DEFORMATION DATA, BELYI MAPS, AND THE LOCAL LIFTING PROBLEM

IRENE I. BOUW, STEFAN WEWERS, AND LEONARDO ZAPPONI

Abstract. We prove existence and nonexistence results for certain differential forms in positive characteristic, called good deformation data. Some of these results are obtained by reduction modulo \( p \) of Belyi maps. As an application, we solve the local lifting problem for groups with Sylow \( p \)-subgroup of order \( p \).

Introduction

The local lifting problem. Let \( k \) be an algebraically closed field of characteristic \( p > 0 \), and let \( G \) be a finite group. A local \( G \)-action is a faithful and \( k \)-linear action \( \phi : G \hookrightarrow \text{Aut}_k(k[[x]]) \) of \( G \) on the ring of formal power series \( k[[x]] \). If such an action exists, then \( G = P \rtimes C \), where \( P \) is a \( p \)-group and \( C \cong \mathbb{Z}/m\mathbb{Z} \) is a cyclic group of order \( m \), with \( (m,p) = 1 \).

The local lifting problem concerns the following question. Given a local \( G \)-action \( \phi \), does there exist a lift of \( \phi \) to an \( R \)-linear action \( \phi_R : G \hookrightarrow R[[x]] \), where \( R \) is a complete discrete valuation ring of characteristic zero with residue field \( k \)? If such a lift exists, we will say \( \phi \) lifts to characteristic zero. See [6] or [5] for a general discussion of the local lifting problem.

In our previous paper [3] we have shown that, for \( G \) the dihedral group of order \( 2p \), every local \( G \)-action can be lifted to characteristic zero. The methods used in [3] apply more generally to the case where the Sylow \( p \)-subgroup \( P \) of \( G \) has order \( p \). In this more general situation not every local \( G \)-action lifts. It is easy to write certain necessary conditions ([3], Proposition 1.3). We already suspected that these conditions are also sufficient ([3], Question 1.4) and reduced the proof of sufficiency to the existence of a certain differential form in characteristic \( p \). This differential form is the deformation datum referred to in the title of the present paper.

Our first new result says that the differential form needed to prove sufficiency always exists. As a consequence, the local lifting problem has now been solved for all groups \( G \) with a Sylow \( p \)-subgroup \( P \) of order \( p \).

Good deformation data. Let \( G = P \rtimes C \), where \( P \) is cyclic of order \( p \) and \( C \) is cyclic of order \( m \) and where \( m \) is prime to \( p \). Choose a generator \( \tau \) of \( P \) and denote by \( \chi : C \to \mathbb{F}_p^\times \) the character such that \( \sigma\tau\sigma^{-1} = \tau^{\chi(\sigma)} \), for \( \sigma \in C \).
Let $\phi : G \hookrightarrow \text{Aut}_k(k[[x]])$ be a local $G$-action. The conductor of $\phi$ is defined as the (positive) integer
\begin{equation}
   h := \text{ord}_x \left( \frac{\phi(\tau)(x)}{x} - 1 \right),
\end{equation}
where $\text{ord}_x(f)$ denotes the order of zero of a power series $f \in k[[x]]$. It is easy to see that $h$ is prime to $p$. We say that the local $G$-action $\phi$ has large conductor if $h > p$ and that it has small conductor if $h < p$.

The results of the present paper concern mainly the case of small conductor. Hence we suppose, for the rest of this Introduction, that $h < p$.

Let $\phi_R : G \hookrightarrow \text{Aut}_R(R[[x]])$ be a lift of $\phi$ to characteristic zero. By a construction going back to [7] (see also [8] and [3]), we can associate to $\phi_R$ a differential form $\omega = f(z) \, dz$ over a rational function field $k(z)$ with the following properties:

- $\omega$ is logarithmic, i.e. of the form $\omega = \frac{dg}{g}$, with $g \in k(z)$.
- $\omega$ has a single zero of order $h - 1$.
- There is a faithful action $C \hookrightarrow \text{Aut}_k(k(z))$ such that $\sigma^* \omega = \chi(\sigma) \cdot \omega$, for $\sigma \in C$.

A differential form $\omega$ with these properties is called a good deformation datum with conductor $h$. (Note that this definition depends on the character $\chi$, which we regard as fixed.)

Conversely, a good deformation datum $\omega$ as above essentially determines a lift of $\phi$ to characteristic zero. In particular, a local $G$-action $\phi$ lifts to characteristic zero if and only if there exists a good deformation datum with the same conductor $h$.

In Section 1 we give necessary conditions for the existence of a good deformation datum with given conductor (Proposition 1.3). Then we show that these conditions are also sufficient, at least for small conductor (Proposition 1.4). In Section 2 we show that these two results give a complete solution to the lifting problem for groups of the form $G = P \rtimes C$, with $|P| = p$.

**Belyi morphisms.** Let us assume, for simplicity, that $m = 1$ in the situation considered above. Let $\omega = f(z) \, dz$ be a good deformation datum with conductor $h$. After a change of coordinate, we may assume that the unique zero of $\omega$ is located at $z = \infty$. Let $z = z_1, \ldots, z = z_r$ be the positions of the poles of $\omega$. Since $\omega$ is logarithmic, it has at most simple poles. Therefore, $r = h + 1$. Moreover, the residue
\[ a_i := \text{Res}_{z=z_i}(\omega) \]
is an element of $\mathbb{F}_p$. Note that $\sum_i a_i = 0$ by the residue theorem. We call the tuple $a = (a_1, \ldots, a_r)$ the type of $\omega$.

In Sections 3 to 6 we consider the following problem: given a tuple $a = (a_1, \ldots, a_r) \in (\mathbb{F}_p^*)^r$ with $\sum_i a_i = 0$, does there exist a good deformation datum $\omega$ of type $a$? This is a refined version of the problem discussed above, where we only fixed the conductor $h$.

Given $a = (a_1, \ldots, a_r)$ as above, it is easy to write a system of algebraic equations whose solutions correspond to good deformation data of type $a$. So far, most attempts to construct good deformation data consisted in trying to solve these equations. For instance, [3], Theorem 5.6, relies on the mysterious fact that the
system of equations corresponding to a particular type \( a \) has a unique solution. The proof of this fact given in [3] is quite complicated and offers no explanation as to why this type \( a \) works and others do not.

In this paper we follow a different path. Consider a good deformation datum \( \omega \) of type \( a = (a_1, \ldots, a_r) \). Then to every choice of lifts \( A_i \in \mathbb{Z} \) of \( a_i \) such that \( \sum_i A_i = 0 \) one can associate an essentially unique rational function \( g \in k(z) \) with the following properties:

- \( \omega = dg/g \),
- \( g \) has exactly \( r \) zeroes/poles, of order \( A_1, \ldots, A_r \), and
- \( g : \mathbb{P}^1_k \to \mathbb{P}^1_k \) is branched exactly over 0, 1 and \( \infty \). The fiber \( g^{-1}(1) \) contains a unique ramification point, with ramification index \( h = r - 1 \).

If, moreover, \( \omega \) has small conductor \( h < p \), then \( g \) is at most tamely ramified. It follows from a theorem of Grothendieck that \( g \) is the reduction modulo \( p \) of a Belyi map, i.e. a rational function \( f : \mathbb{P}^1 \rightarrow \mathbb{P}^1 \) with exactly three critical values 0, 1, \( \infty \). The ramification structure of \( f \) is the same as that of \( g \); in particular, it is completely determined by the tuple \( A = (A_1, \ldots, A_r) \). We say that \( f \) is a Belyi map of type \( A \).

Our new method consists of choosing a suitable lift \( A \) of \( a \) and to construct a Belyi map \( f \) of type \( A \). One then obtains a good deformation datum \( \omega = dg/g \) from the reduction of \( g \) of \( f \) modulo \( p \). Whether this is possible or not for a particular type \( a \) can be easily decided, thanks to Lemma 5.2 which gives a necessary and sufficient condition. This lemma, which is not as well known as it should be, has been discovered independently by several authors ([1], [12]).

The lemma, combined with Grothendieck’s theory of lifting and reduction of tamely ramified coverings, immediately gives necessary and sufficient conditions for the existence of good deformation data of a given type \( a \), in the case where \( m = 1 \). See Corollary 4.2 and Theorem 4.5.

One can adapt the method described above to the case \( m = 2 \) and hence obtain almost complete results in this case as well. This is done in Section 6.

It is not clear how to adapt the method to the case \( m > 2 \). However, one can still use the case \( m = 1 \) to obtain nonexistence results for good deformation data with arbitrary \( m \). It seems that all nonexistence results that have been documented in the literature so far can be explained in this way.

## 1. Good deformation data

Let \( k \) be an algebraically closed field of characteristic \( p > 0 \). We let \( K = k(z) \) denote the rational function field over \( k \), which we regard as the function field of the projective line \( X = \mathbb{P}^1_k \).

Let \( m \geq 1 \) be a positive integer which is prime to \( p \). We choose, once and for all, a primitive \( m \)th root of unity \( \zeta_m \in k^\times \). We denote by \( \sigma : X \rightarrow X \) the automorphism of order \( m \) such that \( \sigma^* z = \zeta_m z \).

**Definition 1.1.** A deformation datum is a differential form \( \omega = f(z) \, dz \in \Omega^1_{K/k} \) with the following properties:

(a) \( \omega \) is an eigenvector for \( \sigma \), i.e.

\[ \sigma^* \omega = \zeta_m \omega, \]
for some \( c \in \mathbb{Z} \), and
\( (b) \) \( \omega \) is logarithmic, i.e. \( \omega = \frac{dg}{g} \), for some \( g \in K^\times \).

A deformation datum \( \omega \) is called primitive if the integer \( c \) in (a) is prime to \( m \). It is called good if it has a unique zero, i.e. there exists a unique point \( x \in X \) with \( \text{ord}_x \omega > 0 \). If this is the case, then the integer
\[
  h := \text{ord}_x \omega + 1
\]
is called the conductor of \( \omega \).

We remark that in our previous papers the definition of the term ‘deformation datum’ is more general. Deformation data occur naturally in a variety of contexts; see e.g. [4], [2]. Here we focus on applications to the local lifting problem, as explained in the Introduction. To save paper we have chosen a more restricted setup from the start, suitable for the applications we have in mind.

The present paper is concerned with the following problem.

**Problem 1.2.** For which \( m \) and \( h \) does there exist a good deformation datum \( \omega \) of conductor \( h \)?

The following proposition gives necessary conditions on \( h \) and \( m \).

**Proposition 1.3.** Fix positive integers \( m \) and \( h \) and assume that there exists a good deformation datum \( \omega \) of conductor \( h \). Then the following holds:

(i) The conductor \( h \) is prime to \( p \).

(ii) \( \omega \) is primitive if and only if \( h \) is prime to \( m \). If this is the case, then
\[
  m \mid (p-1)
\]
(and hence \( \zeta_m \in \mathbb{F}_p^\times \) and
\[
  h \equiv -1 \pmod{m}.
\]

(iii) If \( \omega \) is not primitive, then \( m \mid h \) and \( \sigma^* \omega = \omega \) (i.e. \( c \equiv 0 \pmod{m} \)) in Definition 1.1 (a)).

This is a special case of [3], Lemma 3.3(v). A special case of (ii) can be found in [9], §I.1. For convenience, we recall the proof.

**Proof.** Let \( x \in X \) be the unique zero of \( \omega \). Choose a local coordinate \( w \in k(z) \) at \( x \) and a function \( g \in k(z) \) such that \( \omega = \frac{dg}{g} \). By multiplying \( g \) with a \( p \)th power, if necessary, we can achieve that \( g(x) = 1 \). Writing \( g \) as a power series in \( w \) and computing \( \omega = \frac{dg}{g} \), one sees that \( h = \text{ord}_x \omega + 1 \not\equiv 0 \pmod{p} \). This proves (i).

The statements (ii) and (iii) are trivial for \( m = 1 \). We may therefore assume \( m > 1 \). Since the automorphism \( \sigma : X \to X \) has order \( m \), it has exactly two fixed points, namely \( z = 0 \) and \( z = \infty \). The unique zero \( x \) of \( \omega \) is clearly fixed by \( \sigma \).

Replacing the coordinate \( z \) by \( z^{-1} \), if necessary, we may assume that \( x \) is the point \( z = \infty \) and that \( w = z^{-1} \). Now \( \sigma^* w = \zeta^{-1}_m w \), and condition (a) of Definition 1.1 implies
\[
  h = \text{ord}_z(\omega) + 1 \equiv -c \pmod{m}.
\]
In particular, \( \omega \) is primitive if and only if \( h \) is prime to \( m \).

The same argument used to prove (2) shows that
\[
  \text{ord}_{z=0}(\omega) + 1 \equiv c \pmod{m}.
\]
But \( \text{ord}_x(\omega) \) is either equal to \(-1\) or to 0. In the first case, \( c \) and \( h \) are divisible by \( m \); this corresponds to part (iii) of the proposition. In the second case, \( c \equiv 1 \pmod{m} \), \( h \equiv -1 \pmod{m} \) and \( \omega \) is primitive. This corresponds to part (ii) of the proposition.

It remains to prove that \( m|(p-1) \) in the second case. Let \( z = z_1 \) be a pole of \( \omega \) and set \( a_1 := \text{Res}_{z=z_1}(\omega) \). Set \( z_2 := \sigma(z_1) = \zeta_m z_1 \). Condition (a) of Definition 1.1 together with the congruence \( c \equiv 1 \pmod{m} \), implies that
\[
a_2 := \text{Res}_{z=z_2}(\omega) = \zeta_m^{-1} a_1.
\]
Since \( \omega \) is logarithmic, the residues \( a_1, a_2 \) actually lie in \( \mathbb{F}_p^\times \) (see Lemma 1.5 below). Therefore, \( \zeta_m \in \mathbb{F}_p^\times \), which is equivalent to \( m|(p-1) \). This finishes the proof of the proposition.

The next result says that the necessary conditions given by Proposition 1.3 are also sufficient, at least if \( h < p \). To keep the statement simple, we first deal with the case \( m|h \) (the nonprimitive case). Here one can immediately write a good deformation datum of conductor \( h \) (see also [8], §3.5):
\[
(4) \quad \omega := \frac{h \, dz}{z^{h+1} - z} = \frac{dg}{g}, \quad \text{with } g := (z^h - 1)/z^h.
\]
It therefore suffices to consider the primitive case (part (ii) of Proposition 1.3).

**Proposition 1.4.** Assume \( m|(p-1) \) and let \( h \) be a positive integer with
\[
h < p \quad \text{and} \quad h \equiv -1 \pmod{m}.
\]
Then there exists a good deformation datum with conductor \( h \).

The proof of the proposition is based on the following well-known lemma.

**Lemma 1.5.** Let \( \omega = f(z) \, dz \in \Omega^1_{K/k} \) be a meromorphic differential form on \( X = \mathbb{P}^1_k \). Then \( \omega \) is logarithmic if and only
\[
\text{ord}_x \omega \geq -1 \quad \text{and} \quad \text{Res}_x \omega \in \mathbb{F}_p,
\]
for all \( x \in X \).

**Proof.** Let \( x_1, \ldots, x_r \) be the set of poles of \( \omega \) and set \( a_i := \text{Res}_{x_i} \omega \). After a change of coordinates we may assume that \( x_i \neq \infty \); then the point \( x_i \in X \) is defined by \( z = z_i \), for some \( z_i \in k \).

Now suppose that \( \omega \) has at most simple poles and that \( a_i \in \mathbb{F}_p^\times \), for all \( i \). Choose a lift \( A_i \in \mathbb{Z} \) of \( a_i \). Then
\[
\omega = \sum_{i=1}^r \frac{a_i \, dz}{z - z_i} = \frac{dg}{g},
\]
with
\[
g := \prod_{i=1}^r (z - z_i)^{A_i}.
\]
This shows one direction of the claimed equivalence. The other direction is obvious.

**Proof of Proposition 1.4.** We fix integers \( m \) and \( h \), with \( m \geq 1 \), \( m|(p-1) \), \( 0 < h < p \) and \( h \equiv -1 \pmod{m} \). If \( m = 1 \), then \( m|h \); therefore the existence of the deformation datum already follows from [4]. Assume therefore that \( m > 1 \),
and write \( h = mr - 1 \). The condition \( h < p \) ensures that there exist elements \( z_1, \ldots, z_r \in \mathbb{F}_p^\times \) such that

\[
z_{i,j} := \zeta_m^j z_i \in \mathbb{F}_p^\times, \quad i = 1, \ldots, r, j = 0, \ldots, m - 1,
\]

are pairwise distinct. (Here we use that we excluded the case \( m = 1 \) and \( h = p - 1 \). Define

\[
\sigma := \prod_{i,j} (z^m - z_i^m).
\]

We claim that \( \sigma \) is a good deformation datum of conductor \( h \).

By construction, we have \( \sigma^* \omega = \zeta_m \omega \), where \( \sigma \) is the automorphism of \( X \) with \( \sigma^* z = \zeta_m z \). Furthermore, \( \omega \) has exactly \( mr \) simple poles and no zeroes on \( \mathbb{A}_k^1 \subset X \).

It follows that \( \omega \) has a zero of order \( h = mr - 1 \) at \( \infty \). Finally, the residues of \( \omega \) all lie in \( \mathbb{F}_p \). Therefore, \( \omega \) is logarithmic by Lemma 1.5. This proves the claim and finishes the proof of Proposition 1.4. \( \square \)

2. Applications to the lifting problem

Despite its simple proof, Proposition 1.4 has a nontrivial application to the local lifting problem, as already mentioned in the Introduction.

First some notation. Let \( P = (\tau) \cong \mathbb{Z}/p\mathbb{Z} \) be cyclic of order \( p \), with generator \( \tau \), and \( C = (\sigma) \cong \mathbb{Z}/m\mathbb{Z} \) be cyclic of order \( m \), with generator \( \sigma \). Let \( \chi : C \to (\mathbb{Z}/p\mathbb{Z})^\times \) be a character and \( G := P \rtimes C \) be the corresponding semi-direct product (such that \( \sigma \tau \sigma^{-1} = \tau^{\chi(\sigma)} \), for \( \sigma \in C \)). Let \( \phi : G \to \text{Aut}_k(k[[x]]) \) be a local \( G \)-action. The conductor of \( \phi \) is defined as the positive integer

\[
h := \text{ord}_x \left( \frac{\phi(\tau)(x)}{x} - 1 \right)
\]

(compare with (1)). Standard arguments from the theory of local fields give the following restrictions on the conductor \( h \) (see [3]). First, \( h \) is prime to \( p \). Second, the order of \( h \) in \( \mathbb{Z}/m\mathbb{Z} \) is equal to the order of the character \( \chi \) (equivalently, \( \chi = \chi_h^0 \), where \( \chi_0 : C \to K^\times \) is a primitive character of order \( m \)). Conversely, if \( h \) is a positive integer satisfying these two conditions, then there exists a local \( G \)-action with conductor \( h \).

However, not every local \( G \)-action lifts to characteristic zero. The following theorem gives a necessary and sufficient condition.

**Theorem 2.1.** Let \( \phi : G \to \text{Aut}_k(k[[x]]) \) be a local \( G \)-action, where \( G = P \rtimes C \) is the semi-direct product of a cyclic group \( P \) of order \( p \) and a cyclic group \( C \) of order \( m \), with \((m,p) = 1\). Let \( h \) be the conductor of \( \phi \). Then \( \phi \) lifts to characteristic zero if and only if the following two conditions hold:

(i) The character \( \chi : C \to (\mathbb{Z}/p\mathbb{Z})^\times \) is either trivial or injective. (Equivalently, the conductor \( h \) is either divisible by \( m \) or prime to \( m \)).

(ii) If \( \chi \) is injective, then the congruence \( h \equiv -1 \pmod{m} \) holds.

There are two cases in which conditions (i) and (ii) are automatically true. The first case is when the character \( \chi \) is trivial, i.e. when \( m|h \). Then \( G \) is a cyclic group of order \( pm \), and Theorem 2.1 says that every local \( G \)-action lifts to characteristic zero. We recover a result from [11]. See also [6].
The second case is when $m = 2$ and $\chi$ is not trivial (or equivalently, $h$ is odd). Then $G$ is the dihedral group of order $2p$. Again, conditions (i) and (ii) are automatically verified, and Theorem 2.1 says that every local $G$-action lifts to characteristic zero. This is the main result of [3].

In all other cases (i.e. for $m > 2$ and $m \nmid h$) the congruence $h \equiv -1 \pmod{m}$ is strictly stronger than the condition that $h$ is prime to $m$ (i.e. that $\chi$ is injective). This means that not every local $G$-action lifts to characteristic zero.

**Proof of Theorem 2.1.** Having Proposition 1.4 available, the theorem is a straightforward consequence of the methods of [3]. We only sketch the argument.

By [3], Corollary 3.7, liftability of $\phi$ is equivalent to the existence of a Hurwitz tree of type $(C, \chi)$, conductor $h$ and discriminant $\delta = 0$. Hence the necessity of conditions (i) and (ii) of Theorem 2.1 follows from [3], Lemma 3.3(v).

To prove sufficiency of conditions (i) and (ii), it is natural to distinguish the case of small conductor ($h < p$) from the case of large conductor ($h > p$).

Suppose first that $h < p$. By [7], Theorem III.3.1, a Hurwitz tree of conductor $h < p$ is irreducible, i.e. it is the same thing as a good deformation datum of conductor $h$. Therefore, the sufficiency of conditions (i) and (ii) follows from Proposition 1.4 (and necessity follows directly from Proposition 1.3).

If $h > p$, there may not exist a good deformation datum of conductor $h$. However, one can easily construct a (not necessarily irreducible) Hurwitz tree of type $(C, \chi)$, conductor $h$ and discriminant $\delta = 0$, by adapting the proof of [3], Theorem 4.3 (which deals with the case $m = 2$ and $h > p$ odd) to the more general situation considered here. This completes the proof of Theorem 2.1. □

3. The type

In the rest of this paper, we only consider primitive deformation data.

We fix $m \geq 1$ as in Section 1. Let $\omega = f(z)\, dz$ be a good and primitive deformation datum. After a change of coordinate, we may assume that the unique zero $x$ of $\omega$ is located at the point $z = \infty$ (see the proof of Proposition 1.3). This assumption allows us to identify the points different from $x$ with elements of the field $k$.

Choose a system of representatives $z_1, \ldots, z_r$ of the $\sigma$-orbits of the set of poles of $\omega$. By Lemma 1.5 we have

$$a_i := \text{Res}_{z_i} \omega \in \mathbb{F}_p^\times.$$ 

The tuple $a := (a_1, \ldots, a_r)$ is called the type of $\omega$.

Condition (a) of Definition 1.1 implies that $\omega$ has poles in $z_{i,j} := \zeta_m^j z_i$ and that

$$a_{i,j} := \text{Res}_{z_{i,j}} \omega = \zeta_m^{-jc} a_i, \quad j = 0, \ldots, m - 1,$$

for some $c \in \mathbb{Z}$, prime to $m$. It follows that the points $z_{i,j}$ are pairwise distinct. In particular, if $m > 1$, then $z_{i,j} \in k^\times$.

By the residue theorem we have

$$\sum_{i,j} a_{i,j} = \left( \sum_{i=1}^r a_i \right) \cdot \left( \sum_{j=0}^{m-1} \zeta_m^j \right) = 0. \quad (5)$$

If $m > 1$, then the second sum is zero, and condition (5) coming from the residue theorem is empty.
Definition 3.1. Let $r \geq 2$ be an integer such that $h := mr - 1 \not\equiv 0 \pmod{p}$. A type of length $r$ is an $r$-tuple $a = (a_1, \ldots, a_r)$ with $a_i \in \mathbb{F}_p^\times$. If $m = 1$, then we demand that $\sum a_i = 0$. Two types $a = (a_i)$ and $a' = (a'_i)$ of length $r$ are equivalent if there exists $\pi \in S_r$ and $c_i \in (\mathbb{Z}/m\mathbb{Z})^\times$ with $a'_i = \zeta_m^{c_i} a_{\pi(i)}$, for $i = 1, \ldots, r$.

So the type of a deformation datum $\omega$ is well defined, up to equivalence. We can now formulate a refined version of Problem 1.2

Problem 3.2. Let $a = (a_1, \ldots, a_r)$ be a type. Does there exist a good deformation datum $\omega$ of type $a$?

Let $a = (a_1, \ldots, a_r)$ be a type. Choose elements $z_1, \ldots, z_r \in k^\times$ such that the elements $z_{i,j} := \zeta_m^j z_i \in k^\times$ are pairwise distinct, for $i = 1, \ldots, r$ and $j = 0, \ldots, m - 1$. Set

$$\omega := \sum_{i=1}^r m a_i z_i^{m-1} \frac{dz}{z^m - z_i^m}.$$ 

This is clearly a differential form with at most simple poles in the points $z_{i,j}$ satisfying $\sigma^* \omega = \zeta_m^j \omega$ (condition (a) of Definition 1.1). A short computation shows that

$$\text{Res}_{z_{i,j}} \omega = \zeta_m^{-j} a_i \in \mathbb{F}_p^\times.$$ 

By Lemma 1.5, $\omega$ is logarithmic (condition (b) of Definition 1.1). Therefore, $\omega$ is a deformation datum of type $a$. It is uniquely determined by the choice of the poles $z_i$.

For which choice of $z_1, \ldots, z_r$ is $\omega$ a good deformation datum? One can rewrite

$$\omega = \frac{q(z) \, dz}{\prod_i (z^m - z_i^m)},$$ 

where $q(z) \in k[z]$ is a polynomial of degree at most $h = mr - 1$ whose coefficients are polynomials in the $z_i$. The deformation datum $\omega$ is good if and only if $q(z)$ is a constant. Setting the nonconstant coefficients of $q(z)$ to zero, we obtain a system of polynomial equations in the unknown $z_i$ whose solutions correspond to good deformation data of type $a$. So far, most attempts to construct good deformation data were based on explicitly solving these equations.

In the remaining sections we suggest another approach to Problem 3.2

4. A NECESSARY CONDITION

In this section we assume $m = 1$. We formulate a necessary condition on a given type $a$ for the existence of good deformation data of type $a$ (Corollary 1.2). We then state our main result (Theorem 4.5) which says that this condition is sufficient for large prime $p$. The proof is given in the following section.

Let $\omega$ be a good deformation datum of type $a = (a_1, \ldots, a_r)$. We may assume that the point $z = \infty$ is the unique zero of $\omega$. Then

$$\omega = \sum_{i=1}^r a_i \frac{dz}{z - z_i},$$ 

with $z_1, \ldots, z_r \in k$; see the proof of Lemma 1.5. Note that $\sum a_i = 0$ and that the conductor of $\omega$ is $h = r - 1$, which is prime to $p$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
For $i = 1, \ldots, r$, choose a lift $A_i \in \mathbb{Z}$ of $a_i$ such that
\[
\sum_{i=1}^{r} A_i = 0.
\]
We call $\mathbf{A} = (A_1, \ldots, A_r)$ a lift of the type $\mathbf{a}$. Then the rational function
\[
g := \prod_{i=1}^{r} (z - z_i)^{A_i}
\]
has the property that $g = \frac{d\omega}{\omega}$.

We consider $g$ as a morphism $g : \mathbb{P}^1_k \to \mathbb{P}^1_k$. Let $I \subset \{1, \ldots, r\}$ be the subset of indices $i$ with $A_i > 0$. Note that the degree of $g$ is equal to
\[
\sum_{i \in I} A_i = -\sum_{i \notin I} A_i = \max(A_i, 0).
\]

**Proposition 4.1.** The morphism $g : \mathbb{P}^1_k \to \mathbb{P}^1_k$ is branched exactly above $0, 1, \infty$. More precisely:

(i) $g$ is ramified at the point $z_i$, with ramification index $|A_i|$. Note that $g(z_i) = 0$ if $i \in I$ and $g(z_i) = \infty$ otherwise.

(ii) $g$ is ramified at $\infty$, with ramification index $\geq \min(h, p)$. It is tamely ramified at $\infty$ if and only if the ramification index is equal to $h$. Note that $g(\infty) = 1$.

(iii) $g$ is unramified at all other points.

In particular, if $h < p$, then $g$ is tamely ramified everywhere.

**Proof.** Claim (i) is clear from the definition of $g$. Since $\omega$ is good and $g(\infty) = 1$, the differential form $dg = g\omega$ has a zero at $\infty$ of order $h - 1 = r - 2$ and no zero or pole on $A_k^1 - \{z_1, \ldots, z_r\}$. Claim (iii) follows immediately; claim (ii) as well, but one has to use the fact that the conductor $h$ is prime to $p$. \qed

Given a lifted type $\mathbf{A} = (A_1, \ldots, A_r)$, we set
\[
n_{\mathbf{A}} := \sum_{i=1}^{r} \max(A_i, 0), \quad k_{\mathbf{A}} := \gcd(A_1, \ldots, A_r),
\]
where we make the assumption that $k_{\mathbf{A}} > 0$.

**Corollary 4.2.** Let $\omega$ be a good deformation datum of type $\mathbf{a} = (a_1, \ldots, a_r)$ (with $m = 1$). Then for every lift $\mathbf{A} = (A_1, \ldots, A_r)$ of $\mathbf{a}$ we have
\[
k_{\mathbf{A}} \cdot \min(r - 1, p) \leq n_{\mathbf{A}}.
\]

**Proof.** Let $\mathbf{A} = (A_1, \ldots, A_r)$ be a lift of $\mathbf{a}$ and $k := k_{\mathbf{A}}$. Then $\mathbf{A}' := (A_1/k, \ldots, A_r/k)$ is a lift of $\mathbf{a}' := (a_1/k, \ldots, a_r/k)$ with $n_{\mathbf{A}'} = n_{\mathbf{A}}/k$ and $k_{\mathbf{A}'} = 1$. Moreover, $\omega' := k^{-1}\omega$ is a good deformation datum of type $\mathbf{a}'$. We may therefore assume that $k_{\mathbf{A}} = 1$.

Let $g : \mathbb{P}^1_k \to \mathbb{P}^1_k$ be the rational function associated to $\omega$ and $\mathbf{A}$ by (6). The degree of $g$ is equal to $n_{\mathbf{A}}$ and, by Proposition 4.1 (ii), the ramification index of $g$ at $\infty$ is $\geq \min(r - 1, p)$. The inequality $\min(r - 1, p) \leq n_{\mathbf{A}}$ follows immediately. \qed
Example 4.3. Let $r \geq 4$ be even and $p > r/2$ be a prime. Let 
\[
\mathbf{a} := (1, \ldots, 1, -1, \ldots, -1).
\]
Then $k_{\mathbf{A}} = 1$ and $n_{\mathbf{A}} = r/2 < \min(p, r - 1)$, for the obvious lift $\mathbf{A}$. So Corollary 4.2 implies that there does not exist a good deformation datum of type $\mathbf{a}$.

The special case $p = 5$ and $r = 4$ had been suggested to us by D. Harbater in connection with the lifting problem.

For $p = 3$ and $r = 6$, there does exists a one-parameter family of good deformation data of type $\mathbf{a}$. This shows that the bound in Corollary 4.2 is sharp, in some sense.

Example 4.4. Let $s \geq 3$ and $1 \leq \alpha < s$ be integers and $p > s$ be a prime. Set 
\[
r := s + 2 \quad \text{and} \quad \mathbf{a} := (\alpha - s, 1, \ldots, 1, -\alpha, \ldots, -\alpha) \quad \text{s times}.
\]

Then $k_{\mathbf{A}} = 1$ and $n_{\mathbf{A}} = s < \min(r - 1, p)$ for the obvious lift $\mathbf{A}$. Again, Corollary 4.2 shows that there does not exist a good deformation datum of type $\mathbf{a}$. This result is proved in [7], Example 4.4, by explicit computations.

Here is our main result.

Theorem 4.5. Let $\mathbf{a} = (a_1, \ldots, a_r)$ be a type (with $m = 1$). Suppose that there exists a lift $\mathbf{A}$ of $\mathbf{a}$ such that 
\[
k_{\mathbf{A}} \cdot (r - 1) \leq n_{\mathbf{A}} < k_{\mathbf{A}} \cdot p.
\]
Then there exists a good deformation datum of type $\mathbf{a}$.

The proof of Theorem 4.5 is given at the end of the following section. It is based on the idea, explained in the Introduction, of constructing good deformation data from the reduction modulo $p$ of suitable Belyi maps.

5. Good deformation data from Belyi maps

We keep that assumption that $m = 1$. A Belyi morphism is a finite morphism $f : Y \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$, where $Y$ is a smooth projective curve defined over the field $\overline{\mathbb{Q}}$ of algebraic numbers, such that $f$ is branched exactly over the three points 0, 1 and $\infty$.

Belyi morphisms can be described by some purely topological data. For instance, one can describe them by drawing a dessin d’enfant. An equivalent description, more useful for computations, is the following.

Definition 5.1. Fix an integer $n \geq 1$. A generating system of degree $n$ is a triple $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ of permutations $\sigma_i \in S_n$ with the following properties:

- $\sigma_1 \sigma_2 \sigma_3 = 1$ and
- $G := \langle \sigma_1, \sigma_2, \sigma_3 \rangle \subset S_n$ acts transitively on $\{1, \ldots, n\}$.

Two generating systems $\sigma = (\sigma_i)$ and $\sigma' = (\sigma_i')$ are called equivalent if there is a permutation $\tau \in S_n$ such that $\sigma_i' = \tau \sigma_i \tau^{-1}$, for $i = 1, 2, 3$.

The combinatorial type of a generating system $\sigma$ is the triple of conjugacy classes of the elements $\sigma_i$ in $S_n$:
\[
C(\sigma) = (C(\sigma_1), C(\sigma_2), C(\sigma_3)).
\]
By a standard construction (see e.g. [10]), we can associate to a generating system $\sigma$ a Belyi morphism $f : Y \to \mathbb{P}^1_\bar{Q}$. This gives a one-to-one correspondence between equivalence classes of generating systems of degree $n$ and Belyi morphisms of degree $n$.

If $f$ is the Belyi morphism corresponding to the generating system $\sigma$, then the combinatorial type $C(\sigma)$ can be read from the ramification structure of $f$, as follows. Write $(x_1, x_2, x_3) := (0, 1, \infty)$. Let $f^{-1}(x_i) = \{y_1, \ldots, y_{s_i}\}$ be the fiber above $x_i$, and let $e_j$ denote the ramification index of $f$ at the point $y_j$. Then $C(\sigma_i)$ is the conjugacy class of permutations with cycle structure $(e_1, \ldots, e_{s_i})$. Note that we can compute the genus of the curve $Y$ solely from the combinatorial type, using the Riemann–Hurwitz formula.

We say that a triple $C = (C_1, C_2, C_3)$ of conjugacy classes of $S_n$ is realizable if there exists a generating system $\sigma$ with $C = C(\sigma)$. This means that there exists a Belyi morphism of degree $n$ with combinatorial type $C$.

Let $A = (A_1, \ldots, A_r)$ be a lifted type. Let $C(A) = (C_1, C_2, C_3)$ denote the following triple of conjugacy classes of the symmetric group $S_{n_A}$:

\[
C_1 := (A_i \mid i \in I), \quad C_2 := (r - 1), \quad C_3 := (-A_i \mid i \notin I)
\]

(a conjugacy class in $S_n$ is given as a list of natural numbers indicating the length of the cycles of a permutation, and in which the 1s can be omitted). Note that the genus of $C(A)$ is zero.

**Lemma 5.2.** The triple of conjugacy classes $C(A)$ is realizable if and only if the inequality

\[
k_A \cdot (r - 1) \leq n_A
\]

holds. Here $n_A$ and $k_A$ are defined by \([\mathcal{N}]\).

This lemma has been discovered independently, in various forms, by several authors. For instance, it is a special case (the genus-zero case) of a result of Boccara ([1], Théorème 3.2; our Lemma 5.2 corresponds to the case $l = \lambda = h + k - 1$). It has also been proved by Zannier (see [12], proof of Theorem 1. (A)-(E)). In the preprint version of this paper (arXiv:0801.1418), we gave a proof using dessins d’enfants. Since the key step of the proof is similar in spirit to the proof of Zannier, we decided to leave it out of the present version.

**Proof of Theorem 4.5** Let $a = (a_1, \ldots, a_r) \in (\mathbb{F}_p^*)^r$ be a type. Suppose that there exists a lift $A = (A_1, \ldots, A_r)$ such that

\[
k_A \cdot (r - 1) \leq n_A < k_A \cdot p.
\]

We have to show that there exists a good deformation datum $\omega$ of type $a$. Replacing $a$ by $a' := a/k_A$, we may assume that $k_A = 1$ (compare with the proof of Corollary 4.2).

By Lemma 5.2 there exists a Belyi map $f : \mathbb{P}^1_\bar{Q} \to \mathbb{P}^1_\bar{Q}$ of combinatorial type $C(A)$. After a suitable choice of coordinates, we may assume that $f(\infty) = 1$ and that $\infty$ is the unique ramification point above 1 (with ramification index $r - 1$).

Now we have

\[
f = \prod_{i=1}^r (z - z_i)^{A_i},
\]

for certain pairwise distinct algebraic numbers $z_1, \ldots, z_r \in \bar{Q}$.
Let $v$ be a place of $\mathbb{Q}$ above the prime $p$. Let $k$ denote the residue field of $v$. By our hypothesis, the degree of $f$ is $n_A < p$. Therefore, $f$ has good reduction at $v$ by Grothendieck’s theory of the tame fundamental group. In our concrete situation, this means that the algebraic numbers $z_i$ are $v$-integers and that, moreover, the reduction

$$g = \prod_{i=1}^{r}(z - z_i)^{A_i} \in k(z)$$

of $f$ modulo $v$ is at most tamely ramified and branched exactly over $0, 1, \infty$, with the ramification structure identical to that of $f$. It follows that

$$\omega := \frac{dg}{g}$$

is a good deformation datum of type $a$. This proves the theorem. \hfill \Box

6. The case $m = 2$

Now suppose that $m = 2$. Let $p$ be an odd prime and $a = (a_1, \ldots, a_r)$ be a type. A deformation datum of type $a$ is of the form

$$\omega = \sum_{i=1}^{r} \left( \frac{a_i \, dz}{z - z_i} - \frac{a_i \, dz}{z + z_i} \right) = \sum_{i=1}^{r} \frac{2a_i \, z_i \, dz}{z^2 - z_i^2},$$

where $\pm z_i$ are pairwise distinct elements of $k^\times$. We suppose that $\omega$ is good, i.e. that it has a single zero of order $h := 2r - 1$ at $\infty$. Moreover, we assume that $p > h$.

Choose a lift $A = (A_1, \ldots, A_r)$ of $a_i$ with $A_i > 0$, and set

$$g := \prod_{i=1}^{r} \left( \frac{z - z_i}{z + z_i} \right)^{A_i}.$$ 

Then $\omega = dg/g$. Furthermore, we have

$$g(-z) = \prod_{i=1}^{r} \left( \frac{z + z_i}{z - z_i} \right)^{A_i} = \frac{1}{g(z)}.$$ 

Therefore, there exists a rational function $\tilde{g} \in k(x)$ such that

$$\left( \frac{g(-z) - 1}{g(-z) + 1} \right)^2 = \left( \frac{g(z) - 1}{g(z) + 1} \right)^2 = \tilde{g}(z^2).$$

Proposition 6.1. The morphism $\tilde{g} : \mathbb{P}^1_k \to \mathbb{P}^1_k$ has degree

$$n = n_A := \sum_{i=1}^{r} A_i.$$ 

It is at most tamely ramified and branched exactly over $0, 1, \infty$. More precisely:

(i) The fiber $\tilde{g}^{-1}(1)$ consists of the points $x = z_i^2$, for $i = 1, \ldots, r$. The ramification index of $\tilde{g}$ at the point $x = z_i^2$ is equal to $A_i$.

(ii) Suppose that $n$ is even. Then the fiber $\tilde{g}^{-1}(0)$ consists of the point $x = \infty$ with ramification index $h = 2r - 1$, of the point $x = 0$ with ramification index $1$, and of $(n - 2r)/2$ points with ramification index $2$. The fiber $\tilde{g}^{-1}(\infty)$ consists of $n/2$ points with ramification index $2$. 

(iii) Suppose that $n$ is odd. Then the fiber $\tilde{g}^{-1}(0)$ consists of the point $x = \infty$ with ramification index $h = 2r-1$ and of $(n-2r+1)/2$ points with ramification index 2. The fiber $\tilde{g}^{-1}(\infty)$ consists of the point $x = 0$, which is unramified, and of $(n-1)/2$ points with ramification index 2.

Proof. We have a commutative diagram

\[
\begin{array}{ccc}
P^1 & \overset{\psi}{\longrightarrow} & P^1 \\
g \downarrow & & \downarrow \tilde{g} \\
P^1 & \overset{\phi}{\longrightarrow} & P^1,
\end{array}
\]

where $\psi(z) = z^2 = x$ and $\phi(v) = ((v-1)/(v+1))^2 = u$. In particular, $\phi(0) = \phi(\infty) = 1$, $\phi(1) = 0$ and $\phi(-1) = \infty$. So

$$\tilde{g}^{-1}(1) = \psi(g^{-1}(0) \cup g^{-1}(\infty)) = \{z_1^2, \ldots, z_r^2\}.$$ 

Moreover, since $g$ is ramified at $z = \pm z_i$ of order $A_i$ (Lemma 1.5) and $\psi$ is unramified at $z = \pm z_i$, we see that the ramification index of $\tilde{g}^{-1}$ at $x = z_i^2$ is equal to $A_i$. This proves (i).

One proves (ii) and (iii) in the same manner. The case distinction comes from

$$g(0) = (-1)^n \Rightarrow \tilde{g}(0) = \begin{cases} 
0, & \text{if } n \text{ is even}, \\
\infty, & \text{if } n \text{ is odd}.
\end{cases}$$

\[\square\]

Let $A = (A_1, \ldots, A_r)$ be a lift of $a$ with $A_i > 0$. Set $C(A) = (C_1, C_2, C_3)$, where

$$C_1 := (2r-1, \overbrace{2, \ldots, 2}^{\lfloor(n-2r+1)/2\rfloor}), \quad C_2 := (A_1, \ldots, A_r), \quad C_3 := (2, \ldots, 2)^{\lceil n/2 \rceil}$$

are conjugacy classes in $S_{nA}$. With this notation, we have obtained the following version of Corollary 1.2 and Theorem 1.5 for $m = 2$.

**Theorem 6.2.** Let $a$ be a type, with $m = 2$ and $p > h = 2r-1$.

(i) If there exists a good deformation datum $\omega$ of type $a$, then the triple of conjugacy classes $C(A)$ is realizable, for every lift $A$ of $a$.

(ii) Suppose that there exists a lift $A$ of $a$ such that

(a) $C(A)$ is realizable, and

(b) $n_A < p$.

Then there exists a good deformation datum $\omega$ of type $a$.

We have not tried to find an explicit criterion for realizability in the above situation (such as Lemma 5.3). Instead, we give an example:

**Example 6.3.** For an arbitrary $r \geq 1$, set $m := 2$ and

$$A := (1, \ldots, 1, r).$$

Then $n = h = 2r-1$ and the triple $C(A)$ consists of the following conjugacy classes in $S_n$: $C_1$ is the class of all $n$-cycles, $C_2$ is the class of $r$-cycles and $C_3$ is the class of the product of $r - 1$ disjoint 2-cycles.
Lemma 6.4. Up to equivalence, there is a unique generating system $\sigma$ of combinatorial type $C(A)$.

Proof. The existence of $\sigma$ follows from the identity

$$(1 \, 2 \ldots n) \cdot (n \, n-2 \ldots 3 \, 1) = (2 \, 3)(4 \, 5)\cdots(n-1 \, n).$$

The proof of the uniqueness is an easy exercise. \qed

One can also convince oneself of the truth of Lemma 6.4 by drawing the corresponding dessin d’enfant. If $f : \mathbb{P}^1 \to \mathbb{P}^1$ is a Belyi map of combinatorial type $C(A)$, with $A$ as above, then the inverse image $T := f^{-1}([1, \infty)) \subset \mathbb{C}$ is a pre-clean plane tree with valency list $(h, 1, \ldots, 1)$ (with $r$ repetitions of 1); see e.g. [10]. It is clear that there is, up to isomorphism, a unique realization of such a tree:

$$\begin{array}{c}
T \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \\
\quad \


Institut fuer Reine Mathematik, University of Ulm, Helmholtzstr 18, D-89069 Ulm, Germany

E-mail address: irene.bouw@uni-ulm.de

Institut fuer Algebra, Zahlentheorie und Diskrete Mathematik, University of Hannover, Welfengarten 1, D-30167, Hannover, Germany

E-mail address: wevers@math.uni-hannover.de

Equipe de theorie des nombres, Université Pierre et Marie Curie (Paris 6), 175, rue du Chevaleret, 75013 Paris, France

E-mail address: zapponi@math.jussieu.fr