H. This corresponds to the ramification index e above ∞. The other ramification indices are equal to 1, and we have series

$$\vartheta_j(z)=b_{j,0}+b_{j,1}z+\cdots, \quad j=1,\dots,n-e, \tag{5.4}$$

where the $b_{j,0}$ are the roots of H. We point out that all the coefficients of such series lie in a finite extension L, say, of K.

We can write any solution of the first family (5.3) as $z^{-1/e}\xi(z^{1/e})$, where ξ is a power series satisfying $z^eF(\xi(z)/z)=H(\xi(z)/z)$. Multiplying by z^{n-e} we may write this equation as

$$\xi(z)^n+b_1(z)\xi(z)^{n-1}+\cdots+b_n(z)=0, \tag{5.5}$$

where $b_i(z)$ are polynomials with v-adic integer coefficients. It is well-known and easy to prove that, over a field with ultrametric valuation v, the solution of an equation

$$X^n + r_1 X^{n-1} + \cdots + r_n = 0$$

satisfies $|X|_v \leq \max\{1, |r_1|_v, \ldots, |r_n|_v\}$. Let then $z = z_0$ in (5.5), where $z_0 \in D(0, 1^-)$: observe that $\xi(z_0)$ converges in virtue of Proposition 4.1. Taking into account the estimate just recalled and the estimates $|b_i(z_0)|_v \leq 1$, we get

$$|\xi(z_0)|_v \leq 1 \quad \forall z_0 \in D(0, 1^-).$$

By [5, Prop. 1.1, p. 115] we conclude that $\sup_{i \geq -1} |a_i|_v R^i \leq 1$ for all $R < 1$, whence $|a_i|_v \leq 1$ for all i, namely, the θ_i have v-adic integral coefficients. A similar argument proves the same fact for the series $\vartheta(z)$. Observe that we have obtained, in particular, that the roots of H are v-integral.

We can now write a factorization over $K[[z]]$, namely,

$$z^e F(X) - H(X) = \prod_{i=1}^{e} (zX - (z\theta_i(z^e))) \prod_{j=1}^{n-e} (X - \vartheta_j(z^e)). \tag{5.6}$$

Before going on we observe a fact which, despite its simplicity, will be crucial.

LEMMA 5.7: *Let L be a field with discrete valuation v and valuation ring $\mathcal{O}$. Let, for $i = 1, \ldots, r$, $\sigma_i := \sum_{m=0}^{\infty} s_{i,m} z^m \in \mathcal{O}[[z]]$ be such that $\prod_{i=1}^{r} \sigma_i(z) = \lambda z^e \neq 0$, where $\lambda \in \mathcal{O}$, $e \in \mathbf{N}$. Then $v(s_{i,m}) \geq v(s_{i,0})$ for all i, m.*

Proof: We may absorb z^e in suitable factors on the left, and assume $e = 0$. Now we argue by induction on $V := v(\lambda)$. When $V = 0$ each $s_{i,0}$ is a unit of $\mathcal{O}$, so the lemma is trivially true. Let $V > 0$ and write $\lambda = \pi\lambda^*$, where π is a uniformizer and $v(\lambda^*) = V - 1 \geq 0$. At least one of the σ_i must lie in $\pi\mathcal{O}[[z]]$. Dividing by π and applying the inductive assumption we get the lemma. ∎

Let $\gamma \in K$ be some root of H; we have already remarked that γ is v-integral. Substitute $X = \gamma$ in (5.6), obtaining

$$z^e F(\gamma) = \pm \prod_{i=1}^{e} (a_{-1}\zeta^i + (a_0 - \gamma)z + a_1\zeta^{-i}z^2 + \cdots) \prod_{j=1}^{n-e} (b_{j_0} - \gamma + b_{j,1}z^e + \cdots).$$

Observe that all the series involved have coefficients in $\mathcal{O}_L$, where L is, as above, a finite extension of K containing the coefficients of the Puiseux series. Also,

* The lemma is related to Newton polygons and holds without the assumption that v is discrete, with a slightly more complicated proof.

$F(\gamma) \neq 0$, since F, G, H are coprime. We may apply Lemma 5.7 to the remaining equation, to obtain in particular

$$v(a_0 - \gamma) \geq v(a_{-1}).$$

But a_{-1}^e is the leading coefficient of H, which is divisible by c in $\mathcal{O}$ (see (5.1) above). If $v(c)$ were positive, we would deduce that

$$v(a_0 - \gamma) > 0 \tag{5.8}$$

for all γ. A completely similar argument, letting now γ be any root of F, would yield the same inequality. Finally, by symmetry (5.8) holds on letting γ be any root of G. We have proved that, if $v(c) > 0$, all the roots of F, G, H must be congruent to a given one of them, say γ_0. By a translation, we may assume that $\gamma_0 = 0$ and so we may assume that all the roots of F, G, H are divisible by π, a uniformizer of K, in $\mathcal{O}_K$. We may thus write

$$F(\pi t) = \pi^n F^*(t), \quad G(\pi t) = \pi^n G^*(t), \quad H_1(\pi t) = \pi^{n-e} H_1^*(t),$$

where F^*, G^* are monic and F^*, G^*, H_1^* have v-adic integral roots. Also, since some coefficient of H_1 is a v-unit, the same holds for H_1^*. Substituting in (5.1) we get

$$\pi^e(F^*(t) - G^*(t)) = cH_1^*(t).$$

Since H_1^* has coefficients which are v-integral, not all divisible by π, we see that π^e divides c in $\mathcal{O}$. This would give, however, an equation of type (5.1), where F^*, G^* are in the same family of F, G and have v-adic integral roots, but where c is replaced by c/π^e, contradicting the minimality of $v(c)$ among the equations with the stated properties. Hence $v(c) = 0$, as asserted above.

It is now easy to verify that we have in fact good reduction. We first show that the reductions $\bar{F}, \bar{G}$ of F, G are linearly independent over $K_0(t^p)$. Observe that (5.1) implies that $\bar{F}/\bar{G}$ is nonconstant, since $v(c) = 0$ and $\deg H_1 < n$. Consider the Gauss norm on $K(t)$. Since $\bar{F}/\bar{G}$ is nonconstant, whence transcendental over K_0, this induces the Gauss norm on $K(s)$, where $s = F/G$. If $\bar{F}/\bar{G} \in K_0(t^p)$, the residue field extension would not be separable, contrary to what has been shown to follow from our assumptions.

From (5.1) we have $\deg(\bar{F} - \bar{G}) = \deg \bar{H} \leq n - h - k + 1$. Considering the factorizations which $\bar{F}, \bar{G}$ inherit from F, G, we see from [15, pp. 127, 128] (equivalently from Mason's *abc* theorem in positive characteristic, which applies

in the separable case) that $\bar{F}, \bar{G}$ must be coprime. So the degree of the reduced cover (defined by $\bar{s} = \bar{F}/\bar{G}$) equals n, i.e., the degree of the cover F/G. This completes the verification and Theorem 1 follows.

Corollary 1 follows at once from Theorem 1: any prime of bad reduction must divide some nonzero difference of the stated form. There are at most 2^{h+k} such integers and each of them has $\leq \log n$ prime factors (we may assume $n \geq 3$).

Corollary 2 needs a little more care. We begin by showing that the monodromy group $\mathcal{G}$ is primitive. First, by e.g. [15], $\mathcal{G}$ is transitive, generated by permutations σ, $\tau \in S_n$ such that σ is a product of cycles $\beta_1, \gamma_2, \ldots, \gamma_h$ of lengths $3, 8, \ldots, 8$ while τ is a cycle of length $e = h + k - 1 = (n+1)/4$. Also, since $\mathcal{G}$ is transitive, either it is primitive or the sets of imprimitivity $T_1, \ldots, T_q$, say, all have the same order $m > 1$, say. Assume this is the case. In particular $n = qm$. Each permutation of $\mathcal{G}$ induces a permutation on $\mathcal{T} := \{T_1, \ldots, T_q\}$. A first case is when the cycle τ acts nontrivially on $\mathcal{T}$, inducing, say, the cycle $(T_1, \ldots, T_r)$. The integers moved by τ must then be those in $\bigcup_{i=1}^{r} T_i$. Hence $(n+1)/4 = rm$, which implies $m = 1$, a contradiction. Suppose now that τ fixes $\mathcal{T}$. Then the $(n+1)/4$ integers moved by τ must lie in a same T_i. In particular $m \geq (n+1)/4$, proving that $1 < q \leq 3$. Since q is odd, we have $q = 3$. Suppose the 3-cycle β_1 acts nontrivially on $\mathcal{T}$, inducing, say, (T_1, T_2, T_3). If some integer contained in T_1 would appear in some γ_j, we would have a contradiction, since each γ_j induces a cycle with period dividing 8. Therefore each γ_i fixes T_1, which is easily seen to be impossible. So in fact β_1 acts trivially on $\mathcal{T}$ and the integers it moves must be contained in, say, T_1. Consider any cycle γ_i; it must either act trivially or as a transposition on $\mathcal{T}$. Hence the number of elements in T_2 would be even, a contradiction which proves that $\mathcal{G}$ is primitive.

Now we use Theorem 1 of [13], stating that a primitive permutation group of degree n containing a cycle of order m such that $1 < m < (n-m)!$ is either A_n or S_n. Since

$$1 < \frac{n+1}{4} < \left(\frac{3n-1}{4}\right)! \quad \text{for } n \equiv 3 \pmod 8, \quad n > 3,$$

we get the first assertion of Corollary 2.

Let now $p \equiv 1 \pmod 8$ be a prime $> n/3$ and assume that a cover with the stated data has not potential good reduction at p. By Theorem 1, p must then divide some nonzero integer of the form $3\epsilon + 8m$, where $\epsilon \in \{-1, 0, 1\}$ and $|m| \leq h - 1$. If $\epsilon = 0$, we get $p \leq |m| < n/3$, so $\epsilon = \pm 1$ and $3\epsilon + 8m \equiv \pm 3 \pmod 8$. Since $p \equiv 1 \pmod 8$, we get $3p \leq |3\epsilon + 8m| \leq n$, a contradiction which proves the second assertion.

Finally, let L be any number field. Enlarging it does not affect the conclusion, so we may assume it contains a primitive 8-th root of unity. Let now $s = F/G$ provide an example with the stated data and let $z_0 \in L \smallsetminus \{0, 1\}$ be such that all solutions of $F(t) - z_0 G(t)$ lie in L. Let p be a prime which splits completely in L, such that $n/3 < p < n$; for large n the existence of p follows from classical estimates (see, e.g., [8]). Choose a prime ideal $\mathcal{P}$ of L lying above p and consider the $\mathcal{P}$-adic valuation on L. We may also assume that z_0 is $\mathcal{P}$-integral and that its reduction is not 0 or 1, by taking n large. Observe that $p \equiv 1 \pmod 8$, so the previous statement of Corollary 2 applies to our cover, which then has potential good reduction at $\mathcal{P}$. By the discussion in §2, just after (2.1), we see that, since all zeros of $(F/G) - z_0$ lie in L, the cover has good reduction already over L. Hence we may suppose, by composing F, G with a linear transformation over L, that the example provided by F, G themselves has good reduction. Then the cover in positive characteristic defined by $\bar{F}/\bar{G}$ is unramified except over $0, 1, \infty$, so the n roots of $\bar{F} - \bar{z}_0 \bar{G}$ must be distinct. However, by assumption these roots lie in the residue field of L at $\mathcal{P}$. Such residue field is $\mathbf{F}_p$ by our choice of p. However, since $n > p$, the roots cannot be distinct, a contradiction which proves completely our corollary.

6. Some cases of bad reduction

It is well known, and rather easy to prove, that we cannot have good reduction when p divides some ramification index of the cover. For our covers this means that p divides either some μ_i or ν_j (the indices above 0 and ∞) or the only index other than 1 above 1, i.e., $h + k - 1$ (see [15]). It is known that this condition does not describe all cases of bad reduction (see, e.g., the examples given in the papers of Birch and Malle in [9] or [15]).

We shall give below another condition which implies bad reduction for certain entire families of covers. In [15] we gave a few examples derived from such criterion, but did not state the whole criterion explicitly.

Let q be a power of the prime p and let a, b be natural numbers such that $\mu_1 \pm a = \nu_1 \pm b = q$.

Assume, for instance, that the plus sign holds in both cases, the arguments below being similar in the remaining cases. We have the following:

CRITERION: *Assume that* $a+b+n < \min(2q, q+h+k-1)$. *Then no* (μ, ν)*-cover can have good reduction.*

For the proof, assume the contrary and let $F, G \in K_0[t]$ be monic polynomials describing the reduction of the cover. We may write $F = \prod_{i=1}^{h} \phi_i^{\mu_i}$,

$G = \prod_{j=1}^{k} \psi_j^{\nu_j}$, where ϕ_i and ψ_j are monic linear polynomials. We have $F - G = H$ where $\deg H = n + 1 - h - k$. Also, we may assume that F/G does not lie in $K_0(t^p)$. Then, as e.g. in [15, p. 128], this forces the ϕ_i's and ψ_j's to be pairwise coprime.

Multiply the equation $F - G = H$ by $\phi_1^a \psi_1^b$ to obtain

$$\psi_1^b \phi_1^q \prod_2^h \phi_i^{\mu_i} - \phi_1^a \psi_1^q \prod_2^k \psi_j^{\nu_j} = \phi_1^a \psi_1^b H. \tag{6.1}$$

Hence

$$\psi_1^b(t)\phi_1^q(0) \prod_2^h \phi_i^{\mu_i}(t) - \phi_1^a(t)\psi_1^q(0) \prod_2^k \psi_j^{\nu_j}(t) - \phi_1^a(t)\psi_1^b(t)H(t) \in t^q K_0[t].$$

However, the inequalities we are assuming imply that the degree of the left side is $< q$. So the left side must vanish. Taking into account that the ϕ_i and ψ_j are coprime, one easily derives a contradiction.

The inequality needed to apply the criterion is of course quite restrictive; in particular, the indices μ_1, ν_1 must be "large" and the other indices must be small (many of them must be 1). However, the criterion easily shows that, for given p, there are infinitely many examples of bad reduction with ramification indices prime to p (e.g., take q to be a large power of p, $1 < h = k < q$, $\mu_1 = \nu_1 = q - 1$, $\mu_i = \nu_i = 1$ for $2 \le i \le h$).

On the other hand, we do not know whether there exist, for a given prime p, infinitely many examples with bad reduction, ramification indices prime to p and bounded μ_i, ν_j.

7. Further remarks

(7.1) Under the assumptions of Theorem 1 we may in fact prove potential good reduction for the Galois closure of the cover $s = F/G$ over $K(s)$. We omit the details, which depend on the results in [17].

(7.2) Theorem 1 curiously implies the following rather striking combinatorial result, for which a direct proof seems not easy to find. *Let $\mu := (\mu_1, \dots, \mu_h)$, $\nu := (\nu_1, \dots, \nu_k)$ be sequences of positive integers such that $e := h + k - 1$ is a prime number. Assume that $\sum_{i=1}^h \mu_i = \sum_{i=1}^k \nu_j > e$ and that no integer > 1 divides all the μ_i and the ν_j. Then there exist sets A, B such that $\sum_{i \in A} \mu_i - \sum_{j \in B} \nu_j$ is a nonzero multiple of e.* To see how the above results imply this claim, assume the conclusion not true. By the assumptions and [15] there exists a (μ, ν)-cover

in characteristic zero. Theorem 1 implies it has potential good reduction at e. On the other hand, $e = h + k - 1$ is a ramification index above 1, so, as we have recalled before, there cannot be good reduction.

(7.3) In certain special cases, namely, *if the equation* $\sum_{i\in A} \mu_i = \sum_{j\in B} \nu_j$ *holds only when the common value of the sums is* 0 *or* n, there is a much simpler proof of part of Theorem 1, which we sketch below. (We remark, however, that the assumption is quite restrictive and unnatural. For instance, Corollary 1 would hold only conditionally and Corollary 2 would no longer follow.) The argument follows Davenport's idea [2] to bound below $\deg(f^3 - g^2)$. As in §5, it is sufficient to consider (5.1) and try to prove that, if $v(c) > 0$, the roots of F, G must be congruent modulo v. As in Davenport's argument, the roots ξ_i, $1 \le i \le h$, η_j, $1 \le j \le k$, resp., satisfy a system

$$\sum_{i=1}^{h} \mu_i \xi_i^s - \sum_{j=1}^{k} \nu_j \eta_j^s = 0, \quad 0 \le s \le h + k - 2.$$

We can reduce the system modulo v and group together congruent roots. Observe that, if $v(c) > 0$, we have $\bar{F} = \bar{G}$, so the roots of $\bar{F}$ coincide in some order with the roots of $\bar{G}$ and some nontrivial grouping occurs. If the set of the reductions of the roots consists of the m distinct elements $t_1, \ldots, t_m \in K_0$, the reduced system takes the form

$$\sum_{r=1}^{m} D_r t_r^s = 0, \quad 0 \le s \le h + k - 2,$$

where each D_r has the shape $\sum_A \mu_i - \sum_B \nu_j$. Since $m < h + k$, a Vandermonde argument shows that $D_r \equiv 0 \pmod{p}$ for each r. If $m = 1$, the roots are all congruent, as wanted. Otherwise each D_r is nonzero (by the new assumption), so we get the required divisibility condition for p.

It is possible that such an argument may be refined to yield an even more elementary proof of Theorem 1, but the details look very complicated. However, the argument provides in any case some information; for instance, we see that, in case of bad reduction, there must be a splitting of the roots as above, with $D_r \equiv 0 \pmod{p}$ for all r.

References

[1] S. Beckmann, *Ramified primes in the field of moduli of branched coverings of curves,* Journal of Algebra **125** (1989), 236–255.

[2] H. Davenport, *On* $f^3(t) - g^2(t)$, Norske Vid. Selsk. Forrh. (Trondheim) **38** (1965), 86–87.

[3] M. Deuring, *Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers,* Mathematische Zeitschrift **47** (1942), 643–654.

[4] B. Dwork and P. Robba, *On natural radii of p-adic convergence,* Transactions of the American Mathematical Society **256** (1979), 199–213.

[5] B. Dwork, G. Gerotto and F. Sullivan, *An Introduction to G-functions,* Princeton University Press, 1994.

[6] M. Eichler, *Introduction to the Theory of Algebraic Numbers and Functions,* Academic Press, New York, 1966.

[7] B. Green, M. Matignon and F. Pop, *On valued function fields I,* Manuscripta Mathematica **65** (1989), 357–376.

[8] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers,* II ed., Polish Scientific Publishers & Springer-Verlag, 1990.

[9] L. Schneps ed., *The Grothendieck Theory of Dessins d'Enfants,* London Mathematical Society Lecture Note Series **200**, Cambridge University Press, 1994.

[10] J-P. Serre, *Corps locaux,* Hermann, Paris, 1968.

[11] J-P. Serre, *Topics in Galois Theory,* Jones and Bartlett, Boston, 1992.

[12] W. W. Stothers, *Polynomial identities and hauptmoduln,* The Quarterly Journal of Mathematics (2) **32** (1981), 349–370.

[13] A. Williamson, *On primitive permutation groups containing a cycle,* Mathematische Zeitschrift **130** (1973), 159–162.

[14] U. Zannier, *Some remarks on the S-unit equation in function fields,* Acta Arithmetica **64** (1993), 87–98.

[15] U. Zannier, *On Davenport's bound for the degree of $f^3 - g^2$ and Riemann's Existence Theorem,* Acta Arithmetica **71** (1995), 107–137.

[16] U. Zannier, *Acknowledgement of priority,* Acta Arithmetica **74** (1996), 387.

[17] U. Zannier, *On the reduction modulo p of an absolutely irreducible polynomial $f(x, y)$,* Archiv der Mathematik **68** (1997), 129–138.