WILD MODELS OF CURVES

DINO LORENZINI

ABSTRACT. Let K be a complete discrete valuation field with ring of integers $\mathcal{O}_K$ and algebraically closed residue field k of characteristic $p > 0$. Let X/K be a smooth proper geometrically connected curve of genus $g > 0$, with $X(K) \neq \emptyset$ if $g = 1$. Assume that X/K does not have good reduction, and that it obtains good reduction over a Galois extension L/K of degree p. Let $\mathcal{Y}/\mathcal{O}_L$ be the smooth model of X_L/L. Let $H := \mathrm{Gal}(L/K)$.

In this article, we provide information on the regular model of X/K obtained by desingularizing the wild quotient singularities of the quotient $\mathcal{Y}/H$. The most precise information on the resolution of these quotient singularities is obtained when the special fiber $\mathcal{Y}_k/k$ is ordinary. As a corollary, we are able to produce for each odd prime p an infinite class of wild quotient singularities having pairwise distinct resolution graphs. The information on the regular model of X/K also allows us to gather insight into the p-part of the component group of the Néron model of the Jacobian of X.

KEYWORDS Model of a curve, ordinary curve, cyclic quotient singularity, wild, arithmetical tree, resolution graph, component group, Néron model.

MSC: 14G20 (14G17, 14K15, 14J17)

1. Introduction

Let K be a complete discrete valuation field with valuation v, ring of integers $\mathcal{O}_K$ and residue field k of characteristic $p > 0$, assumed to be *algebraically closed*. Let X/K be a smooth proper geometrically connected curve of genus $g > 0$, with $X(K) \neq \emptyset$ if $g = 1$.

Assume that X/K does not have good reduction, and that it obtains good reduction over a Galois extension L/K. Let $\mathcal{Y}/\mathcal{O}_L$ be the smooth model of X_L/L. Let $H := \mathrm{Gal}(L/K)$ and let $\mathcal{Z}/\mathcal{O}_K$ denote the quotient $\mathcal{Y}/H$. A regular model for X/K can be obtained by resolving the singularities of the scheme $\mathcal{Z}$. Our goal is to obtain information on this regular model when p divides $[L : K]$. Since the presence of wild ramification renders the subject quite challenging, we will restrict our attention in this article to the case where $[L : K] = p$.

Beyond our interest in models of curves *per se*, our motivation for understanding these regular models is two-fold. First, since $\mathcal{X}$ is obtained by desingularizing certain quotient singularities, we hope to gain more insight in the general theory of resolutions of wild quotient singularities by producing interesting classes of examples where the singularities can be resolved explicitly. Second, since from a regular model of the curve one can compute much of the Néron model of its Jacobian, we hope to bring new insight into the structure of the rather mysterious p-part of the component group of the Néron model of a general abelian variety from an increased understanding of the special case of Jacobians of curves.

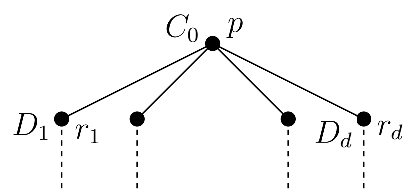
Let us introduce some notation needed to state our theorems. Let σ denote a generator of $H := \mathrm{Gal}(L/K)$. Denote also by σ the automorphism of $\mathcal{Y}_k$ induced by the action of H on $\mathcal{Y}$. The scheme $\mathcal{Z}$ is singular exactly at the images $Q_1, \ldots, Q_d$ of the ramification points $P_1, \ldots, P_d$, of the map $\mathcal{Y}_k \to \mathcal{Y}_k/\langle\sigma\rangle$ (5.2). Consider the regular model $\mathcal{X} \to \mathcal{Z}$

Date: June 6, 2013.

obtained from $\mathcal{Z}$ by a minimal desingularization. Let $\mathcal{X}' \to \mathcal{X}$ denote the regular model of X/K minimal with the property that $\mathcal{X}'_k$ has smooth components and normal crossings. Let f denote the composition $\mathcal{X}' \to \mathcal{Z}$. Let C_0/k denote the strict transform in $\mathcal{X}'$ of the irreducible closed subscheme $\mathcal{Z}_k^{red}$ of $\mathcal{Z}$. Let $D_1, \ldots, D_d$ denote the irreducible components of $\mathcal{X}'_k$ that meet C_0. Let r_i denote the multiplicity of D_i, $i = 1, \ldots, d$, in $\mathcal{X}'_k$.

Recall that to any connected curve $\cup_{\ell=1}^n C_\ell$ on a regular model $\mathcal{X}$ we associate a graph G as follows: the vertices are the irreducible components C_ℓ, and in G the vertices C_i and C_j $(i \neq j)$ are linked by exactly $(C_i \cdot C_j)_{\mathcal{X}}$ edges, where $(C_i \cdot C_j)_{\mathcal{X}}$ denotes the intersection number of C_i and C_j on the regular scheme $\mathcal{X}$. Recall that the *degree* of a vertex v of a graph is the number of edges attached to v. A *node* on a graph is a vertex of degree at least 3. A vertex of degree 1 is a *terminal vertex*. A *chain* is a subgraph of G with vertices $C_0, C_1, \ldots, C_n$, $n \geq 1$, such that C_i is linked to C_{i+1} by exactly one edge in G when $i = 0, \ldots, n-1$, and the degree of C_i is 2 when $i = 1, \ldots, n-1$. If the chain contains a terminal vertex (which can only be C_0 or C_n), the chain is called a *terminal chain*.

Let G denote the graph associated with $\mathcal{X}'_k$. We assume $d \geq 1$. For each $i = 1, \ldots, d$, let G_{Q_i} denote the graph associated with the curve $f^{-1}(Q_i)$. In particular, D_i corresponds to a vertex of G_{Q_i}. We have the following configuration on the graph G (where a positive integer next to a vertex denotes the multiplicity of the corresponding irreducible component in $\mathcal{X}'$).



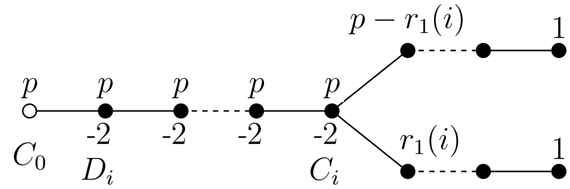
Theorem 5.3. *Let X/K be a curve with potentially good reduction after a wildly ramified extension L/K of degree p, as above. Keep the above notation. Then, for all $i = 1, \ldots, d$, the graph G_{Q_i} contains a node of G, and p divides r_i.*

In contrast, when H is of prime order $q \neq p$, then it is known that $q > r_i$ and that the graph G_{Q_i} does not contain a node of G. In particular, when L/K is tame and $d \geq 3$, the graph G has only a single node, the component C_0 (see, e.g., [14], 2.1).

We propose in 6.1 a combinatorial measure $\gamma_{Q_i} g_{Q_i}$ of the complexity of the graph G_{Q_i}, which we conjecturally relate in 6.2 to the higher ramification data of the morphism $\mathcal{Y}_k \to \mathcal{Y}_k / \langle \sigma \rangle$. This conjectural relationship expresses the fact that the graph G_{Q_i} is 'complicated' only if the higher ramification above Q_i is 'large'. We prove this conjecture in the ordinary case (6.4).

Recall that a smooth proper curve Y/k of genus g is called *ordinary* if its Jacobian J/k is an ordinary abelian variety (that is, $J(k)$ has exactly p^g points of order dividing p). When $\mathcal{Y}_k$ is ordinary, the morphism $\mathcal{Y}_k \to \mathcal{Y}_k / \langle \sigma \rangle$ has the smallest possible ramification data at each Q_i (2.2), and in this case we can use Theorem 5.3 to describe the graph G_{Q_i} explicitly, as in the following theorem, whose statement is slightly strengthened in the version given in section 6. In the graph below, a bullet $\bullet$ represents an irreducible component of the desingularization of Q_i. A negative number next to a vertex is the self-intersection of the component. A positive number next to a vertex is the multiplicity of the corresponding component in $\mathcal{X}'_k$.

Theorem (see 6.8). *Let X/K be a curve with potentially good reduction after a Galois extension L/K of degree p, as above. Assume that $\mathcal{Y}_k$ ordinary. Then, for all $i = 1, \ldots, d$, we have $r_i = p$, and G_{Q_i} is a graph with a single node C_i, of degree 3:*

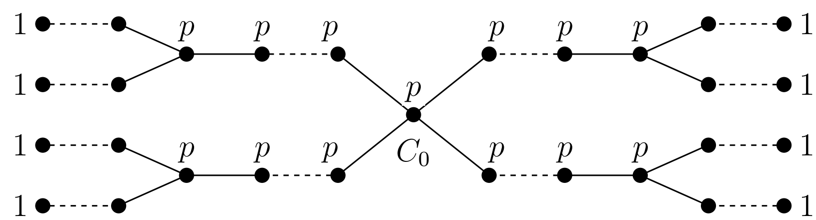


The intersection matrix $N(p, \alpha_i, r_1(i))$ of the resolution of Q_i is uniquely determined as in 4.7 by the two integers α_i and $r_1(i)$, with $1 \leq r_1(i) < p$. The integer α_i denotes the number of vertices of self-intersection -2 (including the node C_i) on the chain in G_{Q_i} connecting the node C_0 to the single node C_i of G_{Q_i}, and the integer α_i is divisible by p.

To further determine the regular model, one would need to determine explicitly the integers α_i and $r_1(i)$. We will address this issue in [20]. In all cases where we have been able to compute α_i and $r_1(i)$, we found them to be related to the valuation of the different of L/K. More precisely, let $(s_{L/K}+1)(p-1)$ denote the valuation of the different of L/K. In [20], 1.1, we present some instances where $\alpha_i = ps_{L/K}$, and $r_1(i) \equiv -s_{L/K}^{-1}$ modulo p. We also show in [20], 4.1, that the singularities Q_i are rational.

Remark 1.1 The same type of intersection matrix, $N(p, \alpha_i, r_1(i))$, also occurs in the resolution of the singularities of the model $\mathcal{Z}$ when X/K has genus $p-1$ and $\mathrm{Jac}(X)/K$ has purely toric reduction after an extension of degree p ([18], 2.2).

Remark 1.2 The special fiber of the model $\mathcal{X}/\mathcal{O}_K$ of X/K in Theorem 6.8 has thus a graph with a central vertex to which d branches are attached, of the form described below, where we picture the case $d = 4$.



Fix any $d > 1$. We establish in 6.8 and 6.13 the existence of some field K of residue characteristic $p > 0$ and of some smooth proper curve X/K with a regular model whose special fiber has a graph of the above type. This is clearly a weak existence result, but our understanding of models in the presence of wild ramification is so limited that even this weak existence result does not follow from the general existence results of Viehweg [30] and Winters [31].

An immediate but surprising corollary to Theorem 6.8 is as follows.

Corollary (see 6.10). *Let X/K be a curve of genus $g > 1$ with potentially good reduction after a Galois extension L/K of degree p, as above. Assume that $\mathcal{Y}_k$ is ordinary. Then $X(K) \neq \emptyset$.*

The information on the regular model of X/K obtained in Theorem 6.8, while incomplete to fully describe the special fiber of the model, suffices to compute several invariants of arithmetical interest. For instance, the set of components of multiplicity 1 on the special fiber of the model is determined, and this information is one of the ingredients needed to apply the method of Chabauty-Coleman to bound the number of $\mathbb{Q}$-rational points on a curve $X/\mathbb{Q}$ using the reduction at a small prime p, as in [21], 1.1. Let A/K denote the Jacobian of A/K, with Néron model $\mathcal{A}/\mathcal{O}_K$ and component group $\Phi_{A/K}$. The information obtained in Theorem 6.8 suffices to compute $\Phi_{A/K}$ and a new canonical subgroup $\Phi^0_{A/K}$ of $\Phi_{A/K}$ that we now define.

1.3 Let A/K be an abelian variety, with Néron model $\mathcal{A}/\mathcal{O}_K$. Let L/K be any finite extension, and let $\mathcal{A}'/\mathcal{O}_L$ denote the Néron model of A_L/L. Denote by

$$\eta : \mathcal{A} \times_{\mathcal{O}_K} \mathcal{O}_L \to \mathcal{A}'$$

the canonical map induced by the functoriality property of Néron models. The special fiber $\mathcal{A}_k$ is an extension of a finite group $\Phi_{A/K}$, called the *group of components*, by the *connected component of zero* $\mathcal{A}^0_k$ of $\mathcal{A}_k$:

$$0 \longrightarrow \mathcal{A}^0_k \longrightarrow \mathcal{A}_k \longrightarrow \Phi_{A/K} \longrightarrow 0.$$

Assume that A_L/L has semi-stable reduction, and consider the natural map $\Phi_{A/K} \to \mathcal{A}'_k/\eta(\mathcal{A}^0_k)$. We let

$$\Phi^0_{A/K} := \mathrm{Ker}(\Phi_{A/K} \longrightarrow \mathcal{A}'_k/\eta(\mathcal{A}^0_k)).$$

The subgroup $\Phi^0_{A/K}$ does not depend on the choice of such an extension L/K, and is functorial in A. Our interest in this subgroup stems from the following conjectures.

When A/K has potentially good reduction and, more generally, when the toric rank of $\mathcal{A}^0_k$ is trivial, we conjecture that the order of the group $\Phi_{A/K}$ is bounded by a constant depending only on the dimension g of A/K ([15], p. 146). This statement is true when A/K is a Jacobian ([15], 2.4), and for the prime-to-p part of $\Phi_{A/K}$ ([16], 2.15). Since $[L : K]^2$ kills the group $\Phi_{A/K}$ when the toric rank of $\mathcal{A}$ is trivial ([11], 1.8), we find that to prove the conjecture that $\Phi_{A/K}$ is bounded by a constant depending only on g, it suffices to prove that the minimal number of generators of $\Phi_{A/K}$ can be bounded by a constant depending on g only. We guess, under the above hypotheses, that $\Phi_{A/K}$ can be generated by $2g$ elements.

Assume now that A/K has potentially good reduction. The p-torsion in $\mathcal{A}'_k$ can always be generated by at most g elements. Thus the above conjecture is proved if the p-part of the kernel $\Phi^0_{A/K}$ can be generated by a number of elements bounded by a constant depending on g only (possibly $2g$). In the ordinary case, where the p-torsion in $\mathcal{A}'_k$ is minimally generated by g elements, one may wonder if $\Phi^0_{A/K}$ can also be generated by g elements. Our next corollary gives some evidence that this latter question may have a positive answer for all abelian varieties with potentially good ordinary reduction.

Let A/K be the Jacobian of a curve X/K with $X(K) \neq \emptyset$. Let $\langle\ ,\ \rangle : \Phi_{A/K} \times \Phi_{A/K} \to \mathbb{Q}/\mathbb{Z}$ denote Grothendieck's pairing. This pairing is non-degenerate ([3], 4.6). Denote by $(\Phi^0_{A/K})^\perp$ the orthogonal of $\Phi^0_{A/K}$ under Grothendieck's pairing.

Corollary (see 6.12). *Let A/K be the Jacobian of a curve X/K of genus $g > 1$ having potentially good ordinary reduction after a Galois extension L/K of degree p, as above. Then $\Phi_{A/K}$ is a $\mathbb{Z}/p\mathbb{Z}$-vector space of dimension $2d-2$, and $\Phi^0_{A/K}$ is a subspace of dimension $d-1$. Moreover, $\Phi^0_{A/K} = (\Phi^0_{A/K})^\perp$.*

It is natural in view of Corollary 6.12 to wonder whether the same result holds for all principally polarized abelian varieties A/K having potentially good ordinary reduction after a Galois extension L/K of degree p. We may also wonder, for any principally polarized abelian variety A/K with potentially good reduction, whether the order of $\Phi^0_{A/K} \cap (\Phi^0_{A/K})^\perp$ can be bounded by a constant depending only on the p-rank of $\mathcal{A}'_k$. We hope to return to these questions in the future.

1.4 Our explicit computation of a regular model of a curve having potentially good ordinary reduction also has an application to quotient singularities. Our current understanding of wild $\mathbb{Z}/p\mathbb{Z}$-quotient singularities of surfaces is quite limited, and few explicit examples are known (see, e.g., [2], [9], for $p = 2$, and [23] for $p = 3$). In contrast to the case of a tame cyclic quotient singularity, where the number of possible resolution graphs is finite once the order of the group is fixed, we show below that for any fixed odd prime p, there are infinitely many graphs that can occur as the resolution graphs of a wild $\mathbb{Z}/p\mathbb{Z}$-quotient singularity, in both mixed characteristic, and in the equicharacteristic case. The analogous result when $p = 2$ is discussed in [19], 4.1.

Corollary 6.14. *Fix any odd prime p. For each integer $m > 0$, there exist a 2-dimensional regular local ring B of equicharacteristic p endowed with an action of $H := \mathbb{Z}/p\mathbb{Z}$, and a 2-dimensional regular local ring B' of mixed characteristic $(0, p)$ endowed with an action of $\mathbb{Z}/p\mathbb{Z}$, such that* $\operatorname{Spec} B^H$ *and* $\operatorname{Spec}(B')^H$ *are singular exactly at their closed point, and the graphs associated with a minimal resolution of* $\operatorname{Spec} B^H$ *and* $\operatorname{Spec}(B')^H$ *have one node and more than m vertices.*

This article is organized as follows. The proof of Theorem 5.3, in section 5, is of a global nature and includes in particular a study of the natural map $\Phi_{A/K} \to \mathcal{A}'_k/\eta(\mathcal{A}^0_k)$. The proof uses two auxiliary results of independent interest. The first result, Proposition 2.5, is discussed in section 2 and is a relation between torsion points in a quotient of two Jacobians. This proposition is one place in our arguments where the tame and wild cases can be seen to differ in an explicit way. The second result, Theorem 3.6, is the main result of section 3, and is a general relation between elements in the component group Φ_M of an arithmetical tree.

Section 4 presents further results of a combinatorial nature on arithmetical trees which are needed in the proof of Theorem 6.8. Section 6 contains the proof of Theorem 6.8 and of its applications. It is my pleasure to thank Qing Liu, Werner Lüktebohmert, and Michel Raynaud, for helpful comments. I also thank the referee for a careful reading of the article.

2. Cyclic morphisms and torsion

Let k be an algebraically closed field of characteristic p. Let $f : D \to C$ be a ramified Galois morphism of smooth connected projective curves over k. Our main result in this section is Proposition 2.5, which will be applied to the case of the quotient morphism $\mathcal{Y}_k \to \mathcal{Y}_k/\langle\sigma\rangle$ in the course of the proof of Theorem 5.3.

2.1 Assume that the Galois group H of f is cyclic of degree q^s, with q prime. Let $P_1, \dots, P_d$ in $D(k)$ be the ramification points. Assume that at each P_i, the morphism is totally ramified, and let $Q_i := f(P_i)$, $i = 1, \dots, d$, be the branch points.

When $q \neq p$, the Riemann-Hurwitz formula is

$$2g(D) - 2 = q^s(2g(C) - 2) + d(q^s - 1). \tag{2.1.1}$$

Moreover, $d \geq 2$. When $g(C) = 0$, this follows immediately from the formula; the general case requires a separate proof.

Assume now that $q = p$. For $P \in D(k)$, let $H_0(P) \supseteq H_1(P) \supseteq \dots$ denote the sequence of higher ramification groups. If P is a ramification point, then $|H_0(P)| = |H_1(P)| = p^s$. Set

$$\delta(P) := \sum_i (|H_i(P)| - 1).$$

Then the *Riemann-Hurwitz formula* is:

$$2g(D) - 2 = p^s(2g(C) - 2) + \sum_{P \in D(k)} \delta(P), \tag{2.1.2}$$

and it may happen that $d = 1$.

2.2 Let $\gamma(D)$ denote the p-rank of D (i.e., the p-rank of $\mathrm{Jac}(D)$). The *Deuring-Shafarevich formula* relates the p-ranks of C and D:

$$\gamma(D) - 1 = p^s(\gamma(C) - 1) + d(p^s - 1). \tag{2.2.1}$$

The curve D is *ordinary* when $\gamma(D) = g(D)$. When D is ordinary, we find, comparing the formulas (2.1.2) and (2.2.1), that $|H_2(P)| = 1$ for all P, and that C is also ordinary. Moreover, when $g(D) > 0$, the equation (2.2.1) shows that $p \leq g(D) + 1$.

When a ramification point P of a Galois morphism $f : D \to C$ is such that $H_2(P) = (0)$, we will say that the morphism is *weakly ramified* at P.

2.3 We record here the following well-known fact (see [8], p. 42, or [28], 1.3, when $K = k(x)$). Let K be a field with $\mathrm{char}(K) = p$. Let $(A, \mathcal{M})$ be a discrete valuation ring with field of fractions K, valuation v_K, and uniformizer π_K. Assume that the residue field k of A is algebraically closed. Let L/K be a cyclic ramified Galois extension of degree p with Galois group H. Let $(B, \mathcal{N})$ denote the integral closure of A in L. Let $H = H_0 \supseteq H_1 \supseteq \dots$ denote the sequence of ramification groups. Then $\sum_{i=0}^{\infty}(|H_i| - 1) = (m + 1)(p - 1)$ for some integer m prime to p.

2.4 Examples of curves with an automorphism of degree p in characteristic p can be given in Artin-Schreier form. Consider the curve $y^p - y = \prod_{i=1}^{d}(x - a_i)^{-n_i}$, where $a_1, \dots, a_s \in k$ are distinct, and the n_i are positive integers coprime to p. The automorphism $y \mapsto y + 1$ has order p. The genus g of the smooth complete curve defined by the above equation is given by the Riemann-Hurwitz formula $2g - 2 = -2p + (p - 1)(\sum_{i=1}^{d}(n_i + 1))$ (see [29], page 8).

The following simple proposition exhibits a key difference between the tame and wild cases.

Proposition 2.5. *Let q be a prime. Let $f : D \to C$ be a ramified cyclic morphism of degree q^s between smooth connected projective curves over k. Let $P_1, \dots, P_d$, $d \geq 2$, denote the ramification points, assumed to be totally ramified. For $i \neq j$, the image ω_{ij} of $P_i - P_j$ in $\mathrm{Jac}(D)/f^*(\mathrm{Jac}(C))$ is of finite order q^s. Let T denote the finite subgroup $\mathrm{Jac}(D)/f^*(\mathrm{Jac}(C))$ generated by $\{\omega_{id},\ i = 1, \dots, d - 1\}$. Then*

(a) *If $q = p$, then T is isomorphic to $(\mathbb{Z}/p^s\mathbb{Z})^{d-1}$, and is generated by $\{\omega_{id},\ i = 1, \dots, d - 1\}$.*
(b) *If $q \neq p$, then T is isomorphic to $(\mathbb{Z}/q^s\mathbb{Z})^{d-2}$, and is generated by $\{\omega_{id},\ i = 1, \dots, d - 2\}$.*

Proof. Let S denote the subgroup of $\mathrm{Div}^0(D)$ with support on the set $\{P_1, \dots, P_d\}$. It is clear that $\{P_i - P_d, i = 1, \dots, d - 1\}$ is a $\mathbb{Z}$-basis for S. Let $S \to T$ denote the natural surjective map. This map factors through S/q^sS, since $q^s(\sum_i b_iP_i) = f^*(\sum_i b_iQ_i)$ with $\sum_i b_iQ_i \in \mathrm{Div}^0(C)$.

Let σ be a generator of $\mathrm{Aut}(D/C)$. Suppose that $\sigma(\mathrm{div}_D(g)) = \mathrm{div}_D(g)$ for some $g \in k(D)^*$. Then $g^\sigma = cg$ for some $c \in k^*$. Since σ has finite order q^s, we find that $c^{q^s} = 1$.

Consider first the case where $q = p$. Then $c = 1$. Thus, $g^\sigma = g$ and $g \in k(C)^*$. Suppose that the divisor $(\sum_i b_iP_i)$ has trivial image in T. Then it is possible to write

$(\sum_i b_iP_i) = f^*(\sum_j R_j) + \mathrm{div}_D(h)$, for some $R_j \in C(k)$ and $h \in k(D)^*$. Then we have $\sigma(\mathrm{div}_D(h)) = \mathrm{div}_D(h)$ and we conclude that $h \in k(C)^*$. Therefore, we have an equality of divisors of the form $(\sum_i b_iP_i) = f^*(E)$ for some $E \in \mathrm{Div}^0(C)$. It follows that $E = \sum_i c_iQ_i$ for some c_i. Hence, the map $S/p^sS \to T$ is an isomorphism, proving Part (a).

Suppose now that $q \neq p$. Fix a primitive q^s-th root ξ of 1. Then $k(D)/k(C)$ is a Kummer extension, generated by the root α of $y^{q^s} - a \in k(C)[y]$ such that $\alpha^\sigma = \xi\alpha$. It is easy to check that for each $i = 0, \ldots, q^s - 1$,

$$\{\beta \in k(D), \beta^\sigma = \xi^i\beta\} = k(C)\alpha^i.$$

The equality $\alpha^\sigma = \xi\alpha$ implies that $\mathrm{div}_D(\alpha)$ can be written as

$$(\sum_{i=1}^{q^s} a_iP_i) + \sum_j c_j(\sum_{i=0}^{q^s-1} \sigma^i(S_j))$$

for some integers a_i and some $S_j \in D(k) \setminus \{P_1, \ldots, P_d\}$. It follows that q^s divides $\sum_{i=1}^{q^s} a_i$ since $\deg(\mathrm{div}_D(\alpha)) = 0$. It follows that the divisor $\sum_j c_j(\sum_{i=0}^{q^s-1} \sigma^i(S_j)) + (\sum_i a_i)P_d$ defines an element in $f^*(\mathrm{Jac}(C))$. Hence, the image ν of $(\sum_i a_iP_i) - (\sum_i a_i)P_d$ in T is trivial. We thus have a map

$$s : S/< q^sS, (\sum_i a_iP_i) - (\sum_i a_i)P_d > \longrightarrow T.$$

Let us note that $(\sum_i a_iP_i) - (\sum_i a_i)P_d \notin q^sS$ because, otherwise, the morphism f given by the Kummer equation $y^{q^s} - a$ would not be totally ramified at $P_1, \ldots, P_d$.

Suppose that the divisor $(\sum_i b_iP_i)$ has trivial image in T. Then it is possible to write $(\sum_i b_iP_i) = f^*(\sum_j R_j) + \mathrm{div}_D(h)$, for some $R_j \in C(k)$ and $h \in k(D)^*$. Then we have $\sigma(\mathrm{div}_D(h)) = \mathrm{div}_D(h)$ and we conclude that $h^\sigma = \xi^ih$ for some $i \in \{0, \ldots, q^s - 1\}$. Therefore, there exists $b \in k(C)^*$ such that $h = b\alpha^i$. Hence, we have an equality of divisors of the form $(\sum_i b_iP_i) = f^*(E) + i[(\sum_i a_iP_i) - (\sum_i a_i)P_d]$ for some $E \in \mathrm{Div}^0(C)$. It follows that $E = \sum_i c_iQ_i$ for some c_i. Hence, the map s is an isomorphism, proving Part (b). □

Corollary 2.6. *Assume that $p \neq 2$. Let D/k be a smooth projective connected hyperelliptic curve of genus g. Denote by τ the hyperelliptic involution. Let σ be an automorphism of order p. Then either σ has a single fixed point, fixed by τ, or it has exactly two fixed points, permuted by τ.*

Proof. The hyperelliptic involution commutes with σ and, hence, it permutes the fixed points $\{P_1, \ldots, P_d\}$. If $d \geq 2$ and two fixed points P_1 and P_2 of σ are fixed by τ, then the divisor class $P_1 - P_2$ is fixed by τ. Proposition 2.5 shows that the class of $P_1 - P_2$ is not trivial and, since $p > 2$, this divisor class is not equal to the class of $-(P_1 - P_2)$. This is a contradiction since τ acts as the $[-1]$-map on $\mathrm{Jac}(D)$. Thus, τ fixes at most one point P_i.

If $d \geq 3$, then we may assume that either $\tau(P_1) = P_2$ and P_3 is fixed, or that $\tau(P_1) = P_2$ and $\tau(P_3) = P_4$. In the first case, we find that $\tau(P_1 - P_3) = (P_2 - P_3) = -(P_1 - P_2) + (P_1 - P_3)$. Using the fact that τ acts as the $[-1]$-map on $\mathrm{Jac}(D)$, we find the relation $-(P_1 - P_3) = -(P_1 - P_2) + (P_1 - P_3)$ in $\mathrm{Jac}(D)$. Looking at this relation in T contradicts Proposition 2.5. The other case is similar and is left to the reader. □

Example 2.7 Assume that $p \neq 2$. Consider a smooth hyperelliptic curve C/k given by an affine equation $y^2 = f(x)$, and let D be its Galois cover given by the equation $z^p - z = x$. The automorphism $\sigma : D \to D$ with $\sigma(z) = z + 1$ has one fixed point P

with $\delta(P) = 3(p-1)$ when $\deg(f)$ is odd, and it has two fixed points P_1 and P_2 with $\delta(P_1) = \delta(P_2) = 2(p-1)$ when $\deg(f)$ is even.

3. Arithmetical trees

Our main result in this section is Proposition 3.6, which will be needed in the proof of Theorem 5.3. This proposition pertains to arithmetical graphs, and we now recall how one associates such an object to any regular model of a curve.

Let X/K be any smooth, proper, geometrically connected, curve of genus g. Let $\mathcal{X}/\mathcal{O}_K$ be a regular model of X/K. Let $\mathcal{X}_k := \sum_{i=1}^{v} r_i C_i$ denote the special fiber of $\mathcal{X}$, where C_i is an irreducible component and r_i is its multiplicity. Let $M := ((C_i \cdot C_j))_{1\le i,j\le v}$ be the associated *intersection matrix*. Denote by G the associated graph. Let ${}^tR := (r_1, \dots, r_v)$, so that $MR = 0$. We call the triple (G, M, R) an *arithmetical graph* (in [13], the additional condition that $\gcd(r_1, \dots, r_v) = 1$ is assumed, and it is $(G, -M, R)$ which is called an arithmetical graph). For the purpose of simplifying the statements of some definitions, we sometimes think of G as a metric space with the natural topology where each edge of G with its two endpoints is homeomorphic to the closed unit interval $[0, 1]$.

Let (G, M, R) be any arithmetical graph on v vertices. Let $M : \mathbb{Z}^v \to \mathbb{Z}^v$ and ${}^tR : \mathbb{Z}^v \to \mathbb{Z}$ be the linear maps associated to the matrices M and R. The *group of components* of (G, M, R) is defined as

$$\Phi_M := \mathrm{Ker}({}^tR)/\mathrm{Im}(M) = (\mathbb{Z}^v/\mathrm{Im}(M))_{\mathrm{tors}}.$$

Motivated by the case of degenerations of curves, we shall denote by $(C, r(C))$ a vertex of G, where $r(C)$ is the coefficient of R corresponding to C. The integer $r(C)$, also denoted simply by r, is called the multiplicity of C. The matrix M is written as $M := ((C_i \cdot C_j))_{1\le i,j\le v}$, and we write $|C_i \cdot C_i| := |(C_i \cdot C_i)|$.

3.1 Denote by $\langle\ ,\ \rangle : \Phi_M \times \Phi_M \to \mathbb{Q}/\mathbb{Z}$ the perfect pairing $\langle\ ,\ \rangle_M$ attached in [3], 1.1, to the symmetric matrix M. Explicit values of this pairing are computed as follows. Let (C, r) and (C', r') be two distinct vertices of G. Define

$$E(C, C') := {}^t\Big(0, \dots, 0, \frac{r'}{\gcd(r, r')}, 0, \dots, 0, \frac{-r}{\gcd(r, r')}, 0, \dots, 0\Big) \in \mathbb{Z}^v,$$

where the first non-zero coefficient of $E(C, C')$ is in the column corresponding to the vertex C and, similarly, the second non-zero coefficient is in the column corresponding to the vertex C'. We say that the pair (C, C') is *uniquely connected* if there exists a path $\mathcal{P}$ in G between C and C' such that, for each edge e on $\mathcal{P}$, the graph $G \setminus \{e\}$ is disconnected. Note that when a pair (C, C') is uniquely connected, then the path $\mathcal{P}$ is the unique shortest path between C and C'. A graph is a tree if and only if every pair of vertices of G is uniquely connected.

Let (C, r) and (C', r') be a uniquely connected pair with associated path $\mathcal{P}$. While walking on $\mathcal{P} \setminus \{C, C'\}$ from C to C', label each encountered vertex consecutively by $(C_1, r_1), (C_2, r_2), \dots, (C_n, r_n)$. Let G_i denote the connected component of C_i in $G \setminus \{\text{edges of } \mathcal{P}\}$. The graph G_i is reduced to a single vertex if and only if C_i is not a node of G. For convenience, we write $(C, r) = (C_0, r_0)$ and $(C', r') = (C_{n+1}, r_{n+1})$ and define G_0 and G_{n+1} accordingly.

3.2 The following facts are proved in [3], 5.1. Let (G, M, R) be any arithmetical graph. Let C and C' be two vertices such that (C, C') is a *uniquely connected* pair of G. Let γ denote the image of $E(C, C')$ in Φ_M. For (D, s) and (D', s') any two distinct vertices on G, let δ denote the image of $E(D, D')$ in Φ_M. Writing $\mathcal{P}$ for the oriented shortest path from C to C' as above, let C_α denote the vertex of $\mathcal{P}$ closest to D in G, and let C_β denote the vertex of $\mathcal{P}$ closest to D'. In other words, $D \in G_\alpha$ and $D' \in G_\beta$. Assume that $\alpha \leq \beta$. (Note that we may have $\alpha = \beta$, and we may have $D = C_\alpha$ or $D' = C_\beta$.) Then if $\alpha < \beta$,

$$\langle \gamma, \delta \rangle = -\mathrm{lcm}(r, r')\mathrm{lcm}(s, s')\Big(\frac{1}{r_\alpha r_{\alpha+1}} + \frac{1}{r_{\alpha+1} r_{\alpha+2}} + \cdots + \frac{1}{r_{\beta-1} r_\beta}\Big) \mod \mathbb{Z}, \tag{3.2.1}$$

and if $C_\alpha = C_\beta$, then $\langle \gamma, \delta \rangle = 0$. Moreover,

$$\langle \gamma, \gamma \rangle = -\mathrm{lcm}(r, r')^2 \Big(\frac{1}{r r_1} + \frac{1}{r_1 r_2} + \cdots + \frac{1}{r_n r'}\Big) \mod \mathbb{Z}. \tag{3.2.2}$$

Note that the negative signs in the expressions (3.2.1) and (3.2.2) are missing in [3], 5.1. Thus, all expressions for $\langle \gamma, \delta \rangle$ computed in section 5 of [3] using 5.1 are correct only after having been multiplied by -1. Similar sign mistakes occurred in [17]. The proof of [3], 5.1, is correct, except that its last line produces the opposite of the stated values for $\langle \gamma, \delta \rangle$ since we assume $\alpha \leq \beta$.

3.3 Let (C, r) be a vertex of G of degree $d \geq 2$. Let (D_i, r_i), $i = 1, \ldots, d$, denote the neighbors of C, that is, the vertices of G linked to C. Let τ_i denote the image of $E(D_i, D_d)$ in Φ_M, for $i \in \{1, \ldots, d-1\}$. We will use repeatedly the following expressions computed using (3.2.1) and (3.2.2):

$$\langle \tau_i, \tau_i \rangle = -\,\mathrm{lcm}(r_i, r_d)^2 \, \frac{r_i + r_d}{r_i r_d r} \mod \mathbb{Z},$$

and when $i \neq j$,

$$\langle \tau_i, \tau_j \rangle = -\,\mathrm{lcm}(r_i, r_d)\,\mathrm{lcm}(r_j, r_d) \frac{1}{r_d r} \mod \mathbb{Z}.$$

These formulas allow us to easily show that τ_i may not always be trivial. For example, let p be a prime dividing r. When $p \nmid r_i r_d (r_i + r_d)$, we find that $\langle \tau_i, \tau_i \rangle \neq 0$ and, thus, $\tau_i \neq 0$. Similarly, when for three distinct indices i, j, and d, we have $p \nmid r_i r_j r_d$, we find that $\langle \tau_i, \tau_j \rangle \neq 0$, showing that both τ_i and τ_j are not trivial.

We claim that r kills τ_i. Indeed, we find, using [17], 2.2, that the images in Φ_M of $E(D_i, C)$ and $E(C, D_d)$ have order dividing $\gcd(r_i, r)$ and $\gcd(r, r_d)$, respectively. Consider the following easy relation between vectors in $\mathbb{Z}^v$ ([17], 3.5): Given any three vertices (A, a), (B, b), and (C, c),

$$bE(A, C) = \frac{c}{\gcd(a, c)} \gcd(a, b) E(A, B) + \frac{a}{\gcd(a, c)} \gcd(b, c) E(B, C) \tag{3.3.1}$$

Using this relation, we find that $r\tau_i = 0$.

Lemma 3.4. *Let (G, M, R) be an arithmetical graph. Consider any two distinct vertices (A, a) and (A', a'), and let $\alpha_{A,A'}$ denote the image of $E(A, A')$ in Φ_M. Then the set $\{\alpha_{AA'}, A \neq A'\}$ is a set of generators for Φ_M.*

Proof. Let us note first that the statement is proved for (G, M, R) as soon as it is proved for $(G, M, R/\gcd(r_1, \ldots, r_v))$. We will thus assume now that $\gcd(r_1, \ldots, r_v) = 1$. Fix a vertex A and consider the subgroup $(\Phi_M)_A$ of Φ_M generated by $\{\alpha_{AA'}$, all $A' \neq A\}$. We claim that $a\Phi_M \subseteq (\Phi_M)_A$. Indeed, an element $\phi \in \Phi_M$ is represented by the class of a vector $(f_D, D \in G)$ such that $\sum f_D r(D) = 0$. It follows that $a\phi = -\sum \gcd(a, r(D)) f_D \alpha_{AD}$. Since $\gcd(r_1, \ldots, r_v) = 1$, ϕ can be expressed in terms of elements of the form $\alpha_{AA'}$. □

The following is a key relation between the τ_is.

Proposition 3.5. *Let (G, M, R) be an arithmetical tree. Let (C, r) be a vertex of degree $d \geq 2$. Keep the notation introduced in* 3.4. *Then $\sum_{i=1}^{d-1} \gcd(r_i, r_d)\tau_i = 0$.*

Proof. Consider any two distinct vertices (A,a) and (A',a'), and let α denote the image of $E(A,A')$ in Φ_M. The previous lemma shows that the group Φ_M is generated by such elements α.

Let $\tau := \sum_{i=1}^{d-1}\gcd(r_i,r_d)\tau_i$. We claim that $\langle \tau,\alpha\rangle = 0$ for all such elements α. This claim, proved below, implies immediately that $\tau = 0$. Indeed, recall that $\langle\ ,\ \rangle$ being perfect, the element τ is trivial if and only if $\langle \tau,\phi\rangle = 0$ for all $\phi\in\Phi_M$.

Let us now prove our claim. Assume first that the path $\mathcal{Q}$ between A and A' contains the vertices D_i and D_d with $i\neq d$. We use (3.2.1) to compute modulo $\mathbb{Z}$ that

$$\begin{aligned}\langle\tau,\alpha\rangle &= \pm\operatorname{lcm}(a,a')\\ &\times\Big(\gcd(r_i,r_d)\operatorname{lcm}(r_i,r_d)(\frac{1}{r_ir}+\frac{1}{rr_d})+\sum_{j\neq i,d}\gcd(r_j,r_d)\operatorname{lcm}(r_j,r_d)(\frac{1}{rr_d})\Big),\end{aligned}$$

which simplifies to

$$\langle\tau,\alpha\rangle = \pm\operatorname{lcm}(a,a')(\sum_{j=1}^{d} r_j)\frac{1}{r}.$$

Since $\sum_{j=1}^{d} r_j = |C\cdot C|r$, we find that $\langle\tau,\alpha\rangle = 0$. When $\mathcal{Q}$ contains D_i and D_j with $i,j\neq d$ and $i\neq j$, we find that modulo $\mathbb{Z}$

$$\begin{aligned}\langle\tau,\alpha\rangle &= \pm\operatorname{lcm}(a,a')\Big(\gcd(r_i,r_d)\operatorname{lcm}(r_i,r_d)\tfrac{1}{r_ir}-\gcd(r_j,r_d)\operatorname{lcm}(r_j,r_d)\tfrac{1}{r_jr}\Big)\\ &= \pm\operatorname{lcm}(a,a')\left(\tfrac{r_d}{r}-\tfrac{r_d}{r}\right)=0.\end{aligned}$$

It is clear that if the path $\mathcal{Q}$ contains no vertices D_i, or if it contains exactly one vertex D_i and does not contain the vertex C, then $\langle\tau,\alpha\rangle = 0$. It remains to consider the case where the path $\mathcal{Q}$ contains exactly one vertex D_i and the vertex C. Then C is an endpoint of $\mathcal{Q}$ and, thus, r divides $\operatorname{lcm}(a,a')$. When $i\neq d$, we find that

$$\langle\tau,\alpha\rangle = \pm\operatorname{lcm}(a,a')\operatorname{lcm}(r_i,r_d)\gcd(r_i,r_d)\frac{1}{r_ir}$$

is 0 modulo $\mathbb{Z}$, and when $i=d$, we find that

$$\langle\tau,\alpha\rangle = \pm\operatorname{lcm}(a,a')\Big(\sum_{i=1}^{d-1}\operatorname{lcm}(r_i,r_d)\gcd(r_i,r_d)\frac{1}{r_ir}\Big)$$

is also 0 modulo $\mathbb{Z}$. □

4. Some combinatorics

Let (G,M,R) be an arithmetical graph. We introduce below a measure $\gamma_D g_D$ of how 'complicated' certain subgraphs G_D of G are, and we describe G_D in Proposition 4.3 when $\gamma_D g_D$ is as small as possible. This result is needed in the proof of Theorem 6.8. A geometric motivation for the introduction of the quantity $\gamma_D g_D$ is found in the genus formula (6.1.1).

4.1 Let (G,M,R) be an arithmetical graph. Fix a vertex $(C_0,r(C_0))$ of G. Assume that C_0 is linked to a vertex $(D,r(D))$ by a single edge e, and that when the edge e is removed from G, then D and C_0 are not in the same connected component of the resulting graph. Let G_D *denote the connected component of* $G\setminus\{e\}$ *that contains* D. Consider the minor N_D of M corresponding to the vertices in G_D. Let

$$\gamma_D := \gcd(r(A), A \text{ vertex of } G_D).$$

Then γ_D divides $r(C_0)$. Indeed, γ_D divides the multiplicity of D and of all vertices linked to D, except possibly that of C_0. But the relation $MR = 0$ implies then that γ_D divides the multiplicity of C_0. Let R_D denote the vector R restricted to the vertices of G_D. By definition, we find that R_D/γ_D is an integer vector.

Let $\beta(G)$ denote the first Betti number of the graph G. Letting $d_G(A)$ denote the degree of a vertex A in the graph G, we have

$$2\beta(G) - 2 = \sum_{\text{vertices } A \text{ of } G} (d_G(A) - 2).$$

Associated with any arithmetical graph (G, M, R) is the following integer invariant $g_0(G) \geq \beta(G)$ ([13], 4.10), defined by the formula

$$2g_0(G) = 2\beta(G) + \sum_{\text{vertices } A \text{ of } G} (r(A) - 1)(d_G(A) - 2). \tag{4.1.1}$$

Let C_0 and D be as above. We now associate to the pair (N_D, R_D) an integer g_D, defined so that the formula below holds:

$$\gamma_D g_D = r(C_0) + r(D) + \sum_{\text{vertices } A \text{ of } G_D} r(A)(d_{G_D}(A) - 2).$$

Since γ_D divides $r(C_0)$, the invariant g_D is indeed an integer. We can rewrite this formula as

(4.1.2) $\gamma_D g_D =$

$$2\beta(G_D) + (r(C_0) - 1) + (r(D) - 1) + \sum_{\text{vertices } A \text{ of } G_D} (r(A) - 1)(d_{G_D}(A) - 2).$$

and we find that

(4.1.3) $g_D =$

$$2\beta(G_D) + (\frac{r(C_0)}{\gamma_D} - 1) + (\frac{r(D)}{\gamma_D} - 1) + \sum_{\text{vertices } A \text{ of } G_D} (\frac{r(A)}{\gamma_D} - 1)(d_{G_D}(A) - 2).$$

4.2 We will make use below of the following facts. Suppose that on G, the vertices D_0, $D_1, \ldots, D_n$ are consecutive vertices on a terminal chain, and D_n is the terminal vertex on this chain (in other words, D_i is linked by one edge to D_{i+1} for $i = 0, \ldots, n-1$, $d_G(D_i) = 2$ for $i = 1, \ldots, n-1$, and $d_G(D_n) = 1$). *Then* $\gcd(r(D_0), r(D_1)) = r(D_n)$, *and if $|D_i \cdot D_i| > 1$ for all $i = 1, \ldots, n$, then*

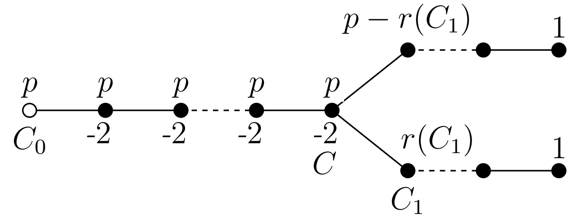
$$r(D_0) > r(D_1) > \cdots > r(D_n).$$

Indeed, the equality $|D_n \cdot D_n| r(D_n) = r(D_{n-1})$ obtained from the relation $MR = 0$ shows that $r(D_n)$ divides $r(D_{n-1})$, and $r(D_n) < r(D_{n-1})$ if $|D_n \cdot D_n| > 1$. Suppose that for some i, we have $r(D_i) > r(D_{i+1})$. Then it follows from $|D_i \cdot D_i| r(D_i) = r(D_{i-1}) + r(D_{i+1})$ and $|D_i \cdot D_i| \geq 2$ that $r(D_{i-1}) > r(D_i)$. The equality $|D_i \cdot D_i| r(D_i) = r(D_{i-1}) + r(D_{i+1})$ implies that $\gcd(r(D_{i-1}), r(D_i)) = \gcd(r(D_i), r(D_{i+1}))$.

Proposition 4.3. *Let (G, M, R) be an arithmetical tree containing a vertex C_0 of prime multiplicity p. Assume that a vertex D linked to C_0 by an edge e has multiplicity divisible by p. Let G_D denote the connected component of $G \setminus \{e\}$ that contains D. Assume in addition that G_D does not contain any vertex A of degree 1 or 2 in G with $|A \cdot A| = 1$. Then*

$$\gamma_D g_D \geq 2(p-1).$$

If $\gamma_D g_D = 2(p-1)$, then $\gamma_D = 1$ and G_D is a graph of the shape depicted below, containing one node C of G only, of multiplicity p and degree 3 in G. The two terminal vertices of G that belong to G_D have multiplicity 1.



Let α denote the number of vertices of G_D on the chain linking C_0 to the node C of G_D (including the node C). Let C_1 and C_1' denote the vertices linked to C on the two terminal chains. Then $1 \leq r(C_1) < p$, and the minor of M corresponding to the vertices of G_D is completely determined by p, α, and $r(C_1)$.

The proof of 4.3 is given in 4.6. We start with a preliminary lemma.

4.4 Let (G, M, R) be an arithmetical tree. For each node $(C, r(C))$ of degree $d(C) \geq 3$ in G, we define an invariant $\mu(C)$ as follows. Let $\rho(C)$ denote the number of terminal chains attached to C, and let $D_1(C), \ldots, D_{\rho(C)}(C)$ be the vertices of G linked to C that belong each to one terminal chain attached to C. Let $r_i(C)$ denote the multiplicity of $D_i(C)$. The multiplicity of the terminal vertex on the chain containing $D_i(C)$ is $\gcd(r(C), r_i(C))$. If no vertex A on the terminal chain has $|A \cdot A| = 1$, then $r_i(C) < r(C)$ (see 4.2). When a chain attached to C is not terminal, we will call it a *connecting chain*. As in [13], 4.7, we let, when $\rho(C) > 0$,

$$\mu(C) := (d(C) - 2)(r(C) - 1) - \sum_{j=1}^{\rho(C)} (\gcd(r(C), r_j(C)) - 1).$$

When $\rho(C) = 0$, we let $\mu(C) := (d(C) - 2)(r(C) - 1)$. It is clear that if $r(C) = 1$, then $\mu(C) = 0$.

Lemma 4.5. *Assume that the terminal chains attached to C do not contain a vertex A with $|A \cdot A| = 1$. Then $\mu(C) \geq 0$, and $\mu(C) = 0$ if and only if $r(C) = 1$ and $\rho(C) = 0$.*

Proof. It is clear that if a node C has $\rho(C) = 0$, then $\mu(C) \geq 0$, and $\mu(C) = 0$ only when $r(C) = 1$. Assume now that $\rho(C) > 0$. Our hypothesis implies that $r(C) > \gcd(r(C), r_i(C))$ for each vertex $D_i(C)$, $i = 1, \ldots, \rho(C)$. In particular, $r(C) > 1$, and we need to prove that $\mu(C) > 0$. Let

$$s := \gcd(r(C), r_1(C), \ldots, r_d(C)).$$

Assume first that $\rho(C) = d(C)$, so that G has a single node. It is proven in [13], 4.1, that if $\rho(C) = d(C)$ and $s = 1$, then $\mu(C) \geq 0$. When $s > 1$, define

$$\mu_s(C) := (d(C) - 2)(\frac{r(C)}{s} - 1) - \sum_{j=1}^{\rho(C)} (\frac{\gcd(r(C), r_j(C))}{s} - 1).$$

The integer $\mu_s(C)$ is nothing but the μ-invariant of the node on the arithmetical graph obtained from G by dividing all its multiplicities by s. Thus $\mu_s(C)$ is even ([13], 3.6), and $\mu_s(C) \geq 0$. Since

$$\mu(C) = -2(s - 1) + s\mu_s(C),$$

we find that $\mu(C) > 0$ if $\mu_s(C) > 0$. *We claim that under our hypotheses,* $\mu(C) > 0$ *when* $s = 1$. Indeed, our hypotheses implies that $r(C) > \gcd(r(C), r_i(C))$ for each vertex $D_i(C)$, $i = 1, \ldots, \rho(C)$. Dropping the reference to C, we can write

$$\begin{array}{rcl} \mu(C) & := & (d-2)(r-1) - \sum_{j=1}^{d}(\gcd(r, r_i) - 1) \\ & \geq & (d-2)(r-1) - d(r/2 - 1) \\ & = & (d-4)r/2 + 2. \end{array}$$

Thus $\mu(C) > 0$ if $d \geq 4$. Assume now that $d = 3$. Then $cr = r_1 + r_2 + r_3$ for some c. Let $h_i = \gcd(r, r_i)$, and assume that $h_1 \geq h_2 \geq h_3$. Then $(h_1, h_2, h_3) = (r/2, r/2, r/2)$, $(r/2, r/2, r/3)$, $(r/2, r/3, r/3)$, and $(r/2, r/3, r/4)$ cannot occur because of the divisibility $r \mid (r_1 + r_2 + r_3)$. Since the cases $(h_1, h_2, h_3) = (r/3, r/3, r/3)$, $(r/2, r/4, r/4)$, and $(r/2, r/3, r/6)$ have $\mu(C) > 0$, we need only to consider $(h_1, h_2, h_3) = (r/2, r/3, r/5)$. In this case, $r_1 = r/2$, $r_2 = r/3$ or $2r/3$, and $r_3 = ar/5$ with $a = 1, \ldots, 4$. The reader will check that $cr = r_1 + r_2 + r_3$ is impossible to achieve with these values, and our claim is proved.

Let us assume now that $0 < \rho(C) < d(C)$. Then

$$\begin{array}{rcl} \mu(C) & := & (d-2)(r-1) - \sum_{j=1}^{\rho}(\gcd(r, r_i) - 1) \\ & \geq & (d-2)(r-1) - (d-1)(r/2 - 1) \\ & = & (d-3)r/2 + 1 > 0. \end{array}$$

□

4.6 *Proof of 4.3.* We claim that G_D contains a node of G. (This node is also a node of G_D, unless it is D itself and $d_G(D) = 3$.) Indeed, the hypotheses that $r(C_0) \leq r(D)$ and $|D \cdot D| > 1$ implies that $d_G(D) > 1$, because the relation $MR = 0$ provides otherwise for the equality $|D \cdot D| r(D) = r(C_0)$, which is a contradiction. Suppose then that D is connected in G_D to D_1. If $d_G(D) = 2$, then we find from the relation $|D \cdot D| r(D) = r(C_0) + r(D_1)$ that $r(D) \leq r(D_1)$. Repeating this discussion with D and D_1 instead of C_0 and D, we find that the graph G_D has a chain of increasing multiplicities $r(D) \leq r(D_1) \leq \ldots$, which eventually leads to a node of G_D (and of G).

In G, C_0 and D are adjacent vertices. Consider the connected component $\mathcal{G}$ of $G \setminus \{D\}$ that contains C_0. Two cases can occur: either (a) $\mathcal{G}$ contains a node of G, or (b) $\mathcal{G}$ does not contain a node of G, in which case we will call $\mathcal{G}$ a terminal chain of G. In the latter case, the terminal vertex on this chain has multiplicity $\gcd(r(C_0), r(D))$ (see 4.2), which equals $r(C_0)$ by hypothesis. The definition of $\gamma_D g_D$ in (4.1.2), along with the fact that we assume that G is a tree, allow us to write:

$$\gamma_D g_D = (r(C_0) - 1) + \sum_{\text{vertices } A \text{ of } G_D} (r(A) - 1)(d_G(A) - 2).$$

In case (a), C_0 is not on a terminal chain of G, so that by definition of $\mu(C)$ in 4.4, we can write:

$$\gamma_D g_D = (r(C_0) - 1) + \sum_{\text{nodes } C \text{ of } G \text{ in } G_D} \mu(C) \tag{4.6.1}$$

(where $\mu(C)$ is computed viewing C as a node of G, and not of G_D). In case (b) where C_0 is on a terminal chain of G whose terminal vertex has multiplicity $r(C_0)$, we have

$$\gamma_D g_D = 2(r(C_0) - 1) + \sum_{\text{nodes } C \text{ of } G \text{ in } G_D} \mu(C).$$

We prove below case (a). The arguments to prove (b) are similar, and are left to the reader. Case (b) will not be used in the remainder of this article.

Assume that we are in case (a). We can apply 4.5 and we obtain that each term $\mu(C)$ in the above sum is non-negative. In view of (4.6.1), since $r(C_0) = p$ by hypothesis, we need to show that $\sum_{\text{nodes } C} \mu(C) \geq p-1$, and we need to describe the graphs for which $\sum_{\text{nodes } C} \mu(C) = (p-1)$.

Denote by C the node of G closest to C_0 in G_D. (This node could be D.) The multiplicity of C is divisible by p since p divides the consecutive multiplicities $r(C_0)$ and $r(D)$ (similar argument as in 4.2). Let np denote the multiplicity of C.

Suppose that C (of degree d in G) has only one connecting chain. If $n = 1$, then all terminal multiplicities at C equal 1 and $\mu(C) = (d-2)(p-1)$. The case $d = 3$ leads to the case described in the statement of 4.3, with $\mu(C) = (p-1)$, $\gamma_D g_D = 2(p-1)$, and $\gamma_D = 1$. When $d > 3$, we have $\mu(C) > p-1$, as desired.

When $n > 1$, the inequality

$$\begin{aligned} \mu(C) &\geq (d-2)(np-1) - (d-1)(np/2-1) \\ &= (d-2)np/2 - np/2 + 1. \end{aligned}$$

shows that we have $\mu(C) > p-1$ unless $d = 3$. When $n > 1$ and $d = 3$, every vertex on the chain linking C to C_0 has multiplicity divisible by p. Thus, either (i) both terminal multiplicities of C are coprime to p (call them n_1 and n_2), or (ii) both are divisible by p (call them m_1p and m_2p).

In case (i), $\mu(C) = np - n_1 - n_2 + 1$, with n_1, n_2 dividing n. It follows that $\mu(C) \geq n(p-2)+1$. Clearly, $\mu(C) > p-1$ unless $p = 2$. Assume that $p = 2$. If $(n_1, n_2) \neq (n, n)$, we find that $\mu(C) = n(p-1)+1 > (p-1)$. The case $(n_1, n_2) = (n, n)$ cannot happen because in that case, n divides the multiplicity of all the components linked to C, which implies then that $n = 2$. But a node of multiplicity 4 cannot have exactly three vertices of multiplicity 2 attached to it.

In case (ii), $\mu(C) = (n - m_1 - m_2)p + 1$, with m_1, m_2 dividing n. The equality $(n - m_1 - m_2) = 0$ is not possible. Indeed, it is only possible if $m_1 = m_2 = n/2$. But since $\gcd(m_1, m_2) = 1$, this case can happen only if $n = 2$. But then $|C \cdot C|$ would equal $3/2$, a contradiction. It follows that $\mu(C) = (n - m_1 - m_2)p + 1 > p - 1$.

Suppose now that C, of multiplicity np, has at least two connecting chains. If $n > 1$, then

$$\mu(C) \geq (d-2)(np-1) - (d-2)(np/2-1) = (d-2)np/2 > p-1,$$

as desired. If $n = 1$, then $\mu(C) = (d-2)(p-1)$. Thus, $\mu(C) > p-1$ if $d > 3$. Suppose now that $d = 3$. Since G_D is a tree with a node C of degree 3, G_D must have at least three terminal vertices. Thus, there must exist at least one additional node C' on the graph G_D which has a terminal chain. It follows that $\mu(C') \geq 1$ (4.5) and, therefore, $\mu(C) + \mu(C') > p-1$, as desired.

4.7 To conclude the proof of 4.3, we now specify the intersection matrix in the case where $\gamma_D g_D = 2(p-1)$. Let (G, M, R) be as in 4.3, and assume that the vertex D is such that $\gamma_D g_D = 2(p-1)$. Let N_D denote the matrix M restricted to the vertices of G_D. Let α denote the number of vertices of G_D on the chain linking C_0 to the node C of G_D (including the node C). Each of these vertices except C is of degree 2. The multiplicity of C is p. Since we assume that no vertex of degree 2 has self-intersection -1, we find that the multiplicity of each of these vertices must be p. It follows that each of these vertices except possibly C must have self-intersection -2.

Let C_1 and C_1' denote the vertices linked to C on the two terminal chains. Since they have degree 1 or 2 and cannot have self-intersection -1, we find that $1 \leq r(C_1) < r(C) = p$, and $r(C_1') < r(C)$. Moreover, from $MR = 0$, we find that $p + r(C_1) + r(C_1') = p|C \cdot C|$. It follows that $|C \cdot C| = 2$, and $r(C_1') = p - r(C_1)$. We claim that N_D depends only on p, α, and $r(C_1)$ and we write it as $N_D = N(p, \alpha, r(C_1))$. Indeed, the pair $(p, r(C_1))$ completely determines all multiplicities and all self-intersections on the terminal chain containing C_1: use $(r, s) = (p, r(C_1))$ in 4.8 below to determine the self-intersections and multiplicities of the terminal chain. Similarly, the pair $(p, r(C_1'))$ completely determines all multiplicities and all self-intersections on the terminal chain containing C_1'. This conclude the proof of 4.3. The matrix N_D is an intersection matrix also introduced in [19], 3.18. □

4.8 Recall the following standard construction. Given an ordered pair of positive integers $r > s$ with $\gcd(r, s) = 1$, we construct an associated intersection matrix $N = N(r, s)$ with vector $R = R(r, s)$ and $NR = -re_1$ as follows (where e_1 denote the first standard basis vector of $\mathbb{Z}^n$). Using the division algorithm, we can find positive integers $b_1, \dots, b_m$ and $s_1 = s > s_2 > \cdots > s_m = 1$ such that $r = b_1 s - s_2$, $s_1 = b_2 s_2 - s_3$, and so on, until we get $s_{m-1} = b_m s_m$. These equations are best written in matrix form:

$$\begin{pmatrix} -b_1 & 1 & \dots & 0 \\ 1 & -b_2 & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & \dots & 1 & -b_m \end{pmatrix} \begin{pmatrix} s_1 \\ \vdots \\ \vdots \\ s_m \end{pmatrix} = \begin{pmatrix} -r \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

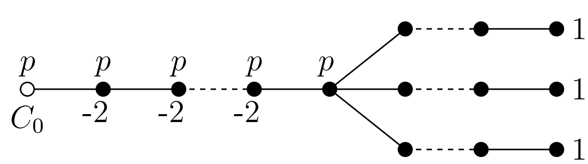
We let $N(r, s)$ denote the above square matrix, and $R(r, s)$ be the column matrix on the left of the 'equal' sign. It is well-known that $\det(N(r, s)) = \pm r$ (see [17], 2.6). We recall also for use in 6.12 that

$$\frac{1}{rs} + \frac{1}{ss_2} + \cdots + \frac{1}{s_{m-1}s_m} = \frac{c}{r}, \tag{4.8.1}$$

where $0 < c < r$ is such that $r \mid cs - 1$ (see [17], 2.8 and 2.6).

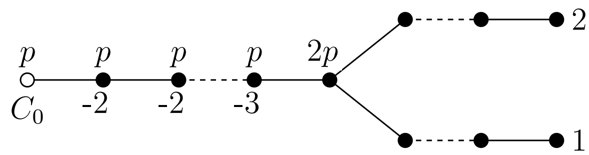
Remark 4.9 In Proposition 4.3, the hypothesis that $\gamma_D g_D = 2(p-1)$ allowed us to completely describe the graph G_D. For a fixed $\gamma_D g_D > 2(p-1)$, the situation is much more complicated and several possible types of graphs G_D may occur. It would follow from our guess in 6.2 that for applications to models of curves, it suffices to classify the cases where $\gamma_D g_D$ is a multiple of $p-1$. We give below several possible types of graphs G_D with $\gamma_D g_D = 3(p-1)$ when p is odd.

(a) G_D is a graph with one node of G only, of multiplicity p and degree 4 in G. The three terminal vertices of G that belong to G_D have multiplicity 1.



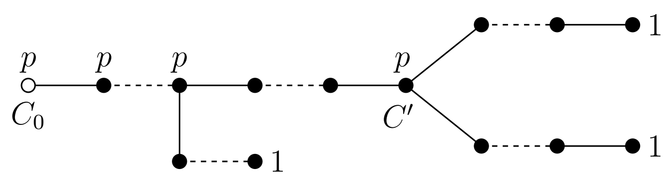
To completely determine the intersection matrix N_D and the vector R_D, one needs to also provide the multiplicities r_1, r_2, and r_3, of the first vertices on each of the three terminal chains, with the conditions $1 \le r_1, r_2, r_3 < p$ and $r_1 + r_2 + r_3$ divisible by p. Such a data can only be provided when p is odd. The self-intersection of the node is then $-(p + r_1 + r_2 + r_3)/p = -2$ or -3.

(b) G_D is a graph with one node of G only, of multiplicity $2p$ and degree 3 in G. The two terminal vertices of G that belong to G_D have multiplicity 1 and 2, respectively.

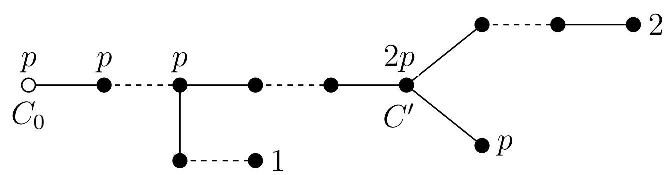


(c) G_D is a graph with 2 nodes C and C' of G. Let C be the node closest to C_0 in G_D. It has multiplicity p and degree 3 in G, and it has a single terminal chain with terminal multiplicity 1. The node C' is connected to C by a connecting chain that contains a vertex of multiplicity *coprime* to p.

(i)



(ii)



We conclude this section with some general remarks concerning the invariant g_D introduced in (4.1.2).

Remark 4.10 Let (G, M, R) be an arithmetical graph. As at the beginning of this section, fix a vertex $(C_0, r(C_0))$ of G. Assume that C_0 is linked to a vertex $(D, r(D))$ by a single edge e, and that when the edge e is removed from G, then D and C_0 are not in the same connected component of the resulting graph. Let G_D denote the connected component of $G \setminus \{e\}$ that contains D. Consider the minor $N = N_D$ of M corresponding to the vertices in G_D. Let n denote the number of vertices of G_D.

(a) *The integer g_D depends only on the matrix N_D and the vertex D on the graph G_D.* To prove this statement, we show that the vector R_D/γ_D is completely determined by N_D and the vertex D. Indeed, let us number the vertices of G_D such that D is the first vertex numbered. Then R_D/γ_D is a vector with positive coefficients such that $N_D(R_D/\gamma_D) = {}^t(-r(C_0)/\gamma_D, 0, \dots, 0)$ (where the superscript t indicates the transpose vector). The existence of such a relation insures that N_D is negative-definite (see [19], 3.3), and the vector R_D/γ_D is a rational multiple of the first column of the unique matrix N^* such that $NN^* = N^*N = \det(N)\mathrm{Id}_n$ ([19], 3.4). The integer $r(C_0)/\gamma_D$ is the order in $\mathbb{Z}^n/\mathrm{Im}(N)$ of the class of the first basis vector e_1 ([19], 3.5).

(b) *The integer g_D is non-negative.* More precisely:

$$g_D - 2\beta(G_D) \geq (\frac{r(C_0)}{\gamma_D}) + \gcd(\frac{r(D)}{\gamma_D}, \frac{r(C_0)}{\gamma_D}) - 2 \geq 0. \tag{4.10.1}$$

To prove the first inequality, complete the pair $(N, R_D/\gamma_D)$ into an arithmetical graph (G', M', R') by adding a chain attached to D, as in [19], 3.15. Clearly, $\beta(G') = \beta(G_D)$.

The graphs G' and G_D differ in only two vertices of degree not equal to 2: the terminal vertex on the new terminal chain on G' has terminal multiplicity $\gcd(\frac{r(D)}{\gamma_D}, \frac{r(C_0)}{\gamma_D})$, and $d_{G'}(D) = d_{G_D}(D) + 1$. Using (4.1.1) and (4.1.3), it is easy to show that

$$\text{(4.10.2)} \quad 2g_0(G', M', R') - 2\beta(G') = g_D - 2\beta(G_D) - (\frac{r(C_0)}{\gamma_D} - 1) - (\gcd(\frac{r(D)}{\gamma_D}, \frac{r(C_0)}{\gamma_D}) - 1).$$

The integer $g_0(G') - \beta(G')$ is always non-negative ([13], 4.10), and the statement follows.

(c) In analogy with the arithmetic genus of curves on surfaces, we define, given $Z \in \mathbb{Z}^n$, a (possibly negative) integer $p_a(Z)$ as follows. If $Z = C_i$ is a vertex of G_D, we let $p_a(Z) = 0$. We let $p_a(rC_i)$ be defined by the formula $2p_a(rC_i) - 2 = r^2C_i^2 + r(|C_i^2| - 2)$ (where we have abbreviated $C_i \cdot C_i$ by C_i^2). Since $r^2 - r$ is always even, $p_a(rC_i)$ is an integer. In general, when $Z = \sum_{i=1}^n r_iC_i$, we let

$$Z^2 := \sum_{1 \leq i,j \leq n} r_ir_j(C_i \cdot C_j),$$

and set

$$2p_a(Z) - 2 := Z^2 + \sum_{i=1}^{n} r_i(|C_i^2| - 2).$$

We leave it to the reader to check that

$$g_D = 2p_a(R_D/\gamma_D) - 2 + \frac{r(D)}{\gamma_D}(\frac{r(C_0)}{\gamma_D} + 1).$$

(d) *The integer g_D is even when either $r(C_0)$ is odd, or $r(D)$ is even.* This can be seen from the formula for g_D in (c), or from (4.10.2).

(e) Assume that G_D is a tree. Then the order $|\det(N)|$ of the group $\Phi_N := \mathbb{Z}^n/N(\mathbb{Z}^n)$ can be computed completely in terms of the vector R_D/γ_D and of the graph G_D (see [19], 3.14), and we find that

$$|\det(N)| = \frac{r(D)}{\gamma_D}\frac{r(C_0)}{\gamma_D} \prod_{\text{vertices } A \text{ of } G_D} \left(\frac{r(A)}{\gamma_D}\right)^{d_{G_D}(A)-2},$$

where $d_{G_D}(A)$ is the degree of the vertex A in the graph G_D. Recall now the formula (4.1.3):

$$g_D = (\frac{r(D)}{\gamma_D} - 1) + (\frac{r(C_0)}{\gamma_D} - 1) + \sum_{\text{vertices } A \text{ of } G_D} (\frac{r(A)}{\gamma_D} - 1)(d_{G_D}(A) - 2).$$

This last expression is surprisingly similar to the expression for $|\det(N)|$. This motivates the following result. *Let $x > 0$ be any integer, and define the function:*

$$\ell(x) := \sum_{q \text{ prime}} \mathrm{ord}_q(x)(q - 1).$$

Then

$$\text{(4.10.3)} \qquad \ell(|\det(N)|) \leq g_D.$$

This result is not used in the remainder of this paper, and we will provide here only a sketch of proof.

Sketch of proof: We complete the pair $(N, R_D/\gamma_D)$ into an arithmetical graph (G', M', R') by adding a chain attached to D, as in [19], 3.15. The order of the component group

$\Phi(M')$ is given in [13], 2.5, and the relation between $\det(N)$ and $|\Phi(M')|$ is discussed in the proof of 3.14 in [19]. We can then bound $|\Phi(M')|$ in terms of $g_0(G', M', R')$ using [13], 4.8, which states that $\ell(|\Phi(M')|) \leq 2g_0(G', M', R')$. The inequality $\ell(|\det(N)|) \leq g_D$ follows then from (4.10.2).

5. The quotient construction

Let K be a complete discrete valuation field with valuation v, ring of integers $\mathcal{O}_K$, uniformizer π_K, and residue field k of characteristic $p > 0$, assumed to be algebraically closed. Let X/K be a smooth proper geometrically connected curve of genus $g > 0$. When $g = 1$, assume in addition that $X(K) \neq \emptyset$. Assume that X/K does not have semi-stable reduction over $\mathcal{O}_K$, and that it achieves good reduction after a cyclic extension L/K of prime degree q.

Let H denote the Galois group of L/K. Let $\mathcal{Y}/\mathcal{O}_L$ be the smooth model of X_L/L. Let σ denote a generator of H. By minimality of the model $\mathcal{Y}$, σ defines an automorphism of $\mathcal{Y}$ also denoted by σ (but note that $\sigma : \mathcal{Y} \to \mathcal{Y}$ is not morphism of $\mathcal{O}_L$-schemes). We also denote by σ the automorphism of $\mathcal{Y}_k$ induced by the action of σ on $\mathcal{Y}$. Let $\mathcal{Z}/\mathcal{O}_K$ denote the quotient $\mathcal{Y}/H$, and let $\alpha : \mathcal{Y} \to \mathcal{Z}$ denote the quotient map. The scheme $\mathcal{Z}$ is normal. The map α induces a natural map $\mathcal{Y}_k \to \mathcal{Z}_k^{red}$ which factors as follows:

$$\mathcal{Y}_k \xrightarrow{\ \rho\ } \mathcal{Y}_k/\langle\sigma\rangle \longrightarrow \mathcal{Z}_k^{red}.$$

5.1 We claim that the first map is Galois of order $|H|$, and that the second map is the normalization map of $\mathcal{Z}_k^{red}$. Indeed, let $\mathrm{Spec}(B)$ denote a dense open set of $\mathcal{Y}$ invariant under the action of H. Then $\mathrm{Spec}(B^H)$ is a dense open set of $\mathcal{Z}$. Let $A := B^H$. Let $P_B = (\pi_L)$ denote the prime ideal of B corresponding to $\mathcal{Y}_k$, and let $P_A := P_B \cap A$. We have the natural maps

$$B^H/P_A \hookrightarrow (B/P_B)^H \hookrightarrow B/P_B.$$

The extension of discrete valuation rings $(B^H)_{P_A} \to B_{P_B}$ induces an extension of residue fields $(B^H)_{P_A}/P_A(B^H)_{P_A} \to B_{P_B}/P_B B_{P_B}$. We claim that this extension has degree $|H|$. Indeed, our assumption is that the curve X/K does not have good reduction over $\mathcal{O}_K$. If the residue extension is trivial, the normalization of the curve $\mathcal{Z}_k^{red}$ is isomorphic to $\mathcal{Y}_k$ and, thus, is of genus g. In addition we find that $P_A B_{P_B} = (P_B B_{P_B})^{|H|}$, so that $\pi_K A_{P_A} = (P_A A_{P_A})$. The special fiber of $\mathcal{Z}$ is then reduced, and the curve X/K has good reduction over $\mathcal{O}_K$, a contradiction. It follows then that $P_A B_{PB} = P_B B_{PB}$, so that $\pi_K A_{P_A} = (P_A A_{P_A})^{|H|}$. Hence, the multiplicity in $\mathcal{Z}$ of the irreducible component $\mathcal{Z}_k^{red}$ equals $|H|$.

It is easy to check that for any $x \in (B/P_B)^H$, $|H|x$ and $x^{|H|}$ belong to A/P_A. Thus, when $|H| \neq p$, A/P_A and $(B/P_B)^H$ have the same fields of fractions. When $|H| = p$, it could happen that A/P_A and $(B/P_B)^H$ do not have the same fields of fractions, in which case the extension of fields of fractions is purely inseparable of degree p, with $(B/P_B)^H = B/P_B$. It follows that the special fiber of $\mathcal{Z}$ also has genus g. When $g > 1$, this is not possible since the multiplicity of $\mathcal{Z}_k$ is p. When $g = 1$, it could happen that $\mathcal{Z}$ is the minimal model of X/K, with a multiple special fiber. This case cannot happen in our situation because of our assumption that $X(K) \neq \emptyset$: A K-rational point always reduces to a smooth point in the special fiber. Thus, the automorphism $\sigma : \mathcal{Y}_k \to \mathcal{Y}_k$ is not trivial. We find that A/P_A and $(B/P_B)^H$ have the same fields of fractions, so that the Dedekind domain $(B/P_B)^H$ is the integral closure of A/P_A.

5.2 Let $P_1, \ldots, P_d$, be the ramification points of the map $\mathcal{Y}_k \to \mathcal{Y}_k/\langle\sigma\rangle$. Let $Q_1, \ldots, Q_d$ be their images in $\mathcal{Z}$. The normal scheme $\mathcal{Z}$ is singular exactly at $Q_1, \ldots, Q_d$. Indeed, the morphism $\mathcal{Y} \to \mathcal{Z}$ is unramified outside these points. If the point Q_i were regular, the morphism would be flat above Q_i ([1], V, 3.6), and the branch locus would then be pure of codimension 1 ([1], VI, 6.8), a contradiction.

Consider the regular model $\mathcal{X} \to \mathcal{Z}$ obtained from $\mathcal{Z}$ by a minimal desingularization. After finitely many blow-ups $\mathcal{X}' \to \mathcal{X}$, we can assume that the model $\mathcal{X}'$ is such that $\mathcal{X}'_k$ has smooth components and normal crossings, and is minimal with this property. Let f denote the composition $\mathcal{X}' \to \mathcal{Z}$. Let C_0/k denote the strict transform in $\mathcal{X}'$ of the irreducible closed subscheme $\mathcal{Z}_k^{red}$ of $\mathcal{Z}$. The curve C_0 has multiplicity $|H|$ in $\mathcal{X}'$. Let $D_1, \ldots, D_d$ denote the irreducible components of $\mathcal{X}'_k$ that meet C_0. Let r_i denote the multiplicity of D_i, $i = 1, \ldots, d$. We assume $d \geq 1$. Our main theorem in this section is:

Theorem 5.3. *Let X/K be a smooth proper geometrically connected curve of genus $g > 0$, with $X(K) \neq \emptyset$ if $g = 1$. Assume that X/K does not have semi-stable reduction over $\mathcal{O}_K$, and that it achieves good reduction after a cyclic extension L/K with Galois group H of prime degree p. Keep the above notation, and let Q_i be a singular point of the quotient $\mathcal{Z} := \mathcal{Y}/H$. Let G_{Q_i} denote the graph associated with the curve $f^{-1}(Q_i)$. Let G denote the graph associated with the special fiber $\mathcal{X}'_k$. Then, for all $i = 1, \ldots, d$, the graph G_{Q_i} contains a node of G and p divides r_i.*

Proof. When $d = 1$, the theorem is immediate: the component C_0 of multiplicity p is a terminal vertex of the graph of $\mathcal{X}'$, and thus $p|C_0 \cdot C_0| = r_1$. Assume that G_{Q_1} does not contain a node of G. Then since $d = 1$, G does not contain a node. Since the resolution is minimal with normal crossings, none of the components of $\mathcal{X}'_k$ can have self-intersection (-1) except possibly for C_0. It is clear that the graph G is not reduced to a single vertex since the model $\mathcal{Z}$ is singular. Thus the graph G has a second terminal vertex C' in addition to C_0. But then, walking on G from C' towards C_0, we find that the multiplicities can only be strictly increasing. This is a contradiction since all multiplicities on G are divisible by p (because two consecutive ones are), and G must contain a node. We assume from now on that $d > 1$.

Let $A := \mathrm{Jac}(X/K)$. Let $\mathcal{A}_K/\mathcal{O}_K$ denote the Néron model of A/K. Let $\mathcal{A}_L/\mathcal{O}_L$ denote the Néron model of A_L/L, and denote by $\eta : \mathcal{A}_K \times_{\mathcal{O}_K} \mathcal{O}_L \to \mathcal{A}_L$ the canonical map induced by the functoriality property of Néron models. The special fiber $(\mathcal{A}_K)_k$ is an extension of a finite group $\Phi_{A/K}$, called the group of components, by the connected component of zero $(\mathcal{A}_K)_k^0$ of $(\mathcal{A}_K)_k$:

$$0 \longrightarrow (\mathcal{A}_K)_k^0 \longrightarrow (\mathcal{A}_K)_k \longrightarrow \Phi_{A/K} \longrightarrow 0.$$

Assume by contradiction that p is coprime to one of the r_is. Without loss of generality, we may assume that $p \nmid r_d$. For each $i = 1, \ldots, d$, choose a point $x_i \in D_i$ such that x_i is a regular point of $(\mathcal{X}'_k)^{red}$. Since K is complete, we can find a closed point R_i of X, of degree r_i over K, and such that the closure of R_i in $\mathcal{X}'$ meets the special fiber $\mathcal{X}_k$ exactly in x_i (see, e.g., [6], 8.4(3)). For each $i = 1, \ldots, d-1$, consider the following divisor of degree 0 on X:

$$S_i := \frac{r_d}{\gcd(r_i, r_d)} R_i - \frac{r_i}{\gcd(r_i, r_d)} R_d.$$

We also denote by S_i its image in $\mathrm{Jac}(X)/K$. We recall below Raynaud's description of the Néron model of a Jacobian in order to be able to describe explicitly the image of S_i under both the reduction map $\mathrm{Jac}(X)(K) \to \Phi_{A/K}$ and the reduction map $\mathrm{Jac}(X)(L) \to (\mathcal{A}_L)_k(k)$. We will be able to contradict the hypothesis that $p \nmid r_d$ by considering the reductions of $\sum_{i=1}^{d-1} \gcd(r_i, r_d) S_i$.

Raynaud exhibited in [24] an explicit separated quotient $Q_K/\mathcal{O}_K$ of the open subfunctor of $\mathrm{Pic}_{\mathcal{X}'/\mathcal{O}_K}$ consisting of line bundles of total degree 0, and he showed that when the residue field k is algebraically closed, $Q_K/\mathcal{O}_K$ is isomorphic to the Néron model of A/K ([4], 9.5/4 (a)). The canonical map $Q_K(K) \to \Phi_{Q_K}$ is described as follows ([4], 9.5/9 and 9.6/1). Represent an element of $Q_K(K)$ by a line bundle $\mathcal{L}$ on X of degree 0. Let $\overline{\mathcal{L}}$ denote an extension of $\mathcal{L}$ to $\mathcal{X}'$. Number the irreducible components of $\mathcal{X}'_k$ as $C_1, \dots, C_v$. Consider the map $\oplus_i \mathbb{Z}C_i \to \mathrm{Hom}(\oplus_i \mathbb{Z}C_i, \mathbb{Z})$ which sends C_i to the map δ_{C_i}, with $\delta_{C_i}(C_j) := (C_i \cdot C_j)$. The group Φ_M is isomorphic to the torsion subgroup of the cokernel of this map. The group of components Φ_{Q_K} is isomorphic to Φ_M, and under this isomorphism, the image of $\mathcal{L}$ under $Q_K(K) \to \Phi_{Q_K}$ is the map $\delta_{\mathcal{L}}$, with $\delta_{\mathcal{L}}(C_i) := (C_i \cdot \overline{\mathcal{L}})$. It follows immediately from these facts that the image in Φ_{Q_K} of $S_i \in \mathrm{Jac}(X)(K)$ can be identified with the image τ_i of the vector $E(D_i, D_d)$ in Φ_M (notation as in 3.1 and 3.4).

Consider now the reduction map $Q_L(L) \to (Q_L)_k(k)$. The closure of any point in the preimage under $X_L \to X$ of the closed point R_i meets the special fiber of the smooth model $\mathcal{Y}$ of X_L only at the point P_i. The line bundle $\mathcal{L}$ corresponding to the divisor S_i pulls back to a line bundle $\mathcal{L}_L$ on X_L. We find that the reduction of $\mathcal{L}_L \in \mathrm{Jac}(X_L)(L)$ is the point of $\mathrm{Jac}(\mathcal{Y}_k)(k)$ corresponding to the divisor $\mathrm{lcm}(r_i, r_d)(P_i - P_d)$.

We may now find a contradiction to the assertion that $p \nmid r_d$ *when the quotient of* $\mathcal{Y}_k$ *by the action of* H *has genus zero.* As we indicated above, the element $\sum_{i=1}^{d-1} \gcd(r_i, r_d) S_i$ in $\mathrm{Jac}(X)(K)$ reduces to the element $\sum_{i=1}^{d-1} \gcd(r_i, r_d)\tau_i$ in Φ_M. Proposition 3.6 shows that the latter element is zero in Φ_M. Thus, $\sum_{i=1}^{d-1} \gcd(r_i, r_d) S_i$ reduces in the connected component $(Q_K)_k^0$. Our additional hypothesis implies that this connected component is unipotent. This follows from [4], 9.5/4 if the greatest common divisor of the multiplicities of the components of $\mathcal{X}'_k$ is 1, and from [12], 7.1, in general. It follows that the image of $(Q_K)_k^0$ under the canonical map $\eta : \mathcal{A}_K \times_{\mathcal{O}_K} \mathcal{O}_L \to \mathcal{A}_L$ is trivial.

Consider now the element $\sum_{i=1}^{d-1} \gcd(r_i, r_d) S_i$ in $\mathrm{Jac}(X_L)(L)$. Our discussion above shows that it reduces to the element $r_d(\sum_{i=1}^{d-1} r_i(P_i - P_d))$ in $\mathrm{Jac}(\mathcal{Y}_k)(k)$. We have thus proved that $r_d(\sum_{i=1}^{d-1} r_i(P_i - P_d)) = 0$ in $\mathrm{Jac}(\mathcal{Y}_k)(k)$. Our hypothesis on the quotient of $\mathcal{Y}_k$ by H implies that each $P_i - P_d$ has order p (2.5). Since $r_d(\sum_{i=1}^{d-1} r_i(P_i - P_d)) = 0$ and we assume that $p \nmid r_d$, we can conclude that $\sum_{i=1}^{d-1} r_i(P_i - P_d) = 0$. Then Proposition 2.5 implies that p divides r_i for all $i = 1, \dots, d-1$. Since $|C_0 \cdot C_0| p = r_1 + \cdots + r_d$, it follows that p divides r_d, which contradicts our assumption.

When the quotient of $\mathcal{Y}_k$ by the action of H has positive genus, the image of $(Q_K)_k^0$ under the canonical map $\eta : \mathcal{A}_K \times_{\mathcal{O}_K} \mathcal{O}_L \to \mathcal{A}_L$ is not trivial, and the following additional considerations must be discussed. Let $\mathrm{Norm}(\mathcal{X}')$ denote the normalization of $\mathcal{X}'$ in the field of fractions of $\mathcal{Y}$. Since $\mathcal{Y}$ is integral over $\mathcal{Z}$, we have a natural map $\mathrm{Norm}(\mathcal{X}') \to \mathcal{Y}$. All components of $\mathcal{X}'$ are rational, except possibly the component C_0 ([19], 2.10).

By construction, we have a natural map $\mathrm{Norm}(\mathcal{X}') \to \mathcal{X}' \times_{\mathcal{O}_K} \mathcal{O}_L$. Let $\mathcal{N} \to \mathrm{Norm}(\mathcal{X}')$ denote a resolution of the singularities of $\mathrm{Norm}(\mathcal{X}')$. Consider the commutative diagram of $\mathcal{O}_L$-morphisms:

$$\begin{array}{ccccc} \mathcal{N} & \longrightarrow & \mathrm{Norm}(\mathcal{X}') & \longrightarrow & \mathcal{Y} \\ & & \downarrow & & \downarrow \\ & & \mathcal{X}' \times_{\mathcal{O}_K} \mathcal{O}_L & \longrightarrow & \mathcal{Z} \times_{\mathcal{O}_K} \mathcal{O}_L \end{array}$$

The maps $\mathcal{N} \longrightarrow \mathrm{Norm}(\mathcal{X}') \longrightarrow \mathcal{X}' \times_{\mathcal{O}_K} \mathcal{O}_L$ induce maps of the associated Picard functors

$$\mathrm{Pic}_{\mathcal{X}'/\mathcal{O}_K} \times_{\mathcal{O}_K} \mathcal{O}_L \cong \mathrm{Pic}_{\mathcal{X}' \times_{\mathcal{O}_K} \mathcal{O}_L/\mathcal{O}_L} \longrightarrow \mathrm{Pic}_{\mathrm{Norm}(\mathcal{X}')/\mathcal{O}_L} \longrightarrow \mathrm{Pic}_{\mathcal{N}/\mathcal{O}_L},$$

whose composition induces the canonical map of Néron models

$$\eta : Q_K \times_{\mathcal{O}_K} \mathcal{O}_L \to Q_L.$$

Considering the special fibers over k, we obtain a commutative diagram:

$$\begin{array}{ccc} \mathrm{Pic}^0_{\mathcal{N}_k/k} & \longrightarrow & (Q_L)^0_k \\ \uparrow & & \uparrow \\ \mathrm{Pic}^0_{\mathcal{X}'_k/k} & \longrightarrow & (Q_K)^0_k \end{array}$$

Since we do not have additional information on the special fiber $\mathcal{X}'_k$, we cannot conclude that the bottom horizontal map is an isomorphism. It is however faithfully flat ([24], 4.1.2). Since the special fiber of $\mathcal{Y}$ is reduced, we find that the top horizontal map is an isomorphism ([4], 9.5/4).

Let D denote the irreducible component of $\mathcal{N}_k$ lying above $\mathcal{Y}_k$. The composition $D \hookrightarrow \mathcal{N}_k \to \mathcal{Y}_k$ is an isomorphism. The image of D in $(\mathcal{X}')^{red}_k$ is the curve C_0, and we will identify the map $D \to C_0$ with the quotient map $\rho : \mathcal{Y}_k \to \mathcal{Y}_k / \langle\sigma\rangle$. Consider the following diagram whose top right horizontal morphism is an isomorphism:

$$\begin{array}{ccccc} \mathrm{Pic}^0_D(k) & \longleftarrow & \mathrm{Pic}^0_{\mathcal{N}_k}(k) & \xrightarrow{\sim} & (Q_L)^0_k(k) \\ {\scriptstyle\rho^*}\uparrow & & \uparrow & & \uparrow \\ \mathrm{Pic}^0_{C_0}(k) & \longleftarrow & \mathrm{Pic}^0_{\mathcal{X}'_k}(k) & \longrightarrow & (Q_K)^0_k(k). \end{array}$$

We may now conclude the proof of Theorem 5.3 using the same method as in the case where the reduction of $\mathrm{Jac}(X)/K$ is purely unipotent. Consider again the element $\sum_{i=1}^{d-1} \gcd(r_i, r_d) S_i$ in $\mathrm{Jac}(X)(K)$, which reduces to the element $\sum_{i=1}^{d-1} \gcd(r_i, r_d)\tau_i$ in Φ_M. Proposition 3.6 shows that the latter element is zero in Φ_M. Thus, $\sum_{i=1}^{d-1} \gcd(r_i, r_d) S_i$ reduces in the connected component $(Q_K)^0_k$. Consider now the element $\sum_{i=1}^{d-1} \gcd(r_i, r_d) S_i$ in $\mathrm{Jac}(X_L)(L)$. Our discussion above shows that it reduces to the element $r_d(\sum_{i=1}^{d-1} r_i(P_i - P_d))$ in $\mathrm{Jac}(\mathcal{Y}_k)(k)$.

Since the morphism $\mathrm{Pic}^0_{\mathcal{X}'_k/k} \to (Q_K)^0_k$ is faithfully flat and since each of the above squares commutes, we find that the element $\sum_{i=1}^{d-1} \gcd(r_i, r_d) S_i$, which reduces to $r_d(\sum_{i=1}^{d-1} r_i(P_i - P_d))$ in $\mathrm{Pic}^0_{\mathcal{Y}_k/k}(k)$, in fact reduces to an element in $\rho^*(\mathrm{Jac}(\mathcal{Y}_k/\langle\sigma\rangle))$. Thus, the image of $r_d(\sum_{i=1}^{d-1} r_i(P_i - P_d))$ in $\mathrm{Jac}(\mathcal{Y}_k)/\rho^*(\mathrm{Jac}(\mathcal{Y}_k/\langle\sigma\rangle))$ is trivial. Each $P_i - P_d$ defines an element of order p in $\mathrm{Jac}(\mathcal{Y}_k)/\rho^*(\mathrm{Jac}(\mathcal{Y}_k/\langle\sigma\rangle))$ (2.5). Since $r_d(\sum_{i=1}^{d-1} r_i(P_i - P_d)) = 0$, we conclude that $\sum_{i=1}^{d-1} r_i(P_i - P_d) = 0$. Then Proposition 2.5 implies that p divides r_i for all $i = 1, \dots, d-1$, and since $|C_0 \cdot C_0| p = r_1 + \cdots + r_d$, we find that p divides r_d, which contradicts our assumption.

Now that we know that p divides r_i, we see that the multiplicities on the chain of G that leaves C_0 starting with D_i can only be increasing or constant, because this chain of vertices of degree 2 contains no vertex of self-intersection -1. If D_i is not a node of G, we continue along this chain and find either a terminal vertex, or a node of G. We cannot find a terminal vertex because the multiplicity of a terminal vertex can only be at most the multiplicity of its unique neighbor, with equality only if the self-intersection of the terminal vertex is -1. Thus, G_{Q_i} contains a node of G. □

Remark 5.4 Let N_i denote the intersection matrix of the exceptional divisor, with smooth components and normal crossings, of a resolution of the $\mathbb{Z}/p\mathbb{Z}$-quotient singularity Q_i. We recall here some properties of N_i:

a) It is negative definite (a lemma attributed to Du Val in [10], 14.1).
b) The graph $G(N_i)$ associated with N_i is a tree, and all components of the exceptional divisor are rational ([19], 2.8).
c) Let n_i denote the number of irreducible components in the exceptional divisor. The Smith group $\Phi_{N_i} := \mathbb{Z}^{n_i}/\mathrm{Im}(N_i)$ is killed by p ([19], 2.6).
d) The fundamental cycle Z of N_i is such that $|Z^2| \leq p$ ([19], 2.3, 2.4).

6. The weakly ramified case

We present in this section some applications of Theorem 5.3. Let us recall our notation. Let K be a complete discrete valuation field with valuation v, ring of integers $\mathcal{O}_K$, uniformizer π_K, and residue field k of characteristic $p > 0$, assumed to be algebraically closed. Let X/K be a smooth proper geometrically connected curve of genus $g > 0$. When $g = 1$, we assume in addition that $X(K) \neq \emptyset$.

Assume that X/K does not have semi-stable reduction over $\mathcal{O}_K$, and that it achieves good reduction after a cyclic extension L/K of prime degree p. Let $H = \langle\sigma\rangle$ denote the Galois group of L/K. Let $\mathcal{Y}/\mathcal{O}_L$ be the smooth model of X_L/L. Let $\mathcal{Z}/\mathcal{O}_K$ denote the quotient $\mathcal{Y}/H$, with singular points $Q_1, \ldots, Q_d$, and $d \geq 1$. Recall the regular model $f : \mathcal{X}' \to \mathcal{Z}$ introduced in 5.2.

6.1 The resolution of a singularity Q of $\mathcal{Z}$ is a local process, and depends only on the local ring $\mathcal{O}_{\mathcal{Z},Q}$. It seems therefore natural to try to relate the 'complexity' of the resolution graph to some local invariants of $\mathcal{O}_{\mathcal{Z},Q}$. In this respect, we propose the following.

Consider the Galois morphism $\rho : \mathcal{Y}_k \to \mathcal{Y}_k/\langle\sigma\rangle$. Associated with any point $Q \in \mathcal{Y}_k/\langle\sigma\rangle$ is the following measure of the ramification of ρ over Q:

$$\nu(Q) := \delta(P) = \sum_{j=0}^{\infty}(|H_j(P)| - 1),$$

where P is the preimage of Q in $\mathcal{Y}_k$ and $H_j(P)$ denotes the j-th higher ramification group at P. (For more general morphisms, we would define $\nu(Q) := \sum_{P\in\rho^{-1}(Q)} \delta(P)$.) Recall from 2.2 that the morphism is *weakly ramified* at P if $\delta(P) = 2(p-1)$. Our guess is that $\nu(Q)$ should also be an important measure of how complicated the exceptional divisor of the resolution of Q is. To formulate this guess more precisely, we compare the expressions of the genus g in the Riemann-Hurwitz formula and in the adjunction formula. The Riemann-Hurwitz formula for the morphism ρ can be rephrased as

$$2g = 2g(\mathcal{Y}_k) = 2|H|g(C_0) - 2(|H| - 1) + \sum_{i=1}^{d} \nu(Q_i).$$

Consider now the model $\mathcal{X}'$. By hypothesis, it is minimal with the property that the special fiber has smooth components and normal crossings. Thus, none of the vertices A in the graph $G := G(\mathcal{X}')$ with degree 1 or 2 can have self-intersection -1 (we use here also the fact that only the curve C_0 can have positive genus ([19], 2.10)). Moreover, since the curve X/K has potentially good reduction, the graph $G(\mathcal{X}')$ is a tree ([19], 2.10). The adjunction formula

$$2g - 2 = \mathcal{X}'_k \cdot \mathcal{X}'_k + \mathcal{X}'_k \cdot \Omega,$$

with Ω a relative canonical divisor of $\mathcal{X}'/\mathcal{O}_K$, can be rewritten as

$$\begin{aligned} 2g &= 2|H|g(C_0) + \sum_{\text{vertex } A \text{ of } G} (r(A)-1)(d_G(A)-2) \\ &= 2|H|g(C_0) - 2(|H|-1) \\ &\qquad + \sum_{i=1}^{d}\Big(|H|-1+\sum_{\text{vertex } A \text{ of } G_{Q_i}} (r(A)-1)(d_G(A)-2)\Big) \\ &= 2|H|g(C_0) - 2(|H|-1) + \sum_{i=1}^{d} \gamma_{D_i} g_{D_i}, \end{aligned} \tag{6.1.1}$$

where $D_1, \ldots, D_d$ are the vertices attached to C_0 in the tree $G(\mathcal{X}')$, and the integers γ_{D_i} and g_{D_i} are defined as in 4.1 and (4.1.2). Since the graph G_{D_i} is nothing but the graph G_{Q_i} of the desingularization of Q_i, we define our measure of the desingularization of Q_i to be $\gamma_{Q_i} g_{Q_i} := \gamma_{D_i} g_{D_i}$ for each $i = 1, \ldots, d$. The integer $g_{Q_i} := g_{D_i}$ depends only on the intersection matrix of the desingularization and the marked vertex D_i on its graph. Since $r(C_0) = p$ and is divisible by γ_{Q_i}, we find that $\gamma_{Q_i} = 1$ or p.

6.2 Our guess regarding the resolution $\mathcal{X}' \to \mathcal{Z}$ of the singularities of $\mathcal{Z}$ is that

$$\gamma_{Q_i} g_{Q_i} = \nu(Q_i) \text{ holds for all } i = 1, \ldots, d.$$

This equality would have interesting implications. For instance, since $H = \mathbb{Z}/p\mathbb{Z}$, we always have $\nu(Q)$ divisible by $p-1$, so that $p-1$ divides $\gamma_{Q_i} g_{Q_i}$ when $\gamma_{Q_i} g_{Q_i} = \nu(Q_i)$. Since $\gamma_{Q_i} = 1$ or p, we find that

$$p-1 \text{ divides } g_{Q_i} \text{ when } \gamma_{Q_i} g_{Q_i} = \nu(Q_i).$$

Examples where $g_{Q_i} = 2(p-1)$ and $3(p-1)$ are given in 4.7 and 4.9. It immediately follows from the Riemann-Hurwitz formula and the adjunction formula that:

Lemma 6.3. *With the above notation and hypotheses,*

$$\sum_{i=1}^{d} \nu(Q_i) = \sum_{i=1}^{d} \gamma_{Q_i} g_{Q_i}. \tag{6.3.1}$$

We now prove the equality $\gamma_{Q_i} g_{Q_i} = \nu(Q_i) = 2(p-1)$ for all $i = 1, \ldots, d$ in the weakly ramified case, using Theorem 5.3.

Theorem 6.4. *Let X/K be a curve with potentially good reduction after a ramified extension L/K of prime degree p. Keep the above notation. Then for all $i = 1, \ldots, d$,*

(a) *We have $\gamma_{Q_i} g_{Q_i} \geq 2(p-1)$ and $\nu(Q_i) \geq 2(p-1)$.*
(b) *If the ramification points of $\mathcal{Y}_k \to \mathcal{Y}_k/\langle\sigma\rangle$ are all weakly ramified (in particular, if $\mathcal{Y}_k$ is ordinary), then $\gamma_{Q_i} g_{Q_i} = \nu(Q_i) = 2(p-1)$.*

Proof. (a) The fact that $\nu(Q_i) \geq 2(p-1)$ follows immediately from the properties of a wildly ramified extension: the higher ramification groups H_0 and H_1 must be non-trivial. To prove that $\gamma_{Q_i} g_{Q_i} \geq 2(p-1)$, we note first that Theorem 5.3 shows that $p \mid r_i$. The inequality follows then from Proposition 4.3.

(b) When the ramification points of $\mathcal{Y}_k \to \mathcal{Y}_k/\langle\sigma\rangle$ are all weakly ramified, we have $\nu(Q_i) = 2(p-1)$ (2.2). It follows from (6.3.1) and from the fact that $\gamma_{Q_i} g_{Q_i} \geq 2(p-1)$ proven in (a) that $\gamma_{Q_i} g_{Q_i} = 2(p-1)$. □

Remark 6.5 Without the use of Theorem 5.3, we could only argue that $\gamma_{Q_i} g_{Q_i} \geq p-1$. Indeed, if $r(C_0)$ does not divide $r(D_i)$, then $\gamma_{D_i} = 1$. Then we can use the fact that $g_{Q_i} \geq r(C_0) - 1$ established in 4.10.

Using the notation γ_{Q_i} introduced in this section, we may now state a corollary to Theorem 5.3.

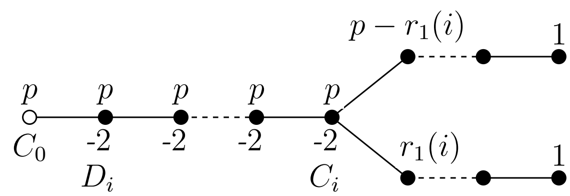
Corollary 6.6. *Let X/K be a curve with potentially good reduction after a wildly ramified Galois extension L/K of degree p, as in* 5.3. *Let N_i denote the intersection matrix associated with the resolution of Q_i. Assume that $\gamma_{Q_i} = 1$. Then p^2 divides* $\det(N_i)$.

Proof. The graph associated with the matrix N_i is G_{Q_i}, with a marked vertex D_i on it. Let R_{D_i} denote the vector of multiplicities of the components of the resolution of Q_i. Then the determinant of N_i can be computed in terms of the coefficients of R_{D_i}/γ_{D_i} (see [19], Theorem 3.14). In particular, it is known that $\frac{r(C_0)}{\gamma_{D_i}} \gcd(\frac{r(C_0)}{\gamma_{D_i}}, \frac{r(D_i)}{\gamma_{D_i}})$ divides $\det(N_i)$. Under our hypotheses, $r(C_0) = p$, p divides $r(D_i)$ (5.3), and $\gamma_{D_i} = 1$. □.

Remark 6.7 Let X/K be a curve with potentially good reduction after a wildly ramified extension L/K of degree p, as in 5.3. Let N_i denote the intersection matrix associated with the resolution of Q_i. Then p kills the Smith group Φ_{N_i} ([19], 2.6) and, thus, $|\det(N_i)|$ is a power of p. It follows from (4.10.3) that $\mathrm{ord}_p(|\det(N_i)|)(p-1) \leq g_{D_i}$.

In the examples of graphs and matrices N_i given in 4.9 with $g_{D_i} = 3(p-1)$, we find that both $|\det(N_i)| = p^2$ and $|\det(N_i)| = p^3$ can occur (in (b) and (c)(ii), respectively, in (a) and (c)(i)).

Theorem 6.8. *Let X/K be a curve with potentially good reduction after a wildly ramified Galois extension L/K of degree p. Assume that all ramification points of $\mathcal{Y}_k \to \mathcal{Y}_k/\langle\sigma\rangle$ are weakly ramified (this is the case if $\mathcal{Y}_k$ is ordinary). Keep the above notation. Then, for all $i = 1, \ldots, d$, we have $r_i = p$, and G_{Q_i} is a graph*[1] *with a single node C_i, of degree* 3*:*



The intersection matrix $N(p, \alpha_i, r_1(i))$ of the resolution of Q_i is uniquely determined as in 4.7 *by the two integers α_i and $r_1(i)$, with $1 \leq r_1(i) < p$. The integer α_i is the number of vertices of self-intersection -2 (including the node C_i) on the chain in G_{Q_i} connecting the node C_0 to the single node C_i of G_{Q_i}, and this integer α_i is divisible by p.*

Proof. Theorem 6.4 (b) shows that $\gamma_{Q_i} g_{Q_i} = 2(p-1)$ for all $i = 1, \ldots, d$. Proposition 4.3 classifies the graphs with $\gamma_{Q_i} g_{Q_i} = 2(p-1)$, and the statement on the shape of the graph follows.

The Smith group of the intersection matrix $N(p, \alpha_i, r_1(i))$ is computed in [19], 3.19 and 3.21, and is found to be of order p^2, and killed by p if and only if p divides α_i. Theorem 2.6(c) of [19] shows that this Smith group must be killed by p. The divisibility $p \mid \alpha_i$ follows. □

[1] A bullet • represents an irreducible component of the desingularization of Q_i. A positive number next to a vertex is the multiplicity of the corresponding component, while a negative number next to a vertex is the self-intersection of the component.

Remark 6.9 It is natural to wonder whether the statements of Theorem 6.4 (b) and 6.8 hold for the resolution of Q_i when P_i is a weakly ramified ramification point of $\mathcal{Y}_k \to \mathcal{Y}_k \langle \sigma \rangle$, without also assuming as we do in 6.4 (b) and 6.8 that all ramification points are weakly ramified.

Corollary 6.10. *Let X/K be a curve with potentially good reduction after a wildly ramified Galois extension L/K of degree p, as in* 6.8. *Suppose that $g > 1$, and that all ramification points of $\mathcal{Y}_k \to \mathcal{Y}_k / \langle \sigma \rangle$ are weakly ramified. Then*
(a) $X(K) \neq \emptyset$.
(b) *Let A/K denote the Jacobian of X/K. Let $\mathcal{A}/\mathcal{O}_K$ be its Néron model. Then the unipotent part U/k of the connected component of the identity in $\mathcal{A}_k/k$ is a product of additive groups $\mathbb{G}_{a,k}$.*
(c) *The group of components $\Phi_{A,K}$ of the Néron model is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{2d-2}$.*

Proof. Part (a) is immediate since it follows from 6.8 that a regular model of X/K contains a component of multiplicity 1. It follows from [22], 2.4, that p kills U, since the maximal multiplicity in the regular model $\mathcal{X}'/\mathcal{O}_K$ is equal to p. That U is now split follows from [27], Ch. VII, no 11, Proposition 11. This proves (b).

The order of $\Phi_{A,K}$ can be computed using the intersection matrix of the regular model $\mathcal{X}'$. Since the associated graph is a tree, we find using [13], 2.5, that $|\Phi_{A,K}| = p^{2d-2}$. Part (c) follows since $\Phi_{A,K}$ is killed by $[L : K]$ because A/K has potentially good reduction ([5]). □

Note that in general the special fiber $\mathcal{A}_k/k$ need not be killed by p, even when its subgroup U and quotient $\Phi_{A,K}$ are both killed by p (see [11] for a general discussion of such phenomena).

6.11 Let A/K be the Jacobian of a smooth proper and geometrically connected curve X/K having a K-rational point. For use in our next corollary, we recall below the main result of [3], Theorem 4.6. Identify A/K with its dual A'/K via the map $-\varphi_{[\Theta]} \colon A \to A'$ as in [3], just before 4.6. Let $\mathcal{X}/\mathcal{O}_K$ denote a regular model of X/K. Let M be the intersection matrix of $\mathcal{X}_k$. Identify, as recalled in [3], 2.3, the component group $\Phi_{A/K}$ with the group of components Φ_M of M (Φ_M is the torsion subgroup of $\mathbb{Z}^v/\mathrm{Im}(M)$). Then Grothendieck's pairing

$$\langle\ ,\ \rangle_K \colon \Phi_{A/K} \times \Phi_{A/K} \longrightarrow \mathbb{Q}/\mathbb{Z}$$

coincides with the pairing $\langle\ ,\ \rangle_M \colon \Phi_{A/K} \times \Phi_{A/K} \longrightarrow \mathbb{Q}/\mathbb{Z}$ considered in 3.1. In particular, this pairing is non-degenerate. Recall also the definition of the functorial subgroup $\Phi^0_{A/K}$ of $\Phi_{A/K}$ in 1.3. We denote by $(\Phi^0_{A/K})^\perp$ the orthogonal of $\Phi^0_{A/K}$ under Grothendieck's pairing.

Corollary 6.12. *Let A/K be the Jacobian of a curve X/K of genus $g > 1$ having potentially good reduction after a Galois extension L/K of degree p, as in* 6.8. *Assume that all ramification points of $\mathcal{Y}_k \to \mathcal{Y}_k / \langle \sigma \rangle$ are weakly ramified. Then $\Phi_{A/K}$ is a $\mathbb{Z}/p\mathbb{Z}$-vector space of dimension $2d-2$, and $\Phi^0_{A/K}$ is a subspace of dimension $d-1$. Moreover, $\Phi^0_{A/K} = (\Phi^0_{A/K})^\perp$.*

Proof. It follows from 6.10 that $X(K) \neq \emptyset$. We can thus use the results of [3] recalled above. We produce below explicit generators for the groups $\Phi_{A/K}$ and $\Phi^0_{A/K}$. For each singular point Q_i on the model $\mathcal{Z}/\mathcal{O}_K$, denote by A_i and B_i the terminal components of multiplicity 1 in the exceptional divisor of the resolution of Q_i in $\mathcal{X}'$. Let $\boldsymbol{\alpha}_i$ denote the image in $\Phi_{A/K}$ of the vector $E(A_i, B_i)$, $i = 1, \ldots, d-1$ (notation as in 3.1). Let $\boldsymbol{\beta}_i$ denote the image in $\Phi_{A/K}$ of the vector $E(A_i, A_d)$, $i = 1, \ldots, d-1$. We have seen in 6.10 that $\Phi_{A/K}$ is a $\mathbb{Z}/p\mathbb{Z}$-vector space of dimension $2(d-1)$.

We claim that $\{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{d-1}, \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{d-1}\}$ *is a basis for* $\Phi_{A/K}$*, and that* $\{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{d-1}\}$ *is a basis for* $\Phi^0_{A/K}$. To prove our claim, consider the matrix $V := (\langle \boldsymbol{\alpha}_i, \boldsymbol{\beta}_j \rangle)_{1 \leq i,j \leq d-1}$ with coefficients in $\mathbb{Q}/\mathbb{Z}$. We can use the computation (4.8.1) to show that V is the diagonal matrix $\operatorname{diag}(c_1/p \pmod{\mathbb{Z}}, \ldots, c_{d-1}/p \pmod{\mathbb{Z}})$, where for each $i = 1, \ldots, d-1$, $0 < c_i < p$ and p divides $c_i r_1(i) - 1$. In particular, $c_i/p \neq 0$ in $\mathbb{Q}/\mathbb{Z}$. It follows that the set $\{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{d-1}, \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{d-1}\}$ is linearly independent in $(\mathbb{Z}/p\mathbb{Z})^{2d-2}$. Hence, it is a basis.

It follows from the explicit computations in [17], 3.7 (a), that $\langle \boldsymbol{\alpha}_i, \boldsymbol{\alpha}_j \rangle = 0$ for all $1 \leq i, j \leq d-1$. Since the pairing $\langle\ ,\ \rangle$ is perfect on $(\mathbb{Z}/p\mathbb{Z})^{2d-2}$, we find that $\{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{d-1}\}$ generates a maximal isotropic subspace.

It remains to show that $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{d-1}$ belong to $\Phi^0_{A/K}$, and that neither $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{d-1}$, nor any non-trivial linear combination of $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{d-1}$, belong to $\Phi^0_{A/K}$. For this, since K is complete, we can pick K-rational points a_i and b_i of X ($i = 1, \ldots, d-1$) whose closure in $\mathcal{X}'$ intersect $\mathcal{X}'_k$ in a smooth point of A_i and B_i, respectively (see, e.g., [4] 9.1/9). Then $a_i - b_i$ and $a_i - a_d$ are divisors of degree 0 on X, which we identify with K-rational points in the Jacobian A/K of X/K. These rational points reduce in the component group $\Phi_{A/K}$ of the Néron model of A/K to the points $\boldsymbol{\alpha}_i$ and $\boldsymbol{\beta}_i$, respectively. Since $A(K) \subset A(L)$, we can reduce $a_i - b_i$ in the special fiber of the Néron model $\mathcal{A}'/\mathcal{O}_L$. This special fiber is isomorphic to the Jacobian of the special fiber $\mathcal{Y}_k$ of the smooth model $\mathcal{Y}/\mathcal{O}_L$ of X_L/L. It is clear that by construction, the reduction of $a_i - b_i$ is trivial, so that $\boldsymbol{\alpha}_i \in \Phi^0_{A/K}$ for $i = 1, \ldots, d-1$. On the other hand, the reduction of $a_i - a_d$ is the divisor $P_i - P_d$, which is a non-trivial p-torsion point when viewed in the quotient $\mathcal{A}'_k/\eta(\mathcal{A}_k)$. This shows that $\boldsymbol{\beta}_i \notin \Phi^0_{A/K}$ for $i = 1, \ldots, d-1$. Moreover, any non-trivial linear combination of the images of the divisors $P_i - P_d$ is not zero in $\mathcal{A}'_k/\eta(\mathcal{A}_k)$ (2.5), so no non-trivial linear combination of $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{d-1}$ belongs to $\Phi^0_{A/K}$. □

Example 6.13 Examples of curves having good reduction after an extension of degree p can be obtained as twists as follows. Choose a smooth proper curve C/k having an automorphism σ_k of order p. Over an appropriate ring $\mathcal{O}_K$ with residue field k, there exists a smooth scheme $\mathcal{Y}^0/\mathcal{O}_K$ with an $\mathcal{O}_K$-automorphism σ such that C is k-isomorphic to $\mathcal{Y}^0_k$, and σ restricted to $\mathcal{Y}^0_k$ induces the given automorphism σ_k. It is shown in [25], section IV, Thm. 2.2, that one can take $\mathcal{O}_K$ to be the Witt ring $W(k)(\zeta_p)$, with ζ_p a primitive p-th root of unity. If one wants a lift in equicharacteristic p, one can trivially take $\mathcal{O}_K = k[[t]]$.

Choose any cyclic (ramified) extension L/K of degree p. The twist of $\mathcal{Y}^0_K/K$ by L/K and σ is a curve X/K which achieves good reduction over L. Starting with an ordinary curve C/k produces a curve X/K having potentially good ordinary reduction over L.

Corollary 6.14. *Fix any odd prime p. For each integer $m > 0$, there exist a regular local ring B of equicharacteristic p endowed with an action of $H := \mathbb{Z}/p\mathbb{Z}$, and a regular local ring B' of mixed characteristic $(0,p)$ endowed with an action of $\mathbb{Z}/p\mathbb{Z}$, such that* $\operatorname{Spec} B^H$ *and* $\operatorname{Spec}(B')^H$ *are singular exactly at their closed point, and the graphs associated with a minimal resolution of* $\operatorname{Spec} B^H$ *and* $\operatorname{Spec}(B')^H$ *have one node and more than m vertices.*

Proof. As we noted in 6.13, there exist a field K of either mixed characteristic $(0,p)$ or of equicharacteristic p and a curve X/K without good reduction over K, and with good ordinary reduction over a Galois extension L/K of degree p. Let $H := \operatorname{Gal}(L/K)$. Let $\mathcal{Y}/\mathcal{O}_L$ denote the smooth model of X_L/L. Let $\mathcal{Z}/\mathcal{O}_K$ denote the quotient $\mathcal{Y}/H$. Let P denote a ramification point of the morphism $\mathcal{Y}_k \to \mathcal{Y}_k/H$, and let $B := \mathcal{O}_{\mathcal{Y},P}$. Theorem

6.8 shows that the resolution of singularity of Spec B^H has an intersection matrix of type $N(p, \alpha, r_1)$ for some $\alpha \geq 1$ and $0 < r_1 < p$.

Immediately after the statement of Theorem 6.8 given in the introduction, we briefly alluded to the fact that the integer α is likely to be related to the valuation of the different of L/K. Thus, in principle, by choosing K and L/K appropriately, the above method will produce examples with α as large as desired. Since at this time we do not know how to prove in general that α is related to the valuation of the different of L/K (except when $p = 2$, and $g = 1$, see [19], 4.1), we proceed below with a different argument to prove the existence of resolutions with α as large as desired.

Consider a quadratic extension K'/K. Since p is odd by hypothesis, the extension K'/K is tame, and one knows how to compute a regular model of $X_{K'}/K'$ from the model $\mathcal{X}/\mathcal{O}_K$ of X/K obtained in Theorem 6.8: Simply normalize the base change $\mathcal{X} \times_{\mathcal{O}_K} \mathcal{O}_{K'}$ and resolve its singularities. A singularity on the normalization can only be the preimage of a closed point of $\mathcal{X}_k$ that belongs to two irreducible components of $\mathcal{X}_k$, and such that both components have odd multiplicity. This singular point is resolved by a single smooth rational curve.

Let $L' := LK'$, with $[L' : K'] = p$. The curve $X_{K'}/K'$ achieves good ordinary reduction over L'. The model $\mathcal{Y}'/\mathcal{O}_{L'} := \mathcal{Y} \times_{\mathcal{O}_L} \mathcal{O}_{L'}$ is smooth, and we let P' denote the preimage of P under the natural map $\mathcal{Y}' \to \mathcal{Y}$. Let $B' := \mathcal{O}_{\mathcal{Y}',P'}$. We leave it to the reader to check, using [7], 4.3, and the desingularization of the normalization of $\mathcal{X} \times_{\mathcal{O}_K} \mathcal{O}_{K'}$, that the resolution of the singularity of Spec$(B')^H$ has an intersection matrix of type $N(p, 2\alpha, r_1')$, where $r_1' := r_1/2$ if r_1 is even, and $r_1' := (r_1 + p)/2$ if r_1 is odd.

Since we can make an infinite chain of quadratic extensions $K \subset K' \subset K'' \subset \dots$, and since the graph associated with $N(p, \beta, r_1)$ has at least β irreducible components, the corollary is proved. □

Remark 6.15 Consider an intersection matrix N, and assume that for some prime p, it satisfies all the conditions listed in 5.4, conditions which would have to be satisfied if this intersection matrix was associated with the resolution of a $\mathbb{Z}/p\mathbb{Z}$-singularity: its graph $G(N)$ is a tree, $|\det(N)|$ is a power of p, the Smith group Φ_N is killed by p, and the fundamental cycle Z has $|Z^2| \leq p$. If $\det(N) = 1$ and $G(N)$ is a tree, then the above conditions are satisfied for every prime at least equal to $|Z^2|$. In particular, when $\det(N) = 1$, the matrix N could potentially be associated with the resolution of a $\mathbb{Z}/p\mathbb{Z}$-singularity for infinitely many primes p.

An interesting consequence of our guess in 6.2 that $\gamma_{Q_i} g_{Q_i} = \nu(Q_i)$ holds for all $i = 1, \dots, d$, is that a matrix N as above can be associated with the resolution of a $(\mathbb{Z}/p\mathbb{Z})$-quotient singularity $\mathcal{X}' \to \mathcal{Z}$ occurring in models of curves as at the beginning of this section *only for finitely many primes* p. Indeed, the choice of a vertex D on N lets us define the integer g_D associated with N and D. If N is the intersection matrix of the resolution of a singularity Q_i of $\mathcal{Z}$ with the marked vertex D linked to C_0, we noted in 6.2 that $p - 1$ must then divide g_D when the equality $\gamma_{Q_i} g_{Q_i} = \nu(Q_i)$ holds. Since there are only finitely many vertices D, the set of integers g_D is finite and, hence, any prime p larger than the maximum of the integers g_D cannot have the property that $p - 1$ divides some g_D.

Remark 6.16 Let X/K be a curve with potentially good reduction over an extension L/K of degree p, as at the beginning of this section. Let Q_i be a singular point of the quotient $\mathcal{Z}$, and consider the graph G_{Q_i} associated with the resolution of Q_i in $\mathcal{X}' \to \mathcal{Z}$. One may wonder whether a node of G in G_{Q_i} could have its multiplicity in $\mathcal{X}'_k$ divisible by p^2. Similar considerations are found in [18], Question 1.4.

References

[1] A. Altman and S. Kleiman, *Introduction to Grothendieck duality theory*, Lecture Notes in Mathematics **146**, Springer-Verlag, Berlin-New York, 1970.
[2] M. Artin, *Wildly ramified* $\mathbb{Z}/2\mathbb{Z}$ *actions in dimension* 2, Proc. AMS **52** (1975), 60-64.
[3] S. Bosch and D. Lorenzini, *Grothendieck's pairing on component groups of Jacobians*, Invent. Math. **148** (2002), 353–396.
[4] S. Bosch, W. Lüktebohmert, and M. Raynaud, *Néron Models*, Springer Verlag, 1990.
[5] B. Edixhoven, Q. Liu, and D. Lorenzini, *The p-part of the group of components of a Néron model*, J. of Alg. Geom. **5** (1996), 801-813.
[6] O. Gabber, Q. Liu, and D. Lorenzini, *The index of an algebraic variety*, Invent. Math., **192** Issue 3 (2013), 567–626.
[7] L. H. Halle, *Stable reduction of curves and tame ramification*, Math. Z. **265** (2010), no. 3, 529-550.
[8] H. Hasse, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*, J. reine angew. Math. **172** (1934), 37–54.
[9] T. Katsura, *On Kummer surfaces in characteristic* 2, Proc. Int. Symp. on Algebraic Geometry (Kyoto Univ., Kyoto, 1977), 525–542, Kinokuniya Book Store, Tokyo, 1978.
[10] J. Lipman, *Rational singularities, with applications to algebraic surfaces and unique factorization*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 195–279.
[11] Q. Liu and D. Lorenzini, *Special fibers of Néron models and wild ramification*, J. reine angew. Math. **532** (2001), 179–222.
[12] Q. Liu, D. Lorenzini, and M. Raynaud, *Néron models, Lie algebras, and reduction of curves of genus one*, Invent. Math. **157** (2004), 455–518.
[13] D. Lorenzini, *Arithmetical graphs*, Math. Ann. **285** (1989), 481-501.
[14] D. Lorenzini, *Dual graphs of degenerating curves*, Math. Ann. **287** (1990), 135 - 150.
[15] D. Lorenzini, *Groups of components of Néron models of Jacobians*, Comp. Math. **73** (1990), 145–160.
[16] D. Lorenzini, *On the group of components of a Néron model*, J. reine angew. Math. **445** (1993), 109-160.
[17] D. Lorenzini, *Reduction of points in the group of components of the Néron model of a Jacobian*, J. reine angew. Math. **527** (2000), 117–150.
[18] D. Lorenzini, *Models of curves and wild ramification*, Pure Appl. Math. Q. (Special issue in honor of John Tate), **6** (2010) no 1, 41–82.
[19] D. Lorenzini, *Wild quotient singularities of surfaces*, to appear in Math. Zeit.
[20] D. Lorenzini, *Wild quotients of products of curves*, Preprint.
[21] D. Lorenzini and T. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), 47-77.
[22] D. Penniston, *Unipotent groups and curves of genus* 2, Math. Ann. **317** (2000), 57-78.
[23] B. Peskin, *Quotient singularities and wild p-cyclic actions*, J. Algebra **81** (1983), 72-99.
[24] M. Raynaud, *Spécialisation du foncteur de Picard*, Publ. Math. IHES **38** (1970), 27–76.
[25] T. Sekiguchi, F. Oort, and N. Suwa, *On the deformation of Artin-Schreier to Kummer*, Ann. Sci. École Norm. Sup. (4) **22** (1989), 345–375.
[26] J.-P. Serre, *Corps Locaux*, Hermann, 1968.
[27] J.-P. Serre, *Groupes Algébriques et Corps de Classes*, Hermann, Paris (1959).
[28] B. Singh, *On the group of automorphisms of function field of genus at least two*, J. Pure Appl. Algebra **4** (1974), 205–229.
[29] D. Subrao, *The p-rank of Artin-Schreier curves*, Manuscripta Math. **16** (1975), 169–193.
[30] E. Viehweg, *Invarianten der degenerierten Fasern in lokalen Familien von Kurven*, J. reine angew. Math. **293/294** (1977), 284–308.
[31] G. Winters, *On the existence of certain families of curves*, Amer. J. Math. **96** (1974), 215–228.

Department of mathematics, University of Georgia, Athens, GA 30602, USA.
E-mail address: `lorenzin@uga.edu`