Rigidity, Reduction, and Ramification

Irene I. Bouw and Rachel J. Pries

Abstract

In this paper we consider wildly ramified G-Galois covers of curves $f : Y \to \mathbb{P}^1_k$ branched at exactly one point over an algebraically closed field k of characteristic p. By computing the reduction of Galois covers of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ branched at 3 points, we prove existence and nonexistence results for such covers f with specified inertia groups and conductors above infinity. These results show that the existence of covers with given inertia in characteristic p is closely related to the arithmetic of covers in characteristic zero. For G equal to A_p or $\mathrm{PSL}_2(p)$, we show that all possible inertia groups occur and that the set of conductors that occur depends on the group.

2000 Mathematical Subject Classification: 14H30, 14G32

1 Introduction

Let k be an algebraically closed field of characteristic p. Understanding the fundamental group of the affine line over k is a hard problem. By Abhyankar's Conjecture, we know a group G occurs as the Galois group of a cover $f : Y \to \mathbb{P}^1_k$ branched only at ∞ if and only if G is a quasi-p group, which means that G is generated by its Sylow p-subgroups, [14]. This determines the set of finite quotients of $\pi_1(\mathbb{A}^1_k)$, but we are far from formulating an analog of Riemann's Existence Theorem. For instance, it is not even known which groups occur as inertia groups above ∞ for such covers f.

Conjecture 1 (Inertia Conjecture) Let G be a finite quasi-p group. Let I be a subgroup of G which is an extension of a cyclic group of order prime-to-p by a p-group P. Suppose that the conjugates of P generate G. Then there exists a G-Galois cover $f : Y \to \mathbb{P}^1_k$ branched only at ∞ with inertia group I at some point of $f^{-1}(\infty)$.

The Inertia Conjecture was formulated by Abhyankar. It is straight forward that the condition on I is necessary. The only subgroups satisfying this condition which are known to occur as inertia group of a G-Galois cover of $\mathbb{P}^1_k$ branched only at ∞ are the Sylow p-subgroups P of G, [7].

Question 2 Suppose there exists a G-Galois cover $f : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia group I. Which filtrations of higher ramification groups occur for such covers?

Results in this paper indicate that the answer to this question may not be easy to formulate in general.

We explore these questions in the case that p exactly divides the order of a quasi-p group G. This is the simplest case; for example, the filtration of higher ramification groups of an inertia group $I \simeq \mathbb{Z}/p \rtimes \mathbb{Z}/n$ is determined by the conductor h. We restrict to inertia groups I for which the prime-to-p part of the center is trivial. For such I, the order of I and the conductor h can be encoded in the invariant $\sigma := h/n$.

The main observation of this paper is that there is a relationship between the existence of G-Galois covers of $\mathbb{P}^1_k$ branched at exactly one point and the arithmetic of covers in characteristic zero. For example, we show that if all covers of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ branched at three points of order p are defined over a small number field then there is no cover of $\mathbb{P}^1_k$ branched at one point with invariant $\sigma = 2$, Lemma 4.3.2. We mainly focus on two classes of groups: A_p and $\mathrm{PSL}_2(p)$. Both groups have the same set of possible inertia groups. But $\mathrm{PSL}_2(p)$ has many (almost) rigid triples whereas A_p has very few. Using this, we prove that the set of σ's that occur depends on the group. The following theorem is proved in Section 5.4.

Theorem 3 *Suppose that $p \geq 7$. Let $m = (p-1)/2$. There exists an A_p-Galois cover of $\mathbb{P}^1_k$ branched only at ∞ with $\sigma = (p-2)/m$, but there is no $\mathrm{PSL}_2(p)$-Galois cover of $\mathbb{P}^1_k$ branched only at ∞ with $\sigma = (p-2)/m$.*

We show that the Inertia Conjecture is true for A_p and $\mathrm{PSL}_2(p)$, giving the first serious evidence for this conjecture. There are some obvious restrictions on σ coming from the Riemann–Hurwitz formula and the Hasse–Arf Theorem, Section 2.1. We show that any sufficiently large σ satisfying these conditions occurs.

Theorem 4 *Suppose $p \geq 5$. Let G be A_p or $\mathrm{PSL}_2(p)$. There exists an (explicit) constant C, depending on G, such that all $\sigma \geq C$ satisfying the obvious necessary conditions describe the ramification of some G-Galois cover $Y \to \mathbb{P}^1_k$ branched at exactly one point.*

The paper also contains some results on Galois covers of $\mathbb{P}^1_k$ branched at one point with Galois group $\mathrm{PSL}_2(\ell)$ where $p \neq \ell$ exactly divides the order of G. Here we prove the Inertia Conjecture for inertia groups I such that the prime-to-p part of the center of I is trivial. In addition, for I the dihedral group of order $2p$ we show that all σ satisfying the necessary conditions occur. For I cyclic of order p we show that all σ satisfying the necessary conditions occur, except possibly $\sigma = 2$ for $\ell \equiv \pm 3 \bmod 8$.

The main technique we use to construct G-Galois covers of $\mathbb{P}^1_k$ is to reduce covers of $\mathbb{P}^1$ from characteristic zero to characteristic p. This approach, introduced by Raynaud in [14], starts with a G-Galois cover $Y_K \to X_K$ in characteristic zero such that p divides the ramification indices. This cover will have bad reduction to characteristic p. Denote the stable reduction by $f : Y \to X$. Under some conditions on the group, there exists a component W of X such that $f|_W$ is a G-Galois cover which is wildly ramified above exactly one point. Moreover, every G-Galois cover of $\mathbb{P}^1_k$ branched at exactly one point will occur over a component of the stable reduction of some cover of $\mathbb{P}^1_K$, Proposition 3.3.3.

In Raynaud's original approach [14], no statements were made on the inertia that occurs for the G-Galois covers constructed by reduction. The key ingredient we use to get information on the inertia is the action of the monodromy on the stable reduction. This provides a link between arithmetic information (like field of moduli) of covers in characteristic zero and the ramification of covers in characteristic p. Our results illustrate that the action of the monodromy on the stable reduction poses strong restrictions on the inertia that can occur over the tails of the stable reduction; see for example Proposition 4.5.2. Roughly speaking, the tails of the reduction of a cover defined over a small number field will have large inertia group. However, in general, these restrictions are not sufficient to completely describe the stable reduction. To do this, we use additional information such as the reduction of the modular curve $X_0(p)$ and some computations on equations for covers discovered by Abhyankar.

We only consider the reduction of covers of $\mathbb{P}^1_K$ branched at three points. All covers of $\mathbb{P}^1_k$ branched at one point constructed in this way have small σ. To obtain existence results for arbitrary large σ, we use patching in equal characteristic following [11].

2 Preliminaries

2.1 Background

Let k be an algebraically closed field of characteristic p. Let G be a finite group. Let I be a subgroup of G which is an extension of $\mathbb{Z}/n$ by $\mathbb{Z}/p$ with $\gcd(n,p) = 1$. Let n'' be the order of the prime-to-p part of the center of I. Let n' be such that $m = n''n'$. If c generates $\mathbb{Z}/n$, then the subgroup $\langle c^{n'} \rangle$ is precisely the subgroup of $\mathbb{Z}/n$ which acts trivially on $\mathbb{Z}/p$. Also, $n'|(p-1)$.

Consider a (wildly ramified) G-Galois cover of smooth connected k-curves $f : Y \to \mathbb{P}^1_k$ branched at a point ξ. (Unless otherwise mentioned, if $f : Y \to \mathbb{P}^1_k$ is a G-Galois cover of curves then we assume Y is smooth and connected.) Let π_η be a uniformizer of Y at $\eta \in f^{-1}(\xi)$ and I the inertia group of η. Recall that the *filtration of higher ramification groups* $\{I_i : i \in \mathbb{N}^+\}$ of the inertia group I at η is defined as follows: if $g \in I$ then $g \in I_i$ if and only if $g(\pi_\eta) \equiv \pi_\eta \mod \pi_\eta^{i+1}$. Recall that the *conductor* of f at η is the largest integer h such that $I_h \neq \{1\}$. The number h is also called the *lower jump* for f since it is the jump in the filtration of higher inertia groups in the lower numbering. The upper jump, (in other words, the jump in the filtration of higher inertia groups in the upper numbering) is $\sigma = h/n \in \mathbb{Q}$, [17, Chapter 4].

There are some necessary conditions on the invariants associated to a G-Galois cover $f : Y \to \mathbb{P}^1_k$ whose branch locus is at most two points and which has inertia I above ∞. In particular, there is a lower bound on the conductor.

Lemma 2.1.1 *Suppose $f : Y \to \mathbb{P}^1_k$ is a G-Galois cover with branch locus contained in $\{0, \infty\}$. Suppose that the inertia group above 0 has order n_0 and the inertia group I above ∞ is wild with order pn and conductor h, where $\gcd(nn_0, p) = 1$. Let n'' be the order of the prime-to-p part of the center of I. Then the values of n and h satisfy the following conditions:*

(a) *The numbers h and n satisfy $h \in \mathbb{N}^+$, $\gcd(h,p) = 1$, and $\gcd(h,n) = n''$.*

(b) *If $G \neq I$, a lower bound for the conductor is $h \geq (np + n_0)/n_0(p-1)$.*

(c) *In particular, if $n_0 = 1$ and $G \neq \mathbb{Z}/p$ then $h \geq n + n''$.*

Proof: By the Riemann-Hurwitz formula, if $r = \#G/np$ is the number of ramification points above ∞, then the genus of Y satisfies

$$g = 1 + \frac{r}{2}(h(p-1) - p\frac{n}{n_0} - 1).$$

The other parts of the proof are immediate from the description of the I-Galois germ of the cover near ∞. □

By Lemma 2.1.1, the conductor h of a G-Galois cover $f : Y \to \mathbb{P}^1$ branched only at ∞ and having inertia $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n$ satisfies $h \equiv an'' \bmod n$ for some a such that $1 \leq a \leq n'$ and $\gcd(a, n') = 1$. Given I and a as above, define $h_{\min}(I,a) = 2n + n''$ if $a = 1$ and $n' = p-1$ and define $h_{\min}(I,a) = n + an''$ otherwise. Note that if h is the conductor of f and $h \equiv an'' \bmod n$ then $h_{\min}(I,a)$ is the minimal possibility for h. Let $h_{\min}(I)$ be the set of all $h_{\min}(I,a)$ for $1 \leq a \leq n'$ and $\gcd(a, n') = 1$.

An alternative definition of the set of values $h_{\min}(I)$ is that the corresponding invariant $\sigma = h/n$ is less than or equal to $(2p-1)/(p-1)$. A geometric interpretation for these σ is that a G-Galois cover $Y \to \mathbb{P}^1_k$ branched at one point with inertia group $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n$ has a non-isotrivial deformation in equal characteristic p if and only if $\sigma > (2p-1)/(p-1)$ [12, Theorem 3.1.11].

The main result of [11] is that under certain conditions on G there exists some $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n \subset G$ and a G-Galois cover $f : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia I and conductor in the set of minimal values $h_{\min}(I)$. The proof of this result involves repeatedly degenerating a cover of $\mathbb{P}^1_k$ branched at exactly one point until the covers of the tails of the reduction have small conductor. In this paper, we use instead reduction of covers of $\mathbb{P}^1$ branched at three points from characteristic 0 to characteristic p. By using information on the field of moduli of the cover in characteristic zero, we are able to prove stronger existence results than in [11]. For example, for G is $\mathrm{PSL}_2(p)$, A_p, or $\mathrm{PSL}_2(\ell)$ (where p strictly divides $\ell \pm 1$) we find a specific inertia group I and minimal conductor $h \in h_{\min}(I)$ for which there exists such a G-Galois cover with inertia I and conductor h.

The following lemma is a version of Abhyankar's lemma. We use it to construct covers branched at one point from covers branched at two points.

Lemma 2.1.2 *Suppose there exists a G-Galois cover $f : Y \to \mathbb{P}^1_k$ with branch locus contained in $\{0, \infty\}$. Suppose that f has inertia group $\mathbb{Z}/n_0$ above 0 and inertia group $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n$ above ∞ with conductor h for some n, n_0 prime-to-p. Let $n^* = \gcd(n, n_0)$. Let $\psi : Z \to \mathbb{P}^1_k$ be the n_0-cyclic cover branched at 0 and ∞. Assume f and ψ are linearly disjoint. Then there exists a G-Galois cover $f' : Y' \to \mathbb{P}^1_k$ branched at exactly one point with inertia group $I' \subset I$ of order pn/n^* and with conductor hn_0/n^*.*

Proof: Choose Y' to be the normalization of $Y \times_{\mathbb{P}^1} Z$ and choose $f' = Y' \to Z$ to be the normalized pullback of f by ψ. Note that genus$(Z) = 0$ and Y' is smooth. Also Y' is connected since f and ψ are linearly disjoint and thus f' is Galois with group G. By Abhyankar's Lemma, f' is now étale over $\psi^{-1}(0)$.

Choose a wildly ramified point $\eta \in Y$. By Abhyankar's Lemma, there are n^* wildly ramified points of Y' lying above η. Choose η' to be one of these points. Replace Y (respectively Y') with the germ of the curve Y at η (respectively Y' at η'). Replace Z with the germ of the curve Z at $f'(\eta')$. Let X (respectively X') be the quotient germ of Y (respectively Y') by $\mathbb{Z}/p$. The cover $Y' \to X$ of germs of curves is cyclic of order pn_0/n^* and is totally ramified at the closed point. Since it dominates the cover $Y \to X$ of germs of curves, it has upper jump h and thus lower jump hn_0/n^*. So the lower jump of $Y' \to X'$ is hn_0/n^*. By Abhyankar's lemma, the cover $X' \to Z$ of germs of curves has order n/n^*. Thus the inertia group of f' at η' is $\mathbb{Z}/p \rtimes \mathbb{Z}/(n/n^*)$ and the conductor is hn_0/n^*. □

Note that the upper jumps σ of f and σ' of f' satisfy $\sigma' = \sigma n_0$.

2.2 Construction of covers via patching

Given a G-Galois cover f with inertia group $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n$, Theorem 2.2.1 allows us to increase the conductor of f by multiples of n. Given two covers f_1 and f_2, Theorem 2.2.2 allows us to change the congruence value of the conductors mod n. The proof of Theorem 2.2.1 (respectively 2.2.2) uses formal patching to construct a family of covers of $\mathbb{P}^1$ over a base Ω so that the following are true: the normalization of the fiber over one point of Ω is f (respectively a semi-stable cover determined by f_1 and f_2); the fiber over the generic geometric point of Ω is a new cover with the desired properties.

Theorem 2.2.1 *Let $f : Y \to X$ be a G-Galois cover of k-curves which is branched at exactly one point ξ. Suppose f has inertia group $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n$ and conductor h at ξ. Let $i \in \mathbb{N}^+$ be such that $(h + in, p) = 1$. Then there exists a G-Galois cover $f' : Y' \to X$ of smooth connected curves branched exactly at the point ξ with inertia I and conductor $h + in$.*

Proof: This is a special case of [11, Theorem 2.3.1]. □

Theorem 2.2.2 *Let G be a group generated by subgroups G_1 and G_2. Let $f_1 : X \to \mathbb{P}^1_k$ and $f_2 : Y \to \mathbb{P}^1_k$ be Galois covers each branched at exactly one point. Suppose f_i has group G_i, inertia I_i, and conductor h_i respectively. Suppose $I_2 \subset I_1 = \mathbb{Z}/p \rtimes \mathbb{Z}/n$ with index r for some r with*

$\gcd(r,p)=1$. *Assume that* $h_2=\gamma h_1$ *for some* γ *such that* $\gcd(\gamma,n)=1$. *Let* $e=h_1+h_2r$ *and let* $c=\gcd(n,e/g')$. *Assume that* $\gcd(e,p)=1$. *Then there exists a* G*-Galois cover* $f':Y'\to\mathbb{P}^1_k$ *branched at exactly one point whose inertia group is the unique subgroup of* I_1 *with order* pn/c *and whose conductor is* e/c.

Proof: This is a special case of [11, Theorem 2.3.4] which is true under less restrictive hypotheses. □

Note that the upper jumps σ', σ_1, and σ_2 of respectively f', f_1 and f_2 in Theorem 2.2.2 satisfy $\sigma'=\sigma_1+\sigma_2$.

3 Stable reduction of Galois covers

3.1 The stable model

Let R_0 be a complete discrete valuation ring whose residue field k is algebraically closed of characteristic p and whose fraction field K_0 is of characteristic zero. Let $f_{K_0}:Y_{K_0}\to X_{K_0}$ be a Galois cover with Galois group G defined over K_0. Note that the branch points of f are not assumed to be K_0-rational. Let $x_1,\dots,x_r$ be the branch points and $y_1,\dots,y_s$ the ramification points of f_{K_0}. To avoid trivial examples, we suppose that $g(X_{K_0})+r\geq 3$. Note that this implies that $g(Y_{K_0})+s\geq 3$.

A *semi-stable* curve over a scheme S is a flat projective morphism $X\to S$ whose geometric fibers are reduced connected curves having at most ordinary double points as singularities. A *mark* C on X/S is a closed subscheme of the smooth locus of X which is the disjoint union of sections $x_i:S\to X$. A marked semi-stable curve $(X;x_i)/S$ is *stably marked* if every geometric fiber X_s satisfies the following condition: every irreducible component of genus zero has at least three points which are either singular in X_s or specializations of the marked points x_i.

Definition 3.1.1 Let R/R_0 be a finite extension of discrete valuation rings. Denote the fraction field of R by K. We say that $f_{K_0}:Y_{K_0}\to X_{K_0}$ *has a stable model over* R if there exists a model $\mathcal{Y}$ over R such that:

(a) the ramification points y_i of f_{K_0} are K-rational;

(b) the marked curve $(Y_{K_0};y_i)$ extends to a stably marked curve $(\mathcal{Y};y_i)$.

In [10] it is proved that the stable model exists and is unique over a sufficiently large extension R of R_0. The action of G extends to $\mathcal{Y}$ by the uniqueness of the stable model. The quotient $\mathcal{X}=\mathcal{Y}/G$ is a marked semi-stable model of X_{K_0}. The model $f:\mathcal{Y}\to\mathcal{X}$ will be called the *stable model* of f_{K_0}. Its special fiber, denoted by $f:Y\to X$, is the *stable reduction* of f_{K_0}.

Definition 3.1.2 The cover $f_{K_0}:Y_{K_0}\to X_{K_0}$ has *admissible reduction* if $\mathcal{Y}\to\mathcal{X}$ is separable. If, in addition, $\mathcal{X}$ is smooth over R then f has *good reduction*. If f_{K_0} does not have admissible reduction, then it has *bad reduction*.

Assumption 3.1.3 In the rest of this paper we will assume that:

(a) p exactly divides the order of G;

(b) X_{K_0} has genus zero and the number of branch points r is 3;

(c) $(X_{K_0};x_i)$ has good reduction, i.e. the stable model $(\mathcal{Z};x_i)$ of $(X_{K_0};x_i)$ is smooth;

(d) the cover f_{K_0} has bad reduction;

(e) the center of G is trivial.

In general it is hard to compute the reduction of a G-Galois cover. Assumption 3.1.3 allows us to use the results of [15], which we recall below.

Let $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ be as in Definition 3.1.1 and Assumption 3.1.3(c). Denote the special fibers of $\mathcal{Y}, \mathcal{X}, \mathcal{Z}$ by Y, X, Z, etc. There exists a contraction $\mathcal{X} \to \mathcal{Z}$. The restriction of $\mathcal{X} \to \mathcal{Z}$ to the special fiber contracts all irreducible components of X but one. Therefore we may regard Z as a component of X, which we will also denote by Z and call the *original component*. The dual graph of X is a tree which we orient from the original component. Let $\mathbb{B}$ be the set of tails. A tail is called *primitive* if one of the branch points specializes to it; otherwise the tail is called *new*. Let $\mathbb{B}_{\text{prim}}$ (resp. $\mathbb{B}_{\text{new}}$) denote the set of primitive (resp. new) tails. Let $\mathbb{P}$ be the set of $i \in \{1, \dots r\} =: \mathbb{I}$ such that p divides the order of the ramification index of x_i in $f_{\bar{K}}$. Note that we may also consider $\mathbb{B}_{\text{prim}}$ to be a subset of $\mathbb{I}$.

For an irreducible component W of Y, we denote by $D(W)$ its decomposition group and by $I(W)$ its inertia group. The inertia group is a p-group.

Lemma 3.1.4 *(a) Let W be an irreducible component of X. Then $f|_W$ is separable if and only if W is a tail.*

(b) Any branch point x_i whose ramification index m_i is prime-to-p specializes to a component of X over which f is separable.

(c) Any branch point x_i whose ramification index m_i is divisible by p specializes to a component of X over which f is inseparable.

Proof: [15, Lemme 3.1.2], [4, Lemma 2.1.2] □

Note that this lemma implies that if p divides one of the ramification indices of f_{K_0}, then f_{K_0} has bad reduction.

If W is a tail of X corresponding to $b \in \mathbb{B}$, then $f|_W$ is wildly ramified at a unique point τ, the point of intersection of W with the rest of X. The inertia group of a point above τ is of order pn for some n which is prime-to-p. Let h be the conductor above τ. Put $\sigma_b = h/n$ (Section 2.1).

Let U be the union of all components of X over which f is inseparable. Let V be any connected component of $f^{-1}(U)$. Over each irreducible component of V the inertia group is the same Sylow p-subgroup of G, we denote it by $I(V)$, [15]. Let $D(V)$ be the decomposition group of V. Since $I(V)$ is a normal subgroup of $D(V)$, the decomposition group $D(V)$ is contained in the normalizer in G of some Sylow p-subgroup.

Notation 3.1.5 Let $N := N_G(P)$ be the normalizer of a fixed Sylow p-subgroup P. Let N' be the quotient of N by the subgroup C' of the centralizer of P consisting of elements with prime-to-p order.

Proposition 3.1.6 (Vanishing cycle formula)

$$\sum_{b \in \mathbb{B}_{\text{new}}} (\sigma_b - 1) = -2 + |\mathbb{P}| + \sum_{b \in \mathbb{B}_{\text{prim}}} (1 - \sigma_b).$$

Proof: [15, Section 3.4.2]. □

Note that if $f_K : Y_K \to \mathbb{P}^1_K$ is branched at three points, then $\sigma_b \leq 2$, for $b \in \mathbb{B}_{\text{new}}$.

3.2 The monodromy

Let k be an algebraically closed field of characteristic p. Let K_0 be a finite extension of the quotient field of $W(k)$. We will choose once and for all a compatible system of roots of unity $\zeta_n \in \bar{\mathbb{Q}}$ for all integers n. Let $f_{K_0} : Y_{K_0} \to X_{K_0}$ be a G-Galois cover defined over K_0 branched at $x_1 = 0, x_2 = 1, x_3 = \infty$. The notations and assumptions are as in Section 3.1. Let $\underline{C} = (C_1, C_2, C_3)$ be a triple of conjugacy classes of G such that for all i the canonical generator of the inertia of a point above x_i (with respect to the fixed roots of unity) is an element of C_i. We call $\underline{C}$ the *class vector* of f.

Definition 3.2.1 Let K be the minimal extension of K_0 over which the stable model $f : \mathcal{Y} \to \mathcal{X}$ is defined. In [20] it is shown that K is unique and Galois over K_0. The *monodromy group* Γ *of* f_{K_0}*, relative to* K_0, is the Galois group of K/K_0.

The monodromy we consider here is slightly different from the one defined in [15] since we consider a slightly different model. The group Γ is called the inner monodromy group in [4]. Note that Γ acts on the stable reduction Y. The following results of Raynaud use this action of Γ on Y to give restrictions on Γ. For more general results see [20].

Proposition 3.2.2 *The monodromy group* Γ *has order prime-to-p.*

Proof: This follows from [15, Prop. 4.2.4], since the center of G is trivial. $\square$

Proposition 3.2.3 *Let e be the ramification index of p in K_0. Let D be the decomposition group of some component of Y above the original component Z. Let $n' = |D'|/p$, where D' is the quotient of D by $D \cap C'$. Then $(p-1)|en'$.*

Proof: This is essentially proved in [15, Prop. 4.2.11 and Cor. 4.2.12], although it is not stated in the same form. For a somewhat more general version, see [20]. We sketch the argument.

Recall that, by assumption, f_{K_0} has bad reduction. Therefore f is inseparable over the original component. Let η be the generic point of the original component. Let S be the complete local ring of $\mathcal{X}$ at η and let S' be the complete local ring of a point of $\mathcal{Y}$ above η. Suppose that D is the Galois group of the Galois extension S'/S. After taking the quotient by the prime-to-p part of the centralizer $D \cap C'$, we may write $D' \simeq \mathbb{Z}/p \rtimes \mathbb{Z}/n'$. Now we can conclude as in the proof of [15, Cor. 4.2.12] that $(p-1)|en'$. $\square$

Example 3.2.4 (a) Suppose that $G = \mathrm{PSL}_2(p)$ and $m = (p-1)/2$. Then $N = N_G(P) \simeq \mathbb{Z}/p \rtimes \mathbb{Z}/m$ where the quotient of order m acts faithfully on the Sylow p-subgroup. Let $\underline{C} = (2A, 3A, pA)$. Then $\underline{C}$ is a rigid triple which is rational over $\mathbb{Q}(\sqrt{p^*})$, [18, Prop. 7.4.2]. The ramification index of p in $\mathbb{Q}(\sqrt{p^*})$ is $e = 2$. We conclude that the integer n' defined in Proposition 3.2.3 is equal to m.

(b) Suppose that $G = \mathrm{PSL}_2(\ell)$, where ℓ is a prime different from p. Suppose that $p \geq 5$ and p exactly divides the order of G. Then $N_G(P)$ is a dihedral group of order either $\ell - 1$ or $\ell + 1$, depending on which of the two integers is divisible by p. Let $\underline{C} = (2A, 3A, \ell A)$. In this case $n' = 2$ and it follows from Proposition 3.2.3 that the corresponding cover has good reduction. (This form of the proposition follows from the main result of [15], but the proof in this case is much easier than in the general case.)

3.3 Lifting to characteristic zero

In this section we show that every G-Galois cover $f : Y \to \mathbb{P}^1_k$ branched at exactly one point can be constructed by reducing a suitable cover from characteristic zero branched at sufficiently many points. We investigate the question how many branch points are needed. Proposition 3.3.3 implies that every cover of $\mathbb{P}^1_k$ only branched at ∞ with $\sigma = 2$ can be lifted to a cover of $\mathbb{P}^1_K$ branched at three points. In Lemma 4.3.2 we use this to give a criterion for the existence of such a cover. Answering the following question affirmatively would allow to strengthen the result of Lemma 4.3.2. A similar strategy is used in Section 5.4.

Question 3.3.1 Let $f : Y \to \mathbb{P}^1_k$ be a G-Galois cover branched at exactly one point with inertia group I an extension of $\mathbb{Z}/n$ by $\mathbb{Z}/p$ with n prime-to-p. Suppose $\sigma \leq 2$. Does there exist a G-Galois cover $g_K : \tilde{Y}_K \to \mathbb{P}^1_K$ branched at three points in characteristic zero such that f is the restriction of the stable reduction of g_K to some new tail?

It seems reasonable to expect to be able to answer this question affirmatively, for example using the methods of [21]. The reason is that (up to an affine linear transformation) for given $\sigma \leq 2$ there is a *unique* local cover of $\mathbb{P}^1_k$ branched at one point with this σ. In this section we prove some weaker versions of Question 3.3.1. The following result is well known and answers the question affirmatively for $\sigma = 2$.

Proposition 3.3.2 *Suppose that $f : Y \to \mathbb{P}^1_k$ is a G-Galois cover which is tame outside ∞ and whose inertia group above ∞ is cyclic of order p. Let h be the conductor at ∞. Let $R = W(k)[\zeta_p]$. There exists a G-Galois cover of smooth curves $f_R : \mathcal{Y} \to \mathbb{P}^1_R$ such that $f_R \otimes k \simeq f$. The generic fiber $f_K := f_R \otimes_R K$ is branched at $h+1$ points of order p and the prime-to-p ramification is the same as that of f.*

Proof: A lift of f restricted to the complete local ring at ∞ is constructed in [16]. The cover f restricted to $\mathbb{A}^1_k$ is tame and can therefore be lifted to characteristic zero [6, Exposé 10, Corollary 3.9]. There is a unique isomorphism between the two lifts over the overlap. By [13, Theorem 3.4], the data of the two lifts and this isomorphism determines a lift $f_R : \mathcal{Y} \to \mathbb{P}^1_R$ of f to a cover over R. The statement on the branch points follows directly from the construction of the local lift. □

Note that f is *not* the reduction of f_K as in Definition 3.1.1. Let $f^1 : \mathcal{Y}^1 \to \mathcal{X}^1$ be the stable model of f_K. Note that f_K has bad reduction since p divides the order of the ramification indices. The reduction $f^1 : Y^1 \to X^1$ has a unique new tail. The restriction of f^1 to this tail is the cover f with which we started.

The following proposition states that every G-Galois cover $f : Y \to \mathbb{P}^1_k$ branched at exactly one point can be constructed by reducing a suitable cover from characteristic zero, if one allows sufficiently many branch points. This provides some motivation for the approach we use in this paper to construct covers. Since we will not use this proposition in what follows, we only sketch the argument.

Proposition 3.3.3 *Let $f : Y \to \mathbb{P}^1_k$ be a G-Galois cover branched at one point with inertia group I of order pn and $\sigma = h/n$. There exists a G-Galois cover $g_K : \tilde{Y}_K \to \mathbb{P}^1_K$ branched at $h+1$ points of order p over some local field K of characteristic zero and a tail W of the stable reduction $g : \tilde{Y} \to X$ of g_K such that $g|_W$ is isomorphic to f.*

Proof: Let f be as in the statement of the proposition. From Theorem 2.2.2 one deduces that there exists a G-Galois cover of semistable curves $f' : Y'_{R'} \to X'_{R'}$ over $R' := k[[t]]$ such that the generic fiber $f' \otimes k((t))$ is a G-Galois cover of smooth curves, branched at one point with $\sigma = h$ and inertia group of order p. The special fiber $f' \otimes k : Y' \to X'$ can be described as follows. The curve X' has two tails over which f' induces a separable G-Galois cover. Over one of these tails f' restricts to the cover f. (See also the proof of Theorem 4.4.2).

Proposition 3.3.2 implies that $f' \otimes k((t))$ lifts to a G-Galois cover of $\mathbb{P}^1$ in characteristic zero, branched at $h+1$ points of order p. The proposition follows from this. □

The following proposition strengthens the result of Proposition 3.3.3 when $\sigma < 2$.

Proposition 3.3.4 *Let $f : Y \to \mathbb{P}^1_k$ be a G-Galois cover branched at one point with inertia group I of order pn and $\sigma = h/n$. Suppose that $\sigma < 2$. Suppose that the prime-to-p part of the center of I is trivial and $p \neq 2$. There exists a cover $g_K : \tilde{Y}_K \to \mathbb{P}^1_K$ over some local field K of characteristic zero and a tail W of the stable reduction $g : \tilde{Y} \to X$ of g_K such that $g|_W$ is isomorphic to f. In addition, g_K can be chosen to be branched at exactly 4 points, which have inertia groups of order p, p, p, and n respectively.*

Proof: Since $\sigma < 2$ we have $n + 1 \leq h < 2n$ and $\gcd(h, n) = 1$. Let $h_2 = 2n - h$ and note that $h_2 \equiv (-1)h \bmod n$. Write $e = h + h_2 = 2n$ and note that $\gcd(e, p) = 1$. Write $c = \gcd(n, e) = n$.

There exists an I-Galois cover $f_2 : Y \to \mathbb{P}^1_k$ branched only at 0 and ∞ with the following properties: the inertia group above 0 is of order n; the cover is totally ramified above ∞ with conductor h_2.

The numeric condition in [11, Theorem 2.3.4] is satisfied since the prime-to-p part of the center of I is trivial. The conclusion of this theorem is that there exists a G-Galois cover of semistable curves $f' : Y'_{R'} \to X'_{R'}$ over $R' := k[[t]]$ such that the generic fiber $f' \otimes k((t))$ is a G-Galois cover of smooth curves branched at only two points. At the first point, the inertia group has order $pn/c = p$ and conductor $h = e/c = 2$. At the second point, the inertia group is of order n.

Proposition 3.3.2 implies that $f' \otimes k((t))$ lifts to a G-Galois cover of $\mathbb{P}^1$ in characteristic zero, branched at 3 points of order p, plus one point of order n. The proposition follows from this. □

It is more complicated to compute the reduction of covers branched at four points rather than three points, because the position of the branch points becomes important. To study this question, one should look at the reduction of the Hurwitz space parameterizing G-Galois covers branched at four points. Partial results on this question have been obtained in [4] and [3]. But in these results it is assumed that p does not divide the order of the ramification indices and therefore the results do not apply to the covers obtained in Proposition 3.3.4.

4 Modular curves and the reduction of Galois covers

4.1 Reduction of the modular curve $X_0(p)$

In this section, we recall some basic results on the reduction of the modular curve $X_0(p)$ to characteristic p; for more details we refer the interested reader to [5], [9].

Let E_λ be the elliptic curve in characteristic $p \neq 2$ given by the equation $y^2 = x(x-1)(x-\lambda)$. Recall that there is a polynomial $\Phi(\lambda)$ of degree $(p-1)/2$ such that the elliptic curve E_λ is supersingular if and only if $\Phi(\lambda) = 0$. We call such λ a *supersingular λ-value*. If λ is supersingular, then $j := j(\lambda)$ is a supersingular j-value. Recall $j = 1728$ (resp. $j = 0$) is supersingular if and only if $p \equiv 3 \bmod 4$ (resp. $p \equiv 2 \bmod 3$). An easy computation proves the following lemma.

Lemma 4.1.1 *The number of supersingular $j \in k - \{0, 1728\}$ is*

$$\left\lfloor \frac{p}{12} \right\rfloor.$$

We denote by $X_0(p)$ the model of the modular curve over $\mathbb{Z}_{(p)}$, as defined in [5], [9]. It is the coarse moduli scheme corresponding to the moduli problem (E, γ), where E is a (generalized) elliptic curve over some $\mathbb{Z}_{(p)}$-scheme and γ is a $\Gamma_0(p)$-level structure on E. There exists a map $\pi : X_0(p) \to \mathbb{P}^1_{\mathbb{Z}_{(p)}}$ which maps (E, γ) to $j(E)$. On the generic fiber, $\pi \otimes \bar{\mathbb{Q}}$ has degree $p+1$ and is branched at $j = 0$, 1728 and ∞ of order 3, 2, and p respectively. The cover $\pi \otimes \bar{\mathbb{Q}}$ is not Galois; the Galois group of its Galois closure is $\mathrm{PSL}_2(p)$. For convenience, we will work over $\mathbb{Z}_p$ rather than $\mathbb{Z}_{(p)}$.

Theorem 4.1.2 *(a) The curve $X_0(p)$ is semistable.*

(b) *The special fiber* $X_0(p) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ *consists of two irreducible components which are isomorphic to* $X_0(1) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$.

(c) *The restriction of* π *to one of the irreducible components is an isomorphism. The restriction of* π *to the other irreducible component is purely inseparable of degree* p.

(d) *The two components intersect above the supersingular* j*-values.*

4.2 Reduction of some covers with Galois group $\mathrm{PSL}_2(p)$

In this section we use the reduction of the modular curve $X_0(p)$ to compute the reduction of some covers of $\mathbb{P}^1$ branched at three points with Galois group $\mathrm{PSL}_2(p)$. Let $m = (p-1)/2$ and $\alpha = \lfloor p/12 \rfloor$. Let k be an algebraically closed field of characteristic p and $R_0 = W(k)(\sqrt{p^*})$. Let K_0 be the quotient field of R_0. Let $G = \mathrm{PSL}_2(p)$, where $p \geq 5$ is a prime. Let $f_{K_0} : Y_{K_0} \to \mathbb{P}^1_{K_0}$ be a G-Galois cover with class vector $\underline{C} = (2A, 3A, pA)$ branched at $0, 1, \infty$, Example 3.2.4. Let $f : \mathcal{Y} \to \mathcal{X}$ be the stable marked model of f_{K_0}. Write $f : Y \to X$ for its special fiber. Let Z be the original component of X. Let X_2 (resp. X_3) be the component of X to which the branch point of order 2 (resp. of order 3) specializes. By the definition of the model, X_2 and X_3 are primitive tails. Note that $f|_{X_i}$ is tamely ramified above the specialization of the branch point of order 2 (resp. 3). It is wildly ramified with inertia group $\mathbb{Z}/p \rtimes \mathbb{Z}/m_i$ at the unique point of intersection of X_i with the rest of X. Here m_i divides $m := (p-1)/2$. Let $\sigma_i = h_i/m_i$ be the invariant describing the wild ramification of $f|_{X_i}$.

Lemma 4.2.1 *This is a more precise version of Lemma 2.1.1:*

(a) $\sigma_2 \geq \lceil m/2 \rceil / m$,

(b) $\sigma_3 \geq \lceil m/3 \rceil / m$.

Proof: This follows from Lemma 2.1.1. Note that if m is even, the decomposition group of an irreducible component above X_2 may be a dihedral group of order $2p$, in which case σ_2 can be $1/2$. If m is odd, N does not contain a dihedral group of order $2p$, and therefore

$$\sigma_2 \geq \frac{\left\lceil \frac{m}{2} + \frac{m+2}{4m} \right\rceil}{m} = \frac{m+1}{2m}.$$

Statement (b) is proved similarly. □

Lemma 4.2.2 *The number of points of the original component* Z *that are singular in* X *is greater than or equal to* $\alpha + 2$.

Proof: We will compare the stable model $X_0(p) \to \mathbb{P}^1_{\mathbb{Z}_p}$ of $X_0(p) \otimes \mathbb{Q}_p \to \mathbb{P}^1_{\mathbb{Q}_p}$ with the stable model $f : \mathcal{Y} \to \mathcal{X}$ of its Galois closure. Let H be the Borel subgroup of G consisting of all upper triangular matrices. Then Y_{K_0}/H is isomorphic to $X_0(p) \otimes K_0$. Let P be the (unique) Sylow p-subgroup of G contained in H. Let $\pi : \mathcal{Y} \to X_0(p)$ be the natural map.

Let Z be the original component of X. By Example 3.2.4, the order of the decomposition group of a component W of $f^{-1}(Z)$ is pm. Therefore, there are $p+1$ such components; call them $W_1, \ldots, W_{p+1}$. There is a unique i such that $P \subset D(W_i)$; it is no restriction to suppose $i = 1$. Then π maps W_1 to one of the two irreducible components of $X_0(p) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ and π maps W_i for $i \neq 1$ to the other irreducible component.

The α supersingular j-values on the original component Z will be singular in X, since the two irreducible components of $X_0(p) \otimes \mathbb{F}_p$ intersect above the supersingular j-values, Theorem 4.1.2. Moreover, by the choice of our model, the branch points of order 2 and 3 will specialize to primitive tails in X. Therefore the points in Z corresponding to $j = 0, 1728$ are singular in X. This proves the lemma. □

Proposition 4.2.3 (Reduction of f) *The curve X has the following components.*

- *The original component Z. If W is a component of Y above Z, then $D(W)$ has order pm and $I(W)$ has order p.*
- *There are α new tails with $\sigma = (m+1)/m$. There is a unique component of Y above each new tail.*
- *Two primitive tails X_2 and X_3 with conductors equal to the minimal possible values as given in Lemma 4.2.1.*

Proof: Lemma 4.2.2 implies

$$|\mathbb{B}_{\mathrm{new}}| \geq \alpha, \quad |\mathbb{P}| = 1, \quad |\mathbb{B}_{\mathrm{prim}}| = 2.$$

Lemma 2.1.1(c) implies that $\sigma_b - 1 \geq 1/m$, for $b \in \mathbb{B}_{\mathrm{new}}$. Therefore Proposition 3.1.6 and Lemma 4.2.1 imply

$$\begin{aligned} \frac{\alpha}{m} \leq \frac{|\mathbb{B}_{\mathrm{new}}|}{m} \leq \sum_{b \in \mathbb{B}_{\mathrm{new}}} (\sigma_b - 1) &= -2 + 1 + \sum_{b \in \mathbb{B}_{\mathrm{prim}}} (1 - \sigma_b) \\ &\leq -1 + (1 - \frac{\lceil \frac{m}{2} \rceil}{m}) + (1 - \frac{\lceil \frac{m}{3} \rceil}{m}) = \frac{\alpha}{m}. \end{aligned}$$

The last equality follows easily by distinguishing the different possibilities for $p \bmod 12$. We conclude that $\sigma_b = (m+1)/m$ for $b \in \mathbb{B}_{\mathrm{new}}$ and $\sigma_i = \lceil m/i \rceil / m$ for $i = 2, 3$. Therefore the decomposition group of a component above Z has order pm.

Suppose $p > 12$ and let D be the decomposition group of a component over one of the new tails. (For $p < 12$ there are no new tails.) Then D is a quasi-p subgroup of $\mathrm{PSL}_2(p)$ which contains an element of order m, therefore $D = \mathrm{PSL}_2(p)$. □

Consider the triple $\underline{C}' = (3A, 3A, pA)$ of $\mathrm{PSL}_2(p)$. Reasoning as in [18, Prop. 7.4.2], one checks that $\underline{C}'$ is rigid. Therefore there exists a G-Galois cover $f'_{K_0} : Y'_{K_0} \to \mathbb{P}^1_K$ with class vector $\underline{C}'$ which is defined over K_0. Let τ be the automorphism of $\mathbb{P}^1$ such that τ flips 0 and 1 and fixes ∞. Since $\underline{C}'$ is rigid, τ lifts to Y'_{K_0}. We have the following diagram

$$\begin{array}{ccc} Y'_{K_0} & \xrightarrow{\mathbb{Z}/2} & Y_{K_0} \\ \downarrow & & \downarrow \\ X'_{K_0} & \xrightarrow{\mathbb{Z}/2} & X_{K_0}. \end{array}$$

Proposition 4.2.4 (Reduction of f') *The curve X' has the following components.*

- *The original component Z'. The decomposition group of a component W' of Y' above Z' has order pm and $I(W')$ has order p.*
- *The number of new tails is 2α if m is even and $2\alpha + 1$ if m is odd. Above each new tail there is a unique component of Y and $\sigma = (m+1)/m$.*
- *Two primitive tails with $\sigma = \lceil m/3 \rceil / m$.*

Proof: The reduction of f'_{K_0} can be deduced from the reduction of f_{K_0}. Let $f : \mathcal{Y} \to \mathcal{X}$ be the stable model of f_{K_0}. Since the action of $\mathbb{Z}/2$ on Y'_{K_0} commutes with the action of G, we can define a model $\tilde{f}' : \tilde{\mathcal{Y}}' \to \tilde{\mathcal{X}}'$ of f'_{K_0} such that

$$\begin{array}{ccc} \tilde{\mathcal{Y}}' & \xrightarrow{\mathbb{Z}/2} & \mathcal{Y} \\ \downarrow & & \downarrow \\ \tilde{\mathcal{X}}' & \xrightarrow{\mathbb{Z}/2} & \mathcal{X}. \end{array}$$

The stable model $\mathcal{Y}' \to \mathcal{X}'$ can now be easily be computed: $\mathcal{Y}'$ is obtained from $\tilde{\mathcal{Y}}'$ by contracting the new tails of genus zero that meet the rest of $\tilde{\mathcal{Y}}'$ in a unique point.

Note that $|D(W')| = mp$. Consider the fixed points of $\tau : X'_{K_0} \to X'_{K_0}$; these are the points with $x = 1/2$ and $x = \infty$. First we consider the point $b' \in X'_{K_0}$ with $x = 1/2$; this is not a branch point of f'_{K_0}. Its image b in X_{K_0} is a branch point of f_{K_0} of order 2, so b specializes to the primitive tail X_2, which has $\sigma_2 = \lceil m/2 \rceil / m$. If m is even, $\sigma_2 = 1/2$ and any irreducible component of $\tilde{Y}'$ above X_2 has genus zero and decomposition group a dihedral group of order $2p$. Since b' is not a branch point of f', we conclude that b' specializes to the original component Z' and not to a tail.

If m is odd, $\gcd(\lceil m/2 \rceil, m) = 1$. This implies that b' specializes to a tail X'_2 of X' with $\sigma'_2 = 2\lceil m/2 \rceil / m = (m+1)/m$ by Lemma 2.1.2. Since b' is not a branch point of f', we conclude that X'_2 is a new tail.

The second fixed point of τ is the branch point x'_3, whose image x_3 in X is the branch point of order p. So x_3 specializes to the smooth locus of Z in X. We conclude that the same holds for x'_3.

Each new tail of X gives 2 new tails in X', with $\sigma = (m+1)/m$. The primitive tail X_3 of X gives two primitive tails in X' with $\sigma = \lceil m/3 \rceil / m$. We conclude that the number of new tails is 2α if m is even and $2\alpha + 1$ if m is odd. □

As a third example, we consider the triple $\underline{C}'' = (pA, pA, pA)$ of $G = \mathrm{PSL}_2(p)$. One checks that this is also a rigid triple which can be defined over K_0 as in the proof of [19, Lemma 3.27]. Let $f''_{K_0} : Y''_{K_0} \to \mathbb{P}^1_{K_0}$ be the G-Galois cover with class vector $\underline{C}''$ branched at $0, 1, \infty$. Consider the action of S_3 on $\mathbb{P}^1$ which permutes $0, 1, \infty$. Since the triple $\underline{C}''$ is rigid, the action of S_3 lifts to Y''_{K_0} and we get a diagram

$$\begin{array}{ccc} Y''_{K_0} & \xrightarrow{S_3} & Y_{K_0} \\ \downarrow & & \downarrow \\ X''_{K_0} & \xrightarrow{S_3} & X_{K_0}. \end{array}$$

Proposition 4.2.5 (Reduction of f'') *The curve X'' has the following components.*

- *The original component Z''. Any component W'' of Y'' above Z'' has decomposition group of order pm and inertia group of order p.*
- *Above every new tail of X'' there is a unique component of Y''. It has invariant $\sigma = (m+1)/m$.*
- *The number of new tails is*

$$\begin{cases} 6\alpha & \text{if } p \equiv 1 \bmod 12, \\ 6\alpha + 2 & \text{if } p \equiv 5 \bmod 12, \\ 6\alpha + 3 & \text{if } p \equiv 7 \bmod 12, \\ 6\alpha + 6 & \text{if } p \equiv 11 \bmod 12. \end{cases}$$

- *There are no primitive tails.*

Proof: This is proven like Proposition 4.2.4. □

Corollary 4.2.6 *Let $G = \mathrm{PSL}_2(p)$. For $p \geq 5$ there exists a G-Galois cover of $\mathbb{P}^1_k$ branched at exactly one point with $\sigma = (m+1)/m$.*

Proof: This follows from Proposition 4.2.5 as the reduction of f'' has a new tail with $\sigma = (m+1)/m$ for every $p \geq 5$. □

4.3 A non-existence result

Let k be an algebraically closed field of characteristic p. In the previous section we showed that there exists a cover of $\mathbb{P}^1_k$ branched at exactly one point in characteristic p with Galois group $\mathrm{PSL}_2(p)$ whose inertia group I at infinity is as large as possible, namely of order pm, and whose invariant σ is the minimal possible value for this inertia group, Section 2.1. From this we will deduce in Section 4.4 that every possible subgroup of I occurs as the inertia group of an G-Galois cover of $\mathbb{P}^1_K$ branched at one point. Moreover, all but finitely many of the possible values of σ occur.

In this section we prove a non-existence result: there does not exist a $\mathrm{PSL}_2(p)$-Galois cover $Y \to \mathbb{P}^1_k$ with Galois group branched only at ∞ with $\sigma = 2$. The proof relies on the lifting result Proposition 3.3.2.

Theorem 4.3.1 *Let $G = \mathrm{PSL}_2(p)$. There is no G-Galois cover $f : Y \to \mathbb{P}^1_k$ branched at exactly one point with $\sigma = 2$.*

Proof: Suppose there exists a G-Galois cover $f : Y \to \mathbb{P}^1_k$ branched at exactly one point with $\sigma = 2$. By Proposition 3.3.2, it extends to a G-Galois cover $f : \mathcal{Y} \to \mathcal{X}$ of smooth R-curves, where $R = W(k)[\zeta_p]$. Let $f_{\bar{K}} : Y_{\bar{K}} \to \mathbb{P}^1_{\bar{K}}$ be the geometric generic fiber. This cover has three branch points of order p. One checks that there is no G-Galois cover with class vector (pA, pA, pB). Therefore the class vector of f_K is either (pA, pA, pA) or (pB, pB, pB). Since these two are permuted by an outer automorphism of G they have the same type of reduction. We conclude from Proposition 4.2.5 that the stable reduction of f_K does not have a tail with $\sigma = 2$. This gives a contradiction. □

The following lemma generalizes Theorem 4.3.1. The lemma illustrates the arithmetic nature of the existence of covers of the affine line with given inertia and conductor at ∞. In practice, it will be hard to find groups satisfying the conditions of the lemma.

Lemma 4.3.2 *Let G be a quasi-p group such that p exactly divides the order of G. Let C_p be the set of conjugacy classes of elements of order p in G and let $a = |C_p|$. Define*

$$b := \max_{(C_1, C_2, C_3)} \#\{\text{covers of } \mathbb{P}^1_{\bar{\mathbb{Q}}} \text{ with class vector } (C_1, C_2, C_3)\}.$$

If $ab < p - 1$, then there is no cover $Y_k \to \mathbb{P}^1_k$ branched at exactly one point with $\sigma = 2$.

Proof: Suppose that $f : Y \to \mathbb{P}^1_k$ is a G-Galois cover branched only at ∞ with $\sigma = 2$. By Proposition 3.3.2, f lifts to a cover $f_K : Y_K \to \mathbb{P}^1_K$ with class vector $\underline{C} = (C_1, C_2, C_3)$ for some $C_i \in C_p$. Let L be the quotient field of $W(k)$. Let K_0/L be a minimal field of definition. Let $L(\underline{C})$ be the smallest subfield of K_0 containing L over which $\underline{C}$ is rational, [18, Chapter 7.1]. Then $[K_0 : L(\underline{C})] \leq b$ and $[L(\underline{C}) : L] \leq a$. Proposition 3.2.3 implies that $[K_0 : L] \geq (p-1)$. We conclude that $ab \geq (p - 1)$. □

Example 4.3.3 Let $G = \mathrm{SL}_2(16)$ and $p = 17$. The group G has 8 conjugacy classes of elements of order 17. One checks, for instance with GAP, that for every triple of conjugacy classes (C_1, C_2, C_3) of elements of order p, the number of covers with this class vector is either 0 or 1. Therefore Lemma 4.3.2 implies that there is no G-Galois cover of $\mathbb{P}^1_k$ branched at one point in characteristic 17 with $\sigma = 2$. In fact, the stable reduction of a G-Galois cover of $\mathbb{P}^1_K$ branched at three points of order $p = 17$ has two new tails with $\sigma = 3/2$. The primes 3 and 5 also exactly divide the order of G, but here Lemma 4.3.2 does not apply as $ab = p - 1$ for these primes.

4.4 Covers with Galois group $\mathrm{PSL}_2(p)$

Proposition 4.4.1 *Suppose I is a subgroup of G which is a semidirect product of $\mathbb{Z}/m$ by $\mathbb{Z}/p$ for some $m < p$. Suppose there exists a G-Galois cover of curves $f_1 : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia I and conductor h. For each $d \in \mathbb{N}$ such that $1 \leq d \leq m$, let $n_d = m/\gcd(m,d)$ and let $h_d = dh/\gcd(m,d)$. Write I_d for the subgroup of I of order pn_d. Then for each such d, there exists a G-Galois cover of curves $f_d : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia I_d and conductor h_d.*

Proof: The proof will proceed by induction on d. For $d = 1$ the statement is true by hypothesis since $n_1 = m$ and $h_1 = h$. We assume the statement is true for $d-1$; in other words, we assume there exists a G-Galois cover of curves $f_{d-1} : Y_{d-1} \to \mathbb{P}^1_k$ branched at exactly one point with inertia $I_{d-1} = \mathbb{Z}/p \rtimes \mathbb{Z}/n_{d-1}$ (where $n_{d-1} = m/\gcd(m, d-1)$) and conductor $h_{d-1} = (d-1)h/\gcd(m, d-1)$.

The covers f_1 and f_{d-1} satisfy the hypotheses of Theorem 2.2.2. In particular, $I_{d-1} \subset I_1$ with index $r = \gcd(m, d-1)$. Also $h_{d-1} = \gamma h_1$ for some $\gcd(\gamma, m) = 1$ since $h_{d-1} = (d-1)h/\gcd(m, d-1)$. Since $r\gamma + 1 = d$, we see that $e = dh$ and $c = \gcd(m, d)$. Note that $\gcd(e, p) = 1$ since $d \leq m < p$.

By Theorem 2.2.2, there exists a G-Galois cover of smooth connected curves $f_d : Y_d \to \mathbb{P}^1_k$ branched at exactly one point with inertia $I_d = \mathbb{Z}/p \rtimes \mathbb{Z}/(m/c) = \mathbb{Z}/p \rtimes \mathbb{Z}/n_d$ and with conductor $e/c = h_d$. This proves the statement for the value d. □

Note that one consequence of Proposition 4.4.1 and Section 2.2 is the following. Let G be a quasi-p group such that p strictly divides the order of G. Suppose that the Inertia Conjecture is true for G; (all subgroups of the form $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n$ occur as the inertia group of a G- Galois cover branched only at ∞). Then all but finitely many of the values for σ occur as the upper jumps of such covers. If the prime-to-p part of the center of $N_G(P)$ is trivial, the Inertia Conjecture for G is equivalent to the statement that all but finitely many σ occur for G.

Theorem 4.4.2 *Let $G = \mathrm{PSL}_2(p)$. Let $m = (p-1)/2$. Let $n|m$. Let a be such that $0 < a \leq n$ and $\gcd(a,n) = 1$. Let $h \in \mathbb{N}$ be such that $\gcd(h,p) = 1$ and $h \equiv a \bmod n$. Assume that $h \geq a(m+1)$. Then there exists a G-Galois cover of curves $f : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n$ and conductor h.*

Proof: Let $h_* = a(m+1)$. Note that any integer $h \in \mathbb{N}$ such that $h \equiv a \bmod n$ and $h \geq a(m+1)$ is of the form $h_* + in$ for some $i \in \mathbb{N}$. Thus by Theorem 2.2.1, it is sufficient to show that there exists a G-Galois cover of curves $f : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n$ and conductor h_*.

By Corollary 4.2.6, there exists a G-Galois cover of curves $f_1 : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia $I = \mathbb{Z}/p \rtimes \mathbb{Z}/m$ and conductor $h = m+1$. Let r be such that $m = nr$ and note that $1 \leq ar \leq m$. By Proposition 4.4.1, for $d = ar$ there exists a G-Galois cover of curves $f : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n_d$ and conductor h_d. Since $\gcd(m, ar) = r\gcd(n,a) = r$, we see that $n_d = m/r = n$ and $h_d = ar(m+1)/r = a(m+1)$. □

Corollary 4.4.3 *The Inertia Conjecture is true when $G = \mathrm{PSL}_2(p)$. In other words, every subgroup $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n$ of G can be realized as the inertia group of a G-Galois cover of $\mathbb{P}^1_k$ which is branched at exactly one point.*

Proof: This is immediate from Theorem 4.4.2. □

4.5 Some constructions for $\mathrm{PSL}_2(\ell)$

In this section, we consider covers of the affine line over an algebraically closed field k of characteristic p with Galois group $G = \mathrm{PSL}_2(\ell)$, where ℓ is a prime different from p. Suppose that p exactly divides the order of G. The normalizer $N := N_G(P)$ of a p-Sylow subgroup P of G is a dihedral group of order $\ell - 1$ or $\ell + 1$, depending on which of the two is divisible by p. Let $n = |N|/2p$. Note that the possible inertia groups of G-Galois covers are cyclic groups of order pd where d divides n or the dihedral group of order $2p$; these are the only subgroups of N that are extensions of a cyclic group of order prime-to-p by a p-group. Let $R_0 = W(k)[\zeta_p + \zeta_p^{-1}]$ and K_0 be the quotient field of K_0.

Lemma 4.5.1 *Let $\underline{C} = (pA, pA, \ell A)$. There exists a cover $f_{K_0} : Y_{K_0} \to \mathbb{P}^1_{K_0}$ with class vector $\underline{C}$ defined over K_0.*

Proof: The triple $\underline{C}$ is not rigid in general. Let $\underline{C}'$ be a lift of $\underline{C}$ to a triple of conjugacy classes in $\mathrm{SL}_2(\ell)$. One easily checks as in [19, Lemma 3.27] that $\underline{C}'$ is a rigid triple in $\mathrm{SL}_2(\ell)$. The conjugacy class ℓA is not rational over $\mathbb{Q}_p$, but becomes rational after an extension that is unramified at p. The conjugacy class pA is also not rational over $\mathbb{Q}_p$. The group G has $(p-1)/2$ conjugacy classes of order p which are rational over $\mathbb{Q}_p(\zeta_p + \zeta_p^{-1})$. Using [19, Theorem 3.25], we conclude that there is some cover $f : Y_{K_0} \to \mathbb{P}^1_{K_0}$ with class vector $\underline{C}$ which is defined over K_0. □

Proposition 4.5.2 *Let $G = \mathrm{PSL}_2(\ell)$. There exists a G-Galois cover $f : Y \to \mathbb{P}^1_k$ which is branched only at ∞ with inertia group $I \simeq D_p$ and $\sigma = 3/2$.*

Proof: Let $f_{K_0} : Y_{K_0} \to \mathbb{P}^1_{K_0}$ be as described in Lemma 4.5.1. The cover f_{K_0} has bad reduction to characteristic p since p divides two of the ramification indices. Denote its stable reduction by $f : Y \to X$. Using Proposition 3.1.6 and Lemma 2.1.1(c), we find

$$\frac{|\mathbb{B}_{\mathrm{new}}|}{2} \leq -2 + 2 + (1 - \frac{1}{2}) = \frac{1}{2}.$$

Therefore $|\mathbb{B}_{\mathrm{new}}| \leq 1$.

Let U be the union of the components of X over which f is inseparable and let V be a connected component of $f^{-1}(U)$. Let $D(V)$ be the decomposition group of V and write $|D(V)| = pn$. Proposition 3.2.3 implies that D contains a dihedral group of order $2p$. This implies that there are at least two tails whose invariant $\sigma = h/2$ is not an integer. We conclude that there is a new tail X_n with $\sigma = 3/2$. The decomposition group of an irreducible component above X_n is a subgroup of G which is a quasi-p group containing a dihedral group of order $2p$. The only such group is G. □

As in the previous section, we ask whether there is a cover $Y \to \mathbb{P}^1_k$ branched at one point in characteristic p with Galois group $\mathrm{PSL}_2(\ell)$ and $\sigma = 2$. The triple $(p*, p*, p*)$, with $p*$ any conjugacy class of elements of order p, is in general not rigid. For small p, one can sometimes show that there is no G-Galois cover in characteristic zero with Nielsen class $(p*, p*, p*)$. For example, let $\ell = 5$ and $p = 3$. One easily checks that $\mathrm{PSL}_2(5) = A_5$ is not generated by two 3-cycles. Therefore there is no A_5-Galois cover of $\mathbb{P}^1$ with class vector $(3A, 3A, 3A)$. However, this is an exception. The reason this happens is that two 3-cycles generate A_4, which is a quasi-3 subgroup of G. For $p \geq 5$, however, the only quasi-p subgroups of G are $\mathbb{Z}/p$, G, and the group of order $p\ell$ when $p | (\ell - 1)$.

The following lemma gives a partial converse to Lemma 4.3.2.

Lemma 4.5.3 *Suppose that $p \geq 5$ and that ℓ is a prime different from p. Let $G = \mathrm{PSL}_2(\ell)$ and suppose that p exactly divides the order of G and $\ell \equiv \pm 1 \bmod 8$. There exists a G-Galois cover $Y \to \mathbb{P}^1_k$ branched only at ∞ with $\sigma = 2$.*

Proof: The condition $\ell \equiv \pm 1 \bmod 8$ assures that G contains an element of order 4. Let $\underline{C} = (\ell A, pA, 4A)$. One easily checks that there exist G-Galois covers over $\bar{\mathbb{Q}}$ with class vector $\underline{C}$. The triple $\underline{C}$ is *not* rigid; there are two covers with this class vector. Let $f : Y \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be one of these covers and let R_0 be a finite extension of $W(k)$ such that f can be defined over its quotient field K_0. Since p divides one of the ramification indices of f, the cover has bad reduction to characteristic p.

Proposition 3.1.6 and Lemma 2.1.1(c) imply:

$$\frac{|\mathbb{B}_{\text{new}}|}{2} \leq -2 + 1 + 2(1 - \frac{1}{2}) = 0.$$

We conclude that there are no new tails and two primitive tails X_4 and X_ℓ which both have $\sigma = 1/2$. A look at the list of subgroups of $\mathrm{PSL}_2(\ell)$ [8, Theorem 8.27] tells us that the decomposition group of a component above X_4 is equal to G. (If $p = 3$ the decomposition group will be isomorphic to S_4.) The lemma now follows from Lemma 2.1.2 applied to the restriction of f to X_4. $\square$

Theorem 4.5.4 *Let $G = \mathrm{PSL}_2(\ell)$ with ℓ prime. Suppose that p strictly divides $\ell \pm 1$ and $p \geq 5$. There exists a G-Galois cover of curves $f : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia I and conductor h in the following cases:*

(a) $I = D_p$ for any h with $\gcd(h, 2p) = 1$ and $h \geq 3$;

(b) $I = \mathbb{Z}/p$ for any h with $\gcd(h, p) = 1$ and $h \geq 3$ if $\ell \equiv \pm 3 \bmod 8$ and $h \geq 2$ if $\ell \equiv \pm 1 \bmod 8$.

Proof: By Proposition 4.5.2, there exists a G-Galois cover $f : Y \to \mathbb{P}^1_k$ branched at one point with inertia D_p and conductor 3. Statement (a) follows immediately by applying Theorem 2.2.1 to f.

Applying Abhyankar's Lemma 2.1.2 to f implies that there exists a G-Galois cover of curves $f' : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia $\mathbb{Z}/p$ and conductor 3. If $\ell \equiv \pm 1 \bmod 8$, then Lemma 4.5.3 shows that such a cover f' exists with conductor 2. Applying Theorem 2.2.1 to f' realizes all the larger conductors. This proves Statement (b). $\square$

It is not immediately clear how to realize the cyclic subgroups $\mathbb{Z}/pn$ of $\mathrm{PSL}_2(\ell)$ as inertia groups of such covers if $n > 1$.

5 Covers with Galois group A_p

5.1 The inertia groups of Abhyankar's covers

In this section, we construct Galois covers of $\mathbb{P}^1_k$ branched at exactly one point with Galois group A_p. We suppose $p \geq 5$ to avoid trivial examples. We compare these results with what we have obtained in the previous section for Galois covers of $\mathbb{P}^1_k$ with Galois group $\mathrm{PSL}_2(p)$. Note that the order of the normalizer of the Sylow p-subgroup in both groups has order pm, where $m = (p-1)/2$. So one might expect that the same σ's occur for both groups. This turns out to be wrong, Section 5.4.

To construct A_p-Galois covers of the affine line we use a different method than for $\mathrm{PSL}_2(p)$-Galois covers. The reason is that we do not know of a suitable family of Hurwitz spaces $\pi : H \to \mathbb{P}^1_\lambda$ in characteristic zero for which the Galois group of the Galois closure is A_p. For instance, the Galois closure of the cover of the Hurwitz spaces described in [4, p. 41] to the λ-line will often be A_n or S_n, but only rarely will p exactly divide $n!$. For the few cases where p exactly divides $n!$, the cover has good reduction to characteristic p, so these covers are not useful for our purposes.

Instead, we consider a family of polynomials with Galois group A_p studied by Abhyankar in [1] and compute the inertia data of the corresponding covers. The results are probably known, but do not seem to have been published. One might do similar computations for the other families in [1].

Proposition 5.1.1 *Let t be an integer with $1 < t \leq (p-1)/2$. Let $F_t = Y^p - Y^t + X$, let L be the Galois closure of $k(X)[Y]/(F)$ over $k(X)$, and let G the Galois group of this extension. Let $f_t : Y_t \to \mathbb{P}^1_k$ be the corresponding G-Galois cover.*

(a) *The cover f_t is ramified of order t above 0. Above ∞ the inertia group I has order $p(p-1)/\gcd(p-1, p-t)$ and $\sigma = (p-t)/(p-1)$.*

(b) *The Galois group of f_t is S_p if t is even and A_p if t is odd.*

Proof: One easily checks the statement on the ramification outside ∞. Let us compute what happens above ∞.

First we rewrite the equation $F = F_t$ by replacing X by $1/X$ and Y by $1/Y$:

$$F = Y^p - Y^{p-t}X + X.$$

Let y be a root of the polynomial F and write $F = (Y-y)G(Y)$. Note that F is irreducible by the Eisenstein Criterion. Then

$$G(Y) = Y^{p-1} + yY^{p-2} + \cdots + y^{t-1}Y^{p-t} + cY^{p-t-1} + \cdots + cy^{p-1},$$

where $c = -y^t/(y^{p-1}-1)$. To compute the conductor of the cover above ∞, we want to compute the valuation of $(y'-y)/y$, where y' is a Galois conjugate of y, or in other words a root of G. (Here we use that F is irreducible.) To do this, we make the substitution $\tilde{G}(Z) := G(y(Z+1))$. One checks that

$$\tilde{G}(Z) = y^{p-1}[(Z+1)^{p-1} + \cdots + (Z+1)^{p-t} + d(Z+1)^{p-1-t} + \cdots d],$$

where $d = -1/(y^{p-t}-1)$. If we expand this we find

$$\frac{\tilde{G}(Z)}{y^{p-1}} = d(-Z^{p-1} + y^{p-t}\sum_{i=0}^{p-2} a_i Z^i),$$

with $a_i \in \mathbb{F}_p^*$. We conclude that the coefficient of Z^i in $\tilde{G}/y^{p-1}$ for $i \neq p-1$ has valuation $p-t$ and therefore

$$\sigma = \nu(z) = \nu((y'-y)/y) = \frac{p-t}{p-1}.$$

From this the statement on the inertia groups follows.

To prove (b), we follow [2]. Let G be the Galois group of f_t. Then p divides the ramification index above ∞, so G is a primitive permutation group on p letters. Moreover, above $X=0$, g_t is ramified of order t at one point, so G contains a t-cycle with $t \leq p/2$. This implies that G is $(p-t+1)$-transitive and therefore that G is isomorphic to either S_p or A_p. If t is even, we conclude G is S_p. Suppose that t is odd. Then $\sigma = (p-t)/(p-1)$ and $p-t$ is even. So we conclude that the order of the inertia group I of f_t above ∞ divides $p(p-1)/2$. Therefore G is generated by odd permutations and we conclude that $G \simeq A_p$. □

Corollary 5.1.2 *Let $1 < t \leq m = (p-1)/2$. There exists an A_p-Galois cover $Y_t \to \mathbb{P}^1_k$ branched only at ∞ with inertia group of order $p(p-1)/\gcd(p-1, t(p-t))$ and $\sigma = t(p-t)/(p-1)$.*

Proof: If t is even, we consider the A_p-Galois subcover of f_t. This cover is ramified of order $t/2$ above zero and has inertia of order pn where $n = m/\gcd(p-1, p-t)$. Its conductor is the same as the conductor of the S_p-Galois cover and $\sigma = (p-t)/m$. This A_p-Galois cover is disjoint from the $t/2$-cyclic cover branched at 0 and ∞. Applying Abhyankar's Lemma 2.1.2, we conclude that there exists an A_p-Galois cover of $\mathbb{P}^1_k$ branched at exactly one point with inertia of order $p(p-1)/\gcd(p-1, t(p-t))$ and $\sigma = t(p-t)/(p-1)$.

For t odd, the cover f_t has Galois group A_p. It is disjoint from the t-cyclic cover branched at 0 and ∞. Thus applying Abhyankar's Lemma 2.1.2 directly to f_t yields the desired cover. □

Remark 5.1.3 In Lemma 4.3.2 we gave a condition under which there does not exist a G-Galois cover $Y \to \mathbb{P}^1_k$ branched at one point with $\sigma = 2$. If $G = A_p$ and $p \geq 7$ there are many covers of $\mathbb{P}^1$ defined over $\bar{\mathbb{Q}}$ branched at three points of order p. For example, if $p = 7$ there are 9 covers with class vector $(7A, 7A, 7A)$ and 5 covers with class vector $(7A, 7A, 7B)$. So the number ab mentioned in Lemma 4.3.2 is equal to 18. If $p = 11$, we have $ab = 2 \cdot 14719$. This suggests that there will be (many?) A_p-Galois covers $Y \to \mathbb{P}^1_k$ in characteristic $p \geq 7$ branched at one point with $\sigma = 2$. Namely, if there is no A_{11}-Galois cover of $\mathbb{P}^1_k$ branched at exactly one point with $\sigma = 2$, all 29,438 A_{11}-Galois covers of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ with class vector $(11A, 11A, 11A)$ can be defined over an extension K of the quotient field of $W(k)$ of degree strictly less than 5. This seems unlikely. However, we have shown $\sigma = 2$ to occur only for $p = 7$. The fact that A_p has few rigid triples on the one hand suggests that all or most σ will occur. On the other hand, it makes it hard to show the existence of covers with given small σ with our methods.

5.2 Alternative approach: reduction from characteristic zero

In this section, we give an alternative proof of Corollary 5.1.2, using reduction of covers from characteristic zero. Using the reduction of certain A_p-covers, we will show in Section 5.4 that the set of σ's that occur for A_p and $\mathrm{PSL}_2(p)$ covers are different for every $p \geq 7$.

Let $\underline{C}_t = (2A, C^{(t)}, pA)$ by the triple of conjugacy classes of S_p where $2A$ and pA represent the conjugacy classes of 2- and p-cycles, and $C^{(t)}$ is the conjugacy class of the product of a t-cycle with a disjoint $(p-t)$-cycle. We assume that $1 \leq t \leq (p-1)/2$. The triple $\underline{C}_t$ is rigid and rational. Let $f_{t,\mathbb{Q}} : Y_{t,\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be the corresponding cover, branched at $0, \beta = t^t(t-p)^{p-t}p^{-p}, \infty$. Then $Z_t := Y_{t,\mathbb{Q}}/(S_{p-1})$ is a curve of genus zero, given by the equation:

$$G_t := Y^t(Y-1)^{p-t} - X = 0,$$

[18, Section 8.3.1].

Proposition 5.2.1 *Let $f_{t,\mathbb{Q}} : Y_{t,\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be the S_p-Galois cover described above. Let $f_t : Y_t \to X$ be the stable reduction of f. Then X has two primitive tails and no new tails. Let X_1 be the primitive tail to which the branch point of order $t(p-t)$ specializes and X_2 the primitive tail to which the branch point of order two specializes.*

(a) The decomposition group of an irreducible component above X_1 has order $p(p-1)$ if $t = 1$ and $p!$ otherwise. The inertia group above ∞ has order $p(p-1)$ and $\sigma_1 = 1/(p-1)$.

(b) Above X_2 there is a unique irreducible component with decomposition group S_p. The inertia group above ∞ has order $p(p-1)$ and $\sigma_2 = (p-2)/(p-1)$.

Proof: Note that the equation defined by G_t still defines a separable field extension in characteristic p which is ramified of order $t(p-t)$ above $X = 0$, so this describes the cover $f_t|X_1$. To find an equation for the cover above X_2, we use the following substitutions of variables.

Substitute $Y = \tilde{Y}/p$ and $X = \tilde{X}/(p^p)$. The equation becomes:

$$\tilde{Y}^t(\tilde{Y} - p)^{p-t} - \tilde{X} = 0.$$

The ramification point of order 2 has coordinates $\tilde{Y} = t$ and $\tilde{X} = t^t(t-p)^{p-t} \equiv t^p \bmod p$.

Substitute $\hat{Y} = t + p^{1/(p-2)}\tilde{Y}$ and $\hat{T} = \beta + p^{p/(p-2)}$. After dividing by $p^{p/(p-2)}$ and reducing mod p, the equation becomes:

$$\hat{Y}^p - \hat{Y}^2 - \hat{X} = 0.$$

From Proposition 5.1.1 we conclude that this equation defines a (separable) S_p-Galois cover which is ramified of order two above 0 and has $\sigma = (p-2)/(p-1)$ over ∞.

Let us return to the restriction of f_t over X_1. Let σ_1 describe the ramification above ∞. Proposition 3.1.6 implies that

$$\sigma_1 \leq -2 + 1 + 1 + 1 - \frac{p-2}{p-1} = \frac{1}{p-1}.$$

Since the decomposition group above the original component has order $p(p-1)$, we conclude that $\sigma_1 = 1/(p-1)$. $\square$

Corollary 5.2.2 *Let $g_{t,\mathbb{Q}} : Y_{t,\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be the A_p-Galois subcover of $f_{t,\mathbb{Q}}$ defined in Proposition 5.2.1. Let $n = t(p-t)/2$ and let nA be the conjugacy class of A_p containing the square of an element in $C^{(t)}$. The class vector of g_t is (nA, pA, pB). The stable reduction of g_t has one primitive tail X_1 with $\sigma = 1/m$ and one new tail X_2 with $\sigma = (p-2)/m$.*

Note that this gives a second proof of Corollary 5.1.2, by applying Abhyankar's Lemma to the covers over the primitive and the new tail of g_t.

5.3 Covers with Galois group A_p

In this section, we use formal patching to prove existence results for A_p-Galois covers with specified inertia group and ramification.

Proposition 5.3.1 *Let $G = A_p$. Let $h \in \mathbb{N}$ be such that $h \geq 3$ and $\gcd(h,p) = 1$. Then there exists a G-Galois cover of curves $f : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia $I = \mathbb{Z}/p$ and conductor h.*

Proof: By Theorem 2.2.1, it is sufficient to show that there exists an A_p-Galois cover of curves $f : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia $I = \mathbb{Z}/p$ and conductor 3. Let $m = (p-1)/2$. Choose an injection $\mathrm{PSL}_2(p) \to A_p$ so that we may regard $\mathrm{PSL}_2(p)$ as a subgroup of A_p.

By Corollary 4.2.6, there exists a $\mathrm{PSL}_2(p)$-Galois cover $f_1 : Y_1 \to \mathbb{P}^1_k$ branched at exactly one point with $\sigma_1 = (m+1)/m$. By Corollary 5.1.2 with $t = 2$, there exists an A_p-Galois cover $f_2 : Y_2 \to \mathbb{P}^1_k$ branched at exactly one point with $\sigma_2 = (p-2)/m$.

The covers f_1 and f_2 satisfy the numeric condition in [11, Theorem 2.3.4]. The conclusion of this theorem is that there exists an A_p-Galois cover $f : Y \to \mathbb{P}^1_k$ which is branched at exactly one point with $\sigma = \sigma_1 + \sigma_2 = (2m-1)/m + (m+1)/m = 3$. Thus f has inertia $\mathbb{Z}/p$ and conductor 3 above its branch point. $\square$

Theorem 5.3.2 *Let $G = A_p$. Let $m = (p-1)/2$ and $n|m$. Let a be such that $0 < a \leq n$ and $\gcd(a,n) = 1$. Let $h \in \mathbb{N}$ be such that $\gcd(h,p) = 1$ and $h \equiv -a \bmod n$. Assume that $h \geq a(p-2)$. Then there exists a G-Galois cover of curves $f : Y \to \mathbb{P}^1_k$ branched at exactly one point with inertia $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n$ and conductor h.*

Proof: This follows from Theorem 2.2.1, Corollary 5.1.2 (with $t = 2$), and Proposition 4.4.1 exactly like the proof of Theorem 4.4.2. $\square$

Note that there are some extra values of σ from Corollary 5.1.2 that are not included in Theorem 5.3.2. For example, choosing $t = (p-1)/2$, we find there exists an A_p-Galois cover of $\mathbb{P}^1_k$ branched only at ∞ with $\sigma = (m+1)/2$.

Corollary 5.3.3 *The Inertia Conjecture is true for $G = A_p$. In other words, every subgroup $I = \mathbb{Z}/p \rtimes \mathbb{Z}/n$ of G can be realized as the inertia group of a G-Galois cover of $\mathbb{P}^1_k$ which is branched at exactly one point.*

Proof: This is immediate from Theorem 5.3.2. $\square$

5.4 A comparison result

Let $m = (p-1)/2$. Let $g_{1,\mathbb{Q}} : Y_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be the A_p-Galois cover with class vector (mA, pA, pB) defined over $\mathbb{Q}$ as in Corollary 5.2.2. Recall that the stable reduction of g_1 has one primitive tail and one new tail with $\sigma = (p-2)/m$. In this section, we will use some techniques from [20] to show that there is no $\mathrm{PSL}_2(p)$-Galois cover of $\mathbb{P}^1_k$ branched at exactly one point with $\sigma = (p-2)/m$. The idea is as follows. Suppose such a $\mathrm{PSL}_2(p)$-Galois cover exists. Then we can construct a $\mathrm{PSL}_2(p)$-Galois cover out of the stable reduction of g_1 by replacing the new tail by the $\mathrm{PSL}_2(p)$-Galois cover with $\sigma = (p-2)/m$. We show that this $\mathrm{PSL}_2(p)$-Galois cover lifts to characteristic zero and has ramification of order p, p, and m. Then we reduce it back to characteristic p and derive a contradiction. Let $R_0 = W(k)(\sqrt{p^*})$ and K_0 its quotient field.

Lemma 5.4.1 *Let $G = \mathrm{PSL}_2(p)$ and $m = (p-1)/2$. There are two G-Galois covers of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ branched at $0, 1, \infty$ with ramification of order p, p, and m (up to outer automorphism.)*

(a) If $p \equiv 1 \bmod 4$ both covers have class vector (pA, pA, mA) and can be defined over K_0.

(b) If $p \equiv 3 \bmod 4$ one cover has class vector (pA, pA, mA) and the other (pA, pB, mA). Both can be defined over K_0.

Proof: This follows by lifting the triples to $\mathrm{SL}_2(p)$ and arguing as in [19, Lemma 3.27]. To prove that the corresponding covers are defined over K_0 use [19, Theorem 3.25]. □

Theorem 5.4.2 *Let $G = \mathrm{PSL}_2(p)$. Suppose $p \geq 7$. There is no G-Galois cover of $\mathbb{P}^1_k$ branched at exactly one point with $\sigma = (p-2)/m$.*

Proof: Let $H = A_p$. Let $g_{1,R} : \mathcal{Y} \to \mathcal{X}$ be the stable model of the H-Galois cover g_{1,K_0} defined in Corollary 5.2.2 and $g_1 : Y \to X$ be its stable reduction. Recall that X has three irreducible components: the original component Z, a primitive tail X_1 and a new tail X_2. Let τ_1 (resp. τ_2) be the intersection point of X_1 (resp. X_2) with Z. The decomposition group of a component above Z has order pm. The decomposition group of a component above X_1 has order pm and $\sigma_1 = 1/m$. The decomposition group of a component above X_2 is the full group H and $\sigma_2 = (p-2)/m$.

Let R/R_0 be minimal such that the stable model is defined over R. In [20] it is shown that the quotient field K of R contains $K_0(\zeta_p, (\zeta_p - 1)^{1/(p-2)})$. This is seen as follows. Let $\mathcal{Z}$ be the stable model of X_{K_0} and write $\mathcal{Y}_0$ for the normalization of $\mathcal{Z}$ in the function field of Y_{K_0}. First we need to enlarge R_0 so that the special fiber Y_0 of $\mathcal{Y}_0$ is reduced. This implies that R contains ζ_p as in Proposition 3.2.3. To prove the statement, one has to analyze the minimal extension of R_0 over which the blow up of $\mathcal{Y}_0$ defining the new tail Y_2 is defined.

Choose an injection $G \to H$ so that we may regard G as a subgroup of H. Suppose there exists a G-Galois cover $f : W \to \mathbb{P}^1_k$ branched at exactly one point with $\sigma = (p-2)/m$. Let $\hat{f} : \hat{\mathcal{O}}_{W,w} \to \hat{\mathcal{O}}_{\mathbb{P}^1_k,\infty}$ (resp. $\hat{g}_1 : \hat{\mathcal{O}}_{Y_2,y} \to \hat{\mathcal{O}}_{X_1,\tau_2}$) be the local cover, where w (resp. y) is some point in the fiber above τ_2. There exists an isomorphism $\mathbb{P}^1_k \xrightarrow{\sim} X_2$ which sends ∞ to τ and whose localization lifts to an isomorphism $\hat{f} \simeq \hat{g}_1$. This follows from Artin–Schreier Theory since $\sigma = (p-2)/m \leq 2$, [12, Theorem 2.4.7]. Let $U = Z \cup X_1$. Let $f_1 : Y' \to X$ be the G-equivariant morphism such that the following conditions hold: the restriction of f_1 to X_2 equals f; the restriction of f_1 to U is $\mathrm{Ind}_{D(V)}^G(V \to U)$ for a suitable connected component V of $g^{-1}(U)$ whose decomposition group is contained in G.

As in [15, Proposition 3.2.6] one shows that there exists a stable G-Galois cover $f_{1,R} : \mathcal{Y}' \to \mathcal{X}$ whose geometric generic fiber is branched at three points of order p, p, m and whose special fiber is f_1. By Lemma 5.4.1, $f_{1,K} : Y'_K \to X_K$ can be descended to K_0. This implies that $\Gamma = \mathrm{Gal}(K/K_0)$ acts on the stable reduction f_1 of $f_{1,K}$. In [20] it is shown that the action of Γ on X_2 induced by f_1 is the same as the action of Γ on X_2 induced by g_1. Let Γ_2 be the image of Γ in $\mathrm{Aut}_k(W)$.

By definition of the monodromy, the action of Γ_2 commutes with the action of G. Since the center of G is trivial we conclude that $G \cap \Gamma_2 = (0)$. Using what we know on the monodromy action for g_1, we conclude that Γ_2 induces an action on X_2 of order $p-2$. Let Γ_2' be a subgroup of Γ_2 which is cyclic of order $p-2$ and acts faithfully on X_2. Note that Γ_2' acts trivially on the original component and therefore fixes τ_2. We obtain the following diagram.

$$\begin{array}{ccc} W & \stackrel{\Gamma_2'}{\to} & W' \\ \downarrow & & \downarrow \\ X_2 & \stackrel{\Gamma_2'}{\to} & X_2'. \end{array}$$

The cover $W' \to X_2'$ is a G-Galois cover branched at two points: above one point the ramification is tame of order $p-2$; above the other point the ramification is wild of order $p(p-1)$ with $\sigma = 1/m$.

We conclude that G contains an element of order $p-2$. This gives a contradiction. □

Corollary 5.4.3 *Let $p \geq 7$. Let $\Sigma_{1,p}$ (resp. $\Sigma_{2,p}$) be the set of $\sigma \in \mathbb{Q}$ for which there exists a cover of $\mathbb{P}_k^1$ with Galois group $\mathrm{PSL}_2(p)$ (resp. A_p) branched at exactly one point whose ramification is described by σ. Then $\Sigma_{1,p} \neq \Sigma_{2,p}$.*

Proof: This follows immediately from Theorem 5.4.2 and Corollary 5.1.2. □

6 Tables

Consider all G-Galois covers $f : Y \to \mathbb{P}_k^1$ of smooth connected curves branched at exactly one point. Here is a summary of the results on inertia groups and conductors from the previous sections. We assume that if $I \subset G$ is a subgroup of the form $\mathbb{Z}/p \rtimes \mathbb{Z}/n$, then the values of the conductor satisfy the necessary conditions $\gcd(h,p) = 1$ and $\gcd(h,n) = n'$.

Table : $G = \mathrm{PSL}_2(p)$ Let $p \geq 5$ and $m = (p-1)/2$.

Inertia	does not exist	exists
$\mathbb{Z}/p$	$h \leq 2$	$h \geq m+1$
$\mathbb{Z}/p \rtimes \mathbb{Z}/n, n \neq 1$	$h \leq n$ $h = p-2$ if $n = m$ and $p > 5$	For $0 < a \leq n$, all $h \equiv a \bmod n$ such that $h \geq a(m+1)$

Table : $G = \mathrm{PSL}_2(\ell)$ Suppose that $p \geq 3$ strictly divides $\ell \pm 1$.

Inertia	does not exist	might exist	exists
$\mathbb{Z}/p$	$h = 1$	$h = 2$ if $\ell \equiv \pm 3 \bmod 8$	$h \geq 3, h = 2$ if $\ell \equiv \pm 1 \bmod 8$
D_p	$h \leq 2$		$h \geq 3$
$\mathbb{Z}/pn, n \neq 1$	$h < 2n$	$h \geq 2n$	

Table : $G = A_p$ Note that $A_5 \simeq \mathrm{PSL}_2(5)$. Let $p \geq 7$ and $m = (p-1)/2$.

Inertia	does not exist	exists
$\mathbb{Z}/p$	$h = 1$	$h \geq 3, h = 2$ if $p = 7$
$\mathbb{Z}/p \rtimes \mathbb{Z}/n, n \neq 1$	$h \leq n$	For $0 < a \leq n$, all $h \equiv -a \bmod n$ such that $h \geq a(p-2)$. Additionally, all $t(p-t)/\gcd(p-1, t(p-t)) + cn$ for $1 < t \leq m$ and $c \in \mathbb{N}^+$

References

[1] S. S. Abhyankar. Galois theory on the line in nonzero characteristic. *Bull. of the AMS*, 27:68–133, 1992.

[2] S. S. Abhyankar. Alternating group coverings of the affine line for characteristic greater than two. *Math. Ann.*, 296:63–68, 1993.

[3] I. I. Bouw. Reduction of metacyclic covers and their Hurwitz spaces. Preprint, 2001.

[4] I. I. Bouw and S. Wewers. Reduction of covers and Hurwitz spaces. Submitted for publication, math.AG/0005120.

[5] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable II*, number 349 in LNM, pages 143–316. Springer-Verlag, 1972.

[6] A. Grothendieck. *Revêtement Étales et Groupe Fondamental (SGA I).* Number 224 in LNM. Springer-Verlag, 1971.

[7] D. Harbater. Formal patching and adding branch points. *Amer. J. Math.*, 115:487–508, 1993.

[8] B. Huppert. *Endliche Gruppen I.* Number 134 in Grundlehren. Springer-Verlag, 1967.

[9] N. M. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves.* Number 108 in Annals of Mathematical Studies. Princeton Univ. Press, 1985.

[10] F. F. Knudsen. The projectivity of the moduli space of stable curves, II. *Math. Scand.*, 52:161–199, 1983.

[11] R. J. Pries. Degeneration of wildly ramified covers of curves. Preprint, 2001.

[12] R. J. Pries. Families of wildly ramified covers of curves. To appear in Amer. J. math.

[13] R. J. Pries. Construction of covers with formal and rigid geometry. In J. Bost, editor, *Courbes semi-stables et groupe fondamental en géometrie algébrique (Luminy, 1998)*, number 187 in Progr. Math. pages 157–167. Birkhäuser, Basel, 2000.

[14] M. Raynaud. Revêtement de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar. *Invent. Math.*, 116:425–462, 1994.

[15] M. Raynaud. Spécialisation des revêtements en caractéristique $p > 0$. *Ann. Scient. Ec. Norm. Sup.*, 32:87–126, 1999.

[16] T. Sekiguchi, F. Oort, and N. Suwa. On the deformation of Artin–Schreier to Kummer. *Ann. Sci. École Norm. Sup.*, 22:345–375, 1989.

[17] J.-P. Serre. *Corps Locaux.* Hermann, 1968.

[18] J.-P. Serre. *Topics in Galois Theory.* Number 1 in Research notes in mathematics. Jones and Bartlett Publishers, 1992.

[19] H. Völklein. *Groups as Galois Groups.* Number 53 in Cambridge Studies in Adv. Math. Cambridge Univ. Press, 1996.

[20] S. Wewers. Galois covers with bad reduction. In preparation.

[21] S. Wewers. Reduction and lifting of special metacyclic covers. Preprint 2001.

Irene I. Bouw
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104
bouw@math.upenn.edu

Rachel J. Pries
Department of Mathematics
Columbia University
New York, NY 10027
pries@math.columbia.edu