

Alternating group covers of the affine line

Jeremy Muskat and Rachel Pries

April 9, 2010

Abstract

For an odd prime $p \equiv 2 \pmod{3}$, we prove Abhyankar's Inertia Conjecture for the alternating group A_{p+2} , by showing that every possible inertia group occurs for a (wildly ramified) A_{p+2} -Galois cover of the projective k -line branched only at infinity where k is an algebraically closed field of characteristic $p > 0$. More generally, when $2 \leq s < p$ and $\gcd(p-1, s+1) = 1$, we prove that all but finitely many rational numbers which satisfy the obvious necessary conditions occur as the upper jump in the filtration of higher ramification groups of an A_{p+s} -Galois cover of the projective line branched only at infinity.

2010 MSC: 11G20 and 12F12.

1 Introduction

Suppose $\phi : Y \rightarrow \mathbb{P}_k^1$ is a G -Galois cover of the projective k -line branched only at ∞ where G is a finite group and k is an algebraically closed field of characteristic $p > 0$. Let $p(G) \subset G$ be the normal subgroup generated by the conjugates of a Sylow p -subgroup. Then the $G/p(G)$ -Galois quotient cover is a prime-to- p Galois cover of \mathbb{P}_k^1 branched only at ∞ . Since the prime-to- p fundamental group of the affine line \mathbb{A}_k^1 is trivial, this implies that $p(G) = G$; a group G satisfying this condition is called *quasi- p* . In 1957, Abhyankar conjectured that a finite group G occurs as the Galois group of a cover $\phi : Y \rightarrow \mathbb{P}_k^1$ branched only at ∞ if and only if G is a quasi- p group [1]. Abhyankar's conjecture was proved by Raynaud [10] and Harbater [7].

Now suppose G_0 is the inertia group at a ramified point of ϕ . Then G_0 is a semi-direct product of the form $G_1 \rtimes \mathbb{Z}/(m)$ where G_1 is a p -group and $p \nmid m$ [12, IV]. Let $J \subset G$ be the normal subgroup generated by the conjugates

of G_1 . Then the G/J -Galois quotient cover is a tame Galois cover of \mathbb{P}_k^1 branched only at ∞ . Since the tame fundamental group of \mathbb{A}_k^1 is trivial, this implies that $J = G$. Based on this, Abhyankar stated the currently unproven Inertia Conjecture.

Conjecture 1.1 (Inertia Conjecture). *[3, Section 16] Let G be a finite quasi- p group. Let G_0 be a subgroup of G which is an extension of a cyclic group of order prime-to- p by a p -group G_1 . Then G_0 occurs as the inertia group of a ramified point of a G -Galois cover $\phi : Y \rightarrow \mathbb{P}_k^1$ branched only at ∞ if and only if the conjugates of G_1 generate G .*

There is not much evidence to support the converse direction of Conjecture 1.1. For every finite quasi- p group G , the Sylow p -subgroups of G do occur as the inertia groups of a G -Galois cover of \mathbb{P}_k^1 branched only at ∞ [6]. For $p \geq 5$, Abhyankar's Inertia Conjecture is true for the quasi- p groups A_p and $\mathrm{PSL}_2(\mathbb{F}_p)$ [5, Thm. 2]. In Theorem 5.2, we prove:

Theorem 1.2. *If $p \equiv 2 \pmod{3}$ is an odd prime, then Abhyankar's Inertia Conjecture is true for the quasi- p group A_{p+2} . In other words, every subgroup $G_0 \subset A_{p+2}$ of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ occurs as the inertia group of an A_{p+2} -Galois cover of \mathbb{P}_k^1 branched only at ∞ .*

Note that the values of m such that A_{p+2} contains a subgroup $G_0 \simeq \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ are exactly the divisors of $p-1$. We also give a second proof of Abhyankar's Inertia Conjecture for the group A_p when $p \geq 5$; this proof uses the original equations of Abhyankar [2] rather than relying on the theory of semi-stable reduction.

More generally, we study the ramification filtrations of A_n -Galois covers $\phi : Y \rightarrow \mathbb{P}_k^1$ branched only at ∞ when p is odd and $p \leq n < 2p$. This condition ensures that the order of A_n is strictly divisible by p , and so the ramification filtration is determined by the order of G_0 and the upper jump σ . The upper jump is a rational number that satisfies some necessary conditions, Notation 5.5. One motivation to study the ramification filtration is that it determines the genus of Y .

In Theorem 4.9, we compute the order of the inertia group and the upper jump of the ramification filtration of Abhyankar's A_{p+s} -Galois cover $\phi_s : Y_s \rightarrow \mathbb{P}_k^1$ branched only at ∞ when $2 \leq s < p$. This determines the genus of Y_s , which turns out to be quite small. When $\gcd(p-1, s+1) = 1$, the inertia group is a maximal subgroup of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ in A_{p+s} . This is

the basis of the proof of Theorem 1.2 when $s = 2$. It also leads to another application, Corollary 5.6, where we use the theory of formal patching to prove:

Corollary 1.3. *Suppose $2 \leq s < p$ and $\gcd(p-1, s+1) = 1$. Then all but finitely many rational numbers σ satisfying the obvious necessary conditions occur as the upper jump of an A_{p+s} -Galois cover of \mathbb{P}_k^1 branched only at ∞ .*

In fact, Corollary 1.3 is a strengthening of Theorem 1.2 when $s = 2$. When $s > 2$, the normalizer of a p -cycle in A_{p+s} contains more than one maximal subgroup of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$. This is because there are many elements of prime-to- p order that centralize a p -cycle in A_{p+s} . Thus, when $s > 2$, more equations will be needed to verify Abhyankar's Inertia Conjecture for the group A_{p+s} using the strategy of this paper.

We would like to thank Irene Bouw for suggesting this approach for this project. The second author was partially supported by NSF grant 07-01303.

2 Background

Let k be an algebraically closed field of characteristic $p \geq 3$. A *curve* in this paper is a smooth connected projective k -curve. A cover ϕ of the projective line branched only at ∞ will be called a *cover of the affine line* and the inertia group at a ramification point of ϕ above ∞ will be called *the inertia group of ϕ* . A *G -Galois cover* is a Galois cover $\phi : Y \rightarrow X$ together with an isomorphism $G \simeq \text{Aut}(Y/X)$; (the choice of isomorphism will not be important in this paper).

2.1 Ramification

Let K be the function field of a k -curve X . A *place* P of K/k is the maximal ideal of a valuation ring $\mathcal{O}_P \subset K$. Let \mathcal{P}_K denote the set of all such places. Let v_P denote the normed discrete valuation on the valuation ring \mathcal{O}_P . A *local parameter* at P is an element $\alpha \in \mathcal{O}_P$ such that $v_P(\alpha) = 1$.

Consider a finite separable extension F/K . Let \tilde{F} be the Galois closure of F/K and let G be the Galois group of \tilde{F}/K . A place $Q \in \mathcal{P}_F$ is said to *lie over* $P \in \mathcal{P}_K$ if $\mathcal{O}_P = \mathcal{O}_Q \cap K$ and we denote this by $Q|P$. For any $Q \in \mathcal{P}_F$ with $Q|P$, there is a unique integer $e(Q|P)$ such that $v_Q(x) = e(Q|P)v_P(x)$ for any $x \in K$. The integer $e(Q|P)$ is the *ramification index* of $Q|P$ in F/K .

The extension F/K is *wildly ramified* at $Q|P$ if p divides $e(Q|P)$. When there exists a ramification point Q such that p divides $e(Q|P)$, we say that the extension is *wildly ramified*.

2.2 Higher Ramification Groups

We will need the following material from [13, Chapter 3].

Definition 2.1. For any integer $i \geq -1$ the i -th lower ramification group of $Q|P$ is

$$G_i(Q|P) = \{\sigma \in G : v_Q(\sigma(z) - z) \geq i + 1 \text{ for all } z \in \mathcal{O}_Q\}.$$

We let G_i denote $G_i(Q|P)$ when the places are clear from context.

Proposition 2.2. *With the notation above, then:*

1. G_0 is the inertia group of $Q|P$, and thus $|G_0| = e(Q|P)$, and G_1 is a p -group.
2. $G_{-1} \supseteq G_0 \supseteq \dots$ and $G_h = \{\text{Id}\}$ for sufficiently large h .

Theorem 2.3 (Hilbert's Different Formula). *The different exponent of F/K at $Q|P$ is*

$$d(Q|P) = \sum_{i=0}^{\infty} (|G_i(Q|P)| - 1).$$

Here is the Riemann-Hurwitz formula for wildly ramified extensions.

Theorem 2.4 (Riemann-Hurwitz Formula). *Let g (resp. g') be the genus of the function field K/k (resp. F/k). Then*

$$2g' - 2 = [F : K](2g - 2) + \sum_{P \in \mathcal{P}_K} \sum_{Q|P} d(Q|P).$$

2.3 Properties of Ramification Groups

Suppose that the order of G is strictly divisible by p . Suppose that F/K is wildly ramified at Q . The following material about the structure of the inertia group and the higher ramification groups can be found in [12, IV].

Lemma 2.5. [12, IV, Cor. 4] If F/K is wildly ramified at $Q \in \mathcal{P}_F$ with inertia group G_0 such that $p^2 \nmid |G_0|$, then G_0 is a semidirect product of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ for some prime-to- p integer m .

The lower numbering on the filtration from Definition 2.1 is invariant under sub-extensions. There is a different indexing system on the filtration, whose virtue is that it is invariant under quotient extensions.

Definition 2.6. [12, IV, Section 3] The *lower jump* of F/K of $Q|P$ is the largest integer h such that $G_h \neq \{1\}$. Let $\varphi(i) = |G_0|^{-1} \sum_{j=1}^i |G_j|$. Define $G^{\varphi(i)} = G_i$. Then $\varphi(h) = h/m$. The rational number $\sigma = h/m$ is the *upper jump*; it is the jump in the filtration of the higher ramification groups in the upper numbering.

Let $\tau \in G_0$ have order p and $\beta \in G_0$ have order m , so that $G_0 \cong \langle \tau \rangle \rtimes \langle \beta \rangle$.

Lemma 2.7. [12, IV, Prop. 9] With notation as above:

1. If $\beta \in G_0$ has order m and h is the lower jump, then $\beta\tau\beta^{-1} = \beta^h\tau$.
2. G_0 is contained in the normalizer $N_G(\langle \tau \rangle)$.

2.4 Alternating groups

Suppose that G is an alternating group A_n . Let $p \leq n < 2p$ so that $p^2 \nmid |G|$. The following lemmas give an upper bound for the size of the inertia group.

Lemma 2.8. Let $\tau = (12 \dots p)$. Then $N_{A_p}(\langle \tau \rangle) = \langle \tau \rangle \rtimes \langle \beta_\circ \rangle$ for some $\beta_\circ \in A_p$ with $|\beta_\circ| = (p-1)/2$.

Proof. Let n_p be the number of Sylow p -subgroups of A_p ; then $n_p = [A_p : N_{A_p}(\langle \tau \rangle)]$. There are $(p-1)!$ different p -cycles in A_p , each generating a group with $p-1$ non-trivial elements. It follows that $n_p = (p-2)!$. Therefore, $|N_{A_p}(\langle \tau \rangle)| = p(p-1)/2$.

Clearly, $\langle \tau \rangle \subset N_{A_p}(\langle \tau \rangle)$; we show the existence of β_\circ . Let $a \in \mathbb{F}_p^*$ with $|a| = p-1$. There exists $\theta \in S_p$ such that $\theta\tau\theta^{-1} = \tau^a$. The permutation θ exists since all p -cycles in S_p are in the same conjugacy class. Let $\beta_\circ = \theta^2$. Then $\beta_\circ \in A_p$ and $\beta_\circ \in N_{A_p}(\langle \tau \rangle)$. Also, for any r ,

$$\beta_\circ^r \tau \beta_\circ^{-r} = \theta^{2r} \tau \theta^{-2r} = \tau^{a^{2r}}.$$

Choosing $r = (p-1)/2$ shows that $\beta_o^{(p-1)/2}$ is contained in the centralizer $C_{A_p}(\langle \tau \rangle) = \langle \tau \rangle$, and it follows that $\beta_o^{(p-1)/2} = 1$. If $1 \leq r < (p-1)/2$, then $\beta_o^r \notin C_{A_p}(\langle \tau \rangle)$ and thus $\beta_o^r \neq 1$. It follows that β_o normalizes $\langle \tau \rangle$ in A_p and β_o has order $(p-1)/2$. \square

Recall that $C_{S_n}(\langle \tau \rangle) = \langle \tau \rangle \times H$ where $H = \{\omega \in S_n : \omega \text{ is disjoint from } \tau\}$.

Lemma 2.9. *Let $2 \leq s < p$ and let $\tau = (12 \dots p)$. Let $H_s \subset S_{p+s}$ be the subgroup of permutations of the set $\{p+1, p+2, \dots, p+s\}$. Then there exists $\theta \in S_p$ such that $|\theta| = p-1$ and $N_{A_{p+s}}(\langle \tau \rangle)$ is the intersection of A_{p+s} with $(\langle \tau \rangle \rtimes \langle \theta \rangle) \times H_s$.*

Proof. The permutation θ in the proof of Lemma 2.8 has order $p-1$ and normalizes τ . The elements of H_s commute with τ and θ . Thus $(\langle \tau \rangle \rtimes \langle \theta \rangle) \times H_s \subset N_{S_{p+s}}(\langle \tau \rangle)$. Performing a similar count as for Lemma 2.8, we find that the number of Sylow p -subgroups in S_{p+s} is $(p+s)!/(s!p(p-1))$. Therefore $|N_{S_{p+s}}(\langle \tau \rangle)| = s!p(p-1)$. Thus $(\langle \tau \rangle \rtimes \langle \theta \rangle) \times H_s = N_{S_{p+s}}(\langle \tau \rangle)$. The result follows by taking the intersection with A_{p+s} . \square

Note that the order of $N_{A_p}(\langle \tau \rangle)$ forces θ to be an odd permutation. Suppose $G_0 = \langle \tau \rangle \rtimes \langle \beta \rangle$ is a subgroup of A_{p+s} . Then $\beta = \theta^i \omega$ where $\omega \in H_s$ and ω is an even permutation if and only if i is even.

Recall that for an inertia group G_0 with $p^2 \nmid |G_0|$, there is a unique lower jump h which encodes information about the filtration of higher ramification groups. The following two lemmas relate the congruence class of h modulo m to the order of the centralizer $C_{G_0}(\langle \tau \rangle)$.

Lemma 2.10. *Let $\pi : X \rightarrow \mathbb{P}_k^1$ be an A_p -Galois cover which is wildly ramified at a point Q above ∞ with inertia group G_0 . If $|G_0| = pm$ and π has lower jump h at Q , then $\gcd(h, m) = 1$.*

Proof. Let $\beta \in A_p$ be such that $G_0 = \langle \tau \rangle \rtimes \langle \beta \rangle$. Notice that $C_{G_0}(\langle \tau \rangle) = \langle \tau \rangle$ since there are no elements of A_p disjoint from τ . Then $\beta^i \notin C_{G_0}(\langle \tau \rangle)$ for all $1 \leq i < m$. By Lemma 2.7(1), if $1 \leq i < m$, then $\tau \neq \beta^i \tau \beta^{-i} = \beta^{ih} \tau$. Notice that $\beta^{ih} \neq 1$ which implies that $m \nmid ih$ for each $1 \leq i < m$. Hence $\gcd(h, m) = 1$. \square

Lemma 2.11. *Let $2 \leq s < p$, and let $\phi : Y \rightarrow \mathbb{P}_k^1$ be an A_{p+s} -Galois cover which is wildly ramified at a point Q above ∞ with inertia group G_0 . If $|G_0| = pm$ and ϕ has lower jump h at Q , then $C_{G_0}(\langle \tau \rangle) \cong \mathbb{Z}/(p) \times \mathbb{Z}/(m')$ where $m' = \gcd(h, m)$.*

Proof. Let $\beta \in A_{p+s}$ be such that $G_0 = \langle \tau \rangle \rtimes \langle \beta \rangle$. Let $m' = \gcd(h, m)$. Then Lemma 2.7(1) implies $\beta^{m/m'} \tau \beta^{-m/m'} = \beta^{m \cdot h/m'} \tau = \tau$. The last equality is true because $|\beta| = m$ and $h/m' \in \mathbb{Z}$. It follows that $\beta^{m/m'} \in C_{G_0}(\langle \tau \rangle)$, that is $\langle \tau \rangle \times \langle \beta^{m/m'} \rangle \subset C_{G_0}(\langle \tau \rangle)$.

Suppose that $\alpha \in \langle \beta \rangle \cap C_{G_0}(\langle \tau \rangle)$. Lemma 2.7(1) implies $\tau = \alpha \tau \alpha^{-1} = \alpha^h \tau$. It follows that $|\alpha|$ divides h and m , so $|\alpha|$ divides m' and $\alpha \in \langle \beta^{m/m'} \rangle$. Hence $C_{G_0}(\langle \tau \rangle) = \langle \tau \rangle \times \langle \beta^{m/m'} \rangle$. \square

3 Newton Polygons

Suppose f defines a degree n extension F of $k(x)$ that is ramified above the place (x) . Let \tilde{F} be the splitting field of f over $k(x)$. Let Q be a ramified place in \tilde{F} above (x) . Let G_0 be the inertia group of $\tilde{F}/k(x)$ at Q . Let ϵ be a local parameter of the valuation ring \mathcal{O}_Q . Let v_Q denote the valuation at Q .

The Galois extension $\tilde{F}/k(x)$ yields a totally ramified Galois extension of complete local rings $k[[\epsilon]]/k[[x]]$. Let $f_2 \in k[[x]][y]$ be the minimal polynomial for ϵ . Let $e = e(Q|0)$ be the degree of f_2 . Define a polynomial $N(z) \in \hat{\mathcal{O}}_Q[z]$ such that

$$\epsilon^{-e} N(z) := \epsilon^{-e} f_2(\epsilon(z+1)) = \prod_{\omega \in G_0} \left(z - \left(\frac{\omega(\epsilon) - \epsilon}{\epsilon} \right) \right). \quad (3.1)$$

Define coefficients $b_i \in \hat{\mathcal{O}}_Q$ such that $N(z) = \sum_{i=1}^e b_i z^i$. The Newton polygon Δ of $N(z)$ is obtained by taking the lower convex hull of the set of points $\{(i, v_Q(b_i))\}_{i=1}^e$. Since f_2 is monic, the polygon is a sequence of line segments with increasing negative slopes.

The next proposition shows that the higher ramification groups of $\tilde{F}/k(x)$ at Q are determined by the slopes of Δ . This is not surprising because, as in [8, Chapter 2], the Newton polygon of $N(z)$ relates the valuations of the coefficients and roots of $N(z)$ and the higher ramification groups are determined by studying the valuation of the roots of $N(z)$.

Proposition 3.1. [11, Thm. 1] *Let $\{V_0, V_1, \dots, V_r\}$ be the vertices of Δ and $-h_j$ the slope of the edge joining V_{j-1} and V_j . The slopes are integral and the lower jumps in the sequence of higher ramification groups are $h_r < h_{r-1} < \dots < h_1$.*

Lemma 3.2. *For $1 < t < p - 2$, let $f_{1,t}(y) = y^p - xy^{p-t} + x \in k(x)[y]$. Let $F_t/k(x)$ be the corresponding extension of function fields and $\tilde{F}_t/k(x)$ its Galois closure. Let Q be a place of \tilde{F}_t lying over 0 . Then $e(Q|0) = pm$ for some integer m such that $p \nmid m$. Then the Newton polygon Δ_t of $\tilde{F}_t/k(x)$ has two line segments, one having integral slope $-m(p-t)/(p-1)$ and the other having slope 0.*

Proof. Let G be the Galois group of the extension $\tilde{F}_t/k(x)$. Notice that G is contained in S_p ; therefore the order of G is strictly divisible by p . The extension is branched over $x = 0$. Let P and Q be places lying above 0 in F_t and \tilde{F}_t respectively. The format of the equation $f_{1,t}$ implies that $e(P|0) = p$; let m be the integer such that $e(Q|0) = pm$. Then $p \nmid m$ since $p^2 \nmid |G|$. Let G_0 be the inertia group at Q . Let x, η , and ϵ be local parameters of \mathcal{O}_x , \mathcal{O}_P , and \mathcal{O}_Q respectively. The extension $\mathcal{O}_Q/k[[x]]$ is totally ramified with Galois group G_0 of order pm .

Field	Complete Local Ring	Local Parameter
\tilde{F}_t	$\hat{\mathcal{O}}_Q$	ϵ
$ $	$ _m$	$ $
F_t	$\hat{\mathcal{O}}_P$	η
$ $	$ _p$	$ $
$k(x)$	$k[[x]]$	x

Notice that any root of $f_{1,t}$ is a local parameter at P since

$$p = v_P(x) = v_P\left(\frac{y^p}{y^{p-t} + 1}\right) = p v_P(y).$$

Thus we can assume that η is a root of $f_{1,t}$. Now consider η as an element of $\hat{\mathcal{O}}_Q$. Then η can be expressed as a power series in the local parameter ϵ with coefficients in k , that is $\eta = u \cdot \epsilon^m$ where u is a unit of $\hat{\mathcal{O}}_Q$. Also u is an m -th power in the complete local ring $\hat{\mathcal{O}}_Q$ so by changing the local parameter ϵ we can suppose $\eta = \epsilon^m$. It follows that ϵ satisfies the equation

$$f_{2,t}(\epsilon) = \epsilon^{pm} - x\epsilon^{m(p-t)} + x = 0. \quad (3.2)$$

The polynomial $f_{2,t}(\epsilon)$ is Eisenstein at the prime (x) . Now we consider

$$N(z) = f_{2,t}(\epsilon(z+1)) = \epsilon^{pm}(z+1)^{pm} - x\epsilon^{m(p-t)}(z+1)^{m(p-t)} + x. \quad (3.3)$$

Dividing both sides of Equation 3.3 by ϵ^{pm} produces a vertical shift by $-pm$ to the Newton polygon Δ_t . Vertical and horizontal shifts do not affect the slopes of the line segments of Δ_t . Substituting $x = \epsilon^{pm}/(\epsilon^{m(p-t)} - 1)$ and letting $d = 1/(\epsilon^{m(p-t)} - 1)$, then

$$\frac{N(z)}{\epsilon^{pm}} = (z + 1)^{pm} - d\epsilon^{m(p-t)}(z + 1)^{m(p-t)} + d.$$

Notice that $N(0) = 0$ so we can factor a power of z from $N(z)$. The effect on Δ_t is a shift in the horizontal direction by -1 . This results in

$$\frac{N(z)}{z\epsilon^{pm}} = \sum_{i=0}^{m-1} \binom{m}{i} z^{p(m-i)-1} + -d\epsilon^{m(p-t)} \sum_{i=0}^{m(p-t)-1} \binom{m(p-t)}{i} z^{m(p-t)-i-1}.$$

Let $z^{-1}\epsilon^{-pm}N(z) = \sum_{j=0}^{pm-1} b_j z^j$. The valuation of each b_j is greater than or equal to zero. The ramification polygon Δ_t is determined by calculating the valuations of the specific coefficients that determine the lower convex hull of Δ_t :

1. $v_Q(b_0) = v_Q(dmt\epsilon^{m(p-t)}) = m(p-t)$.
2. For $1 \leq j < p-1$, let $i_j = m(p-t) - j - 1$, then

$$v_Q(b_j) = v_Q\left(-d\epsilon^{m(p-t)} \binom{m(p-t)}{i_j}\right) \geq m(p-t).$$

$$3. v_Q(b_{p-1}) = v_Q\left(m - d\epsilon^{m(p-t)} \binom{m(p-t)}{m(p-t)-p}\right) = 0.$$

4. $v_Q(b_{pm-1}) = v_Q(1) = 0$.

The vertices of Δ_t are thus $(0, m(p-t))$, $(p-1, 0)$, and $(pm-1, 0)$. \square

Lemma 3.3. *For $2 \leq s < p$, let $g_s(y) = y^{p+s} - xy^s + 1 \in k(x)[y]$. Let $L_s/k(x)$ be the corresponding extension of function fields and $\tilde{L}_s/k(x)$ its Galois closure. Let Q be a place of \tilde{L}_s lying over ∞ . Then $e(Q|\infty) = pm$ for some integer m such that $p \nmid m$ and the Newton polygon Δ'_s of $\tilde{L}_s/k(x)$ has two line segments, one having integral slope $-m(p+s)/(p-1)$ and the other having slope 0.*

Proof. Let G be the Galois group of the extension $\tilde{L}_s/k(x)$. Notice that G is contained in S_{p+s} ; therefore the order of G is strictly divisible by p . The extension is branched over ∞ . Let $P_{(\infty,0)}$ and $P_{(\infty,\infty)}$ be the two places of L_s lying above ∞ . The format of the equation g_s implies that $P_{(\infty,0)}$ and $P_{(\infty,\infty)}$ have ramification indices p and s respectively, see e.g., Lemma 4.8. Let Q be a place of \tilde{L}_s lying above $P_{(\infty,0)}$. Let m be the integer $e(Q|\infty)/p$. Let G_0 be the inertia group at Q . Let x^{-1} , η , and ϵ be local parameters of $\mathcal{O}_{x^{-1}}$, $\mathcal{O}_{P_{(\infty,0)}}$, and \mathcal{O}_Q respectively.

Field	Complete Local Ring			Local Parameter
\tilde{L}_s	Q		$\hat{\mathcal{O}}_Q$	ϵ
	$m $		$m $	
L_s	$P_{(\infty,0)}$	$P_{(\infty,\infty)}$	$\hat{\mathcal{O}}_{P_{(\infty,0)}}$	η
	$p\backslash$	$/s$	$p $	
$k(x)$	∞		$k[[x^{-1}]]$	x^{-1}

Then $\hat{\mathcal{O}}_Q/k[[x^{-1}]]$ is a totally ramified Galois extension with Galois group G_0 of order pm . By the same reasoning as for Lemma 3.2, there exists a local parameter ϵ of $\hat{\mathcal{O}}_Q$ that satisfies $\epsilon^m = \eta$. Therefore ϵ satisfies the irreducible equation

$$g_{2,s}(\epsilon) = \epsilon^{m(p+s)} - x\epsilon^{ms} + 1 = 0. \quad (3.4)$$

We calculate the ramification polygon Δ'_s by considering

$$N(z) = g_{2,s}(\epsilon(z+1)) = \epsilon^{m(p+s)}(z+1)^{m(p+s)} - x\epsilon^{ms}(z+1)^{ms} + 1. \quad (3.5)$$

Since $N(0) = 0$, it follows that

$$\frac{N(z)}{z\epsilon^{m(p+s)}} = (z+1)^{ms} \sum_{i=0}^{m-1} \binom{m}{i} z^{p(m-i)-1} - (1 + \epsilon^{-m(p-s)}) \sum_{i=0}^{ms-1} \binom{ms}{i} z^{ms-1-i}.$$

Let $z^{-1}\epsilon^{-m(p+s)}N(z) = \sum_{j=1}^{m(p+s)-1} b_j z^j$. The valuation of each b_j is non-negative. The ramification polygon Δ'_s is determined when we calculate the valuations of the specific coefficients that determine the lower convex hull of Δ'_s .

1. $v_Q(b_0) = m(p+s)$.
2. $v_Q(b_j) \geq m(p+s)$ for $1 \leq j < p-1$.

$$3. \ v_Q(b_{p-1}) = 0.$$

$$4. \ v_Q(b_{m(p+s)-1}) = 0.$$

The vertices of Δ'_s are thus $(0, m(p-s))$, $(p-1, 0)$, and $(m(p+s)-1, 0)$. \square

4 A_n -Galois covers of the affine line

Suppose $\pi : X \rightarrow \mathbb{P}_k^1$ is an A_n -Galois cover branched only at ∞ . The cover is wildly ramified at each point $Q \in X$ above ∞ . The complexity of the wild ramification is directly related to the power of p that divides the ramification index $e(Q|\infty)$. For this reason, we concentrate on Galois groups A_n such that the order of A_n is strictly divisible by p . We use some equations of Abhyankar to study A_n -Galois covers when p is odd and $p \leq n < 2p$. The goal is to determine the inertia groups and upper jumps that occur for A_n -Galois covers $\pi : X \rightarrow \mathbb{P}_k^1$ branched only at ∞ . This ramification data also determines the genus of the curve X .

4.1 Two useful lemmas

The following is a version of Abhyankar's Lemma which will be needed to construct a G -Galois cover of \mathbb{P}_k^1 branched only at ∞ from a G -Galois cover of \mathbb{P}_k^1 branched at 0 and ∞ .

Lemma 4.1 (Refined Abhyankar's Lemma). *Let m , r_1 , and r_2 be prime-to- p integers. Suppose $\pi : X \rightarrow \mathbb{P}_k^1$ is a G -Galois cover with branch locus $\{0, \infty\}$. Suppose π has ramification index r_1 above 0 and inertia group $G_0 \cong \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ above ∞ with lower jump h . Let $\psi : \mathbb{P}_k^1 \rightarrow \mathbb{P}_k^1$ be an r_2 -cyclic cover with branch locus $\{0, \infty\}$. Assume that π and ψ are linearly disjoint.*

Then the pullback $\pi' = \psi^\pi$ is a G -Galois cover $\pi' : X' \rightarrow \mathbb{P}_k^1$ with branch locus contained in $\{0, \infty\}$, with ramification index $r_1/\gcd(r_1, r_2)$ above 0, with inertia group $G'_0 \subset G_0$ of order $pm/\gcd(m, r_2)$ above ∞ and with lower jump $hr_2/\gcd(m, r_2)$. If σ and σ' are the upper jumps of π and π' respectively, then $\sigma' = r_2\sigma$.*

Proof. Consider the fibre product:

$$\begin{array}{ccc} X & \leftarrow & X' \\ \pi \downarrow & & \downarrow \pi' \\ \mathbb{P}_k^1 & \leftarrow & \mathbb{P}_k^1 \\ & \psi & \end{array}$$

All the claims follow from the classical version of Abhyankar's Lemma [7, Lemma X.3.6] except for the information about the lower and upper jumps of π' . Consider the composition $\psi\pi'$ which has ramification index $pmr_2/\gcd(m, r_2)$ above ∞ . Since upper jumps are invariant under quotients, the upper jump of $\psi\pi'$ equals σ . Thus the lower jump of $\psi\pi'$ equals $\sigma mr_2/\gcd(m, r_2) = hr_2/\gcd(m, r_2)$ by Definition 2.6. This equals the lower jump of π' since lower jumps are invariant for subcovers and the claim about the upper jump of π' follows from Definition 2.6. \square

The following lemma is useful to compare ramification information about a cover and its Galois closure. Let $S_n^1 := \text{Stab}_{S_n}(1)$.

Lemma 4.2. *If $\rho : Z \rightarrow W$ is a cover with Galois closure $\pi : X \rightarrow W$, then the branch locus of ρ and of π are the same.*

Proof. The branch locus of ρ is contained in the branch locus of π since ramification indices are multiplicative. Assume that b is in the branch locus of π but not in the branch locus of ρ . We will show that this is impossible. The Galois group H of π is a transitive subgroup of S_n , where n is the degree of ρ . The Galois group H' of $X \rightarrow Z$ is a subgroup of H with index n . After identifying H with a subgroup of S_n , we can assume without loss of generality that $H' \subset S_n^1$. Let $Q \in X$ be a ramification point lying above b with inertia group G_0 . Conjugating G_0 by an element $\omega \in H$ results in an inertia group at some point of X above b . Since b is not a branch point of ρ , we have that $\omega G_0 \omega^{-1} \subset S_n^1$ for all $\omega \in H$. This is impossible since H is transitive on the set $\{1, 2, \dots, n\}$. Therefore the branch loci must be the same. \square

4.2 A_p -Galois covers of the affine line

Let $p \geq 5$. In this section, we find A_p -Galois covers $\pi : X \rightarrow \mathbb{P}_k^1$ branched only at ∞ with a small upper jump.

Notation 4.3. Let t be an integer with $1 < t < p-2$ and let $f_t = y^p - y^t + x$. Consider the curve Z_t with function field $F_t := k(x)[y]/(f_t)$. Let $\pi_t : X_t \rightarrow \mathbb{P}_k^1$ be the Galois closure of $\rho_t : Z_t \rightarrow \mathbb{P}_k^1$; the function field of X_t is the Galois closure \tilde{F}_t of $F_t/k(x)$. Let ζ be a $(p-t)$ th root of unity.

Abhyankar proved that the Galois group of π_t is A_p when t is odd and S_p when t is even [2, Section 20]. For the proof, he showed that the Galois group is doubly transitive on the set $\{1, 2, \dots, p\}$ and contains a certain cycle

type. We now study the ramification of the cover π_t . The following result can be found in [2, Section 20].

Lemma 4.4. *The cover $\pi_t : X_t \rightarrow \mathbb{P}_k^1$ has one ramified point above $x = 0$ with ramification index t and is unramified above all other points of \mathbb{A}_k^1 .*

Proof. When $x = 0$ in the equation f_t , then $y = 0$ or $y = \zeta^i$ for some $1 \leq i \leq p - t$. There are $p - t + 1$ points in the fibre of ρ above the point $x = 0$ which we denote by $P_{(0,0)}$ and $P_{(0,\zeta)}, \dots, P_{(0,1)}$. Since $p - t + 1 < p$, then $x = 0$ is a branch point of ρ .

The value $y = 0$ is the only solution to $\partial f / \partial y = 0$. Therefore $P_{(0,0)}$ is the only ramification point above \mathbb{A}_k^1 . The Galois group H of π_t is either S_p or A_p . Thus Lemma 4.2 implies that π_t is unramified above all points of \mathbb{A}_k^1 except $x = 0$.

Because $p = \sum_{P \mid 0} e(P \mid 0)$, it follows that $P_{(0,0)}$ has ramification index t . Let $Q \in X_t$ be a point lying above $P_{(0,0)}$. It remains to show that $e(Q|P_{(0,0)}) = 1$.

Let H' be the Galois group of $X_t \rightarrow Z_t$. Without loss of generality we can suppose that $H' \subset S_p^1$. Since $p \nmid |H'|$, Lemma 2.5 implies that $G_0(Q|0)$ is a cyclic group of order $t \cdot c$ for some prime-to- p integer c .

Assume $c \neq 1$. If ω is a generator for $G_0(Q|0)$; then $\omega \notin S_p^1$ since $P_{(0,0)}$ is ramified over 0. Then $G_0(Q|P_{(0,0)}) = \langle \omega^t \rangle \subset S_p^1$. By the assumption on c , the automorphism ω^t is not the identity. Since H is transitive on $\{1, 2, \dots, p\}$, there exists $\gamma \in H$ such that $\gamma\phi^t\gamma^{-1} \notin S_p^1$.

There exists a point \tilde{Q} in the fiber of X_t above 0 such that $G_0(\tilde{Q}|0) = \langle \gamma^{-1}\phi\gamma \rangle$. Since $\gamma \notin S_p^1$, the point \tilde{Q} is in the fibre of π_t over 0 but not in the fibre above $P_{(0,0)}$. Furthermore, $\gamma\phi^t\gamma^{-1} = (\gamma\phi\gamma^{-1})^t \in G_0(\tilde{Q}|0)$. Hence $G_0(\tilde{Q}|0) \not\subset S_p^1$. Therefore, for some i , the extension $P_{(0,\zeta^i)}|0$ is ramified. This gives a contradiction so the assumption that $c \neq 1$ is false. \square

Lemma 2.5 implies that the inertia group G_0 at a point of X_t over ∞ is of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ where $p \nmid m$. To determine the upper jump σ of π_t over ∞ , we use the equation f_t to understand the ramification that occurs in the quotient map $\rho_t : Z_t \rightarrow \mathbb{P}_k^1$.

Lemma 4.5. *The cover $\pi_t : X_t \rightarrow \mathbb{P}_k^1$ has ramification index $p(p-1)/\gcd(p-1, t-1)$ and upper jump $\sigma = (p-t)/(p-1)$ above ∞ .*

Proof. Let P_∞ be a point of Z_t that lies above ∞ . Then

$$-e(P_\infty|\infty) = v_{P_\infty}(x) = v_{P_\infty}(y^p - y^t) = p v_{P_\infty}(y).$$

Therefore $p|e(P_\infty|\infty)$ and it follows that ρ is totally ramified at P_∞ .

Consider the change of variables $x \mapsto 1/x$ and $y \mapsto 1/y$. Understanding the ramification over ∞ is equivalent to understanding the ramification over $x = 0$ of the cover with equation $f_{1,t} = y^p - xy^{p-t} + x$. By Lemma 3.2, the absolute value of the non-zero slope of the ramification polygon Δ_t of $\tilde{F}_t/k(x)$ is $m(p-t)/(p-1)$; this is the lower jump by Lemma 3.1. By Definition 2.6, the upper jump is $\sigma = (p-t)/(p-1)$.

By Lemma 2.10, h and m are co-prime, therefore $h = (p-t)/\gcd(p-t, t-1)$ and $m = (p-1)/\gcd(p-1, t-1)$ and $|G_0| = pm$. \square

Theorem 4.6. *For $1 < t < (p-2)$, let $m_t = (p-1)/\gcd(p-1, t(t-1))$. Then there exists an A_p -Galois cover $\pi'_t : X'_t \rightarrow \mathbb{P}_k^1$ branched only at ∞ with ramification index pm_t and upper jump $\sigma'_t = t(p-t)/(p-1)$. The genus of X'_t is $1 + |A_p|(t(p-t) - p - 1/m_t)/2p$.*

Proof. Let $d_1 = \gcd(p-1, t-1)$ and let $m = (p-1)/d_1$. Consider the Galois cover $\pi_t : X_t \rightarrow \mathbb{P}_k^1$ from Notation 4.3. Lemma 4.4 states that π_t has ramification index t above 0 and is unramified above $\mathbb{A}_k^1 - \{0\}$. Lemma 4.5 states that the inertia group G_0 above ∞ has order pm and upper jump $\sigma_t = (p-t)/(p-1)$.

If t is odd, then π_t has Galois group A_p . Let $m^* = \gcd(m, t)$. Since A_p is simple, the cover π_t is linearly disjoint from the t -cyclic cover $\psi : \mathbb{P}_k^1 \rightarrow \mathbb{P}_k^1$ with equation $z^t = x$. Applying Lemma 4.1, the pullback $\pi'_t = \psi^*\pi_t$ is a cover $\pi'_t : X'_t \rightarrow \mathbb{P}_k^1$ with Galois group A_p . The map π'_t is branched only at ∞ with inertia group G'_0 of order pm/m^* and upper jump $\sigma'_t = t(p-t)/(p-1)$. Notice that $d_1m^* = \gcd(p-1, t(t-1))$, so the inertia group has order $pm/m^* = p(p-1)/\gcd(p-1, t(t-1))$.

If t is even, then π_t has Galois group S_p . Let Y_t be the smooth projective curve corresponding to the fixed field $\tilde{F}_t^{A_p}$. Let $\mu_t : X_t \rightarrow Y_t$ be the subcover with Galois group A_p .

The branch locus of the degree 2 quotient cover $Y_t \rightarrow \mathbb{P}_k^1$ is contained in $\{0, \infty\}$. The ramification index must be 2 over both 0 and ∞ . By the Riemann-Hurwitz formula, Y_t has genus 0. Therefore $\mu_t : X_t \rightarrow \mathbb{P}_k^1$ is an A_p -Galois cover of the projective line.

Let P_0 (resp. P_∞) be the point of Y_t above 0 (resp. ∞). Since ramification indices are multiplicative, μ_t has ramification index $t/2$ over P_0 and $|G_0|/2$ over P_∞ . It can be seen that $|G_0|/2 = pm/2$ is an integer from Lemma 4.6 since t is even. The lower jump of μ_t is the same as the lower jump of π_t since lower jumps are invariant under subextensions. Therefore the upper jump of μ_t is 2σ .

The cover μ_t is linearly disjoint from the $t/2$ -cyclic cover $\psi : \mathbb{P}_k^1 \rightarrow \mathbb{P}_k^1$ with equation $z^{t/2} = x$. Let $\bar{m} = \gcd(m/2, t/2)$. Applying Lemma 4.1, the pullback $\pi'_t = \psi^* \mu_t$ is an A_p -Galois cover $\pi'_t : X'_t \rightarrow \mathbb{P}_k^1$. The map π'_t is branched only at ∞ where it has inertia group G'_0 of order $pm/(2\bar{m})$ and upper jump $\sigma'_t = t(p-t)/(p-1)$. Notice that $pm/2\bar{m} = pm/m^*$, so $|G'_0| = p(p-1)/\gcd(p-1, t(t-1))$.

The genus calculation is immediate from the Riemann-Hurwitz formula, Theorem 2.4. \square

The smallest genus for an A_p -Galois cover obtained using the method of Theorem 4.6 is

$$g = 1 + |A_p|(p^2 - 5p + 2)/2p(p-1).$$

This occurs when $t = 2$ or $t = p-2$ and the upper jump is $\sigma = 2(p-2)/(p-1)$. To see this, consider the derivative $d\sigma/dt = (p-2t)(p-1)$. Since this value of σ is less than 2, it is possible that this is the smallest genus that occurs among all A_p -Galois covers of the affine line. We find A_p -Galois covers with slightly larger upper jumps in Section 5.4.

4.3 A_{p+s} -Galois covers of the affine line

In this section, we find A_n -Galois covers of the projective line branched only at ∞ with small upper jump when p is odd and $p < n < 2p$.

Notation 4.7. Let s be an integer with $2 \leq s < p$. Consider the group A_{p+s} of even permutations on $p+s$ elements and the subgroup $H_s \subset S_{p+s}$ of permutations on $\{p+1, p+2, \dots, p+s\}$. Let $g_s = y^{p+s} - xy^s + 1$. Consider the curve Z'_s with function field $L_s := k(x)[y]/(g_s)$. Let $\phi_s : Y_s \rightarrow \mathbb{P}_k^1$ be the Galois closure of $\rho'_s : Z'_s \rightarrow \mathbb{P}_k^1$; the function field of Y_s is the Galois closure \tilde{L}_s of $L_s/k(x)$.

Abhyankar proved that the Galois group of ϕ_s is A_{p+s} except when $p = 7$ and $s = 2$ [2, Section 11]. The following result can be found in [2, Section 21].

Lemma 4.8. *The cover ρ'_s is branched only at ∞ . The fibre over ∞ consists of two points $P_{(\infty,0)}$ and $P_{(\infty,\infty)}$ which have ramification indices p and s respectively.*

Proof. There are no simultaneous solutions to the equations $g_s = 0$ and $\partial g_s / \partial y = 0$. Therefore the cover ρ'_s is not branched over any points of \mathbb{A}_k^1 . Since the tame fundamental group of \mathbb{A}_k^1 is trivial, ρ'_s must be wildly ramified above ∞ . The fibre of Z'_s over ∞ consists of two points $P_{(\infty,0)}$ and $P_{(\infty,\infty)}$. The first point can be seen by applying the change of variables $x \mapsto 1/x$ to g_s . This produces the equation $xy^{p+s} - y^s + x$. Taking the partial derivative with respect to y yields the point $P_{(\infty,0)}$. The second point can be seen by applying the change of variables $y \mapsto 1/y$ to $xy^{p+s} - y^s + x$ resulting in the equation $x - y^p + xy^{p+s}$. Taking the partial derivative with respect to y yields the point $P_{(\infty,\infty)}$. To show that $e(P_{(\infty,0)}|\infty) = p$ and $e(P_{(\infty,\infty)}|\infty) = s$, let P be either $P_{(\infty,0)}$ or $P_{(\infty,\infty)}$ and consider the valuation v_P . The result follows since

$$-e(P|\infty) = v_P(x) = v(y^p + y^{-s}) = \min\{pv_P(y), -sv_P(y)\}.$$

□

Theorem 4.9. *Let $2 \leq s < p$. If $p = 7$, assume $s \neq 2$. Let $m_s = (p-1)s/\gcd(p-1, s(s+1))$. Then there exists an A_{p+s} -Galois cover $\phi_s : Y_s \rightarrow \mathbb{P}_k^1$ branched only at ∞ with inertia group G_0 of order pm_s and upper jump $\sigma_s = (p+s)/(p-1)$. The genus of Y_s is $1 + |A_{p+s}|(s - 1/m_s)/2p$.*

In [4, Cor. 2.2], the author proves that the genus of Y_s in Theorem 4.9 is the smallest genus that occurs among all A_{p+s} -Galois covers of the affine line.

Proof. Consider the cover $\phi_s : Y_s \rightarrow \mathbb{P}_k^1$ defined in Notation 4.7. Abhyankar proved that ϕ_s has Galois group A_{p+s} [2, Section 11]. By Lemmas 4.2 and 4.8, ∞ is the only branch point of ϕ_s . Let Q be a point of Y_s lying above ∞ . The cover ϕ_s is wildly ramified at Q with $p^2 \nmid e(Q|\infty)$. By Lemma 2.5, the inertia group G_0 at Q is of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ for some prime-to- p integer m .

Let h be the lower jump of ϕ_s at Q . The Newton polygon of ϕ_s is the same as the Newton polygon Δ'_s calculated in Lemma 3.3. Therefore, $h = m(p+s)/(p-1)$, because this is the negative of the slope of the line segment of Δ'_s . By Definition 2.6, the upper jump is $\sigma_s = (p+s)/(p-1)$.

Write $m = m'm''$ where m' is the order of the prime-to- p center of G_0 . Lemma 2.7(1) implies that $m' = \gcd(h, m)$. Since $h/m = \sigma_s = (p+s)/(p-1)$, it follows that $m'' = (p-1)/\gcd(p-1, s+1)$.

Without loss of generality, we can suppose that $\tau = (12\dots p) \in G_0$. By Lemma 2.9, $G_0 = \langle \tau \rangle \rtimes \langle \beta \rangle$ for some β of the form $\beta = \theta^i \omega$. Recall that $\theta \in S_p$ acts faithfully by conjugation on τ and $\omega \in H_s$ commutes with τ . The inertia group G_0 acts transitively on $\{p+1, p+2, \dots, p+s\}$ by Lemma 4.8. Thus ω is a cycle of length s .

The order of β is m , the order of θ^i is m'' , and the order of β is s . Thus $m = \text{lcm}(m'', s)$. It follows that $m' = s/\gcd(p-1, s)$ and $m = (p-1)s/\gcd(p-1, s(s+1))$. The genus calculation is immediate from the Riemann-Hurwitz formula, Theorem 2.4. \square

5 Applications

5.1 Support for the Inertia Conjecture

In this section, we first give a new proof of Abhyankar's Inertia Conjecture for the group A_p ; this proof does not use the theory of semi-stable reduction. Then we prove Abhyankar's Inertia Conjecture for the group A_{p+2} for an odd prime $p \equiv 2 \pmod{3}$.

Corollary 5.1. [5, Cor. 3.1.5] *Let $p \geq 5$. Abhyankar's Inertia Conjecture is true for the alternating group A_p . In other words, every subgroup $G_0 \subset A_p$ of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ can be realized as the inertia group of an A_p -Galois cover of \mathbb{P}_k^1 branched only at ∞ .*

Proof. Suppose $G_0 \subset A_p$ satisfies the conditions of Conjecture 1.1. Since $p^2 \nmid |A_p|$, then $G_0 \simeq \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ for some prime-to- p integer m . Thus the second claim implies the first.

Consider a subgroup $G_0 \subset A_p$ of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$. The goal is to show that G_0 is the inertia group of an A_p -Galois cover of the affine line. Without loss of generality, we can suppose that $\tau = (12\dots p) \in G_0$. By Lemma 2.7(2), $G_0 \subset N_{A_p}(\langle \tau \rangle)$. Lemma 2.8 implies that $N_{A_p} \simeq \mathbb{Z}/(p) \rtimes \mathbb{Z}/((p-1)/2)$.

It thus suffices to prove, for every $m \mid (p-1)/2$, that there exists an A_p -Galois cover of the affine line, with an inertia group of order pm . Letting $t = 2$, Theorem 4.6 shows the existence of such a cover π_2 with an inertia

group of order $p(p-1)/2$. Since A_p is simple, π_2 is linearly disjoint from the degree r_2 cyclic cover of \mathbb{P}_k^1 which is branched at 0 and ∞ . The proof then follows by Lemma 4.1, taking $r_2 = (p-1)/2m$. \square

Corollary 5.2. *If $p \equiv 2 \pmod{3}$ is an odd prime, then Abhyankar's Inertia Conjecture is true for $G = A_{p+2}$. In other words, every subgroup $G_0 \subset A_{p+2}$ of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ can be realized as the inertia group of an A_{p+2} -Galois cover of \mathbb{P}_k^1 branched only at ∞ .*

Proof. Suppose $G_0 \subset A_{p+2}$ satisfies the conditions of Conjecture 1.1. Since $p^2 \nmid |A_{p+2}|$, then $G_0 \simeq \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ for some prime-to- p integer m . Thus the second claim implies the first.

Consider a subgroup $G_0 \subset A_{p+2}$ of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$. The goal is to show that G_0 is the inertia group of an A_{p+2} -Galois cover of the affine line. Without loss of generality, we can suppose that $\tau = (12\dots p) \in G_0$. By Lemma 2.7(2), $G_0 \subset N_{A_{p+2}}(\langle \tau \rangle)$. By Lemma 2.9, $N_{A_{p+2}}(\langle \tau \rangle) = \langle \tau \rangle \rtimes \langle \beta \rangle$ where $\beta = \theta(p+1 \ p+2)$. Recall that θ is an odd permutation of order $p-1$ defined in the proof of Lemma 2.8.

It thus suffices to prove, for every $m \mid (p-1)$, that there exists an A_{p+2} -Galois cover of the affine line, with an inertia group of order pm . Letting $s = 2$, Theorem 4.9 shows the existence of such a cover ϕ_2 with an upper jump $\sigma_2 = (p+2)/(p-1)$. Since $p \equiv 2 \pmod{3}$, the upper jump σ_2 is written in lowest terms and thus $m = p-1$. Since A_{p+2} is simple, ϕ_2 is linearly disjoint from a degree r_2 cyclic cover of \mathbb{P}_k^1 which is branched at 0 and ∞ . The proof then follows by Lemma 4.1, taking $r_2 = (p-1)/m$. \square

When $s > 2$, more equations are needed to prove Abhyankar's Conjecture for A_{p+s} because the normalizer $N_{A_{p+s}}(\langle \tau \rangle)$ contains more than one maximal subgroup of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$.

5.2 Formal Patching Results

Suppose $\pi : X \rightarrow \mathbb{P}_k^1$ is a G -Galois cover which is wildly ramified above ∞ with last upper jump σ . Using the theory of formal patching, it is possible to produce a different G -Galois cover with the same branch locus, but with a larger upper jump above ∞ . The formal patching proof is non-constructive and we do not describe it in this paper. Here are the results that we will use: the first allows us to change the congruence value of the lower jump modulo m and the second allows us to increase the lower jump by a multiple of m .

Lemma 5.3. [5, Prop. 3.1.1] Suppose $\pi : X \rightarrow \mathbb{P}_k^1$ is a G -Galois cover branched only at ∞ with inertia group $G_0 \cong \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ with $p \nmid m$ and with lower jump h . For each $d \in \mathbb{N}$ such that $1 \leq d \leq m$, let $m_d = m/\gcd(m, d)$ and $h_d = dh/\gcd(m, d)$. Let $G_0^d \subset G_0$ be the subgroup of order $p m_d$. Then there exists a G -Galois cover $\pi' : X' \rightarrow \mathbb{P}_k^1$ branched only at ∞ with inertia group G_0^d and lower jump h_d . If σ and σ' are the upper jumps of π and π' respectively, then $\sigma' = d\sigma$.

Theorem 5.4. [9, Special case of Theorem 2.3.1] Let $\pi : X \rightarrow \mathbb{P}_k^1$ be a G -Galois cover branched only at ∞ with inertia group $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ and upper jump $\sigma = h/m$. Then for $i \in \mathbb{N}$ with $\gcd(h + im, p) = 1$, there exists a G -Galois cover branched only at ∞ with the same inertia group and upper jump $\sigma' = \sigma + i$.

5.3 Realizing almost all upper jumps for A_{p+s} -Galois covers

Here are the necessary conditions on the upper jump of an A_{p+s} -Galois cover of the affine line.

Notation 5.5. Let $2 \leq s < p$. Suppose $\phi : Y \rightarrow \mathbb{P}_k^1$ is an A_{p+s} -Galois cover branched only at ∞ where it has upper jump $\sigma = h'/m''$ written in lowest terms. Then σ satisfies these necessary conditions: $\sigma > 1$; $p \nmid h'$; and $m''|(p-1)$.

Corollary 5.6. Suppose $2 \leq s < p$ and $\gcd(p-1, s+1) = 1$. Then all but finitely many rational numbers σ satisfying the necessary conditions of Notation 5.5 occur as the upper jump of an A_{p+s} -Galois cover of \mathbb{P}_k^1 branched only at ∞ .

Proof. Theorem 4.9 implies that there exists an A_{p+s} -Galois cover of \mathbb{P}_k^1 branched only at ∞ with upper jump $\sigma_s = (p+s)/(p-1)$. The condition on s implies that σ is written in lowest terms and thus $m'' = p-1$. The corollary then follows from Lemma 5.3 and Theorem 5.4. \square

5.4 Realizing lower jumps for A_n -Galois covers with inertia $\mathbb{Z}/(p)$

Question 5.7. Suppose G is a quasi- p group whose order is strictly divisible by p . For which prime-to- p integers h does there exist a G -Galois cover

$\pi : X \rightarrow \mathbb{P}_k^1$ branched only at ∞ with inertia group $\mathbb{Z}/(p)$ and lower jump h

By Theorem 5.4, all sufficiently large prime-to- p integers h occur as the lower jump of a G -Galois cover of the affine line with inertia $\mathbb{Z}/(p)$. The question is thus how large h needs to be to guarantee that it occurs as the lower jump of such a cover. In [5, Thm. 3.1.4], the authors prove that every prime-to- p integer $h \geq p - 2$ occurs as the lower jump of an A_p -Galois cover of the affine line with inertia group $\mathbb{Z}/(p)$. The next corollary improves on that result.

Corollary 5.8. *Let $p \geq 5$. Let $h_0 = (p + 1)/\gcd(p + 1, 4)$. There exists an A_p -Galois cover of \mathbb{P}_k^1 branched only at ∞ with inertia group $\mathbb{Z}/(p)$ and lower jump h for every prime-to- p integer $h \geq h_0$.*

Proof. It suffices to prove that there exists an A_p -Galois cover of the affine line with inertia group $\mathbb{Z}/(p)$ and lower jump h_0 ; once this small value is realized for the lower jump of such a cover, then all larger prime-to- p integers occur as the lower jump of such a cover by Theorem 5.4. Note that the upper and lower jumps are equal when the inertia group has order p .

Let $t = (p - 1)/2$. Then $\gcd(p - 1, t(t - 1))$ equals $(p - 1)/2$ if $p \equiv 1 \pmod{4}$ and equals $p - 1$ if $p \equiv 3 \pmod{4}$. Consider the A_p -Galois cover $\pi_t : X_t \rightarrow \mathbb{P}_k^1$ in Theorem 4.6 which is branched only at ∞ . If $p \equiv 3 \pmod{4}$, then π_t has inertia group of order p and upper jump $(p + 1)/4$. When $p \equiv 1 \pmod{4}$, then π_t has inertia group of order $2p$ and upper jump $(p + 1)/4$. In the latter case, taking $d = 2$ in Lemma 5.3 yields an A_p -Galois cover of the affine line with inertia group of order p and upper jump $(p + 1)/2$. \square

We now provide a partial answer to Question 5.7 for all other alternating groups whose order is strictly divisible by p .

Corollary 5.9. *Let $2 \leq s < p$. If $p = 7$, assume $s \neq 2$. Let $h_s = s(p + s)/\gcd(p - 1, s(s + 1))$. There exists an A_{p+s} -Galois cover of \mathbb{P}_k^1 branched only at ∞ with inertia group $\mathbb{Z}/(p)$ and lower jump h for every prime-to- p integer $h \geq h_s$.*

Proof. By Theorem 4.9, there exists an A_{p+s} -Galois cover $\phi_s : Y_s \rightarrow \mathbb{P}_k^1$ branched only at ∞ with inertia group G_0 of order pm_s and upper jump $\sigma_s = (p + s)/(p - 1)$ where $m_s = (p - 1)s/\gcd(p - 1, s(s + 1))$. Applying Lemma 4.1 with $r_2 = m_s$ produces an A_{p+s} -Galois cover of the affine line with inertia group $\mathbb{Z}/(p)$ and lower jump h_s . This completes the proof by Theorem 5.4. \square

Corollary 5.10. *Let $p \neq 7$ be an odd prime. Let $h_1 = 2(p+2)/\gcd(p-1, 3)$. There exists an A_{p+1} -Galois cover of \mathbb{P}_k^1 branched only at ∞ with inertia group $\mathbb{Z}/(p)$ and lower jump h for every prime-to- p integer $h \geq h_1$.*

Proof. By Theorem 4.9, letting $s = 2$, there exists an A_{p+2} -Galois cover $\phi_2 : Y_2 \rightarrow \mathbb{P}_k^1$ branched only at ∞ with inertia group G_0 of order pm_2 and upper jump $\sigma_2 = (p+2)/(p-1)$ where $m_2 = (p-1)/\gcd(p-1, 3)$. The lower jump h of ϕ_2 equals $(p+2)/\gcd(p-1, 3)$.

Consider the A_{p+1} -Galois subcover $\tilde{\phi} : Y_2 \rightarrow Z'_2$ of ϕ_2 . It is branched above $P_{(\infty, 0)}$ where it has ramification index m_2 and above $P_{(\infty, \infty)}$ where it has ramification index $pm_2/2$. The lower jump of $\tilde{\phi}$ above $P_{(\infty, \infty)}$ equals the lower jump h of ϕ_2 . The upper jump of $\tilde{\phi}$ is thus $\tilde{\sigma} = 2(p+2)/(p-1)$. Applying the Riemann-Hurwitz formula to ϕ_2 and $\tilde{\phi}$, we note that Z'_2 has genus 0. Another way to see this is that the equation g_2 yields that $x = (y^{p+s} + 1)/y_s$ and so the function field of Z'_2 is $L_2 \simeq k(y)$.

Thus $\tilde{\phi}$ is an A_{p+1} -Galois cover of the projective line branched at two points. Note that $\tilde{\phi}$ is disjoint from an m_2 -cyclic cover of the projective line branched at $\{0, \infty\}$. Applying Lemma 4.1 with $r_2 = m_2$ removes the tamely ramified branch point. In particular, it yields a Galois cover $\tilde{\phi}' : Y'_2 \rightarrow \mathbb{P}_k^1$ branched only at ∞ , with ramification index p . The upper (and lower) jump of $\tilde{\phi}'$ is $\sigma' = m_2 \tilde{\sigma}$ which equals $2(p+2)/\gcd(p-1, 3)$. This completes the proof by Theorem 5.4. \square

5.5 Realizing small upper jumps for A_p -Galois covers

The upper jump $\sigma = h/m$ of an A_p -Galois cover of the affine line satisfies the necessary conditions $\sigma > 1$, $\gcd(h, m) = 1$, $m \mid (p-1)/2$, and $p \nmid h$. As a generalization of Question 5.7, we can ask which σ satisfying the necessary conditions occur as the upper jump of an A_p -Galois cover of the affine line.

In [5, Thm. 2], the authors prove that all but finitely many σ which satisfy the necessary conditions occur as the upper jump of an A_p -Galois cover of the affine line. That result generalizes both Corollary 5.8 (where $m = 1$) and Corollary 5.1 (which can be rephrased as stating that all divisors of $(p-1)/2$ occur as the denominator of σ for such a cover). Specifically, given a divisor m of $(p-1)/2$ and a congruence value of h modulo m , [5, Thm. 3.1.4] provides a lower bound on h above which all $\sigma = h/m$ (satisfying the necessary conditions) are guaranteed to occur. The bound is $a(p-2)$ where a is such that $1 \leq a \leq m$ and $a \equiv -h \pmod{m}$.

p	σ obtained from [5, Thm. 3.1.4]	σ unknown from [5]	Theorem 4.6
5	3, 4, 6, ... 3/2, 7/2, 9/2, ...	2 None	None
7	5, 6, 8, ... 5/3, 8/3, 10/3, ...	2, 3, 4 4/3	2, 3, 4
11	9, 10, 12, ... 9/5, 14/5, 19/5, ...	2, 3, 4, 5, 6, 7, 8 6/5, 7/5, 8/5, 12/5	3, 4, 5, 6, 7, 8 12/5
13	11, 12, 14, 15, ... 11/2, 15/2, 17/2, ... 11/3, 14/3, 17/3, ... 11/6, 17/6, 23/6, ...	2, 3, ..., 10 3/2, 5/2, 7/2, 9/2 4/3, 5/3, 7/3, 8/3, 10/3 7/6	3, 4, 5, 6, 7, 8, 9, 10 5/2, 7/2, 9/2 10/3

Theorem 4.6 improves on [5, Thm. 3.1.4] by providing some new values of σ which were not previously known to occur as the upper jump of an A_p -Galois cover of the affine line. Corollary 5.8 is an example of that improvement; here are two more examples.

Example 5.11. Small primes: The first column of the table shows the values of σ that are achieved in [5, Thm. 3.1.4]. The second column contains rational numbers satisfying the necessary conditions whose status was not known from [5]. The final column contains new values of σ which are guaranteed to occur in Theorem 4.6.

Example 5.12. Suppose $p \equiv 1 \pmod{3}$ and $m = (p-1)/6$ and $h \equiv -1 \pmod{m}$. Then the lower bound on h to guarantee that h/m occurs as the upper jump of an A_p -Galois cover of the affine line from [5, Thm. 3.1.4] is $p-2$ and from Theorem 4.6 is $(p-3)/2$. Suppose $p \equiv 2 \pmod{3}$ and $m = (p-1)/2$ and $h \equiv -3 \pmod{m}$. Then the lower bound on h to guarantee that h/m occurs as the upper jump of an A_p -Galois cover of the affine line from [5, Thm. 3.1.4] is $3(p-2)$ and from Theorem 4.6 is $3(p-3)/2$.

Proof. The previous lower bounds are a direct application of [5, Thm. 3.1.4]. For the new lower bounds, when $t = 3$, then Theorem 4.6 states that $\sigma_3 = 3(p-3)/(p-1)$ occurs as an upper jump of an A_p -Galois cover of the affine line. If $p \equiv 1 \pmod{3}$, then $m = (p-1)/6$ and $h = (p-3)/2$; (note that $h \equiv -1 \pmod{m}$). If $p \equiv 2 \pmod{3}$, then $m = (p-1)/2$ and $h = 3(p-3)/2$; (note that $h \equiv -3 \pmod{m}$). \square

References

- [1] Shreeram Abhyankar. Coverings of algebraic curves. *Amer. J. Math.*, 79:825–856, 1957.
- [2] Shreeram S. Abhyankar. Galois theory on the line in nonzero characteristic. *Bull. Amer. Math. Soc. (N.S.)*, 27(1):68–133, 1992.
- [3] Shreeram S. Abhyankar. Resolution of singularities and modular Galois theory. *Bull. Amer. Math. Soc. (N.S.)*, 38(2):131–169 (electronic), 2001.
- [4] Irene I. Bouw. Covers of the affine line in positive characteristic with prescribed ramification. Accepted for publication to Fields Communications Volume WIN - Women In Numbers (Proceedings of the WIN Workshop, Banff International Research Station, Banff Canada), editors A. Cojocaru, K. Lauter, R. Pries, R. Scheidler.
- [5] Irene I. Bouw and Rachel J. Pries. Rigidity, reduction, and ramification. *Math. Ann.*, 326(4):803–824, 2003.
- [6] David Harbater. Formal patching and adding branch points. *Amer. J. Math.*, 115(3):487–508, 1993.
- [7] David Harbater. Abhyankar’s conjecture on Galois groups over curves. *Invent. Math.*, 117(1):1–25, 1994.
- [8] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
- [9] Rachel J. Pries. Conductors of wildly ramified covers. II. *C. R. Math. Acad. Sci. Paris*, 335(5):485–487, 2002.
- [10] M. Raynaud. Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d’Abhyankar. *Invent. Math.*, 116(1-3):425–462, 1994.
- [11] John Scherk. The ramification polygon for curves over a finite field. *Canad. Math. Bull.*, 46(1):149–156, 2003.

- [12] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.
- [13] Henning Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.