ABSTRACT

Title of Dissertation: CLASS GROUPS OF CHARACTERISTIC-p FUNCTION FIELD ANALOGUES OF $\mathbb{Q}(n^{1/p})$

Steven Reich
Doctor of Philosophy, 2021

Dissertation Directed by: Professor Lawrence Washington
Department of Mathematics

In the theory of cyclotomic function fields, the Carlitz module Λ_M associated to a polynomial M in a global function field of characteristic p provides a strong analogy to the roots of unity μ_p in a number field. In this work, we consider a natural extension of this theory to give a compatible analogue of the p-th root of an integer n.

The most fundamental case, and the one which most closely mimics the number field situation, is when the Carlitz module is defined by a linear polynomial (which can be assumed to be T) in $k = \mathbb{F}_q(T)$. The Carlitz module Λ_T generates a degree-$(q-1)$ extension $k(\Lambda_T)$ which shares many properties with the field $\mathbb{Q}(\mu_p)$, where μ_p is the module of p-th roots of unity.

To form the analogue of $\mathbb{Q}(\sqrt[p]{n})$, we define a degree-q extension F/k associated to a polynomial $P(T) \in k$, for which the normal closure is formed by adjoining Λ_T. In the introduction, we describe in detail the parallels between this construction and

that in the number field setting. We then compute the class number h_F for a large number of such fields. The remainder of the work is concerned with proving results about the class groups and class numbers of this family of fields. These are:

- a formula relating the class number of F to that of its normal closure, along with a theorem about the structure of the class group of the normal closure
- a formula relating the class number of a compositum of such F to the class numbers of the constituent fields
- conditions on $P(T)$ for when the characteristic, p, of F divides its class number, along with bounds on the rank of the p-part of the class group.

CLASS GROUPS OF CHARACTERISTIC-p FUNCTION FIELD ANALOGUES OF $\mathbb{Q}(n^{1/p})$

by

Steven Reich

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2021

Advisory Committee:
Professor Lawrence Washington, Chair/Advisor
Professor Patrick Brosnan
Professor Niranjan Ramachandran
Professor James Schafer
Professor William Gasarch

Dedication

This work is dedicated to my family: my parents Robert and Elizabeth, and my brother Daniel. This would not have been possible without your love and support.

"Behold, I am doing a new thing;
now it springs forth, do you not perceive it?
I will make a way in the wilderness
and rivers in the desert." — Isaiah 43:19

Acknowledgments

I would first like to thank my advisor, Professor Lawrence Washington, for his encouragement and insight throughout my graduate career. His zeal for mathematics, and more importantly his care for the people around him, continue to be an inspiration to me.

I would also like to recognize all members of the Mathematics Department: the faculty, staff, and students, who have all contributed to making this experience a worthwhile one. I am especially thankful to my friends and peers who helped to make these years enjoyable.

I am grateful as well to the Human Language Technology Center of Excellence at Johns Hopkins University, which provided funding for three semesters of my graduate studies. In particular, I thank Dr. Nicholas Andrews, who has consistently advocated in my support.

There are many other people responsible for shaping my identity as a mathematician and as a person, including teachers who nurtured my curiosity, and friends who have enriched my life. I regret that I cannot thank each of them individually, and surely I am indebted to some in ways that I am not even aware. However, I would be remiss to not recognize my dear friend Dr. Patrick Devlin, who has been inspiring my interest in mathematics since we were kids.

Most of all, I want thank my wonderful family, and praise God.

Table of Contents

Chapter 1: Introduction and background

1.1 Carlitz modules and 'cyclotomic' function fields

We begin by describing the basic theory of cyclotomic function fields. We generally follow the constructions given by Goss [7] (cf. also [27]).

Let $k = \mathbb{F}_q(T)$, with q a power of a prime p, and k^{sep} a separable closure. The Frobenius map $F : k^{sep} \to k^{sep}$ defined by $F(x) = x^q$ is additive, as are its powers F^i under composition (including the identity map F^0). Multiplication by an element of $\mathcal{O}_k = \mathbb{F}_q[T]$ also represents an additive endomorphism of k^{sep}. We may thus define an injective homomorphism $C : \mathcal{O}_k \to End(k^{sep})$, where $C(T) = F + TF^0$, $C(\omega) = \omega F^0$ for $\omega \in \mathbb{F}_q$, and $C(M)$ for arbitrary $M \in \mathcal{O}_k$ is determined by extending linearly from these relations. As a nontrivial example,

$$C(T^2+1) = C(T)^2+C(1) = (F+TF^0)\circ(F+TF^0)+F^0 = F^2+(T^q+T)F+(T^2+1)F^0.$$

Using this construction, we can associate to a polynomial M the *Carlitz module* $\Lambda_M = \{\lambda \in k^{sep} \,|\, C(M)(\lambda) = 0\}$ (first introduced by Carlitz in [4]). This is isomorphic as an $\mathcal{O}_k$-module to $\mathcal{O}_k/(M)$, which has cardinality $q^{deg(M)}$, and generates an abelian extension $k(\Lambda_M)/k$ with Galois group isomorphic to $(\mathcal{O}_k/M)^\times$.

We will focus on the case $M = T$, for which the analogy with the number field setting is most clear. The Carlitz module Λ_T is generated as an $\mathbb{F}_q$-module by a fixed nonzero root λ of $C(T)(x) = x^q + Tx$. The extension $k(\lambda)/k$ has Galois group isomorphic to $\mathcal{O}_k[T]/(T) \cong \mathbb{F}_q^\times$, and the integral closure of $\mathcal{O}_k$ in $k(\lambda)$ is $\mathcal{O}_k[\lambda]$. Additionally, this extension is unramified outside of T and $1/T$ (which we consider as the infinite prime of k), and these primes are totally ramified. In particular, $(T) = (\lambda)^{q-1}$ and $(1/T) = (1/\lambda)^{q-1}$.

This should be reminiscent of the p-th roots of unity generated by a primitive root ζ_p, with the multiplicative structure μ_p replaced by the additive structure Λ_T. The extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ has Galois group $(\mathbb{Z}/p\mathbb{Z})^\times$ and its ring of integers is $\mathbb{Z}[\zeta_p]$. The only finite prime that ramifies is p, and its ramification is total.

The parallel between the behavior of the respective infinite primes is slightly more nuanced. The maximal real subfield $\mathbb{Q}(\zeta_p)^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is the fixed field of the image of $\mathbb{Z}^\times = \{\pm 1\}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. The infinite prime of $\mathbb{Q}$ splits completely in $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$, and the primes above it ramify in $\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p)^+$. In the function field setting, the maximal 'real' subfield $k(\lambda)^+$ is the fixed field of $\mathcal{O}_k^\times \cong \mathbb{F}_q^\times$, which in this case is the full Galois group (i.e., $k(\lambda)^+ = k$), and $1/T$ is totally ramified in $k(\lambda)/k$. (We note that in the more general case that M is a power of a monic irreducible polynomial, $k(\Lambda_M)^+$ is a non-trivial extension of k in which $1/T$ splits completely.)

Hayes [11] gives an even deeper connection between Carlitz modules and roots of unity: an analogue of the Kronecker-Weber theorem. He shows that any finite abelian extension of k in which $1/T$ is not wildly ramified is contained in a constant field extension of $k(\Lambda_M)$ for some $M \in \mathcal{O}_k$.

1.2 The analogue of $\mathbb{Q}(\sqrt[p]{n})$

We now describe the construction of a function field which parallels that of $\mathbb{Q}(\sqrt[p]{n})$, continuing the analogy (and notation) of the previous section. Much of the following can be done for a general Carlitz module Λ_M, but for concreteness we continue to focus on Λ_T, since this is the situation we consider in later sections.

Let $P(T) \in \mathcal{O}_k$ be such that $P(T) \neq Q(T)^q + TQ(T)$ for any $Q(T) \in \mathcal{O}_k$, and fix a root $\gamma \in k^{sep}$ of $C(T)(x) - P(T) = x^q + Tx - P(T)$. We will show in Proposition 1.1 below that this is irreducible. By the linearity of $C(T)$, the full set of roots in k^{sep} is $\{\gamma + \omega\lambda \,|\, \omega \in \mathbb{F}_q\}$. Thus the extension $k(\gamma)/k$ is of degree q, and its normal closure is formed by adjoining λ. The Galois group $Gal(k(\lambda, \gamma)/k)$ has normal subgroup $G = Gal(k(\lambda, \gamma)/k(\gamma)) \cong \mathbb{F}_q^+$, which permutes the roots $\gamma + \omega\lambda$, and the subgroup $\Delta = Gal(k(\lambda, \gamma)/k(\gamma)) \cong Gal(k(\lambda)/k) \cong \mathbb{F}_q^\times$, which acts on G via a cyclotomic character. This closely mirrors the number field situation, in which $\mathbb{Q}(\zeta_p, \sqrt[p]{n})$ is the normal closure of $\mathbb{Q}(\sqrt[p]{n})$, and the Galois subgroup structure is essentially the same.

By a change of variables, the polynomial defining $k(\lambda, \gamma)/k(\lambda)$ can be put in the form $x^q - x - \frac{P(-\lambda^{q-1})}{\lambda^q}$, whereby this is an Artin-Schreier extension (but note that the extension $k(\gamma)/k$ is not[1], as Artin-Schreier extensions are necessarily Galois). Hasse [10] considered general Artin-Schreier extensions as an analogue of adjoining p-th roots of n, but we argue that our construction gives a more precise analogy because of the relationship it enjoys with the cyclotomic theory.

[1]Except when $q = 2$, where the Carlitz module generates a trivial extension of k, in analogy with the square roots of unity which of course lie in $\mathbb{Q}$.

Proposition 1.1. *Suppose $P(T) \in \mathcal{O}_k$ is not of the form $Q(T)^q + TQ(T)$ for any $Q(T) \in \mathcal{O}_k$. Then $x^q + Tx - P(T)$ is irreducible over k.*

Proof. Clearly this is true for $q = 2$, so we assume $q > 2$. The condition shows that $x^q + Tx - P(T)$ does not have a root in k. Now, if $\gamma \in k^{sep}$ is a fixed root, the set of all roots in k^{sep} is $\{\gamma + \omega\lambda \,|\, \omega \in \mathbb{F}_q\}$, where λ is a nonzero root of $x^q + Tx$ (i.e., a generator of the Carlitz module Λ_T). If one of the roots γ is in $K = k(\lambda)$, we would have $F = k(\gamma)$ is Galois over k (since K/k is abelian). But this would mean F contains another root $\gamma + \omega\lambda$, and thus that $F = K$. Since $[K : k] = q - 1$, this would mean $x^q + Tx - P(T)$ has an irreducible factor of degree $q - 1$, and thus a linear factor, contradicting the above.

Now, let $L = k(\lambda, \gamma)$, the splitting field of $x^q + Tx - P(T)$. Since $Gal(L/k)$ has $Gal(K/k) \cong \mathbb{F}_q^\times$ as a quotient, we can obtain an element $\sigma \in Gal(L/k)$ of order $q - 1$ by lifting a generator of $Gal(K/k)$ and (if necessary) raising it to a suitable power. We observe that σ cannot fix all the roots of $x^q + Tx - P(T)$ (in fact, it cannot fix more than one, otherwise it would fix all of L, since both γ and λ can be obtained as $\mathbb{F}_q$-linear combinations of any two distinct roots). Without loss of generality, suppose γ is not fixed by σ, i.e. that $\sigma(\gamma) = \gamma + \omega\lambda$ for some $\omega \in \mathbb{F}_q^\times$. Then $\sigma^i(\gamma) = \gamma + \omega(1 + \sigma + \cdots + \sigma^{i-1})(\lambda)$. If σ^i fixes γ, then we must have $(1 - \sigma^i)(\lambda) = (1 - \sigma)(1 + \sigma + \cdots + \sigma^{i-1})(\lambda) = (1 - \sigma)(0)$, and thus σ^i fixes λ as well. But then σ^i fixes L, so i must be a multiple of $q - 1$. This says that the orbit of γ under $\langle\sigma\rangle$ has order $q - 1$. Thus the degree of the minimal polynomial for γ must be at least $q - 1$, and divides $x^q + Tx - P(T)$ which cannot have a linear factor.

Therefore $x^q + Tx - P(T)$ is the minimal polynomial, and so it is irreducible. $\square$

This proposition contrasts with what one might expect from the number field situation, where requiring that $x^q - n$ does not have a root in $\mathbb{Q}$ does not guarantee irreducibility. This (as well as the simpler fact that $[k(\Lambda_T) : k] = q - 1$ rather than $\phi(q)$) illustrates an interesting subtlety: even when q is not prime, our situation more closely resembles that of the p-th roots of unity (and n) than that of q-th roots. In fact, the correct analogue of the latter is the Carlitz module Λ_{T^r} of a power of T (or some other irreducible polynomial), but this goes beyond the scope necessary for our purposes.

We summarize the correspondence between the number field and function field settings in the following table.

Table 1.1: Dictionary of relevant concepts for number fields and function fields.

Number fields	Function fields
$\mu_p = \{\zeta_p^i\}$, roots of $x^p - 1$	$\Lambda_T = \{\omega\lambda \mid \omega \in \mathbb{F}_q\}$, roots of $x^q + Tx$
$Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$	$Gal(k(\lambda)/k) \cong \mathbb{F}_q^\times$
$\mathbb{Z}[\zeta_p]$, the ring of integers in $\mathbb{Q}(\zeta_p)$	$\mathcal{O}_k[\lambda]$, the integral closure of $\mathcal{O}_k$ in $k(\lambda)$
p totally ramified in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$	T totally ramified in $k(\lambda)/k$
Infinite prime splits in $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$, totally ramified in $\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p)^+$	$1/T$ splits in $k(\lambda)^+/k$, totally ramified in $k(\lambda)/k(\lambda)^+$
Kronecker-Weber theorem	Hayes' explicit class field theory
$\sqrt[p]{n}$, a root of $x^p - n$ where n is not a p-th power	γ, a root of $x^q + Tx - P(T)$ where $P(T) \neq Q(T)^q + TQ(T)$
$\mathbb{Q}(\zeta_p, \sqrt[p]{n})$, the normal closure of $\mathbb{Q}(\sqrt[p]{n})$, has Galois group $\cong \mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$	$k(\lambda, \gamma)$, the normal closure of $k(\gamma)$, has Galois group $\cong \mathbb{F}_q^+ \rtimes \mathbb{F}_q^\times$
$Gal(\mathbb{Q}(\zeta_p, \sqrt[p]{n})/\mathbb{Q}(\zeta_p)) \cong \mathbb{Z}/p\mathbb{Z}$ permutes the roots $\zeta_p^i \sqrt[p]{n}$	$Gal(k(\lambda, \gamma)/k(\lambda)) \cong \mathbb{F}_q^+$ permutes the roots $\gamma + \omega\lambda$

1.3 Results to be presented

In this work, we are primarily concerned with the *degree-0 divisor class group* of fields in the family we have described above. We take the divisor group D_F of a function field F to mean the free abelian group indexed by its (finite and infinite) primes, and the degree-0 divisor group D_F^0 to be the subgroup of such elements with total degree 0. Then the class group Cl_F^0 is the quotient of D_F^0 by the principal divisors P_F. The class number is its cardinality h_F.

As in previous sections, let F be the field generated over $\mathbb{F}_q(T)$ by a root γ of $x^q + Tx - P(T)$, and let $L = F(\lambda)$ denote its normal closure. We briefly summarize the results that will be presented in subsequent chapters.

- Chapter 2: we compute the class number of many F with $q = p$ a small prime and $P(T)$ of low degree.
- Chapter 3: we show that $h_L = h_F^{q-1}$, and when $q = p$ is prime, that Cl_L^0 is a $(p-1)$-st power of a group.
- Chapter 4: we consider composita $K = F_1 F_2 \dots F_n$ of such fields, showing that $h_K = \prod h_{F_i}$.
- Chapter 5: we give complete conditions on $P(T)$ that determine when h_F is divisible by the characteristic p. For the case $q = p = 2$, we show that the 2-class group is always cyclic and give additional conditions for 4- and 8-divisibility of the class number.

Chapter 2: Explicit computation of class numbers

The theoretical results presented in subsequent chapters were motivated by direct computations of the class numbers of members of the family of fields. In this chapter, we describe the approach by which these calculations were made and provide tables of the class numbers of over 100 distinct fields.

We employ standard theory about zeta functions of curves and their function fields (see e.g. [9, 22, 24, 26]) to compute the class number of a field F. First, the zeta function[1] of $F/\mathbb{F}_q(T)$ of genus g can be expressed as

$$Z(F,t) = \frac{G(t)}{(1-t)(1-qt)},$$

where $G(t)$ a polynomial with the following properties:

- $deg(G(t)) = 2g$
- $G\left(\frac{1}{qt}\right) = q^g t^{2g} G(t)$
- If z is a root of $G(t)$, then $|z| = \frac{1}{\sqrt{q}}$
- $G(1) = h_F$.

[1]The zeta function is actually $\zeta_F(s) = Z(F, q^{-s})$, but we refer to $Z(F,t)$ as a zeta function for brevity.

In order to find $G(t)$, we express the zeta function in terms of rational points on a curve that determines F:

$$Z(F,t) = \exp\left(\sum_{i=1}^{\infty} \#\tilde{C}(\mathbb{F}_{q^i})\frac{t^i}{i}\right) = \exp\left(\sum_{i=1}^{\infty} \#C(\mathbb{F}_{q^i})\frac{t^i}{i}\right)\prod_x \frac{1-t^{d_x}}{1-t^{e_x}},$$

where $\tilde{C}$ is a non-singular model of a curve C with function field F. Each term of the rightmost product is a ratio of Euler factors corresponding to a singular point x, and $d_x|e_x$. Thus we arrive at the expression

$$G(t) = \exp\left(\sum_{i=1}^{\infty} \#C(\mathbb{F}_{q^i})\frac{t^i}{i}\right)\frac{(1-t)(1-qt)}{f(t)},$$

where $f(t)$ is a polynomial (possibly equal to 1) all of whose roots are roots of unity. We outline the computational algorithm as applied to $x^q + Tx - P(T)$ below.

Algorithm 1: Computation of class number

Input: $q = p^r$, p prime
$P(T) \in \mathbb{F}_q[T]$

Set $f(x,T) = x^q + Tx - P(T)$
Set $K = (q-1)deg(P(T)) \approx 2g$
for $k = 1, \ldots, K$ **do**
    $n_k = 1$ (accounting for the point at infinity)
    for $\omega \in \mathbb{F}_{q^k}$ **do**
        $n_k \leftarrow n_k + deg(\gcd(x^{q^k} - x, f(x,\omega)))$
$G(t) = \exp\left(\sum_{k=1}^{K} \frac{n_k}{k}t^k\right)(1-t)(1-qt) \mod t^{K+1}$
if $\exists z$ *such that* $G(z) = 0$ *and* $|z| \notin \{1, \frac{1}{\sqrt{q}}\}$ **then**
    Increase K
    go to 3
while $\exists z$ *such that* $G(z) = 0, |z| = 1$ **do**
    $G(t) \leftarrow G(t)/(t-z)$
return $G(t)$ and $h = G(1)$

The results of these computations are given in the following tables. We omit cases of low degree ($deg(P(T)) < 3$ for $q = 2$, and < 2 otherwise) since these are genus 0. We also note that by a change of variables, fields of this kind can always be generated by a $P(T)$ with no terms of degree divisible by q, except for $q = 2$ when there may be a quadratic term, and hence we only list $P(T)$ with this property.

Table 2.1: Class numbers of extensions $F/\mathbb{F}_2(T)$ determined by various $P(T)$.

$P(T)$	$G_F(t)$	h_F
T^3	1	1
$T^3 + T$	$1 + t + 2t^2$	4
$T^3 + T^2$	1	1
$T^3 + T^2 + T$	$1 - t + 2t^2$	2
T^5	$1 + 2t^2$	3
$T^5 + T$	$1 + t + 2t^3 + 4t^4$	8
$T^5 + T^2$	$1 + 2t^2$	3
$T^5 + T^2 + T$	$1 - t - 2t^3 + 4t^4$	2
$T^5 + T^3$	$1 + 2t + 2t^2$	5
$T^5 + T^3 + T$	$1 - t + 2t^2 - 2t^3 + 4t^4$	4
$T^5 + T^3 + T^2$	$1 - 2t + 2t^2$	1
$T^5 + T^3 + T^2 + T$	$1 + t + 2t^2 + 2t^3 + 4t^4$	10
T^7	$1 + 4t^4$	5
$T^7 + T$	$1 + t + 2t^2 + 4t^3 + 4t^4 + 4t^5 + 8t^6$	24
$T^7 + T^2$	$1 + 4t^4$	5
$T^7 + T^2 + T$	$1 - t + 2t^2 - 4t^3 + 4t^4 - 4t^5 + 8t^6$	6
$T^7 + T^3$	$1 + 2t + 4t^2 + 4t^3 + 4t^4$	15
$T^7 + T^3 + T$	$1 - t - 4t^5 + 8t^6$	4
$T^7 + T^3 + T^2$	$1 - 2t + 4t^2 - 4t^3 + 4t^4$	3
$T^7 + T^3 + T^2 + T$	$1 + t + 4t^5 + 8t^6$	14
$T^7 + T^5$	$1 + 2t + 2t^2 + 4t^3 + 4t^4$	13
$T^7 + T^5 + T$	$1 - t + 2t^2 - 2t^3 + 4t^4 - 4t^5 + 8t^6$	8
$T^7 + T^5 + T^2$	$1 - 2t + 2t^2 - 4t^3 + 4t^4$	1
$T^7 + T^5 + T^2 + T$	$1 + t + 2t^2 + 2t^3 + 4t^4 + 4t^5 + 8t^6$	22
$T^7 + T^5 + T^3$	$1 + 2t^2 + 4t^4$	7
$T^7 + T^5 + T^3 + T$	$1 + t - 2t^3 + 4t^5 + 8t^6$	12
$T^7 + T^5 + T^3 + T^2$	$1 + 2t^2 + 4t^4$	7
$T^7 + T^5 + T^3 + T^2 + T$	$1 - t + 2t^3 - 4t^5 + 8t^6$	6

Table 2.2: Class numbers of extensions $F/\mathbb{F}_2(T)$ determined by various $P(T)$ (cont.)

$P(T)$	$G_F(t)$	h_F
T^9	$1 - 2t^3 + 8t^6$	7
$T^9 + T$	$1 + t + 2t^2 + 2t^3 + \ldots$ [2]	48
$T^9 + T^2$	$1 + 2t^3 + 8t^6$	11
$T^9 + T^2 + T$	$1 - t + 2t^2 - 2t^3 + 6t^4 - \ldots$	18
$T^9 + T^3$	$1 + 2t + 4t^2 + 6t^3 + 8t^4 + 8t^5 + 8t^6$	37
$T^9 + T^3 + T$	$1 - t + 2t^302t^4 + 4t^5 - 8t^7 + 16t^8$	12
$T^9 + T^3 + T^2$	$1 - 2t + 4t^2 - 6t^3 + 8t^4 - 8t^5 + 8t^6$	5
$T^9 + T^3 + T^2 + T$	$1 + t - 2t^3 - 2t^4 - 4t^5 + 8t^7 + 16t^8$	18
$T^9 + T^5$	$1 + 2t + 2t^2 + 2t^3 + 4t^4 + 8t^5 + 8t^6$	27
$T^9 + T^5 + T$	$1 - t + 2t^2 - 4t^3 + 2t^4 - \ldots$	8
$T^9 + T^5 + T^2$	$1 - 2t + 2t^2 - 2t^3 + 4t^4 - 8t^5 + 8t^6$	3
$T^9 + T^5 + T^2 + T$	$1 + t + 2t^2 + 4t^3 + 2t^4 + \ldots$	50
$T^9 + T^5 + T^3$	$1 + 2t^2 + 2t^3 + 4t^4 + 8t^6$	17
$T^9 + T^5 + T^3 + T$	$1 + t + 2t^4 + 8t^7 + 16t^8$	28
$T^9 + T^5 + T^3 + T^2$	$1 + 2t^2 - 2t^3 + 4t^4 + 8t^6$	13
$T^9 + T^5 + T^3 + T^2 + T$	$1 - t + 2t^4 - 8t^7 + 16t^8$	10
$T^9 + T^7$	$1 + 2t + 4t^2 + 6t^3 + 8t^4 + 8t^5 + 8t^6$	37
$T^9 + T^7 + T$	$1 - t - 2t^3 + 6t^4 - 4t^5 - 8t^7 + 16t^8$	8
$T^9 + T^7 + T^2$	$1 - 2t + 4t^2 - 6t^3 + 8t^4 - 8t^5 + 8t^6$	5
$T^9 + T^7 + T^2 + T$	$1 + t + 2t^3 + 6t^4 + 4t^5 + 8t^7 + 16t^8$	38
$T^9 + T^7 + T^3$	$1 + 2t^3 + 8t^6$	11
$T^9 + T^7 + T^3 + T$	$1 + t + 2t^2 + 2t^3 + 2t^4 + \ldots$	44
$T^9 + T^7 + T^3 + T^2$	$1 - 2t^3 + 8t^6$	7
$T^9 + T^7 + T^3 + T^2 + T$	$1 - t + 2t^2 - 2t^3 + 2t^4 - \ldots$	14
$T^9 + T^7 + T^5$	$1 + 2t^2 - 2t^3 + 4t^4 + 8t^6$	13
$T^9 + T^7 + T^5 + T$	$1 + t - 2t^4 + 8t^7 + 16t^8$	24
$T^9 + T^7 + T^5 + T^2$	$1 + 2t^2 + 2t^3 + 4t^4 + 8t^6$	17
$T^9 + T^7 + T^5 + T^2 + T$	$1 - t - 2t^4 - 8t^7 + 16t^8$	6
$T^9 + T^7 + T^5 + T^3$	$1 + 2t + 2t^2 + 2t^3 + 4t^4 + 8t^5 + 8t^6$	27
$T^9 + T^7 + T^5 + T^3 + T$	$1 - t + 2t^2 + 2t^4 + 8t^6 - 8t^7 + 16t^8$	20
$T^9 + T^7 + T^5 + T^3 + T^2$	$1 - 2t + 2t^2 - 2t^3 + 4t^4 - 8t^5 + 8t^6$	3
$T^9 + T^7 + T^5 + T^3 + T^2 + T$	$1 + t + 2t^2 + 2t^4 + 8t^6 + 8t^7 + 16t^8$	38

[2] We truncate the polynomial for space in some cases, but note that the remaining terms can be recovered using the functional equation for $G(t)$.

Table 2.3: Class numbers of extensions $F/\mathbb{F}_3(T)$ determined by various $P(T)$.

$P(T)$	$G_F(t)$	h_F
T^2	1	1
T^2+T	$1+2t+3t^2$	6
T^2+2T	$1-t+3t^2$	3
T^4	$1+9t^4$	10
T^4+T	$1+2t+6t^2+9t^3+18t^4+18t^5+27t^6$	81
T^4+2T	$1-t-9t^5+27t^6$	18
T^4+T^2	$1+3t^2+9t^4$	13
T^4+T^2+T	$1-t+6t^3-9t^5+27t^6$	24
T^4+T^2+2T	$1+2t+3t^2+6t^3+9t^4+18t^5+27t^6$	66
T^4+2T^2	$1+3t+6t^2+9t^3+9t^4$	28
T^4+2T^2+T	$1-t+3t^3-9t^4+27t^6$	21
T^4+2T^2+2T	$1-t+3t^2-6t^3+9t^4-9t^5+27t^6$	24
T^5	$1+27t^6$	28
T^5+T	$1-t-27t^7+81t^8$	54
T^5+2T	$1+2t+6t^2+9t^3+18t^4+\ldots$	252
T^5+T^2	$1+3t+6t^2+9t^3+18t^4+27t^5+27t^6$	91
T^5+T^2+T	$1-t+3t^2+3t^3+9t^5+27t^6-27t^7+81t^8$	96
T^5+T^2+2T	$1-t+3t^3-9t^4+9t^5-27t^7+81t^8$	57
T^5+2T^2	$1+3t^2+9t^4+27t^6$	40
T^5+2T^2+T	$1+2t+3t^2+6t^3+18t^4+\ldots$	210
T^5+2T^2+2T	$1-t-3t^3+9t^4-9t^5-27t^7+81t^8$	51
T^5+T^4	$1+3t+9t^2+15t^3+27t^4+27t^5+27t^6$	109
T^5+T^4+T	$1-t-3t^3+12t^4-9t^5-27t^7+81t^8$	54
T^5+T^4+2T	$1-t+6t^3-6t^4+18t^5-27t^7+81t^8$	72
$T^5+T^4+T^2$	$1-3t^3+27t^6$	25
$T^5+T^4+T^2+T$	$1+2t+3t^2+6t^3+12t^4+\ldots$	204
$T^5+T^4+T^2+2T$	$1-t+3t^2-3t^3+3t^4-\ldots$	75
$T^5+T^4+2T^2$	$1+6t^3+27t^6$	34
$T^5+T^4+2T^2+T$	$1-t+3t^2-3t^3+12t^4-\ldots$	84
$T^5+T^4+2T^2+2T$	$1+2t+3t^2+6t^3+12t^4+\ldots$	204
T^5+2T^4	$1+3t^3+27t^6$	31
T^5+2T^4+T	$1+2t+6t^2+12t^3+24t^4+\ldots$	270
T^5+2T^4+2T	$1-t+3t^3-3t^4+9t^5-27t^7+81t^8$	63
$T^5+2T^4+T^2$	$1+3t^2+3t^3+9t^4+27t^6$	43
$T^5+2T^4+T^2+T$	$1-t+6t^4-27t^7+81t^8$	60
$T^5+2T^4+T^2+2T$	$1+2t+3t^2-3t^4+27t^6+54t^7+81t^8$	165
$T^5+2T^4+2T^2$	$1+3t+6t^2+12t^3+18t^4+27t^5+27t^6$	94
$T^5+2T^4+2T^2+T$	$1-t-3t^3+6t^4-9t^5-27t^7+81t^8$	48
$T^5+2T^4+2T^2+2T$	$1-t+3t^2-3t^3+15t^4-\ldots$	87

Table 2.4: Class numbers of extensions $F/\mathbb{F}_5(T)$ determined by various $P(T)$.

$P(T)$	$G_F(t)$	h_F
T^2	$1+5t^2$	6
T^2+T	$1+4t+10t^2+20t^3+25t^4$	60
T^2+2T	$1-t-5t^3+25t^4$	20
T^2+3T	$1-t+5t^2-5t^3+25t^4$	25
T^2+4T	$1-t-5t^3+25t^4$	20
T^3	$1+125t^6$	126
T^3+T	$1-t+5t^2+10t^3+50t^5+125t^6-125t^7+625t^8$	690
T^3+2T	$1-t-5t^3+25t^4-25t^5-125t^7+625t^8$	495
T^3+3T	$1-t+5t^3-25t^4+25t^5-125t^7+625t^8$	505
T^3+4T	$1+4t+15t^2+40t^3+100t^4+\ldots$	1860
T^3+T^2	$1+5t+15t^2+35t^3+75t^4+125t^5+125t^6$	381
T^3+T^2+T	$1-t+5t^2-5t^3+40t^4-\ldots$	640
T^3+T^2+2T	$1-t+5t^2-5t^3+15t^4-\ldots$	615
T^3+T^2+3T	$1-t-5t^3+15t^4-25t^5-125t^7+625t^8$	485
T^3+T^2+4T	$1-t-5t^3+40t^4-25t^5-125t^7+625t^8$	510
T^3+2T^2	$1+5t^2-5t^3+25t^4+125t^6$	151
T^3+2T^2+T	$1+4t+15t^2+30t^3+80t^4+\ldots$	1780
T^3+2T^2+2T	$1-t-5t^3+5t^4-25t^5-125t^7+625t^8$	475
T^3+2T^2+3T	$1-t+10t^3-20t^4+50t^5-125t^7+625t^8$	540
T^3+2T^2+4T	$1-t-20t^4-125t^7+625t^8$	480
T^3+3T^2	$1+5t^3+125t^6$	131
T^3+3T^2+T	$1-t+5t^2-15t^3+20t^4-\ldots$	560
T^3+3T^2+2T	$1+4t+10t^2+15t^3+20t^4+\ldots$	1500
T^3+3T^2+3T	$1-t+5t^2-5t^3+45t^4-\ldots$	645
T^3+3T^2+4T	$1-t+20t^4-125t^7+625t^8$	520
T^3+4T^2	$1+15t^3+125t^6$	141
T^3+4T^2+T	$1-t+10t^2-15t^3+60t^4-\ldots$	730
T^3+4T^2+2T	$1-t+5t^3-15t^4+25t^5-125t^7+625t^8$	520
T^3+4T^2+3T	$1+4t+10t^2+25t^3+60t^4+\ldots$	1600
T^3+4T^2+4T	$1-t-5t^3+10t^4-25t^5-125t^7+625t^8$	480
T^4	$1+75t^5+3125t^{10}$	3201

Table 2.5: Class numbers of extensions $F/\mathbb{F}_7(T)$ determined by various $P(T)$.

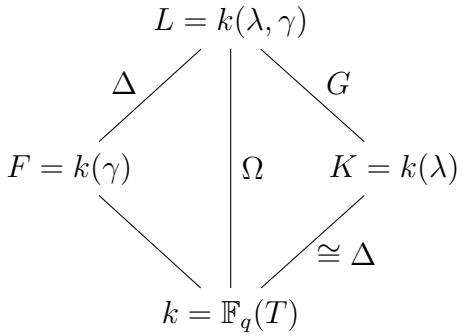
$P(T)$	$G_F(t)$	h_F
T^2	$1+49t^4$	50
T^2+T	$1+6t+21t^2+56t^3+147t^4+294t^5+343t^6$	868
T^2+2T	$1-t+7t^2+7t^3+49t^4-49t^5+343t^6$	357
T^2+3T	$1-t+7t^2+49t^4-49t^5+343t^6$	350
T^2+4T	$1-t-14t^3-49t^5+343t^6$	280
T^2+5T	$1-t+14t^3-49t^5+343t^6$	308
T^2+6T	$1-t+7t^2-14t^3+49t^4-49t^5+343t^6$	336
T^3	$1+16807t^{10}$	16808

We remark on some trends observed in the above tables. For all examples here, the field $F/\mathbb{F}_q(T)$ generated by $P(T)$ has class number divisible by $p = char(F)$ if and only if $P(T)$ has a linear term and $deg(P(T)) \geq 2$ (or ≥ 3, for $q = 2$). For $q = 2$, we notice some additional behavior: $4|h_F$ if and only if $2|h_F$ and $P(T)$ has no quadratic term, and $8|h_F$ if and only if $4|h_F$ and $P(T)$ has no cubic term. These observations are the basis for Theorems 5.1 and 5.8, which show that these trends hold in general.

Similar calculations to the above can be performed to find the class number of two types of extensions: the normal closure of one of these fields, or of the compositum of multiple such fields. Studying the results of such computation led to our initial conjecture of Theorems 3.1 and 3.2 (for the normal closure), and Theorems 4.1 and 4.3 (for composita). Since these theorems allow us to exactly determine the class numbers (indeed, the $G(t)$) of such extensions in terms of subfields of the kind we have already presented, we forego listing examples here.

Chapter 3: Relation to the Galois closure

Let $k = \mathbb{F}_q(T)$ where $q = p^r$ and p is prime. Let λ be a non-zero root of $x^q + Tx$, and γ be a root of $x^q + Tx - P(T)$, where $P(T) \in \mathbb{F}_q[T]$ but $P(T) \neq Q(T)^p + TQ(T)$ for any $Q(T) \in k$. We have the following lattice of fields:[1]



The main objective of this chapter is to prove the following theorems about Cl_L^0, the group of degree-0 divisor classes group of L:

Theorem 3.1. *The class numbers of L and F are related via $h_L = h_F^{q-1}$.*

Theorem 3.2. *When $q = p$ is prime, Cl_L^0 is isomorphic to a $(p-1)$-st power of a finite abelian group.*

In many cases (for instance, when the non-p part of the class number is squarefree and the p part of the class group is cyclic), these combine to say that

[1] The edge labels indicate the Galois groups of the corresponding extensions, which will be described in Section 3.1

$Cl_L^0 = (Cl_F^0)^{p-1}$. However, this is not known in general.

Theorem 3.1 is inspired by one proved by Honda about pure cubic number fields [14]:

Theorem 3.3. *Let $F = \mathbb{Q}(\sqrt[3]{n})$, and $L = \mathbb{Q}(\sqrt[3]{n}, \zeta_3)$ be its normal closure. Then $h_L = h_F^2$ or $h_L = \frac{1}{3}h_F^2$.*

Theorem 3.2 is an analogue of a recent result of Schoof (which itself was also inspired by Honda's). In [25], he proves the following:

Theorem 3.4. *Let $p > 2$ be a regular prime and $n \in \mathbb{Z}$ not a p-th power. Suppose that all prime divisors $l \neq p$ of n are primitive roots mod p. Then the ideal class group Cl_L of $L = \mathbb{Q}(\zeta_p, \sqrt[p]{n})$ and the kernel of the norm map $N_{L/\mathbb{Q}(\zeta_p)}$ fit into the exact sequences*

$$0 \to V \to \ker(N_{L/\mathbb{Q}(\zeta_p)}) \to A^{p-1} \to 0 \text{ and}$$

$$0 \to \ker(N_{L/\mathbb{Q}(\zeta_p)}) \to Cl_L \to Cl_{\mathbb{Q}(\zeta_p)} \to 0,$$

where A is a finite abelian group and V is an $\mathbb{F}_p$-vector space of dimension at most $\left(\frac{p-3}{2}\right)^2$. In particular, if $\#Cl_{\mathbb{Q}(\zeta_p)} = 1$, then Cl_L/V is a $(p-1)$-st power of a finite abelian group.

3.1 Proof of the class number relation

Let k, F, K, and L be as described above, and define $\Omega = \mathrm{Gal}(L/k)$, $G = \mathrm{Gal}(L/K)$, and $\Delta = \mathrm{Gal}(L/F) \cong \mathrm{Gal}(K/k)$. These groups have the presentations

- $G = \langle \tau_1, \ldots, \tau_r \,|\, \tau_i^p = 1,\ \tau_i\tau_j = \tau_j\tau_i \rangle \cong \mathbb{F}_q^+$,

- $\Delta = \langle \sigma \,|\, \sigma^{q-1} = 1 \rangle \cong \mathbb{F}_q^\times$,

- $\Omega = \langle \sigma \in \Delta, \tau \in G \,|\, \sigma\tau\sigma^{-1} = \tau^{\omega(\sigma)} \rangle \cong G \rtimes_\omega \Delta$.

The isomorphism $G \to \mathbb{F}_q^+$ is given by ν, where $\nu(\tau)$ is the element of $\mathbb{F}_q$ such that $\tau(\gamma) = \gamma + \nu(\tau)\lambda$, and $\omega : \Delta \to \mathbb{F}_q^\times$ is the cyclotomic character defined by $\sigma(\lambda) = \omega(\sigma)\lambda$. Refer to the field diagram above for a depiction of these relationships.

Now, Ω can be conveniently realized as the matrix group

$$\left\{ \begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} \;\middle|\; a, x \in \mathbb{F}_q, a \neq 0 \right\},$$

with $\sigma \leftrightarrow \begin{pmatrix} \omega(\sigma) & 0 \\ 0 & 1 \end{pmatrix}$ for $\sigma \in \Delta$ and $\tau \leftrightarrow \begin{pmatrix} 1 & \nu(\tau) \\ 0 & 1 \end{pmatrix}$ for $\tau \in G$. Thus the elements with $a = 1$ are identified with the elements of G, and those with $x = 0$ with the elements of Δ.

We are interested in four characters of Ω which we will show fit an arithmetic relation. These are:

- χ_L, for the regular representation (permutation representation on Ω)

- χ_K, for the permutation representation on Ω/G

- χ_F, for the permutation representation on Ω/Δ

- χ_k, for the trivial representation (permutation representation on Ω/Ω).

Proposition 3.5.

$$\chi_L - \chi_k = \chi_K - \chi_k + (q-1)(\chi_F - \chi_k).$$

Proof. We know of course that χ_k takes the value 1 on every element of Ω, and that χ_L takes $|\Omega| = q(q-1)$ on the identity and 0 elsewhere.

Now, $\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a^{-1}x \\ 0 & 1 \end{pmatrix}$. This says that each coset of Ω/Δ can be represented by a unique element of G, and each coset of Ω/G by a unique element of Δ.

We have $\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & (ab)^{-1}x \\ 0 & 1 \end{pmatrix}$, so an element of Ω fixes a coset of Ω/G if and only if $a = 1$. This says that $\chi_K \begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} = |\Omega/G| = q - 1$ for $a = 1$, and 0 for $a \neq 1$.

On the other hand, $\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & ax + y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, so an element of Ω fixes a coset of Ω/Δ if and only if $x = y(1-a)$. This means that $\chi_F \begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} = |\Omega/\Delta| = q$ for $a = 1, x = 0$, 0 for $a = 1, x \neq 0$, and 1 for $a \neq 1$.

Using the values ascertained above, the relation holds for each element $\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix}$ of Ω as follows:

- For $a = 1, x = 0$: $q(q-1) - 1 = (q-1) - 1 + (q-1)(q-1)$.
- For $a = 1, x \neq 0$: $0 - 1 = (q-1) - 1 + (q-1)(0-1)$.
- For $a \neq 1$: $0 - 1 = 0 - 1 + (q-1)(1-1)$.

□

This arithmetic relation between characters gives rise to a corresponding multiplicative relation between L-functions, and thus zeta functions [26]:

Corollary 3.5.1. *Let ζ_* denote the zeta function for the field $*$. Then*

$$\frac{\zeta_L}{\zeta_k} = \frac{\zeta_K}{\zeta_k} \cdot \left(\frac{\zeta_F}{\zeta_k}\right)^{q-1}.$$

Schmidt [24] gives the residue formula

$$\lim_{s\to 1}(s-1)\zeta(s) = \frac{q^{1-g}h}{(q-1)\log q}$$

and the functional equation

$$\zeta(1-s) = q^{(g-1)(2s-1)}\zeta(s)$$

for the zeta function of a function field in positive characteristic, where g and h denote the genus and class number, respectively[2]. These combine to give a formula for the residue of $\zeta(1-s)$ at 1:

$$\lim_{s\to 1}(s-1)\zeta(1-s) = \lim_{s\to 1}(s-1)q^{(g-1)(2s-1)}\zeta(s) = \frac{h}{(q-1)\log q}.$$

As K and k have trivial class group, applying this equation to the relation in Corollary 3.5.1 gives $h_L = h_F^{q-1}$, completing the proof of Theorem 3.1.

[2]See Roquette [22] for an English reference summarizing these results, but note a typo in the numerator of the residue formula (reversing the sign of the exponent).

3.2 Proof of class group structure theorem

We now restrict to the case that $q = p$ is prime, and set $k = \mathbb{F}_p(T)$, $K = k(\lambda)$, $F = k(\gamma)$, and $L = k(\lambda, \gamma)$. As before, $\Omega = \mathrm{Gal}(L/k)$, $G = \mathrm{Gal}(L/K)$, and $\Delta = \mathrm{Gal}(L/F) \cong \mathrm{Gal}(K/k)$. We remark that now $G = \langle \tau \mid \tau^p = 1 \rangle \cong \mathbb{F}_p^+$ is cyclic.

Naturally, there is a Galois action of Ω on Cl_L^0. The norm element $N_G = \sum_G \tau$ of G gives a map $Cl_L^0 \to Cl_L^0$ that factors through Cl_K^0, which is trivial. Thus Cl_L^0 is a module over the group ring $\mathbb{Z}[\Omega]/(N_G)$, or alternately a module over $\mathbb{Z}[G]/(N_G)$ with a twisted action of Δ (by which we mean that Δ acts on Cl_L^0 in a way that is consistent with the action of Δ on $\mathbb{Z}[G]/(N_G)$). Now, $\mathbb{Z}[G]/(N_G) \cong \mathbb{Z}[\zeta_p]$ as a Δ-module (because N_G is the p-th cyclotomic polynomial evaluated at τ), so we may freely apply standard facts about ζ_p to τ. (We opt to keep the notation in terms of τ rather than ζ_p, to maintain coherence with the function field setting.)

We proceed by separately considering the p part and the non-p part of Cl_L^0.

3.2.1 The non-p part of Cl_L^0

In this section, let M denote the non-p part of the degree-0 divisor class group of L. The following proposition describes the Δ-module structure of M.

Proposition 3.6. *The map*

$$\varphi : M^{\Delta} \otimes_{\mathbb{Z}} \mathbb{Z}[G]/(N_G) \to M$$

given by $\sum_i m_i \otimes [\tau^i] \mapsto \sum_i \tau^i m_i$ *is an isomorphism of* Δ*-modules.*

Proof. Suppose first that $\sum_i \tau^i m_i = 0$ (and note that since N_G acts trivially, this sum can be assumed to be over $1 \leq i \leq p-1$). Then $\sum_i \tau^{i\omega(\sigma)} m_i = 0$ for all σ, and thus for $1 \leq j \leq p-1$,

$$\begin{aligned} 0 &= \sum_{\sigma \in \Delta} \tau^{-j\omega(\sigma)}(1 - \tau^{j\omega(\sigma)}) \sum_i \tau^{i\omega(\sigma)} m_i \\ &= \sum_i \sum_{\sigma \in \Delta} (1 - \tau^{j\omega(\sigma)}) \tau^{(i-j)\omega(\sigma)} m_i. \end{aligned}$$

$\sum_\sigma (1 - \tau^{j\omega(\sigma)}) \tau^{(i-j)\omega(\sigma)}$ acts as $p - 1 + (1 - N_G) = p$ for $i = j$, and as 0 for $i \neq j$, so this says $pm_j = 0$, and thus $m_j = 0$, for all j (since M has order prime to p). Therefore φ is injective.

Now suppose $m \in M$. Then for any i, $N_\Delta(\tau^i m) = \sum_\sigma \tau^{i\omega(\sigma)} \sigma(m) \in M^\Delta$, and accordingly,

$$\begin{aligned} &\sum_{i=1}^{p-1} \tau^{-i\omega(\sigma')}(1 - \tau^{i\omega(\sigma')}) \sum_\sigma \tau^{i\omega(\sigma)} \sigma(m) \\ =&\sum_\sigma \sum_{i=1}^{p-1} (1 - \tau^{i\omega(\sigma')}) \tau^{i(\omega(\sigma) - \omega(\sigma'))} \sigma(m) \in im(\varphi) \text{ for all } \sigma' \in \Delta. \end{aligned}$$

$\sum_i (1 - \tau^{i\omega(\sigma')}) \tau^{i(\omega(\sigma) - \omega(\sigma'))}$ acts as p for $\sigma' = \sigma$ and as 0 for $\sigma' \neq \sigma$, so this says that each $p\sigma'(m)$, and in particular pm, is in $im(\varphi)$. Therefore φ is surjective (again using that M has order prime to p). □

Ignoring the module structure gives $M \cong (M^\Delta)^{p-1}$ as abelian groups, which settles the non-p part of Theorem 3.2.

3.2.2 The p part of Cl_L^0

From this section forward, M will denote the p part of the degree-0 divisor class group of L. Having only p-power torsion allows us to strengthen the $\mathbb{Z}[G]/(N_G)$-module structure previously described to a $\mathbb{Z}_p[G]/(N_G)$-module structure, still with the twisted Δ-action as before. $A = \mathbb{Z}_p[G]/(N_G)$ is a discrete valuation ring, and its maximal ideal is generated by $\tau - 1$ (just as $\zeta_p - 1$ generates the maximal ideal of $\mathbb{Z}_p[\zeta_p]$). Furthermore, $(\tau - 1)^{p-1} = (p)$ as ideals of A, which will be key to this section's results.

As before, Δ acts on τ, and thus on $\tau - 1$, by the cyclotomic character $\omega : \Delta \to \mathbb{F}_p^\times$. We have a filtration of ideals

$$A \supset (\tau - 1)A \supset (\tau - 1)^2 A \supset \dots$$

with successive quotients $\mathbb{F}_p$, $\mathbb{F}_p(\omega)$, $\mathbb{F}_p(\omega^2)$, $\dots$, where $X(\omega^i)$ denotes that the default action of Δ on the module X is twisted by the character ω^i.

We now prove two results which characterize the structure of A-modules with particularly 'nice' Δ-action:

Lemma 3.7. [25, Prop. 3.1] *Let M' be a finite A-module with twisted Δ-action. Then Δ acts trivially on $M'/(\tau - 1)M'$ if and only if there exist $n_1, n_2, \dots, n_t \geq 1$ such that*

$$M' \cong \bigoplus_{i=1}^{t} A/(\tau - 1)^{n_i} A.$$

Proof. Suppose first that the isomorphism holds. Then $M'/(\tau - 1)M'$ is a direct

sum of $A/(\tau-1)A \cong \mathbb{F}_p$ terms with trivial Δ action.

Conversely, suppose that Δ acts trivially on $M'/(\tau-1)M'$. Then the map $M'^{\Delta} \to (M'/(\tau-1)M')^{\Delta} = M'/(\tau-1)M'$ is surjective (its cokernel is the first Δ-cohomology group of $(\tau-1)M'$, which is trivial because Δ and M' have comprime orders). This says that there are Δ-invariant elements $v_1, \ldots, v_t$ which generate M' over A, i.e. that there is a surjective map from $A^t \to M'$ taking 1 in the i-th coordinate to v_i. By the finiteness of M', this descends to a surjective map

$$\varphi : \bigoplus_{i=1}^{t} A/(\tau-1)^{n_i}A \to M'.$$

If φ is not injective, there is a nonzero element x in the kernel, and we may assume $x = (x_1, \ldots, x_t) \in \bigoplus_i (\tau-1)^{n_i-1}A/(\tau-1)^{n_i}A$. Now, Δ acts on x by ω^m for some m, but by ω^{n_i-1} on each of these summands, so x_i is zero unless $n_i - 1 = m + k_i(p-1)$ for some k_i. Reordering if necessary, let the first s coordinates of x be exactly those which are nonzero, and choose n_1 to be minimal among $n_1, \ldots, n_s$. For $i = 1, \ldots, s$, define μ_i such that $x_i = (\tau-1)^m p^{k_i}\mu_i$, and $m_i \in \mathbb{Z}$ such that $m_i \equiv \mu_i \mod (\tau-1)^N$, where N is the maximum of the n_i. Notice that μ_i, and thus m_i, is a unit in A.

We are now able to construct a new map

$$\varphi' : A/(\tau-1)^{n_1-1}A \oplus \bigoplus_{i=2}^{t} A/(\tau-1)^{n_i}A \to M',$$

which takes the basis vector $e_1 = (1, 0, \ldots, 0)$ to $\sum_{i=1}^{s} m_i p^{k_i-k_1} v_i$, and e_i to v_i for

$i \neq 1$. This is well-defined because

$$\begin{aligned}\varphi'((\tau-1)^m p^{k_1} e_1) &= \sum_{i=1}^{s} (\tau-1)^m p^{k_i} m_i v_i \\ &= \sum_{i=1}^{s} (\tau-1)^m p^{k_i} \mu_i v_i = \sum_{i=1}^{s} x_i v_i = \varphi(x) = 0.\end{aligned}$$

Furthermore, φ' is surjective because, by the surjectivity of φ, $m_1 v_1 \in im(\varphi')$, and m_1 is invertible. If φ' is not injective, we repeat this procedure until we reach a map that is, at which point we will have found a direct sum of finite quotients of A which is isomorphic to M'. □

Proposition 3.8. *Let M' be a finite A-module with twisted Δ-action, such that Δ acts trivially on $M'/(\tau-1)M'$ and by ω^{-1} on $M'[\tau-1]$. Then there exists a finite abelian p-group H such that*

$$M \cong H \otimes_{\mathbb{Z}_p} A.$$

Proof. Suppose $M' \cong A/(\tau-1)^n A$ for some positive integer n. Then $M'[\tau-1] = (\tau-1)^{n-1}A/(\tau-1)^n A \cong \mathbb{F}_p(\omega^{n-1})$. By assumption, this requires $n = (p-1)m$ for some positive integer m, whereby $A/(\tau-1)^n A \cong A/p^m A \cong \mathbb{Z}/p^m\mathbb{Z} \otimes_{\mathbb{Z}_p} A$.

By the previous lemma, a general M' satisfying the condition on $M'/(\tau-1)M'$ is a direct sum of such $\mathbb{Z}/p^m\mathbb{Z} \otimes_{\mathbb{Z}_p} A$, proving the proposition. □

It remains to show that this proposition can be applied to (a twist of) M. We will achieve this by exploring the Galois cohomology of Cl_L^0 and related objects.

3.2.3 Galois cohomology of Cl_L^0

In this section, $\hat{H}^i(X)$ is the i-th Tate G-cohomology group of X. We fix the notations

- P_L, the principal L-divisors
- D_L^0, the L-divisors of degree 0
- $\mathbb{I}_L^0$, the ideles of total valuation 0
- $C_L^0 = \mathbb{I}_L^0/L^\times$, the idele classes of total valuation 0
- U_L, the product of the local unit groups $U_\mathfrak{L}$ of L.

We have the following commutative diagram of Ω-modules in which the rows and columns are exact:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \mathbb{F}_p^\times & \to & L^\times & \to & P_L & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & U_L & \to & \mathbb{I}_L^0 & \to & D_L^0 & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & U_L/\mathbb{F}_p^\times & \to & C_L^0 & \to & Cl_L^0 & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 0 & &
\end{array}$$

We will make use of various long exact sequences induced in cohomology by the above diagram in order to study $\hat{H}^i(Cl_L^0)$ for $i = -1, 0$. We remark that a G-cohomology group of an Ω-module is an $\mathbb{F}_p[\Delta]$-module (because it is killed by p and is G-invariant), and any map induced in cohomology by any of the maps in the diagram is Δ-equivariant. Furthermore, since G is a cyclic group, we have Δ-isomorphisms $\hat{H}^i(X) \to \hat{H}^{i-2}(X)(\omega^{-1})$ for every $i \in \mathbb{Z}$ and Ω-module X, given by cupping with a generator of $\hat{H}^{-2}(\mathbb{Z}) \cong H_1(\mathbb{Z}) \cong G \cong \mathbb{Z}/p\mathbb{Z}(\omega)$.

Lemma 3.9. *C_L^0 and $\mathbb{F}_p^\times$ have trivial Tate G-cohomology.*

Proof. The degree map on the idele class group gives rise to the sequence

$$0 \to C_L^0 \to C_L \to \mathbb{Z} \to 0.$$

This gives rise to a long exact sequence which includes

$$H^0(C_L) \to H^0(\mathbb{Z}) \to \hat{H}^1(C_L^0) \to \hat{H}^1(C_L),$$

where the first two terms are standard (i.e. non-Tate) cohomology. We have that $H^0(C_L) = C_L^G = C_K$ [1, p. 2]. The leftmost map, then, is the degree map on C_K *as a subgroup of* C_L. An idele class of C_K which has valuation 1 at an inert prime and valuation 0 elsewhere maintains this property when extended to C_L. Since G is cyclic, there are (infinitely many) primes inert in L/K by the Chebotarev density theorem, and thus the map $H^0(C_L) \to H^0(\mathbb{Z})$ is surjective. We also have $\hat{H}^1(C_L) = 0$ [1, p. 19], and so $\hat{H}^1(C_L^0) = 0$.

Passing the first exact sequence to Tate cohomology and recognizing that $\hat{H}^0(C_L) \cong \mathbb{Z}/p\mathbb{Z}$ [1, p. 19], $\hat{H}^0(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$, and $\hat{H}^{-1}(\mathbb{Z}) \cong \hat{H}^1(\mathbb{Z}) = 0$, we have that $\hat{H}^0(C_L^0) = 0$ as well.

As for $\mathbb{F}_p^\times$, it is a finite module of order prime to the order of G, and so has trivial Tate G-cohomology. □

Applying this lemma to the long exact sequences induced by the leftmost column and bottom row of the diagram immediately gives:

Corollary 3.9.1. *$\hat{H}^{-1}(Cl_L^0) \cong \hat{H}^0(U_L)$ and $\hat{H}^0(Cl_L^0) \cong \hat{H}^1(U_L)$.*

Lemma 3.10. *Δ acts trivially on $\hat{H}^1(U_L)$ and $\hat{H}^2(U_L)$.*

Proof. We write ℓ for a prime of k, $\mathfrak{l}$ for a prime of K above ℓ, and $\mathfrak{L}$ for a prime of L above $\mathfrak{l}$. We have decomposition groups $\Omega_{\mathfrak{L}} = D(\mathfrak{L}/\ell)$, $G_{\mathfrak{L}} = D(\mathfrak{L}/\mathfrak{l})$, and $\Delta_{\mathfrak{l}} = D(\mathfrak{l}/\ell)$. For each i, $\hat{H}^i(U_L)$ can be expressed as a product of local cohomology groups:

$$\begin{aligned}
\hat{H}^i(U_L) &= \hat{H}^i\Big(\prod_{\mathfrak{L} \text{ of } L} U_{\mathfrak{L}}\Big) \\
&= \hat{H}^i\Big(\prod_{\mathfrak{l} \text{ of } K} \bigoplus_{\mathfrak{L}|\mathfrak{l}} U_{\mathfrak{L}}\Big) \\
&= \bigoplus_{\ell \text{ ram in } L} \bigoplus_{\mathfrak{l}|\ell} \hat{H}^i\Big(\bigoplus_{\mathfrak{L}|\mathfrak{l}} U_{\mathfrak{L}}\Big) \\
&= \bigoplus_{\ell \text{ ram in } L} \bigoplus_{\mathfrak{l}|\ell} \hat{H}^i(G_{\mathfrak{L}}, U_{\mathfrak{L}}),
\end{aligned}$$

with the last equality by applying Shapiro's Lemma to $\bigoplus_{\mathfrak{L}|\mathfrak{l}} U_{\mathfrak{L}} = \mathrm{Ind}_{G_{\mathfrak{L}}}^{G} U_{\mathfrak{L}}$. Furthermore, as discussed in Section 1.1, any prime that ramifies in L ramifies totally

in K, which means that $\Delta_{\mathfrak{l}} = \Delta$ and any action it has on $\hat{H}^1(U_L)$ is on a single summand $\hat{H}^i(G_{\mathfrak{L}}, U_{\mathfrak{L}})$. Thus for $i = 1, 2$, it is sufficient to show that Δ acts trivially on $\hat{H}^i(G_{\mathfrak{L}}, U_{\mathfrak{L}})$.

We look first at $i = 1$. Since G and Δ have coprime orders, the inflation-restriction sequence

$$0 \to \hat{H}^1(\Delta_{\mathfrak{l}}, U_{\mathfrak{l}}) \to \hat{H}^1(\Omega_{\mathfrak{L}}, U_{\mathfrak{L}}) \to \hat{H}^1(G_{\mathfrak{L}}, U_{\mathfrak{L}})^{\Delta_{\mathfrak{l}}} \to 0$$

is exact. Now, from local class field theory, $\hat{H}^1(G_{\mathfrak{L}}, U_{\mathfrak{L}})$ is cyclic of order equal to the ramification index $e_{\mathfrak{L}/\mathfrak{l}}$ [1, p. 9], and likewise $\hat{H}^1(\Omega_{\mathfrak{L}}, U_{\mathfrak{L}}) \cong \mathbb{Z}/e_{\mathfrak{L}/\ell}\mathbb{Z}$ and $\hat{H}^1(\Delta_{\mathfrak{l}}, U_{\mathfrak{l}}) \cong \mathbb{Z}/e_{\mathfrak{l}/\ell}\mathbb{Z}$. This forces $\hat{H}^1(G_{\mathfrak{L}}, U_{\mathfrak{L}})^{\Delta_{\mathfrak{l}}} = \hat{H}^1(G_{\mathfrak{L}}, U_{\mathfrak{L}})$, and so the action of $\Delta = \Delta_{\mathfrak{l}}$ on $\hat{H}^1(U_L)$ is trivial.

Next we take $i = 2$. Again by the coprime orders of G and Δ, and also using that $\hat{H}^1(G_{\mathfrak{L}}, L_{\mathfrak{L}}) = 0$ by Hilbert's Theorem 90, the sequence

$$0 \to \hat{H}^2(\Delta_{\mathfrak{l}}, K_{\mathfrak{l}}) \to \hat{H}^2(\Omega_{\mathfrak{L}}, L_{\mathfrak{L}}) \to \hat{H}^2(G_{\mathfrak{L}}, L_{\mathfrak{L}})^{\Delta_{\mathfrak{l}}} \to 0$$

is exact. But local class field theory gives us that these cohomology groups are dual to the decomposition groups that define them [1, p. 9], and so by order considerations, we must have $\hat{H}^2(G_{\mathfrak{L}}, L_{\mathfrak{L}})^{\Delta_{\mathfrak{l}}} = \hat{H}^2(G_{\mathfrak{L}}, L_{\mathfrak{L}})$. Since the inclusion-induced map $\hat{H}^2(G_{\mathfrak{L}}, U_{\mathfrak{L}}) \to \hat{H}^2(G_{\mathfrak{L}}, L_{\mathfrak{L}})$ is injective (its kernel is $\hat{H}^1(G_{\mathfrak{L}}, \mathbb{Z})$, which is trivial), we conclude that $\hat{H}^2(U_L)$ is Δ-invariant as well. □

We are now ready to connect the cohomological theory back to M, the p-part

of Cl_L^0.

Corollary 3.10.1. *Δ acts trivially on $M[\tau - 1]$ and via ω on $M/(\tau - 1)M$.*

Proof. By Corollary 3.9.1 and the fact that N_G kills M, we have

$$M[\tau - 1] \cong \hat{H}^0(Cl_L^0) \cong \hat{H}^1(U_L) \text{ and}$$

$$M/(\tau - 1)M \cong \hat{H}^{-1}(Cl_L^0) \cong \hat{H}^0(U_L) \cong \hat{H}^2(U_L)(\omega),$$

which have the claimed actions by Lemma 3.10. □

Finally, we can prove the p part of our result:

Proposition 3.11. *M is a $(p-1)$-st power of some finite abelian p-group.*

Proof. We consider the twist $M' = M(\omega^{-1})$. The previous result says that Δ acts trivially on $M'/(\tau - 1)M'$ and by ω^{-1} on $M'[\tau - 1]$. Thus Proposition 3.8 may be applied to M'. As abelian groups, $M \cong M'$, so we are done. □

Combining this with Proposition 3.6, we have that the p part and non-p part of Cl_L^0 are each the $(p-1)$-st power of an abelian group, and so the proof of Theorem 3.2 is complete.

Chapter 4: Class numbers of composite fields

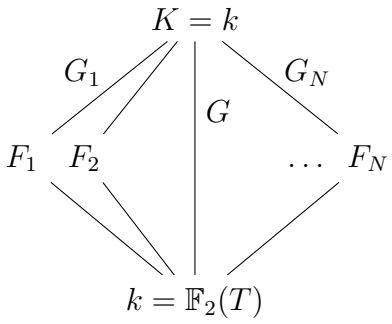
We now consider composita of multiple members of this family of fields. Let $\{P_i(T)\}_{i=1}^n$ be a set of linearly independent polynomials in $k = \mathbb{F}_q(T)$ whose span does not contain a polynomial of the form $P(T) = Q(T)^q + TQ(T)$. Then the extensions F_i, each given by a fixed root of $x^q + Tx - P_i(T)$, are independent, i.e., their compositum K is a degree q^n extension of k. The $N = \frac{q^n-1}{q-1}$ monic linear combinations of the P_i determine N distinct subfields of degree q over k. We will show in this chapter that the class number of K is exactly the product of the class numbers of these subfields.

The corresponding situation has been studied in the number field setting, especially for quadratic and cubic extensions. Herglotz [12] proves that the class number of $\mathbb{Q}(\sqrt{m_1}, \ldots \sqrt{m_n})$ is *almost* the product of the class numbers of its quadratic subfields, with a possible deficiency in the 2-part of the class group related to the unit group of the composite field. Parry [18] finds a similar result for bicubic fields: the class number of $\mathbb{Q}(\sqrt[3]{m_1}, \sqrt[3]{m_2})$ is the product of the class numbers of its cubic subfields, possibly divided by some power of 3. For general p, Ohta [17] (following an earlier result of Nakagoshi [16]) proves a similar statement about the non-p part of the class groups in an abelian number field extension of type $(p, p, \ldots, p)$.

4.1 The case $q = 2$

Let $\{P_i(T)\}_{i=1}^n$ be a set of polynomials in $k = \mathbb{F}_2(T)$ whose span does not contain any polynomial of the form $Q(T)^2 + TQ(T)$. Then the extensions F_i each given by a root of $x^2 + Tx - P_i(T)$ are independent, i.e., their compositum K is a degree 2^n extension of k. The Galois group of K/k is $G \cong (\mathbb{Z}/2\mathbb{Z})^n$.

There are $N = 2^n - 1$ quadratic subfields[1] of K, which correspond to the non-trivial linear combinations of the P_i (and the index-2 subgroups G_i of G of which they are the fixed fields). The situation is illustrated in the following diagram:



Theorem 4.1. *The class numbers of these fields are related by* $h_K = \prod_{i=1}^N h_{F_i}$.

We write χ_F to denote the character of the permutation representation of G acting on $G/\mathrm{Gal}(K/F)$.

Lemma 4.2. $\chi_K - \chi_k = \sum_{i=1}^N (\chi_{F_i} - \chi_k)$

Proof. Clearly $\chi_k(G) = 1$, $\chi_K(1) = |G| = 2^n$, and $\chi_K(G\backslash 1) = 0$.

Now, each χ_{F_i} is the character of the permutation representation of G on G/G_i. Since G is abelian, $\chi_{F_i}(G_i) = 2$ and $\chi_{F_i}(G\backslash G_i) = 0$. Furthermore, any given

[1] We denote the complementary subfields $F_{n+1}, \ldots, F_N$, but their ordering is unimportant.

non-zero element of G is contained in $2^{n-1}-1$ of the subgroups G_i and not contained in 2^{n-1} of them. Thus for $g \neq 1$,

$$\sum_{i=1}^{N}(\chi_{F_i}(g) - \chi_k(g)) = \sum_{g\in G_i} 1 + \sum_{g\notin G_i} -1 = 2^{n-1} - 1 - 2^{n-1} = -1 = \chi_K(g) - \chi_k(g),$$

and for $g = 1$,

$$\sum_{i=1}^{N}(\chi_{F_i}(1) - \chi_k(1)) = N(2-1) = 2^n - 1 = \chi_K(1) - \chi_k(1).$$

□

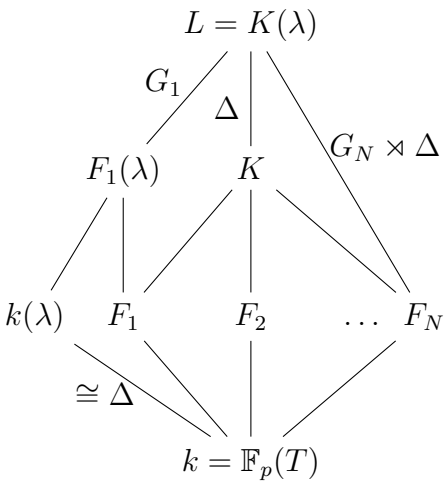
As in Section 3.1, this character relation gives a multiplicative relation of class numbers, and since $h_k = 1$, this proves Theorem 4.1.

4.2 The case $q \neq 2$

Let $q \neq 2$ be a power of a prime p, and let $\{P_i(T)\}_{i=1}^n$ be a set of polynomials in $k = \mathbb{F}_q(T)$ whose span does not contain a polynomial of the form $Q(T)^q + TQ(T)$. Then the extensions F_i, each given by a fixed root of $x^q + Tx - P_i(T)$, are independent. We note there are $N = \frac{q^n-1}{q-1}$ subfields (including the F_i) of K determined by the projective linear combinations of the P_i.

The Galois closure of each F_i (and thus their compositum) is formed by adjoining a non-zero root λ of $x^q + Tx = 0$. The Galois closure L of K has Galois group $\Omega = G \rtimes_\omega \Delta$, where $G \cong (\mathbb{F}_q^+)^n$, $\Delta \cong \mathbb{F}_q^\times$, and Δ acts on G via the cyclotomic

character ω. The fields and Galois groups are illustrated in the following diagram:



Theorem 4.3. $h_K = \prod_{i=1}^{N} h_{F_i}$

Lemma 4.4. $h_L = h_K^{q-1}$

Proof. Following the proof of Proposition 3.5, we get the relations

$$\chi_{F_1(\lambda)} = \chi_{k(\lambda)} + (q-1)(\chi_{F_1} - \chi_k)$$

$$\chi_{F_1F_2(\lambda)} = \chi_{F_1(\lambda)} + (q-1)(\chi_{F_1F_2} - \chi_{F_1})$$

$$\ldots$$

$$\chi_L = \chi_{F_1\ldots F_{n-1}(\lambda)} + (q-1)(\chi_K - \chi_{F_1\ldots F_{n-1}}).$$

Recalling that $h_k = h_{k(\lambda)} = 1$, converting to class numbers and successively substituting gives

$$h_{F_1(\lambda)} = h_{F_1}^{q-1}$$

$$h_{F_1F_2(\lambda)} = h_{F_1(\lambda)} \left(\frac{h_{F_1F_2}}{h_{F_1}} \right)^{q-1} = h_{F_1F_2}^{q-1}$$

$$\dots$$

$$h_L = h_{F_1 \dots F_{n-1}(\lambda)} \left(\frac{h_K}{h_{F_1 \dots F_{n-1}}} \right)^{q-1} = h_K^{q-1}$$

□

Lemma 4.5. $\chi_L - \chi_{k(\lambda)} = (q-1) \sum_{i=1}^{N} (\chi_{F_i} - \chi_k)$.

Proof. Clearly $\chi_k(\Omega) = 1$, $\chi_L(1) = |\Omega| = q^n(q-1)$, and $\chi_L(\Omega \backslash 1) = 0$.

$\chi_{k(\lambda)}$ is the permutation representation of Ω on $\Omega/G \cong \Delta$. But G acts trivially on Δ, from which we see $\chi_{k(\lambda)}(G) = q-1$, and $\chi_{k(\lambda)}(\Omega \backslash G) = 0$.

For a given i, χ_{F_i} is the permutation representation of Ω on $\Omega/(G_i \rtimes \Delta)$. The cosets can be represented by $\{\tau^s\}_{s \in \mathbb{F}_q}$ for a fixed $\tau \in G \backslash G_i$. Since G is abelian, it is easy to see that $\chi_{F_i}(G_i) = q$ and $\chi_{F_i}(G \backslash G_i) = 0$.

Now we consider an element of $\Omega \backslash G$, which can be represented by $\tau^t \sigma \tilde{\tau}$, with $t \in \mathbb{F}_q$, $1 \neq \sigma \in \Delta$, and $\tilde{\tau} \in G_i$. Its action sends the coset represented by τ^s to $\tau^{t+s\omega(\sigma)}$. This is equal to τ^s exactly when $s = \frac{t}{1-\omega(\sigma)}$, and so $\chi_{F_i}(\Omega \backslash G) = 1$.

We can now show the character relation holds for each element of Ω. For 1:

$$\begin{aligned}
(q-1) \sum_{i=1}^{N} (\chi_{F_i}(1) - \chi_k(1)) &= (q-1)N(q-1) \\
&= (q-1)(q^n - 1) \\
&= q^n(q-1) - (q-1) \\
&= \chi_L(1) - \chi_{k(\lambda)}(1).
\end{aligned}$$

For $g \in \Omega \backslash G$:

$$\begin{aligned}(q-1)\sum_{i=1}^{N}(\chi_{F_i}(g)-\chi_k(g)) &= (q-1)N(1-1)\\ &= 0-0\\ &= \chi_L(g)-\chi_{k(\lambda)}(g).\end{aligned}$$

For $g \in G$, $g \neq 1$, we note that g is contained in $\frac{q^{n-1}-1}{q-1} = \frac{N-1}{q}$ of the subgroups G_i, and not contained in q^{n-1} of them. Thus:

$$\begin{aligned}(q-1)\sum_{i=1}^{N}(\chi_{F_i}(g)-\chi_k(g)) &= (q-1)\left(\sum_{g\in G_i}(q-1)+\sum_{g\notin G_i}-1\right)\\ &= (q-1)(q^{n-1}-1-q^{n-1})\\ &= 0-(q-1)\\ &= \chi_L(G)-\chi_{k(\lambda)}(g).\end{aligned}$$

Therefore the relation holds for all of Ω. □

As before, we convert this to a multiplicative class number relation, which simplifies to $h_L = (\prod_{i=1}^{N} h_{F_i})^{q-1}$. Combining this with Lemma 4.4 completes the proof of Theorem 4.3.

Chapter 5: p-divisibility of the class number

In this chapter, we consider the question of when the class number of the field generated over $\mathbb{F}_q(T)$ by a root of $x^q + Tx - P(T)$ is divisible by the characteristic p. The analogous question for quadratic number fields has been studied (albeit originally in the language of genera of quadratic forms) dating back to Gauss' genus theory [6]. In modern terms, Gauss proves that the 2-torsion of the narrow class group has rank $t - 1$, generated by the t ramified primes (see e.g. [5, 13]).

Redéi and Reichardt extend this theory to study the 2^n-torsion of the class group of quadratic number fields. Reichardt [21] characterizes the rank of the 2^n-torsion in terms of the number of "D-decompositions of the n-th kind", the number of ways of splitting the discriminant D into the product of two discriminants meeting certain criteria. They also derive residue conditions for a D-decomposition to be of the second kind [20], and of the third kind (for certain cases) [19]. One of the cases about which the most is known is $D = -4p$, which gives an imaginary quadratic field in which either one or two primes ramify (and thus cyclic 2-class group). In this case, the 2- and 4- divisibility conditions reduce to:

$$2|h(-4p) \Leftrightarrow p = x^2 + 4y^2$$

$$4|h(-4p) \Leftrightarrow p = x^2 + 8y^2$$

and Barrucand and Cohn [3] show that

$$8|h(-4p) \Leftrightarrow p = x^2 + 32y^2$$

(see [15] for an overview). We will see that this case closely resembles ours when $q = 2$, where T and $1/T$ play the role of of p and 2, respectively, in terms of their ramification / splitting behavior. We give conditions on the polynomial $P(T)$ that determine when the class number of the corresponding field is divisible by 2, 4, and 8, and show that the 2-class group is always cyclic.

The more general question of when p divides the class number of a pure degree-p field has not been studied as thoroughly, but Honda [14] determines the conditions for $p = 3$. Given our somewhat 'nicer' setting, we are able to give a complete description of when the class number of the extension of $\mathbb{F}_q(T)$ corresponding to $P(T)$ is divisible by the characteristic.

5.1 The case $q = 2$

Let $k = \mathbb{F}_2(T)$ and $P(T) \in \mathcal{O}_k = \mathbb{F}_2[T]$ such that $P(T) \neq Q(T)^2 + TQ(T)$ for any $Q(T) \in \mathcal{O}_k$. By a change of variables, it suffices to consider $P(T)$ to comprise

only terms of odd degree, except possibly a quadratic term.

Theorem 5.1. *Let $F = k(\gamma)$, where γ is a root of $x^2 + Tx - P(T)$, with $P(T)$ in the form described above.*[1] *We denote by Cl_F^0 its degree-0 divisor class group, and $h_F = |Cl_F^0|$. Then:*

1. *The 2-Sylow subgroup of Cl_F^0 is cyclic.*
2. *$2|h_F$ if and only if $ord_T(P(T) - T) \geq 2$ and $deg(P(T)) \geq 3$.*
3. *$4|h_F$ if and only if $ord_T(P(T) - T) \geq 3$.*
4. *$8|h_F$ if and only if $ord_T(P(T) - T) \geq 5$.*

As we will show momentarily, the infinite prime $1/T$ of k ramifies in F in all but a few cases. When it does, Rosen [23] shows that there is an isomorphism between Cl_F^0 and the ideal class group of $\mathcal{O}_F$, the integral closure of $\mathcal{O}_k$ in F (alternatively, the ring of functions with poles only at infinity), given by:

$$\begin{aligned} Cl_F^0 &\cong Cl(\mathcal{O}_F) \\ \sum n_{\mathfrak{p}}[\mathfrak{p}] &\mapsto \prod_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathfrak{p}^{n_{\mathfrak{p}}} \\ \sum n_{\mathfrak{p}}[\mathfrak{p}] - (\sum n_{\mathfrak{p}})[\mathfrak{p}_\infty] &\mapsfrom \prod_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathfrak{p}^{n_{\mathfrak{p}}}, \end{aligned}$$

where $\mathfrak{p}_\infty$ is the prime above $1/T$. He also shows that this permits a characterization of the Hilbert class field H/F as the maximal abelian unramified extension of F in

[1] Despite being in characteristic 2, we will use subtraction in our notation when it is helpful for giving intuition or remaining consistent with the more general case.

which $\mathfrak{p}_\infty$ splits completely, which enjoys many of the same properties as the Hilbert class field of a number field.

The following lemmas identify the behavior of T and $1/T$ in F/k in terms of $P(T)$. We reiterate that both $deg(P(T))$ and $ord_T(P(T))$ are odd or equal to 2.

Lemma 5.2. *T ramifies in F if $ord_T(P(T)) = 1$, is inert if $ord_T(P(T)) = 2$, and splits if $ord_T(P(T)) > 2$.*

Proof. Suppose $ord_T(P(T)) = 1$. Then $x^2 + Tx - P(T)$ is an Eisenstein polynomial at T, and thus T ramifies in the extension it generates (which is F).

Now suppose $ord_T(P(T)) = 2$. Then the change of variables $Tx \leftarrow\!\shortmid\, x$ and division by T^2 changes the polynomial defining F to $x^2 + x - \frac{P(T)}{T^2}$, which has discriminant 1. Thus denoting a root by α, the integral closure of $\mathcal{O}_k$ in F is given by $\mathcal{O}_F = \mathbb{F}_2[T, \alpha]$. Since $\alpha^2 + \alpha \equiv 1 \mod T$,

$$\mathcal{O}_F/T\mathcal{O}_F \cong \mathbb{F}_4,$$

so T is inert in F.

Finally, suppose $ord_T(P(T)) > 2$. The change of variables $Tx \leftarrow\!\shortmid\, x$ and division by T^2 changes the polynomial defining F to $x^2 + x - \frac{P(T)}{T^2}$. This polynomial splits into (distinct) factors mod T, so T splits in F. □

Lemma 5.3. *$1/T$ ramifies in F if $deg(P(T)) > 2$, is inert if $deg(P(T)) = 2$, and splits if $deg(P(T)) = 1$ (i.e., $P(T) = T$).*

Proof. Suppose $d = deg(P(T)) > 2$. The change of variables $T^{\frac{d+1}{2}}x \leftarrow\!\shortmid\, x$ and

division by T^{d+1} changes the polynomial defining F to $x^2 + \left(\frac{1}{T}\right)^{\frac{d-1}{2}} x - \frac{P(T)}{T^{d+1}}$. This is Eisenstein at $1/T$, and thus $1/T$ ramifies.

Both cases when $d \leq 2$ follow from the corresponding facts for T in the previous lemma, noting that the change of variables $T^2 x \leftarrow\!\shortmid x$ gives $x^2 + \frac{1}{T}x - \frac{P(T)}{T^4}$. □

Lemma 5.4. *If $deg(P(T)) > 2$, then $\mathcal{O}_L^\times = \{1\}$.*

Proof. [This also follows from the analogue of the S-unit theorem, stated e.g. in [23]; we provide this elementary proof for the sake of self-containment.]

If $ord_T(P(T)) = 1$, T ramifies in F, so $\mathcal{O}_L = \mathbb{F}_2[T, \gamma]$ is the full integral closure of $\mathcal{O}_k$ in L, as it has discriminant $-T^2$. If $ord_T(P(T)) \geq 2$, then $\mathcal{O}_L = \mathbb{F}_2[T, \frac{\gamma}{T}]$, as in Lemma 5.2.

For the first case, suppose $f(T) + \gamma g(T) \in \mathcal{O}_L^\times$ with $f, g \neq 0$. Then

$$1 = N(f(T) + \gamma g(T)) = f(T)^2 + P(T)g(T)^2 + Tf(T)g(T).$$

Let d, m, n denote the degrees of P, f, g respectively. To achieve the necessary cancellation, we must have one of the following:

1. $2m = 2n + d \geq m + n + 1$
2. $2m = m + n + 1 \geq 2n + d$
3. $2n + d = m + n + 1 \geq 2m$.

(1) is impossible since d is assumed to be odd. Case (2) would imply $m = n + 1$, and thus $2n + 2 \geq 2n + d$, contradicting the condition on d. Finally, (3) would give

$n+1 \geq m$, and thus $2n+d > 2n+2 \geq m+n+1$, a contradiction. Therefore one of f, g must be 0, and clearly this requires $f = 1, g = 0$.

In the case that $ord_T(P(T)) \geq 2$, a similar degree argument shows that if

$$1 = N(f(T) + \frac{\gamma}{T}g(T)) = f(T)^2 + \frac{P(T)}{T^2}g(T)^2 + f(T)g(T),$$

we must have $f = 1, g = 0$. □

Proof of Theorem 5.1(1,2).

In the cases when $1/T$ does not ramify in F ($P(T) = T$, T^2, or $T^2 + T$), F is genus 0, so the theorem is true. We henceforth assume $1/T$ ramifies in F (i.e., $deg(P(T)) > 2$). This permits us to use the isomorphism $Cl_F^0 \cong Cl(\mathcal{O}_F)$ and consider the behavior of finite ideals.

Suppose $I \in \mathcal{I}_{\mathcal{O}_F}$ such that $I^2 \in P_{\mathcal{O}_F}$, and let σ be the non-trivial element of $Gal(F/k)$. Then $\sigma(I)/I = N(I)/I^2 = (a)$, with $N(a) = 1$. By Hilbert's Theorem 90, $a = b/\sigma(b)$ for some $b \in F$, and so the class of I contains the fixed ideal $J = bI$. Thus J is a product of (principal) ideals of $\mathcal{O}_k$ and primes of $\mathcal{O}_F$ above ramified primes. This shows that the 2-torsion of $Cl(\mathcal{O}_F)$ is generated by the ramified primes. Since T is the only prime which may ramify, the 2-Sylow subgroup is cyclic, and trivial if T is unramified.

Now, suppose T does ramify. If the prime above T is the principal ideal (b), we would thus have $(b)^2 = T\mathcal{O}_F$, which by Lemma 5.4 requires $b^2 = T$. But this contradicts the separability of F, and thus the prime above T is non-principal. Therefore $2|h_F$ in this case, which occurs when $ord_T(P(T) - T) \geq 2$. □

The Hilbert class field theory of Rosen [23] tells us that a rational (degree-1) prime $\mathfrak{p}$ of $\mathcal{O}_F$ splits completely in a subextension H' of the Hilbert class field H if and only if the class $[\mathfrak{p}]$ is contained in the subgroup of $Cl(\mathcal{O}_F)$ isomorphic to $Gal(H/H')$. This will be critical for the following proposition, which is the analogue for our situation of one of Reichardt [21, Thm. 1], and follows approximately the same proof.

Proposition 5.5. *Let F be a field as above whose class group has 2-rank 1. Then the 2^n-rank is 1 if and only if there exists an unramified cyclic extension H_{n-1}/F of degree 2^{n-1} in which the primes of F above T and $1/T$ split completely.*

Proof. Suppose such an extension H_{n-1}/F exists, and let $H \supset H_{n-1}$ be the Hilbert class field of F, so that $Cl(\mathcal{O}_F) \cong Gal(H/F)$. Let G_{n-1} denote the subgroup of $Cl(\mathcal{O}_F)$ corresponding to $Gal(H/H_{n-1})$. Since the prime $\mathfrak{p}$ above T splits completely in H_{n-1}, its class lies in G_{n-1}. Recalling that this class is the unique 2-torsion element of $Cl(\mathcal{O}_F)$, we must have that G_{n-1} has 2-rank 1. Since $Cl(\mathcal{O}_F)/G_{n-1} \cong \mathbb{Z}/2^{n-1}\mathbb{Z}$, $Cl(\mathcal{O}_F)$ must therefore have 2^n rank 1.

For the converse, suppose H contains a subfield H_n which is cyclic of degree 2^n over F, and denote by G_n the subgroup of $Cl(\mathcal{O}_F)$ corresponding to $Gal(H/H_n)$. Since $\mathfrak{p}^2 = (T)$ is principal, its class is trivial in the quotient $Cl(\mathcal{O}_F)/G_n$. Thus $[\mathfrak{p}]$ is contained in a subgroup G_{n-1} of $Cl(\mathcal{O}_F)$ such that $G_{n-1}/G_n \cong \mathbb{Z}/2\mathbb{Z}$. Since $[\mathfrak{p}] \in G_{n-1}$, $\mathfrak{p}$ splits completely in the fixed field H_{n-1} of the corresponding subgroup of $Gal(H/F)$, and $Gal(H_{n-1}/F) \cong Cl(\mathcal{O}_F)/G_{n-1} \cong \mathbb{Z}/2^{n-1}\mathbb{Z}$. □

Proof of Theorem 5.1(3).

Suppose $ord_T(P(T)-T) \geq 2$ and $deg(P(T)) \geq 3$. Let F_1 be the field generated by a root α of $x^2 + Tx - (P(T) - T)$, and F_2 by a root of $x^2 + Tx - T$. By Lemmas 5.2 and 5.3, T is unramified and $1/T$ is ramified in F_1, while T is ramified and $1/T$ splits in F_2. Thus the compositum $K = F_1F_2$ is an unramified degree-2 extension of F in which the (unique) prime above $1/T$ splits.

Since the 2-rank of the class group is 1, K is the unique quadratic subextension of the Hilbert class field of F. In the case that $ord_T(P(T) - T) = 2$, T is inert in K/F, so by Proposition 5.5, $4 \nmid h_F$. On the other hand, if $ord_T(P(T) - T) \geq 3$, then T splits in K/F, so $4|h_F$. □

We now construct explicitly the degree-4 subextension of the Hilbert class field of F (when it exists), which we will use to prove the last statement of Theorem 5.1.

Let α be a root of $x^2 + Tx - (P(T) - T)$, where $ord_T(P(T) - T) \geq 3$. Then T splits in $F_1 = k(\alpha)$, and at one of the primes above T, we can express $\frac{\alpha}{T}$ as a power series in T (in particular, a power series in $\frac{P(T)-T}{T^2}$):

$$\left(\frac{\alpha}{T}\right)^2 + \frac{\alpha}{T} = \frac{P(T) - T}{T^2}$$

$$\frac{\alpha}{T} = \sum_{k=0}^{\infty} \left(\frac{P(T) - T}{T^2}\right)^{2^k},$$

and the conjugate $\frac{\alpha+T}{T} = 1 + \frac{\alpha}{T}$. At the other prime above T, these power series are reversed.

Let s be an integer greater than $\frac{deg(P(T))-1}{2}$. The power series for $\frac{\alpha}{T}$ above contains finitely many terms of degree less than s. We denote by $f(T)$ the polynomial

comprising these terms. Finally, we define $K_\alpha = F_1(\beta)$, where β is a root of

$$x^2 + x - \frac{\alpha/T - f(T)}{T^s},$$

and similarly the conjugate extension $K_{\alpha+T} = F_1(\beta')$, where β' is a root of

$$x^2 + x - \frac{(\alpha+T)/T - f(T)}{T^s}.$$

We remark that the particular fields these define depend on the choice of s. We will soon choose a specific s, but the following two lemmas hold for any $s > \frac{deg(P(T))-1}{2}$. We also note that this construction requires $ord_T(P(T) - T) \geq 3$, and we continue to assume that $P(T)$ has no terms of even degree.

Lemma 5.6. *The prime of F_1 above $1/T$ splits in both K_α and $K_{\alpha+T}$.*

Proof. Let $d = deg(P(T))$. Then

$$\left(\frac{\alpha/T}{T^{(d-1)/2}}\right)\left(\frac{(\alpha+T)/T}{T^{(d-1)/2}}\right) = \frac{P(T) - T}{T^{d+1}},$$

so the prime of F_1 above $1/T$ is $(\frac{\alpha/T}{T^{(d-1)/2}}, \frac{1}{T})$. By construction, $s > \max\{\frac{d-1}{2}, deg(f)\}$, so $\frac{\alpha/T - f(T)}{T^s}$ (and its conjugate) have positive valuation at this prime. Therefore mod this prime, the polynomial $x^2 + x - \frac{\alpha/T - f(T)}{T^s}$ splits (as does its conjugate), so the prime splits in both K_α and $K_{\alpha+T}$. □

Lemma 5.7. *Let s be as before, and suppose further that it is a power of 2. One prime of F_1 above T is unramified in K_α and ramified in $K_{\alpha+T}$, and the other prime*

above T does the reverse. In particular, if $ord_T(P(T) - T) = 3$, the unramified primes are inert, and if $ord_T(P(T) - T) > 3$, they split.

Proof. Consider the prime above T where $\frac{\alpha}{T} = \sum_{k=0}^{\infty} \left(\frac{P(T)-T}{T^2}\right)^{2^k}$. The right-hand side contains T^{2^k}, for all $k \geq 0$, as a summand if $ord_T(P(T)-T) = 3$, and contains no terms of degree a power of two otherwise. Furthermore, by construction $\alpha/T - f(T)$ has only terms of degree $\geq s$. Thus we see that

$$\frac{\alpha/T - f(T)}{T^s}$$

has valuation 0 at the prime in question if $ord_T(P(T)-T) = 3$, and positive valuation otherwise, corresponding to the prime being inert and splitting, respectively, in K_α. On the other hand, the polynomial defining $K_{\alpha+T}$ is

$$x^2 + x - \frac{(\alpha + T)/T - f(T)}{T^s} = x^2 + x - \left(\frac{\alpha/T - f(T)}{T^s} + \frac{1}{T^s}\right).$$

Because s is a power of 2, a change of variables allows us to replace $\frac{1}{T^s}$ by $\frac{1}{T}$ in the last term, which thus has valuation -1 at the prime in question. Therefore the prime is ramified[2] in $K_{\alpha+T}$.

At the other prime above T, the power series associated to $\frac{\alpha}{T}$ and $\frac{\alpha+T}{T}$ are reversed, and so the behavior in K_α and $K_{\alpha+T}$ is reversed. □

We are now prepared to show that when s is the least power of 2 greater than $\frac{deg(P(T))-1}{2}$, the composite field $L = K_\alpha K_{\alpha+T}$ is an unramified degree-4 extension

[2]Since a change of variables can make the polynomial Eisenstein; see also [10].

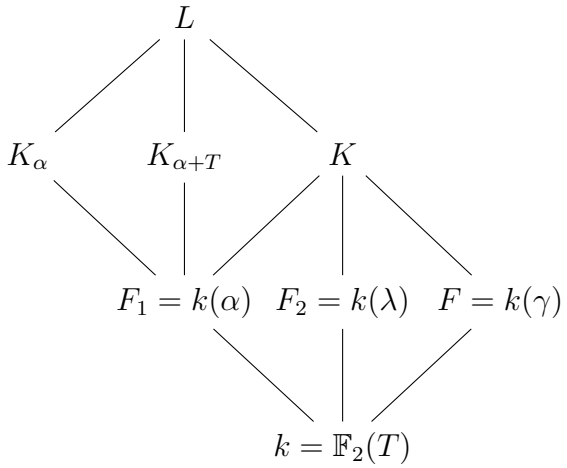
of F in which the prime above $1/T$ splits completely, and complete the proof of Theorem 5.1.

Proof of Theorem 5.1(4).

Let $L = K_\alpha K_{\alpha+T}$, with $K_\alpha, K_{\alpha+T}$ defined by s, the least power of 2 greater than $\frac{deg(P(T))-1}{2}$. The linearity of $x^2 + x$ means that L contains a solution to

$$x^2 + x = \frac{(\alpha+T)/T - f(T)}{T^s} - \frac{\alpha/T - f(T)}{T^s} = \frac{1}{T^s}.$$

By a change of variables, this is equivalent to containing a root of $x^2 + Tx - T$, so L contains F_2. Since it is defined as an extension of F_1, it thus contains $K = F_1F_2$. More specifically, K is the third and final intermediate subfield of L/F_1. The situation is illustrated in the diagram below.



We recall the splitting/ramification behavior of T and $1/T$ in the lower right diamond from Lemmas 5.2 and 5.3 and the proof of Theorem 5.1(3): the (unique) prime of F above each of T and $1/T$ splits in K/F; the primes of F_1 above T ramify and the prime above $1/T$ splits in K/F_1.

From the preceding two lemmas, we also have that each prime of F_1 above T is unramified in one of K_α/F_1 and $K_{\alpha+T}/F_1$, and the prime above $1/T$ splits in both. Thus the primes above T are unramified in L/K, and the primes above $1/T$ split in L/K. Therefore L is an unramified degree-4 extension of F in which the prime above $1/T$ splits completely[3].

Furthermore, the previous lemma shows that the primes above T split completely in L/F if and only if $ord_T(P(T) - T) > 3$. By Proposition 5.5, this means that $8|h_F$ if and only if $ord_T(P(T) - T) > 3$, which completes the proof. □

5.2 The case $q \neq 2$

Let q be a power of a prime p. Let $k = \mathbb{F}_q(T)$ and $P(T) \in \mathcal{O}_k = \mathbb{F}_q[T]$ such that $P(T) \neq Q(T)^q + TQ(T)$ for any $Q(T) \in \mathcal{O}_k$. By a change of variables, it suffices to consider $P(T)$ to be monic and comprise only terms of degree not divisible by q.

Theorem 5.8. *Let $F = k(\gamma)$, where γ is a root of $x^q + Tx - P(T)$, with $P(T)$ in the form described above. Then $p|h_F$ if and only if $deg(P(T)) \geq 2$ and $ord_T(P(T)) = 1$.*

It will be convenient at times to work with the Galois closure $F(\lambda)$ of F, where $\lambda^{q-1} = -T$. By Theorem 3.1, $h_{F(\lambda)} = h_F^{q-1}$, so the question of p-divisibility is the same for each, and since the degrees $[F : k] = [F(\lambda) : k(\lambda)] = q$ and $[k(\lambda) : k] = [F(\lambda) : F] = q - 1$ are relatively prime, it is easy to relate ramification in F/k to ramification in $F(\lambda)/k(\lambda)$ (or $/k$). Obviously $(T) = (\lambda)^{q-1}$ and $(1/T) = (\frac{1}{\lambda})^{q-1}$, i.e. both ramify completely in $k(\lambda)/k$.

[3]Since the 2-rank of the class group of F is 1, it is the unique such extension, and cyclic.

Lemma 5.9. *T is totally ramified in F if $ord_T(P(T)) = 1$, otherwise it is unramified (and λ splits completely in $F(\lambda)/k(\lambda)$).*

Proof. If $ord_T(P(T)) = 1$, $x^q + Tx - P(T)$ is Eisenstein at T, and thus ramifies completely.

Suppose $ord_T(P(T)) \geq 2$. Then $F(\lambda)/k(\lambda)$ is given by $x^q - \lambda^{q-1}x - P(-\lambda^{q-1})$, or by a change of variables, the Artin-Schreier polynomial $x^q - x - \frac{P(-\lambda^{q-1})}{\lambda^q}$. This polynomial splits into (distinct) linear factors mod λ, and thus λ splits completely in $F(\lambda)$ (and T is unramified in F/k). □

Lemma 5.10. *$1/T$ is totally ramified in F if $deg(P(T)) \geq 2$, otherwise it is unramified (and $1/\lambda$ splits completely in $F(\lambda)/k(\lambda)$).*

Proof. The only case when $deg(P(T)) < 2$ is $P(T) = \omega T$, $\omega \in \mathbb{F}_q^\times$. In this case, a change of variables gives $x^q - x - \frac{1}{-\lambda}$ as the polynomial which generates the extension $F(\lambda)/k(\lambda)$. As in the previous lemma, this polynomial splits mod $1/\lambda$, and so $1/\lambda$ splits completely in $F(\lambda)$ (and $1/T$ is unramified in F/k).

Now suppose that $ord_T(P(T)) \geq 2$, so that by the previous lemma, λ splits completely in $F(\lambda)/k(\lambda)$, and consider the subfield of $F(\lambda)$ fixed by the inertia group of a prime above $1/\lambda$. This is an unramified extension of $k(\lambda)$ in which λ splits completely. But $k(\lambda)$ has class number 1, so the extension is trivial, and thus $1/\lambda$ must be totally ramified in $F(\lambda)/k(\lambda)$ (and so must $1/T$ in F/k).

Finally, suppose $ord_T(P(T)) = 1$ and $deg(P(T)) \geq 2$. Then the compositum of F with the extension given by $x^q + Tx - T$ (which, from above, is unramified at $1/T$) contains a root of $x^q + Tx - (P(T) - \omega T)$, where ωT is the linear term of $P(T)$.

By the above, this generates an extension in which $1/T$ has ramification index q, and therefore $1/T$ must ramify completely in F/k. □

Proof of Theorem 5.8.

F has genus 0 if $deg(P(T)) < 2$, and so the theorem holds. We henceforth assume $deg(P(T)) \geq 2$, which means that $1/T$ is totally ramified in $F(\lambda)/k$, and thus that $Cl(\mathcal{O}_{F(\lambda)}) \cong Cl^0_{F(\lambda)}$ and $Cl(\mathcal{O}_F) \cong Cl^0_F$.

Suppose $ord_T(P(T)) > 1$, meaning λ is unramified in $F(\lambda)/k(\lambda)$, and that there exists a degree-p unramified extension $K/F(\lambda)$ in which the prime above $1/\lambda$ splits completely. Then the subfield of K fixed by the decomposition group of (a prime above) $1/\lambda$ is a nontrivial extension of $k(\lambda)$ which is unramified everywhere and split completely at $1/\lambda$. But $k(\lambda)$ is genus 0, so such an extension must be trivial. Thus p does not divide $h_{F(\lambda)}$.

Now suppose that $ord_T(P(T)) = 1$. Then $ord_T(P(T) - \omega T) \geq 2$ for some $\omega \in \mathbb{F}_q^\times$. Let F_1 be the field generated by $x^q + Tx - (P(T) - \omega T)$ and F_2 by $x^q + Tx - T$. Then (similar to the proof of Theorem 5.1(3)), the compositum $F_1F_2(\lambda)$ is a degree-q unramified extension of $F(\lambda)$ in which the (unique) prime above $1/T$ splits completely. Therefore $q|h_{F(\lambda)}$.

Appealing to Theorem 3.1, this completes the proof of Theorem 5.8. □

Now, in the case that $q = p$, we can say a bit more about the structure of Cl^0_F, using a method similar to the proof of Theorem 5.1(1). We continue to assume that $1/T$ ramifies completely in $F(\lambda)/k$.

Suppose $I \in \mathcal{I}_{\mathcal{O}_{F(\lambda)}}$ such that $I^p \in P_{\mathcal{O}_{F(\lambda)}}$, and let σ be a generator for $G =$

$Gal(F(\lambda)/k(\lambda))$. Then for some $g \in \mathbb{Z}[G]$, we have $(\sigma-1)^{p-1}(I) = N(I)/g(I^p) \in P_{\mathcal{O}_{F(\lambda)}}$, i.e. $(\sigma-1)^{p-1}$ kills $Cl(\mathcal{O}_{F(\lambda)})[p]$. For $0 \leq k \leq p-2$, we have the following exact sequence, in which we denote $A = Cl(\mathcal{O}_{F(\lambda)})[p]$:

$$0 \to A[\sigma-1] \cap (\sigma-1)^k A \to (\sigma-1)^k A \xrightarrow{\sigma-1} (\sigma-1)^k A.$$

If the class of I is in $A[\sigma-1]$, then $\sigma(I)/I = (a)$ with $N(a) = \omega \in \mathcal{O}_{k(\lambda)}^{\times} = \mathbb{F}_p^{\times}$ (all units of $\mathcal{O}_{k(\lambda)}$ are constant by the S-unit theorem, since there is only one prime at infinity). By Hilbert's Theorem 90, $a/\omega = b/\sigma(b)$ for some $b \in F(\lambda)$, and so the class of I contains the fixed ideal $J = bI$. This means J is a product of (principal) ideals of $\mathcal{O}_{k(\lambda)}$ and primes of $\mathcal{O}_{F(\lambda)}$ above those which ramify in $F(\lambda)/k(\lambda)$. Consequently, $A[\sigma-1]$ is cyclic, and $dim_{\mathbb{F}_q}((\sigma-1)^k A/(\sigma-1)^{k+1}A) = dim_{\mathbb{F}_q}(A[\sigma-1] \cap (\sigma-1)^k A) \leq 1$ for each k. Since $(\sigma-1)^{p-1}A$ is trivial, this means A has rank at most $p-1$. (In fact, by Theorem 3.2, A must have rank exactly 0 or $p-1$.)

Because the prime above T is totally ramified in $F(\lambda)/F$, the map $Cl(\mathcal{O}_{F(\lambda)}) \to Cl(\mathcal{O}_F)$ induced by the norm is onto (see [23, Prop 2.2]). Therefore the rank of the p-Sylow subgroup of $Cl(\mathcal{O}_F) \cong Cl_F^0$ is at most $p-1$.

Chapter 6: Future Work

Some interesting questions remain, both about this family of fields and generalizations of it. We now explore some of these possible directions for future research and the accompanying challenges they present.

For one, do the class number relations of Theorems 3.1 and 4.3 extend to structural relations between class groups? For instance, if $F/\mathbb{F}_p(T)$ is a member of this family of fields and L is its normal closure, can we say in general that $Cl_L^0 = (Cl_F^0)^{p-1}$? By the discussion following the proof of Theorem 5.8, this relation would imply that the p-part of Cl_F^0 is always cyclic. Thus it may be possible to find a counterexample by determining the class group structure of various F with $p^2|h_F$.

An obvious generalization is to higher-rank Carlitz modules. In this work we only considered Λ_T and a root γ of $C(T)(x) - P(T) = x^q + Tx - P(T)$ as the analogues of roots of μ_p and $\sqrt[p]{n}$, respectively. This can certainly be expanded to instead consider Λ_M and a root of $C(M)(x) - P(T)$, for a general polynomial $M \in k$. Many of the techniques presented here can likely be applied to some extent (especially for M monic and irreducible, or a power of such, the cases which have been most studied in the cyclotomic function field literature). However, a significant obstacle is that while $k(\Lambda_T)$ has trivial class group (a property which is key to most

of our results), this is not true of $k(\Lambda_M)$ in general. Nonetheless, we expect our results to largely generalize, albeit to less simple statements.

Finally, the theory of cyclotomic function fields leads naturally to Iwasawa theoretic questions about towers of extensions. The extension $\cup_{i=1}^{\infty} k(\Lambda_{M^i})/k(\Lambda_M)$, for M monic and irreducible, can be seen as an analogue of the $\mathbb{Z}_p$-extension $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)$. The growth of the p-part of the class group in this tower, and congruence relations on the real and relative parts of the class group, have been studied [2,8]. But as in the number field case, $\cup_{i=1}^{\infty} k(\Lambda_{M^i})$ can be used to construct a 'cyclotomic $\mathbb{Z}_p$-extension'[1] of *any* function field over $\mathbb{F}_q(T)$. It would be interesting to study such towers over members of the family of fields we consider here, and we hope that the results of this work will be useful to that end.

[1] We remark that unlike in the number field case, the Galois group of such an extension is not in fact isomorphic to $\mathbb{Z}_p$, but rather to a countably infinite product of such groups.

Bibliography

[1] Emil Artin and John Torrence Tate. *Class field theory*, volume 366. American Mathematical Soc., 1968.

[2] Sunghan Bae and Pyung-Lyun Kang. Class numbers of cyclotomic function fields. *Acta Arithmetica*, 102:251–259, 2002.

[3] Pierre Barrucand and Harvey Cohn. Note on primes of type $x^2 + 32y^2$, class number, and residuacity. *Journal für die reine und angewandte Mathematik*, 1969(238):67–70, 1969.

[4] Leonard Carlitz. A class of polynomials. *Transactions of the American Mathematical Society*, 43(2):167–182, 1938.

[5] David A Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[6] CF Gauss. *Disquisitiones Arithmeticae*. 1801.

[7] David Goss. The arithmetic of function fields 2: the 'cyclotomic' theory. *Journal of Algebra*, 81(1):107–149, 1983.

[8] Li Guo and Linghsueh Shu. Class numbers of cyclotomic function fields. *Transactions of the American Mathematical Society*, 351(11):4445–4467, 1999.

[9] H Hasse. Über die kongruenzzetafunktionen. *Ber. Preuß. Akad. Wiss. H*, 17:250–263, 1934.

[10] Helmut Hasse. Theorie der relativ-zyklischen algebraischen funktionenkörper, insbesondere bei endlichem konstantenkörper. *Journal für die reine und angewandte Mathematik*, 1935(172):37–54, 1935.

[11] David R Hayes. Explicit class field theory for rational function fields. *Transactions of the American Mathematical Society*, 189:77–91, 1974.

[12] Gustav Herglotz. Über einen dirichletschen satz. *Mathematische Zeitschrift*, 12(1):255–261, 1922.

[13] David Hilbert. *The theory of algebraic number fields*. Springer Science & Business Media, 2013.

[14] Taira Honda. Pure cubic fields whose class numbers are multiples of three. *Journal of Number Theory*, 3(1):7–12, 1971.

[15] Angelo Iadarola. On the 8-rank of quadratic class groups.

[16] Norikata Nakagoshi. A note on l-class groups of certain algebraic number fields. *Journal of Number Theory*, 19(2):140–147, 1984.

[17] Kiichiro Ohta. On the p-class groups of relatively abelian number fields. *Bull. Fac. Gen. Ed. Gifu Univ.*, 23:21–23, 1987.

[18] Charles J Parry. Bicyclic bicubic fields. *Canadian Journal of Mathematics*, 42(3):491–507, 1990.

[19] László Rédei. Über die grundeinheit und die durch 8 teilbaren invarianten der absoluten klassengruppe im quadratischen zahlkörper. *Journal für die reine und angewandte Mathematik*, 1934(171):131–148, 1934.

[20] László Rédei and H Reichardt. Die anzahl der durch vier teilbaren invarianten der klassengruppe eines beliebigen quadratischen zahlkörpers. *Journal für die reine und angewandte Mathematik*, 1934(170):69–74, 1934.

[21] Hans Reichardt. Zur struktur der absoluten idealklassengruppe im quadratischen zahlkörper. *Journal für die reine und angewandte Mathematik*, 1934(170):75–82, 1934.

[22] Peter Roquette et al. Class field theory in characteristic p, its origin and development. In *Class field theory–Its centenary and prospect*, pages 549–631. Mathematical Society of Japan, 2001.

[23] Michael Rosen. The Hilbert class field in function fields. In *Exposition. Math*, volume 5, pages 365–378, 1987.

[24] Friedrich Karl Schmidt. Analytische zahlentheorie in körpern der charakteristik p. *Mathematische Zeitschrift*, 33(1):1–32, 1931.

[25] René Schoof. On the ideal class group of the normal closure of $\mathbf{Q}(\sqrt[n]{n})$. *Journal of Number Theory*, 216:69–82, 2020.

[26] Jean-Pierre Serre. Zeta and L functions. In *Arithmetical Algebraic Geometry, Proc. of a Conference held at Purdue Univ., Dec. 5-7, 1963*. Harper and Row, 1965.

[27] Dinesh S Thakur. Iwasawa theory and cyclotomic function fields. *CONTEMPORARY MATHEMATICS*, 174:157–157, 1994.