GALOIS EXTENSIONS RAMIFIED AT ONE PRIME

Jing Long Hoelscher

A Dissertation

in

Mathematics

Presented to the Faculties of the University of Pennsylvania in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

2007

David Harbater
Supervisor of Dissertation

Ching-Li Chai
Graduate Group Chairperson

Acknowledgments

I want to use this page to express my appreciation to all the many people who made my five-year stay in the graduate program at the University of Pennsylvania a remarkable and fulfilling experience.

First I would like to thank my advisor David Harbater, who has very generously spent his time and energy on supervising me with my work. He greatly assisted me with my writing and continually stimulated my thinking.

My special thanks go to my husband Corey Hoelscher, who has always been there for me, enjoying my happiness and sharing my worries.

I also want to devote my thanks to the other two members of my dissertation committee, Florian Pop and Ted Chinburg, who have provided my with a lot of help and suggestions during their busy semesters; and to Stephen Shatz, who has consistently supported me and encouraged me during my difficult times.

ABSTRACT

GALOIS EXTENSIONS RAMIFIED AT ONE PRIME

Jing Long Hoelscher

David Harbater, Advisor

This thesis studies Galois extensions of global fields and associated Galois groups with one ramified prime, in both the number field and function field cases. Over $\mathbb{Q}$ some restrictions on both solvable and nonsolvable Galois groups ramified only at one prime are shown. We also give a description of tamely ramified meta-abelian Galois groups and examples of infinite class field towers with one finite prime ramified. Over real quadratic fields $\mathbb{Q}(\sqrt{d})$, results about nilpotent Galois groups ramified only at one prime in $\mathbb{Q}(\sqrt{d})$ are shown. Over function fields $\mathbb{F}_q(t)$, a stronger version of the forward direction of "Abhyankar's conjecture" is proved. Finally, we give a simple description of cyclotomic function fields with a view toward developing Iwasawa theory for cyclotomic function fields.

Contents

List of Tables

Chapter 1

Introduction

1.1 Overview

One of the most fundamental problems of Galois theory is that of determining which finite groups can occur as Galois groups over a given field. For an algebraically closed field K, this inverse Galois problem is solved affirmatively for $K(t)$, i.e. *every* finite group occurs as a Galois group over $K(t)$ (see Corollary 1.5 in [Ha1]). Over the field $\mathbb{Q}$ and function fields $\mathbb{F}_q(t)$ over a finite field $\mathbb{F}_q$, the same is believed to be true but the problem remains open.

In both the function field and number field cases, one can also ask about the "fine structure" of the inverse Galois problem, i.e. which groups occur as Galois groups with specified ramifications? In the function field case, this means studying Galois groups of finite branched covers of projective curves X with specified branch locus. In the number field case, it deals with the Galois groups over a number field F ramified only at a given finite set of primes of F. In both cases we know that *not* every finite group occurs with prescribed ramification. As the number and the size of ramified primes increases, more finite groups are allowed to occur as Galois groups. And in the "limit", we expect all finite groups to occur. This thesis is concerned with descriptions of finite groups that can occur as Galois groups with given ramifications, or which can be ruled out.

In the case of function fields, my focus is on curves over finite fields. On the other hand, over an algebraically closed field k of characteristic p, the situation is better understood. There, a precise form of the above question was posed in Abhyankar's Conjecture [Ab], which was proved by M. Raynaud [Ra] and D. Harbater [Ha2]. Namely, given a smooth connected projective k-curve X with genus g and a finite set S of $n > 0$ closed points of X, we may consider the set $\pi_A(X-S)$ of finite groups that occur as Galois groups over X with ramification only at S. Let $U = X - S$; then $\pi_A(U)$ consists of all finite quotients of the fundamental group $\pi_1(U)$. For a finite group G, let $p(G)$ denote the subgroup of G generated by the subgroups of p-power order. We call a finite group G a *quasi-p group* if $G = p(G)$. Abhyankar's

conjecture says that a necessary and sufficient condition for a finite group G to be in $\pi_A(U)$ is that $G/p(G)$ can be generated by a set of at most $2g+n-1$ elements. A consequence of Abhyankar's conjecture is that

$$\pi_A(\mathbb{A}^1) = \{\text{quasi-}p \text{ groups}\}.$$

It is unknown precisely which groups are Galois groups of *tamely* ramified covers of U, but each must have at most $2g+n-1$ generators.

This last assertion carries over to curves over a finite field $\mathbb{F}_q$, if one restricts to *geometric* curves (with no extensions of constants), since base change to $\bar{\mathbb{F}}_q(t)$ does not change the Galois group (see Proposition 1.2.15 below). In fact, if we allow extensions of constants, there will be one more generator, i.e. the Frobenius. In the case of function fields over finite fields, we count the number of ramified primes according to their degree; here $\deg(\mathfrak{p}) = \log_q(\text{Norm}(\mathfrak{p}))$. Motivated by this and the analogy between function fields and number fields, Harbater posed a corresponding conjecture in [Ha3] for the open set $U_n = \text{Spec}(\mathbb{Z}[\frac{1}{n}])$ of $\text{Spec}(\mathbb{Z})$:

CONJECTURE 1.1.1. *[Harbater, 1994] There is a constant C such that for every positive square free integer n, every group in $\pi_A^t(U_n)$ has a generating set with at most $\log n + C$ elements.*

That is, if $G \in \pi_A^t(U_n)$, i.e. G is a Galois group over $\mathbb{Q}$ ramified only at primes p dividing n and each p does not divide its ramification index e_p, then the growth of the number of generators of G is asymptotic to $\log(n)$. Also note that if $G \in \pi_A(U_n)$, Conjecture 1.1.1 implies that $G/p(G)$ has at most $\log n + C$ generators, which is relevant to Corollary 1.4.2 below. Harbater has some results in [Ha3] for the case $n = 2$, which can be regarded as evidence for this conjecture. I have extended his results to bigger primes. In addition I prove a stronger version of the conjecture in the case of function fields over finite fields.

This thesis describes finite groups that can occur as Galois groups over number fields or function fields $\mathbb{F}_q(t)$ with only one prime ramified. For abelian Galois groups, class field theory provides a complete answer to both situations. In the solvable case, Section 2.1, we apply class field theory and group theory to towers of abelian extensions to get some restrictions on solvable groups that can occur as Galois groups over $\mathbb{Q}$ ramified at only one prime. Theorem 2.1.1 and its corollaries generalize some results in [Ha3] to give more evidence for the Conjecture 1.1.1. We also give a complete description of tamely ramified meta-abelian extensions over $\mathbb{Q}$. In Section 2.2, where the group needs not be solvable, finite towers of abelian extensions do not suffice. There we use the Odlyzko discriminant bound, local class field theory and group theory to rule out certain non-solvable groups as Galois groups over $\mathbb{Q}$ ramified only at one prime. In Section 2.3, some examples of infinite class field towers ramified only at one prime are shown, where class field theory and group cohomology are used. In Section 2.4, we show some results about nilpotent groups as Galois groups over a quadratic number field using class field theory. In

Chapter 3, by combining the Frobenius action with the branch cycle description of a lift of a tame cover to characteristic 0, we give some restriction on Galois groups occurring tamely over function fields $\mathbb{F}_q(t)$. We also present a "hands-on" description of cyclotomic function fields and take steps to develop Iwasawa theory for cyclotomic function fields.

1.2 Background

In this section, we will review some background material that will be necessary in what follows.

1.2.1 Class Field Theory

Let K denote a field complete under a discrete valuation, L be a finite separable extension of K. Serre has a very nice description of the inertia group:

COROLLARY 1.2.1 ([Se3], Corollary 4). *Assume the characteristic of the residue field of L is $p > 0$. The inertia group I is the semi-direct product of a cyclic group of order prime to p with a normal subgroup whose order is a power of p.*

In a number field K, an *idèle* $\alpha = (\alpha_{\mathfrak{p}})$ is a tuple $(\alpha_{\mathfrak{p}})$ of elements $\alpha_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$, where $\alpha_{\mathfrak{p}}$ is a unit in the ring $\mathcal{O}_{\mathfrak{p}}$ of the integers of $K_{\mathfrak{p}}$, for all most all $\mathfrak{p}$. The *idèle group* I_K (i.e. the set of all *idèle*s) of K is the restricted product of $K_{\mathfrak{p}}^*$'s with respect to the unit groups $\mathcal{O}_{\mathfrak{p}}^*$,

$$I_K = \prod_{\mathfrak{p}} K_{\mathfrak{p}}^*.$$

The quotient group $C_K = I_K/K^*$ is called the *idèle class group*. Given a modulus $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$, define

$$U_{\mathfrak{p}}^{n_{\mathfrak{p}}} = \begin{cases} 1 + \mathfrak{p}^{n_{\mathfrak{p}}}, & \text{if } \mathfrak{p} \nmid \infty \\ \mathbb{R}_+^* \subset K_{\mathfrak{p}}^*, & \text{if } \mathfrak{p} \text{ is real} \\ \mathbb{C}^* = K_{\mathfrak{p}}^*, & \text{if } \mathfrak{p} \text{ is complex} \end{cases}$$

The *congruence subgroup* $C_K^{\mathfrak{m}} = I_K^{\mathfrak{m}} K^*/K^*$ mod $\mathfrak{m}$ is formed from the idèle group $I_K^{\mathfrak{m}} = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$. The *ray class field* $K^{\mathfrak{m}}$ mod $\mathfrak{m}$ is the class field $K^{\mathfrak{m}}/K$ for the congruence subgroup $C_K^{\mathfrak{m}}$, which satisfies canonically

$$\mathrm{Gal}\,(K^{\mathfrak{m}}/K) \cong C_K/C_K^{\mathfrak{m}}.$$

PROPOSITION 1.2.2 ([Ne], Corollary 6.3). *Every finite abelian extension L/K is contained in a ray class field $K^{\mathfrak{m}}/K$ for some module $\mathfrak{m}$.*

In the case $\mathfrak{m} = 1$, the ray class field $K^{\mathfrak{m}}$ is the big Hilbert class field, which is the maximal unramified abelian extension of K.

PROPOSITION 1.2.3 ([Ne], Exercise 13, Page 368). *For every module $\mathfrak{m}$, one has an exact sequence*

$$1 \longrightarrow \mathcal{O}_+^*/\mathcal{O}_+^{\mathfrak{m}} \longrightarrow (\mathcal{O}/\mathfrak{m})^* \longrightarrow Cl_K^{\mathfrak{m}} \longrightarrow Cl_K^1 \longrightarrow 1,$$

where $\mathcal{O}_+^*$, resp. $\mathcal{O}_+^{\mathfrak{m}}$, is the group of totally positive units of $\mathcal{O}$, resp. of totally positive units $\equiv 1$ mod $\mathfrak{m}$.

The Hilbert class field, also called the small Hilbert class field, is defined to be the maximal unramified abelian extension H/K in which all infinite places split completely. The Galois group $G = \mathrm{Gal}\,(H/K)$ is canonically isomorphic to the ideal class group of K.

PROPOSITION 1.2.4 ([Ne], Theorem 7.5). *In the Hilbert class field H of K, every ideal $\mathfrak{a}$ of K becomes a principal ideal.*

For the class number of a p-extension over $\mathbb{Q}$, there is a useful result by Harbater:

PROPOSITION 1.2.5 ([Ha3], Proposition 2.8). *Let p and q be (possibly equal) prime numbers. Let G be a p-group, and let $\mathbb{Q} \subset K$ be a G-Galois extension ramified only at q.*

(a) The extension $\mathbb{Q} \subset K$ is totally ramified over q.

(b) The class number of K is prime to p.

1.2.2 Discriminant Bounds

In the case the Galois group is non-solvable, we will use the upper bound and the lower bound on discriminants of Galois extensions to rule out some finite groups. In class field theory, we have an upper bound for the discriminant:

THEOREM 1.2.6 ([Ne], Theorem 2.6). *Suppose L/K is a Galois extension of algebraic number fields with $[L : K] = n$ and $\mathfrak{p}$ is a prime ideal of the ring $\mathcal{O}_K$ of integers of K. Then $\mathfrak{p}$ is ramified in L/K if and only if $\mathfrak{p} \mid \mathfrak{d}_{L/K}$, where $\mathfrak{d}_{L/K}$ is the discriminant of L/K. Furthermore, let $\mathfrak{p}^s$ be the maximal power of $\mathfrak{p}$ dividing $\mathfrak{d}_{L/K}$, and let e be the ramification index of $\mathfrak{p}$ in L/K. Then one has:*

$$\begin{cases} s = n(1 - \frac{1}{e}) & \text{if } \mathfrak{p} \text{ is tamely ramified,} \\ n \leq s \leq n(1 - \frac{1}{e} + v_{\mathfrak{p}}(e)) & \text{if } \mathfrak{p} \text{ is wildly ramified.} \end{cases} \tag{1.2.7}$$

For the lower bound, we have the Odlyzko discriminant bound:

PROPOSITION 1.2.8 ([Od], Corollary 1). *Let K be any algebraic number field, $\mathfrak{d}_{K/\mathbb{Q}}$ the absolute value of the discriminant of K, and r_1 and $2r_2$ the numbers of real and complex conjugate fields, respectively. Then*

$$\mathfrak{d}_{K/\mathbb{Q}} \geq (60.1)^{r_1}(22.2)^{2r_2}e^{-254}; \tag{1.2.9}$$

$$\mathfrak{d}_{K/\mathbb{Q}} \geq (58.6)^{r_1}(21.8)^{2r_2}e^{-70}. \tag{1.2.10}$$

If the zeta function of K satisfies the General Riemann Hypothesis (GRH), then

$$\mathfrak{d}_{K/\mathbb{Q}} \geq (188.3)^{r_1}(41.6)^{2r_2}e^{-3.7\times 10^8}. \tag{1.2.11}$$

1.2.3 Fundamental Groups

Let X be a smooth connected projective k-curve and U an open subset of X. Denote k^{ac} the algebraic closure of k. The *algebraic* (or *étale*) *fundamental group* $\pi_1(U)$ is defined to be the inverse limit of the inverse system of groups occurring as Galois groups of pointed étale Galois covers of U (see SGA I [Gro]). Define $\pi_A(U)$ to be the set of finite quotients of the algebraic fundamental group $\pi_1(U)$, i.e. the set of the finite groups that can occur as Galois group of étale Galois covers of U. In the situation $\mathrm{char}(k) = p > 0$, denote $\pi_A^t(U)$ the set of Galois groups of tamely ramified covers (these groups may have order divisible by p), and $\pi_A^{p'}(U)$ the set of Galois groups of étale Galois cover of U with order prime to p. In situation $\mathrm{char}\, k = 0$, we can still talk about $\pi_A^{p,t}(U)$ and $\pi_A^{p'}(U)$ after we fix a prime p.

Case ($k = \mathbb{C}$). In this classical case, the situation is well understood by Riemann's Existence Theorem:

THEOREM 1.2.12 (Riemann's Existence Theorem). *Let X be a smooth connected complex projective curve with genus g, and $U = X - \{\xi_1, ..., \xi_n\}$ with $n \geq 0$ be an open subset of X. Then the algebraic fundamental group $\pi_1(U)$ is the profinite completion of the topological fundamental group*

$$\pi_1^{\mathrm{top}}(U) = \langle a_1, ..., a_g, b_1, ..., b_g, c_1, ..., c_n \mid \prod_{i=1}^{g}[a_i, b_i]\prod_{j=1}^{n} c_j = 1\rangle$$

So in the complex case, if $n > 0$, the algebraic fundamental group $\pi_1(U)$ is isomorphic to the free profinite group on $2g+n-1$ generators, and $\pi_A(U)$ consists of the finite groups having $2g+n-1$ generators. Fix a prime p; then $\pi_A^{p,t}(U)$ consists of the finite groups on $2g+n$ generators, $\{a_1, ..., a_g, b_1, ..., b_g, c_1, ..., c_n\}$, subject to the relations $\prod_{i=1}^{g}[a_i, b_i]\prod_{j=1}^{n} c_j = 1$ and $p \nmid \mathrm{ord}(c_i)$ for all $i = 1, ..., n$, whereas $\pi_A^{p'}(U)$ consists of the finite groups on $2g+n-1$ generators and of order prime to p, with an injective map $\pi_A^{p'}(U) \hookrightarrow \pi_A^t(U)$.

Case ($k = k^{ac}$ & $\mathrm{char}(k) = 0$). More generally, we can consider the case k is any algebraically closed field of characteristic 0. Grothendieck [Gro] has shown the algebraic fundamental group $\pi_1(U)$ is also the free profinite group on $2g+n-1$ generators, and $\pi_A(U)$, $\pi_A^{p'}(U)$ and $\pi_A^{p,t}(U)$ (for a fixed prime p) are also the same as in the situation when $k = \mathbb{C}$.

Case ($k = k^{ac}$ & $\mathrm{char}(k) = p > 0$). Now we consider the case when k is still algebraically closed, but of characteristic $p > 0$. Less is known in this situation. The main result is Harbater and Raynaud's proof of the Abhyankar Conjecture:

THEOREM 1.2.13 (Abhyankar Conjecture, proved by Harbater [Ha2], Raynaud [Ra]). *Let X be a smooth connected projective curve with genus g over an algebraically closed field k of characteristic $p > 0$, and $U = X - \{\xi_1, ..., \xi_n\}$ with $n > 0$. Then*

$$\pi_A(U) = \{G \mid G/p(G) \ \ has \ \ 2g + n - 1 \ \ generators\}.$$

As a consequence, the condition $G \in \pi_A(U_{\mathbb{C}})$ implies $G \in \pi_A(U_k)$. We know $\pi_A^{p'}(U)$ is the same as in the situation when k is algebraically closed and of characteristic 0. For $\pi_A^t(U)$, it is strictly smaller than the counterpart in the characteristic 0 algebraically closed situation. In fact we know

$$\pi_A^{p'}(U_k) \subseteqq \pi_A^t(U_k) \subsetneqq \pi_A^{p,t}(U_{\mathbb{C}}).$$

Here is an example for the strictness for $\pi_A^t(U_k) \subsetneqq \pi_A^{p,t}(U_{\mathbb{C}})$.

Example 1.2.14. Assume $\mathrm{char}(k) = p \neq 2$, and $\lambda \in \mathbb{P}^1_{\mathbb{C}}$. Let $E/\mathbb{P}^1_{\mathbb{C}}$ be the branched cover of degree 2 and branched at $\{0, 1, \infty, \lambda\}$; thus E is an elliptic curve. We can take the maximal unramified elementary abelian p-cover E'/E with $\mathrm{Gal}\,(E'/E) \cong (\mathbb{Z}/p)^2$, and $E'/\mathbb{P}^1_{\mathbb{C}}$ is a Galois cover with Galois group $G = (\mathbb{Z}/p)^2 \rtimes \mathbb{Z}/2$; so $G \in \pi_A^{p,t}(U_{\mathbb{C}})$ for $U_{\mathbb{C}} = \mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty, \lambda\}$.

$$\begin{array}{c} E' \\ \Big| \ (\mathbb{Z}/p)^2 \\ E \\ \Big| \ \mathbb{Z}/2 \\ \mathbb{P}^1_{\mathbb{C}} \end{array}$$

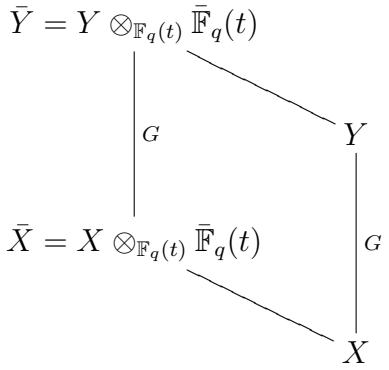
But $G \notin \pi_A^t(U_k)$, since any G-Galois cover of U_k has to be wildly ramified somewhere. To see this, take a Galois cover $E'^*/\mathbb{P}^1_k$ with Galois group G. It will dominate a degree 2 cover $E^*/\mathbb{P}^1_k$ unbranched away from $\{0, 1, \infty, \lambda'(\in k)\}$.

$$\begin{array}{c} E'^* \\ \Big| \ (\mathbb{Z}/p)^2 \\ E^* \\ \Big| \ \mathbb{Z}/2 \\ \mathbb{P}^1_k \end{array}$$

But the p-rank of E^* is either 0 or 1, since the genus of E^* is at most 1. Thus E^* has no connected unramified cover of Galois group $(\mathbb{Z}/p)^2$, so $E'^*/\mathbb{P}^1_k$ has be wildly ramified somewhere. Thus $G \notin \pi^t_A(U_k)$.

It is unknown what exactly $\pi^t_A(U_k)$ is, but each finite group in $\pi^t_A(U)$ has $2g+n-1$ generators ([Gro], XIII, Corollary 2.12). As for $\pi_1(U)$, it is still very much unknown although we know the finite quotients.

Case ($k = \mathbb{F}_q$). We restrict only to regular covers Y/X, i.e. k is algebraically closed in the function field of Y. Given such a regular cover, we can lift it to $\bar{\mathbb{F}}_q$.



So G corresponds to a cover $\bar{Y}/\bar{X}$ in the algebraic closure $\bar{\mathbb{F}}_q$. If Y/X is a tame cover, so is $\bar{Y}/\bar{X}$. Due to Grothendieck, G has at most $2g + n - 1$ generators, where g is the genus of the k-curve X. Say a point $\mathfrak{p}$ splits into $\deg(\mathfrak{p})$ points over $\bar{\mathbb{F}}_q$. Thus counting the number of ramified primes according to their degree $\deg(\mathfrak{p}) = \log_q(\mathrm{Norm}(\mathfrak{p}))$, we have the following:

PROPOSITION 1.2.15. *Let X be a smooth projective curve over a finite field $\mathbb{F}_q$. Then there exists a constant C such that for all open subsets $U = X - D \subset X$, where D is an effective divisor of X, every group in $\pi^t_A(U)$ has a generating set with at most $\log_q(\mathrm{Norm}(D)) + C$ elements.*

1.3 Analogy between number fields and function fields

There are various analogies between algebraic number fields and algebraic function fields of one variable, as shown by A. Weil (see [We]), Dinesh Thakur (see [Th]), etc. Let K be an algebraic number field. An archimedean prime $\mathfrak{p}$ is real or complex depending on whether or not the completion $K_\mathfrak{p}$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. The real primes are given by embeddings $\tau : K \longrightarrow \mathbb{R}$, and the complex primes are induced by the pairs of complex conjugate non-real embeddings $\tau : K \longrightarrow \mathbb{C}$. If $K_\mathfrak{p}$ is a p-adic field, then $\mathfrak{p}$ corresponds to a nonarchimedean finite prime. Given any $\alpha \in K$,

number fields	function fields
the rational number field $\mathbb{Q}$	the rational function field $\mathbb{F}_q(t)$
the rational integer ring $\mathbb{Z}$	the polynomial ring $\mathbb{F}_q[t]$
the completion $\mathbb{R}$ of $\mathbb{Q}$	the Laurent series field $\mathbb{F}_q((\frac{1}{t}))$
an algebraic closure $\mathbb{C}$ of $\mathbb{R}$	the completion of an algebraic closure of $\mathbb{F}_q((\frac{1}{t}))$

Table 1.1: Basic analogies between $\mathbb{Q}$ and $\mathbb{F}_q(t)$

for each $\mathfrak{p}$ of K, we can associate a corresponding valuation $v_\mathfrak{p}$ as follows:

$$v_\mathfrak{p}(\alpha) = \begin{cases} \log(\mid \tau\alpha \mid) & \text{if } K_\mathfrak{p} \text{ is a real infinite prime,} \\ 2\log(\mid \tau\alpha \mid) & \text{if } K_\mathfrak{p} \text{ is a complex infinite prime,} \\ -v_\mathfrak{p}(\alpha)\log(\mathrm{Norm}(\mathfrak{p})) & \text{if } \mathfrak{p} \text{ is a finite prime,} \end{cases} \tag{1.3.1}$$

and elementary algebraic number theory gives the following (see page 185 of [Ne]):

PROPOSITION 1.3.2. *Given any $\alpha \in K^*$, one has $v_\mathfrak{p} = 0$ for almost all $\mathfrak{p}$, and*

$$\sum_\mathfrak{p} v_\mathfrak{p}(\alpha) = 0. \tag{1.3.3}$$

The relation 1.3.3 can be considered as an arithmetic analogy of a particular case of Cauchy's Theorem. Let K be an algebraic function field of one variable over $\mathbb{C}$. Given any $\alpha \in K$, and a point $\mathfrak{p}$ on the Riemann surface of K, denote by $v_\mathfrak{p}$ the order of α at the point $\mathfrak{p}$, and define the following:

$$v_\mathfrak{p}(\alpha) = \begin{cases} -n & \text{if } \alpha \text{ has } \mathfrak{p} \text{ as a pole of order } n, \\ n & \text{if } \alpha \text{ has } \mathfrak{p} \text{ as a zero of order } n, \\ 0 & \text{if } \mathfrak{p} \text{ is neither a pole nor a zero of } \alpha. \end{cases} \tag{1.3.4}$$

Then we have $\sum_\mathfrak{p} v_\mathfrak{p} = \frac{1}{2\pi i}\int_\gamma d(\log(\alpha))$, where γ is a Jordan curve containing all poles and zeros of α. By Cauchy's theorem, we have $\int_\gamma d(\log(\alpha)) = 0$, which implies

$$\sum_\mathfrak{p} v_\mathfrak{p}(\alpha) = 0. \tag{1.3.5}$$

Considering that the residue degree of a number field is always finite, function fields over a finite field are the closest analog to number fields. At the basic level Table 1.1 gives a dictionary between number fields and function fields. We can also consider the fundamental group $\pi_1(U_n)$, $\pi_A(U_n)$, $\pi_A^t(U_n)$ for "curves" of the form $U_n = \mathrm{Spec}(\mathbb{Z}[\frac{1}{n}])$, where n is a square-free positive integer. In the function field $\mathbb{F}_q(t)$, a square-free polynomial f of degree d has norm q^d and defines a set of d geometric points. If we let $U \subset \mathbb{A}^1_{\mathbb{F}_q}$ be the set where $f \neq 0$, then by Proposition 1.2.15, we know every element in $\pi_A^t(U)$ is generated by d elements. In the number field case, the open subset U_n of $\mathrm{Spec}(\mathbb{Z})$ is the non-vanishing set of the integer n, of norm n. By the analogy between number fields and function fields $\mathbb{F}_q(t)$, Harbater posed the Conjecture 1.1.1.

1.4 Previous Results

In support of the Conjecture 1.1.1, Harbater has shown some evidence in [Ha3].

THEOREM 1.4.1 ([Ha3], Theorem 2.6). *(a) If $p < 23$ is a prime, then $\pi_1^t(U_p)$ is a cyclic group of order $p-1$.*

(b) The group $\pi_1^t(U_{23})$ is not cyclic.

COROLLARY 1.4.2 ([Ha3], Corollary 2.7). *If $p < 23$ is prime, and G is in $\pi_A(U_p)$, then $G/p(G)$ is a cyclic group of order dividing $p-1$.*

PROPOSITION 1.4.3 ([Ha3], Proposition 2.17). *Let K be a Galois extension of $\mathbb{Q}$ ramified only over 2, and let $\mathbb{Q} \subset K_0$ be an intermediate Galois extension whose degree is a power of 2. Then either*

(i) $\mathrm{Gal}\,(K/K_0)$ is a quasi-2 group; or

(ii) there is a non-trivial abelian unramified extension $K_0 \subset L$ of odd degree such that $L \subset K$ and L is Galois over $\mathbb{Q}$.

In particular, every group in $\pi_A(U_2)$ is a quasi-2 group. This gives evidence to Conjecture 1.1.1. Furthermore, [Ha3] also shows the following results about $\pi_A(U_2)$:

THEOREM 1.4.4 ([Ha3], Theorem 2.20). *Let G be a solvable group in $\pi_A(U_2)$. Then either G is a 2-group or order < 16, or G has a quotient of order 16.*

LEMMA 1.4.5 ([Ha3], Lemma 2.22). *If $G \in \pi_A(U_2)$ and $\mid G \mid \leq 300$, then G is solvable.*

THEOREM 1.4.6 ([Ha3], Theorem 2.23). *Let $\mathbb{Q} \subset K$ be a Galois extension ramified only over 2, with Galois group G and ramification index e. Then 16 divides e unless G is a 2-group of order < 16 (in which case the extension is totally ramified).*

1.5 Related results

In the early 1970s, Serre conjectured in [Se2] that every continuous irreducible odd representation of $G_{\mathbb{Q}}$ into $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$, unramified outside p, comes from a cusp form of some weight on $\mathrm{SL}(2,\mathbb{Z})$. Serre's conjecture has the following consequence: every two-dimensional irreducible odd representation of $G_{\mathbb{Q}}$ over $\bar{\mathbb{F}}_p$ that is unramified outside p has a twist coming from an eigenform f on $\mathrm{SL}(2,\mathbb{Z})$ of weight at most $p+1$. As we know, the spaces $S_k(\mathrm{SL}(2,\mathbb{Z}))$ of cusp forms for $\mathrm{SL}(2,\mathbb{Z})$ are zero when $k \leq 11$. So Serre's conjecture would predict the non-existence of certain continuous irreducible mod p representation of degree 2 of $G_{\mathbb{Q}}$, thus the non-existence of certain Galois extensions of $\mathbb{Q}$ unramified outside p.

In the case $p = 2$, Tate has shown the non-existence of certain Galois extension of $\mathbb{Q}$ unramified outside 2 in a letter to Serre in 1973.

THEOREM 1.5.1 ([Ta], Theorem). *Let G be the Galois group of a finite extension $K/\mathbb{Q}$ which is unramified at every odd prime. Suppose there is an embedding $\rho : G \hookrightarrow \mathrm{SL}_2(k)$, where k is a finite field of characteristic 2. Then $K \subset \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ and Trace$(\rho(\sigma)) = 0$ for each $\sigma \in G$.*

The non-existence in the case $p = 3$ was also proved by Serre in [Se1]. In 1997, Sharon Brueggeman showed, in accordance with Serre's conjecture, the non-existence of certain Galois extensions unramified outside 5.

THEOREM 1.5.2 ([Br1], Theorem 1.1). *Assume GRH. Let G be the Galois group of a finite Galois extension $K/\mathbb{Q}$ which is unramified outside 5. Let $\rho : G \hookrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_5)$ be a faithful semisimple odd representation. Then $\rho = \chi_5^a \oplus \chi_5^b$ for $a = 0$ or 2 and $b = 1$ or 3, where χ_5 is the cyclotomic character.*

In 2002, Hyunsuk Moon and Yuichiro Taguchi [TM] extended previously-known results about the non-existence of certain continuous irreducible mod p representations of degree 2 of $G_{\mathbb{Q}}$ by improving Tate's discrimant bound. In 2006, Chandrashekhar Khare proved the level one case of Serre's conjecture, which generalizes the results of Tate and Serre to all primes p:

THEOREM 1.5.3 ([Kh], Theorem 1.1). *Let $\bar{\rho} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ be a continuous, odd irreducible representation unramified outside p. Then $\bar{\rho}$ arises from a newform in $S_{k(\bar{\rho})}(\mathrm{SL}_2(\mathbb{Z}))$.*

On the other hand, there has also been much progress, by Brueggeman, Jones and Doud using improved discriminant bounding and polynomial searching, in determining the non-existence of various Galois extensions of $\mathbb{Q}$ which are unramified outside a single prime p.

THEOREM 1.5.4 ([Br2], Theorem 4.1). *Let K be a number field which is ramified only at a single prime p and $p \leq 7$. Then its Galois group is not isomorphic to $\mathrm{SL}(3, 2)$, A_7, or S_7.*

COROLLARY 1.5.5 ([Jo2], Theorem 2.2). *If G is the Galois group of a finite extension of $\mathbb{Q}$ unramified away from 2 and $\mid G \mid > 8$, then $\mid G \mid$ is a multiple of 16.*

THEOREM 1.5.6 (Jones, 2006). *There do not exist any extensions of $\mathbb{Q}$ of degree n which are unramified away from 2 where $10 \leq n \leq 15$.*

Chapter 2

Number Field Case

This chapter addresses the case that the base field is a number field. In Sections 2.1 and 2.2, we consider finite groups in $\pi_A(U_p)$ where $U_p = \mathrm{Spec}(\mathbb{Z}[\frac{1}{p}])$, i.e. Galois groups over $\mathbb{Q}$ only ramified at p (and possibly infinity). We will give some examples of infinite class field towers in Section 2.3. In Section 2.4, we look at nilpotent extensions over a quadratic number field $\mathbb{Q}(\sqrt{d})$. In the last section 2.5, we will try to use modular forms to construct more Galois extension over number fields.

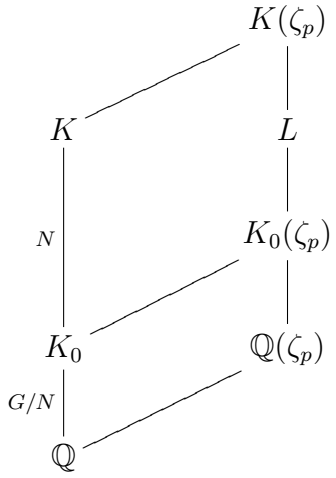
2.1 Solvable Extensions over $\mathbb{Q}$

2.1.1 Evidence for Conjecture 1.1.1

A consequence of the Conjecture 1.1.1 would be that if $G \in \pi_A(U_p)$ for some prime p, without assuming the ramification to be tame, then $G/p(G)$ is generated by at most $\log(p) + C$ elements. Thus if p is very small, we expect G to be very close to being a quasi-p group. In fact, this holds when $p < 23$ as seen in the Corollary 1.4.2, i.e. $G/p(G)$ is cyclic of order dividing $p - 1$. The following theorem is a generalization of this idea and of Proposition 1.4.3, but with an extra assumption on solvability.

THEOREM 2.1.1. *Let K be a finite Galois extension of $\mathbb{Q}$ ramified only at a single finite prime $p > 2$, with the Galois group $G = \mathrm{Gal}\,(K/\mathbb{Q})$ solvable. Let $K_0/\mathbb{Q}$ be an intermediate abelian extension of $K/\mathbb{Q}$. Let $N = \mathrm{Gal}\,(K/K_0)$ and $p(N)$ be the*

quasi p-part of N.



Suppose N is solvable. Then either

(i) $N/p(N) \subset \mathbb{Z}/(p-1)$; or

(ii) there is a non-trivial abelian unramified subextension $L/K_0(\zeta_p)$ of $K(\zeta_p)/K_0(\zeta_p)$ of degree prime to p with L Galois over $\mathbb{Q}$.

We will first give some corollaries, then prove a lemma and a proposition that will be used in the proof of Theorem 2.1.1, given at the end of this section.

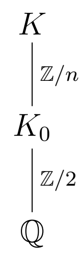
Remarks.
- If we let $K_0 = \mathbb{Q}$ and $p < 23$, Theorem 2.1.1 is just Corollary 1.4.2 in the solvable case.
- The proof of Theorem 2.1.1 shows that the condition (i) can be replaced by the condition $K/\mathbb{Q}$ is a quasi-p extension of a totally ramified extension.

Using 2.1.1, we can show some dihedral groups cannot be in $\pi_A(U_p)$ for some primes p.

COROLLARY 2.1.2. *Suppose $p \equiv 1 \pmod 4$ is a regular prime such that the class number of $\mathbb{Q}(\sqrt{p})$ is 1 (for example, in the range $2 \leq p \leq 100$, this is the case when $p = 5, 13, 17, 29, 41, 53, 61, 73, 89, 97$). Then there are no dihedral groups in $\pi_A(U_p)$ except D_2, the cyclic group of order 2.*

Proof. Suppose that $K/\mathbb{Q}$ is a Galois extension with group D_{2n} with order $2n$, ramified only at a finite prime p and possibly at ∞. Denote by K_0 the fixed field

of the cyclic subgroup $\mathbb{Z}/n < D_{2n}$.



By Theorem 1.2.2 in [JY], we know n is not divisible by p. Now apply Theorem 2.1.1. By the assumption the class number of K_0 is 1, we know the condition (ii) in Theorem 2.1.1 fails. By the second remark above we have $K/\mathbb{Q}$ is totally ramified, since p does not divide the order of D_{2n}. So $\mathrm{Gal}\,(K/\mathbb{Q}) \cong P \rtimes C$, where P is a p-group and C is a cyclic group. We know P has to be trivial, since again $p \nmid 2n$. Thus $\mathrm{Gal}\,(K/\mathbb{Q})$ is cyclic; a contradiction.

□

As a direct consequence of 2.1.1, we have:

COROLLARY 2.1.3. *Let $K/\mathbb{Q}$ be a Galois extension ramified only at prime p and possibly at ∞, where $\mathbb{Q}(\zeta_{p^n})$ is a sub-extension with Galois group* $\mathrm{Gal}\,(K/\mathbb{Q}(\zeta_{p^n})) = G$*. Suppose the class number of $\mathbb{Q}(\zeta_{p^n})$ is 1. Then $G/p(G)$ is cyclic of order dividing $p-1$.*

Proof. Take $\mathbb{Q}(\zeta_{p^n})$ to be the intermediate extension K_0 and apply Theorem 2.1.1. Since the class number of K_0 is 1, the condition (ii) in Theorem 2.1.1 does not hold. So condition (i) holds, i.e. $G/p(G)$ is cyclic of order dividing $p-1$. □

LEMMA 2.1.4. *Under the hypotheses of Theorem 2.1.1, if K_0 is a maximal p-power subextension of $K/\mathbb{Q}$, then the condition (i) can be replaced by the condition that either G is a cyclic p-group or $N/p(N)$ is a nontrivial subgroup of $\mathbb{Z}/(p-1)$.*

Proof. It suffices to show that if N is a quasi-p group, then G is a cyclic p-group. So assume G is not a cyclic group. The Galois group $\mathrm{Gal}\,(K_0/\mathbb{Q})$ is cyclic since any finite p-group in $\pi_A(U_p)$ is cyclic; so K_0 is the unique maximal p-power sub-extension of $K/\mathbb{Q}$ by class field theory. Denote by N the Galois group $\mathrm{Gal}\,(K/K_0)$. Then it is the minimal subgroup of G with index a power of p, since it corresponds to the unique maximal p-power sub-extension K_0; Furthermore it is normal by the Sylow's theorem. We know N is nontrivial, since G is not a p-group by assumption. Now G is a nontrivial solvable group, so G has a normal subgroup $\bar{N} \subset N$ such that $N/\bar{N}$ is of the form $(\mathbb{Z}/q)^n$ for some prime q and some integer $n \geq 1$. We know $q \neq p$ from the minimality of N. So N is not a quasi-p-group since every p-subgroup of N is contained in the proper subgroup $\bar{N}$. □

The above lemma gives evidence for Conjecture 1.1.1. Now Applying Lemma 2.1.4 to the prime 3 gives the following:

COROLLARY 2.1.5. *If G is a solvable group in $\pi_A(U_3)$, then either G is cyclic, or $G/p(G) \cong \mathbb{Z}/2$, or G has a cyclic quotient of order 27.*

Proof. Let $K/\mathbb{Q}$ be a Galois extension ramified only at 3 with Galois group $G = \mathrm{Gal}\,(K/\mathbb{Q})$. Take $K_0/\mathbb{Q}$ to be a maximal p-power sub-extension of $K/\mathbb{Q}$. The Galois group $\mathrm{Gal}\,(K_0/\mathbb{Q})$ is cyclic since any finite p-group in $\pi_A(U_p)$ is cyclic; so K_0 is the unique maximal p-power sub-extension of $K/\mathbb{Q}$ by class field theory. So we know K_0 is the unique maximal p-power sub-extension. If G is not cyclic, then N is not quasi-p by Lemma 2.1.4. Now suppose G is not cyclic and $G/p(G) \ncong \mathbb{Z}/2$ and apply Theorem 2.1.1. Since the condition (i) in Theorem does not hold, the condition (ii) has to hold, thus the class group of $K_0(\zeta_p)$ is nontrivial. So $|\,\mathrm{Gal}\,(K_0/\mathbb{Q})\,| \geq 27$, i.e. G has a cyclic quotient of order 27. □

COROLLARY 2.1.6. *Suppose $K/\mathbb{Q}$ is a Galois extension with nontrivial Galois group G, ramified only at 3 and possibly at ∞, with ramification index e. Then $9|e$ unless $G/p(G) \cong \mathbb{Z}/2$ or $G \cong \mathbb{Z}/3$.*

Proof. If G is solvable, by Corollary 2.1.5 we know $27 \mid e$ unless $G/p(G) \cong \mathbb{Z}/2$ or G is cyclic. In the case G is cyclic, we know by class field theory $K/\mathbb{Q}$ is totally ramified, so $e = n = |G|$. If G is non-solvable, it has order ≥ 60. On one hand, We know $|\,\mathfrak{d}_{K/\mathbb{Q}}\,|^{\frac{1}{n}} \geq 12.23$ from the discriminant table (page 400 in [Od]) for extensions of degree ≤ 60; on the other hand, by applying Theorem 1.2.6 we have $|\,\mathfrak{d}_{K/\mathbb{Q}}\,|^{\frac{1}{n}} \leq 3^{1+v_3(e)-\frac{1}{e}} < 3^{1+v_3(e)}$. Combining these two inequalities gives

$$12.23 \leq |\,\mathfrak{d}_{K/\mathbb{Q}}\,|^{\frac{1}{n}} < 3^{1+v_3(e)},$$

thus $v_3(e) \geq 2$ and $9 \mid e$. □

Remark. Corollary 2.1.6 applies even in the nonsolvable case.

For the proof of Theorem 2.1.1, we first need a lemma and proposition.

LEMMA 2.1.7. *Let $G = P \rtimes \mathbb{Z}/(l_1 l_2)$ be a semidirect product of a p-group P by a cyclic group $\mathbb{Z}/l_1 l_2$, with p, l_2 distinct primes and $p \nmid l_1$. Denote by s the highest power of l_2 which divides l_1, i.e. $l_2^s \,||\, l_1$. Suppose G has a normal subgroup $N \cong \mathbb{Z}/l_2^{s+1}$ with the quotient group $G/N \cong \mathbb{Z}/(l_1 l_2^{-s} p^m)$. Then $G = \mathbb{Z}/p^m \times \mathbb{Z}/(l_1 l_2)$.*

Proof. Let $\theta : \mathbb{Z}/(l_1 l_2) \longrightarrow \mathrm{Aut}(P)$ be the homomorphism corresponding to the semi-direct product $G = P \rtimes \mathbb{Z}/(l_1 l_2)$, which sends an element $a \in \mathbb{Z}/(l_1 l_2)$ to an automorphism $\theta_a \in \mathrm{Aut}(P)$. Since the l_2-sylow subgroup N is normal in G, it is the unique l_2-sylow subgroup by the Sylow's theorem. Identify $\mathbb{Z}/l_2^{s+1}$ with the subset of $G = P \rtimes \mathbb{Z}/(l_1 l_2) \cong P \rtimes (\mathbb{Z}/l_1 l_2^{-s} \times \mathbb{Z}/l_2^{s+1})$, consisting of all pairs of

the form $(1,b)$ with $b \in \mathbb{Z}/l_2^{s+1}$. We claim $\mathbb{Z}/l_2^{s+1}$ acts trivially on P in G. Now $\forall (k,a) \in P \rtimes \mathbb{Z}/(l_1 l_2)$, we have

$$\begin{aligned}(k,a)(1,b)(k,a)^{-1} &= (k, ab)((\theta_{a^{-1}}(k))^{-1}, a^{-1}) \\ &= (k\theta_{ab}((\theta_{a^{-1}}(k))^{-1}), b) \\ &= (k\theta_{ba}(\theta_{a^{-1}}(k^{-1})), b) \\ &= (k\theta_b(k^{-1}), b)\end{aligned}$$

Since $\mathbb{Z}/l_2^{s+1} \lhd G$ by the assumption, we know $(k,a)(1,b)(k,a)^{-1}$ is of the form $(1,b)$. So $\theta_b(k^{-1}) = k^{-1}, \forall k \in \mathbb{Z}/p^m$, i.e. θ_b is trivial for all $b \in \mathbb{Z}/l_2^{s+1}$.

Next we will show the isomorphism

$$P \rtimes_\theta (\mathbb{Z}/(l_1 l_2^{-s}) \times \mathbb{Z}/l_2^{s+1}) \cong (P \rtimes_{\theta'} \mathbb{Z}/(l_1 l_2^{-s})) \times \mathbb{Z}/l_2^{s+1} \tag{2.1.8}$$

where the homomorphism $\theta' : \mathbb{Z}/l_1 l_2^{-s} \longrightarrow \mathrm{Aut}(P)$ is the restriction of θ onto $\mathbb{Z}/(l_1 l_2^{-s})$. On the one hand the LHS and RHS of 2.1.8 are the same as underlying sets, on the other hand we consider the binary operation in each group. Pick any two elements $(a_1,b_1,c_1),(a_2,b_2,c_2) \in \mathbb{Z}/p^m \rtimes (\mathbb{Z}/(l_1 l_2^{-s}) \times \mathbb{Z}/l_2^{s+1})$. We have

$$\begin{aligned}(a_1,b_1,c_1)(a_2,b_2,c_2) &= (a_1,(b_1,c_1))(a_2,(b_2,c_2)) \\ &= (a_1\theta_{(b_1,c_1)}(a_2), (b_1b_2, c_1c_2)) \\ &= (a_1\theta_{(b_1,c_1)}(a_2), b_1b_2, c_1c_2).\end{aligned}$$

And if we pick any two elements $(a_1,b_1,c_1),(a_2,b_2,c_2) \in (\mathbb{Z}/p^m \rtimes \mathbb{Z}/l_1 l_2^{-s}) \times \mathbb{Z}/l_2^{s+1}$,

$$\begin{aligned}(a_1,b_1,c_1)(a_2,b_2,c_2) &= ((a_1,b_1)(a_2,b_2), c_1c_2) \\ &= ((a_1\theta'_{b_1}(a_2), b_1b_2), c_1c_2) \\ &= (a_1\theta'_{b_1}(a_2), b_1b_2, c_1c_2).\end{aligned}$$

Since $\mathbb{Z}/l_2^{s+1}$ acts trivially on P, we know $\theta_{(b_1,c_1)}(a_2) = \theta'_{b_1}(a_2)$. So the LHS and RHS of 2.1.8 have the same binary operations. We can conclude isomorphism 2.1.8. Now we consider the quotient group $G/(\mathbb{Z}/l_2^{s+1})$. By the assumption it is isomorphic to $\mathbb{Z}/(l_1 l_2^{-s} p^m)$. So by isomorphism 2.1.8 we have

$$\mathbb{Z}/(l_1 l_2^{-s} p^m) \cong G/(\mathbb{Z}/l_2^{s+1}) \cong P \rtimes_{\theta'} \mathbb{Z}/l_1 l_2^{-s}.$$

So $G \cong (P \rtimes_{\theta'} \mathbb{Z}/(l_1 l_2^{-s})) \times \mathbb{Z}/l_2^{s+1} \cong \mathbb{Z}/(l_1 l_2^{-s} p^m) \times \mathbb{Z}/(l_2^{s+1}) \cong \mathbb{Z}/p^m \times \mathbb{Z}/(l_1 l_2)$. □

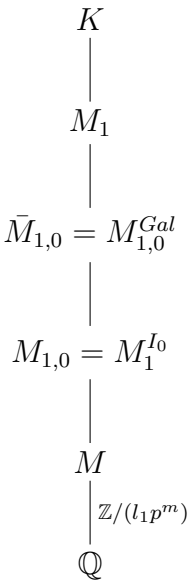
Proposition 2.1.9. *Let K be a finite Galois extension of $\mathbb{Q}$ ramified only over a single prime $p > 2$, with $G = \mathrm{Gal}(K/\mathbb{Q})$ solvable, and let $M/\mathbb{Q}$ be a proper abelian subextension of $K/\mathbb{Q}$ such that $p \nmid |\mathrm{Gal}(K/M)|$. Denote p^m the highest power of p dividing the order of G. Assume K/M is not totally ramified and that there is no non-trivial abelian unramified extension over $\mathbb{Q}(\zeta_p^{m+1})$ of degree prime to p which is contained in $K(\zeta_p)$ and is Galois over $\mathbb{Q}$. Then G is abelian.*

Proof. Since $\mathrm{Gal}\,(M/\mathbb{Q})$ is abelian, we know by class field theory $\mathrm{Gal}\,(M/\mathbb{Q})$ is a subgroup of $\mathbb{Z}/p^m \times \mathbb{Z}/(p-1)$. Denote $\mathrm{Gal}\,(M/\mathbb{Q}) = \mathbb{Z}/(p^m l_1)$ with $l \mid p-1$. Let $N = \mathrm{Gal}\,(K/M)$. Since N is solvable, being a normal subgroup of the solvable group G, there is a normal subgroup N_0 of N such that $N/N_0 \cong \mathbb{Z}/l_2$, for some prime l_2 such that $(l_2, p) = 1$. Let M_0 be the fixed field of N_0 in K/M, so $\mathrm{Gal}\,(M_0/M) \cong \mathbb{Z}/l_2$. Let M_1 be the Galois closure of M_0 over $\mathbb{Q}$, so $\mathrm{Gal}\,(M_1/M)$ is a minimal normal subgroup of a solvable group $\mathrm{Gal}\,(M_1/\mathbb{Q})$. From page 85 of [Rot], we know that $\mathrm{Gal}\,(M_1/M) \cong (\mathbb{Z}/l_2)^t$ for some $t \geq 1$. So the Galois group $\mathrm{Gal}\,(M_1/M_0) \cong (\mathbb{Z}/l_2)^{t-1}$.

$$
\begin{array}{c}
K \\
| \\
M_1 = (K^{N_0})^{Gal} \\
| \ (\mathbb{Z}/l_2)^{t-1} \\
M_0 = K^{N_0} \\
| \ \mathbb{Z}/l_2 \\
M \\
| \ \mathbb{Z}/(l_1 p^m) \\
\mathbb{Q}
\end{array}
$$

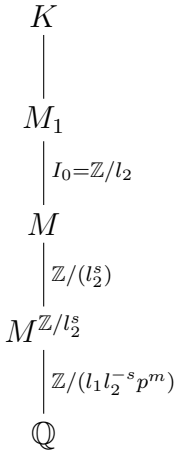
Pick a prime $\mathfrak{p}$ of M_1 over the prime p of $\mathbb{Q}$, let $I_0 \subset \mathrm{Gal}\,(M_1/M)$ be the inertia group of $\mathfrak{p}$ in M_1 over M. Since $\mathrm{Gal}\,(M_1/M) \cong (\mathbb{Z}/l_2)^t$ is abelian, its subgroup I_0 is normal and the quotient by I_0 is abelian. So the fixed field $M_{1,0} = M_1^{I_0}$ of I_0 in M_1/M is unramified over M at the prime $\mathfrak{p} \cap \mathcal{O}_{M_2}$, thus $M_{1,0}$ is an unramified extension of M contained in M_1. Let $\bar{M}_{1,0}$ be the Galois closure of $M_{1,0}$ over $\mathbb{Q}$. So $\bar{M}_{1,0}$ is contained in M_1 and unramified over M, being the composite of unramified extensions (the conjugates of $M_{1,0}$) of M. So $\bar{M}_{1,0}$ is abelian over M since it is contained in M_1. If $\bar{M}_{1,0}/M$ is not trivial, then $\bar{M}_{1,0}(\zeta_p)$ is a non-trivial abelian unramified extension over $M(\zeta_p) = \mathbb{Q}(\zeta_{p^{m+1}})$ (since $\mathrm{Gal}\,(M/\mathbb{Q}) \cong \mathbb{Z}/(l_1 p^m)$, we know $M(\zeta_p)$ is contained in $\mathbb{Q}(\zeta_{p^{m+1}})$. So $[M(\zeta_p) : \mathbb{Q}] = p^m(p-1) = [\mathbb{Q}(\zeta_{p^{m+1}}) : \mathbb{Q}]$ shows $M(\zeta_p) = \mathbb{Q}(\zeta_{p^{m+1}})$.) of degree prime to p such that $\bar{M}_{1,0}(\zeta_p) \subset K(\zeta_p)$ and

$\bar{M}_{1,0}$ is Galois over $\mathbb{Q}$, contrary to the assumption.



So actually $\bar{M}_{1,0} = M$, and so $I_0 = \mathrm{Gal}\,(M_1/M) \cong (\mathbb{Z}/l_2)^t$. But the inertia group I_0 is cyclic, because M_1 is at most tamely ramified at $\mathfrak{p}$ over M since the degree of the extension M_1/M is prime to p. So $t = 1$, and the field M_1 is totally ramified over M at $\mathfrak{p}$ with $\mathrm{Gal}\,(M_1/M) \cong \mathbb{Z}/l_2$. It follows M_1 is totally ramified over $\mathbb{Q}$ at the prime p, since $M/\mathbb{Q}$ is totally ramified at p. So $\mathrm{Gal}\,(M_1/\mathbb{Q})$ is isomorphic to the inertia group $I \cong P \rtimes C$ of M_1 over $\mathbb{Q}$ at $\mathfrak{p}$, where P is a p-group and C a cyclic group of order prime to p. So C is a cyclic group of order $l_1 l_2$, thus $I \cong \mathbb{Z}/p^m \rtimes \mathbb{Z}/l_1 l_2$ with l_1, l_2 relatively prime to p. On the other hand, let l_2^s be the highest power of l_2 which divides l_1, so $s \geq 0$. Consider the invariant field $M^{\mathbb{Z}/l_2^s}$ of $\mathbb{Z}/l_2^s$ in $M/\mathbb{Q}$. It is Galois over $\mathbb{Q}$ since $M/\mathbb{Q}$ is abelian, so $\mathrm{Gal}\left(M_1/M^{\mathbb{Z}/l_2^s}\right) \lhd \mathrm{Gal}\,(M_1/\mathbb{Q})$. Since $M_1/M^{\mathbb{Z}/l_2^s}$ is totally ramified, and tamely ramified, $\mathrm{Gal}\left(M_1/M^{\mathbb{Z}/l_2^s}\right)$ is a cyclic group by the Corollary 4 of page 68 of [Se3]. So $\mathrm{Gal}\left(M_1/M^{\mathbb{Z}/l_2^s}\right) \cong \mathbb{Z}/l_2^{s+1}$. And the quotient group $I/(\mathbb{Z}/l_2^{s+1}) \cong \mathbb{Z}/(l_1 l_2^{-s} p^m)$. It follows from the Lemma 2.1.7 that

$I \cong \mathbb{Z}/(p^m) \times \mathbb{Z}/l_1 l_2$.



Since M_1 strictly contains M, we know K/M_1 is not totally ramified, for otherwise K/M is also totally ramified, contrary to the assumption.

Now if $K \neq M_1$ we can repeat the above procedure with M_1 playing the role of M. There exists a sub-extension M_2/M_1 with $\mathrm{Gal}\,(M_2/M_1) \cong (\mathbb{Z}/l_3)$ for some prime $l_3 \neq p$, and the Galois group $\mathrm{Gal}\,(M_2/\mathbb{Q}) \cong \mathbb{Z}/(p^m) \times \mathbb{Z}/l_1 l_2 l_3$. Keep doing this process. It will stop when K equals some M_k with $\mathrm{Gal}\,(K/\mathbb{Q}) \cong \mathbb{Z}/p^m \times \mathbb{Z}/(l_1 ... l_{k+1})$ since G is a finite group. Equivalently, G is abelian. □

Now we can give the proof for Theorem 2.1.1:

Proof. The quasi-p part $p(N)$ of N is normal in G, since it is characteristic in the normal subgroup $N \lhd G$. Replacing G and N by $G/p(N)$ and $N/p(N)$ respectively, we may assume N has degree prime to p. We will show K/K_0 is cyclic of order dividing $p-1$, otherwise (ii) follows.

We may assume $K_0 \neq K$. First assume that K/K_0 is totally ramified. Then $K/\mathbb{Q}$ is totally ramified, since $K_0/\mathbb{Q}$ is totally ramified at p, so $G \cong P \rtimes C$ with P a p-group and C a subgroup of $\mathbb{Z}/(p-1)$. Since $K_0/\mathbb{Q}$ is Galois, $N \lhd G$. So N is cyclic of order dividing $p-1$.

Otherwise we assume K/K_0 is not totally ramified. Then the result follows from Proposition 2.1.9. □

2.1.2 Meta-abelian extensions over $\mathbb{Q}$

To understand solvable extensions, we can decompose them into finite towers of abelian extensions. The first case is meta-abelian extensions, i.e. G'' is trivial. Theorem 2.1.11 below gives an answer for tamely ramified extensions.

PROPOSITION 2.1.10. *The ray class number of $K = \mathbb{Q}(\zeta_p)$ mod $\mathfrak{m} = (1-\zeta_p)^k$ (for some integer k) is a product of a power of p and the class number of K.*

Proof. By class field theory, one has an exact sequence for the modulus $\mathfrak{m} = (1-\zeta_p)^k$,

$$1 \to \mathcal{O}_+^*/\mathcal{O}_+^{\mathfrak{m}} \to (\mathcal{O}_K/\mathfrak{m})^* \to Cl_K^{\mathfrak{m}} \to Cl_K^1 \to 1,$$

where $\mathcal{O}_+^*$, resp. $\mathcal{O}_+^{\mathfrak{m}}$, is the group of totally positive units of $\mathcal{O}_K$, resp. of totally positive units $\equiv 1 \bmod \mathfrak{m}$. The ray class number of K modulo $\mathfrak{m}$ is

$$|Cl_K^{\mathfrak{m}}| = \frac{|Cl_K^1| \cdot |(\mathcal{O}_K/\mathfrak{m})^*|}{|\mathcal{O}_+^*/\mathcal{O}_+^{\mathfrak{m}}|}.$$

By [CDO], Proposition 1.4, we can calculate the order of $(\mathcal{O}_K/\mathfrak{m})^*$, i.e.

$$|(\mathcal{O}_K/\mathfrak{m})^*| = (p-1)p^{k-1}.$$

The order of the group $\mathcal{O}_+^*/\mathcal{O}_+^{\mathfrak{m}}$ is $|\mathcal{O}^*/\mathcal{O}^{\mathfrak{m}}|$, since $\mathbb{Q}(\zeta_p)$ is totally complex and all units are totally positive. There is a natural surjective homomorphism $\mathcal{O}^*/\mathcal{O}^{\mathfrak{m}} \twoheadrightarrow \mathcal{O}^*/\mathcal{O}^{(1-\zeta_p)}$, so $|\mathcal{O}^*/\mathcal{O}^{(1-\zeta_p)}|$ divides $|\mathcal{O}^*/\mathcal{O}^{\mathfrak{m}}|$. Since $\mathcal{O}^*/\mathcal{O}^{(1-\zeta_p)} \hookrightarrow (\mathcal{O}_K/(1-\zeta_p))^* \cong \mathbb{F}_p^*$, and there are $p-1$ cyclotomic units

$$(\zeta_p^i - 1)/(\zeta_p - 1) \equiv i \pmod{(\zeta_p - 1)}, \qquad 1 \le i \le p-1,$$

We have $\mathcal{O}^*/\mathcal{O}^{(1-\zeta_p)} \cong (\mathcal{O}_K/(1-\zeta_p))^* \cong \mathbb{F}_p^*$. Thus

$$|\mathcal{O}^*/\mathcal{O}^{(1-\zeta_p)}| = |(\mathcal{O}_K/(1-\zeta_p))^*| = p-1,$$

which divides $|\mathcal{O}^*/\mathcal{O}^{\mathfrak{m}}|$. Thus $\frac{|Cl_K^{\mathfrak{m}}|}{|Cl_K^1|} = \frac{|(\mathcal{O}_K/\mathfrak{m})^*|}{|\mathcal{O}^*/\mathcal{O}^{\mathfrak{m}}|}$ is a power of p. Since K is totally complex. $Cl_K^1 \cong Cl_K$. So the Ray Class Number of K is the product of a power of p and the class number of K. □

Remark. Using [PARI2], we can compute the Ray Class groups of some cyclotomic number fields as in Table 2.1. The Ray Class Numbers of the cyclotomic number fields $\mathbb{Q}(\zeta_{23})$, $\mathbb{Q}(\zeta_{29})$, $\mathbb{Q}(\zeta_{31})$, $\mathbb{Q}(\zeta_{37})$, $\mathbb{Q}(\zeta_{41})$, $\mathbb{Q}(\zeta_{43})$ and $\mathbb{Q}(\zeta_{47})$ all have order equal to the class number of $\mathbb{Q}(\zeta_p)$ times a power of p, which is consistent with the proposition above. In fact, in this table, when p is regular and $\wp = (p)$ the Ray Class Number is $|Cl_K| \cdot p^{(p-3)/2}$, where $|Cl_K|$ is the class number of K.

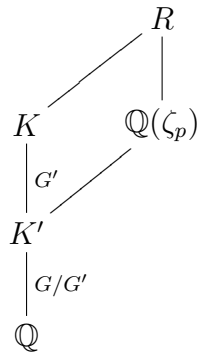
Let $K/\mathbb{Q}$ be a Galois extension with Galois group G. Considering the fixed field K' of the commutator subgroup G', we get the following theorem by applying Proposition 2.1.10 and class field theory:

THEOREM 2.1.11. *Suppose $G = \mathrm{Gal}\,(K/\mathbb{Q}) \in \pi_A^t(U_p)$ is a meta-abelian group. Then K is contained in the Hilbert class field of $\mathbb{Q}(\zeta_p)$.*

K	$\mathfrak{p}$	Cl_K	$Cl_K^{\mathfrak{p}}$	$Cl_K^{\mathfrak{p}^2}$
$\mathbb{Q}(\zeta_{23})$	$23\mathcal{O}_K$	$\mathbb{Z}/3$	$\mathbb{Z}/(3\cdot 23)\times(\mathbb{Z}/23)^9$	$\mathbb{Z}/(3\cdot 23^2)\times(\mathbb{Z}/23^2)^9\times(\mathbb{Z}/23)^2$
$\mathbb{Q}(\zeta_{29})$	$29\mathcal{O}_K$	$(\mathbb{Z}/2)^3$	$(\mathbb{Z}/2\cdot 29)^3\times(\mathbb{Z}/29)^{10}$	$(\mathbb{Z}/2\cdot 29^2)^3\times(\mathbb{Z}/29^2)^{10}\times(\mathbb{Z}/29)^2$
$\mathbb{Q}(\zeta_{31})$	$31\mathcal{O}_K$	$\mathbb{Z}/9$	$(\mathbb{Z}/9\cdot 31)\times(\mathbb{Z}/31)^{13}$	$(\mathbb{Z}/9\cdot 31^2)\times(\mathbb{Z}/31^2)^{13}\times(\mathbb{Z}/31)^2$
$\mathbb{Q}(\zeta_{37})$	$37\mathcal{O}_K$	$\mathbb{Z}/37$	$\mathbb{Z}/(37^2)\times(\mathbb{Z}/37)^{17}$	$(\mathbb{Z}/37^3)\times(\mathbb{Z}/37^2)^{16}\times(\mathbb{Z}/37)^3$
$\mathbb{Q}(\zeta_{41})$	$41\mathcal{O}_K$	$(\mathbb{Z}/11)^2$	$(\mathbb{Z}/41\cdot 11)^2\times(\mathbb{Z}/41)^{17}$	$(\mathbb{Z}/41^2\cdot 11)^2\times(\mathbb{Z}/41^2)^{17}\times(\mathbb{Z}/41)^2$
$\mathbb{Q}(\zeta_{43})$	$43\mathcal{O}_K$	$\mathbb{Z}/211$	$(\mathbb{Z}/211\cdot 43)\times(\mathbb{Z}/43)^{19}$	$\mathbb{Z}/(211\cdot 43^2)\times(\mathbb{Z}/43^2)^{19}\times(\mathbb{Z}/43)^2$
$\mathbb{Q}(\zeta_{47})$	$47\mathcal{O}_K$	$\mathbb{Z}/(5\cdot 139)$	$(\mathbb{Z}/5\cdot 139\cdot 47)\times(\mathbb{Z}/47)^{21}$	$\mathbb{Z}/(5\cdot 139\cdot 47^2)\times(\mathbb{Z}/47^2)^{21}\times(\mathbb{Z}/47)^2$

Table 2.1: Ray class groups of cyclotomic number fields

Proof. Consider the fixed field K' of G'. Since G/G' is abelian, and K' is tamely ramified and only ramified at p, we know K' is contained in $\mathbb{Q}(\zeta_p)$.



Since K/K' is abelian and ramified only at p, we know K is contained in a ray class field R of $\mathbb{Q}(\zeta_p)$ for a modulus $\wp = (1-\zeta_p)^k$ for some k. From Proposition 2.1.10, we know that $|Cl^{\wp}_{\mathbb{Q}(\zeta_p)}|$ is a product of a power of p and the class number of $\mathbb{Q}(\zeta_p)$. By class field theory $R/\mathbb{Q}(\zeta_p)$ is of degree $|Cl^{\wp}_{\mathbb{Q}(\zeta_p)}|$, a product of a power of p and the class number $Cl_{\mathbb{Q}(\zeta_p)}$. Therefore R corresponds to a p-extension of the Hilbert class field H of $\mathbb{Q}(\zeta_p)$. Pick any prime ℓ in R. The inertia degree of ℓ $|I^{\ell}_{R/\mathbb{Q}(\zeta_p)}| = |I^{\ell}_{R/H}|$ in $R/\mathbb{Q}(\zeta_p)$ divides $[R:H]$ and is a power of p. So $|I_{K/K'}|$ is also a power of p. But $K/\mathbb{Q}$ is tamely ramified. So $I^{\ell}_{K/(K'\cap H)}$ is trivial, thus K/K' is unramified, i.e. K is contained in the Hilbert class field of $\mathbb{Q}(\zeta_p)$. □

2.2 Nonsolvable Extensions over $\mathbb{Q}$

One extreme situation of non-solvable groups is the class of simple groups.

LEMMA 2.2.1. *Let $2 \leq p < 23$ be a prime, and $G \in \pi_A(U_p)$ with G non-abelian. Then $p \mid |G|$.*

Proof. If $p \nmid |G|$, then the quasi p-part $p(G)$ of G is trivial since it is generated by all p-Sylow subgroups of G. By Corollary 1.4.2, we know $G = G/p(G)$ is cyclic of order dividing $p-1$. Contradiction; thus $p \mid |G|$. □

LEMMA 2.2.2. *Let $K/\mathbb{Q}$ be a Galois extension ramified only at p with $G = \mathrm{Gal}\,(K/\mathbb{Q})$ a non-abelian simple group. If $2 \leq p < 23$, then G is a quasi p-group.*

Proof. We will show for a nontrivial simple group G, a prime $p \mid |G|$ if and only if G is a quasi p-group. If $p \mid |G|$ then $p(G) \neq \{1\}$. Since $p(G) \lhd G$ and G is simple, so $p(G) = G$, i.e. G is a quasi p-group. Conversely, if G is quasi p-group, then $p(G) = G \neq \{1\}$, so $p \mid |G|$. If $G \in \pi_A(U_p)$ with $2 < p < 23$, by Lemma 2.2.1 we know $p \mid G$, thus G is a quasi p-group. □

We can use above lemmas together with the Odlyzko discriminant bound to show various simple groups cannot be in $\pi_A(U_p)$:

Examples 2.2.3. For $2 \leq p < 23$, we consider A_5, S_5, $\mathrm{SL}(3,2)$.

- $\mathrm{SL}(3,2) \notin \pi_A(U_p)$ for $2 \leq p < 23$.

  Proof. The group $\mathrm{SL}(3,2)$ is of order $168 = 2^3 \cdot 3 \cdot 7$. When $p \neq 2, 3, 7$, if we assume $G \in \pi_A(U_p)$, by Lemma 2.2.1 we would have $p \mid |G|$, contradiction. In the case $p = 2$, Harbater showed $\mathrm{SL}(3,2) \notin \pi_A(U_2)$ (Example 2.21(c), [Ha3]). In the case $p = 7$, Brueggeman showed $\mathrm{SL}(3,2) \notin \pi_A(U_7)$ in [Br2](see Theorem 1.5.4). For the case $p = 3$, we assume $G \in \pi_A(U_3)$. Let $L/\mathbb{Q}$ be a corresponding Galois extension and let e be the ramification index of the prime above p. Applying the discriminant upper bound (Theorem 1.2.6), we get $|\mathfrak{d}_{L/\mathbb{Q}}|^{1/168} \leq 3^{1+v_3(e)-1/e}$. The largest power of 3 dividing $|\mathrm{SL}(3,2)| = 168$ is 3, so $v_3(e) \leq 1$, thus

  $$|\mathfrak{d}_{L/\mathbb{Q}}|^{1/168} \leq 3^{1+v_3(e)-1/e} \leq 3^{1+1} = 9.$$

  On the other hand, by the Odlyzko discriminant bound (Table 1, [Od]),

  $$|\mathfrak{d}_{L/\mathbb{Q}}|^{1/168} \geq 15.12,$$

  when the degree of the extension is at least 160. Contradiction. □

- The alternating group $A_5 \notin \pi_A(U_p)$ for $2 \leq p < 23$.

Proof. The group A_5 is of order $60 = 2^2 \cdot 3 \cdot 5$. When $p \neq 2, 3, 5$, by Lemma 2.2.1, we know $G \in \pi_A(U_p)$ would imply $p \mid |G|$, contradiction. For $p = 2$, Harbater showed that $A_5 \notin \pi_A(U_p)$ (Example 2.21(a), [Ha3]). For $p = 5$, we know $A_5 \notin \pi_A(U_5)$ from the table [Jo1]. For $p = 3$, we assume the simple group A_5 lies in $\pi_A(U_3)$ and let $L/\mathbb{Q}$ be a corresponding Galois extension. Applying the discriminant upper bound (Theorem 1.2.6), we have $|\mathfrak{d}_{L/\mathbb{Q}}|^{1/60} \leq 3^{1+v_3(e)-1/e}$. Since the largest power of 3 dividing $|A_5| = 60$ is 3, we get $v_3(e) \leq 1$, thus

$$|\mathfrak{d}_{L/\mathbb{Q}}|^{1/60} \leq 3^{1+v_3(e)-1/e} \leq 3^{1+1} = 9.$$

On the other hand, by the Odlyzko discriminant bound (Table 1, [Od]),

$$|\mathfrak{d}_{L/\mathbb{Q}}|^{1/60} \geq 12.23,$$

when the degree of the extension is at least 60. Contradiction. □

- The symmetric group $S_5 \notin \pi_A(U_p)$ for $2 \leq p < 23$.

Proof. The group S_5 is of order $120 = 2^3 \cdot 3 \cdot 5$. When $p \neq 2, 3, 5$, by Lemma 2.2.1 we know $G \notin \pi_A(U_p)$, for otherwise we would have $p \mid |G|$, contradiction. For $p = 2$, Harbater showed $S_5 \notin \pi_A(U_p)$ (Example 2.21(a), [Ha3]). For $p = 5$, we know $S_5 \notin \pi_A(U_p)$ from the table [Jo1]. For $p = 3$, similarly as A_5, we have

$$|\mathfrak{d}_{L/\mathbb{Q}}|^{1/120} \leq 3^{1+v_3(e)-1/e} \leq 3^{1+1} = 9.$$

But by the Odlyzko bound (Theorem 1.2.6), we have

$$|\mathfrak{d}_{L/\mathbb{Q}}|^{1/120} \geq 14.38,$$

for extensions of degree at least 120, contradiction. □

The examples above can be used to show the following proposition, which is a generalization of a result which handles the case $p = 2$ in [Ha3].

PROPOSITION 2.2.4. *Let $2 \leq p < 23$ be a prime number. If $G \in \pi_A(U_p)$ and $|G| \leq 300$, then G is solvable.*

Proof. Assume there exist non-solvable groups $G \in \pi_A(U_p)$ with order ≤ 300, and let G be such a group of smallest order. Pick a nontrivial normal subgroup N of G. The quotient group G/N is also in $\pi_A(U_p)$ but with smaller order, hence solvable. We know N is also non-solvable, then the order of the group N is at least 60. So $|G/N| \leq 5$, thus G/N is abelian. By Lemma 2.5 in [Ha3] we know G is isomorphic to either A_5, S_5 or $\mathrm{SL}(3, 2)$. By examples above, these groups do not lie in $\pi_A(U_p)$ for $2 \leq p < 23$. Contradiction. □

2.3 Infinite class field towers

Let $K = K^{(0)}$ be an algebraic number field. For $i = 0, 1, 2, ...$, define $K^{(i+1)}$ to be the Hilbert class field of $K^{(i)}$, i.e. the maximal abelian unramified extension of $K^{(i)}$. In [Haj], Hajir defined the "length of the Hilbert class field tower of K" to be the smallest non-negative integer i such that $K^{(i)} = K^{(i+1)}$ if such an integer exists, and ∞ otherwise. This integer is denoted $l(K)$. In the latter case that $l(K) = \infty$, we say that K *admits an infinite class field tower*. I. R. Šafarevič gave an example of an infinite class tower of a number field ramified at seven primes over $\mathbb{Q}$ (see [Sh]). A natural question is this: Does there exist a number field ramified only at one prime over $\mathbb{Q}$, which admits an infinite class field tower? The answer to this question is:

THEOREM 2.3.1. *There do exist algebraic number fields ramified over $\mathbb{Q}$ at only one prime which admit infinite class towers.*

Proof. Let $K = \mathbb{Q}(\zeta_p)$, let H be the Hilbert class field of K, and let $L = H(\sqrt[p]{1-\zeta_p})$. We can carefully choose p such that:

1. $\mathbb{Q}(\zeta_p)$ has a big class number h, i.e. $h \geq 2p^2 - 2p + 4$.
2. $\mathbb{Q}(\zeta_p)$ has class field tower length 1, i.e. the class number of the Hilbert class field is 1.

Such choices of p exist by Farshid Hajir (see [Haj]). (For example, I believe $p = 61$ satisfies both conditions. The class number of $\mathbb{Q}(\zeta_{61})$ is $76301 = 41 \cdot 1861$, and strong computational evidence shows the class number of the Hilbert Class Field of $\mathbb{Q}(\zeta_{61})$ is 1.)

Let Ω be the maximal unramified extension of L, and let $G = \mathrm{Gal}\,(\Omega/L)$ be the Galois group. Let $G(q)$ be its maximal q-quotient for a prime number q. The group $G(q)$ corresponds, by Galois theory, to the maximal unramified q-extension of L, say $L(q)$. If we show that there exists a prime number q such that $L(q)/L$ is infinite, then the class tower of L does not stop. And $L/\mathbb{Q}$ is only ramified at p. So we may assume that $\Omega = L(q)$ and $G = G(q)$. Suppose the theorem is false, i.e. for every prime number q, $L(q)/L$ is a finite extension. So G is a finite q-group and $L(q)$ admits no cyclic unramified extensions of degree q. By Proposition 29 in [Sh] we know that

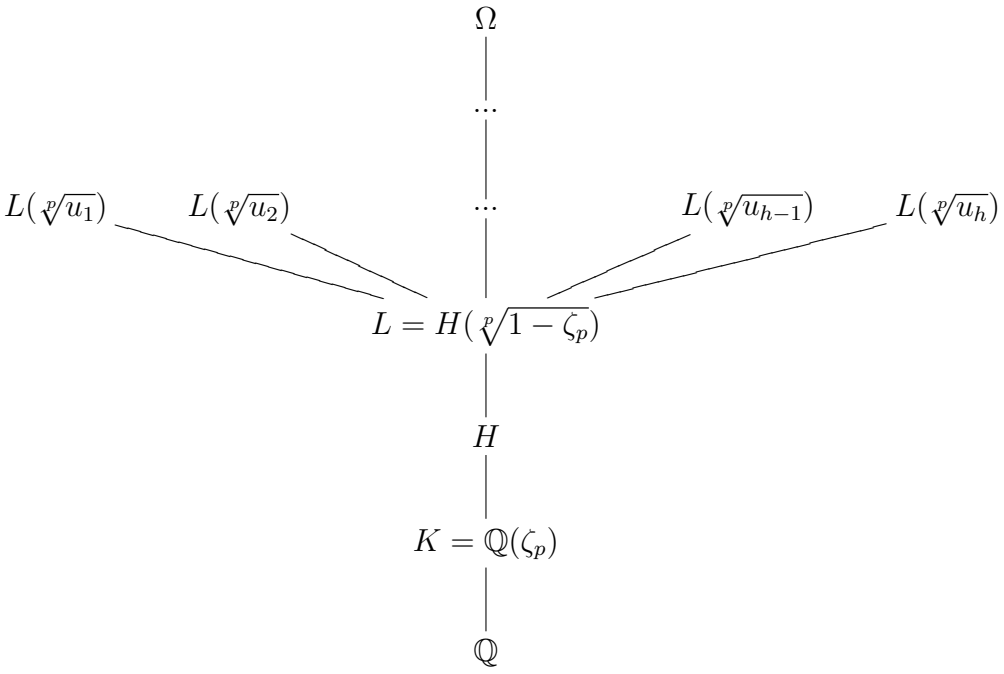
$$h_2 - h_1 \leq r_1 + r_2 = r_2 = p(p-1)h/2, \tag{2.3.2}$$

Where $h_i = \dim H^i(G, \mathbb{Z}/q\mathbb{Z})$, and r_1, r_2 denote the number of real and complex

conjugates of L, and h denotes the class number of K.

$$\begin{array}{ccc} H & & (u_1), ..., (u_h) \\ | & & | \\ K = \mathbb{Q}(\zeta_p) & & (1-\zeta_p) \\ | & & | \\ \mathbb{Q} & & (p) \end{array}$$

On the other hand, the principal prime ideal $(1-\zeta_p)$ splits completely into principal ideals $(1-\zeta_p) = \prod_{i=1}^{h}(u_i)$ in the Hilbert class field H.



Now we have h distinct unramified extensions $L(\sqrt[p]{u_i}))$ over L, so

$$h_1(G) \geq h. \tag{2.3.3}$$

By the Safarevic-Golod Theorem in [Sh], we have

$$h_2 > 1/4h_1^2. \tag{2.3.4}$$

Combining all the inequalities, we have

$$1/4h^2 - h \leq 1/4h_1^2 - h_1 < h_2 - h_1 < p(p-1)h/2 \Longrightarrow h < 2p^2 - 2p + 4.$$

But from the choice of p, we know that $h \geq 2p^2 - 2p + 4$, contradiction. □

Remark 2.3.5. The infinite class tower in Theorem 2.3.1 allows wild ramification and is also ramified at ∞. A natural problem is then to try to remove either condition and determine if an infinite tower still exists.

2.4 Extensions over quadratic fields

Given any real quadratic number field $K = \mathbb{Q}(\sqrt{d})$, we now consider nilpotent algebraic extensions L of K ramified over only one prime $\mathfrak{p}$ of K. Say $\mathfrak{p}|p$, a rational prime. If p remains prime in K, then there exist such extensions L of infinite degree over K (see Theorem 2.4.12). But if p splits and K has class number 1, then $[L : K]$ must be finite, and can be bounded in terms of d (see Theorem 2.4.6 for the case $p = 2$ and Theorem 2.4.7 for the general case).

2.4.1 Split Case

We now assume the rational prime $p = \mathfrak{p} \cap \mathbb{Z}$ splits in the real quadratic field $K = \mathbb{Q}(\sqrt{d})$ with d a positive prime. We also assume the class number of K is 1.

In the case $p = 2$, the splitting condition is equivalent to that $d = 1 \bmod 8$, thus $2 = \mathfrak{p}_1\mathfrak{p}_2$ splits completely in $K/\mathbb{Q}$. Also for the fundamental units, we have:

LEMMA 2.4.1. *Let $d \equiv 1 \pmod 8$ be a positive prime integer, then the fundamental unit $u = \frac{a+b\sqrt{d}}{2}$ of $\mathbb{Q}(\sqrt{d})$ has the property that a and b are both even (i.e. $u \in \mathbb{Z}[\sqrt{d}]$), with $\frac{a}{2}$ and $\frac{b}{2}$ of different parities.*

Proof. Since $d \equiv 1 \pmod 8$ is a prime, the norm $\mathrm{Norm}(u)$ of the fundamental unit u is -1 (see page 174 of [Ri]), i.e.

$$\frac{a^2 - b^2 d}{4} = \mathrm{Norm}(u) = -1.$$

So $a^2 + 4 = b^2 d \equiv b^2 \pmod 8$. We know a square mod 8 can only be $0, 1$, or 4. As a conclusion, both a and b have to be even; and we have $(\frac{a}{2})^2 + 1 \equiv (\frac{b}{2})^2 \pmod 2$, which implies $\frac{a}{2}$ and $\frac{b}{2}$ are of different parities. □

Remark. Lemma 2.4.1 is consistent with the results in Table 2.2 computed using [PARI2]. In fact, the conclusion in the Lemma 2.4.1 is still true even when d is not a prime.

Now we consider any abelian extension L over the real quadratic field $K = \mathbb{Q}(\sqrt{d})$ ramified only at one finite prime of K. It turns out that $\mathrm{Gal}\,(L/K)$ is a finite cyclic 2-group.

d	$u(d)$	d	$u(d)$	d	$u(d)$
17	$3+2\omega$	137	$1595+298\omega$	241	$66436843+9148450\omega$
33	$19+8\omega$	145	$11+2\omega$	249	$8011739+1084152\omega$
41	$27+10\omega$	153	$2001+352\omega$	257	$15+2\omega$
57	$131+40\omega$	161	$10847+1856\omega$	265	$5699+746\omega$
65	$7+2\omega$	177	$57731+9384\omega$	273	$683+88\omega$
73	$943+250\omega$	185	$63+10\omega$	281	$1000087+126890\omega$
89	$447+106\omega$	193	$1637147+253970\omega$	297	$45779+5640\omega$
97	$5035+1138\omega$	201	$478763+72664\omega$	305	$461+56\omega$
105	$37+8\omega$	209	$43331+6440\omega$	313	$119691683+14341370\omega$
113	$703+146\omega$	217	$3583111+521904\omega$	321	$-227+24\omega$
129	$15371+2968\omega$	233	$21639+3034\omega$	329	$2245399+262032\omega$

Table 2.2: Fundamental units $u(d)$ of $\mathbb{Q}(\sqrt{d})$, where $\omega = \frac{1+\sqrt{d}}{2}$.

PROPOSITION 2.4.2. *Suppose $K = \mathbb{Q}(\sqrt{d})$ has class number 1, where d is a positive prime such that $d \equiv 1 \pmod 8$ (so 2 splits as $2 = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ in K). If L is an abelian extension of K that is ramified only at $\mathfrak{p}_1$, then $\mathrm{Gal}\,(L/K)$ is a finite 2-group.*

Proof. Any abelian extension L/K ramified only at $\mathfrak{p}_1$ is contained in some ray class field for some modulus $\mathfrak{p}_1^k$ with k some positive integer. By class field theory, we have the following exact sequence:

$$1 \to \mathcal{O}_+^*/\mathcal{O}_+^{\mathfrak{p}_1^k} \to (\mathcal{O}_K/\mathfrak{p}_1^k)^* \to Cl_K^{\mathfrak{p}_1^k} \to Cl_K^1 \to 1. \tag{2.4.3}$$

By Proposition 1.4 in [CDO], we can calculate the order

$$|(\mathcal{O}_K/\mathfrak{p}_1^k)^*| = (p^f - 1) \cdot p^{f(k-1)} = 2^{k-1}.$$

Since the norm $\mathrm{Norm}(u)$ of the fundamental unit is -1, we have $\mathcal{O}_+^* = \{u^{2n}\}_{n=0}^{\infty}$. Picking $k = 1$, we get $|(\mathcal{O}_K/\mathfrak{p}_1)^*| = 1$. This forces

$$|\mathcal{O}_+^*/\mathcal{O}_+^{\mathfrak{p}_1}| = 1 \quad \text{i.e.} \quad u^2 \equiv 1 \pmod{\mathfrak{p}_1},$$

thus $u^2 = (\frac{a+b\sqrt{d}}{2})^2 \equiv 1 \mod 2$. By Lemma 2.4.1, we can write $a = 2a'$ and $b = 2b'$, where a' and b' have different parities. So $u = 1 + 2(\frac{a'-1+b'\sqrt{d}}{2}) \equiv 1 \pmod 2$, where $\frac{a'-1+b'\sqrt{d}}{2} \in \mathcal{O}_K$. Since $2 = \mathfrak{p}_1\mathfrak{p}_2$, there exists an integer $m \geq 2$ such that the fundamental unit $u^2 = 1 \pmod{\mathfrak{p}_1^m}$ but not $1 \pmod{\mathfrak{p}_1^{m+1}}$. Since the extension is Galois, $u^2 = 1 \pmod{2^m}$ but not $1 \pmod{2^{m+1}}$.

Case ($k \leq m$). We have $\mathcal{O}_+^{\mathfrak{p}_1^k} = \{u^{2n}\}_{n=0}^{\infty} = \mathcal{O}_+^*$, i.e. $|\mathcal{O}_+^*/\mathcal{O}_+^{\mathfrak{p}_1^k}| = 1$. So

$$|Cl_K^{\mathfrak{p}_1^k}| = \frac{|(\mathcal{O}_K/\mathfrak{p}_1^k)^*||Cl_K^1|}{|\mathcal{O}_+^*/\mathcal{O}_+^{\mathfrak{p}_1^k}|} = 2^{k-1}, \qquad k \leq m.$$

Case ($k > m$). We have $u^2 = 2^m \cdot t + 1$ for some $t \notin 2 \cdot \mathcal{O}_K$, so

$$u^4 = 2^{m+1}t(2^{m-1}t + 1) + 1 \equiv 1 \ (\mod 2^{m+1}),$$

but $u^4 \neq 1 \ (\mod 2^{m+2})$ since $m > 1$. Use induction we get $u^{2^{k-m+1}} \equiv 1 \ (\mod 2^k)$ and $u^{2^{k-m+1}} \neq 1 \ (\mod 2^{k+1})$. Thus $|\mathcal{O}_+^*/\mathcal{O}_+^{\mathfrak{p}_1^k}| = 2^{k-m}$ and

$$|Cl_K^{\mathfrak{p}_1^k}| = \frac{|(\mathcal{O}_K/\mathfrak{p}_1^k)^*||Cl_K^1|}{|\mathcal{O}_+^*/\mathcal{O}_+^{\mathfrak{p}_1^k}|} = \frac{2^{k-1}}{2^{k-m}} = 2^{m-1}, \qquad k \geq m.$$

Since L/K is abelian, it is contained in a ray class field R of K for some module $\mathfrak{p}_1^k$. Now we know the ray class number $|Cl_K^{\mathfrak{p}_1^k}|$ is a finite power of 2. So the ray class field R is a finite 2-extension of K. Thus L is a finite abelian 2-extension of K. □

Remark. Given $K = \mathbb{Q}(\sqrt{d})$ as in the assumption in 2.4.2. Then any abelian extension L/K ramified only at $\mathfrak{p}_1$ has degree

$$[L : K] \leq 2^{m-1},$$

where m is defined as in the proof of 2.4.2, which depends only on d.

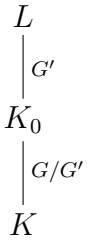
Example 2.4.4. The ray class field of $\mathbb{Q}(\sqrt{17})$ mod $\mathfrak{p}_1^2 = (\frac{5+\sqrt{17}}{2})^2$ is the field $\mathbb{Q}(\sqrt{17}, \sqrt{4+\sqrt{17}})$. Here $\mathfrak{p}_1 = (\frac{5+\sqrt{17}}{2})$ and $\mathfrak{p}_2 = (\frac{5-\sqrt{17}}{2})$ are the two primes in $\mathbb{Q}(\sqrt{17})$ above 2. The maximal abelian extension of $\mathbb{Q}(\sqrt{17})$ ramified only at $\mathfrak{p}_1$ is of degree 4.

In the next proposition we will show that any 2-extension over K ramified only at $\mathfrak{p}_1$ has to be cyclic.

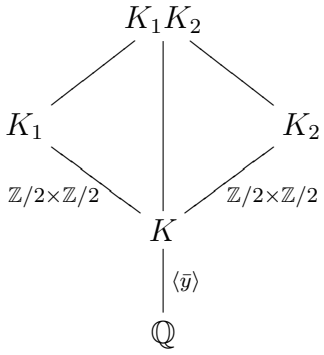
PROPOSITION 2.4.5. *Suppose $K = \mathbb{Q}(\sqrt{d})$ has class number 1, where d is a positive prime such that $d \equiv 1$ mod 8. If L is a totally real 2-extension of K that is ramified only at $\mathfrak{p}_1$, then* Gal (L/K) *is a cyclic 2-group.*

Proof. Let G be the Galois group of a finite 2-extension L/K. Take the fixed subfield K_0 of the commutator subgroup G'; then K_0 is the maximal abelian subextension of L/K. If K_0 is cyclic over K, by the Burnside Basis Theorem, L/K

will also be cyclic.



Otherwise G/G' has a quotient $\mathbb{Z}/2 \times \mathbb{Z}/2$, which corresponds to a subfield K_1/K. K_1 is not Galois over $\mathbb{Q}$ since it is totally ramified over $\mathfrak{p}_1$ but unramified over $\mathfrak{p}_2$. Take the conjugate extension K_2 of K_1 over $\mathbb{Q}$, which is totally ramified over $\mathfrak{p}_2$ over K and unramified over $\mathfrak{p}_1$. The compositum K_1K_2 will be Galois over $\mathbb{Q}$ with Galois group $H = ((\mathbb{Z}/2)^2 \times (\mathbb{Z}/2)^2) \rtimes \mathbb{Z}/2$, since K_1/K and K_2/K are linearly disjoint, using the fact K_1 is totally ramified over $\mathfrak{p}_1$ (by class number 1) and unramified over $\mathfrak{p}_2$; whereas K_2 is totally ramified over $\mathfrak{p}_2$ and unramified over $\mathfrak{p}_1$.



Suppose x_1, x_2 are generators of Galois group of K_1/K; that x_3, x_4 are generators of the Galois group of K_2/K; and that $\bar{y}$ is the generator of the Galois group of $K/\mathbb{Q}$. In the semidirect product $((\mathbb{Z}/2)^2 \times (\mathbb{Z}/2)^2) \rtimes \mathbb{Z}/2$, the action of y is to send x_1 to x_3, and send x_2 to x_4. Take the subgroup H_0 of H generated by x_1x_3 and x_2x_4; so $H_0 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. The action of y on H_0 sends x_1x_3 to $x_3x_1 = x_1x_3$, and sends x_2x_4 to $x_4x_2 = x_2x_4$; so H_0 is normal in H. The quotient $H/H_0 = \{\bar{x}_1 = \bar{x}_3, \bar{x}_2 = \bar{x}_4, \bar{y} | \bar{x}_1^2 = 1, \bar{x}_2^2 = 1, \bar{y}^2 = 1, \bar{x}_1\bar{x}_2 = \bar{x}_2\bar{x}_1, \bar{x}_1\bar{y} = \bar{y}\bar{x}_1, \bar{x}_2\bar{y} = \bar{y}\bar{x}_2\} \cong (\mathbb{Z}/2)^3$. The quotient of (H/H_0) by the normal subgroup generated by $\bar{y}$, $(H/H_0)/\{\bar{y}\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, corresponds to a totally real abelian extension over $\mathbb{Q}$ ramified only at 2 with Galois group $(\mathbb{Z}/2)^2$, which is impossible. □

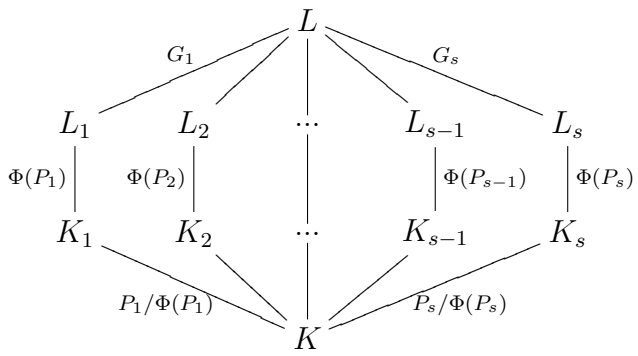
Using the above, we obtain the following theorem about nilpotent extensions over K ramified only at $\mathfrak{p}_1$.

THEOREM 2.4.6. *Suppose $K = \mathbb{Q}(\sqrt{d})$ has class number 1, where d is a positive prime such that $d \equiv 1 \pmod 8$ (so 2 splits as $2 = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ in K). Then the maximal nilpotent quotient $(\pi_1^{tr})^{nilp}(U_{K,\mathfrak{p}_1})$ of $\pi_1(U_{K,\mathfrak{p}_1})$ that corresponds to a totally real extension is a finite cyclic 2-group, whose order can be explicitly bounded in terms of d. So if L is a totally real nilpotent Galois extension of K that is ramified only at $\mathfrak{p}_1$, then $\mathrm{Gal}\,(L/K)$ is a finite cyclic 2-group.*

Proof. Suppose L/K is a totally real maximal nilpotent extension. Denote by G the Galois group $\mathrm{Gal}\,(L/K)$. So G is a nilpotent group. We can decompose G into a direct product of p-groups for various primes:

$$G = \prod_{j=1}^{s} P_j$$

For each $G_i := \prod_{j \neq i} P_j$, we denote its fixed subfield of L/K by L_i. For the Frattini subgroup $\Phi(P_i)$ of each P_i, we denote its fixed subfield of L_i/K by K_i.



If $2 \mid |P_i|$, then L_i is a totally real 2-extension over K that is ramified only at $\mathfrak{p}_1$. By Proposition 2.4.5, L_i/K is a cyclic 2-extension, thus abelian. By Proposition 2.4.2, the Galois group $\mathrm{Gal}\,(L_i/K)$ is a *finite* cyclic 2-group of order at most 2^{m-1}, where m is the integer such that $u^2 \equiv 1 \pmod{\mathfrak{p}_1^m}$ and $u^2 \neq 1 \pmod{\mathfrak{p}_1^{m+1}}$.

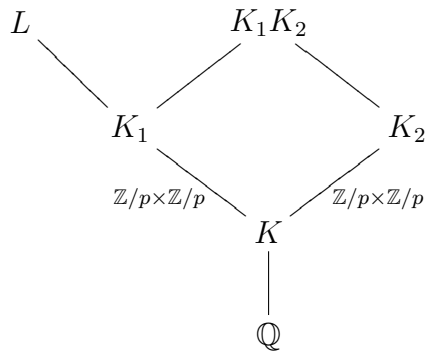
If $2 \nmid |P_i|$, then L_i is a totally real p-extension over K, where $p \mid |P_i|$ is different from 2. Here K_i/K is abelian; so by Proposition 2.4.2, $\mathrm{Gal}\,(K_i/K)$ is a finite 2-group, thus trivial. So $P_i \cong \mathrm{Gal}\,(L_i/K)$ is also trivial.

So the Galois group $\mathrm{Gal}\,(L/K)$ is a finite cyclic 2-group of order at most 2^{m-1}. □

We can extend Theorem 2.4.6 to the case of an odd rational prime p that splits into two primes $\mathfrak{p}_1\mathfrak{p}_2$ in the base field $K = \mathbb{Q}(\sqrt{d})$, with the positive integer d congruent to a square $\pmod p$.

THEOREM 2.4.7. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with class number 1. Suppose d is a square modulo p, and L/K is a p-extension ramified only at $\mathfrak{p}_1$, where $p = \mathfrak{p}_1\mathfrak{p}_2$ is an odd prime. Then $G = \mathrm{Gal}\,(L/K)$ is finite cyclic, and its order can be bounded depending on d.*

Proof. Consider the fixed subfield K' of the commutator subgroup G' in L/K. If $\mathrm{Gal}\,(K'/K)$ is cyclic, then by Burnside Basis Theorem, so is $\mathrm{Gal}\,(L/K)$. Otherwise we can take an intermediate field K_1/K of L/K with Galois group $\mathbb{Z}/p \times \mathbb{Z}/p$. Since K_1/K is (totally) ramified only at $\mathfrak{p}_1$, it is not Galois over $\mathbb{Q}$. So we can take the conjugate field K_2 of K_1 which is (totally) ramified over K only at $\mathfrak{p}_2$. Let $H = \mathrm{Gal}\,(K_1K_2/\mathbb{Q})$ be the Galois group of the compositum of K_1 and K_2 over $\mathbb{Q}$.



Here $\mathrm{Gal}\,(K_1/K) \cong \mathrm{Gal}\,(K_2/K) \cong \mathbb{Z}/p \times \mathbb{Z}/p$, and so $H \cong ((\mathbb{Z}/p \times \mathbb{Z}/p) \times (\mathbb{Z}/p \times \mathbb{Z}/p)) \rtimes \mathbb{Z}/2$. Suppose $\bar{x}_1, \bar{x}_2$ are generators of the Galois group of $K_1/K \cong \mathbb{Z}/p \times \mathbb{Z}/p$; $\bar{x}_3, \bar{x}_4$ are generators of the Galois group of $K_2/K \cong \mathbb{Z}/p \times \mathbb{Z}/p$; and y is a generator of the Galois group of $K/\mathbb{Q}$. In the semidirect product $((\mathbb{Z}/p \times \mathbb{Z}/p) \times (\mathbb{Z}/p \times \mathbb{Z}/p)) \rtimes \mathbb{Z}/2$, the action of y is to send x_1 to x_3, and send x_2 to x_4. Take the subgroup H_0 of H generated by $x_1x_3^{-1}$ and $x_2x_4^{-1}$; so $H_0 \cong \mathbb{Z}/p \times \mathbb{Z}/p$. The action of y on H_0 sends $x_1x_3^{-1}$ to $x_3x_1^{-1} = (x_1x_3^{-1})^{-1}$, and sends $x_2x_4^{-1}$ to $x_4x_2^{-1} = (x_2x_4^{-1})^{-1}$, so H_0 is normal in H. The quotient $H/H_0 = \{\bar{x}_1 = \bar{x}_3, \bar{x}_2 = \bar{x}_4, \bar{y} | \bar{x}_1^p = 1, \bar{x}_2^p = 1, \bar{y}^2 = 1, \bar{x}_1\bar{x}_2 = \bar{x}_2\bar{x}_1, \bar{x}_1\bar{y} = \bar{y}\bar{x}_1, \bar{x}_2\bar{y} = \bar{y}\bar{x}_2\} \cong (\mathbb{Z}/p \times \mathbb{Z}/p) \times \mathbb{Z}/2$. The quotient of (H/H_0) by the normal subgroup generated by $\bar{y}$, $(H/H_0)/\{\bar{y}\} \cong \mathbb{Z}/p \times \mathbb{Z}/p$, corresponds to an abelian extension over $\mathbb{Q}$ ramified only at p with Galois group $(\mathbb{Z}/p)^2$; which is impossible. So $\mathrm{Gal}\,(L/K)$ is a cyclic p-group, thus abelian. We can use similar argument to the one in the case of prime 2 to get that G is bounded depending on d, by considering the following exact sequence:

$$1 \to \mathcal{O}_+^*/\mathcal{O}_+^{\mathfrak{p}_1^k} \to (\mathcal{O}_K/\mathfrak{p}_1^k)^* \to Cl_K^{\mathfrak{p}_1^k} \to Cl_K^1 \to 1. \tag{2.4.8}$$

□

2.4.2 Non-Split Case

On the other hand, in the non-split case, $\mathrm{Gal}\,(L/K)$ can be arbitrarily large. For example, in the case of the prime 2, the ray class number can be any arbitrary power of 2:

PROPOSITION 2.4.9. *Suppose that the class number of $K = \mathbb{Q}(\sqrt{d})$ is 1, where $d \equiv 5 \pmod 8$ is a positive prime. Let $u = \frac{a+b\sqrt{d}}{2}$ be the fundamental unit of K, and assume that a, b are both odd. Then the ray class number of K mod 2^k for any positive integer k is as follows:*

$$|Cl_K^{2^k}| = \begin{cases} 1 & \text{for } k = 1, \\ 2^k & \text{for } k \geq 2. \end{cases}$$

Proof. Under the above assumption, we know 2 is inert in K with residue degree $f = 2$. Again we look at the following exact sequence:

$$1 \to \mathcal{O}_+^*/\mathcal{O}_+^{2^k} \to (\mathcal{O}_K/2^k)^* \to Cl_K^{2^k} \to Cl_K^1 \to 1.$$

We know $|(\mathcal{O}_K/2^k)^*| = (p^f - 1) \cdot p^{f(k-1)} = 3 \cdot 2^{2(k-1)}$ and $\mathcal{O}_+^* = \{u^{2n}\}$. For $\mathcal{O}_+^{2^k}$, let $u^n = \frac{a_n+b_n\sqrt{d}}{2}$. Since a, b are odd, by Lemma 4 of page 173 of [Ri], a_n, b_n are even if and only if 3 divides n. So $u^3 = \frac{a_3+b_3\sqrt{d}}{2}$ with a_3, b_3 even. Let $a_3 = 2a_3', b_3 = 2b_3'$. So $-1 = N(u^3) = a_3'^2 - b_3'^2 d$. Working modulo 4, we know $a_3'^2 \equiv 0 \pmod 4$ and $b_3'^2 d \equiv 1 \pmod 4$. So we can write $a_3' = 2a_3''$, $b_3' = 2b_3'' + 1$ and $d = 8k + 5$. We get $4a_3''^2 - 4b_3''(b_3'' + 1) = 8k + 4$, so $a_3'' \notin 2\mathcal{O}_K$. Now write $u^3 = 2t + 1$ with $t = \frac{a_3'-1+b_3'\sqrt{d}}{2}$. Then $N(t) = -a_3''$ and $N(t+1) = a_3''$, which are both odd. So we have

$$u^6 = 4t(t+1) + 1 \equiv 1 \pmod{2^2} \quad \text{and} \quad u^6 \neq 1 \pmod{2^3}.$$

Using induction we can get

$$u^{3\cdot 2^{k-1}} \equiv 1 \pmod{2^k} \quad \text{and} \quad u^{3\cdot 2^{k-1}} \neq 1 \pmod{2^{k+1}}.$$

So $|\mathcal{O}_+^*/\mathcal{O}_+^{2^k}| = 3 \cdot 2^{k-2}$ and we have the following:
Case $(k = 2)$. We know $|\mathcal{O}_+^*/\mathcal{O}_+^2| = 3$. So

$$|Cl_K^2| = \frac{|(\mathcal{O}_K/2)^*| \cdot |Cl_K^1|}{|\mathcal{O}_+^*/\mathcal{O}_+^2|} = 1.$$

Case $(k \geq 2)$. We know $|\mathcal{O}_+^*/\mathcal{O}_+^{2^k}| = 3 \cdot 2^{k-2}$, so

$$|Cl_K^{2^k}| = \frac{|(\mathcal{O}_K/2^k)^*||Cl_K^1|}{|\mathcal{O}_+^*/\mathcal{O}_+^{2^k}|} = \frac{3 \cdot 2^{2(k-1)}}{3 \cdot 2^{k-2}} = 2^k$$

□

Remark 2.4.10. In fact if we remove the condition the class number of K is 1, following the same proof above we can get

$$|Cl_K^{2^k}| = \begin{cases} cl_K^1 = |Cl_K^1| & \text{for } k = 1, \\ 2^k cl_K^1 = 2^k |Cl_K^1| & \text{for } k \geq 2. \end{cases}$$

So the ray class field of K mod 2 is just the big Hilbert class field of K.

By Corollary 1.4.2, every group in $\pi_A(U_2)$ is a quasi-2 group. We have a similar statement below for Galois groups over quadratic fields ramified only at one prime. Define $\pi_A(U_{\mathbb{Q}(\sqrt{d}),\,\mathfrak{p}})$ to be the set of finite quotients of $\pi_1(U_{\mathbb{Q}(\sqrt{d}),\,\mathfrak{p}})$, where $\mathfrak{p}$ is a prime in $\mathbb{Q}(\sqrt{d})$, and $U_{\mathbb{Q}(\sqrt{d}),\,\mathfrak{p}} = \operatorname{Spec} \mathcal{O}_{\mathbb{Q}(\sqrt{d})} - \{\mathfrak{p}\}$. So $\pi_A(U_{\mathbb{Q}(\sqrt{d}),\,\mathfrak{p}})$ consists of finite groups that can occur as a Galois group over $\mathbb{Q}(\sqrt{d})$ with ramification only at $\mathfrak{p}$.

PROPOSITION 2.4.11. *Let $d \equiv 1 \pmod 4$, let $u = \frac{a+b\sqrt{d}}{2}$ be the fundamental unit of $K = \mathbb{Q}(\sqrt{d})$, and suppose a, b are both odd. Suppose $\mathfrak{p}$ is the prime in $\mathbb{Q}(\sqrt{d})$ above $p = 2$. Then every group in $\pi_A(U_{\mathbb{Q}(\sqrt{d}),\mathfrak{p}})$ is a quasi-2 group.*

Proof. Take any group $G \in \pi_A(U_{\mathbb{Q}(\sqrt{d}),\mathfrak{p}})$; so $G/p(G)$ is of odd order, thus solvable. If $G/p(G)$ is nontrivial, then there exists a nontrivial abelian odd extension of $\mathbb{Q}(\sqrt{d})$ ramified only at $\mathfrak{p}$. This is impossible, since we know by Proposition 2.4.2 and Proposition 2.4.9 that the ray class number of K mod $\mathfrak{p}^k$ for any integer k is a power of 2 , which cannot be odd. Thus $G/p(G)$ is trivial, i.e. G is a quasi-2 group. □

THEOREM 2.4.12. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field, and suppose p remains prime in K. Let R_k be the ray class field of K mod p^k.*

a) Then for $k \gg 0$, $R_{k+1} = R_k(\zeta_{p^{k+1}})$.

b) Suppose $p = 2$, and the fundamental unit of K is $u = \frac{a+b\sqrt{d}}{2}$ with a, b both odd. Let H be the big Hilbert class field of K. Then $R_k = H(\sqrt{2u}, \zeta_{2^k})$ if $k \geq 2$, and $R_k = H$ if $k = 1$.

Proof. First we look at the case $p = 2$. When $k = 1$, the ray class field is the big Hilbert class field by Remark 2.4.10. When $k \geq 2$, the conductor of $K(\zeta_{2^k})/K$ divides 2^{k-2}, and the conductor of $K(\sqrt{2u})$ over K is 2^2, so the conductor of $H(\sqrt{2u}, \zeta_{2^k})/K$ divides 2^k. Also $[H(\sqrt{2u}, \zeta_{2^k}) : K] = 2^k$ which equals to the ray class number, so $H(\sqrt{2u}, \zeta_{2^k})$ is the ray class field R_K of K mod p^k, and $R_{k+1} = R_k(\zeta_{p^{k+1}})$.

Now we consider the case $p > 2$. Again we look at the following exact sequence:

$$1 \to \mathcal{O}_+^*/\mathcal{O}_+^{p^k} \to (\mathcal{O}_K/p^k)^* \to Cl_K^{p^k} \to Cl_K^1 \to 1.$$

We will computer the ratio $\frac{|Cl_K^{p^{k+1}}|}{|Cl_K^{p^k}|}$, where

$$|Cl_K^{p^k}| = \frac{|(\mathcal{O}_K/p^k)^*||Cl_K^1|}{|\mathcal{O}_+^*/\mathcal{O}_+^{p^k}|} = \frac{(p^2-1)\cdot p^{2(k-1)}\cdot|Cl_K^1|}{|\mathcal{O}_+^*/\mathcal{O}_+^{p^k}|}.$$

For $|\mathcal{O}_+^*/\mathcal{O}_+^{p^k}|$, we can always pick k big enough such that $\mathcal{O}_+^*/\mathcal{O}_+^{p^k} \neq \mathcal{O}_+^*/\mathcal{O}_+^{p^{k+1}}$. Take a generator $\bar{u}_0$ in $\mathcal{O}_+^*/\mathcal{O}_+^{p^k}$; and denote by u_0^s the smallest power of u_0 such that $u_0^s \equiv 1 \bmod p^k$. So we can write $u_0^s = tp^k + 1$, where $t \in \mathcal{O}_K$ and $p \nmid t$. Then $u_0^{sp} = (tp^k+1)^p \equiv 1 \bmod p^{k+1}$, so $\frac{|\mathcal{O}_+^*/\mathcal{O}_+^{p^{k+1}}|}{|\mathcal{O}_+^*/\mathcal{O}_+^{p^k}|} = p$ when $k >> 0$. Now we have

$$\frac{|Cl_K^{p^{k+1}}|}{|Cl_K^{p^k}|} = \frac{\frac{|(\mathcal{O}_K/p^{k+1})^*||Cl_K^1|}{|(\mathcal{O}_K/p^k)^*||Cl_K^1|}}{\frac{|\mathcal{O}_+^*/\mathcal{O}_+^{p^{k+1}}|}{|\mathcal{O}_+^*/\mathcal{O}_+^{p^{k+1}}|}} = \frac{p^2}{p} = p,$$

so R_{k+1}/R_k is of degree p. While $\mathbb{Q}(\zeta_{p^{k+1}})/\mathbb{Q}(\zeta_p)$ is of conductor p^k, the conductor of $R_k(\zeta_{p^{k+1}})/R_k$ divides p^k and is of degree p, so $R_{k+1} = R_k(\zeta_{p^{k+1}})$ for $k \gg 0$. □

2.5 Modular forms

Another tool we can use to construct a Galois extension over $\mathbb{Q}$ with given ramification is modular forms. By P. Deligne [De], we can attach a semisimple continuous representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ to every eigenform, whose image corresponds to a finite Galois extension over $\mathbb{Q}$ with given ramification. If we restrict Galois groups over $\mathbb{Q}$ to semisimple subgroups of $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$, we can construct such Galois groups by using modular forms, assuming Serre's conjecture in [Se2]:

Conjecture 2.5.1. *(Serre) Let p be a prime number and $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ a continuous irreducible odd representation. Then there exists an eigenform f in $M^0(N(\rho), k(\rho), \epsilon(\rho))_{\bar{\mathbb{F}}_p}$ such that ρ is isomorphic to ρ_f.*

In the level one case (corresponding to one ramified prime) this was proved recently by C. Khare in [Kh]. Thus each two-dimensional irreducible odd representation of $\mathrm{Gal}\left(\bar{\mathbb{Q}}/\mathbb{Q}\right)$ over $\bar{\mathbb{F}}_p$ that is unramified outside p has a twist coming from an eigenform on $\mathrm{SL}(2,\mathbb{Z})$ of weight at most $p+1$. For all $k < 11$ the spaces $S_k(\mathrm{SL}(2,\mathbb{Z}))$ are trivial, so there are no such representations $\rho : \mathrm{Gal}\left(\bar{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ when $p < 11$. As a result, if $K/\mathbb{Q}$ is a Galois extension over $\mathbb{Q}$ ramified only at p, and $G = \mathrm{Gal}\,(K/\mathbb{Q})$ is a semisimple subgroup of $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$, then G is abelian. For the case $k = 12j + r \geq 11$, $\dim S_k(\mathrm{SL}(2,\mathbb{Z})) = j+2$ if $r = 1, 4, 6, 8, 10$ and $j+1$ otherwise. The drawback of this method is that it doesn't provide any information

about Galois groups that are not semisimple inside $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$. In particular there is the following example.

Example 2.5.2. The Frobenius group $F_{20} \cong \langle x, y \,|\, x^4 = y^5 = 1, yx = xy^2 \rangle$ inside $\mathrm{GL}_2(\mathbb{F}_5)$ is not a semi-simple subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$, and it corresponds to the Galois extension of the polynomial $x^5 - 5$ or $x^5 + 5x^3 + 5x - 1$, which is only ramified at 5.

Proof. Take $x = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$ and $y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. We have $x^4 = y^5 = 1$ and

$$yx = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = xy^2.$$

So $F_{20} \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in F_5^*, b \in F_5 \right\} \subset \mathrm{GL}_2(\mathbb{F}_5)$, which is not a semi-simple subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$. On the other hand, we know F_{20} is the Galois group of the splitting fields of the equations $x^5 - 5$ and $x^5 + 5x^3 + 5x - 1$ by [PARI2]. □

Chapter 3

Function Field Case

In this chapter, we consider extensions of function fields $k = \mathbb{F}_q(t)$ ramified only at one finite prime $\mathfrak{f}$, generated over k by an irreducible polynomial $f \in \mathbb{F}_q[t]$ with $\deg(f) = d$, where $\mathbb{F}_q$ is a finite field of order a power of p. We restrict to *geometric* extensions, i.e. there are no constant extensions.

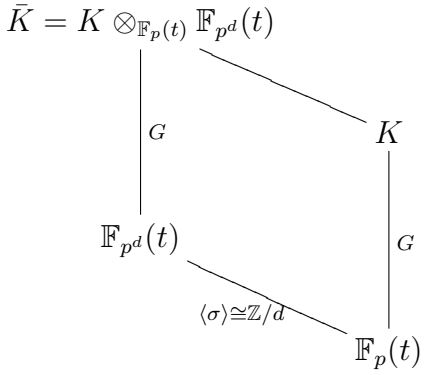
3.1 Tamely ramified covers

In this section, we will denote by k the rational function $\mathbb{F}_p(t)$, and denote by $\mathfrak{f}$ the ideal generated by an irreducible polynomial $f \in \mathbb{F}_p[t]$. Let $U_\mathfrak{f} = \mathbb{A}^1_k - (f = 0)$.

PROPOSITION 3.1.1. *Let K be the function field of a geometric Galois cover of the affine line over $\mathbb{F}_p$ with Galois group G and ramified only at a finite prime $\mathfrak{f}$ and possibly at ∞, with all ramification tame. Then there exist $x_1, x_2, ..., x_d, x_\infty \in G$ such that $\langle x_1, ..., x_d, x_\infty \rangle = G$ and $x_1 ... x_d x_\infty = 1$ with $x_1^p \sim x_2, ..., x_d^p \sim x_1$ and $x_\infty^p \sim x_\infty$ (i.e. conjugate in G). Moreover, the order of each of $x_1, \ldots, x_d$ is equal to the ramification index over $\mathfrak{f}$, and the order of x_∞ is the ramification index at ∞. So if $K/\mathbb{F}_p(t)$ is unramified at ∞, then $x_\infty = 1$.*

Proof. Suppose $\deg(\mathfrak{f}) = d$. After the base change to $\mathbb{F}_{p^d}(t)$, the prime $\mathfrak{f}$ splits into d primes $\mathfrak{f}_1, ..., \mathfrak{f}_d$ with degree 1, which correspond to d finite places $P_1, ..., P_d$ of $\mathbb{F}_{p^d}(t)$. Since ∞ has degree 1 in $\mathbb{F}_q(t)$, there is a unique place P_∞ of $\mathbb{F}_{q^d}(t)$ above

∞.



For each place P_i, where $1 \leq i \leq d$ or $i = \infty$, there are g places $Q_{i,1}, Q_{i,2}, ..., Q_{i,g}$ of $\bar{K}$ above P_i, since $\bar{K}$ is Galois over $\mathbb{F}_p(t)$. Each place $Q_{i,j}$ has an inertia group $I_{i,j}$. Since the extension is tamely ramified, each $I_{i,j}$ is cyclic, say generated by $x_{i,j}$, i.e. $I_{i,j} = \langle x_{i,j} \rangle$. Fixing i, the inertia groups $I_{i,j}$ are all conjugate in G. The Galois group $\mathrm{Gal}\left(F_{p^d}(t)/F_p(t)\right) \cong \mathbb{Z}/d = \langle\sigma\rangle$ is generated by the Frobenius map σ, which cyclicly permutes the places P_i where $1 \leq i \leq d$; say $\sigma(P_i) = P_{i+1}$. Also, $\sigma(P_\infty) = P_\infty$. On the other hand, there is a choice of places Q_i above P_i for $1 \leq i \leq d$ and $i = \infty$ such that the generators x_i of the corresponding inertia groups generate the Galois group G, i.e. $\langle x_1, ..., x_d, x_\infty \rangle = G$, and $x_1 x_2 ... x_d x_\infty = 1$. (Namely, these Q_i's are specializations of corresponding ramification points of a lift of this tame cover to characteristic 0, as in [Gro] XIII.) Since all the places P_i with $1 \leq i \leq d$ lie over the same closed point $\mathfrak{f}$, there is an additional condition on the group G. Namely, the Frobenius map σ takes the place Q_1 to some Q_2' over P_2; but the inertia group I_2 and I_2' are conjugate, so $x_1^p \sim x_2$. Similarly $x_2^p \sim x_3, ..., x_d^p \sim x_1$. Since the Frobenius map σ maps the place Q_∞ to some place Q_∞' over P_∞, we have $x_\infty^p \sim x_\infty$. $\square$

Now we consider Galois covers of the projective line $\mathbb{P}^1_{\mathbb{F}_p(t)}$ ramified only at a finite prime $\mathfrak{f}$, generated by an irreducible polynomial f in $\mathbb{F}_p[t]$, and unramified at ∞. So $U_\mathfrak{f} = \mathbb{P}^1_{\mathbb{F}_p(t)} - (f = 0)$.

Corollary 3.1.2. *Let n be a positive integer. Suppose the degree d of the prime $\mathfrak{f}$ is not divisible by n, and consider the group $G \cong P \rtimes \mathbb{Z}/(p^n - 1)$, where P is a p-group of order p^n and the semi-direct product G corresponds to the action of $\mathbb{F}_{p^n}^*$ on $\mathbb{F}_{p^n}$. Then $G \notin \pi_A^t(U_\mathfrak{f})$ where $U_\mathfrak{f} = \mathbb{P}^1_{\mathbb{F}_p(t)} - (f = 0)$.*

Proof. Otherwise suppose $G \in \pi_A^t(U_\mathfrak{f})$, where $d = \deg(f)$ is not divisible by n. By Proposition 3.1.1, we have $G = \langle x_1, \ldots, x_d \rangle$ with relations $x_1^p \sim x_2, \ldots, x_d^p \sim x_1$ and $x_1 \cdots x_d = 1$. From the relation $x_1^p \sim x_2, \ldots, x_d^p \sim x_1$, we have $x_i^{p^d} \sim x_i$ for $1 \leq i \leq d$. Write $x_i = (a_i, b_i)$, where $a_i \in P$ and $b_i \in \mathbb{Z}/(p^n - 1)$. Then $x_i \notin P$, for otherwise all x_i's are in the normal subgroup P and can not generate the group

G. Also one of b_i has to be a generator of $\mathbb{Z}/(p^2-1)$, otherwise the x_i's will not generate the whole group G. So $b_i^{p^d} = b_i$, which implies $p^d \equiv 1 \pmod{p^n-1}$. Since $p^d \equiv 1 \pmod{p^n-1}$ if and only if $n \mid d$, we have $n|d$. This is a contradiction. $\square$

Example. Let $p = 2$ and $n = 2$ in Corollary 3.1.2. We have $A_4 \notin \pi_A^t(U_\mathfrak{f})$ for any prime generated by an irreducible polynomial $f \in \mathbb{F}_p[t]$ of odd degree.

Remark. In fact, the conclusion in 3.1.2 can also be obtained using cyclotomic function fields, which we will introduce in the next section, i.e. there are no cyclic extensions of order $p^n - 1$ over $\mathbb{F}_p(t)$ ramified only at one finite prime $\mathfrak{f}$ (and the ramification is tame) of degree not divisible by n.

Applying the proposition to dihedral groups $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1}\rangle$ and symmetric groups S_n, we can get other corollaries:

COROLLARY 3.1.3. *For any integer $k \geq 1$, the dihedral group $D_{4k} \notin \pi_A^t(U_f)$. For the case of D_{4k+2}, when the degree of the finite prime $d = deg(f)$ is odd, we also have $D_{4k+2} \notin \pi_A^t(U_f)$.*

Proof. Suppose that $K/\mathbb{F}_p(t)$ is a geometric Galois extension with group D_{2n}, ramified only at a finite prime f with $\deg f = d$. Applying Proposition 3.1.1, we know $G = \langle x_1, ..., x_d\rangle$ with relations $x_1...x_d = 1$ and $x_1^p \sim x_2, ..., x_d^p \sim x_1$. Now we divide the situation into two cases (n is even and n is odd):

Case ($n = 2k$). The conjugacy classes in D_{2n} are

$$\{1\}, \{r^k\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, ..., \{r^{\pm(k-1)}\}, \{sr^{2b} \mid b = 1, ..., k\}, \{sr^{2b-1} \mid b = 1, ..., k\}.$$

If one of $x_1, ..., x_d$ is a power of r, then all the x_i's have to be a power of r because of the conjugate relations. This is a contradiction since such x_i's cannot generate the group D_{2n}. So we have $x_i = sr^{t_i}$, $1 \leq i \leq d$, for some integers t_i. If some t_i is even, then again by the conjugate relations all t_i's have to be even. This is a contradiction since such x_i's cannot generate the group D_{2n}. So we can write $x_i = sr^{2k_i+1}$, $1 \leq i \leq d$, which implies

$$sr^{2k_1+1} \cdot sr^{2k_2+1} \cdots sr^{2k_{d-1}+1} \cdot sr^{2k_d+1} = 1.$$

This is impossible. Therefore $D_{4k} \notin \pi_A^t(U_f)$.

Case ($n = 2k + 1$). The conjugacy classes in D_{2n} are

$$\{1\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, ..., \{r^{\pm k}\}, \{sr^b \mid b = 1, ..., n\}.$$

Similarly we can write $x_i = sr^{k_i}$, $1 \leq i \leq d$, which gives

$$sr^{k_1} \cdot sr^{k_2} \cdots sr^{k_{d-1}} \cdot sr^{k_d} = 1.$$

This is impossible if $2 \nmid d$. Thus $D_{4k+2} \notin \pi_A^t(U_f)$ if the degree of the prime f is odd.

□

COROLLARY 3.1.4. *In the case $p = 2$, any symmetric group $S_n \notin \pi_A^t(U_f)$ for any prime f of $\mathbb{F}_p(t)$. If $p \neq 2$ and f is of odd degree, then any symmetric group $S_n \notin \pi_A^t(U_f)$.*

Proof. Suppose that $K/\mathbb{F}_p(t)$ is a geometric Galois extension with group S_n, ramified only at a finite prime f with $\deg f = d$. Applying Proposition 3.1.1, we know there exist $x_1, ..., x_d$ such that $G = \langle x_1, ..., x_d \rangle$ with relations

$$x_1 \cdots x_d = 1 \qquad \text{and} \qquad x_1^p \sim x_2, ..., x_d^p \sim x_1.$$

When $p = 2$, all x_i's are even permutations since two permutations are conjugate in S_n if and only if they have the same cycle structure. This is impossible since they cannot generate S_n. So $S_n \notin \pi_A^t(U_f)$ in the case $p = 2$.

When $p \neq 2$, all x_i's are of the same parity. Since they generate S_n, they have to be odd permutations. So if d is odd, the product $\prod_{i=1}^d x_i$ of an odd number of odd permutations x_i's is still an odd permutation, which cannot be 1, contradiction. So $S_n \notin \pi_A^t(U_f)$ when $p \neq 2$ and f is of odd degree. □

3.2 Cyclotomic function fields

Analogously to cyclotomic number fields, L. Carlitz [Ca1] defined a "cyclotomic function field" $\mathbb{F}_q(t)(\lambda_f)$ for a polynomial $f \in \mathbb{F}_q[t]$, where λ_f is a primitive root of the equation $C_f(z) = 0$ for the Carlitz module C for $\mathbb{F}_q[t]$. Later D. Hayes [Hay1] published an exposition of Carlitz's idea and showed that it provided an explicit class field theory for rational function fields. Later developments, due independently to Hayes [Hay2] and V. Drinfeld [Dr], showed that Carlitz's ideas can be generalized to provide an explicit class field theory for any global function field.

Consider extensions over function fields $\mathbb{F}_q(t)$ where $\mathbb{F}_q$ is a finite field of order q, a power of p. The extension is ramified only at one finite prime (f), generated by an irreducible polynomial in $\mathbb{F}_q[t]$, and possibly at ∞. Similarly to cyclotomic number fields, Carlitz established a corresponding cyclotomic function field, such that for any finite abelian extension of $\mathbb{F}_q(t)$ in which ∞ is tamely ramified is contained in a constant field extension of a cyclotomic function field for some polynomial $f \in \mathbb{F}_q[t]$.

Let $k = \mathbb{F}_q(t)$, let $A = \mathbb{F}_q[t]$ and let k^{ac} be the algebraic closure of k. Carlitz showed in [Ca1] and [Ca2] that the additive group of k^{ac} becomes a right module over A under the following action: For any $u \in k^{ac}$ and any polynomial $f \in A$, define

$$u^f = f(\varphi + \mu)(u),$$

where $\varphi : k^{ac} \to k^{ac}$ is the Frobenius automorphism $\varphi(u) = u^q$ and $\mu : k^{ac} \to k^{ac}$ is the multiplication by t, i.e. $\mu(u) = tu$. For example $u^t = u^q + tu$. It is easy to

check that $(f,u) \to u^f$ gives the additive group of k^{ac} an A-module structure. For any polynomial $f \in A$ and $f \neq 0$, the *cyclotomic function field* $\mathbb{F}_q(t)(\lambda_f)$ is the field obtained from $\mathbb{F}_q(t)$ after adjoining a primitive root of the equation:

$$u^f = 0.$$

We will list some properties of Carlitz fields below:

1. Let $f \in \mathbb{F}_q[t]$ be a polynomial and let $(f) = (f_1)^{e_1}(f_2)^{e_2} \cdots (f_t)^{e_t}$ be its prime decomposition. Then the cyclotomic function field $\mathbb{F}_q(t)(\lambda_f)$ is the compositum of the cyclotomic function fields $\mathbb{F}_q(t)(\lambda_{f_i^{m_i}})$ (see Theorem 12.8 in [Ros]).

2. For an irreducible $f \in \mathbb{F}_q[t]$ with $\deg f = d$, the extension $\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t)$ has degree $\Phi(f^n) = q^{dn} - q^{d(n-1)}$, and the Galois group G_n is isomorphic to the group of units of $\mathbb{F}_q[t]/(f^n)$ (see Theorem 2.3 in [Hay1]), i.e.

$$G_n = \mathrm{Gal}\,(\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t)) \cong (\mathbb{F}_q[t]/(f^n))^*.$$

3. The infinite prime ∞ of $\mathbb{F}_q(t)$ splits completely into $\frac{\Phi(f^n)}{q-1}$ prime divisors ∞_i's in the sub-extension

$$\mathbb{F}_q(t)(\lambda_f)^+ := \mathbb{F}_q(t)(\prod_{\theta \in \mathbb{F}_q^*} \theta\lambda_f) = \mathbb{F}_q(t)(\lambda_f^{q-1})$$

   of index $q-1$ and then each ∞_i is totally ramified in $\mathbb{F}_q(t)(\lambda_f)$ (see Theorem 3.10.1 in [Th]). In particular, the infinite prime ∞ of $\mathbb{F}_q(t)$ is tamely ramified in $\mathbb{F}_q(t)(\lambda_f)/\mathbb{F}_q(t)$ with residue degree 1.

4. For any polynomial $f \in \mathbb{F}_q[t]$, the constant field of $\mathbb{F}_q(t)(\lambda_f)$ is $\mathbb{F}_q$ (see the corollary after Theorem 12.14 in [Ros]), i.e. $\mathbb{F}_q(t)(\lambda_f)/\mathbb{F}_q(t)$ is a geometric extension.

5. Any geometric abelian extension of $\mathbb{F}_q(t)$ with tame ramification at ∞ and trivial residue degree is contained in a cyclotomic function field $\mathbb{F}_q(t)(\lambda_f)$ for some f (see §5 in [Hay1]).

6. The conductor of $\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t)$ is f^n. Let $\mathfrak{D}$ be the different of the extension $\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t)$, where f a monic irreducible polynomial in $\mathbb{F}_q[t]$ with $\deg f = d$. Then (see Theorem 4.1 in [Hay1])

$$\mathfrak{D} = \mathfrak{f}^s \cdot \prod_{\mathfrak{p}|\infty} \mathfrak{p}^{q-2},$$

   where $\mathfrak{f}$ is the unique prime of $\mathbb{F}_q(t)(\lambda_{f^n})$ lying over f and $s = n(q^{nd} - q^{(n-1)d}) - q^{(n-1)d}$.

7. For an irreducible $f \in \mathbb{F}_q[t]$ with $\deg f = d$, denote by G_n the Galois group $\mathrm{Gal}\,(\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t))$. Then G_n can be decomposed into a product $G'_n \times G''_n$, where $G'_n \cong (\mathbb{F}_q[t]/(f))^*$ is a cyclic group of order $q^d - 1$ and G''_n is a product of cyclic p-groups $G_n^{(i,j)}$ with orders $g_n^{(j)}$ (see Proposition 3.2 in [GS]), i.e.

$$G_n \cong G'_n \times \prod_{i=1}^{r} (G_n^{(i,1)} \times ... \times G_n^{(i,m)}),$$

where $g_n^{(1)} \geq ... \geq g_n^{(m)}$. The order of G''_n is $q^{d(n-1)}$. In particular, when $n = 1$, the order of G''_n is 1. Let p^{d_n} be the exact power of p dividing n. For each $0 \leq i$, write $n = u_i p^i + v_i$, $0 \leq v_i < p^i$. Then for any integer k with $1 \leq k \leq g_n^{(1)}$, the number of $G_n^{(i,j)}$ with order exactly p^k is :

$$\begin{cases} rd(u_{k-1} - 2u_k + u_{k+1}) & \text{for } k < d_n, \\ rd(u_{k-1} - 2u_k + u_{k+1} + 1) & \text{for } k = d_n, \\ rd(u_{k-1} - 2u_k + u_{k+1} - 1) & \text{for } k = d_n + 1, \\ rd(u_{k-1} - 2u_k + u_{k+1}) & \text{for } k > d_n + 1, \end{cases} \tag{3.2.1}$$

Now we consider the polynomial u^f. It is a separable polynomial in u of degree q^d,

$$u^f = \sum_{i=0}^{d} [{}^f_i] u^{q^i},$$

where d is the degree of f and $[{}^f_i]$ is a polynomial in A of degree $(d-i)q^i$. For the coefficients, we know that $[{}^f_0] = f$, and $[{}^f_d]$ is the leading coefficient of f. But the formula for $[{}^f_d]$ is really complicated to compute $[{}^f_d]$.

Example. Take the irreducible polynomial $f = t^2 + t + 1$. Then

$$u^f = u^{q^2} + (t^q + t + 1)u^q + (t^2 + t + 1)u.$$

The cyclotomic function field for $f = t^2 + t + 1$ is the field obtained by adjoining the roots of the equation $0 = u^f = u^{q^2} + (t^q + t + 1)u^q + (t^2 + t + 1)u$ in k^{ac} to $\mathbb{F}_q(t)$.

It is hard to describe explicitly what cyclotomic function fields are in general. There is an explicit way to describe the cyclotomic function field over $k = \mathbb{F}_q(t)$ ramified only at one prime $f \in \mathbb{F}_q[t]$. Consider a degree d irreducible polynomial $f = \prod_{i=1}^{d}(t - \alpha_i)$, where $\alpha_i \in \mathbb{F}_{q^d}$ are the d roots of f, for $1 \leq i \leq d$.

Proposition 3.2.2. *For $f = \prod_{i=1}^{d}(t - \alpha_i)$ as above, the cyclotomic function field $\mathbb{F}_q(t)(\lambda_f)/\mathbb{F}_q(t)$ is the unique maximal cyclic geometric sub-extension K_0 of $K = \mathbb{F}_{q^d}(t)(y_0)$ over $\mathbb{F}_q(t)$ such that the residue degree of the prime f is 1, where*

K is the Kummer extension $\mathbb{F}_{q^d}(t)(y_0)/\mathbb{F}_{q^d}(t)$ *of degree* q^d-1 *over the constant extension* $\mathbb{F}_{q^d}(t)/\mathbb{F}_q(t)$ *and*

$$y_0^{q^d-1} = \prod_{i=1}^{d}(x-\alpha_i)^{q^{d-i}}.$$

Proof. First we will show that the extension $\mathbb{F}_{q^d}(t)(y_0)/\mathbb{F}_q(t)$ is abelian with Galois group $\mathbb{Z}/(q^d-1)\times\mathbb{Z}/d$, thus it descends to a cyclic sub-extension of $\mathbb{F}_q(t)$ of degree q^d-1. We consider the tower of extensions

$$\begin{array}{c} \mathbb{F}_{q^d}(t)(y_0) \\ \Big| \ \mathbb{Z}/(q^d-1)\cong<\tau> \\ \mathbb{F}_{q^d}(t) \\ \Big| \ \mathbb{Z}/d\cong<\sigma^r> \\ \mathbb{F}_q(t) \end{array}$$

The Frobenius automorphism σ^r generates $\mathrm{Gal}\left(\mathbb{F}_{q^d}(t)/\mathbb{F}_q(t)\right)$, where

$$\sigma^r : \mathbb{F}_{q^d}(t) \longrightarrow \mathbb{F}_{q^d}(t)$$

sends $\alpha_i \to (\alpha_i)^q = \alpha_{i+1}$ for $1 \le i \le d-1$, $\alpha_d \to (\alpha_d)^q = \alpha_1$, and sends t to t.

Let τ generate $\mathrm{Gal}\left(\mathbb{F}_{q^d}(t)(y_0)/\mathbb{F}_{q^d}(t)\right)$, where

$$\tau : \mathbb{F}_{q^d}(t)(y_0) \longrightarrow \mathbb{F}_{q^d}(t)(y_0)$$

fixes t and α_i, for all $1 \le i \le d$, and sends y_0 to $\alpha_1 y_0$.

Take a lift $\bar{\sigma}^r$ of σ^r in $\mathrm{Gal}\left(\mathbb{F}_{q^d}(t)(y_0)/\mathbb{F}_q(t)\right)$. Then

$$\bar{\sigma}^r : \mathbb{F}_{q^d}(t)(y_0) \to \mathbb{F}_{q^d}(t)(y_0)$$

sends $\alpha_d \to \alpha_1$, $t \to t$, $\alpha_i \to \alpha_{i+1}$ for $1 \le i \le d-1$. To get the image of y_0 under the action of $\bar{\sigma}^r$, we consider the image of $y_0^{q^d-1} = \prod_{i=1}^{d}(x-\alpha_i)^{q^{d-i}}$,

$$(x-\alpha_1)^{q^{d-1}}\ldots(x-\alpha_{d-1})^{q^1}(x-\alpha_d)^{q^0} \mapsto (x-\alpha_2)^{q^{d-1}}\ldots(x-\alpha_d)^{q^1}(x-\alpha_1)^{q^0}.$$

The image of $y_0^{q^d-1}$ is $(x-\alpha_2)^{q^{d-1}}\ldots(x-\alpha_d)^{q^1}(x-\alpha_1)^{q^0} = (\dfrac{y_0^q}{x-\alpha_1})^{q^d-1}$. So we can pick $\dfrac{y_0^q}{x-\alpha_1}$ to be the image of y_0 under the action of $\bar{\sigma}^r$. We know that τ and $\bar{\sigma}$ generate $\mathrm{Gal}\left(\mathbb{F}_{q^d}(t)(y_0)/\mathbb{F}_q(t)\right)$. To check τ and $\bar{\sigma}$ commute, we will look at the

images of α_i for $1 \leq i \leq d$ and y_0 under the actions of $\tau\bar{\sigma}^r$ and $\bar{\sigma}^r\tau$. The action of $\tau\bar{\sigma}^r$ is as follows:

$$\begin{array}{ccccc} \alpha_1 & \xrightarrow{\tau} & \alpha_1 & \xrightarrow{\bar{\sigma}^r} & \alpha_2, \\ \vdots & & \vdots & & \vdots \\ \alpha_d & \xrightarrow{\tau} & \alpha_d & \xrightarrow{\bar{\sigma}^r} & \alpha_1, \\ y_0 & \xrightarrow{\tau} & \alpha_1 y_0 & \xrightarrow{\bar{\sigma}^r} & \dfrac{\alpha_2 y_0^q}{x-\alpha_1}; \end{array}$$

and the action of $\bar{\sigma}^r\tau$ is as follows:

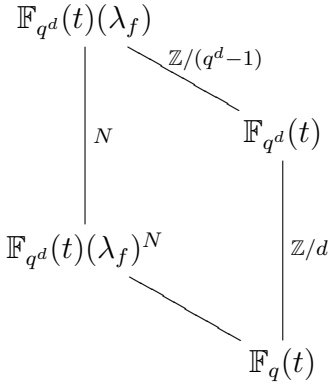
$$\begin{array}{ccccc} \alpha_1 & \xrightarrow{\bar{\sigma}^r} & \alpha_2 & \xrightarrow{\tau} & \alpha_2, \\ \vdots & & \vdots & & \vdots \\ \alpha_d & \xrightarrow{\bar{\sigma}^r} & \alpha_1 & \xrightarrow{\tau} & \alpha_1, \\ y_0 & \xrightarrow{\bar{\sigma}^r} & \dfrac{y_0^q}{x-\alpha_1} & \xrightarrow{\tau} & \dfrac{\alpha_1^q y_0^q}{x-\alpha_1}. \end{array}$$

Since $\alpha_1^q = \alpha_2$, we know $\tau\bar{\sigma}^r = \bar{\sigma}^r\tau$. So there is an isomorphism

$$\mathrm{Gal}\,(K/\mathbb{F}_q(t)) \cong \mathbb{Z}/(q^d-1) \times \mathbb{Z}/d,$$

where the residue extension at the prime f corresponds to the summand $\mathbb{Z}/d$, generated by $(0,1)$. Denote by N_0 the subgroup generated by $(0,1)$. Let K_0 be the fixed field of N_0 in $K/\mathbb{F}_q(t)$. Then K_0 is a maximal cyclic geometric sub-extension of $K/\mathbb{F}_q(t)$.

Next we will show K_0 is the only such sub-extension with residue degree 1 at the prime f. Consider all possible sub-extensions of degree q^d-1 inside $K/\mathbb{F}_q(t)$. Each such sub-extension corresponds to a quotient group of $\mathbb{Z}/(q^d-1) \times \mathbb{Z}/d$ by a subgroup of order d.



The element $(0,1)$ is not in any subgroup N of order d other than N_0, for otherwise $(0,i) \in N$ for $1 \leq i \leq d$, which would imply $N_0 \subset N$. But N is a subgroup of order d, thus $N_0 \subset N$. But N is of order d, so $N = N_0$. So N_0 is the unique subgroup of

$\mathbb{Z}/(q^d-1)\times\mathbb{Z}/d$, which is of order d, such that $\overline{(0,1)}=0$ in the quotient group; i.e. the fixed field K_0 of N_0 is the unique sub-extension of degree q^d-1 with residue degree 1.

Finally we will show K_0 is the cyclotomic function field $\mathbb{F}_q(t)(\lambda_f)$. We know $K_0/\mathbb{F}_q(t)$ is a cyclic extension ramified only at f and ∞ with residue degree 1 at the prime f. By Property 5 above of Carlitz fields, we know K_0 is contained in a cyclotomic function field $\mathbb{F}_q(t)(\lambda_{f^m})$ for some m. The Galois group $\mathrm{Gal}\,(\mathbb{F}_q(t)(\lambda_{f^m})/\mathbb{F}_q(t))$ has a unique p-Sylow subgroup by Sylow's theorem. Thus there is only one sub-extension of degree q^d-1 in $\mathbb{F}_q(t)(\lambda_{f^m})/\mathbb{F}_q(t)$. Since $\mathbb{F}_q(t)(\lambda_f)$ is the sub-extension of degree q^d-1, we have $K_0=\mathbb{F}_q(t)(\lambda_f)$. □

Notice that in Proposition 3.2.2, the cyclotomic function field is tamely ramified. We can generalize Proposition 3.2.2 to the wildly ramified case, i.e. a description of cyclotomic function fields $\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t)$ for any positive integer n. Let $\omega_1,\ldots,\omega_r$ be a basis of $\mathbb{F}_q$ as vector space over $\mathbb{F}_p$. Again $f=\prod_{i=1}^{d}(t-\alpha_i)$ will denote a degree d irreducible polynomial in $\mathbb{F}_q[t]$, where $\alpha_i\in\mathbb{F}_{q^d}$ are the d roots of f, for $1\le i\le d$.

THEOREM 3.2.3. *The cyclotomic function field $\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t)$ is given by the compositum of the Kummer extension K_0 and the Witt-Artin-Schreier extensions $K_n^{(i,j)}$ for $i=1,...,r$, $j=1,...,d(n-1)$, where $q=p^r$, K_0 and $K_n^{(i,j)}$'s are defined inductively as follows:*

1) *K_0 is defined as in Proposition 3.2.2, i.e. the unique maximal cyclic geometric sub-extension of $\mathbb{F}_{q^d}(t)(y_0)/\mathbb{F}_q(t)$ such that the residue degree of the prime f is 1, where*
$$y_0^{q^d-1}=\prod_{i=1}^{d}(x-\alpha_i)^{q^{d-i}}.$$

2) *When $p\nmid[\frac{j-1}{d}]+1$, then $K_n^{(i,j)}=\mathbb{F}_q(t)(y_{ij})$, with*
$$y_{ij}^p-y_{ij}=\frac{\omega_i t^{j-[\frac{j-1}{d}]-1}}{f^{1+[\frac{j-1}{d}]}}.$$

3) *When $p\mid[\frac{j-1}{d}]+1$, then $K_n^{(i,j)}$ is the unique $\mathbb{Z}/p$ geometric extension of $K_n^{(i,t_j)}$ with residue degree 1, which is cyclic over $\mathbb{F}_q(t)$ with ramification occurs only at f, where $t_j=j-d(p-1)(\frac{[\frac{j-1}{d}]+1}{p})$.*

Before we prove Theorem 3.2.3, we need two lemmas. Both lemmas are under the same assumptions as before, i.e. let $\omega_1,\ldots,\omega_r$ be a basis of $\mathbb{F}_q$ as vector space over $\mathbb{F}_p$; let f be an irreducible polynomial with degree d; and let $\alpha_1,\ldots,\alpha_d\in\mathbb{F}_{p^d}(t)$ be the d roots of f.

LEMMA 3.2.4. *Let K_2'' be the maximal p-sub-extension of the extension $\mathbb{F}_q(t)(\lambda_{f^2})$ over $\mathbb{F}_q(t)$. Then K_2'' is the compositum of rd Artin-Scheier extensions $K_2^{(i,j)}$, where*

$$K_2^{(i,j)} = \mathbb{F}_q(t)(y_{ij}) \qquad with \qquad y_{ij}^p - y_{ij} = \frac{\omega_i t^{j-1}}{f},$$

for $1 \le i \le r,\ 1 \le j \le d$.

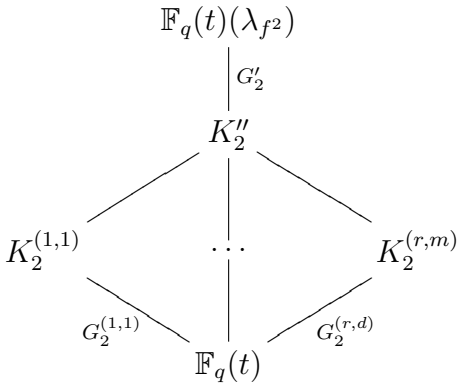
Proof. By Property 7 of cyclotomic function fields, we know the Galois group $G_2 = \mathrm{Gal}\,(\mathbb{F}_q(t)(\lambda_{f^3})/\mathbb{F}_q(t))$ is a product of a cyclic group G_2' of order q^d-1 and a product G_2'' of cyclic p-groups $G_n^{(i,j)}$:

$$G_2 \cong G_2' \times G_2'' \cong \mathbb{Z}/(q^d-1) \times (\prod_{(i,j)} G_2^{(i,j)}).$$

So K_2'' is the fixed field of G_2', and the Galois group $\mathrm{Gal}\,(K_2''/\mathbb{F}_q(t)) \cong G_2''$. Applying Proposition 3.2 in [GS] to the cyclotomic function field $\mathbb{F}_q(t)(\lambda_{f^2})$, we know G_2'' is a product of $\mathbb{Z}/p$'s, and the number of $\mathbb{Z}/p$'s is rd, i.e.

$$G_2'' \cong \prod_{1\le i\le r, 1\le j\le d} G_2^{(i,j)} \cong (\mathbb{Z}/p)^{rd}.$$

Denote by $K_2^{(i_0,j_0)}$ the fixed field of $G_2' \times \prod_{(i,j)\neq(i_0,j_0)} G_2^{(i,j)}$ in $\mathbb{F}_q(t)(\lambda_{f^2})$ over $\mathbb{F}_q(t)$. Then the Galois group $\mathrm{Gal}\left(K_2^{(i,j)}/\mathbb{F}_q(t)\right) \cong G_2^{(i,j)}$. And K_2'' is the compositum of all the $K_2^{(i,j)}$'s. We know $\mathbb{F}_q(t)(\lambda_{f^2})/\mathbb{F}_q(t)$ is ramified and totally ramified only at the prime $\mathfrak{f}$, generated by the irreducible polynomial f. So each $K_2^{(i,j)}/\mathbb{F}_q(t)$ is also ramified only at the prime $\mathfrak{f}$ and it is cyclic of degree p.



So each $K_2^{(i,j)}$ is an Artin-Scheier extension over $\mathbb{F}_q(t)$ ramified only at f, which can be expressed in the following way:

$$K_2^{(i,j)} = \mathbb{F}_q(t)(y_{ij}), \qquad \text{where} \qquad y_{ij}^p - y_{ij} = \beta_{ij}; \quad \beta_{i,j} \in \mathbb{F}_q(t).$$

Using the partial fraction decomposition of $\beta_{i,j}$ to adjust the function y_{ij}, we can assume $\beta_{i,j}$ is in the standard form, i.e.

$$\beta_{ij} = \frac{q_{ij}(t)}{f^{\gamma_{ij}}},$$

where $q_{ij}(t)$ is a polynomial relatively prime to f with $\deg(q_{ij}(t)) < \deg(f^{\gamma_{ij}}) = d\gamma_{ij}$. The exponent $\mathfrak{f}$ in the discriminant $\mathfrak{d}_{K_n^{(i,j)}/\mathbb{F}_q(t)}$ is

$$(p-1)(\gamma_{ij}+1).$$

On the other hand, we know, from Property 6, the exponent of $\mathfrak{f}$ in the discriminant $\mathfrak{d}_{\mathbb{F}_q(t)(\lambda_{f^2})/\mathbb{F}_q(t)}$ is $2q^{2d} - 3q^d$. Using these discriminant, we can conclude that $\gamma_{ij} = 1$ for all i, j's. Otherwise suppose there exists a $\gamma_{ij} \geq 2$.

Case $(p > 2)$. In this case, we would have the discriminant $\mathfrak{d}_{\mathbb{F}_q(t)(\lambda_{f^2})/\mathbb{F}_q(t)}$ given as follows:

$$2q^{2d} - 3q^d = \mathfrak{d}_{\mathbb{F}_q(t)(\lambda_{f^2})/\mathbb{F}_q(t)} \geq 3(p-1)\frac{q^{2d}-q^d}{p} > 2q^{2d} - 3q^d;$$

this is a contradiction.

Case $(p = 2)$. The extension $K_2''/\mathbb{F}_q(t)$ is totally ramified, so each intermediate extension has to be ramified. Thus we have

$$\begin{aligned} 2q^{2d} - 3q^d = \mathfrak{d}_{\mathbb{F}_q(t)(\lambda_{f^2})/\mathbb{F}_q(t)} &\geq 3(p-1)\frac{q^{2d}-q^d}{p} + (1+p+p^2+...+p^{rd-2})(q^d-1) \\ &= 2q^{2d} - 3q^d + 1 \\ &> 2q^{2d} - 3q^d, \end{aligned}$$

again getting a contradiction.

So the y_{ij}'s satisfying

$$y_{ij}^p - y_{ij} = \frac{\omega_i t^{j-1}}{f} \qquad \text{for} \qquad 1 \leq i \leq r,\ 1 \leq j \leq d$$

form a basis for the extension $K_n''/\mathbb{F}_q(t)$. □

The next lemma describes how the Galois group

$$G_{n+1}'' = \mathrm{Gal}\left(\mathbb{F}_q(t)(\lambda_{f^{n+1}})/\mathbb{F}_q(t)\right)$$

is obtained from the Galois group $G_n'' = \mathrm{Gal}\left(\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t)\right)$. For any $n \geq 2$, the group G_n'' is a product $\prod_{(i,j)} G_n^{(i,j)}$ of cyclic p-groups $G_n^{(i,j)}$. Denote the number of $G_n^{(i,j)}$'s with order exactly p^k by $S_{n,k}$.

LEMMA 3.2.5. *Let p^{d_n} be the exact power of p dividing n. If $d_n = 0$, we have*

$$S_{n+1,k} = \begin{cases} S_{n,k} + rd & \text{if } k = 1, \\ S_{n,k} & \text{otherwise.} \end{cases}$$

If $d_n \geq 1$, we have

$$S_{n+1,k} = \begin{cases} S_{n,k} - rd & \text{if } k = d_n, \\ S_{n,k} + rd & \text{if } k = d_n + 1, \\ S_{n,k} & \text{otherwise.} \end{cases}$$

Equivalently, when $p \nmid n$, we have $G''_{n+1} = G''_n \times (\mathbb{Z}/p)^{rd}$; and when $p \mid n$, we know G''_{n+1} has rd more copies of $\mathbb{Z}/p^{1+d_n}$ and rd less copies of $\mathbb{Z}/p^{d_n}$,

Proof. The extension $\mathbb{F}_q(t)(\lambda_{f^{n+1}})/\mathbb{F}_q(t)(\lambda_{f^n})$ is of degree $q^d = p^{rd}$. For each $i \geq 0$, we can write $n = u_i p^i + v_i$ with $0 \leq v_i < p^i$. We will divide the situation into three cases as follows, and apply Result 3.2.1 in Property 7 of cyclotomic function fields.

Case ($n \neq 0, -1 \pmod p$). We have $d_n = 0$ and $d_{n+1} = 0$. Applying 3.2.1, we know the number of $G_n^{(i,j)}$ with order p is $rd(n - 2u_1 + u_2 - 1)$, while the number of $G_{n+1}^{i,j}$ with order p is $rd(n + 1 - 2u_1 + u_2 - 1)$, the difference is exactly rd. So $G''_{n+1} = G''_n \times (\mathbb{Z}/p)^{rd}$.

Case ($n = -1 \pmod p$). Here $d_n = 0$. Let $n+1 = u'_i p^i + v'_i$, then $n = u'_{d_{n+1}} p^{d_{n+1}} - 1$.

- $d_{n+1} = 1$. By 3.2.1, the number of $G_n^{(i,j)}$ with order p is $rd(n - 2u_1 + u_2 - 1)$, while the number of $G_{n+1}^{(i,j)}$ with order p is $rd(n + 1 - 2u'_1 + u'_2 + 1)$. We have $n + 1 = u'_1 p$ and $n = (u'_1 - 1)p + (p - 1)$, so $u_1 = u'_1 - 1$ and $u'_2 = u_2$, thus $G''_{n+1} = G''_n \times (\mathbb{Z}/p)^{rd}$.

- $d_{n+1} \geq 2$. By 3.2.1, the number of $G_n^{(i,j)}$ with order p is $rd(n - 2u_1 + u_2 - 1)$, while the number of $G_{n+1}^{(i,j)}$ with order p is $rd(n + 1 - 2u'_1 + u'_2)$. We have $n + 1 = u'_2 p^2$ and $n = (u'_2 - 1)p^2 + (p^2 - 1)$, so $u'_1 = u_1 + 1$ and $u'_2 = u_2 + 1$, thus $G''_{n+1} = G''_n \times (\mathbb{Z}/p)^{rd}$.

Case ($n = 0 \pmod p$). Here $d_{n+1} = 0$. Let $n = u_i p^i + v_i$ and $n + 1 = u'_i p^i + v'_i$.

- $d_n = 1$. We have $n = u_1 p$ and $n + 1 = u_1 p + 1$, so $u_1 = u'_1$, $u'_2 = u_2$ and $u'_3 = u_3$. By 3.2.1, the number of $G_n^{(i,j)}$ with order p is $rd(n - 2u_1 + u_2 + 1)$, while the number of $G_{n+1}^{(i,j)}$ with order p is $rd(n + 1 - 2u'_1 + u'_2 - 1)$, so G''_{n+1} has rd copies of $\mathbb{Z}/p$ less than G''_n. Also the number of $G_n^{(i,j)}$ with order p^2 is $rd(u_1 - 2u_2 + u_3 - 1)$, while the number of $G_{n+1}^{(i,j)}$ with order p^2 is $rd(u'_1 - 2u'_2 + u'_3)$. So G''_{n+1} has rd copies of $\mathbb{Z}/p^2$ more than G''_n.

- $d_n \geq 2$. We know $u'_i = u_i$ for all $i \geq 1$. The number of $G_n^{(i,j)}$ with order p^{d_n} is $rd(u_{d_n-1} - 2u_{d_n} + u_{d_n+1} + 1)$, while the number of $G_{n+1}^{(i,j)}$ with order p^{d_n} is $rd(u'_{d_n-1} - 2u'_{d_n} + u'_{d_n+1})$. The number of $G_n^{(i,j)}$ with order p^{d_n+1} is $rd(u_{d_n} - 2u_{d_n+1} + u_{d_n+2} - 1)$, while the number of $G_{n+1}^{(i,j)}$ with order p^{d_n+1} is $rd(u'_{d_n} - 2u'_{d_n+1} + u'_{d_n+2})$. So G''_{n+1} has rd more copies of $\mathbb{Z}/p^{d_n+1}$ and rd less copies of $\mathbb{Z}/p^{d_n}$.

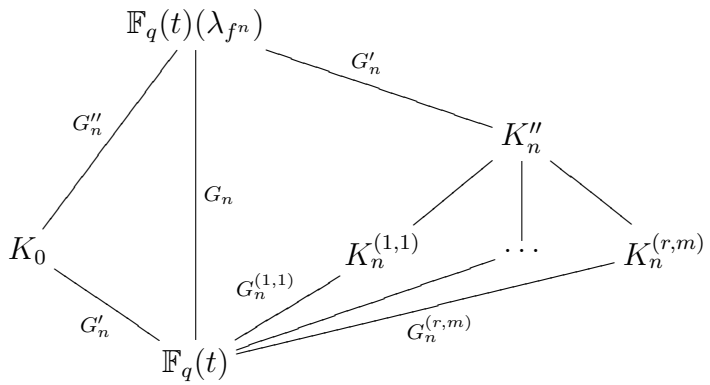
So when $p \nmid n$, we have $G''_{n+1} = G''_n \times (\mathbb{Z}/p)^{rd}$; and when $p \mid n$, we know G''_{n+1} has rd more copies of $\mathbb{Z}/p^{1+d_n}$ and rd less copies of $\mathbb{Z}/p^{d_n}$, where d_n is the exact power of p that divides n. □

Now we can give the proof for Theorem 3.2.3.

Proof. The Galois group $G_n = \mathrm{Gal}\,(\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t))$ can be decomposed as a product of a cyclic group G'_n of order $q^d - 1$ and a product G''_n of cyclic p-groups $G_n^{(i,j)}$ with order $g_n^{(j)}$ by Property 7, i.e.

$$G_n \cong G'_n \times G''_n = G'_n \times \prod_{i=1}^{r} (G_n^{(i,1)} \times ... \times G_n^{(i,m)}),$$

where $g_n^{(1)} \geq ... \geq g_n^{(m)}$, and the Galois group G''_n is of order $q^{d(n-1)}$. Let K_0 be the fixed field of G''_n in $\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t)$. Let K''_n be the fixed field of G'_n in $\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t)$. And let $K_n^{(a,b)}$ be the fixed field of $G'_n \times \prod_{(i,j)\neq(a,b)} G_n^{(i,j)}$ in $\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t)$. So the cyclotomic function field $\mathbb{F}_q(t)(\lambda_{f^n})$ is the compositum of the K_0 and $K_n^{(i,j)}$'s. We will give descriptions of the K_0 and $K_n^{(i,j)}$'s.



First we consider the field K_0. Since the Sylow-p subgroup G''_n is normal in G_n, it is the unique Sylow-p subgroup by the Sylow's theorem. So the field K_0 is the unique subfield of order $q^d - 1$ in $\mathbb{F}_q(t)(\lambda_{f^n})/\mathbb{F}_q(t)$. Thus it is the cyclotomic function field $\mathbb{F}_q(t)(\lambda_f)$, which is the Kummer extension known from Proposition 3.2.2.

Next we will give descriptions of $K_n^{(i,j)}$'s. Each field $K_n^{(i,j)}$ is a cyclic p-extension over $\mathbb{F}_q(t)$, so it is a Witt-Artin-Scheier extension. We will use induction on n to show the field $K_n^{(i,j)}$ is described as in 2) and 3). The induction starts with $n = 2$, since G_n'' is trivial when $n = 1$. The case $n = 2$ is dealt in Lemma 3.2.4. Suppose ok for $\leq n$, we consider the case $n + 1$. We will analyze the situation in two cases using lemma 3.2.5.

- When $p \nmid n$, we know $G_{n+1}'' = G_n'' \times (\mathbb{Z}/p)^{rd}$. But these new $\mathbb{Z}/p$ extensions all have conductor f^{n+1}. So the y_{ij}'s for $1 \leq i \leq r, d(n-1)+1 \leq j \leq dn$ satisfying
$$y_{ij}^p - y_{ij} = \frac{\omega_i t^{j-1-[\frac{j-1}{d}]}}{f^n} = \frac{\omega_i t^{j-1-[\frac{j-1}{d}]}}{f^{1+[\frac{j-1}{d}]}}$$
form a basis for the extension K_{n+1}''/K_n''.

- When $p \mid n$, we know G_{n+1}'' has rd more copies of $\mathbb{Z}/p^{1+d_n}$ and rd less copies of $\mathbb{Z}/p^{d_n}$, where d_n is the exact power of p that divides n. The sub-extensions of $K_n''/\mathbb{F}_q(t)$ corresponding to each copy of $\mathbb{Z}/q^{d_n}$ are $K_n^{(i,t_j)}$ for $1 \leq i \leq r$ and $d(n-1)+1 \leq j \leq dn$, where $t_j = j - d(p-1)(\frac{[\frac{j-1}{d}]+1}{p}$. Since K_n'' is contained in K_{n+1}'', so each sub-extension $K_{n+1}^{i,j}$ of $K_{n+1}''/\mathbb{F}_q(t)$ corresponding to $\mathbb{Z}/p^{1+d_n}$, where $1 \leq i \leq r$ and $d(n-1)+1 \leq j \leq dn$, is the unique cyclic $\mathbb{Z}/p$-extension of $K_n^{(i,t_j)}$ ramified only at the prime above f, such that $K_{n+1}^{i,j}/\mathbb{F}_q(t)$ is an Witt-Artin-Schreier extension over $\mathbb{F}_q(t)$ with conductor f^{n+1}.

So $\mathbb{F}_q(t)(\lambda_{f^n})$ is the compositum of the K_0 and $K_n^{(i,j)}$ as described in the theorem. □

Using this explicit description on of cyclotomic function fields, we can easily calculate the genus, discriminant and class number of abelian extensions over $\mathbb{F}_q(t)$ ramified over only one prime. This helps to understand abelian and solvable extensions over $\mathbb{F}_q(t)$ ramified over only one prime.

3.3 Riemann-Hurwitz formula

Let $K/\mathbb{F}_q(t)$ be a finite, separable, geometric extension of degree n with Galois group G, ramified only at one finite place f of degree d and unramified at ∞. Denote by g the genus of K. Let m be the conductor of the extension $K/\mathbb{F}_q(t)$, so the ith ramification group G_i vanishes for all $i \geq m$. Denote the order $|G_i|$ of the ramification group G_i by e_i. We have by the Riemann-Hurwitz formula,
$$\begin{aligned} 2g-2 &= n(2\cdot 0 - 2) + (e_0 + e_1 + e_2 + ... + e_{m-1} - m)\frac{nd}{e_0} \\ &= -2n + (e_0 + e_1 + e_2 + ... + e_{m-1} - m)\frac{nd}{e_0} \end{aligned}$$

Case $(g = 0)$.

PROPOSITION 3.3.1. *Let $K/\mathbb{F}_q(t)$ be a finite, separable, geometric extension with Galois group G, ramified only at one finite place f of degree d and unramified at ∞. Assume the genus of K is 0. If $K/\mathbb{F}_q(t)$ is tamely ramified, then K is contained in the cyclotomic function field $\mathbb{F}_q(t)(\lambda_f)$; if $K/\mathbb{F}_q(t)$ is wildly ramified, then G is a p-group.*

Proof. Plugging in $g = 0$ into the Riemann-Hurwitz formula, we have

$$-2e_0 = -2ne_0 + (e_0 + e_1 + e_2 + ... + e_{m-1} - m)dn.$$

So $n|2e_0$. Suppose $n = 2e_0$, then the inertia group $I = G_0$ is normal in G, since every subgroup of index 2 is normal.

$$\begin{array}{c} K \\ \Big| I \\ K^I \\ \Big| \mathbb{Z}/2 \\ \mathbb{F}_q(t) \end{array}$$

In this case, the fixed field K^I of I in $K/\mathbb{F}_q(t)$ is unramified over $\mathbb{F}_q(t)$ of degree 2; a contradiction. But $e_0|n$, so we get $n = e_0$, i.e. $K/\mathbb{F}_q(t)$ is totally ramified. By Corollary 4 of Chapter IV in [Se3], we know $G = P \rtimes C$ for some p-group P and some cyclic group C of order prime to p.

- If $m = 1$, i.e. $K/\mathbb{F}_q(t)$ is tamely ramified. Then $G = C$ is cyclic of order prime to p, and K is contained in the cyclotomic function field $\mathbb{F}_q(t)(\lambda_f)$. Since K is unramified over $\mathbb{F}_q(t)$ at ∞, we have K is actually inside $\mathbb{F}_q(t)(\lambda_f)^+$.

- If $m \geq 2$, i.e. $K/\mathbb{F}_q(t)$ is wildly ramified. The fixed field K^P of P will be contained in the cyclotomic function field $\mathbb{F}_q(t)(\lambda_f)^+$, since it is abelian over $\mathbb{F}_q(t)$, unramified at ∞ and only ramified at the finite place f. By the Riemann-Hurwitz formula, we have

  $$d \leq (1 + \frac{e_1}{e_0} + ... + \frac{e_{m-1}}{e_0} - \frac{m}{e_0})d = \frac{2n-2}{n} < 2.$$

  So $d = 1$.Thus K^P is just $\mathbb{F}_q(t)$, i.e. G is a p-group.

□

Case $(g = 1)$. We have $2e_0 = (e_0 + e_1 + ... + e_{m-1} - m)d$.

m	d	e_0	e_1
$m=1$	4	2	1
	3	3	1

Table 3.1: Ramification indexes of $K/\mathbb{F}_q(t)$ with $g(K)=1$ and $m=1$.

- If $m=1$, then either $d=4, e_0=2$ or $d=3, e_0=3$.
- If $m \geq 2$, we have $2=(1+\frac{e_1}{e_0}+...+\frac{e_{m-1}}{e_0}-\frac{m}{e_0})d \geq d$. If $d=2$, then $e_1+...+e_{m-1}=m$. But $e_i>1$ for $i<m$, which implies $m=e_1+...+e_{m-1} \geq 2(m-1)$. So $m=2$ and $e_1=2$. If $d=1$, then $e_0=e_1+...+e_{m-1}-m$.

m	d	e_0	e_1	e_2	...	e_m
$m \geq 2$	2	*	2	1	...	1
	1	$e_0=e_1+\cdots+e_{m-1}-m$				

Table 3.2: Ramification indexes of $K/\mathbb{F}_q(t)$ with $g(K)=1$ and $m \geq 2$.

Case ($g=2$). We have $2e_0=-2ne_0+(e_0+...+e_{m-1}-m)dn$, so $n|2e_0$. So as in the case $g=0$, we have $n=e_0$. So $K/\mathbb{F}_p(t)$ is totally ramified. Thus $G=P \rtimes C$ for some p-group P and some cyclic group C.

- If $m=1$, we have $2e_0=-2ne_0+(e_0-1)dn$. Since $K/\mathbb{F}_q(t)$ is totally ramified, we know $n=e_0$. So $2n+2=(n-1)d$. As a result we have either $d=3, n=5$, or $d=4, n=3$, or $d=6, n=2$. So K is a Galois extension over $\mathbb{F}_q(t)$ of prime degree, thus cyclic. So K is an abelian extension over $\mathbb{F}_q(t)$ contained in the cyclotomic function field $\mathbb{F}_q(t)(\lambda_f)^+$.

m	d	n	e_0	e_1
$m=1$	3	5	5	1
	4	3	3	1
	6	2	2	1

Table 3.3: Ramification indexes of $K/\mathbb{F}_q(t)$ with $g(K)=2$ and $m=1$.

- If $m \geq 2$, we have $d \leq (1+\frac{e_1}{e_0}+...+\frac{e_{m-1}}{e_0}-\frac{m}{e_0})d=\dfrac{2n+2}{n} \leq 3$. So $d=1,2,3$. If $d=3$, we have $m=2, n=e_0=e_1=2$ and $G \cong \mathbb{Z}/2$. If $d=2$, then either $m=3, e_1=e_2=2$ or $m=2, e_1=3$. If $d=1$, then G is a p-group.

Case ($g=1+2^s$ with $s \geq 0$).

	m	e_0	e_1	e_2	e_3
$d=3$	2	2	2	1	1
$d=2$	3	*	2	2	1
	2	*	3	1	1
$d=1$	G is a p-group				

Table 3.4: Ramification indexes of $K/\mathbb{F}_q(t)$ with $g(K)=2$ and $m \geq 2$.

PROPOSITION 3.3.2. *Let $K/\mathbb{F}_q(t)$ be a finite, separable, geometric extension with Galois group G, ramified only at one prime f and unramified at ∞. Assume the genus of K is $1+2^s$ for some integer $s \geq 0$. Then $K/\mathbb{F}_q(t)$ is totally ramified, thus G is a semi-direct product $P \rtimes C$ of a p-group P and a cylclic group C of order prime to p.*

Proof. Plugging in $g = 1+2^s$ into the Riemann-Hurwitz formula, we have

$$2^{s+1}e_0 = -2ne_0 + (e_0 + ... + e_{m-1} - m)dn,$$

so $n|2^{s+1}e_0$. We can write $n = 2^t e_0$, since $e_0|n$. Suppose $t \geq 1$, the inertia group I is normal in G, since every subgroup of index 2 is normal. In this case, the fixed field of I in $K/\mathbb{F}_q(t)$ is unramified over $\mathbb{F}_q(t)$ of degree 2. This is impossible. So $t = 0$ and $n = e_0$, and $K/\mathbb{F}_p(t)$ is totally ramified. By Corollary 4 of Chapter IV in [Se3], we know G is a semi-direct product $P \rtimes C$ of a p-group P and a cylclic group C of order prime to p. □

3.4 Iwasawa theory

Iwasawa theory is a Galois module theory of ideal class groups, initiated by K. Iwasawa, as part of the theory of cyclotomic number fields (see [Gr]), which gives a description of the p-part of the class number of the intermediate subextension of a $\mathbb{Z}/p$-extension.

Let F be a finite extension of $\mathbb{Q}$. Let p be a prime number. Suppose that F_∞ is a Galois extension of F with $\Gamma = \mathrm{Gal}\,(F_\infty/F) \cong \mathbb{Z}_p$. The nontrivial closed subgroups of Γ are of the form $\Gamma_n = p^n\Gamma$ for $n \geq 0$. Denote by F_n the fixed field of Γ_n in F_∞/F, then we obtain a tower of number fields

$$F = F_0 \subset F_1 \subset ... \subset F_n \subset ...$$

such that F_n/F is a cyclic extension of degree p^n. The main structure theorem of Iwasawa theory is as follows:

THEOREM 3.4.1 (Iwasawa, [Iw]). *For each n, let p^{e_n} be the p-part of the class number of the field F_n defined above. Then there exist integers λ, μ, ν such that $e_n = \lambda p^n + \mu n + \nu$ for all n.*

Unlike the case in number fields, where $\pi_1^p(U_p) \cong \mathbb{Z}_p$ by class field theory, in function fields it is a free pro-p-group with infinitely many generators. But if we restrict the ramification, that will give an upper bound for the generators depending on the conductor.

PROPOSITION 3.4.2. *Let $K/\mathbb{F}_p(t)$ be a finite geometric Galois extension whose Galois group G is a finite p-group. Suppose that K is ramified only at one prime f of degree d and conductor m. Then G is generated by $d(m-1-[\frac{m-1}{p}])$ elements.*

Proof. Let $\Phi(G)$ be the Frattini subgroup of the p-group G. The quotient group $G/\Phi(G)$ corresponds to an elementary abelian extension over $\mathbb{F}_p(t)$ ramified only at f, which is contained in the cyclotomic function field $\mathbb{F}_p(t)(\lambda_{f^m})$. The Galois group $\mathrm{Gal}\,(\mathbb{F}_p(t)(\lambda_{f^m})/\mathbb{F}_p(t))$ is generated by at most $d(m-1-[\frac{m-1}{p}])$ elements, where $[n]$ is the largest integer no more than n. By the Burnside basis theorem, G is also generated by at most $d(m-1-[\frac{m-1}{p}])$ elements. □

Remark. Define the ramification of $K/\mathbb{F}_p(t)$ at f to be of *depth* m, if the ith ramification group G_i vanishes for all $i \geq m$. Then the depth-m ramified part of π_1^p is the free pro-p group with $d(m-1-[\frac{m-1}{p}])$ generators.

Having the explicit description in Proposition 3.2.3 of cyclotomic function fields, we can construct an analog of Iwasawa theory for Carlitz fields more easily. Fix a positive integer m and consider any $\mathbb{Z}_p^m$ extension F_∞ over a function field F of characteristic p ramified only at one prime f. Pick a set of generators $\gamma_1, ..., \gamma_m$ of $G = \mathrm{Gal}\,(F_\infty/F) \cong \mathbb{Z}_p^m$. Let $\Gamma_i = \langle \gamma_1^{p^{[\frac{i+m-1}{m}]}}, ..., \gamma_m^{p^{[\frac{i}{m}]}} \rangle$ for all $i \geq 0$ and denote the fixed field of Γ_i by F_i.

$$\begin{array}{c} F_\infty \\ \Big| \Gamma_i \\ F_i \\ \Big| \Gamma/\Gamma_i \\ F \end{array}$$

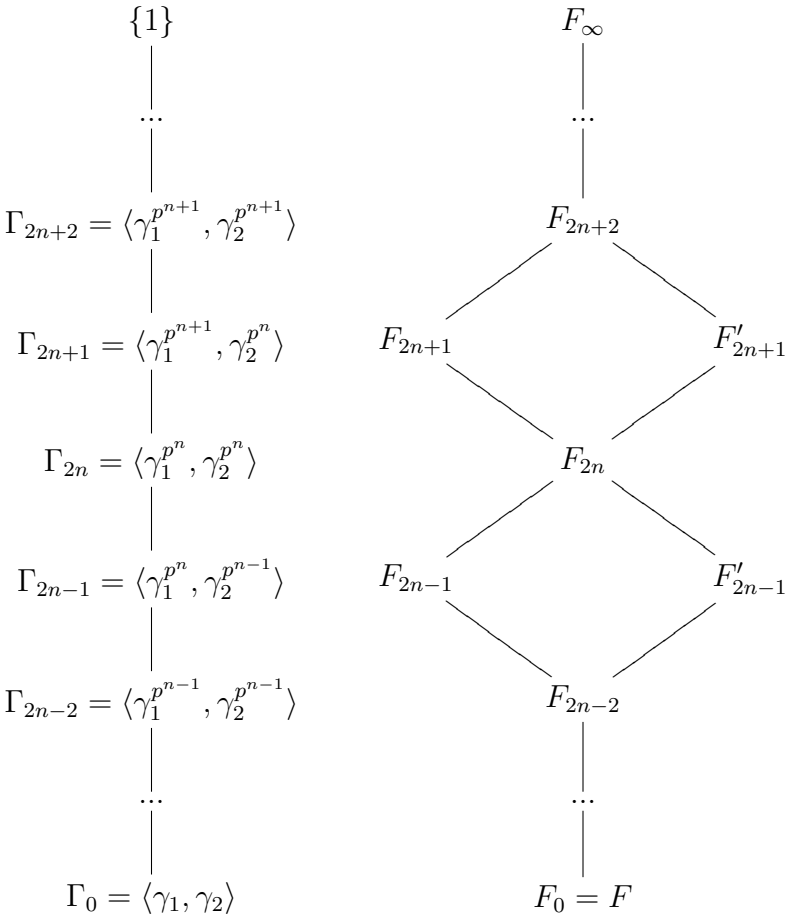
Let p^{e_n} be the highest power of p dividing the class number of F_n. In the case of $m = 1$, i.e. geometric cyclotomic $\mathbb{Z}_p$-extensions, R. Gold, H. Kisilevsky [GK] and A. Aiba [Ai] have some results about the Iwasawa modules and Iwasawa invariants. Much less is known if $m > 1$. When $m = 2$, the author believes it is possible to prove the following conjecture.

CONJECTURE 3.4.3. *Given F_∞/F ramified only at one prime f where it is totally ramified with $\mathrm{Gal}\,(F_\infty/F) \cong \mathbb{Z}_p^2$, consider its sub-extensions F_{2n+k} with $0 \leq k < 2$*

as above. Then there exist integers λ, μ_1, μ_2 and ν depending only on f such that $e_{2n+k} = \mu_1 p^{2n} + (\lambda n + \mu_2)p^n + \nu$ for all n.

In the remainder of this section, We give a partial proof of Conjecture 3.4.3.

We pick a set of generators of $\mathrm{Gal}\,(F_\infty/F) = \langle \gamma_1, \gamma_2 \rangle$. For all $n \geq 0$, as before we denote by F_{2n} the fixed field of $\Gamma_{2n} = \langle \gamma_1^{p^n}, \gamma_2^{p^n} \rangle$, F_{2n+1} the fixed field of $\Gamma_{2n+1} = \langle \gamma_1^{p^{n+1}}, \gamma_2^{p^n} \rangle$. Also we denote by F'_{2n+1} the fixed field of $\langle \gamma_1^{p^n}, \gamma_2^{p^{n+1}} \rangle$

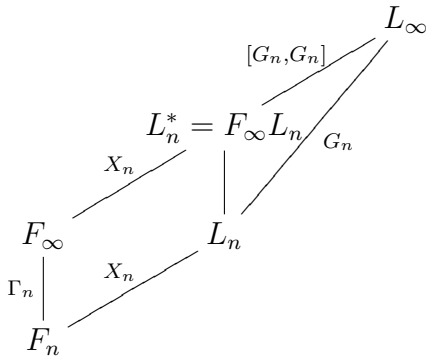


We consider the tower of function fields

$$F = F_0 \subset F_1 \subset ... \subset F_n \subset ....$$

Let L_n be the maximal abelian p-extension of F_n; so $[L_n, F_n]$ equals the p-class number p^{e_n} of F_n. Let $L_\infty = \bigcup_n L_n$, $G_n = \mathrm{Gal}\,(L_\infty/F_n)$ and $X = \mathrm{Gal}\,(L_\infty/F_\infty)$. Let L_n^* denote the maximal abelian extension of F_n contained in L_∞ and $X_n = \mathrm{Gal}\,(L_n^*/F_\infty)$. Then $L_n^* = L_n F_\infty \subset L_n^*$, since $L_n \subset L_n^*$ and $F_\infty \subset L_n^*$. On the other hand, by assumption there is only one prime ramified in L_n^*/F_n; L_n^* is totally ramified over L_n; but L_n^* is unramified over F_∞. So $L_n^* \subset L_n F_\infty$. Thus $L_n^* = L_n F_\infty$. We have $\mathrm{Gal}\,(L_n/F_n) \cong X_n$, since F_∞/F_n and L_n/F_n are linearly disjoint. Since L_n^*

is defined to be the maximal abelian extension of F_n inside L_∞, the Galois group $\mathrm{Gal}\,(L_\infty/L_n^*)$ is the commutator group $[G_n, G_n]$ of $G_n = \mathrm{Gal}\,(L_\infty/F_n)$.



To determine p^{e_n}, which is the order of $\mathrm{Gal}\,(L_n/F_n)$, we can consider the extension L_n^*/F_∞, which is a quotient of $X = \mathrm{Gal}\,(L_\infty/F_\infty)$ by the commutator subgroup of $G_n = \mathrm{Gal}\,(L_\infty/F_n)$,

$$\mathrm{Gal}\,(L_n/F_n) \cong X/[G_n, G_n].$$

We have the following exact sequence

$$0 \longrightarrow X \longrightarrow G_n \longrightarrow \Gamma_n \longrightarrow 0.$$

Being a projective limit of finite abelian p-groups, X is a compact $\mathbb{Z}_p$-module. For the commutator subgroup $[G_n, G_n]$, we claim

$$[G_n, G_n] = X^{\Gamma_n - 1} \equiv \{\gamma(x)x^{-1} \mid \gamma \in \Gamma_n, x \in X\},$$

Hence

$$\mathrm{Gal}\,(L_n/F_n) \cong X/X^{\Gamma_n - 1}.$$

Denoting the power series ring in two variables over $\mathbb{Z}_p$ by Λ, we know X is a finitely generated torsion Λ-module. By the structure theorem for torsion modules over discrete valuation rings, we have

$$X \cong \Lambda/P_i^{r_i}$$

as a pseudo-isomorphism with P_i's are height 1 primes of Λ. (Here, two modules are said to be *pseudo-isomorphic* if they have isomorphic localizations at each height 1 primes of Λ.) It seems possible to show $e_{2n+k} = \mu_1 p^{2n} + (\lambda n + \mu_2)p^n + \nu$ using a similar argument from the paper [CM] by Cuoco and Monsky.

Remark 3.4.4. Conjecture 3.4.3 coincides with the result in [CM] in the number field case.

Bibliography

[Ab] S. Abhyankar, *Coverings of algebraic curves*, Amer. J. Math. **79** (1957), 825-856.

[Ai] Akira Aiba, *On the vanishing of Iwasawa invariants of geometric cyclotomic $\mathbb{Z}_p$-extensions*, Acta Arithmetica **108** (2003), no. 2, 113-122.

[Br1] Sharon Brueggeman, *The nonexistence of certain Galois extensions unramified outside* 5, Journal of Number Theory **75** (1999), 47-52.

[Br2] Sharon Brueggeman, *Septic number fields which are ramified only at one small prime*, J. Symbolic Computation **31** (2001), 549-555.

[Ca1] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J., **1** (1935), 137-168.

[Ca2] L. Carlitz, *A class of polynomials*, Trans. Amer. Math. Soc., **43** (1938), 167-182.

[CDO] H. Cohen; Diaz y Diaz; M. Oliver, *Computing Ray Class Groups, Conductors and Discriminants*, Mathematics of Computation, **67** (1998).

[CM] Albert A. Cuoco; Paul Monsky, *Class numbers in $\mathbb{Z}_p^d$-extensions*, Mathematische Annalen, **255** (1981), 235-258.

[De] P. Deligne, *Formes modulaires et representations l-adiques*, Seminaire Bourbaki, expose **355** (1971), 139-172.

[Dr] V.G. Drinfeld (Russian), *Elliptic Modules*, Math. Sbornik **94** (1974), 594-627. English translation: Math. USSR, Sbornik **23** (1977), 159-170.

[GK] R. Gold; H. Kisilevsky, *On geometric $\mathbb{Z}_p$-extensions of function fields*, Manuscripta Math. **62** (1988), 145-161.

[GS] Li Guo; Linghsueh Shu, *Class number of cyclotomic function fields*, Transactions of the American Mathematical Society **351** (1999), no. 11, 4445-4467.

[Gr] Ralph Greenberg, *Iwasawa theory—past and present.* Class field theory—its centenary and prospect (Tokyo, 1998), 335-385, Adv. Stud. Pure Math., **30** Math. Soc. Japan, Tokyo, (2001)

[Gro] A. Grothendieck, *Revêtements étales et groupe fondamental*, SGA 1, Lecture Notes in Math., vol. **224**, Springer-Verlag, Berlin-Heidelberg-New York, (1971)

[Ha1] David Harbater, *Mock covers and Galois extensions*, J. Algebra, **91** (1984), No.2, 281-293.

[Ha2] David Harbater, *Abhyankar's conjecture on Galois groups over curves*, Invent. Math., **117** (1994), No.1, 1-25.

[Ha3] David Harbater, *Galois groups with prescribed ramification*, Contemporary Mathematics, **174** (1994), 35-60.

[Haj] Farshid Hajir, *On the class number of Hilbert Class Fields*, Pacific Journal of Mathematics, **181** (1997), no. 3, 177-187.

[Hay1] D.R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc., **189** (1974), 77-91.

[Hay2] D.R. Hayes, *Explicit class field theory in global function fields*, Studies in Algebra and Number Theory, (1979), 173-217.

[Iw] K. Iwasawa, *On* Γ*-extensions of algebraic number fields*, Bull. Amer. Math. Soc., **65** (1959), 183-226.

[Jo1] John Jones, *Tables of number fields with prescribed ramification*, available from `http://math.asu.edu/~jj/numberfields/`.

[Jo2] John Jones, *Number fields unramified away from* 2, available from `http://hobbes.la.asu.edu/papers/awayfrom2.pdf`.

[JY] Christian Jensen and Noriko Yui, *Polynomials with* D_p *as Galois group*, Journal of Number Theory, **15** (1982).

[Kh] Chandrashekhar Khare, *Serre's modularity conjecture: the level one case*, Duke Math. Journal, **134** (2006), no. 3, 557-589.

[Ma] Daniel J. Madden, *Arithmetic in Generalized Artin-Schreier Extensions of* $k(x)$, Journal of Number Theory, **10** (1978), 303-323

[Ne] Jürgen Neukirch, *Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg New York, **67** (1999).

[Od] A.M. Odlyzko, *On conductor and discriminants*, Algebraic Number Fields, (1994), 377-407.

[PARI2] The PARI-Group, *PARI/GP,Version 2.3.1*, Bordeaux, 2006, available from `http://pari.math.u-bordeaux.fr/`.

[Ra] M. Raynaud, *Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d' Abhyankar*, Invertiones Math., **116** (1994), 425-462.

[Ri] Paulo Ribenboim, *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, NY, 2001.

[Ros] Michael Rosen, *Number theory in function fields*, Graduate texts in mathematics, **210**, Springer-Verlag New York, (2002).

[Rot] Joseph J. Rotman, *Theory of groups*, Reprint of the 1984 original, Wm. C. Brown Publisher, (1988).

[Se1] Jean-Pierre Serre, *Œuvres*, Volume III, Springer-Verlag, Berlin, Heidelberg, and New York, (1986).

[Se2] Jean-Pierre Serre, *Sur les representations de degre* 2 *de* $\mathrm{Gal}\left(\bar{\mathbb{Q}}/\mathbb{Q}\right)$, Duke Mathematical Journal, **54** (1987), no.1, 179-230.

[Se3] Jean-Pierre Serre, *Local Fields*, Graduate Texts in Mathematics, Springer-Verlag, (1979).

[Sh] Stephen S. Shatz, *Profinite groups, arithmetic, and geometry*, Annals of Mathematics Studies (67), Princeton University Press, (1972).

[Ta] John Tate, *The non-existence of certain Galois extension of* $\mathbb{Q}$ *unramified outside* 2, Contemporary Mathematics, Volume **174** (1994), 153-156.

[Th] Dinesh S. Thakur, *Function field arithmetic*, World Scientific Publishing Co. Pte. Ltd., (2004).

[TM] Hyunsuk Moon and Yuichiro Taguchi, *Refinement of Tate's discrimiant Bound and non-existence theorem for mod p Galois representations*, Documenta Mathematica, Extra volume Kato, (2003), 641-654.

[Wa] Lawrence C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, Springer-Verlag, (1996).

[We] A. Weil, *Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques*, Revue Scient., **77**, (1939), 104-106; reprinted in Oeuvres Scient., Springer-Verlag, **1**, (1980), 236-240.