DISSERTATION

ALGEBRAIC CURVES OVER FIELDS OF PRIME CHARACTERISTIC

Submitted by

Jeremy Muskat

Department of Mathematics

In partial fulfillment of the requirements

for the degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Summer 2007

COLORADO STATE UNIVERSITY

June 21, 2007

WE HEREBY RECOMMEND THAT THE DISSERTATION PREPARED UNDER OUR SUPERVISION BY JEREMY MUSKAT ENTITLED "ALGEBRAIC CURVES OVER FIELDS OF PRIME CHARACTERISTIC" BE ACCEPTED AS FULFILLING IN PART REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY.

Committee on Graduate Work

Dr. Jeff Achter

Dr. Hari Iyer

Dr. Holger Kley

Dr. Chris Peterson

Adviser: Dr. Rachel Pries

Department Head: Dr. Simon Tavener

ABSTRACT OF DISSERTATION

ALGEBRAIC CURVES OVER FIELDS OF PRIME CHARACTERISTIC

The theory of Algebraic curves was mostly developed in the 19-th century. Chapter 2 determines the zeta function for a famous curve that was mentioned in the last entry of Gauss's journal. We find that for $p \equiv 3 \bmod 4$ the zeta function of the curve $C : x^2t^2 + y^2t^2 + x^2y^2 - t^4 = 0$ in $\mathbb{P}^2$ defined over $\mathbb{F}_p$ is

$$Z_C(u) = \frac{(1+pu^2)(1+u)^2}{(1-pu)(1-u)}.$$

Algebraic curves are covers of the projective line. Every curve has a birational invariant associated to it known as the genus. Let X be a smooth projective curve that is an A_n-Galois covering of the projective line branched only at infinity. Chapter 3 investigates what possibilities there are for the genus of X. For example let $d_2 = \gcd(p-1, p+2)$. There exists a curve X that is an A_{p+2}-Galois cover of the projective line branched only at infinity with the genus of X being

$$g = 1 + \frac{|A_{p+2}|}{2}\left(-1 - \frac{d_2}{p(p-1)} + \frac{(p+2)}{p}\right).$$

Jeremy Muskat
Department of Mathematics
Colorado State University
Fort Collins, Colorado 80523
Summer 2007

ACKNOWLEDGEMENTS

I would like to express my gratitude to my advisor, Rachel Pries, for her support, patience, and encouragement throughout my graduate studies. Rachel's guidance was invaluable. Her own work ethic and dedication to mathematics has inspired me over the past four years. Her technical and editorial advice was essential to the completion of this dissertation.

My thanks also go to the members of my committee, Jeff Achter, Holger Kley, Chris Peterson, and Hari Iyer. Special thanks go to Jeff Achter for reading previous drafts of this dissertation and providing many valuable comments that improved the presentation and contents of this dissertation.

Last, but not least, I would like to thank my family Barry, Toby, Jamie, and Josh for their continual support throughout my life. The encouragement of my parents was in the end what made this dissertation possible.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

Let p always represent an odd prime. My research involves algebraic curves viewed over fields of characteristic p. There are many questions that can be asked about algebraic curves in this setting. The first part of my dissertation deals with determining the zeta function of a specific algebraic curve. The second part of my thesis gives the possible genera of curves that are wildly ramified Galois covers of the projective line whose Galois group is a specific alternating group.

For a field k, an algebraic curve over k is the set of values $x, y \in k$ that satisfy the equation $f(x, y) = 0$. Here $f(x, y)$ is a polynomial in x and y with coefficients in k. When the field k is finite it is possible to count the number of points that lie on the curve. The number of points is related to the zeta function of the curve.

Zeta functions are generating functions that capture information about primes in rings or points on curves. The most famous zeta function is the Riemann zeta function $\zeta(s) = \sum n^{-s}$. This is the subject of the unproven Riemann hypothesis which states that the only zeros of $\zeta(s)$ lying in the strip $0 \leq \mathrm{Re}(z) \leq 1$ lie on the line $\mathrm{Re}(s) = 1/2$.

Algebraic curves over finite fields also have associated zeta functions. They catalogue the number of rational points a curve contains over finite fields of increasing prime power. The zeta function of the curve C is the series $Z_C(u) = \exp\left(\sum N_s u^s/s\right)$, where N_s is the number of points on C with coordinates in the finite field $\mathbb{F}_{p^s}$.

This information has found applications in cryptography and coding theory. For example, efficient error correcting codes have been linked to maximal curves which are curves that have as many rational points as possible over a finite field. Error correcting codes are used in satellite broadcasting, deep space telecommunications, CD players, high speed modems, and cellular phones. For this and many other reasons, determining zeta functions associated with curves over finite fields has been an important problem in number theory.

Chapter 2 was inspired by Gauss's final conjecture [9, Chapter 11]. The subject of the conjecture was the projective curve $C : x^2t^2+y^2t^2+x^2y^2-t^4 = 0$. Theorem 2.4.1 determines the zeta function of C when $p \equiv 3 \bmod 4$. My result was stated in a paper by F. Castro and C. Moreno [5] without proof. The proof was missing from their references as well.

The Weil conjectures, which became theorems by 1974, imply that the zeta function of a smooth projective variety is a rational function, it satisfies a functional equation, and that its zeroes are in restricted places [9, Chapter 11.4]. In fact Weil had proven these statements for curves in 1949. The last statement is modeled after the Riemann hypothesis. Gauss's curve C contains two nodal singularities at the points at infinity, hence the Weil conjectures do not directly apply. The method I use to determine the zeta

function of Gauss's curve is to compare it to its normalization, which is a smooth curve with complex multiplication.

Algebraic curves are covers of the projective line. If the curve is irreducible and has enough automorphisms, then the cover is Galois. Chapter 3 focuses on curves that are Galois covers of the projective line. In particular in Chapter 3, the Galois group is the alternating group A_n of even permutations on n elements. The curves in Chapter 3 have function fields that are the splitting field of a degree n equation. The Galois action on the roots of the equation is difficult to understand in this context. The reason is because it is impossible to solve for the roots of this equation by radicals. This is because A_n is a simple group when $n \geq 5$.

My interests are in Galois covers of the projective line over an algebraically closed field k of characteristic $p > 2$ with Galois group A_n.

Question 1 Let X be a smooth projective curve and $\pi : X \to \mathbb{P}^1_k$ an A_n-Galois cover of the projective line. What are the possibilities for the genus of X?

The geometric genus of a complex curve is a birational invariant defined to be the dimension of the vector space of holomorphic 1-forms on X. In other words,

$$g(X) = \dim(H^0(X, \Omega^1_X)).$$

The topological genus of a Riemann surface is the number of holes or handles on the surface. For smooth algebraic curves these definitions coincide when the algebraic curve is viewed as a complex manifold. For example, an elliptic curve is a curve of genus one. Figure 1.1 depicts how the genus of an elliptic

curve can be seen by treating the elliptic curve as a complex manifold. The definition of the geometric genus carries over to curves defined over any base field, when Ω is taken to be the sheaf of Kahler differentials [8, Chapter 8].

Figure 1.1: An elliptic curve viewed as a real curve and as a complex manifold

Hilbert's Nullstellensatz implies that understanding the algebraic extensions of function fields is equivalent to understanding the geometric cover of curves. Let F represent the function field of the smooth curve X. The inclusion map $i : k(x) \hookrightarrow F$ corresponds to a ramified covering map $\pi : X \to \mathbb{P}^1_k$.

$$\begin{array}{ccc} F & & X \\ {\scriptstyle i}\uparrow & \longleftrightarrow & {\scriptstyle \pi}\downarrow \\ k(x) & & \mathbb{P}^1_k \end{array}$$

Throughout Chapter 3 we will move between the algebraic and geometric interpretation depending on which fits the context.

Over the complex numbers, Riemann's Existence Theorem [17, Chapter 2] says that for each n, the group A_n occurs as the Galois group of an extension of $\mathbb{C}(x)$. An extension of $\mathbb{C}(x)$ corresponds to a cover of $\mathbb{P}^1_{\mathbb{C}}$. Riemann's Existence Theorem also describes all the types of ramification that can occur in the extension.

The Riemann-Hurwitz formula relates the genus of X to the genus of $\mathbb{P}^1_k$. The formula shows that the genus of X depends on the inertia groups of π

at the ramified points of X. Working over $\mathbb{C}$, the Riemann-Hurwitz formula states:

$$2g(X) - 2 = \deg(\pi)(2 \cdot 0 - 2) + \sum_{P \in X} (e(P) - 1).$$

In the formula, $g(X)$ is the genus of X and $e(P)$ is the ramification index of the point $P \in X$. Working over $\mathbb{C}$, Riemann's Existence Theorem combined with the Riemann-Hurwitz formula gives a complete answer to Question 1 when $k = \mathbb{C}$. We do not yet have an analog for Riemann's Existence Theorem in positive characteristic.

For the case when the characteristic is positive the construction of a Galois cover with Galois group A_n is complicated. In fact, it is only known how to create such covers for specific values of n. Abhyankar [2] provided equations that produce Galois covers with Galois group A_n for specific values of n.

For $n = p$ or $p + 2 \leq n < p$, Chapter 3 introduces equations corresponding to A_n-Galois covers $\pi : X \to \mathbb{P}^1_k$ branched only at ∞. For each n, the ramification over ∞ is completely described and used to determine the genus of X. For example, let $1 < t < (p-2)$ and $d_2 = \gcd(p-1, t(p-t))$. I show there exists an A_p-Galois cover $\pi : X \to \mathbb{P}^1_k$ branched only at ∞ with genus of X being

$$g = 1 + \frac{|A_p|}{2}\left(-1 - \frac{d_2}{p(p-1)} + \frac{t(p-t)}{p}\right).$$

Furthermore, let $d_2 = \gcd(p-1, p+2)$. I show there exists an A_{p+2}-Galois cover $\pi : X \to \mathbb{P}^1_k$ branched only at ∞ with the genus of X being

$$g = 1 + \frac{|A_{p+2}|}{2}\left(-1 - \frac{d_2}{p(p-1)} + \frac{(p+2)}{p}\right).$$

Also for $2 < l^c < p$ with l a prime such that $l \nmid (p-1)$. Let $d_4 = \gcd(p-1, p+l^c)$. I show there exists an A_{p+l^c}-Galois cover $\pi : X \to \mathbb{P}^1_k$ branched only at ∞ with the genus of X being

$$g = 1 + \frac{|A_{p+l^c}|}{2}\left(-1 - \frac{d_4}{p(p-1)l^c} + \frac{p+l^c}{p}\right).$$

Chapter 2

GAUSS'S CURVE

For $p \equiv 3 \bmod 4$, we give a proof that the zeta function of the curve $C : x^2t^2 + y^2t^2 + x^2y^2 - t^4 = 0$ in $\mathbb{P}^2$ defined over $\mathbb{F}_p$ is

$$Z_C(u) = \frac{(1+pu^2)(1+u)^2}{(1-pu)(1-u)}.$$

2.1 Introduction

The last entry in Gauss's mathematical diary is the following conjecture.

Conjecture 2.1.1. *Suppose $p \equiv 1$ mod 4, and $a \equiv 1$ mod $(2+2i)$ is such that $p = a^2 + b^2$. Then the number of solutions to $x^2 + y^2 + x^2y^2 = 1$ over $\mathbb{F}_p$ is $p + 1 - 2a$.*

Gauss's conjecture accounts for four points at infinity. It is interesting to note that Gauss is thinking of the curve projectively. Gauss counted the points birationally. Counting the points geometrically yields two points at infinity. Using Gauss's insight, and counting points geometrically, led to the following theorem.

Theorem 2.1.2. *[9, Chapter 11.5] Consider the curve $C : x^2t^2 + y^2t^2 + x^2y^2 - t^4 = 0$ in $\mathbb{P}^2$ defined over $\mathbb{F}_p$ where $p \equiv 1$ mod 4. Write $p = a^2 + b^2$*

with b even and with $a \equiv (-1)^{b/2} \bmod (2+2i)$. Then the number of points in $C(\mathbb{F}_p)$ is $N_1 = p - 1 - 2a$. Furthermore

$$Z_C(u) = \frac{(1 - 2au + pu^2)(1-u)}{1-pu}.$$

The focus of Chapter 2 is an analogue for Theorem 2.1.2 for the case when $p \equiv 3 \bmod 4$. We give a proof that when $p \equiv 3 \bmod 4$ the number of points in $C(\mathbb{F}_{p^s})$ is

$$N_s(C) = \begin{cases} p^s + 3 & \text{if } 2 \nmid s; \\ p^s - 2(i\sqrt{p})^s - 1 & \text{if } 2|s. \end{cases}$$

This yields the zeta function

$$Z_C(u) = \frac{(1+pu^2)(1+u)^2}{(1-pu)(1-u)}.$$

Consider a smooth projective curve X. The Weil conjectures imply that the complex absolute value of the roots of $Z_X(u)$ is $\sqrt{p}$. Notice, for $p \equiv 3 \bmod 4$ the zeta function of C has roots with complex absolute value 1. Therefore $Z_C(u)$ does not satisfy the conclusion of the Weil conjectures.

This result appears in [5], but its proof does not appear in the given reference [9]. The method we use to determine the zeta function of C is to find a correspondence between the solutions of $x^2t^2 + y^2t^2 + x^2y^2 - t^4$ and the solutions of two other equations. The solutions to these other equations can be counted using Jacobi sums and the Weil conjectures.

2.2 Near Bijections

Definition 2.2.1. *Consider a projective plane curve X defined over $\mathbb{F}_p$. The zeta function of X is the series given by*

$$Z_X(u) = \exp\Big(\sum_{s=1}^{\infty} \frac{\mathrm{N_s(X)u^s}}{\mathrm{s}}\Big) \text{ where } \mathrm{N_s(X)} \text{ denotes the size of } \mathrm{X}(\mathbb{F}_{\mathrm{p^s}}).$$

Therefore the sequence $N_s(X)$ determines the zeta function $Z_X(u)$. The converse is often true; the following explains how to reverse the process.

Fact 2.2.2. *[9, Chapter 11.1] If the zeta function of a projective plane curve X is rational, meaning $Z_X(u) = \Pi_i(1 - a_i u)\Pi_j(1 - b_j u)^{-1}$ for some $a_i, b_j \in \mathbb{C}$, then $N_s(X) = \sum_j b_j^s - \sum_i a_i^s$.*

We will use the following notation throughout Chapter 2. Let X denote the curve in $\mathbb{P}^2$ given by the zero locus of a homogeneous polynomial $F \in \mathbb{F}_p[x, y, t]$. Let X_0 represent the affine curve given by the zero locus of the polynomial $f(x, y) = F(x, y, 1)$. Let $N_s(X_0)$ denote the size of $X_0(\mathbb{F}_{p^s})$. Suppose that p is a prime and $p \equiv 3 \bmod 4$. Let $\zeta_8 = \sqrt{2}/2 + \sqrt{2}i/2$, then $\zeta_8 \in \mathbb{F}_{p^s}$ if and only if s is even.

Proposition 2.2.3. *Consider the curves $C_0 : x^2 + y^2 + x^2y^2 - 1 = 0$ and $G_0 : z^2 + w^4 - 1 = 0$ over $\mathbb{F}_p$. Then*

$$N_s(C_0) = \begin{cases} N_s(G_0) & \text{if } 2 \nmid s; \\ N_s(G_0) - 2 & \text{if } 2 | s. \end{cases}$$

Proof. Consider the map

$$\mu : G_0(\mathbb{F}_{p^s}) \to C_0(\mathbb{F}_{p^s}) \quad \text{where} \quad (w, z) \mapsto \left(w, \frac{z}{1 + w^2}\right)$$

The map μ is defined for all $(w, z) \in G_0(\mathbb{F}_{p^s})$ such that $w^2 \not\equiv -1 \bmod p$. Notice that if $x^2 + y^2 + x^2y^2 - 1 = 0$ then $((1 + x^2)y)^2 = 1 - x^4$. Define $\tilde{\mu} : C_0(\mathbb{F}_{p^s}) \to G_0(\mathbb{F}_{p^s})$ by $\tilde{\mu}(x, y) = (x, (1 + x^2)y)$. The maps μ and $\tilde{\mu}$ are inverses of each other. Therefore μ is a bijection for s odd and a bijection away from the points $(0, \pm\sqrt{-1}) \in G_0(\mathbb{F}_{p^s})$ for s even. Hence $N_s(C_0) = N_s(G_0)$ for s odd and $N_s(C_0) = N_s(G_0) - 2$ for s even. □

Proposition 2.2.4. *Consider the curve* $E_0 : y^2 - x^3 + 4x = 0$ *over* $\mathbb{F}_p$. *Then* $N_s(C_0) = N_s(E_0) - 3$ *for* s *even.*

Proof. Consider the following map defined over $\mathbb{F}_{p^s}$ for s even.

$$\alpha : E_0(\mathbb{F}_{p^s}) \to G_0(\mathbb{F}_{p^s}) \quad \text{where} \quad (x, y) \mapsto \left(\frac{\zeta_8 y}{2x}, \frac{y^2 + 8x}{4x^2}\right)$$

The map α is well defined away from $(0, 0) \in E_0(\mathbb{F}_{p^s})$ since

$$((y^2 + 8x)/4x^2)^2 - (\zeta_8 y/2x)^4 - 1 = 0.$$

Consider the following map defined over $\mathbb{F}_{p^s}$ for s even.

$$\tilde{\alpha} : G_0(\mathbb{F}_{p^s}) \to E_0(\mathbb{F}_{p^s}) \quad \text{where} \quad (w, z) \mapsto \left(\frac{2}{z + iw^2}, \frac{4\zeta_8^7 w}{z + iw^2}\right).$$

The map $\tilde{\alpha}$ is well defined for all points of $G_0(\mathbb{F}_{p^s})$ since there is no point (w, z) in $G_0(\mathbb{F}_{p^s})$ such that $z + iw^2 = 0$. Also

$$(4\zeta_8^7 w/(z + iw^2))^2 - (2/(z + iw^2))^3 + 4(2/(z + iw^2)) = 0.$$

The maps α and $\tilde{\alpha}$ are inverses. Therefore $\alpha : E_0(\mathbb{F}_{p^s}) - \{(0, 0)\} \to G_0(\mathbb{F}_{p^s})$ is a bijection and $N_s(G_0) = N_s(E_0) - 1$ for s even. Proposition 2.2.3 proves the proposition. □

2.3 Counting Points

This section will focus on counting the number of points on some of the curves found in Section 2.2.

2.3.1 Jacobi Sums

The multiplicative characters of $\mathbb{F}_{p^s}^*$ form a cyclic group of order $p^s - 1$. Let $S_{m,s}$ be the set of multiplicative characters of $\mathbb{F}_{p^s}^*$ of order m. Therefore, for each $m|(p^s - 1)$ the size of $S_{m,s}$ is $\phi(m)$. Let $\chi_{m,s}$ denote one of the multiplicative characters of order m on $\mathbb{F}_{p^s}^*$. Extend $\chi_{m,s}$ to $\mathbb{F}_{p^s}$ by defining $\chi_{m,s}(0) = 0$ for $m \neq 1$ and $\chi_{1,s}(0) = 1$. For the remainder of Chapter 2 we drop the word multiplicative and refer to $\chi_{m,s}$ as a character of $\mathbb{F}_{p^s}$.

Proposition 2.3.1. *[9, Chapter 8.2] For $a \in \mathbb{F}_{p^s}$, let $N_s(x^n = a)$ denote the number of solutions to the equation $x^n = a$ over $\mathbb{F}_{p^s}$. Then*

$$N_s(x^n = a) = \sum_{m|n} \sum_{\chi \in S_{m,s}} \chi(a)$$

where the sum is over all characters of order m dividing n.

Definition 2.3.2. *For any two characters $\chi_{m,s}$ and $\chi_{n,s}$ of $\mathbb{F}_{p^s}$, set*

$$J(\chi_{m,s}, \chi_{n,s}) = \sum_{\substack{a,b \in \mathbb{F}_{p^s} \\ a+b=1}} \chi_{m,s}(a)\chi_{n,s}(b).$$

Then we call $J(\chi_{m,s}, \chi_{n,s})$ a Jacobi sum.

Proposition 2.3.3. *[9, Chapter 8.2] $J(\chi_{1,s}, \chi_{1,s}) = p^s$, and for $m \neq 1$, $J(\chi_{m,s}, \chi_{1,s}) = 0$. For $p \equiv 3 \bmod 4$, $J(\chi_{2,s}, \chi_{2,s}) = -(\chi_{2,s}) = -(-1)^s$.*

Notice that there is only one character of order 2.

2.3.2 $G_0 : z^2 + w^4 - 1$

Lemma 2.3.4. *Let G_0 be the affine curve with equation $z^2 + w^4 - 1 = 0$. Then $N_s(G_0) = p^s + 1$ when s is odd*

Proof. For odd values of s, $p^s \equiv 3 \bmod 4$. Hence the group of characters on $\mathbb{F}_{p^s}$ does not contain a character of order 4. Proposition 2.3.1 implies that $N(x^4 = b) = N(x^2 = b)$. Therefore

$$N_s(G_0) = \sum_{\substack{a,b \in \mathbb{F}_{p^s} \\ a+b=1}} N(x^2 = a)N(x^4 = b) = \sum_{\substack{a,b \in \mathbb{F}_{p^s} \\ a+b=1}} N(x^2 = a)N(x^2 = b).$$

Using Proposition 2.3.1, 2.3.3, and Definition 2.3.2 we can simplify the above sum as follows:

$$N_s(G_0) = \sum_{\substack{a,b \in \mathbb{F}_{p^s} \\ a+b=1}} (1 + \chi_{2,s}(a))(1 + \chi_{2,s}(b)) = J(\chi_{1,s}, \chi_{1,s}) + J(\chi_{2,s}, \chi_{2,s}).$$

Thus $N_s(G_0) = p^s - (\chi_{2,s}) = p^s + 1$. □

2.3.3 $D_0 : v^2 - u^4 - 1$

Lemma 2.3.5. *Let D_0 be the affine curve with equation $v^2 - u^4 - 1 = 0$. Then $N_1(D_0) = p - 1$.*

Proof. Recall that $p \equiv 3 \bmod 4$, so the group of characters on $\mathbb{F}_p$ does not contain a character of order 4. Therefore

$$N_1(D_0) = \sum_{\substack{a,b \in \mathbb{F}_p \\ a-b=1}} N(x^2 = a)N(x^2 = b).$$

Consider the element $b' = -b$ in $\mathbb{F}_p$. Then

$$\begin{aligned} N_1(D_0) &= \sum_{\substack{a,b' \in \mathbb{F}_p \\ a+b'=1}} (1 + \chi_{2,1}(a))(1 + \chi_{2,1}(-b')) = p + \chi_{2,1}(-1)J(\chi_{2,1}, \chi_{2,1}) \\ &= p - (-\chi_{2,1}(-1)) = p - 1. \end{aligned}$$

□

2.3.4 $\mathbf{E_0 : y^2 - x^3 + 4x}$

Our goal for this section is to determine $N_s(E_0)$. We will use the Weil conjectures [9, Chapter 11.4] in combination with Jacobi sums to achieve this.

Consider the elliptic curve $E : y^2t - x^3 + 4xt^2$. The Weil conjectures imply that

$$Z_E(u) = \frac{(1 - a_p u + pu^2)}{(1-u)(1-pu)} \quad \text{where} \quad N_1(E) = p + 1 - a_p.$$

In order to completely determine $Z_E(u)$, we just need to determine $N_1(E)$. This is accomplished by demonstrating a near bijection between the points of E and the points of D_0.

Lemma 2.3.6. *Let E_0 be the affine curve with the equation $y^2 - x^3 + 4x = 0$. Then $N_s(E_0) = p^s - 2(i\sqrt{p})^s$ when s is even.*

Proof. The elliptic curve E has only one point $[0, 1, 0]$ at infinity. Therefore $N_1(E) = 1 + N_1(E_0)$.

Define

$$\gamma : D_0(\mathbb{F}_p) \to E_0(\mathbb{F}_p) \qquad \tilde{\gamma} : E_0(\mathbb{F}_p) \to D_0(\mathbb{F}_p)$$

$$(u, v) \mapsto \left(\tfrac{2}{v-u^2}, \tfrac{4u}{v-u^2}\right) \qquad (x, y) \mapsto \left(\tfrac{y}{2x}, \tfrac{y^2+8x}{4x^2}\right)$$

For similar reasons as in Proposition 2.2.4, the map γ and $\tilde{\gamma}$ are inverses of each other away from the point $(0, 0)$ of $E_0(\mathbb{F}_p)$. Therefore $N_1(E_0) = N_1(D_0) + 1$.

By Lemma 2.3.5, $N_1(D_0) = p - 1$, so $N_1(E) = p + 1$ and $a_p = 0$. It follows that

$$Z_E(u) = \frac{(1 + pu^2)}{(1-u)(1-pu)} = \frac{(1 + i\sqrt{p}u)(1 - i\sqrt{p}u)}{(1-u)(1-pu)}.$$

Fact 2.2.2 implies

$$N_s(E) = (1^s + p^s) - ((i\sqrt{p})^s + (-i\sqrt{p})^s).$$

Therefore when s is even, $N_s(E) = p^s - 2(i\sqrt{p})^s + 1$ and $N_s(E_0) = p^s - 2(i\sqrt{p})^s$. □

2.4 The Zeta Function for C

In this section we find the zeta function of Gauss's curve for the case when $p \equiv 3 \bmod 4$. Gauss's curve $C : x^2t^2 + y^2t^2 + x^2y^2 - t^4 = 0$ contains two ordinary double points at infinity. Therefore C does not satisfy the hypothesis of the Weil Conjectures. The zeta function $Z_C(u)$ has a different form than the zeta function of a smooth projective plane curve of similar degree.

Theorem 2.4.1. *Consider the curve $C : x^2t^2 + y^2t^2 + x^2y^2 - t^4$ over $\mathbb{F}_p$ where $p \equiv 3$ mod 4. Then*

$$N_s(C) = \begin{cases} p^s + 3 & \text{if } 2 \nmid s; \\ p^s - 2(i\sqrt{p})^s - 1 & \text{if } 2|s. \end{cases}$$

and

$$Z_C(u) = \frac{(1+u)^2(1+pu^2)}{(1-u)(1-pu)}.$$

Proof. Recall from Lemma 2.3.4 that $N_s(G_0) = p^s + 1$ for odd s, and from Lemma 2.3.6 that $N_s(E_0) = p^s - 2(i\sqrt{p})^s$ for even s. Putting this together with Proposition 2.2.3 and 2.2.4 we have that

$$N_s(C_0) = \begin{cases} p^s + 1 & \text{if } 2 \nmid s; \\ p^s - 2(i\sqrt{p})^s - 3 & \text{if } 2|s. \end{cases}$$

The curve $C : x^2t^2 + x^2y^2 + y^2 - t^4$ has the two points $P_1 = [1,0,0]$ and $P_2 = [0,1,0]$ at infinity. Therefore

$$N_s(C) = \begin{cases} p^s + 3 & \text{if } 2 \nmid s; \\ p^s - 2(i\sqrt{p})^s - 1 & \text{if } 2|s. \end{cases}$$

In order to calculate the zeta function, notice that N_s can be rewritten for any value of s as

$$N_s(C) = p^s + 1 - (i\sqrt{p})^s - (-i\sqrt{p})^s - 2(-1)^s.$$

Therefore

$$Z_C(u) = \exp\Big(\sum_{s=1}^{\infty} \frac{(p^s + 1 - (i\sqrt{p})^s - (-i\sqrt{p})^s - 2(-1)^s)u^s}{s}\Big).$$

Using the identity $\sum_{s=1}^{\infty} w^s s^{-1} = -\ln(1-w)$ we get the desired result

$$Z_C(u) = \frac{(1+u)^2(1+pu^2)}{(1-u)(1-pu)}.$$

□

2.5 Normalization of Singular Curves

Gauss's curve C is an example of a projective plane curve with singularities. It has two ordinary double points at $P_1 = [1,0,0]$ and $P_2 = [0,1,0]$. By [7, Chapter 17], there exists a nonsingular projective curve $\tilde{C}$ along with a normalization map $\nu : \tilde{C} \to C$. For every nonsingular point P of C, the preimage $\nu^{-1}(P)$ consists of only one point.

Another approach to determining $Z_C(u)$ is to identify $\tilde{C}$ and its zeta function $Z_{\tilde{C}}(u)$. Then $N_s(C)$ can be calculated by comparing it to $N_s(\tilde{C})$ while considering the size and field of definition of $\nu^{-1}(P_1)$ and $\nu^{-1}(P_2)$. This is essentially what we have done in Sections 2.2-2.4 with $\tilde{C} = E$ and $\nu = \mu \circ \alpha$.

Let C_{sing} represent the set of singular points of C. Let $Q|P$ denote the set of points $q \in \tilde{C}$ such that $\nu(Q) = P$. Also let $\deg(P) = \dim(\tilde{\mathcal{O}}_P/\mathcal{O}_P)$ where $\tilde{\mathcal{O}}_P$ is the integral closure of $\mathcal{O}_P$. The following proposition explains how

the zeta function of a singular curve is related to the zeta function of its normalization. It is a consequence of the Euler product representation of the zeta function [10, Chapter 8.4].

Proposition 2.5.1. *[5, Section 2] Let C be a complete irreducible algebraic projective curve with normalization $\tilde{C}$. Then*

$$\frac{Z_C(u)}{Z_{\tilde{C}}(u)} = \Pi_{P \in C_{sing}} \frac{\Pi_{Q|P}(1 - u^{\deg(Q)})}{1 - u^{\deg(P)}}.$$

When $p \equiv 3 \bmod 4$, C has two degree one singular points $P_1 = [1, 0, 0]$ and $P_2 = [0, 1, 0]$. For each of these, there is one point of degree 2 on E, hence $Z_C(u)/Z_E(u) = (1 + u)^2$.

Chapter 3

ALTERNATING GROUP COVERS WITH WILD RAMIFICATION

Every composite number can be factored into a prime number decomposition. There is a similar decomposition for curves having the same automorphism group. Curves with large genus that are Galois covers of the projective line branched over many points can be constructed from curves of smaller genus that are Galois covers of the projective line branched over fewer points. This is accomplished with the theory of formal patching. Therefore the goal in answering Question 1 is to find curves of small genus that are coverings of the projective line branched at a minimal number of points.

In order to answer Question 1 we must use a modified version of the Riemann-Hurwitz formula. The situation is more complicated because the extensions that are needed are wildly ramified. An extension is wildly ramified when there exists a ramification point whose ramification index is divisible by the characteristic of the base field. Section 3.1 introduces the theory and definitions needed for a wildly ramified extension in terms of function fields. In Section 3.2 we begin answering Question 1 in a more geometric context.

3.1 Extensions of Function Fields.

The genus of a function field F is the genus of the unique smooth projective curve X with function field F. The goal of Section 3.1 is to determine the genus of a function field defined by an Artin-Schreier extension. We will calculate the genus of several types of function fields. The intent of these examples is to familiarize ourselves with the terminology and techniques needed to extend these results to Section 3.2 where we consider a more general extension of function fields. We assume throughout Chapter 3 that k is an algebraically closed field of characteristic p.

3.1.1 Notation and Definitions

The purpose of Section 3.1.1 is to introduce the notations that will be used throughout Sections 3.1 and 3.2. We introduce Theorem 3.1.7, the Wild Riemann-Hurwitz formula, without proof. This will be an important tool throughout Chapter 3.

Definition 3.1.1. *[16, Chapter 1] An algebraic function field F/k of one variable over k is an extension field F containing k such that F is a finite algebraic extension of $k(x)$ for some element $x \in F$ which is transcendental over k.*

Definition 3.1.2. *[16, Chapter 3] An algebraic function field F'/k is called an algebraic extension of F/k if F' is an algebraic extension of F.*

A place P of F/k is the maximal ideal of some valuation ring $\mathcal{O}_P \subset F$. Let $\mathcal{P}_F$ denote the set of all such places. Let v_P denote the discrete valuation on the valuation ring $\mathcal{O}_P$. Then a local parameter at P, is any $\alpha \in \mathcal{O}_P$ such that $v_P(\alpha) = 1$. Given an algebraic extension F'/F, a place $Q \in \mathcal{P}_{F'}$

is said to lie over $P \in \mathcal{P}_F$ if $\mathcal{O}_P = \mathcal{O}_Q \cap F$ and we will denote this by $Q|P$. For any $Q \in F'$ with $Q|P$, there is a unique integer $e(Q|P)$ such that $v_Q(x) = e(Q|P)v_P(x)$ for any $x \in F$. Such an integer is called the ramification index of $Q|P$ in F'/F.

Definition 3.1.3. *[16, Chapter 3] Let F'/F be a finite separable extension, and consider a basis $\{z_1, \ldots, z_n\}$ of F'/F. Then there is a uniquely determined dual basis $\{z_1^*, \ldots, z_n^*\} \subset F'$ such that*

$$Tr_{F'/F}(z_i z_j^*) = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{otherwise.} \end{cases}$$

Definition 3.1.4. *[16, Chapter 3] For $P \in \mathcal{P}_F$, let $\tilde{\mathcal{O}}_P$ denote the integral closure of $\mathcal{O}_P$ in F'. Then the complementary module over $\mathcal{O}_P$ is the set*

$$C_P = \{z \in F' : \mathrm{Tr}_{F'/F}(z \cdot \tilde{\mathcal{O}}_P) \subset \mathcal{O}_P\}.$$

Proposition 3.1.5. *[16, Chapter 3] With the notation as in Definition 3.1.4, the following holds:*

1. *C_P is an $\tilde{\mathcal{O}}_P$-module, and $\tilde{\mathcal{O}}_P \subset C_P$.*

2. *If $\{z_1, z_2, \ldots, z_n\}$ is an integral basis of $\tilde{\mathcal{O}}_P$ over $\mathcal{O}_P$, then*

$$C_P = \sum_{i=1}^{n} \mathcal{O}_P \cdot z_i^*,$$

   where $\{z_1^*, z_2^*, \ldots, z_n^*\}$ is the dual basis of $\{z_1, z_2, \ldots, z_n\}$.

3. *There is an element $t \in F'$ such that $C_P = t \cdot \tilde{\mathcal{O}}_P$. Moreover $v_Q(t) \leq 0$ for all $Q|P$.*

Definition 3.1.6. *[16, Chapter 3] With the notation as in Definition 3.1.4, suppose $C_P = t \cdot \tilde{\mathcal{O}}_P$. For $Q|P$, define the exponent of the different by*

$$d(Q|P) = -v_Q(t).$$

With the notation that has been introduced in Section 3.1.1, Theorem 3.1.7 can be stated. It is a generalization of the Riemann-Hurwitz formula stated in Section 3.2. The generalized formula is valid for extensions that are wildly ramified.

Theorem 3.1.7 (Riemann-Hurwitz Genus Formula). *[16, Chapter 3] Let F/k be an algebraic function field of genus g. Let F'/F be a finite separable extension with g' the genus of F'/k. Then we have*

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

3.1.2 Example: $y^p - y = x^{ap-1}$

Throughout Section 3.1.2, fix a to be a positive integer. Let F be the function field $k(x)[y]/(y^p - y - x^{ap-1})$. Let $\pi : X \to \mathbb{P}^1_k$ be the $\mathbb{Z}/(p)$-Galois map of smooth projective curves associated to the extension $k(x) \subset k(x)[y]/(y^p - y - x^{ap-1})$.

A consequence of the Riemann-Hurwitz formula from Theorem 3.1.7 is that every nontrivial extension of $\mathbb{P}^1_k$ must be ramified. The point α is a ramification point if and only if α is in the zero locus of $y^p - y - x^{ap-1}$ and $\partial(y^p - y - x^{ap-1})/\partial y$. Since k is a field of characteristic p, the partial derivative is never zero, and the ramification occurs at a place Q_∞ in F above where x equals infinity. Furthermore the ramification index always divides the degree of a Galois extension of function fields, hence it must be p. Therefore Q_∞ is the unique place above ∞ and $F/k(x)$ is totally ramified over ∞. Our goal is to determine the genus of X. We start by proving Lemmas 3.1.8, 3.1.9, and 3.1.10.

Lemma 3.1.8. *Consider the function field F defined by $y^p - y = x^{ap-1}$. Then*

$$Tr_{F/k(x)}(y^b) = \begin{cases} -1 & \text{if } b = p-1; \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The set $\{1, y, y^2, \ldots, y^{p-1}\}$ is a basis for F over $k(x)$. Galois theory gives us that $F/k(x)$ is a cyclic Galois extension of degree p. The automorphisms of $F/k(x)$ are given by $\sigma_\gamma(y) = y + \gamma$ with $\gamma \in \mathbb{F}_p \subset k$.

$$\begin{aligned} \mathrm{Tr}_{F/k(x)}(y^b) = \sum_{\gamma=0}^{p-1}(y+\gamma)^b = \sum_{\gamma=0}^{p-1}\sum_{l=0}^{b}\binom{b}{l} y^{i-l}\gamma^l = py^b + \sum_{\gamma=1}^{p-1}\sum_{l=1}^{b}\binom{b}{l} y^{b-l}\gamma^l \\ = \sum_{l=1}^{b}\binom{b}{l} y^{b-l}\sum_{\gamma=1}^{p-1}\gamma^l. \end{aligned} \tag{3.1.1}$$

Modulo p we compute

$$\sum_{\gamma=1}^{p-1}\gamma^l = \begin{cases} -1 & \text{if } l = p-1\ ; \\ 0 & \text{otherwise.} \end{cases}$$

Evaluating Equation 3.1.1 for $b \neq p-1$ results in $\mathrm{Tr}_{F/k(x)}(y^b) = 0$. The only nontrivial calculation of Equation 3.1.1 occurs when $b = p-1$. Notice that each sum in Equation 3.1.1 equals 0 when $l \neq p-1$. Therefore

$$\mathrm{Tr}_{F/k(x)}(y^{p-1}) = \sum_{\gamma=1}^{p-1}\gamma^{p-1} = -1.$$

□

Lemma 3.1.9. *Consider the function field F defined by $y^p - y = x^{ap-1}$. Then a basis for C_∞ over $\mathcal{O}_\infty$ is given by*

$$\{-y^{p-1}, -x^{\lceil (ap-1)/p \rceil}y^{p-2}, -x^{\lceil 2(ap-1)/p \rceil}y^{p-3}, \ldots, -x^{\lceil (p-1)(ap-1)/p \rceil}\}.$$

The notation $\lceil m \rceil$ denotes the smallest integer which is at least m.

Proof. Notice that $\tilde{\mathcal{O}}_\infty = \cap_{Q|\infty}\mathcal{O}_Q = \mathcal{O}_{Q_\infty}$ since $Q_\infty|\infty$ is totally ramified. If $z \in F$ then $z = \sum_{s=0}^{p-1} f_s(x)y^s$ for some $f_s(x) \in k(x)$. In order to find a basis for $\mathcal{O}_{Q_\infty}$ over $\mathcal{O}_\infty$, notice that $z \in \mathcal{O}_{Q_\infty}$ if $\upsilon_{Q_\infty}(z) \geq 0$. We begin by calculating $\upsilon_{Q_\infty}(y)$:

$$-p(ap-1) = \upsilon_{Q_\infty}(x^{ap-1}) = \upsilon_{Q_\infty}(y^p - y) = \min\{\upsilon_{Q_\infty}(y^p), \upsilon_{Q_\infty}(y)\} = p\upsilon_{Q_\infty}(y).$$

The last equality is because $\upsilon_{Q_\infty}(y^p) \neq \upsilon_{Q_\infty}(y)$. Therefore $\upsilon_{Q_\infty}(y) = 1 - ap$ and

$$\begin{aligned} 0 \leq \upsilon_{Q_\infty}(z) = \upsilon_{Q_\infty}(\sum_{s=0}^{p-1} f_s(x)y^s) &= \min\{\upsilon_{Q_\infty}(f_s(x)y^s)\}_{s=0}^{p-1} \\ &= \min\{p \cdot \upsilon_\infty(f_s(x) - s(ap-1)\}_{s=0}^{p-1} \end{aligned}$$

Therefore $z \in \mathcal{O}_{Q_\infty}$ if $\upsilon_\infty(f_s(x)) \geq s(ap-1)/p$ for $0 \leq s \leq p-1$. A valuation is always an integer, therefore we require $\upsilon_\infty(f_s(x)) \geq \lceil s(ap-1)/p \rceil$. Otherwise stated, $f_s(x) \in x^{-\lceil s(ap-1)/p \rceil}\mathcal{O}_\infty$. A basis for $\mathcal{O}_{Q_\infty}$ over $\mathcal{O}_\infty$ is

$$\{1, x^{-\lceil (ap-1)/p \rceil}y, x^{-\lceil 2(ap-1)/p \rceil}y^2, \ldots, x^{-\lceil \lceil (p-1)(ap-1)/p \rceil}y^{p-1}\}.$$

It follows from Lemma 3.1.8, Proposition 3.1.5 and Definition 3.1.3 that a basis for C_∞ over $\mathcal{O}_\infty$ is given by

$$\{-y^{p-1}, -x^{\lceil (ap-1)/p \rceil}y^{p-2}, -x^{\lceil 2(ap-1)/p \rceil}y^{p-3}, \ldots, -x^{\lceil (p-1)(ap-1)/p \rceil}\}.$$

□

Lemma 3.1.10. *With the notation as in Proposition 3.1.5,*

$$C_\infty = x^{a(p-1)} \cdot \mathcal{O}_{Q_\infty}.$$

Proof. Consider $z \in C_\infty$; our goal is to show that $z = x^{a(p-1)}z'$ with $z' \in \mathcal{O}_{Q_\infty}$. Lemma 3.1.9 implies that there exists $g_s(x) \in \mathcal{O}_\infty$ such that

$$\begin{aligned} z = \sum_{s=0}^{p-1} g_s(x) x^{\lceil s(ap-1)/p \rceil} y^{p-1-s} &= x^{a(p-1)} \sum_{s=0}^{p-1} g_s(x) x^{\lceil s(ap-1)/p \rceil - a(p-1)} y^{p-1-s} \\ &= x^{a(p-1)} z'. \end{aligned}$$

For each $s = 0, \ldots, p-1$, let $h_s = g_s(x) x^{\lceil \frac{s(ap-1)}{p} \rceil - a(p-1)} y^{p-1-s}$. Then

$$\begin{aligned} v_{Q_\infty}(h_s) =& p v_\infty(g_s(x)) - p\left(\left\lceil \frac{s(ap-1)}{p} \right\rceil - a(p-1)\right) - (ap-1)(p-1-s) \\ \geq& -aps + ap(p-1) - (ap-1)(p-1-s) \\ \geq& p-1-s \\ \geq& 0. \end{aligned}$$

Therefore $z' \in \mathcal{O}_{Q_\infty}$ and $z \in x^{a(p-1)} \cdot \mathcal{O}_{Q_\infty}$.

Conversely, assume that $z \in x^{a(p-1)} \cdot \mathcal{O}_{Q_\infty}$. From Lemma 3.1.9

$$z = x^{a(p-1)} \sum_{s=0}^{p-1} g_s(x) x^{-\lceil s(ap-1)/p \rceil} y^s = \sum_{s=0}^{p-1} g_s(x) x^{-\lceil s(ap-1)/p \rceil + a(p-1)} y^s.$$

Recall the basis for C_∞ from Lemma 3.1.9. We will show $z \in C_\infty$ by demonstrating that

$$x^{-\lceil s(ap-1)/p \rceil + a(p-1)} = x^{\lceil (p-1-s)(ap-1)/p \rceil}.$$

For $s = p-1$;

$$-\left\lceil \frac{s(ap-1)}{p} \right\rceil + a(p-1) = -\left\lceil ap - a - 1 + \frac{1}{p} \right\rceil + a(p-1) = 0.$$

Clearly

$$\left\lceil \frac{(p-1-s)(ap-1)}{p} \right\rceil = 0.$$

For the cases when $s = 0, \ldots, p-2$;

$$-\left\lceil \frac{s(ap-1)}{p} \right\rceil + a(p-1) = -\left\lceil as - \frac{s}{p} \right\rceil + a(p-1) = a(p-1-s),$$

and

$$\left\lceil \frac{(p-1-s)(ap-1)}{p} \right\rceil = \left\lceil ap - a - as - 1 + \frac{1+s}{p} \right\rceil = a(p-1-s).$$

It follows that $z \in C_\infty$. □

Proposition 3.1.11. *Consider the function field F defined by $y^p - y = x^{ap-1}$. Then the genus g of F is given by*

$$g = \frac{(p-1)(ap-2)}{2}.$$

Proof. The genus of $\mathbb{P}^1_k$ is 0 and the only ramification occurs at the unique extension Q_∞ above ∞. Theorem 3.1.7 shows

$$g = 1 - p + 1/2 \sum_{Q|P} d(Q|P).$$

There is only the need to compute what occurs above ∞. Definition 3.1.6 and Lemma 3.1.10 imply that

$$d(Q_\infty|\infty) = -v_{Q_\infty}(x^{a(p-1)}) = ap(p-1).$$

Applying Theorem 3.1.7 concludes the proof, because

$$g = 1 - p + 1/2 \sum_{Q|P} d(Q|P) = 1 - p + \frac{ap(p-1)}{2} = \frac{(p-1)(ap-2)}{2}.$$

□

3.1.3 Higher Order Ramification Groups

In the proof of Proposition 3.1.11, the most difficult step is in calculating the different exponent $d(Q_\infty|\infty)$. Notice that the power of x in the equation $y^p - y = x^{ap-1}$ is congruent to -1 modulo p. This fact allowed us to directly compute a generator for C_∞ as an $\mathcal{O}_{Q_\infty}$-module. It is not always simple to

calculate the different exponent directly from its definition. An alternate approach to determining the different is provided in Theorem 3.1.14. We introduce the idea of higher order ramification groups for the purpose of Theorem 3.1.14. Our goal is to generalize the result from Proposition 3.1.11 to the curve $y^p - y = f(x)$ where $f(x) \in k[x]$ and $\deg(f(x)) = j \not\equiv 0 \bmod p$.

Definition 3.1.12. *[16, Chapter 3] Consider a Galois extension F'/F of algebraic function fields with Galois group G, a place $P \in \mathcal{P}_F$ and a place $Q \in \mathcal{P}_{F'}$ lying over P. For any integer $i \geq -1$ the i-th 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 will let G_i denote $G_i(Q|P)$ when the places are clear from context. Clearly each G_i is a subgroup of G.

Proposition 3.1.13. *[16, Chapter 3] With the notation above, we have:*

1. *G_0 is the inertia group of $Q|P$, in particular the order of G_0 is $e(Q|P)$.*
2. *$G_{-1} \supseteq G_0 \supseteq \cdots$ and $G_m = \{\mathrm{Id}\}$ for sufficiently large m.*
3. *Let $\omega \in G_0$, $i \geq 0$ and η a local parameter at Q. Then*

$$\omega \in G_i \quad \Leftrightarrow \quad v_Q(\omega(\eta) - \eta) \geq i + 1.$$

4. *The group G_1 is a p-group. Furthermore, the integers $i \geq 1$ such that $G_i \neq G_{i+1}$ are all congruent to one another mod p.*

The Galois extension F'/F is wildly ramified at $Q|P$ if p divides the size of $G_0(Q|P)$.

Theorem 3.1.14 (Hilbert's Different Formula). *[16, Chapter 3] Consider a Galois extension F'/F of algebraic function fields, a place $P \in \mathcal{P}_F$ and a place $Q \in \mathcal{P}_{F'}$ lying over P. Then the different exponent is*

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

Using Theorem 3.1.14 we can rephrase Theorem 3.1.7 as

$$2g' - 2 = [F' : F](2g - 2) + \sum_{P \in \mathcal{P}_F} \sum_{Q|P} \sum_{i=0}^{\infty}(|G_i(Q|P)| - 1).$$

3.1.4 Example: $y^p - y = f(x)$

Throughout Section 3.1.4, fix $f(x)$ such that $f(x) \in k[x]$ with $\deg(f(x)) = j \not\equiv 0 \bmod p$. Let F be the function field $k(x)[y]/(y^p - y - f(x))$ where $f(x) \in k[x]$ with $\deg(f(x)) = j \not\equiv 0 \bmod p$.

Proposition 3.1.15. *Consider the function field F defined above. Then the genus g of F is given by*

$$g = \frac{(p-1)(j-1)}{2}.$$

Proof. Following the proof of Lemma 3.1.8 and Proposition 3.1.11 we conclude that $F/k(x)$ is a cyclic Galois extension of degree p with $G = \{\sigma_\gamma : \sigma(y) = y + \gamma \text{ where } \gamma = 0, 1 \ldots, p-1\}$ as its Galois group. The only ramification of $F/k(x)$ occurs at $Q_\infty|\infty$, and furthermore $e(Q_\infty|\infty) = p$.

Notice that $v_\infty(1/x) = 1$. Therefore $1/x$ is a local parameter for $\mathcal{O}_\infty$. We need to determine an element of F that is a local parameter of $\mathcal{O}_{Q_\infty}$. We have

$$-pj = e(p_\infty|\infty) \cdot v_\infty(f(x)) = v_{Q_\infty}(f(x)) = v_{Q_\infty}(y^p - y),$$

and

$$v_{Q_\infty}(y^p - y) \geq \min\{p \cdot v_{Q_\infty}(y), v_{Q_\infty}(y))\} = p \cdot v_{Q_\infty}(y).$$

It follows that $v_{Q_\infty}(y) = -j$. Recall that j and p are relatively prime so there exist integers a and b with $ap - bj = 1$. Therefore we conclude that $x^a y^b$ in F is a local parameter of $\mathcal{O}_{Q_\infty}$ since $v_{Q_\infty}(x^a y^b) = 1$.

Consider the generator $\sigma_1 \in G$. In order to determine which higher order ramification groups σ_1 belongs to, we calculate

$$\begin{aligned}\sigma_1(x^a y^b) - x^a y^b = x^a(y+1)^b - x^a y^b = x^a \cdot \sum_{l=0}^{b} \binom{b}{l} y^{b-l} - x^a y^b \\ = \sum_{l=1}^{b} \binom{b}{l} x^a y^{b-l}.\end{aligned}$$

Therefore

$$\begin{aligned}v_{Q_\infty}(\sigma_1(x^a y^b) - x^a y^b) = \min\left\{v_{Q_\infty}\left(\binom{b}{l} x^a y^{b-l}\right)\right\}_{l=1}^{b} &= v_{Q_\infty}(bx^a y^{b-l}) \\ &= ap - (b-1)j = j+1.\end{aligned}$$

Therefore $G_i = G$ for $0 \leq i \leq j$, and $\{\mathrm{Id}\} = G_{j+1} = G_{j+2} = \cdots$. It follows that

$$d(Q_\infty|\infty) = \sum_{i=0}^{j}(|G_i(Q_\infty|\infty)| - 1) = (j+1)(p-1).$$

Now to finish the calculation above using Theorem 3.1.7 we see that

$$g = 1 - p + \frac{\deg\left(\mathrm{Diff}(F/k(x))\right)}{2} = 1 - p + \frac{(j+1)(p-1)}{2} = \frac{(p-1)(j-1)}{2}.$$

□

3.1.5 Properties of Ramification Groups

Let $F/k(x)$ be a ramified Galois extension with Galois group G. Suppose that the order of G is strictly divisible by p, that is p is the largest power

of p dividing $|G|$. Let Q be a ramified place of F. Let G_0 be the inertia group at Q. Section 3.1.5 discusses the structures of the inertia group G_0 and higher order ramification groups from Definition 3.1.12. We've defined a lower numbering filtration which behaves well with sub-extensions. We use this to define a filtration with a different indexing system, whose virtue is that it is well behaved with quotient extensions.

Lemma 3.1.16. *[15, Chapter 4] Suppose $F/k(x)$ is a Galois extension. If $F/k(x)$ is wildly ramified at $Q \in F$ with inertia group G_0 such that $p^2 \nmid |G_0|$, then*

1. *G_0 is a semidirect product of a subgroup whose order is p and a cyclic group of order prime to p, i.e.*

$$G_0 \cong \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m) \cong \langle \tau \rangle \rtimes \langle \beta \rangle.$$

   Here τ has order p and β has order m which is prime to p.

2. *Recall from Proposition 3.1.13 the filtration of higher order ramification groups $G_0 \supset G_1 \supset \cdots \supset G_h \supsetneq \{1\}$. The lower jump h of $F/k(x)$ at Q is the largest positive integer such that $G_h \neq \{1\}$.*

3. *If $\beta \in G_0$ and $\tau \in G_h$ for $i \geq 1$, then*

$$\beta\tau\beta^{-1} = \beta^h\tau.$$

4. *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 called the upper jump; it is the jump in the filtration of the higher order ramification groups in the upper numbering.*

5. *The lower numbering is invariant under sub-extensions and the upper numbering is invariant under quotient extensions.*

Consider a Galois extension $F/k(x)$ with Galois group G and a ramification point Q satisfying the conditions of Lemma 3.1.16. If G_0 is the inertia group at Q such that $p^2 \nmid |G_0|$, then Lemma 3.1.16(1) implies that G_0 is a subgroup of the normalizer of $\langle\tau\rangle$ in G. Without loss of generality assume that G is contained in some permutation group. Also assume that Q is the ramified place in F with inertia group $G_0 = \langle\tau\rangle \rtimes \langle\beta\rangle$ where $\tau = (12\ldots p)$. Since $G_0 \subset N_G(\langle\tau\rangle)$, the following two lemmas give an upper bound for the size of the inertia group when G is an alternating group. Let $C_{G_0}(\langle\tau\rangle)$ represent the centralizer of $\langle\tau\rangle$ in G_0.

Lemma 3.1.17. *Let $\tau = (12\ldots p)$. Then $N_{A_p}(\langle\tau\rangle) = \langle\tau\rangle \rtimes \langle\beta\rangle$ for some $\beta \in A_p$ with $|\beta| = (p-1)/2$.*

Proof. First we calculate the size of the normalizer. Let n_p be the number of Sylow p-groups in A_p, then

$$n_p = [A_p : N_{A_p}(\langle\tau\rangle)]. \tag{3.1.2}$$

There are $p!/p$ different p-cycles in A_p, each generating a p-group with $p-1$ distinct elements. It follows that

$$n_p = \frac{p(p-1)\cdots 1}{p(p-1)} = (p-2)!.$$

Therefore solving Equation 3.1.2 results in $|N_{A_p}(\langle\tau\rangle)| = p(p-1)/2$.

We have shown that the normalizer has the size claimed. It is still left to show that it has the desired structure. Clearly $\langle\tau\rangle \subset N_{A_p}(\langle\tau\rangle)$; we show the existence of β.

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 $\beta = \theta^2$. Then $\beta \in A_p$, $\beta \notin \langle\tau\rangle$, and $\beta \in N_{A_p}(\langle\tau\rangle)$. Furthermore, for any r

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

Choosing $r = (p-1)/2$ shows that $\beta^{(p-1)/2} \in C_{A_p}(\langle\tau\rangle) = \langle\tau\rangle$, and it follows that $\beta^{(p-1)/2} = 1$. If $1 \leq r < (p-1)/2$, then $\beta^r \notin C_{A_p}(\langle\tau\rangle)$ and thus $\beta^r \neq 1$. Therefore $r = (p-1)/2$ is the minimal exponent such that $\beta^r = 1$. It follows that $\beta \notin \langle\tau\rangle$, β normalizes $\langle\tau\rangle$ in A_p, and β has order $(p-1)/2$. □

Lemma 3.1.18. *Let $2 \leq s < p$ and let $\tau = (12\cdots p)$. Let H_s be the subgroup of A_{p+s} that corresponds to the even permutations on the set $\{p+1, p+2, \ldots, p+s\}$. Then there exists $\theta_1 \in A_{p+s}$ such that $|\theta_1| = p-1$, and*

$$N_{A_{p+s}}(\langle\tau\rangle) = (\langle\tau\rangle \times H_s) \rtimes \langle\theta_1\rangle.$$

Proof. Let θ be the same as in the proof of Lemma 3.1.17. The size of $N_{A_p}(\langle\tau\rangle)$ forces θ to be an odd permutation. Let $\theta_1 = \theta \cdot (p+1, p+2)$. Then $\theta_1 \in N_{A_{p+s}}(\langle\tau\rangle) = \langle\tau\rangle$, and $|\theta_1| = p-1$. The subgroup H_s centralizes τ since each element of H_s is disjoint from τ. Hence

$$(\langle\tau\rangle \times H_s) \rtimes \langle\theta_1\rangle \subset N_{A_{p+s}}(\langle\tau\rangle).$$

Performing a similar count to the one in Lemma 3.1.17, we find that the number of Sylow p-subgroups in A_{p+s} is

$$n_p = \frac{(p+s)(p+s-1)\ldots(s+1)}{p(p-1)} = \frac{(p+s)!}{s!p(p-1)}.$$

Therefore $|N(\langle\tau\rangle)| = p(p-1)s!/2$, and the structure follows. □

Recall that for an inertia group G_0 satisfying Lemma 3.1.16, there is a unique lower jump. The lower jump h encodes information about the filtration of higher order ramification groups. The following two lemmas relate h to the size of $C_{G_0}(\langle\tau\rangle)$. Recall that

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

Lemma 3.1.19. *Let $\pi : X \to \mathbb{P}^1_k$ be an A_p-Galois cover. Assume that π is wildly ramified over a branch point b. Let G_0 be the inertia group at some point $Q \in X$ above b. Assume that $|G_0| = pm$ and π has lower jump h at b. Then* $\gcd(h, m) = 1$.

Proof. Let $\beta \in A_p$ 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 $1 \leq i < m$. Therefore for $1 \leq i < m$,

$$\tau \neq \beta^i \tau \beta^{-i} = \beta^{ih}\tau.$$

The last equality is a result of $\tau \in G_h$ and Lemma 3.1.16(3). Notice that $\beta^{ih} \neq 1$ which implies that $m \nmid ih$ for each $1 \leq i < m$. Hence $\gcd(h, m) = 1$. □

Lemma 3.1.20. *Let $2 \leq s < p$, and let $\pi : X \to \mathbb{P}^1_k$ be an A_{p+s}-Galois cover. Assume π is wildly ramified over a branch point b. Let G_0 be the inertia group at some point $Q \in X$ above b. Assume that $|G_0| = pm$ and π has lower jump h at b. Let* $\gcd(h, m) = m'$, *then $C_{G_0}(\langle\tau\rangle) \cong \mathbb{Z}/(p) \times \mathbb{Z}/(m')$.*

Proof. Let $\beta \in A_{p+s}$ such that $G_0 = \langle\tau\rangle \rtimes \langle\beta\rangle$. Assume that $\gcd(h, m) = m'$. Then Lemma 3.1.16(3) implies

$$\beta^{m/m'} \tau \beta^{-m/m'} = \beta^{m \cdot h/m'} \tau = \tau.$$

The last equality is because the order of β is m and h/m' is a positive integer. 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 3.1.16(3) implies

$$\tau = \alpha\tau\alpha^{-1} = \alpha^h\tau.$$

It follows that $|\alpha|$ divides h and m, so $|\alpha|$ must divide their greatest common divisor m'. Since $\mathbb{Z}/(m)$ is cyclic, it must be the case that $\alpha \in \langle\beta^{m/m'}\rangle$. Hence $C_{G_0}(\langle\tau\rangle) = \langle\tau\rangle \rtimes \langle\beta^{m/m'}\rangle$. □

3.1.6 Newton Polygons

Every polynomial has a Newton polygon associated to each valuation of the field of coefficients. Section 3.1.6 gives a brief survey of the theory of Newton Polygons. Let v be a valuation of the field $k(x)$. Let

$$f(y) = a_n y^n + a_{n-1}y^{n-1} + \cdots a_1 y + a_0 \in k[x][y] \text{ where } a_n \cdot a_0 \neq 0.$$

Let $\tilde{F}$ be the splitting field of f over $k(x)$. Let v_Q be a valuation of $\tilde{F}$ lying above the valuation v on $k(x)$. Let $v(0) = \infty$. The Newton polygon of f relates the valuation v_Q on the roots of f to the valuation v on the coefficients of f. The Newton polygon Δ of f is the lower convex hull in the plane of the set of points

$$\{(0, v(a_0)), (1, v(a_1)), \ldots, (n, v(a_n))\}.$$

The polygon is a sequence of line segments with increasing slopes of negative values.

Proposition 3.1.21. *[11, Chapter 2] Let $\tilde{F}$ be the splitting field of f over $k(x)$. Let v_Q be a valuation on $\tilde{F}$ lying above the valuation v on $k(x)$.*

If $(i, v(a_i)) \leftrightarrow (j, v(a_j))$ *is a line segment of slope* $-m$ *occurring in the Newton polygon of* f*, then* $f(x)$ *has exactly* $j - i$ *roots with each root* r *having valuation* $v_Q(r) = m$.

Suppose f defines a degree n Galois extension of $k(x)$ that is ramified above 0. Note that it does not matter where the ramification occurs. The reason for choosing the ramification to occur over 0 is to simplify the notation. Let Q be a ramified place in the splitting field of f above 0. Let η be a local parameter of the valuation ring $\mathcal{O}_Q$. The following manipulation of f results in a polynomial $N(z)$ whose roots determine the structure of the higher order ramification groups at Q from Proposition 3.1.13.

$$\frac{N(z)}{\eta^n} := \frac{f(\eta(z+1))}{\eta^n} = \prod_{\omega \in G} z - \left(\frac{\omega(\eta) - \eta}{\eta}\right). \tag{3.1.3}$$

The polynomial $\eta^{-n}N(z) \notin k[x][z]$, therefore Proposition 3.1.21 does not directly apply. We introduce the following proposition to overcome the limitation of Proposition 3.1.21. The Galois extension $F/k(x)$ yields a ramified Galois extension of local rings $k[[\eta]]/k[[x]]$. The local extension may or may not be defined by the polynomial f above. Let $f_2 \in k[[x]][y]$ be the defining polynomial of the extension of local rings. Notice that η is a root of f_2. Let n_2 be the degree of f_2, then $n_2 = e(Q|0)$. Define coefficients $b_i \in \mathcal{O}_Q$ so that

$$\eta^{-n_2}N(z) = \eta^{-n_2}f_2(\eta(z+1)) = \eta^{-n_2}\sum_{i=1}^{e} b_i z^i \in \mathcal{O}_Q[z]. \tag{3.1.4}$$

The Newton polygon Δ of $k[[\eta]]/k[[x]]$ is obtained by taking the lower convex hull of the set of points $\{(i, v_Q(b_i))\}_{i+1}^{e}$. There is a difference between Equations 3.1.3 and 3.1.4. Equation 3.1.3 is written as a product over all

automorphisms in the Galois group G. Equation 3.1.4 has a similar representation as a product over all automorphisms in the inertia group at Q. Proposition 3.1.22 relates higher order ramification groups to the line segments of Δ.

Proposition 3.1.22. *[14] Let $\{V_1, V_2, \ldots, V_r\}$ be the vertices of Δ and $-m_j$ the slope of the edge joining V_{j-1} and V_j. The slopes are integral and the jumps in the sequence $G_1 \supset G_2 \supset \cdots$ of higher order ramification groups are $m_r < m_{r-1} < \cdots$.*

Lemma 3.1.23. *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 in $\tilde{F}_t$ lying over 0 and G_0 the corresponding inertia group. Then the order of G_0 is pm for some integer m where $p \nmid m$. Let Δ_t be the ramification polygon of $\tilde{F}_t/k(x)$. Then Δ_t is the polygon consisting of two line segments, one having integral slope $-m(p-t)/(p-1)$ and the other having slope 0.*

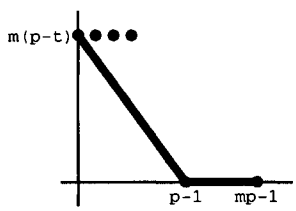

Figure 3.1: Ramification polygon Δ_t.

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 size of G is strictly divisible by p. The extension is branched over 0. Let P and Q be places lying above 0 in F_t and $\tilde{F}_t$ respectively. The equation $f_{1,t}$ implies that $e(P|0) = p$; let m be

the integer such that $e(Q|0) = pm$. Notice that $p \nmid m$ since $p^2 \nmid G_0$. 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, as in Figure 3.2. The extension of complete local rings $\hat{\mathcal{O}}_P/k[[x]]$ 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
$\vert$	$\vert_{\mathrm{m}}$	$\vert$
F_t	$\hat{\mathcal{O}}_P$	η
$\vert$	$\vert_{\mathrm{p}}$	$\vert$
$k(x)$	$k[[x]]$	x

Figure 3.2: Corresponding extension of complete local rings.

We can assume that η is a root of $f_{1,t}$. Notice that any root of $f_{1,t}$ would correspond to a local parameter of F_t since

$$p = v_P(x) = v_P\Big(\frac{\eta^p}{\eta^{p-t}+1}\Big) = pv_P(\eta).$$

Now consider η as an element in $\mathcal{O}_Q$. Then η can be expressed as a power series in the local parameter ϵ with coefficients in k, that is

$$\eta = c_m\epsilon^m + c_{m+1}\epsilon^{m+1} + \cdots = u \cdot \epsilon^m \text{ where } u \text{ is a unit of } \mathcal{O}_Q.$$

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

$$f_{2,t}(\epsilon) = \epsilon^{pm} - x\epsilon^{m(p-t)} + x = 0. \tag{3.1.5}$$

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

$$N(z) = f_{2,t}(\epsilon(z+1)) = \epsilon^{pm}(z+1)^{pm} - x\epsilon^{m(p-t)}(z+1)^{m(p-t)} + x. \tag{3.1.6}$$

Divide both sides of Equation 3.1.6 by ϵ^{pm}. The effect to the Newton polygon Δ_t is a vertical shift by $-pm$. The effect of vertical and horizontal shifts do not affect the slopes of the line segments of Δ_t. Let $d = 1/(u^{-t}\epsilon^{m(p-t)} + u^{-p})$, then

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

Notice that $G(0) = 0$ so the constant term must be 0, therefore we can factor out a power of z. The effect on Δ_t is a shift in the horizontal direction by -1. Eliminating the irrelevant power of z results in

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

Let $z^{-1}\epsilon^{-pm}N(z) = \sum_{j=1}^{pm-1} b_j z^j$. 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. $v_Q(b_0) = v_Q(-d\epsilon^{m(p-t)}) = m(p-t)$.

2. For $1 \leq j < p-1$ and $1 \leq i < m(p-t) - (p-1)$,

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

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

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

Therefore the vertices of Δ_t are $(0, m(p-t))$, $(p-1, 0)$, and $(pm-1, 0)$. □

Lemma 3.1.24. *For $2 \leq s < p$ let $\overline{f_s}(y) = y^{p+s} - xy^s + 1 \in k(x)[y]$. Let $F_s/k(x)$ be the corresponding extension of function fields and $\tilde{F}_s/k(x)$ its Galois closure. Let Q be a place in $\tilde{F}_s$ lying over ∞ and G_0 the corresponding inertia group. Then the order of G_0 is pm for some integer m where $p \nmid m$. Let $\overline{\Delta}_s$ be the ramification polygon of $\tilde{F}_s/k(x)$. Then $\overline{\Delta}_s$ is the polygon consisting of two line segments, one having integral slope $-m(p+s)/(p-1)$ and the other with slope 0.*

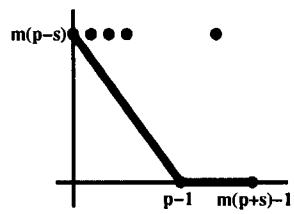

Figure 3.3: Ramification polygon $\overline{\Delta}_s$.

Proof. Let G be the Galois group of the extension $\tilde{F}_s/k(x)$. Notice that G is contained in S_{p+s}, therefore the size 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 F_s lying above ∞. Then the equation $\overline{f_s}$ implies that $P_{(\infty,0)}$ and $P_{(\infty,\infty)}$ have ramification index p and s respectively. Let Q be a place of $\tilde{F}_s$ lying above $P_{(\infty,0)}$. Let m be the integer such that $e(Q|0) = pm$. 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, as in Figure 3.4.

The extension $\tilde{F}_s/k(x)$ is not totally ramified over ∞. However $\hat{\mathcal{O}}_Q/k[[x^{-1}]]$ is a totally ramified Galois extension with Galois group G_0 of order pm. By

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

Figure 3.4: Corresponding extension of complete local rings.

the same reasoning as for Lemma 3.1.23, there exists a local parameter ϵ of $\hat{\mathcal{O}}_Q$ that satisfies $\epsilon^m = \eta$. Therefore ϵ satisfies the irreducible equation

$$\overline{f}_{2,s}(\epsilon) = \epsilon^{m(p+s)} - x\epsilon^{ms} + 1 = 0. \tag{3.1.7}$$

We calculate the ramification polygon $\overline{\Delta}_s$ by considering

$$N(z) = \overline{f}_{2,s}(\epsilon(z+1)) = \epsilon^{m(p+s)}(z+1)^{m(p+s)} - x\epsilon^{-ms}(z+1)^{ms} + 1. \tag{3.1.8}$$

It follows that

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

Let $z^{-1}\epsilon^{-m(p+s)}N(z) = \sum_{j=1}^{m(p+s)-1} b_j z^j$. The valuation v_Q lies over ∞ so it is the negative of the valuation in Lemma 3.1.23. The valuation of each b_j is greater than or equal to zero. The ramification polygon $\overline{\Delta}_s$ follows when we calculate the valuations of the specific coefficients that determine the lower convex hull of $\overline{\Delta}_s$.

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 $\overline{\Delta}_s$ are $(0, m(p-s))$, $(p-1, 0)$, and $(m(p+s)-1, 0)$. □

3.2 A_n Galois covers of the projective line

In 1957 Abhyankar conjectured that a finite group G occurs as the Galois group of a cover $\pi : X \to \mathbb{P}^1_k$ branched only at ∞ if and only if G is a quasi- p group [1]. One says that G is a quasi-p group if it is generated by its Sylow p-subgroups. For $n \geq p \geq 5$, A_n is an example of a quasi-p group. Abhyankar's conjecture was proven by 1994 by work of Raynaud [13] and Harbater [6]. Abhyankar also stated the currently unproven Inertia Conjecture.

Conjecture 3.2.1 (Inertia Conjecture). *[1] 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_P. Suppose that the conjugates of G_P generate G. Then there exists a G-Galois cover $\pi : X \to \mathbb{P}^1_k$ branched only at ∞ with inertia group G_0 at some point of $\pi^{-1}(\infty)$.*

There is not much evidence to support the Inertia Conjecture in the literature. Bouw and Pries were able to show that the conjecture was true for A_p and $\mathrm{PSL}_2(\mathbb{F}_p)$ [4]. Section 3.2.5 shows the Inertia Conjecture is true for A_{p+2}.

3.2.1 Galois Covers Branched only at ∞.

Let $\pi : X \to \mathbb{P}^1_k$ be a Galois covering branched only at ∞. The extension is wildly ramified at any point $Q \in X$ lying over ∞. The complexity of the wild ramification is directly related to the power of p that divides the ramification index $e(Q)$. The ramification index is the size of the corresponding inertia group G_0, and the size of an inertia group divides the size of the Galois group. For this reason we concentrate on Galois groups A_n such

that the size of A_n is strictly divisible by p. It is known how to construct A_n-Galois covers when $n = p$ or $p + 1 < n < 2p$.

The Riemann-Hurwitz formula from Theorem 3.1.7 relates the genus of X to the upper jump σ. Small values of σ correspond to a small genus. We restate Question 1 in terms of the upper jump.

Question 2 Let $n = p$ or $p+1 < n < 2p$. Let $\pi : X \to \mathbb{P}^1_k$ be an A_n-Gaois cover of the projective line branched only at ∞. Let $P \in X$ with inertia group G_0 and upper jump σ. What small values of σ can be realized?

In order to answer Question 2 we state some technical lemmas that will be needed. The following is a version of Abhyankar's Lemma. This version gives a technique to construct a G-Galois cover of $\mathbb{P}^1_k$ branched only at ∞ from a G-Galois cover of $\mathbb{P}^1_k$ branched at 0 and ∞.

Lemma 3.2.2 (Refined Abhyankar's Lemma). *[4] Suppose there exists a G-Galois cover $\pi : X \to \mathbb{P}^1_k$ with branch locus contained in $\{0, \infty\}$. Suppose that π has inertia group $\mathbb{Z}/(t)$ above 0 and inertia group $G_0 = \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ above ∞ with lower jump h where m, t are prime to p. Let $m^* = \gcd(m, t)$. Let $\psi : \mathbb{P}^1_k \to \mathbb{P}^1_k$ be a t-cyclic cover branched at 0 and ∞. Assume that π and ψ are linearly disjoint. Then there exists a G-Galois cover $\pi' : \tilde{X} \to \mathbb{P}^1_k$ branched at exactly one point with inertia group $G'_0 \subset G_0$ of order pm/m^* and with lower jump ht/m^*.*

The variables x and z in Figure 3.5 represent two different parameters on $\mathbb{P}^1_k$. Let σ and σ' be the upper jumps of π and π' respectively. Lemma 3.2.2 implies that $\sigma' = t\sigma$.

$$\begin{array}{ccccc} & X & \leftarrow & \tilde{X} & \\ \pi & \downarrow & & \downarrow & \pi' \\ & \mathbb{P}^1_x & \leftarrow & \mathbb{P}^1_z & \\ & & \psi & & \end{array}$$

Figure 3.5: Refined Abhyankar's Lemma

Lemma 3.2.3. *[4] Suppose there exists a G-Galois cover of $\mathbb{P}^1_k$ branched only over ∞. Assume that $G_0 = \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ is the inertia group 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 be the subgroup of G_0 of order pm_d. Then for each d there exists a G-Galois cover of $\mathbb{P}^1_k$ branched only over ∞ with inertia group G_0^d and lower jump h_d.*

3.2.2 A_p Galois covers of the projective line

Let $p \geq 5$. In Section 3.2.2 we focus attention on the situation when the Galois group is the alternating group A_p of even permutations on p elements. Recall that our goal in answering Question 2 is to determine A_p-Galois covers $\pi : X \to \mathbb{P}^1_k$ branched only at ∞ with a small upper jump.

Abhyankar provided the equation of a curve whose Galois closure is an A_p or S_p Galois cover of the projective line. For $p > 2$, he considered the affine curve given by the zero locus of $f_t = y^p - y^t + x$ where t is an integer with $1 < t < p-2$. The curve $Z(f_t)$ corresponds to the function field $F_t = k(x)[y]/(f)$. The extension $F_t/k(x)$ is not Galois since there are not enough automorphisms of F_t that fix $k(x)$. The Galois closure $\tilde{F}_t$ of F_t has Galois group A_p for t odd and S_p for t even [2]. Abhyankar proved this by showing the Galois group is doubly transitive on the set $\{1, 2, \ldots, p\}$ and contained a certain cycle type. Abhyankar used the twisted derivative to eliminate roots of f_t and understand the extension's first two

stages [3]. Unfortunately the twisted derivative becomes computationally intensive after one twist. We defer the definition of the twisted derivative until Definition 3.2.1.

Let X_t be the smooth projective curve corresponding to the function field $\tilde{F}_t$. There is a covering map $\pi : X_t \to \mathbb{P}^1_k$ as in Figure 3.6.

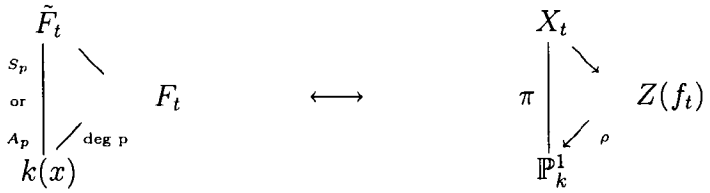

Figure 3.6: Extensions of $k(x)$ correspond to coverings of $\mathbb{P}^1_k$.

For the remainder of Section 3.2.2 we will assume that $\pi : X_t \to \mathbb{P}^1_k$ is this Galois cover with Galois group A_p or S_p. Lemma 3.1.16(1) implies that the inertia group G_0 at a point of X_t over ∞ is always of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ where $p \nmid m$. Let h be the lower jump so that G_h is the last non-trivial ramification group in the lower numbering.

In order to determine the upper jump σ corresponding to the higher order ramification groups of π over ∞, we concentrate on determining the ramification that occurs. Some difficulties are that a defining equation for X_t is not known, and for $p \geq 5$ the Galois group A_p is simple. Therefore it is impossible to find a primitive element for $\tilde{F}_t$ by radicals. Without this knowledge it is hard to understand the Galois action on X_t. We can however use equation f_t to understand the ramification that occurs in the quotient map $\rho : Z(f_t) \to \mathbb{P}^1_k$.

Lemma 3.2.4. *Let $1 < t < p-2$, and let X_t and $Z(f_t)$ be defined as in Figure 3.6. Let $\pi : X_t \to \mathbb{P}^1_k$ and $\rho : Z(f_t) \to \mathbb{P}^1_k$ be the S_p or A_p-Galois cover and the degree p quotient cover respectively. Then the branch locus of ρ is the same as the branch locus of π.*

Proof. Assume that the Galois group is S_p. The branch locus of ρ is contained in the branch locus of π since ramification indices are multiplicative. Let b be in the branch locus of π but not in the branch locus of ρ. We will show that this is impossible. The Galois subcover $\mu : X_t \to Z(f_t)$ has a Galois group that is a subgroup of S_p of order $(p-1)!$. There are p possible choices for this subgroup. Without loss of generality assume

$$\mathrm{Gal}(\mu) = S_P^1 = \mathrm{Stab}_{S_p}(1).$$

Let $Q \in X_t$ be a ramification point lying above b with inertia group G_0. Conjugating G_0 by elements in S_p results in an inertia group at some point lying above b. Since b is not a branch point of ρ, we have that

$$\omega G_0(Q|b)\omega^{-1} \subset S_p^1 \text{ for all } \omega \in S_p.$$

This is impossible since S_p is transitive on the set $\{1, 2, \ldots, p\}$. Therefore the branch loci must be the same. The same explanation works for A_p since A_p is transitive on $\{1, 2, \ldots, p\}$ as well. □

Figure 3.2.2 depicts the ramification over the place 0 in $k(x)$ of the extension. The are multiple points above each place $P \in F$ in Figure 3.2.2. The number of points is irrelevant to our calculations. Let $Q_{(0,0)}$ and $Q_{(0,\zeta_{p-t})}, \ldots, Q_{(0,1)}$ in Figure 3.2.2 represent the set of places in $\tilde{F}_t$ above the places $P_{(0,0)}$ and $P_{(0,\zeta_{p-t})}, \ldots, P_{(0,1)}$ of F_t respectively.

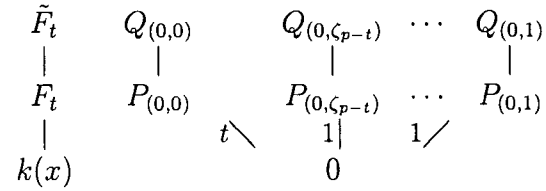

Figure 3.7: Ramification above 0 of the extension in Lemma 3.2.5.

Lemma 3.2.5. *The extension $\tilde{F}_t/k(x)$ is ramified with inertia group of order t above 0 and at no other finite points.*

Proof. The point $(0,0)$ of $Z(f_t)$ corresponds to the only solution to $\partial f/\partial y = 0$. Therefore $P_{(0,0)}$ is the only ramified place in F_t occurring over a finite place in $k(x)$. The places of F_t above 0 are $P_{(0,0)}, P_{(0,\zeta_{p-t})}, \ldots, P_{(0,1)}$. Ramification only occurs at $P_{(0,0)}$ so $e(P_{(0,\zeta_{p-t}^i)} \mid 0) = 1$ which forces $e(P_{(0,0)} \mid 0) = t$ because of the identity

$$p = [F_t : k(x)] = \sum_{P \mid 0} e(P \mid 0).$$

Lemma 3.2.4 implies that the ramified places in $\tilde{F}_t$ occurring over a finite place in $k(x)$ must occur over 0. Let $Q \in \tilde{F}_t$ be any place lying above $P_{(0,0)}$. We are just left with showing that $e(Q|P_{(0,0)}) = 1$. Recall that $\tilde{F}_t/k(x)$ is Galois with Galois group A_p or S_p. Assume that the Galois group is S_p and the Galois group of $\tilde{F}_t/F_t$ is S_p^1. Then

$$|G(Q|0)| = |G(P_{(0,0)}|0)| \cdot |G(Q|P_{(0,0)})| = t \cdot |G(Q|P_{(0,0)})|.$$

Notice that $G(Q|P_{(0,0)}) \subset S_p^1$, so $p \nmid |G(Q|P_{0,0})|$. Therefore Lemma 3.1.16(1) implies that $G_0(Q \mid 0)$ is a cyclic group of order $t \cdot c$ for some integer c prime to p. Our goal is to show that $c = 1$.

Suppose $c \neq 1$, and let $G_0(Q \mid 0) = \langle \phi \rangle$. Notice $\phi \notin S_p^1$; if it were then all ramification would occur in the extension $Q \mid P_{(0,0)}$. Consider the t-th power

of ϕ which generates $G_0(Q \mid P_{(0,0)})$, that is $G_0(Q \mid P_{(0,0)}) = \langle \phi^t \rangle \subset S_p^1$. Recall that S_p is transitive on $\{1, 2, \ldots, p\}$. Hence, there exists a $\gamma \in S_p$ such that $\gamma\phi^t\gamma^{-1} \notin S_p^1$. Notice that $\gamma \notin S_p^1$. Therefore there exist a point $\tilde{Q}$ in $\tilde{F}_t$ not above $P_{(0,0)}$, but lying over 0 with $G_0(\tilde{Q}|0) = \langle \gamma^{-1}\phi\gamma \rangle$. Furthermore $(\gamma\phi\gamma^{-1})^t = \gamma\phi^t\gamma^{-1} \in G_0(\tilde{Q}|0)$. Hence $G_0(\tilde{Q}|0) \not\subset S_p^1$. Therefore for some $j \neq 0$, the extension $P_{(0,j)}|0$ is ramified. This contradicts the work we have previously done. Therefore the assumption that $c \neq 1$ is false.

A similar proof works when the Galois group is A_p. □

Lemma 3.2.6. *The extension $\tilde{F}_t/k(x)$ is ramified with inertia group of order $p(p-1)/\gcd(p-1, p-t)$ above ∞ with upper jump $\sigma = (p-t)/(p-1)$.*

Proof. Let P_∞ be any place of F_t that lies above ∞. Then

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

Therefore $p|e(P_\infty|\infty)$ and $e(P_\infty|\infty) \leq p$ so we must have equality. It follows that ρ is totally ramified at P_∞. Our goal is to determine the ramification of π over ∞.

Consider the maps $x \mapsto 1/x$ and $y \mapsto 1/y$. Understanding ramification over ∞ is equivalent to understanding the ramification over 0 of the map corresponding to the curve $f_{1,t} : y^p - xy^{p-t} + x$ obtained after applying the above maps to f.

The polynomial $f_{1,t}$ is the same polynomial that was considered in Lemma 3.1.23. Therefore the ramification polygon Δ_t of $\tilde{F}_t/k(x)$ consists of one line segment with integral slope $-m(p-t)/(p-1)$. This represents the jump in the filtration of higher order ramification groups in the lower numbering

i.e., the lower jump. Recall from Lemma 3.1.16(4) that we can use this to calculate the upper jump σ. We conclude that $\sigma = (p-t)/(p-1)$.

Lemma 3.1.19 implied that h and m are co-prime, therefore we conclude that

$$h = \frac{p-t}{\gcd(p-1,p-t)},\ m = \frac{p-1}{\gcd(p-1,p-t)},\ \text{and}\ |G_0| = \frac{p(p-1)}{\gcd(p-1,p-t)}.$$

□

Theorem 3.2.7. *For $1 < t < (p-2)$, there exists an A_p-Galois cover of $\mathbb{P}^1_k$ branched only at ∞ with ramification group having order $p(p-1)/\gcd(p-1,t(p-t))$ and upper jump $t(p-t)/(p-1)$.*

Proof. Let $d_1 = \gcd(p-1,p-t)$ and $m = (p-1)/d_1$. Let X be the Galois closure of the curve corresponding to f_t. Then there exist a Galois cover $\pi : X_t \to \mathbb{P}^1_k$ branched at 0 and at ∞. The Galois group is either A_p or S_p depending on whether t is even or odd respectively. Lemma 3.2.5 implies that the map π is ramified of order t above 0. Lemma 3.2.6 implies that the inertia group G_0 above ∞ has order pm and upper jump $\sigma = (p-t)/(p-1)$.

Consider the case when t is odd. The Galois group of the covering $\pi : X_t \to \mathbb{P}^1_k$ is A_p. Let $m^* = \gcd(m,t)$. Since A_p is simple, the cover π is linearly disjoint from the t-cyclic cover $\psi : \mathbb{P}^1_k \to \mathbb{P}^1_k$ with equation $z^t = x$. Applying Lemma 3.5 yields a Galois covering $\pi' : X'_t \to \mathbb{P}^1_k$ with Galois group A_p. The map π' is branched only at ∞ with inertia group G'_0 of order pm/m^* and upper jump $\sigma' = t(p-t)/(p-1)$. Notice that $d_1 m^* = \gcd(p-1,t(p-t))$, so the inertia group has size $pm/m^* = p(p-1)/\gcd(p-1,t(p-t))$.

Assume t even. The Galois group of the covering $\pi : X_t \to \mathbb{P}^1_k$ is S_p. Consider the Galois subcover corresponding to the subgroup A_p. If $\tilde{F}_t$ is

the function field of X_t, let Y be the smooth projective curve corresponding to the fixed field $\tilde{F}_t^{A_p}$. Let $\mu : X_t \to Y$ be the corresponding covering map.

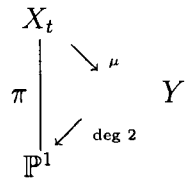

Figure 3.8: A_p subcover.

Consider the degree 2 extension $Y/\mathbb{P}_k^1$. The branch locus of the extension must be contained in the branch locus of π since ramification indices are multiplicative. The Riemann-Hurwitz formula implies that there are unique ramified points P_0 and P_∞ of Y lying over 0 and ∞ respectively. The ramification indices $e(P_0|0)$ and $e(P_\infty|\infty)$ must be 2. Ramification indexes are multiplicative so the map μ is ramified of order $t/2$ over 0 and order $|G_0|/2$ over ∞. It can be seen that $|G_0|/2 = pm/2$ is an integer from Lemma 3.2.7 since t is even.

Applying the Riemann-Hurwitz formula to the extension $Y/\mathbb{P}_k^1$ results in:

$$2g(Y) - 2 = 2(2g(\mathbb{P}_k^1) - 2) + (2-1) + (2-1).$$

This forces $g(Y) = 0$, thus $Y \cong \mathbb{P}_k^1$. Therefore we have that $\mu : X_t \to \mathbb{P}_k^1$ is Galois with Galois group A_p. The lower jump of μ is the same as the lower jump of π since it is invariant under sub-extensions. Therefore the upper jump of μ is 2σ. The cover μ is linearly disjoint from the $t/2$-cyclic cover $\psi : \mathbb{P}_k^1 \to \mathbb{P}_k^1$ with equation $z^{t/2} = x$. Let $\overline{m} = \gcd(m/2, t/2)$. Applying Lemma 3.5 yields a Galois covering $\overline{\pi} : \overline{X_t} \to \mathbb{P}_k^1$ with Galois group A_p. The map $\overline{\pi}$ is branched only at ∞ with inertia group $\overline{G}_0$ of order $pm/(2\overline{m})$ and

upper jump $\overline{\sigma} = t(p-t)/(p-1)$. Notice that $pm/2(\overline{m}) = pm/m^*$, so the inertia group has size $p(p-1)/\gcd(p-1, t(p-t))$. □

Corollary 3.2.8. *Let $1 < t < (p-2)$ and $d_2 = \gcd(p-1, t(p-t))$. There exists an A_p-Galois cover $\pi : X \to \mathbb{P}^1_k$ branched only at ∞ with genus of X being*

$$g = 1 + \frac{|A_p|}{2}\left(-1 - \frac{d_2}{p(p-1)} + \frac{t(p-t)}{p}\right).$$

Proof. With the hypotheses as above, the Riemann-Hurwitz formula simplifies to

$$2g(X) - 2 = -2|A_p| + \frac{|A_p|}{|G_0|}\Big(|G_0| - 1 + (p-1)m\sigma\Big).$$

Corollary 3.2.8 is immediate from Proposition 3.1.13 and the definition of σ in Theorem 3.2.7. □

The smallest value of σ that can be achieved using the method of Theorem 3.2.7 is $2(p-2)/(p-1)$ when $t = 2$ and $t = p-2$. This can be seen by treating σ as a function of t and considering the derivative.

$$\frac{d\sigma}{dt} = \frac{p-2t}{p-1}.$$

Notice that $d\sigma/dt \geq 0$ for $2 \leq t \leq (p-1)/2$, and $d\sigma/dt \leq 0$ for $(p-1)/2 < t \leq p-2$.

It follows that the smallest genus obtained using the method of Theorem 3.2.7 is

$$g = 1 + \frac{|A_p|}{2p(p-1)}\left(p^2 - 5p + 2\right).$$

Let $\pi : X \to \mathbb{P}^1_k$ be an A_n-Galois cover branched only at ∞. Suppose σ is the upper jump of π. The following theorem states when it is possible

to produce a different A_n-Galois covering of $\mathbb{P}^1_k$ branched only at ∞ with a larger upper jump.

Theorem 3.2.9. *[12, Special case of Theorem 2.3.1] Let $\pi : X \to \mathbb{P}^1_k$ be an A_n-Galois cover branched only at infinity 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 an A_n-Galois cover branched only at infinity with the same inertia group and upper jump $\sigma' = (h/m) + i$.*

Corollary 3.2.10. *For $p \equiv 1$ mod 4, there exists an A_p-Galois cover with inertia group $\mathbb{Z}/(p)$ and lower jump h_1 for every $h_1 \geq (p+1)/2$ relatively prime to p. For $p \equiv 3$ mod 4, there exists an A_p-Galois cover with inertia group $\mathbb{Z}/(p)$ and lower jump h_3 for every $h_3 \geq (p+1)/4$ relatively prime to p.*

Proof. For $1 < t < p-2$, let $d_2 = \gcd(p-1, t(p-t))$. Theorem 3.2.7 implies that there exists an A_p-Galois cover branched only at ∞ with inertia group having order $p(p-1)/d_2$ and upper jump $t(p-t)/(p-1)$. Taking $d = (p-1)/d_2$ in Lemma 3.2.3 yields an A_p-Galois cover branched only at ∞ with inertia group $\mathbb{Z}/(p)$ and upper jump $t(p-t)/d_2$. Lemma 3.1.16(4) implies that that the upper jump is the same as the lower jump since the inertia group is $\mathbb{Z}/(p)$. Therefore $t(p-t)/d_2$ is an integer. The smallest integer $t(p-t)/d_2$ correspond to the largest possible value for d_2. The largest value of d_2 is obtained when $t = (p-1)/2$, it is

$$d_2 = \gcd\left(p-1, \frac{(p-1)(p+1)}{4}\right) = \begin{cases} \dfrac{p-1}{2}, & \text{for } p \equiv 1 \bmod 4\ ; \\ p-1, & \text{for } p \equiv 3 \bmod 4\ . \end{cases}$$

It follows that for $t = (p-1)/2$, one can realize the lower jump $h_1 = (p+1)/2$ (respectively $h_3 = (p+1)/4$) when $p \equiv 1 \bmod 4$ (respectively $p \equiv 1 \bmod 4$). The rest of the values of h_1 and h_3 follow from Theorem 3.2.9. □

3.2.3 Comparison with Previous Results

There are answers to Question 2 for the case when $n = p$. We state them as the following theorem.

Theorem 3.2.11. *[4] Let $G = A_p$. Let $c = (p-1)/2$ and $m|c$. Let a be such that $0 < a \leq m$ and $\gcd(a, m) = 1$. Let $h \in \mathbb{N}$ be such that $\gcd(h, p) = 1$ and $h \equiv -a \bmod m$. Assume that $h \geq a(p-2)$. Then there exists a G-Galois cover of curves $\pi : X \to \mathbb{P}^1_k$ branched at exactly one point with $G_0 = \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ and lower jump h.*

Theorem 3.2.11 can be difficult to decode. Table 3.1 is intended to clarify the situation. Column 2 of Table 3.1 shows the values of σ that are achieved from Theorem 3.2.11 for the first few primes. Column 3 depicts possible upper jumps not realized by Theorem 3.2.11. The possible upper jumps are acquired from the congruence conditions that $\sigma = h/m > 1$, $p \nmid h$, and $m|(p-1)/2$. These conditions follow from the Riemann-Hurwitz formula and Lemma 3.1.17. Column 4 shows the new upper jumps obtained from Theorem 3.2.7.

p	σ obtained from Theorem 3.2.11	σ missed in Theorem 3.2.11	Theorem 3.2.7
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

Table 3.1: Values of σ obtained from Theorem 3.2.11

For example, Table 3.1 displays that Theorem 3.2.11 misses the values $\sigma = 2, 3, 4$ for $p = 7$. We can recover the value $\sigma = 2$ by considering $t = 3$ in Theorem 3.2.7. The values $\sigma = 3$ and 4 occur by Corollary 3.2.10.

Column 1 shows that $p - 2$ is the smallest integral value obtained from Theorem 3.2.11. Corollary 3.2.10 provides smaller integral values of σ for all $p > 5$.

3.2.4 A_{p+s} Galois covers of the projective line

Let $p \geq 5$. Assume that $2 \leq s < p$ and A_{p+s} is the group of even permutations on $p + s$ elements. Let H_s be the group of even permutations on the set $\{p + 1, p + 2, \ldots, p + s\}$. The goal of Section 3.2.4 is to obtain similar results to Section 3.2.2 when $\pi : X \to \mathbb{P}^1_k$ is a Galois cover branched only at ∞ with Galois group A_{p+s}.

Abhyankar provided an equation as a starting point [2]. Let $\overline{f}_s = y^{p+s} - xy^s + 1$ where $2 \leq s < p$. He proved that the Galois closure $\tilde{F}_s$ of $F_s = k(x)[y]/(\overline{f_s})$ over $k(x)$ has Galois group A_{p+s} using the technique of the twisted derivative. There is a special case when $s = 2$, the Galois group is A_{p+s} when $p \neq 7$. Let X_s be the smooth curve corresponding to the function field $\tilde{F}_s$. Then there is an A_{p+s}-Galois covering $\pi : X_s \to \mathbb{P}^1_k$. The inertia group G_0 at a point of X_s lying over ∞ is of the form $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ where $p \nmid m$. Let h be the lower jump, so that $G_1 = G_2 = \cdots = G_h \cong \mathbb{Z}/(p)$ and $\{1\} = G_{h+1} = G_{h+2} = \cdots$.

Lemma 3.2.12. *The extension $F_s/k(x)$ is branched only at ∞. The extension contains two places $P_{(\infty,0)}$ and $P_{(\infty,\infty)}$ above ∞ with ramification index p and s respectively.*

Proof. There are no simultaneous solutions to the equations $\overline{f_s} = 0$ and $\partial\overline{f_s}/\partial y = 0$. Therefore the extension is not branched over any finite points. The Riemann-Hurwitz formula implies that all nontrivial extensions of $\mathbb{P}^1_k$ are ramified. Therefore the ramification of π must occur over ∞. There are two points $(\infty, 0)$ and (∞, ∞) of $Z(\overline{f_s})$ lying over ∞. The first point is obtained by applying the map $x \mapsto 1/x$ to $\overline{f_s}$. This produces the equation $xy^{p+s} - y^s + x$. Taking the partial derivative with respect to y yields the point $(\infty, 0)$. The second point is realized by applying the map $y \mapsto 1/y$ to $xy^{p+s} - y^s + x$ resulting in $x - y^p + xy^{p+s}$. Taking the partial derivative with respect to y yields the point (∞, ∞). Let $P_{(\infty,0)}$ and $P_{(\infty,\infty)}$ be the corresponding places of F_s. The ramification indices can be calculated in terms of the valuations at the places $P_{(\infty,0)}$ and $P_{(\infty,\infty)}$. For $P = P_{(\infty,0)}$ or $P_{(\infty,\infty)}$,

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

It follows that the ramification index is p when P is $P_{(\infty,0)}$ and the ramification index is s when P is $P_{(\infty,\infty)}$. □

Lemma 3.2.12 describes the ramification of the quotient extension. There is more that can be said about the extension using the twisted derivative.

Definition 3.2.13. *Let f be a nonconstant monic irreducible polynomial in $k(x)[y]$. Let α be a root of f in some extension of $k(x)$. Then the twisted derivative of f at α is defined to be*

$$D_\alpha f(y) = \frac{f(y+\alpha) - f(\alpha)}{y}.$$

The twisted derivative is $k(x)$-linear, and it satisfies a twisted power and twisted product rule.

The twisted derivative can be used to eliminate the roots of a polynomial f. Let $\tilde{F}$ be the splitting field of f so that $\tilde{F}/k(x)$ is Galois with Galois group G. Let α be a root of f in some extension of $k(x)$. Let $D_\alpha f$ be the twisted derivative of f at α. Then $\tilde{F}$ is the splitting field of $D_\alpha f$ over $k(x,\alpha)$. Consider G as a subgroup of some permutation group. Then the Galois group of $\tilde{F}/k(x,\alpha)$ is a one-point stabilizer of G.

Lemma 3.2.14. *[3] Let $\overline{f_s} = y^{p+s} - xy^s + 1$. Let $d_3 = \gcd(p-1, p+s)$ and α a root of $\overline{f_s}$ in some extension of $k(x)$. Let $D_\alpha \overline{f_s}$ be the twisted derivative of $\overline{f_s}$ at α and η a root of $D_\alpha \overline{f_s}$ in some extension of $k(x,\alpha)$. Then $D_\alpha \overline{f_s}$ yields the equation*

$$\alpha^{p+s} = \frac{\eta^s s^{p-1}}{(\eta+s)^p g(\eta)} \text{ where } g(\eta) = \sum_{i=1}^{t} \binom{t}{i} \eta^{t-i} t^{i-1}. \tag{3.2.1}$$

Proof. Let $h_{1,s} = y^{p+s}\overline{f_s}(1/y)$. The polynomial $h_{1,s}$ is the polynomial obtained by reciprocating the roots of $\overline{f_s}$. Let $h_{2,s}$ be the twisted derivative of $h_{1,s}$ at $1/\alpha$. Note that $h_{2,s}$ is a polynomial in $k(x,\alpha)[y]$. Let $h_{3,s} = y^{p+s-1}h_{2,s}(1/y)$. The polynomial $h_{3,s}$ is the polynomial obtained by reciprocating the roots of $h_{2,s}$. Let $h_{4,s} = (s\alpha)^{p+s-1}h_{3,s}(y/(s\alpha))$. The polynomial $h_{4,s}$ is the polynomial obtained by multiplying the roots of $h_{3,s}$ by $s\alpha$. Equation 3.2.1 is obtained by evaluating $h_{4,s}$ at η. The basic transformations of reciprocating the roots and multiplying the roots by $t\alpha$ do not change the Galois group. The effect of these transformations is purely cosmetic in order to obtain an explicit equation for α in terms η. □

Equation 3.2.1 explains the second level of ramification in Figure 3.9. Let $W_{(\infty,0,0)}$ be a place in the degree $p+s-1$ extension of $k(x,\alpha)$. Assume $W_{(\infty,0,0)}$ lies over $P_{(\infty,0)}$ with ramification index s. Let $W_{(\infty,0,i)}$ be a set of places in the degree $p+s-1$ extension of $k(x,\alpha)$. Assume the set of places $W_{(\infty,0,i)}$ lies over $P_{(\infty,0)}$ with each place having ramification index $(p-1)/d_3$. Define $W_{(\infty,\infty,j)}$ and $W_{(\infty,\infty,1)}$ similarly. The denominator in Equation 3.2.1 explains the ramification that occurs over $P_{(\infty,\infty)}$ in Figure 3.9. The factor $(y+s)^p$ corresponds to the ramified place $W_{(\infty,\infty,1)}$, with ramification index p. The factor $g(\eta)$ corresponds to the set of unramified places $W_{(\infty,\infty,j)}$. The numerator in Equation 3.2.1 explains the ramification that occurs over $P_{(\infty,0)}$ in Figure 3.9. The factor η^s corresponds to the ramified place $W_{(\infty,0,0)}$, with ramification index s. The factor t^{p-1} corresponds to the set of ramified places $W_{(\infty,0,i)}$, with ramification index $(p-1)/d_3$.

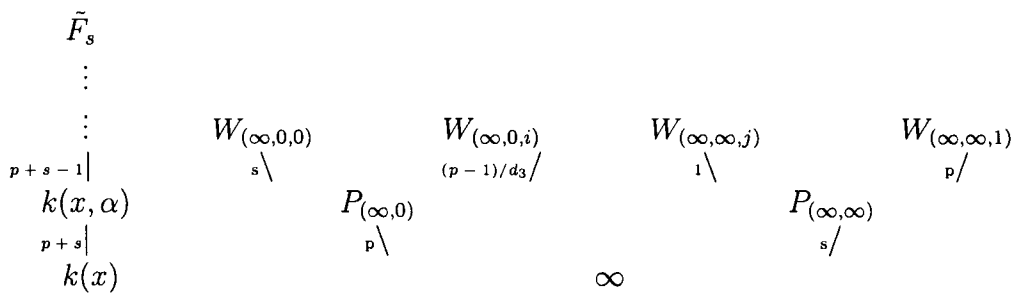

Figure 3.9: Ramification over ∞ [3].

Theorem 3.2.15. *Let $2 \leq s < p$ and $d_3 = \gcd(p-1, p+s)$. If $s = 2$ assume that $p \neq 7$. There exists an A_{p+s}-Galois cover $\pi : X \to \mathbb{P}^1_k$ branched only at ∞. The inertia group has size pm for some m with $p \nmid m$, and the upper jump is $\sigma = (p+s)/(p-1)$.*

Proof. Consider $\pi : X_s \to \mathbb{P}^1_k$ defined above. Abhyankar's work implies that π is an A_{p+s}-Galois cover. A proof similar to the proof of Lemma 3.2.4 shows that ∞ is the only branch point of π.

Let Q be any place in $\tilde{F}_s$ lying above ∞. The extension $\tilde{F}_s/k(x)$ is wildly ramified at Q with $p^2 \nmid e(Q|\infty)$. Let G_0 be the inertia group at Q, then $|G_0| = pm$ for some integer m where $p \nmid m$.

The Newton polygon of π is the same as the Newton polygon $\overline{\Delta}_s$ calculated in Lemma 3.1.24. Therefore the lower jump h of π is the negative of the slope of the decreasing line segment of $\overline{\Delta}_s$. It follows that $h = m(p+s)/(p-1)$ is an integer. Lemma 3.1.16(4) implies that the upper jump σ is $(p+s)/(p-1)$. □

Let $\pi : X_s \to \mathbb{P}^1_k$ be the cover from Theorem 3.2.15. Let G_0 be the inertia group at some point Q of $\tilde{F}_s$ over ∞. Since $p^2 \nmid |G_0|$ we may assume that $G_0 = \langle\tau\rangle \rtimes \langle\beta\rangle$ where $\tau = (12\cdots p)$ and $\beta \in A_{p+s}$ with $|\beta| = m$. Let σ be the upper jump of π at Q. There are some necessary conditions that σ must satisfy. The upper jump $\sigma = h/m > 1$, $p \nmid h$, and $m|(p-1)s!/2$. These conditions follow from the Riemann-Hurwitz formula and Lemma 3.1.18. Furthermore, let $\gcd(h,m) = m'$ and $m_1 = m/m'$. Then Lemma 3.1.20 implies $\beta^{m'} \notin C_{A_{p+s}}(\langle\tau\rangle)$. Therefore m_1, the order of $\beta^{m'}$, must divide $p-1$.

Corollary 3.2.16. *Let* $\gcd(p-1, p+4)$. *Then all but finitely many upper jumps* σ *occur for an* A_{p+4}*-Galois cover of the projective line branched only at* ∞.

Proof. Theorem 3.2.15 implies that an A_{p+4}-Galois cover of $\mathbb{P}^1_k$ branched only at ∞ exists. Furthermore $\sigma = (p+4)/(p-1)$. The corollary follows from Lemma 3.2.3 and Theorem 3.2.9. □

Let G be a quasi-p group with order strictly divisible by p. Let P be a Sylow-p subgroup. Suppose the prime to p part of the center of $N_G(P)$ is trivial. Then the inertia conjecture for G is equivalent to the statement that all but finitely many σ occur for G. Unfortunately when $G = A_{p+4}$ this is not the situation since $p < |C_{A_{p+4}}(\langle\tau\rangle)|$. However it gives some motivation to consider $C_{A_{p+s}}(\langle\tau\rangle)$ in general. The size of G_0 is restricted by the size of $C_{A_{p+s}}(\langle\tau\rangle)$. The goal of the next two lemmas is to place restrictions on m.

Lemma 3.2.17. *Let d_3, s, m, and π be defined as in Theorem 3.2.15. Let h be the lower jump of G_0 and $m' = \gcd(h, m)$. Then $m = (p-1)m'/d_3$ and $m' = sr/\gcd(s, p-1)$ for some positive integer r.*

Proof. The ramification indices that occur in Figure 3.9 force the order of G_0 to be divisible by $p(p-1)s/(d_3 \cdot \gcd(s, p-1))$. So, for some positive integer r,

$$|G_0| = \frac{p(p-1)sr}{d_3 \cdot \gcd(s, p-1)}.$$

Theorem 3.2.15 implies that the upper jump is $\sigma = (p+s)/(p-1)$. Therefore we can solve for

$$h = \frac{m'(p+s)}{d_3} \text{ and } m = \frac{m'(p-1)}{d_3}.$$

The size of the inertia group is pm. Considering m and $|G_0|$ above results in $m' = sr/\gcd(s, p-1)$. □

Corollary 3.2.18. *Let $2 < l^c < p$ where l is a prime such that $l \nmid (p-1)$ and c is a positive integer. Let $d_4 = \gcd(p-1, p+l^c)$. Then there exists an A_{p+l^c} Galois cover of $\mathbb{P}^1_k$ branched only at ∞ with ramification group having order $p(p-1)l^c/d_4$ and upper jump $\sigma' = (p+l^c)/(p-1)$.*

Proof. Theorem 3.2.15 implies that there exists such a cover with an inertia group $G_0 = \langle\tau\rangle \rtimes \langle\beta\rangle$ where $|\beta| = m$. Let h be the lower jump, and $m' = \gcd(h, m)$. Let $\beta_1 = \beta^{m/m'}$, then Lemma 3.1.20 implies that $C_{G_0}(\langle\tau\rangle) = \langle\tau\rangle \times \langle\beta_1\rangle$. Notice that β_1 is disjoint from τ since β_1 commutes with τ. Therefore $\beta_1 \in H_s$. Now, s divides the order of β_1. When $s = l^c$ there is only one possibility for $\beta_1 \in H_s$, namely $\beta_1 = (p+1, p+2, \ldots, p+s)$. The results follow since $\gcd(l^c, p-1) = 1$. □

Corollary 3.2.19. *Let l^c and d_4 be defined as in Corollary 3.2.18. Then there exists an A_{p+l^c}-Galois cover $\pi : X \to \mathbb{P}^1_k$ branched only at ∞ with the genus of X being*

$$g = 1 + \frac{|A_{p+l^c}|}{2}\left(-1 - \frac{d_4}{p(p-1)l^c} + \frac{p+l^c}{p}\right).$$

Proof. The proof is immediate from the Riemann-Hurwitz formula and Corollary 3.2.19. □

The significance of Corollary 3.2.18 is that it eliminates any ambiguity in the order of the inertia group G_0 from Theorem 3.2.17. For example if $s = 3$ and $p > 3$, Corollary 3.2.18 implies that $|G_0| = 3p(p-1)/\gcd(p-1, 4)$. When s is not a power of a prime there is still more that can be said about the size of G_0. In Corollary 3.2.18 we use the size of $C_{G_0}(\langle\tau\rangle)$ to restrict the size of G_0. In the following lemma we use the ramification that occurs in the quotient extension in Figure 3.10 to restrict the size of G_0.

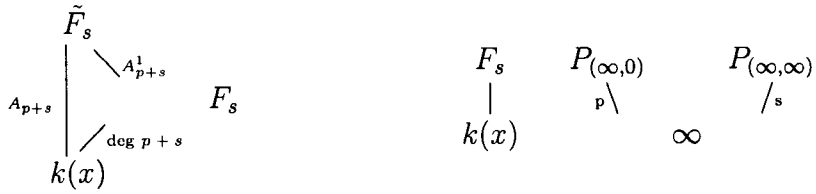

Figure 3.10: A sub and quotient extensions of $\tilde{F}_s/k(x)$.

Corollary 3.2.20. *Let* $\gcd(s, p-1) = 1$. *Let* d_3, s, m, *and* π *be defined as in Theorem 3.2.15. Let* h *be the lower jump of* G_0 *and* $m' = \gcd(h, m)$. *Then* $m = (p-1)m'/d_3$, *and for any prime* $l|m'$ *implies the=at* $l|s$.

Proof. Let $G_0 = \langle \tau \rangle \rtimes \langle \beta \rangle$ where $|\beta| = m$. Assume $m' = l_1^{c_1} \cdots l_w^{c_w}$, and let

$$\beta_i = \beta^{m/l_i}.$$

Then β_i is a l_i-cycle in G_0. Since A_{p+s} is transitive on the set $\{1, 2, \ldots, p\}$, there exists a $\gamma \in A_{p+s}$ such that $\gamma\beta_i\gamma^{-1} \notin A^1_{p+s}$. Therefore $\gamma\beta_i\gamma^{-1}$ is a l_i-cycle in the inertia group $\gamma G_0 \gamma^{-1}$ at some place $\tilde{Q} \in \tilde{F}_s$. Notice that $(\gamma\beta_i\gamma^{-1})^j$ is a l_i-cycle for every $1 \leq j < l_i$. The fact that $\gamma\beta_i\gamma^{-1} \notin A^1_{p+s}$ implies that some non trivial power of it must occur as ramification in the quotient extension in Figure 3.10. Therefore $l_i|p$ or $l_i|s$. Since the size of A_{p+s} is strictly divisible by p, l_i must divide s. □

When $\gcd(s, p-1) = 1$, Corollary 3.2.20 implies that for many values of s, the value m' is forced to be s. Therefore the size of the inertia group is determined. In fact $m' = s$ for all $s = l_1^{c_1} \cdots l_w^{c_w}$ such that $l_i^{c_i+1} > s - \sum_{j=1}^{w} l_j^{e_j}$ for each $1 \leq i \leq w$. The first value of s such that m' might not equal s is $s = 21$. This is because it is possible for A_{21} to contain an element of order $3 \cdot 21$ corresponding to a $9, 7$-cycle.

A similar statement to that of Corollary 3.2.19 can be stated for each s such that m' is forced to be s.

3.2.5 Support for the Inertia Conjecture

Corollary 3.2.21. *[4] The Inertia Conjecture is true for $G = A_p$. Every subgroup $G_0 = \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ of A_p can be realized as the inertia group of an A_p-Galois cover of $\mathbb{P}^1_k$ branched only at ∞.*

Proof. Let $\pi : X \to \mathbb{P}^1_k$ be a wildly ramified A_p-Galois cover branched only at ∞. Let G_0 be the inertia group at some point $Q \in X$. Lemmas 3.1.16(1) and 3.1.17 imply that $G_0 \cong \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ and $G_0 \subset \langle \tau \rangle \rtimes \langle \beta \rangle$ for some $\beta \in A_p$ with $|\beta| = (p-1)/2$. For the value $t = 2$, Theorem 3.2.7 shows the existence of the inertia group G_0 having size $p(p-1)/2$. Corollary 3.2.3 implies that the Inertia Conjecture for $G = A_p$. □

Corollary 3.2.22. *Let $p \equiv 2$ mod 3. The Inertia Conjecture is true for $G = A_{p+2}$. Every subgroup $G_0 = \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ of A_{p+2} can be realized as the inertia group of an A_{p+2}-Galois cover of $\mathbb{P}^1_k$ branched only at ∞.*

Proof. Let $\pi : X \to \mathbb{P}^1_k$ be a wildly ramified A_{p+2}-Galois cover branched only at ∞. Let G_0 be the inertia group at some point $Q \in X$. Lemmas 3.1.16(1) and 3.1.18 imply that $G_0 \cong \mathbb{Z}/(p) \rtimes \mathbb{Z}/(m)$ and $G_0 \subset \langle \tau \rangle \rtimes \theta_1 \rangle$ for some $\theta_1 \in A_{p+2}$ with $|\theta_1| = p - 1$. For the value $s = 2$, and m' and d_3 defined as in Lemma 3.2.17, Lemma 3.2.17 produces an inertia group of order $pm'(p-1)/d_3$. Notice that $m' = 1$ since the prime to p part of $C_{A_{p+2}}(\langle \tau \rangle)$ is trivial. Furthermore $d_3 = 1$ when $p \equiv 2$ mod 3. Hence $|G_0| = p(p-1)$. The inertia conjecture follows for the Galois group A_{p+2} from Corollary 3.2.3. □

Chapter 4

CONCLUSION

The result of Chapter 2 determined the zeta function of a curve with two ordinary singular points at infinity. Proposition 2.5.1 verifies that there is a relationship between the zeta function of a curve and the zeta function of the normalization of that curve. Future work will determine the zeta functions of singular curves besides for the one considered in Chapter 2.

The results of Chapter 3 found evidence to support Abhyankar's Inertia Conjecture. For a Galois cover $\pi : X \to \mathbb{P}^1_k$, Chapter 3 developed a method for determining the size of an inertia group at ∞ of a Galois extension if we were provided an equation for any non-Galois quotient extension. We obtained results supporting the conjecture for certain alternating groups. In the future I would like to find supporting evidence for the Inertia conjecture for all the groups that were considered in Question 2. Abhyankar also has provided equations corresponding to Galois covers with Galois groups besides for the alternating groups considered. In the future I will apply the technique of Chapter 3 to these covers with a goal of finding more evidence to support the Inertia conjecture.

Bibliography

[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. Alternating group coverings of the affine line for characteristic greater than two. *Math. Ann.*, 296(1):63–68, 1993.

[4] Irene I. Bouw and Rachel J. Pries. Rigidity, reduction, and ramification. *Math. Ann.*, 326(4):803–824, 2003.

[5] Francis N. Castro and Carlos J. Moreno. L-functions of singular curves over finite fields. *J. Number Theory*, 84(1):136–155, 2000.

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

[7] Joe Harris. *Algebraic geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. A first course, Corrected reprint of the 1992 original.

[8] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[9] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[10] Dino Lorenzini. *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1996.

[11] 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.

[12] Rachel J. Pries. Conductors of wildly ramified covers. II. *C. R. Math. Acad. Sci. Paris*, 335(5):485–487, 2002.

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

[14] John Scherk. The ramification polygon for curves over a finite field. *Canad. Math. Bull.*, 46(1):149–156, 2003.

[15] 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.

[16] Henning Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.

[17] Helmut Völklein. *Groups as Galois groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996. An introduction.