Fields Institute Communications
Volume **00**, 0000

Semi-direct Galois covers of the affine line

Linda Gruendken
Department of Mathematics, University of Pennsylvania, David Rittenhouse Lab, 209 South 33rd Street, Philadelphia, PA 19104-6395
lindagr@math.upenn.edu

Laura Hall-Seelig
Department of Mathematics and Statistics, Lederle Graduate Research Tower, University of Massachusetts, Amherst, MA 01003-9305
hall@math.umass.edu

Bo-Hae Im
Department of Mathematics, Chung-Ang University, 221, Heukseok-dong, Dongjak-gu, Seoul 156-756 South Korea
imbh@cau.ac.kr

Ekin Ozman
Department of Mathematics, University of Wisconsin-Madison, 480 Lincoln Drive, Madison, WI 53706
ozman@math.wisc.edu

Rachel Pries
Department of Mathematics, Colorado State University, Fort Collins, CO 80523-1874, USA
pries@math.colostate.edu

Katherine Stevenson
Department of Mathematics, California State University, 18111 Nordhoff St, Northridge, CA 91330-8313
katherine.stevenson@csun.edu

Abstract. Let k be an algebraically closed field of characteristic $p > 0$. Let G be a semi-direct product of the form $(\mathbb{Z}/\ell\mathbb{Z})^b \rtimes \mathbb{Z}/p\mathbb{Z}$ where b is a positive integer and ℓ is a prime distinct from p. In this paper, we study Galois covers $\psi : Z \to \mathbb{P}^1_k$ ramified only over ∞ with Galois group G. We find the minimal genus of a curve Z which admits a covering map of this form and we give an explicit formula for this genus in terms of ℓ and p. The minimal genus occurs when b equals the order a of ℓ modulo b and we also prove that the number of curves Z of this minimal genus which admit such a covering map is at most $(p-1)/a$ when p is odd.

1991 *Mathematics Subject Classification.* 14H30, 14E20, 14F40.

This project was initiated at the workshop WIN Women in Numbers in November 2008. The authors would like to thank the Banff International Research Station for hosting the workshop and the National Security Agency, the Fields Institute, the Pacific Institute for the Mathematical Sciences, Microsoft Research, and University of Calgary for their financial support. Author Pries was partially supported by NSF grant 07-01303. Author Im was partially supported by the Korea Science and Engineering Foundation (KOSEF) grant (No. R01-2007-000-10660-0) funded by the Korea government (MOST). The authors would also like to thank the referee for helpful comments.

1 Introduction

Let k be an algebraically closed field of characteristic $p > 0$. In sharp contrast with the situation in characteristic 0, there exist Galois covers $\psi : Z \to \mathbb{P}^1_k$ ramified only over infinity. By Abhyankar's Conjecture [2], proved by Raynaud and Harbater [9], [4], a finite group G occurs as the Galois group of such a cover ψ if and only if G is quasi-p, i.e., G is generated by p-groups. This result classifies all the finite quotients of the fundamental group $\pi_1(\mathbb{A}^1_k)$. It does not, however, determine the profinite group structure of $\pi_1(\mathbb{A}^1_k)$ because this fundamental group is an infinitely generated profinite group.

There are many open questions about Galois covers $\psi : Z \to \mathbb{P}^1_k$ ramified only over infinity. For example, given a finite quasi-p group G, what is the smallest integer g for which there exists a cover $\psi : Z \to \mathbb{P}^1_k$ ramified only over infinity with Z of genus g? As another example, suppose G and H are two finite quasi-p groups such that H is a quotient of G. Given an unramified Galois cover ϕ of $\mathbb{A}^1_k$ with group H, under what situations can one dominate ϕ with an unramified Galois cover ψ of $\mathbb{A}^1_k$ with Galois group G? Answering these questions will give progress towards understanding how the finite quotients of $\pi_1(\mathbb{A}^1_k)$ fit together in an inverse system. These questions are more tractible for quasi-p groups that are p-groups since the maximal pro-p quotient $\pi_1^p(\mathbb{A}^1_k)$ is free (of infinite rank) [10].

In this paper, we study Galois covers $\psi : Z \to \mathbb{P}^1_k$ ramified only over ∞ whose Galois group is a semi-direct product of the form $(\mathbb{Z}/\ell\mathbb{Z})^b \rtimes \mathbb{Z}/p\mathbb{Z}$, where ℓ is a prime distinct from p. Such a cover ψ must be a composition $\psi = \phi \circ \omega$ where $\omega : Z \to Y$ is unramified and $\phi : Y \to \mathbb{P}^1_k$ is an Artin-Schreier cover ramified only over ∞. The cover ϕ has an affine equation $y^p - y = f(x)$ for some $f(x) \in k[x]$ with degree s prime-to-p. The ℓ-torsion $\mathrm{Jac}\,(Y)[\ell]$ of the Jacobian of Y is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^{2g_Y}$. When $f(x) = x^s$, we determine how an automorphism τ of Y of order p acts on $\mathrm{Jac}\,(Y)[\ell]$. This allows us to construct a Galois cover $\psi_a : Z_a \to \mathbb{P}^1_k$ ramified only over ∞ which dominates ϕ, such that the Galois group of ψ_a is $(\mathbb{Z}/\ell\mathbb{Z})^a \rtimes \mathbb{Z}/p\mathbb{Z}$ where a is the order of ℓ modulo p (Section 3). We prove that the genus of Z_a is minimal among all natural numbers that occur as the genus of a curve Z which admits a covering map $\psi : Z \to \mathbb{P}^1_k$ ramified only over ∞ with Galois group of the form $(\mathbb{Z}/\ell\mathbb{Z})^b \rtimes \mathbb{Z}/p\mathbb{Z}$. We also prove that the number of curves Z of this minimal genus which admit such a covering map is at most $(p-1)/a$ when p is odd (Section 4).

2 Quasi-p semi-direct products

We recall which groups occur as Galois groups of covers of $\mathbb{P}^1_k$ ramified only over ∞.

Definition 2.1 *A finite group is a quasi p-group if it is generated by all of its Sylow p-subgroups.*

It is well-known that there are other equivalent formulations of the quasi-p property, such as the next result.

Lemma 2.2 *A finite group is a quasi p-group if and only if it has no nontrivial quotient group whose order is relatively prime to p.*

The importance of the quasi-p property is that it characterizes which finite groups occur as Galois groups of unramified covers of the affine line.

Theorem 2.3 *A finite group occurs as the Galois group of a Galois cover of the projective line $\mathbb{P}^1_k$ ramified only over infinity if and only if it is a quasi-p group.*

Proof This is a special case of Abhyankar's Conjecture [2] which was jointly proved by Harbater [4] and Raynaud [9]. □

We now restrict our attention to groups G that are semi-direct products of the form $(\mathbb{Z}/\ell\mathbb{Z})^b \rtimes \mathbb{Z}/p\mathbb{Z}$. The semi-direct product action is determined by a homomorphism $\iota : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}\,((\mathbb{Z}/\ell\mathbb{Z})^b)$.

Lemma 2.4 *Suppose a quasi-p group G is a semi-direct product of the form $(\mathbb{Z}/\ell\mathbb{Z})^b \rtimes \mathbb{Z}/p\mathbb{Z}$ for a positive integer b.*

1. *Then G is not a direct product.*
2. *Moreover, $b \geq \mathrm{ord}_p(\ell)$ where $\mathrm{ord}_p(\ell)$ is the order of ℓ modulo p.*

Proof Part (1) is true since $(\mathbb{Z}/\ell\mathbb{Z})^b$ cannot be a quotient of the quasi-p group G. For part (2), the structure of a semi-direct product $(\mathbb{Z}/\ell\mathbb{Z})^b \rtimes \mathbb{Z}/p\mathbb{Z}$ depends on a homomorphism $\iota : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}\,(\mathbb{Z}/\ell\mathbb{Z})^b$. By part (1), ι is an inclusion. Thus $\mathrm{Aut}\,(\mathbb{Z}/\ell\mathbb{Z})^b \simeq \mathrm{GL}_b(\mathbb{Z}/\ell\mathbb{Z})$ has an element of order p. Now

$$|\mathrm{GL}_b(\mathbb{Z}/\ell\mathbb{Z})| = (\ell^b - 1)(\ell^b - \ell)\cdots(\ell^b - \ell^{b-1}).$$

Thus $\ell^\beta \equiv 1 \bmod p$ for some positive integer $\beta \leq b$ which implies $b \geq \mathrm{ord}_p(\ell)$. □

Lemma 2.5 *If $a = \mathrm{ord}_p(\ell)$, then there exists a semi-direct product of the form $(\mathbb{Z}/\ell\mathbb{Z})^a \rtimes \mathbb{Z}/p\mathbb{Z}$ which is quasi-p. It is unique up to isomorphism.*

Proof If $a = \mathrm{ord}_p(\ell)$, then there is an element of order p in $\mathrm{Aut}\,((\mathbb{Z}/\ell\mathbb{Z})^a)$ and so there is an injective homomorphism $\iota : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}\,((\mathbb{Z}/\ell\mathbb{Z})^a)$. Thus there exists a non-abelian semi-direct product G of the form $(\mathbb{Z}/\ell\mathbb{Z})^a \rtimes \mathbb{Z}/p\mathbb{Z}$. To show that G is quasi-p, suppose N is a normal subgroup of G whose index is relatively prime to p. Then N contains an element τ of order p. By [3, 5.4, Thm. 9], since G is not a direct product and $(\mathbb{Z}/\ell\mathbb{Z})^a$ is normal in G, the subgroup $\langle\tau\rangle$ is not normal in G. Thus $\langle\tau\rangle$ is a proper subgroup of N. It follows that ℓ divides $|N|$ and so N contains an element h of order ℓ by Cauchy's theorem. Recall that $\mathrm{Aut}\,((\mathbb{Z}/\ell\mathbb{Z})^\beta)$ contains no element of order p for any positive integer $\beta < a$. Thus the group generated by the conjugates of h under τ has order divisible by ℓ^a. Thus $N = G$ and G has no non-trivial quotient group whose order is relatively prime to p. By Lemma 2.2, G is quasi-p.

The uniqueness follows from [8, Lemma 6.6]. □

3 Explicit construction of $(\mathbb{Z}/\ell\mathbb{Z})^a \rtimes \mathbb{Z}/p\mathbb{Z}$-Galois covers of $\mathbb{A}^1_k$

In this section, we give concrete examples of Galois covers $\psi : Z \to \mathbb{P}^1_k$ ramified only over ∞ with Galois group of the form $(\mathbb{Z}/\ell\mathbb{Z})^a \rtimes \mathbb{Z}/p\mathbb{Z}$. To compute the genus of the covering curve Z, we will need to determine the higher ramification groups of ψ.

Definition 3.1 *Let L/K be a Galois extension of function fields of curves with Galois group G and let P, P' be primes of K and L such that $P'|P$. Let $\nu_{P'}$ and $\mathcal{O}_{P'}$ be the corresponding valuation function and valuation ring for P'. For any integer $i \geq -1$, the ith ramification group of $P'|P$ is*

$$I_i(P'|P) = \{\sigma \in G \mid \nu_{P'}(\sigma(z) - z) \geq i + 1, \forall z \in \mathcal{O}_{P'}\}.$$

Lemma 3.2 *Suppose $f(x) \in k[x]$ is a polynomial of degree s for a positive integer s prime to p. Let $\phi : Y \to \mathbb{P}^1_k$ be the cover of curves corresponding to the field extension*

$$k(x) \hookrightarrow k(x)[y]/(y^p - y - f(x)).$$

1. *Then $\phi : Y \to \mathbb{P}^1_k$ is a Galois cover with Galois group $\mathbb{Z}/p\mathbb{Z}$ ramified only at the point P_∞ over ∞.*
2. *The ith ramification group at P_∞ satisfies*
$$I_i = \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } i \le s \\ 0 & \text{if } i > s. \end{cases}$$
3. *The genus g_Y of Y is equal to*
$$g_Y = (p-1)(s-1)/2.$$

Proof For part (1), note that the extension $k(x) \hookrightarrow k(x)[y]/(y^p - y - f(x))$ is cyclic of degree p, with Galois group generated by the automorphism $\tau : y \mapsto y+1$ of order p. Let P be a finite prime of $k(x)$ and let ν_P be the corresponding valuation. Then $\nu_P(f(x)) \ge 0$, hence P is unramified by [12, Prop. III.7.8(b)]. For the infinite prime ∞ with corresponding valuation υ_∞, we have
$$\nu_\infty(f(x) - (z^p - z)) \le 0$$
for all $z \in k[x]$ thus P_∞ is totally ramified by [12, Prop. III.7.8(c)].

To prove part (2), we note that furthermore
$$\upsilon_{P_\infty}(y^p - y) = \upsilon_{P_\infty}(f(x)) = \upsilon_{P_\infty}(x^s) = -sp,$$
which implies that
$$\upsilon_{P_\infty}(y) = -s.$$
Now let $\widehat{\theta}$ be the completion of the valuation ring of $k(x)[y]/(y^p - y - f(x))$ at P_∞, and let π_∞ be a generator of the unique prime in $\widehat{\theta}$. Then write $y = \pi_\infty^{-s}u$, where u is a unit in $\widehat{\theta} \simeq k[[\pi_\infty]]$. Since k is algebraically closed, $\sqrt[s]{u} \in \widehat{\theta}$, and so $\sqrt[s]{y} \in \widehat{\theta}$. After possibly changing π_∞, we can assume without loss of generality that $\sqrt[s]{y} = \pi_\infty^{-1}$. Recalling that τ acts on y by $\tau(y) = y+1$, we have
$$\begin{aligned} \tau(\pi_\infty) &= \tau\,(1/y)^{1/s} = (\pi_\infty^s/(1+\pi_\infty^s))^{1/s} \\ &= \pi_\infty(1 - \pi_\infty^s + \pi_\infty^{2s} - + \ldots)^{\frac{1}{s}} \\ &= \pi_\infty - (1/s)\pi_\infty^{s+1} + a_{2s+1}\pi_\infty^{2s+1} - + \ldots. \end{aligned}$$
Thus $\upsilon_{P_\infty}(\tau(\pi_\infty) - \pi_\infty) = s+1$, which completes the proof of part (2).

To find the genus g_Y of Y for part (3), we make use of the Riemann-Hurwitz formula
$$2g_Y - 2 = p(-2) + \sum_{i=0}^{\infty} (|I_i| - 1)\,,$$
where I_i denotes the ith ramification group at P_∞, [5, Thms. 7.27 & 11.72]). From part (2), we then obtain that $g_Y = (p-1)(s-1)/2$. □

Recall the following facts about the pth cyclotomic polynomial $\Phi_p(t) := t^{p-1} + \cdots + 1$, which is the minimal polynomial over $\mathbb{Q}$ of a primitive pth root of unity ζ_p. Now $\mathbb{Q}(\zeta_p)$ is a Galois extension of $\mathbb{Q}$, unramified over ℓ since $\ell \ne p$, and all primes over ℓ have the same residue field degree. The irreducible factors of $\Phi_p(t)$ modulo ℓ are in one-to-one correspondence with the primes of $\mathbb{Z}[\zeta_p]$ over ℓ, and each of their degrees is equal to the residue field degree of the corresponding prime over ℓ. The latter equals the order $a = \mathrm{ord}_p(\ell)$ of ℓ modulo p [3, Ch. 12.2, Exercise #20].

We shall soon explicitly construct a cover of $\mathbb{P}^1_k$ ramified only over ∞ with Galois group $(\mathbb{Z}/\ell\mathbb{Z})^a \rtimes \mathbb{Z}/p\mathbb{Z}$. But before we do so, we start with a specific example.

Example 3.3 Let p be an odd prime. Consider the Artin-Schreier cover $\phi : Y_2 \to \mathbb{P}^1_k$ corresponding to the field extension $k(x) \hookrightarrow k(x)[y]/(y^p - y - x^2)$. By Lemma 3.2(3), the genus of Y_2 is $g_Y = (p-1)/2$.

Let $\mathrm{Jac}\,(Y)$ be the Jacobian of Y. The automorphism τ of Y given by $\tau(y) = y + 1$ defines an automorphism of $\mathrm{Jac}\,(Y)$ of order p.

Now we describe the action of τ on the subgroup $\mathrm{Jac}\,(Y)[2]$ of 2-torsion points of $\mathrm{Jac}\,(Y)$ explicitly. Note that since $2g_Y = (p-1)$, then $\mathrm{Jac}\,(Y)[2]$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{p-1}$ by [7, pg. 64]. Thus we can represent τ as an element of $\mathrm{GL}_{p-1}(\mathbb{Z}/2\mathbb{Z})$.

For $0 \le i \le p-1$, let P_i denote the closed point of Y at which the function $y - i$ vanishes. For each i, the divisors P_i and $D_i = P_i - P_\infty$ on Y can be identified with elements of $\mathrm{Jac}\,(Y)$. Let O be the identity element of $\mathrm{Jac}\,(Y)$, i.e., the linear equivalence class of principal divisors. Then the divisor $2D_i$ is equivalent to O since $\mathrm{div}(y-i) = 2D_i$. Moreover since $\mathrm{div}(x) = D_0 + D_1 + \cdots + D_{p-1}$ is equivalent to 0, we have $D_i \in \mathrm{Jac}\,(Y)[2]$ with the only relation $D_{p-1} = -(D_0 + D_1 + \cdots + D_{p-2})$. In particular, $D_0, \ldots, D_{p-2}$ form a basis of $\mathrm{Jac}\,(Y)[2]$. With respect to this basis, the action of τ can be represented by the $(p-1) \times (p-1)$-matrix

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -1 \\ 1 & 0 & \ldots & 0 & -1 \\ 0 & 1 & \ldots & 0 & -1 \\ \vdots & \vdots & \ddots & 0 & -1 \\ 0 & 0 & \ldots & 1 & -1 \end{pmatrix}.$$

The characteristic polynomial of τ is $\Phi_p(t) = 1 + t + \ldots t^{p-1} \in (\mathbb{Z}/2\mathbb{Z})[t]$, which factors into irreducible polynomials each of degree equaling the order of 2 modulo p. In particular, τ acts irreducibly on $\mathrm{Jac}\,(Y)[2]$ if and only if 2 is a primitive root modulo p, i.e., if and only if p is an Artin prime.

For example, if $p = 3$, then τ acts irreducibly on $\mathrm{Jac}\,(Y)[2]$ with minimal polynomial $\Phi_3(t) = t^2 + t + 1$. If $p = 7$, then 2 has order 3 modulo 7 and the factorization of $\Phi_7(t)$ into irreducible polynomials is $\Phi_7(t) \equiv (x^3 + x^2 + 1)(x^3 + x + 1)$ modulo 2. Thus the action of τ on $\mathrm{Jac}\,(Y)[2]$ can be represented by the 6×6-matrix

$$\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

where A_1 and A_2 are the irreducible 3-dimensional companion matrices of $x^3 + x^2 + 1$ and $x^3 + x + 1$ respectively.

For the rest of the paper, let $\phi_s : Y_s \to \mathbb{P}^1_k$ be the Artin-Schreier cover corresponding to the field extension

$$k(x) \hookrightarrow k(x)[y]/(y^p - y - x^s).$$

We show that ϕ_s can be dominated by a Galois cover of $\mathbb{P}^1_k$ with Galois group of the form $(\mathbb{Z}/\ell\mathbb{Z})^a \rtimes \mathbb{Z}/p\mathbb{Z}$ for a equal to the order of ℓ modulo p.

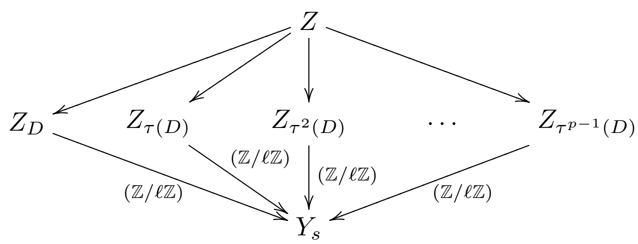
Proposition 3.4 *Let s and ℓ be primes distinct from p. Let $\phi_s : Y_s \to \mathbb{P}^1_k$ be the Artin-Schreier cover with affine equation $y^p - y = x^s$. Let $a = \mathrm{ord}_p(\ell)$ be the order of ℓ modulo p. Then there exists an unramified Galois cover $\omega : Z_a \to Y_s$ with Galois group $(\mathbb{Z}/\ell\mathbb{Z})^a$ such that $\psi_a = \phi_s \circ \omega : Z_a \to \mathbb{P}^1_k$ is a Galois cover of $\mathbb{P}^1_k$ ramified only over ∞ whose Galois group is a semi-direct product of the form $(\mathbb{Z}/\ell\mathbb{Z})^a \rtimes \mathbb{Z}/p\mathbb{Z}$.*

Proof By Lemma 3.2(1), $\phi_s : Y_s \to \mathbb{P}^1_k$ is a Galois cover with Galois group $\mathbb{Z}/p\mathbb{Z}$ ramified only at the point P_∞ over ∞. The genus g_s of Y_s is $(p-1)(s-1)/2$. Consider two commuting automorphisms of Y_s defined by

$$\tau : \begin{cases} x \mapsto x, \\ y \mapsto y+1, \end{cases} \qquad \sigma : \begin{cases} x \mapsto \zeta_s x, & \text{where } \zeta_s \text{ is a primitive } s\text{th root of unity,} \\ y \mapsto y. \end{cases}$$

Let $\mathrm{Jac}\,(Y_s)$ be the Jacobian of Y_s. Then τ and σ define commuting automorphisms of $\mathrm{Jac}\,(Y_s)$ of orders p and s respectively. Therefore, $\mathrm{End}\,(\mathrm{Jac}\,(Y_s))$ contains a ring isomorphic to $\mathbb{Z}[\zeta_p, \zeta_s] \cong \mathbb{Z}[\zeta_{ps}]$, which is a $\mathbb{Z}$-module of rank $\phi(ps) = (p-1)(s-1) = 2g_s$. Then $\mathbb{Q}(\zeta_{ps})$ is contained in $\mathrm{End}\,(\mathrm{Jac}\,(Y_s)) \otimes \mathbb{Q}$. In other words, $\mathrm{Jac}\,(Y_s)$ has complex multiplication by $\mathbb{Q}(\zeta_{ps})$.

For a prime ℓ distinct from p, the automorphism τ induces an action on the subgroup $\mathrm{Jac}\,(Y_s)[\ell]$ of ℓ-torsion points of $\mathrm{Jac}\,(Y_s)$. Recall that there is a bijection between ℓ-torsion points D of $\mathrm{Jac}\,(Y_s)$ and unramified $(\mathbb{Z}/\ell\mathbb{Z})$-Galois covers $\omega_D : Z_D \to Y_s$ [6, Prop. 4.11]. Also D has order ℓ if and only if Z_D is connected. This induces a bijection between orbits of τ on the set of unramified $(\mathbb{Z}/\ell\mathbb{Z})$-Galois covers $\omega_D : Z_D \to Y_s$ and on the set of ℓ-torsion points of $\mathrm{Jac}\,(Y_s)$. For a point D of order ℓ of $\mathrm{Jac}\,(Y_s)$, consider the compositum $\omega : Z \to Y_s$ of all of the conjugates $\omega_{\tau^j(D)} : Z_{\tau^i(D)} \to Y_s$ for $0 \le j \le p-1$:



Then Z is invariant under τ and so $\phi_s \circ \omega : Z \to \mathbb{P}^1_k$ is Galois. Moreover, $\phi_s \circ \omega$ is the Galois closure of $\phi_s \circ \omega_D : Z_D \to \mathbb{P}^1_k$.

Suppose there is a non-trivial one-dimensional τ-invariant subspace of $\mathrm{Jac}\,(Y_s)[\ell]$ with eigenvalue 1; i.e. τ acts trivially on this subgroup of order ℓ. This yields a cover $\psi_s \circ \omega_1 : Z_1 \to Y_s \to \mathbb{P}^1_k$. Since the action of τ is trivial, $\psi_s \circ \omega_1$ is Galois, ramified only over ∞, with abelian Galois group $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. This contradicts Lemma 2.4.

Since τ has order p, the minimal polynomial $m_\tau(t)$ of τ divides $t^p - 1 = (t-1)(t^{p-1} + \cdots + 1)$ in $(\mathbb{Z}/\ell\mathbb{Z})[t]$. From the preceding paragraph, there is no non-trivial one-dimensional τ-invariant subspace of $\mathrm{Jac}\,(Y_s)[\ell]$ with eigenvalue 1. This implies that $m_\tau(t)$ divides the pth cyclotomic polynomial $\Phi_p(t) = t^{p-1} + \cdots + 1$ in $(\mathbb{Z}/\ell\mathbb{Z})[t]$. The irreducible factors of $\Phi_p(t)$ in $(\mathbb{Z}/\ell\mathbb{Z})[t]$ all have degree a. Thus the degree of $m_\tau(t)$ equals a.

Since $2g_s = (p-1)(s-1)$, we have $\mathrm{Jac}\,(Y_s)[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^{(p-1)(s-1)}$, so we can represent τ as an element of $\mathrm{GL}_{(p-1)(s-1)}(\mathbb{Z}/\ell\mathbb{Z})$. We can choose a basis of $\mathrm{Jac}\,(Y_s)[\ell]$ such that τ is represented as an element of $\mathrm{GL}_{(p-1)(s-1)}(\mathbb{Z}/\ell\mathbb{Z})$ in block form. The first irreducible subrepresentation of τ has dimension a. Moreover, since $\mathbb{Q}(\zeta_{ps})$ is a Galois extension of $\mathbb{Q}$, the block form of τ consists entirely of irreducible blocks of the same size. In particular, the number of irreducible blocks is $(p-1)(s-1)/a$. In other words, τ can be represented by an element of $\mathrm{GL}_{(s-1)(p-1)}(\mathbb{Z}/\ell\mathbb{Z})$ of the form

$$\begin{pmatrix} A_1 & & 0 \\ & A_2 & \\ & \ddots & \\ 0 & & A_{(p-1)(s-1)/a} \end{pmatrix},$$

where A_i is an $a \times a$ matrix representing an a-dimensional irreducible subrepresentation of τ on $\mathrm{Jac}\,(Y_s)[\ell]$.

Using the bijection between orbits of $\mathrm{Jac}\,(Y_s)[\ell]$ and orbits of $(\mathbb{Z}/\ell\mathbb{Z})$-covers of Y_s under τ and the above observation for the action of τ on $\mathrm{Jac}\,(Y_s)[\ell]$, there exists an unramified $(\mathbb{Z}/\ell\mathbb{Z})^a$-Galois cover $\omega : Z_a \to Y_s$ such that $\psi_a = \phi_s \circ \omega : Z_a \to \mathbb{P}^1_k$ is a Galois cover of $\mathbb{P}^1_k$ with Galois group of the form $(\mathbb{Z}/\ell\mathbb{Z})^a \rtimes \mathbb{Z}/p\mathbb{Z}$. Also ψ_a is ramified only over infinity since ϕ_s is ramified only over ∞ and since ω is unramified. □

4 Minimal genus of $(\mathbb{Z}/\ell\mathbb{Z})^b \rtimes \mathbb{Z}/p\mathbb{Z}$-Galois covers of $\mathbb{A}^1_k$

In this section, we find the minimal genus of a curve Z that admits a covering map $\psi : Z \to \mathbb{P}^1_k$ ramified only over ∞, with Galois group of the form $(\mathbb{Z}/\ell\mathbb{Z})^b \rtimes \mathbb{Z}/p\mathbb{Z}$. The minimal genus depends only on ℓ and p. We consider the cases p odd and $p = 2$ separately. We also prove that the number of curves Z of this minimal genus which admit such a covering map is at most $(p-1)/a$ when p is odd and at most $\ell + 1$ when $p = 2$. The following lemma will be useful.

Lemma 4.1 *Let G be a semi-direct product of the form $(\mathbb{Z}/\ell\mathbb{Z})^b \rtimes \mathbb{Z}/p\mathbb{Z}$ where ℓ is a prime distinct from p. If $\psi : Z \to \mathbb{P}^1_k$ is a Galois cover ramified only over ∞ with Galois group G, then the subcover $\omega : Z \to Y$ with Galois group $(\mathbb{Z}/\ell\mathbb{Z})^b$ is unramified.*

Proof The quotient of G by the normal subgroup $N = (\mathbb{Z}/\ell\mathbb{Z})^b$ is $\mathbb{Z}/p\mathbb{Z}$. Thus the cover ψ is a composition $\psi = \phi \circ \omega$ where $\phi : Y \to \mathbb{P}^1_k$ has Galois group $\mathbb{Z}/p\mathbb{Z}$ and is totally ramified at the unique point P_∞ over ∞ and where $\omega : Z \to Y$ has Galois group N and is branched only over P_∞. Then ω is a prime-to-p abelian cover of Y. Let g be the genus of Y. Then by [1, XIII, Cor. 2.12], the prime-to-p fundamental group of $Y - \{P_\infty\}$ is isomorphic to the prime-to-p quotient Γ of the free group on generators $\{a_1, b_1, \ldots, a_g, b_g, c\}$ subject to the relation $\prod_{i=1}^{g}[a_i, b_i] = c^{-1}$. The cover ω corresponds to a surjection of Γ onto N where c maps to the canonical generator of inertia γ of a point of Z over P_∞. Thus N is generated by elements $\{\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g, \gamma\}$ subject to the relation $\prod_{i=1}^{g}[\alpha_i, \beta_i] = \gamma^{-1}$. Then $\gamma = 1$ since N is abelian and so ω is unramified. □

Theorem 4.2 *Let p be an odd prime. Let ℓ be a prime distinct from p and let a be the order of ℓ modulo p. Then:*

1. *There exists a Galois cover $\psi_a : Z_a \to \mathbb{P}^1_k$ ramified only over ∞ whose Galois group is a semi-direct product of the form $(\mathbb{Z}/\ell\mathbb{Z})^a \rtimes \mathbb{Z}/p\mathbb{Z}$ such that $g_{Z_a} = 1 + \ell^a(p-3)/2$.*
2. *The integer g_{Z_a} is the minimal genus of a curve Z which admits a covering map $\psi : Z \to \mathbb{P}^1_k$ ramified only over ∞ with Galois group of the form $(\mathbb{Z}/\ell\mathbb{Z})^b \rtimes \mathbb{Z}/p\mathbb{Z}$ for any positive integer b.*
3. *There are at most $(p-1)/a$ isomorphism classes of curves Z which admit a Galois covering map as in part (1) with minimal genus g_{Z_a}.*

Proof By the construction in Proposition 3.4, there exists a Galois cover $\psi_a : Z_a \to \mathbb{P}^1_k$ ramified only over ∞ whose Galois group is a semi-direct product of the form $(\mathbb{Z}/\ell\mathbb{Z})^a \rtimes \mathbb{Z}/p\mathbb{Z}$. We compute the genus of the curve Z_a. Recall that ψ_a is a composition $\psi = \phi_2 \circ \omega$ where $\omega : Z \to Y_2$ is an unramified $(\mathbb{Z}/\ell\mathbb{Z})^a$-Galois cover and $\phi_2 : Y_2 \to \mathbb{P}^1_k$ has Artin-Schreier equation $y^p - y = x^2$. Then Y_2 has genus $g_{Y_2} = (p-1)/2$ by Lemma 3.2(3). By the Riemann-Hurwitz formula, $2g_{Z_a} - 2 = \ell^a(2g_{Y_2} - 2) = \ell^a(p-3)$, i.e., $g_{Z_a} = 1 + \ell^a(p-3)/2$. This completes part (1).

For part (2), suppose $\psi : Z \to \mathbb{P}^1_k$ is a Galois cover ramified only over ∞ with Galois group of the form $(\mathbb{Z}/\ell\mathbb{Z})^b \rtimes \mathbb{Z}/p\mathbb{Z}$. If g is the genus of Z, we will show that $g \geq g_{Z_a}$. As described in the proof of Lemma 4.1, the cover ψ is a composition $\psi = \phi \circ \omega$ where $\phi : Y \to \mathbb{P}^1_k$ has Galois group $\mathbb{Z}/p\mathbb{Z}$ and is ramified only over ∞ and where ω is unramified with group $(\mathbb{Z}/\ell\mathbb{Z})^b$. By the Riemann-Hurwitz formula, $2g-2 = \ell^b(2g_Y - 2)$.

By Artin-Schreier theory, ϕ is given by an equation $y^p - y = f(x)$ where $f \in k[x]$ has degree s for some integer s relatively prime to p. Since the genus g_Y of Y is $(p-1)(s-1)/2$ by Lemma 3.2 (3), we should make s as small as possible. The value $s=1$ is impossible since then Y is a projective line and there do not exist Galois covers of the projective line ramified only over one point with Galois group $\mathbb{Z}/\ell\mathbb{Z}$. Thus $s=2$ yields the smallest possible value for g_Y, namely $(p-1)/2$. Recall that $b \geq a$ by Lemma 2.4. Thus $g \geq 1 + \ell^a(p-3)/2 = g_{Z_a}$.

For part (3), suppose $\psi : Z \to \mathbb{P}^1_k$ is a Galois cover ramified only over ∞ with Galois group of the form $(\mathbb{Z}/\ell\mathbb{Z})^a \rtimes \mathbb{Z}/p\mathbb{Z}$ and the genus of Z satisfies $g_Z = 1 + \ell^a(p-3)/2$. As in part (2), ψ factors as $\phi \circ \omega$ where $\omega : Z \to Y$ is an unramified $(\mathbb{Z}/\ell\mathbb{Z})^a$-Galois cover, where $\phi : Y \to \mathbb{P}^1_k$ is an Artin-Schreier cover ramified only over ∞, and where Y has genus $(p-1)/2$. By Lemma 3.2(3), Y has an affine equation $y^p - y = a_2x^2 + a_1x + a_0$ for some $a_0, a_1 \in k$ and $a_2 \in k^*$. Since p is odd and k is algebraically closed, it is possible to complete the square and write $a_2x^2 + a_1x + a_0 = x_1^2 + \epsilon$ where $x_1 = \sqrt{a_2}x + a_1/2\sqrt{a_2}$. After modifying by an automorphism of the projective line, specifically by the affine linear transformation $x \mapsto x_1$, the equation for Y can be rewritten as $y^p - y = x_1^2 + \epsilon$. Since k is algebraically closed, there exists $\delta \in k$ such that $\delta^p - \delta = \epsilon$. Let $y_1 = y - \delta$. After the change of variables $y \mapsto y_1$, the curve Y is isomorphic to the curve Y_2 with affine equation $y_1^p - y_1 = x_1^2$. Thus there is a unique possibility for the isomorphism class of the curve Y.

From the proof of Proposition 3.4, there is a bijection between τ-invariant connected unramified $(\mathbb{Z}/\ell\mathbb{Z})^a$-Galois covers of Y_2 and orbits of τ on points D of order ℓ on $\mathrm{Jac}\,(Y_2)$. The action of τ on $\mathrm{Jac}\,(Y_2)[\ell]$ decomposes into $(p-1)/a$ irreducible subrepresentations. Each of these is distinct, because the irreducible factors of $\Phi_p(t) \in (\mathbb{Z}/\ell\mathbb{Z})[t]$ are distinct. Thus there are $(p-1)/a$ choices for a τ-invariant unramified $(\mathbb{Z}/\ell\mathbb{Z})^a$-Galois cover of Y_2. Thus there are at most $(p-1)/a$ isomorphism classes of curves Z which admit a Galois covering map as in part (1) with minimal genus g_{Z_a}. □

We note that the set of curves which are unramified $(\mathbb{Z}/\ell\mathbb{Z})^a$-Galois covers of Y_2 may contain fewer than $(p-1)/a$ isomorphism classes of curves.

Theorem 4.3 *Let $p = 2$ and let ℓ be an odd prime. Then:*

1. *There exists a Galois cover $\psi : Z \to \mathbb{P}^1_k$ ramified only over ∞ with Galois group of the form $\mathbb{Z}/\ell\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.*
2. *The minimal genus of a curve Z which admits a covering map as in part (1) is $g_Z = 1$.*
3. *There are at most $\ell + 1$ isomorphism classes of curves Z which admit a Galois covering map as in part (1) with minimal genus $g_Z = 1$.*

Proof Note that the order of ℓ modulo 2 is $a = 1$. For part (1), Lemma 2.5 shows that there exists a semi-direct product of the form $\mathbb{Z}/\ell\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ which is quasi-2. The result is then immediate from Theorem 2.3.

Suppose $\psi : Z \to \mathbb{P}^1_k$ is a Galois cover ramified only over ∞ with Galois group as in part (1). As before, ψ factors as a composition $\phi \circ \omega$. where $\omega : Z \to Y$ has Galois group $\mathbb{Z}/\ell\mathbb{Z}$ and $\phi : Y \to \mathbb{P}^1_k$ is an Artin-Schreier extension with affine equation $y^2 - y = f(x)$ for some $f(x) \in k[x]$ of odd degree s. By Lemma 4.1, ω is unramified.

The minimal genus for Z will thus occur when s is as small as possible. As before, $s = 1$ is impossible, and so $s = 3$ is the smallest choice. In this case, by Lemma 3.2(3), $g_Y = 1$, i.e., Y is an elliptic curve. By the Riemann-Hurwitz formula, the minimal genus for Z is $g_Z = 1 + \ell(g_Y - 1) = 1$, which completes part (2).

For part (3), since k is algebraically closed, we can complete the cube of $f(x)$ and make the corresponding change of variables, which is a scaling and translation of x. So we can assume that Y has affine equation $y^2 - y = x^3 + a_1 x + a_0$ for some $a_0, a_1 \in k$. Then it follows from [11, Appendix A, Prop. 1.1c] that the j-invariant of Y is $j(Y) = 0$ and that the discriminant is $\Delta(Y) = (-1)^4 = 1$. Since k is algebraically closed, by [11, Appendix A, Prop. 1.2b], all elliptic curves Y with $j(Y) = 0$ are isomorphic over k. Thus there is a unique choice for Y up to isomorphism. Without loss of generality, we may assume that $Y = Y_3$ has affine equation $y^2 - y = x^3$.

From the proof of Proposition 3.4, the action of τ on $\mathrm{Jac}\,(Y_3)[\ell]$ decomposes into the direct sum of two 1-dimensional subrepresentations. In other words, the action of τ is diagonal with both eigenvalues equal to -1. The number of non-trivial τ-invariant subgroups of $\mathrm{Jac}\,(Y_3)[\ell]$ is the number of subgroups of order ℓ in $(\mathbb{Z}/\ell\mathbb{Z})^2$, which is $\ell + 1$. As in Theorem 4.2, this implies that there are at most $\ell + 1$ isomorphism classes of curves Z which admit a Galois covering map as in part (1) with minimal genus $g_Z = 1$. □

We note that the set of curves which are unramified $\mathbb{Z}/\ell\mathbb{Z}$-Galois covers of Y_3 may contain fewer than $\ell + 1$ isomorphism classes of curves.

References

[1] *Revêtements étales et groupe fondamental*. Springer-Verlag, Berlin, 1971. Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1), Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud, Lecture Notes in Mathematics, Vol. 224.

[2] Shreeram Abhyankar. Coverings of algebraic curves. *Amer. J. Math.*, 79:825–856, 1957.

[3] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[4] David Harbater. Abhyankar's conjecture on Galois groups over curves. *Invent. Math.*, 117(1):1–25, 1994.

[5] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[6] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[7] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[8] Rachel Pries and Katherine Stevenson. *A survey of Galois theory of curves in characteristic p*. WIN - Women In Numbers, Fields Communication Volume.

[9] M. Raynaud. Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar. *Invent. Math.*, 116(1-3):425–462, 1994.

[10] I. Shafarevitch. On p-extensions. *Rec. Math. [Mat. Sbornik] N.S.*, 20(62):351–363, 1947.

[11] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[12] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.