UNIVERSITY OF CALIFORNIA SAN DIEGO

Iwasawa theory of Taelman class modules

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Mathematics

by

Zachary Higgins

Committee in charge:

Professor Cristian Popescu, Chair
Professor Kiran Kedlaya
Professor Daniele Micciancio
Professor Claus Sorensen
Professor Hans Wenzl

2021

The dissertation of Zachary Higgins is approved, and it is acceptable in quality and form for publication on microfilm and electronically.

University of California San Diego

2021

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor Cristian Popescu for the endless guidance, encouragement, and insight he has provided in the past five years. Certainly none of this would have been possible without his advising. I would also like to thank Joe Ferrara and Nathan Green for all the helpful discussions we had while working together.

I am grateful to Kiran Kedlaya and Claus Sorensen for all that they have taught me during my time in graduate school and also for serving on my thesis committee. I am also grateful to Daniele Micciancio and Hans Wenzl for taking the time to serve on my thesis committttee.

While in San Diego, I have had to opportunity to meet many wonderful friends that have made my experience in graduate school an enjoyable one. There are too many to list by name, but you know who you are, and I appreciate all of you.

I would like to thank Haley for all love and support she has given me the last seven years and for being my companion in life. I look forward to all the good times still to come.

Finally, I would like to thank my parents, sister, and the rest of my family for all the support they have given me throughout my life, which has helped get me to where I am today.

Chapter 3 contains material from: J. Ferrara, N. Green, Z. Higgins, C. Popescu, *An equivariant Tamagawa number formula for Drinfeld modules and applications*, submitted

(2020). The dissertation author was one of the primary investigators and authors of this paper.

VITA

2015 B.S in Mathematics, University of Florida

2021 Ph.D. in Mathematics, University of California San Diego

PUBLICATIONS

J. Ferrara, N. Green, Z. Higgins, C. Popescu, *An equivariant Tamagawa number formula for Drinfeld modules*, submitted.

A. Godbole, Z. Higgins, Z. Koch, *Finite representability of integers as 2-sums*, Integers 18B, (2018), Paper No. A3, 12 pp.

D. Ehrmann, Z. Higgins, V. Nitica, *The geometric structure of max-plus hemispaces*, Linear Algebra Appl., 489, (2016), 144 - 166.

A. Godbole, Z. Higgins, E. Kelley, B. Sieben, *Universal and near-universal cycles of set partitions*, Electron. J. Combin. 22 (2015), no. 4, Paper 4.48, 15 pp.

ABSTRACT OF THE DISSERTATION

Iwasawa theory of Taelman class modules

by

Zachary Higgins

Doctor of Philosophy in Mathematics

University of California San Diego, 2021

Professor Cristian Popescu, Chair

In this dissertation, we study the Taelman class modules associated to a Drinfeld module in certain $\mathbb{Z}_p^{\aleph_0}$-towers of function fields. We show that the inverse limit of these class modules is finitely generated and torsion as a module over the Iwasawa algebra. Using the Equivariant Tamagawa Number Formula for Drinfeld modules [7], we then propose an Iwasawa main conjecture for these modules which would precisely describe the Fitting ideal of their inverse limit as a module over the Iwasawa algebra.

Chapter 1

Introduction

Iwasawa theory arose from the efforts of Kenkichi Iwasawa to transfer the ideas of the Weil conjectures from the setting of function fields to number fields. Broadly speaking, Iwasawa theory is the study of arithmetic objects (e.g. class groups, Selmer groups, etc.) in $\mathbb{Z}_p$-towers (or, more generally, $\mathbb{Z}_p^d$-towers for some $d \in \mathbb{Z}$) of number fields. One takes a limit of the arithmetic objects at finite levels to get a module at the infinite level over the Iwasawa algebra and tries to prove an Iwasawa main conjecture relating its Fitting ideal to a p-adic L-function.

In this thesis, we apply ideas of classical Iwasawa theory to a function field context to study a new type of "class module" recently defined by Lenny Taelman [17]. Let K be a function field, i.e. the field of rational functions on a smooth projective curve defined over a finite field $\mathbb{F}_q$, and let A be the ring of functions which are regular away from a fixed closed point ∞. Taelman defined a new "class module" $H(E/A)$ associated to any

Drinfeld module E defined over A. The definition of $H(E/A)$ arises from a function field analogue to (a reformulation of) the Dirichlet unit theorem for number fields. In the case where $A = \mathbb{F}_q[t]$, Taelman [18] proves a beautiful class number formula which states that the value at 0 of the L-function of the Drinfeld module is equal to the product of the unique monic generator of the Fitting ideal $\mathrm{Fitt}^0_A(H(E/A))$ of $H(E/A)$ with a "regulator" term. This was later generalized by the author with Ferrera, Green, and Popescu [7] to an Equivariant Tamagawa Number Formula (ETNF) for Drinfeld modules. In this case, if K/F is a finite abelian extension of function fields of Galois group G and E is a Drinfeld A-module (with $A = \mathbb{F}_q[t]$) defined over the integral closure O_F of A in F, then the value at 0 of the G-equivariant L-function associated to E is related to $\mathrm{Fitt}^0_{A[G]}(H(E/O_K))$ and a G-equivariant regulator term.

We will study the structure of these Taelman class groups in $\mathbb{Z}_p^{\aleph_0}$-towers $\mathcal{K}_\infty/K$ which are unramified at all finite primes. Let $\mathcal{K}_\infty/K$ be such an extension, set $\Gamma = \mathrm{Gal}(\mathcal{K}_\infty/K)$, and let $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$ be a sequence of finite Galois extensions of K with $\Gamma_n = \mathrm{Gal}(K_n/K)$ such that $\Gamma = \varprojlim \Gamma_n$. In each K_n, let O_{K_n} denote the integral closure of A. If $\mathfrak{p}$ is a prime of A, and $H(E/O_{K_n})_\mathfrak{p} := H(E/O_{K_n}) \otimes_A A_\mathfrak{p}$ the $\mathfrak{p}$-primary part of the A-module $H(E/O_{K_n})$, one can view $H_\infty^{(\mathfrak{p})} := \varprojlim H(E/O_{K_n})_\mathfrak{p}$ as a module over the Iwasawa algebra $A_\mathfrak{p}[[\Gamma]] := \varprojlim A_p[\Gamma_n]$. We will show that this module is finitely generated and torsion as an $A_\mathfrak{p}[[\Gamma]]$-module, and therefore its Fitting ideal $\mathrm{Fitt}^0_{A_\mathfrak{p}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$ exists and is nontrivial. In the case where $A = \mathbb{F}_q[t]$, we will use the ETNF for Drinfeld modules to state an Iwasawa main conjecture for $H_\infty^{(\mathfrak{p})}$ which describes $\mathrm{Fitt}^0_{A_\mathfrak{p}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$ precisely.

1.1 Structure of this dissertation

In Chapter 2, we will cover the background material - the basics of Drinfeld modules and their Taelman class modules - needed for the rest of the paper. In chapter 3, we briefly describe Taelman's class number formula to provide context for the ETNF. We then describe the algebraic constructions necessary to understand the ETNF before stating the main result. Finally, in Chapter 4, we define the relevant Iwasawa modules, prove that they are finitely generated and torsion over the Iwasawa algebra, and use the ETNF to state an Iwasawa main conjecture.

Chapter 2

Preliminaries

2.1 Drinfeld Modules

In this section, we will give a brief introduction to Drinfeld modules, only covering the notions needed for the rest of the paper. See [9] for a complete treatment of the basic properties of Drinfeld modules.

Let p be a prime, and let q be a power of p. Let K be the field of rational functions of a smooth projective curve C over $\mathbb{F}_q$. Fix a closed point $\infty \in C$, let d be the degree of ∞ over $\mathbb{F}_q$, and let v_∞ denote the ∞-adic valuation on K. Let $A \subseteq K$ denote the ring of functions which are regular away from ∞. An *A-field* is a field F with an $\mathbb{F}_q$-algebra morphism $\iota : A \to F$.

Let $F\{\tau\}$ denote the ring of skew polynomials in τ, with the relation

$$\tau a = a^q \tau$$

for all $a \in F$.

Definition 2.1.1. A *Drinfeld A-module over F* is an $\mathbb{F}_q$-algebra morphism $\varphi_E : A \to F\{\tau\}$ such that for all $a \in A$,

$$\varphi_E(a) = \iota(a)\tau^0 + \text{higher order terms.}$$

A Drinfeld module φ_E naturally gives rise to a functor

$$E : (F - \text{algebras}) \to (A - \text{modules})$$

where for any F-algebra M, the action of $a \in A$ on $E(M)$ is given by $\varphi_E(a)$, where τ acts as the q-power Frobenius.

Drinfeld modules (and their higher dimensional analogues) are central objects of study in function field arithmetic.

One can show (see Lemma 4.5.1 and Proposition 4.5.3 of [9]) that for any Drinfeld module φ, there is a positive integer r such that for any $a \in A$, we have

$$\deg_\tau(\varphi(a)) = -dv_\infty(a),$$

where $\deg_\tau(\varphi(a))$ is the degree of $\varphi(a)$ as a polynomial in τ, and $-dv_\infty(a)$ is the degree of the finite part of the divisor of a. This r is called the *rank* of φ.

For any Drinfeld module E, there is a unique power series $\exp_E \in F[[x]]$ - the *exponential function* associated to E - of the form

$$\exp_E = \sum_{i=0}^{\infty} e_i x^{q^i}$$

with $e_0 = 1$ such that $\exp_E(ax) = (\varphi_E(a))(\exp_E(x))$ for all $a \in A$. Let k_∞ denote the completion of k at ∞, and let $\mathbb{C}_\infty = \widehat{\overline{k_\infty}}$ denote the completion of the algebraic closure of k_∞. $\mathbb{C}_\infty$ is both algebraically closed and complete. The exponential function gives an analytic function $\exp_E : \mathbb{C}_\infty \to \mathbb{C}_\infty$ which is an open map and is surjective.

In general, it is not obvious how to construct Drinfeld modules. However, there is a theory for constructing Drinfeld modules via lattices due to Drinfeld (see [5] and [6]) that is analogous to the theory of elliptic curves over $\mathbb{C}$. An *A-lattice* is an A-submodule $\Lambda \subseteq \mathbb{C}_\infty$ of finite rank which is discrete in $\mathbb{C}_\infty$. Any such A-lattice Λ gives rise to an exponential function

$$\exp_L(x) = x \prod_{\alpha \in L \setminus \{0\}} \left(1 - \frac{x}{\alpha}\right).$$

Also, for each $a \in A$, one can define the polynomial

$$\varphi(a) = ax \prod_{0 \neq \alpha \in a^{-1}L/L} \left(1 - \frac{x}{\exp_\Lambda(\alpha)}\right).$$

One then checks that the polynomials $\varphi(a)$ are $\mathbb{F}_q$-linear and therefore are polynomials in x^q, so they can be viewed as elements of $\mathbb{C}_\infty\{\tau\}$

In this paper, we will restrict our attention to the case where $k = \mathbb{F}_q(t)$ and $A = \mathbb{F}_q[t]$. This is the setting originally considered by Taelman ([17] and [18]). The simplicity of the ring structure of $\mathbb{F}_q[t]$ allows us to prove precise class number formulas which exactly identify a special value of the L-function associated to a Drinfeld module. Recently, there has been an effort to extend the results we will discuss in this introduction to Drinfeld A-modules for more general A (see [1]). Unfortunately, when working with a more general A, the best "class number formula" one can hope for is an equality of A-submodules of k_∞ rather than an equality of elements in k_∞.

2.2 Taelman Class Modules

Let k be the field of rational function on a smooth projective curve X defined over $\mathbb{F}_q$, and let A be the ring of functions which are regular away from a fixed closed point ∞ of X. Let K be a finite separable extension of k, and let O_K denote the integral closure of A in K. Let $\varphi : A \to O_K\{\tau\}$ be a Drinfeld A-module defined over O_K. In [17], Taelman associates a "class module" to E in the following way. Let k_∞ denote the completion of k at ∞. Let $K_\infty = K \otimes_k k_\infty$ and let $K_\infty^{\mathrm{sep}} = K \otimes_k k_\infty^{\mathrm{sep}}$, where k_∞^{sep} is a separable closure of k_∞. Note that K_∞^{sep} is isomorphic to $[K : k]$ many copies of k_∞^{sep}. Hence, $\exp_E$ induces a surjective map $\exp_E : K_\infty^{\mathrm{sep}} \to K_\infty^{\mathrm{sep}}$. Let Λ_E denote the kernel of this map. Thus, we have an exact sequence

$$0 \longrightarrow \Lambda_E \longrightarrow K_\infty^{\mathrm{sep}} \xrightarrow{\exp_E} E(K_\infty^{\mathrm{sep}}) \longrightarrow 0. \tag{2.1}$$

Now, the absolute Galois group $G_{k_\infty} := \mathrm{Gal}(k_\infty^{\mathrm{sep}}/k_\infty)$ acts on K_∞^{sep} in the obvious way. Furthermore, the action of G_{k_∞} commutes with $\exp_E$ by the uniqueness of $\exp_E$. Hence, the sequence (2.1) is G_{k_∞} equivariant. Taking G_{k_∞} invariants gives the long exact sequence

$$0 \longrightarrow \Lambda_E^{G_{k_\infty}} \longrightarrow K_\infty \xrightarrow{\exp_E} E(K_\infty) \longrightarrow H^1(G_{k_\infty}, \Lambda_E) \longrightarrow H^1(G_{k_\infty}, K_\infty^{\mathrm{sep}}) = 0, \tag{2.2}$$

where $H^1(G_{k_\infty}, K_\infty^{\text{sep}}) = 0$ by the additive version of Hilbert's Theorem 90. Note that O_K sits inside K_∞ diagonally, and so there is a map $E(O_K) \to H^1(G_{k_\infty}, \Lambda_E)$.

Definition 2.2.1. The *Taelman class module* $H(E/O_K)$ of E over O_K is defined to be the cokernel of the map $E(O_K) \to H^1(G_{k_\infty}, \Lambda_E)$.

Remark. The terminology "Taelman" class module is not used in the literature. Most papers simply call it a "class module" or "class group".

Note that $H(E/O_K)$ is an A-module since (2.2) is an exact sequence of A-modules. It fits into an exact sequence of topological A-modules

$$0 \longrightarrow \frac{K_\infty}{\exp_E^{-1}(O_K)} \xrightarrow{\exp_E} \frac{E(K_\infty)}{E(O_K)} \longrightarrow H(E/O_K) \longrightarrow 0.$$

Theorem 2.2.2 (Theorem 1 of [17]). *The class module $H(E/O_K)$ is finite. The A-module $\exp_E^{-1}(E(O_K))$ is a discrete and co-compact A-submodule of K_∞.*

2.3 Fitting Ideals

Definition 2.3.1. Let R be a ring and let M be a finitely generated R-module. For any index set J, set $R^{(J)} := \bigoplus_{j\in J} R$. Let

$$R^{(J)} \xrightarrow{\varphi} R^n \longrightarrow M \longrightarrow 0$$

be a presentation of M. The *i-th Fitting ideal*, denoted $\text{Fitt}_R^i(M)$, is defined to be the ideal of R generated by all the $(n-i)\times(n-i)$ minors of the (possibly infinite) matrix for φ.

We will only deal with 0-th Fitting ideals in this paper, so we will refer to the 0-th Fitting ideal of M as *the* Fitting ideal of M, and we will denote it by $\mathrm{Fitt}_R(M)$.

One can show that this definition is independent of the choice of presentation (see Lemma 15.8.2 of [16]). We will use the following two properties of Fitting ideals throughout the paper (see Section 15.8 of [16] for more properties of Fitting ideals).

Proposition 2.3.2. *Let R, R' be rings, and let M_1, M_2 be finitely generated R-modules.*

1. *If $R \to R'$ is a ring morphism, then $\mathrm{Fitt}^i_{R'}(M \otimes_R R')$ is the ideal of R' generated by the image of $\mathrm{Fitt}^i_R(M)$*

2. *If $M_1 \to M_2$ is a surjective R-module morphism, then $\mathrm{Fitt}^i_R(M_1) \subseteq \mathrm{Fitt}^i_R(M_2)$.*

Proof. Part (1) follows from the fact that if

$$R^{(J)} \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

is a presentation of M as an R-module, then

$$R^{(J)} \otimes_R R' \longrightarrow (R^n) \otimes_R R' \longrightarrow M \otimes_R R' \longrightarrow 0$$

is a presentation of $M \otimes_R R'$ as an R'-module.

For part (2), if

$$R^{(J_1)} \longrightarrow R^n \longrightarrow M_1 \longrightarrow 0$$

is a presentation of M_1, then the compostion $R^n \to M_1 \to M_2$ is surjective, and there is a free module $R^{(J_2)}$ containing $R^{(J_1)}$ and a map $R^{(J_2)} \to R^n$ extending the map $R^{(J_1)} \to R^n$ such that

$$R^{(J_2)} \longrightarrow R^n \longrightarrow M_2 \longrightarrow 0$$

is a presentation of M_2. □

There is another equivalent definition of Fitting ideals that is often more convenient to use (see [15] for more details on this alternative definition). Suppose that

$$R^{(J)} \xrightarrow{\varphi} R^n \longrightarrow M \longrightarrow 0$$

is a presentation of the finitely generated R-module M. For any R-module N, let $N^* = \mathrm{Hom}_R(N, R)$ denote the dual of N. There is a natural evaluation map $\mathrm{ev}_N : N \otimes_R N^* \to R$ given by $\mathrm{ev}_N(x \otimes f) = f(x)$. To simplify notation, we will denote the evaluation map $\mathrm{ev}_{\bigwedge^{n-i} R^n} : \bigwedge^{n-i} R^n \otimes \left(\bigwedge^{n-i} R^n\right)^* \to R$ simply by ev_i. Now, there is an isomorphism

$$\bigwedge^{n-i}(R^n)^* \to \left(\bigwedge^{n-i} R^n\right)^*, \quad f_1 \wedge \cdots \wedge f_{n-i} \mapsto \psi_{f_1,\ldots,f_{n-i}}, \text{ where}$$

$$\psi_{f_1,\ldots,f_{n-i}}(x_1 \wedge \cdots \wedge x_{n-i}) = \det((f_i(x_j))_{i,j}) \text{ for any } x_1, \ldots, x_{n-i} \in R^n.$$

Then $\mathrm{Fitt}^i_R(M)$ is the image of the composition

$$\begin{array}{c} \bigwedge^{n-i} \bigoplus_{j\in J} R \otimes \bigwedge^{n-i}(R^n)^* \xrightarrow{(\wedge^{n-i}\varphi)\otimes 1} \bigwedge^{n-i} R^n \otimes \bigwedge^{n-i}(R^n)^* \xrightarrow{\sim} \bigwedge^{n-i} R^n \otimes \left(\bigwedge^{n-i} R^n\right)^* \\ \downarrow \mathrm{ev}_i \\ R \end{array}$$

which the reader can check is given by the mapping

$$a_1 \wedge \cdots \wedge a_{n-i} \otimes f_1 \wedge \cdots \wedge f_{n-i} \mapsto \det((f_k(\varphi(a_\ell)))_{k,\ell}).$$

In particular, the 0-th Fitting ideal is the image of the composition

$$\bigwedge^n R^{(J)} \xrightarrow{\wedge^n \varphi} \bigwedge^n R^n \xrightarrow{\det} R$$

where $\det : \bigwedge^n R^n \xrightarrow{\sim} R$ is the natural determinant map.

Chapter 3

The Equivariant Tamagawa Number Formula for Drinfeld Modules

3.1 Taelman's Class Number Formula

In this section, we will briefly describe Taelman's class number formula to help the reader understand the obstacles and workarounds involved in stating and proving the ETNF for Drinfeld modules, which is a G-equivariant version of the class number formula. The proofs for statements in this section can be found in [18].

Let $k = \mathbb{F}_q(t)$ and $A = \mathbb{F}_q[t]$. Fix a finite separable extension $K/\mathbb{F}_q(t)$ (with field of constants $\mathbb{F}_q$), and let O_K be the integral closure of A in K.

Definition 3.1.1. For a finitely generated A-module M, we define $|M|$ to be the unique monic generator of $\mathrm{Fitt}_A(M)$.

It is easy to show that for a finite abelian group G, viewed naturally as a $\mathbb{Z}$-module, we have $\mathrm{Fitt}_{\mathbb{Z}}(G) = n\mathbb{Z}$, where n is the cardinality of G. Thus, $|M|$ should be thought of as the "A-size" of an A-module M.

Let $\varphi_E : A \to O_K\{\tau\}$ be a Drinfeld module. The special value of the L-function associated to E that we will be interested in is given by

$$\Theta^E(0) = \prod_{v \in \mathrm{MSpec}(O_K)} \frac{|E(O_K/v)|}{|O_K/v|}.$$

We will postpone defining the actual L-function associated to E until Section 3.5, where we define the G-equivariant L-function associated to E. The classical, nonequivariant L-function can be obtained, of course, by letting G be trivial in the construction of the G equivariant L-function.

Definition 3.1.2. An *A-lattice* in K_∞ is a free A-submodule $\Lambda \subseteq K_\infty$ such that

$$\Lambda \otimes_A k_\infty = K_\infty.$$

Note that an A-lattice Λ must have A-rank equal to $\dim_{k_\infty}(K_\infty)$ and must therefore be discrete and cocompact inside K_∞ (since $A \subseteq k_\infty$ is discrete and cocompact).

Definition 3.1.3. Define the set of *monic elements* of $k_\infty = \mathbb{F}_q((t^{-1}))$ to be

$$\mathbb{F}_q((t^{-1}))^+ = \bigcup_{n \in \mathbb{Z}} t^{-n}(1 + t^{-1}\mathbb{F}_q[[t^{-1}]]).$$

In particular, a polynomial $f \in \mathbb{F}_q[t]$ is monic by the above definition if it is monic in the usual sense. Note that there is an obvious isomorphism

$$\mathbb{F}_q((t^{-1}))^\times \cong \mathbb{F}_q((t^{-1}))^+ \times \mathbb{F}_q^\times,$$

and each equivalence class of $\mathbb{F}_q((t^{-1}))^\times/\mathbb{F}_q^\times$ contains a unique monic element.

Definition 3.1.4. Let Λ_1, Λ_2 be two A-lattices in K_∞. Let $f : K_\infty \to K_\infty$ be a k_∞-linear transformation such that $f(\Lambda_1) = \Lambda_2$. Such an f can be constructed by choosing A-bases $\vec{e_1}$ and $\vec{e_2}$ for Λ_1 and Λ_2, respectively, which are therefore both k_∞-bases for K_∞ as well by the definition of A-lattice, and setting $f(\vec{e_1}) = \vec{e_2}$. We define the lattice index $[\Lambda_1 : \Lambda_2]$ to be the unique monic element in the coset $\det(f) \cdot \mathbb{F}_q^\times$.

Note that $[\Lambda_1 : \Lambda_2]$ is well-defined - if $g : K_\infty \to K_\infty$ is another k_∞-linear transformation such that $g(\Lambda_1) = \Lambda_2$, then $f^{-1} \circ g$ restricts to an A-linear automorphism of Λ_1, and therefore $\det(f^{-1} \circ g) \in A^\times = \mathbb{F}_q^\times$. It follows that $\det(f) \cdot \mathbb{F}_q^\times = \det(g) \cdot \mathbb{F}_q^\times$, so $[\Lambda_1 : \Lambda_2]$ is well-defined.

Recall that by Theorem 1 of [17] (Theorem 2.2.2 above), $H(E/O_K)$ is finite, so $|H(E/O_K)|$ is well-defined. Also by Theorem 1 of [17], $\exp_E^{-1}(O_K)$ is an A - lattice. Since O_K is clearly an A-lattice as well, $[O_K : \exp_E^{-1}(O_K)]$ is well defined. The following theorem is Taelman's class number formula.

Theorem 3.1.5 (Theorem 1 of [18])**.** *For any Drinfeld A-module defined over O_K, we have*

$$\Theta^E(0) = [O_K : \exp_E^{-1}(O_K)]|H(E/O_K)|.$$

Remark. Recall that we are restricting our attention here to the case where $k = \mathbb{F}_q(t)$ and $A = \mathbb{F}_q[t]$. Recently, Anglés, Dac, and Tavares-Ribeiro [1] extended this result to the case of Drinfeld A-modules with A the ring of functions in a function field k which are regular away from a fixed closed point ∞. Since A is not necessarily a PID (and even if it was there may be no canonical way to choose generators for principal ideals), they work with a special L-*lattice* (an A-lattice in k_∞ closely related to the corresponding L-function) and show that it is equal to $[O_K : \exp_E^{-1}(O_K)]_A \operatorname{Fitt}_A(H(E/O_K))$ (Corollary 5.9 of [1]), where $[O_K : \exp_E^{-1}(O_K)]_A$ is a suitable generalization of the lattice indices described above.

3.2 Setup

The purpose of the rest of this chapter is to introduce the algebraic constructions and state the main result of [7] since these will be used later in this thesis.

Let p be a prime, and let q be a power of p. Set $k = \mathbb{F}_q(t)$ and $A = \mathbb{F}_q[t]$. Let K, F be finite separable extensions of k, both with field of constants equal to $\mathbb{F}_q$, and assume K/F is abelian with Galois group G. Let O_F and O_K be the integral closures of A inside F and K, respectively. Let $\varphi_E : A \to O_F\{\tau\}$ be a Drinfeld A-module defined over O_F.

Our goal is to state an Equivariant Tamagawa Number Formula (ETNF) – a G-equivariant version of Taelman's class number formula – for the data above. We will not prove the formula; a proof can be found in [7]. First, we will show that one can reduce to the case where G is a p-group.

Lemma 3.2.1. *Let R be a Dedekind domain of characteristic p with field of fractions F. Let G be a finite abelian group, with $G = P \times \Delta$, where P is the Sylow-p subgroup of G and Δ its complement. Then there exists an $n \in \mathbb{Z}_+$ and finite extensions $R_1, \ldots, R_n$ of*

R such that

$$R[G] \cong \prod_{i=1}^{n} R_i[P].$$

Proof. Let

$$\widehat{\Delta}(F^{\text{sep}}) = \{\chi : \Delta \to (F^{\text{sep}})^{\times}\}$$

denote the set of F-valued characters of Δ. One can check that the irreducible idempotents of $F^{\text{sep}}[G]$ are given by

$$e_\psi = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \psi(\delta)\delta^{-1}$$

for $\psi \in \Delta$.

Now, the group $G_F = \text{Gal}(F^{\text{sep}}/F)$ acts naturally on $\widehat{\Delta}(F^{\text{sep}})$ by composition. Let

$$\widehat{\Delta}(R) = \widehat{\Delta}(F^{\text{sep}})/\sim$$

denote the equivalence classes of $\widehat{\Delta}(F^{\text{sep}})$ induced by the action of G_F. Then the irreducible idempotents of $R[G]$ are given by, for each $[\chi] \in \widehat{\Delta}(R)$,

$$e_{[\chi]} = \sum_{\psi \in [\chi]} e_\psi = \frac{1}{|\Delta|} \sum_{\psi \in [\chi], \delta \in \Delta} \psi(\delta)\delta^{-1}.$$

Thus, we obtain a decomposition

$$R[G] = \prod_{[\chi] \in \widehat{\Delta}(R)} e_{[\chi]} R[G] \cong \prod_{[\chi] \in \widehat{\Delta}(R)} R(\chi)[P],$$

where $R(\chi)$ is the smallest extension of R containing the values of χ, and $e_{[\chi]}R[G] \cong R(\chi)[P]$ by evaluating χ on the elements of Δ:

$$e_{[\chi]}R[G] \to R(\chi)[P]$$

$$e_{[\chi]} \sum_{\delta \in \Delta, \sigma \in P} a_{\delta\sigma} \delta\sigma \mapsto \sum_{\delta \in \Delta, \sigma \in P} a_{\delta\sigma} \chi(\delta)\sigma.$$

□

Note that when P is trivial, i.e. $p \nmid |G|$, we get the decompositions

$$\mathbb{F}_q[t][G] \cong \prod_{[\chi] \in \widehat{G}(\mathbb{F}_q)} \mathbb{F}_q(\chi)[t], \quad \mathbb{F}_q((t^{-1}))[G] \cong \prod_{[\chi] \in \widehat{G}(\mathbb{F}_q)} \mathbb{F}_q(\chi)((t^{-1}))$$

In particular, $\mathbb{F}_q[t][G]$ and $\mathbb{F}_q((t^{-1}))[G]$ are products of polynomial rings or Laurent series rings, respectively, over finite extensions of $\mathbb{F}_q$. By applying Taelman's class number formula on each of these character components, one can easily deduce a G-equivariant class number formula (assuming $p \nmid |G|$). This is done, for example, in [2] and in Section 1 of [7].

When $p||G|$, the same componentwise argument applies, so we only need to prove a G-equivariant formula for G a p-group. Thus, we will often be able to reduce to the case where G is a p-group.

3.3 Fitting Ideals

Let M be an $A[G]$-module. Our first goal is to identify a criterion for when $\mathrm{Fitt}_{A[G]}(M)$ is principal and, in such cases, identify a canonical generator of $\mathrm{Fitt}_{A[G]}(M)$. This is done via the following proposition, which is a simpler version of Proposition 4.1 of [10].

Proposition 3.3.1. *Let R be a local ring, and let M be an $R[t]$-module. Suppose that, as an R-module, M is free of rank n. Let $\{e_i\}$ be an R-basis for M and suppose that the* *action of t on M in the basis $\{e_i\}$ is given by the matrix $A_t \in M_n(R)$. Then $Fitt_{R[t]}(M)$ is principal and is generated by $|M|_{R[t]} := (det_{R[t]}(t \cdot I_n - A_t))$.*

Proof. It suffices to show that the sequence

$$R[t]^n \xrightarrow{\phi_t} R[t]^n \xrightarrow{\pi} M \longrightarrow 0.$$

is exact, where ϕ_t is the $R[t]$-module homomorphism which has matrix $t \cdot I_n - A_t$ in the standard bases on $R[t]^n$ and π is the projection which maps the standard basis of $R[t]^n$ to the R-module basis $\{e_i\}$ of M. Clearly, π is surjective and Im $\phi_t \subseteq \ker \pi$.

Now, let $\iota : R^n \to R[t]^n$ denote the canonical inclusion map. Note that $\pi \circ \iota : R^n \to M$ is an isomorphism of R-modules, so Im $\iota \cap \ker \pi = 0$. We claim that

$$\text{Im } \iota + \text{Im } \phi_t = R[t]^n.$$

This, along with the fact that Im $\phi_t \subseteq \ker \pi$ and Im $\iota \cap \ker \pi = 0$, will imply that Im $\phi_t = \ker \pi$. To prove this, for every $m \in \mathbb{Z}_+$, let $\phi_{t,m} : R[t]^n \to R[t]^n$ be the endomorphism whose matrix is $(t^m \cdot I_n - A_t^m)$ in the standard basis of $R[t]^n$. Note that Im $\phi_{t,m} \subseteq$ Im ϕ_t for all m since we can write $\phi_{t,m} = \phi_t \circ \alpha_{t,m}$, where $\alpha_{t,m}$ has matrix $(t^{m-1} \cdot I_n + t^{m-2} A_t + \cdots + A_t^{m-1})$ in the standard basis of $R[t]^n$. Since A_t^m has entries in R, this implies that $t^m \cdot f_i \in$ Im $\phi_t +$ Im ι for each standard basis vector f_i of $R[t]^n$. Since this holds for all m, it follows that $R[t]^n \subseteq$ Im $\phi_t +$ Im ι, as desired. □

Corollary 3.3.2. *Let $R = \prod_i R_i$ be a semi-local ring, and let M be an $R[t]$-module which is finitely generated and projective as an R-module. Then $Fitt_{R[t]}(M)$ is principal and is generated by $|M|_{R[t]} := \sum_i |M \otimes_R R_i|_{R_i[t]}$.*

Proof. By properties of Fitting ideals,

$$\mathrm{Fitt}_{R[t]}(M) = \bigoplus_i \mathrm{Fitt}_{R_i[t]}(M) = \bigoplus_i \mathrm{Fitt}_{R_i[t]}(M \otimes_R R_i)$$

Since each R_i is local, the projective R_i-module $M \otimes_R R_i$ is free and therefore $|M \otimes_R R_i|_{R_i[t]}$ is well-defined by Proposition 3.3.1. Hence, $\mathrm{Fitt}_{R[t]}(M)$ is generated by $\sum_i |M \otimes_R R_i|_{R_i[t]}$.

□

Now, in order to apply the above results to our situtation, we need to show that $\mathbb{F}_q[G]$ is semilocal and we need a useful criterion for determining when a module is $\mathbb{F}_q[G]$-projective.

Proposition 3.3.3. *Let P be a finite abelian p-group, and let R be a ring of characteristic p. Let I_P denote the augmentation ideal of $R[P]$, i.e. I_P is the kernel of the R-algebra morphism $s : R[P] \to R$ given by $s(\sigma) = 1$ for all $\sigma \in P$. Then there is a correspondence*

$$\mathrm{Spec}(R) \leftrightarrow \mathrm{Spec}(R[P])$$

$$\mathfrak{p} \leftrightarrow \mathfrak{p}_G := (\mathfrak{p}, I_P).$$

For any prime $\mathfrak{p}$ of R and any $R[P]$-module M, we have that $R_{\mathfrak{p}}[P] \cong R[P]_{\mathfrak{p}_G}$ and $M_{\mathfrak{p}_P} \cong M_{\mathfrak{p}}$.

Proof. For any $\sigma \in P$, since R has characteristic p and $|P|$ is a power of p, we have

$$(\sigma - 1)^{|P|} = \sigma^{|P|} - 1^{|P|} = 1 - 1 = 0.$$

Hence, the generators of I_P are all nilpotent, so it follows that I_P is contained in every prime ideal of $R[P]$. Since $R[P]/I_P \cong R$ via the augmentation map, the result follows.

Now, fix a prime $\mathfrak{p}$ of R, and let $\mathfrak{p}_P$ be the corresponding prime of $R[P]$. We have a map

$$f : R_{\mathfrak{p}}[P] \to R[P]_{\mathfrak{p}_P}$$
$$\sum_{\sigma \in P} \frac{a_\sigma}{b_\sigma}\sigma \mapsto \sum_{\sigma \in P} \frac{a_\sigma \sigma}{b_\sigma}.$$

To get a map in the other direction, suppose that $a = \sum_{\sigma \in P} a_\sigma \sigma \in R[P] \setminus \mathfrak{p}_P$. This means that $s_P(a) \notin \mathfrak{p}$, where $s_P : R[P] \to R$ is the augmentation map. By the result above, $R_{\mathfrak{p}}[P]$ is a local ring with maximal ideal $(\mathfrak{p}, P)$, and therefore

$$R_{\mathfrak{p}}[P]^\times = \{x \in R_{\mathfrak{p}}[P] | s_P(x) \notin \mathfrak{p}\}.$$

Thus, $a \in R_{\mathfrak{p}}[P]^\times$, and it follows that the map

$$g : R[P]_{\mathfrak{p}_P} \to R_{\mathfrak{p}}[P]$$
$$\frac{a}{b} \mapsto ab^{-1}$$

is well-defined. One can check that g and f are inverses. A similar argument shows that $M_{\mathfrak{p}_P} \cong M_{\mathfrak{p}}$. □

Thus, if R is a Dedekind domain of characteristic p and G is a finite abelian group such that $G = P \times \Delta$ where P is the Sylow p-subgroup of G, then by Lemma 3.2.1 we have a decomposition

$$R[G] = \prod_{[\chi] \in \widehat{\Delta}(R)} e_{[\chi]} R[G] \cong \prod_{[\chi] \in \widehat{\Delta}(R)} R(\chi)[P],$$

and by Proposition 3.3.3 each of the $R(\chi)[P]$ are local rings. Hence, $R[G]$ is semilocal.

We can now give a nice characterization of projective modules over the the group rings we will be working with. Recall that for a G-module M, $\widehat{H}^i(G, M)$ denotes the i-th Tate cohomology group of M, for any $i \in \mathbb{Z}$. We say that a G-module M is *G-cohomologically trivial*, abbreviated G-c.t., if $\widehat{H}^i(H, M) = 0$ for all $i \in \mathbb{Z}$ and all subgroups H of G.

Proposition 3.3.4. *Let R be a Dedekind domain of characteristic p, let G be a finite abelian p-group, and let M be a finitely generated $R[G]$-module. Then M is $R[G]$-projective if and only if M is R-projective and G-cohomologically trivial.*

Proof. First, note that if R is a DVR with uniformizer π, then the proposition follows by replacing $\mathbb{Z}, p$, and $\mathbb{F}_p$ with R, π, and R/π, respectively, in Theorems IV.6, IV.7, and IV.8 of [4].

Now, suppose R is a Dedekind domain. If M is $R[G]$-projective, then by viewing M as a direct summand of a free $R[G]$-module, we see that M is R-projective and G-c.t. Now, suppose that M is R-projective and G-c.t. By Proposition 3.3.3, the maximal ideals of $R[G]$ are of the form $\mathfrak{m}_G = (\mathfrak{m}, I_G)$ where $\mathfrak{m}$ is a maximal ideal of R. We have that M is $R[G]$-projective if and only if $M_{\mathfrak{m}_G} = M_{\mathfrak{m}}$ is projective as an $R_{\mathfrak{m}_G} = R_{\mathfrak{m}}[G]$-module (the equalities are by Proposition 3.3.3) for each maximal ideal $\mathfrak{m}$ of R. Since each $R_{\mathfrak{m}}$ is a DVR, this occurs if and only if $M_{\mathfrak{m}}$ is $R_{\mathfrak{m}}$-projective and G-c.t. for each $\mathfrak{m} \in \mathrm{MSpec}(R)$. Finally, note that M is G-c.t. if and only if $M_{\mathfrak{m}}$ is G-c.t. for all $\mathfrak{m} \in \mathrm{MSpec}(R)$ since $\widehat{H}^i(H, \mathcal{M})_{\mathfrak{m}} \cong \widehat{H}^i(H, \mathcal{M}_m)$ for any subgroup $H \leq G$ and any $i \in \mathbb{Z}$ (since localizing at $\mathfrak{m}$ a projective resolution of M gives a projective resolution of $\mathcal{M}_{\mathfrak{m}}$). This proves the proposition. $\square$

Hence, if M is a finitely generated $\mathbb{F}_q[t][G]$-module which is G-cohomologically trivial, then M is $\mathbb{F}_q[G]$-projective by Proposition 3.3.4, and therefore $\mathrm{Fitt}_{\mathbb{F}_q[G][t]}(M)$ is principal by Corollary 3.3.2 (which applies since $\mathbb{F}_q[G]$ is semilocal by Lemma 3.2.1 and Proposition 3.3.3).

Recall that we have the decomposition

$$\mathbb{F}_q[t][G] \cong \prod_{[\chi]\in\widehat{G}(\mathbb{F}_q)} \mathbb{F}_q(\chi)[P][t],$$

of the group ring $\mathbb{F}_q[t][G]$ given by Lemma 3.2.1. We will say that an element $f \in \mathbb{F}_q[t][G]$ is *monic* if its image under the projection $\mathbb{F}_q[t][G] \to \mathbb{F}_q(\chi)[P][t]$ arising from the decomposition above is a monic polynomial (in the usual sense) for each $[\chi] \in \widehat{G}(\mathbb{F}_q)$. Note that if M is a finite G-c.t. $\mathbb{F}_q[t][G]$-module, then the generator $|M|_{\mathbb{F}_q[t][G]}$ given by Corollary 3.3.2 is monic.

Definition 3.3.5. For a finitely generated $\mathbb{F}_q[t][G]$-module M which is G-cohomologically trivial, we define $|M|_G$ to be the unique monic generator of $\mathrm{Fitt}_{\mathbb{F}_q[G][t]}(M)$ given by Corollary 3.3.2.

We will also need the following result later:

Proposition 3.3.6. *Let R be a local ring, and let M_1, M_2, M_3 be $R[t]$-modules which are finitely generated and free as R-modules, and which fit into an exact sequence*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0.$$

Then

$$|M_2|_G = |M_1|_G \cdot |M_3|_G.$$

Proof. Since $M_2 \cong M_1 \oplus M_3$ as R-modules, we can find and R-basis $\vec{e_1}$ for M_1, which extends to an R-basis $\vec{e_2}$ of M_2, which projects to an R-basis $\vec{e_3}$ of M_3. If we let $A_{1,t}, A_{2,t}, A_{3,t}$ denote the matrices of the action of t on M_1, M_2, M_3 in the bases $\vec{e_1}, \vec{e_2}, \vec{e_3}$, respectively, then

$$A_{2,t} = \begin{pmatrix} A_{1,t} & * \\ 0 & A_{3,t} \end{pmatrix}.$$

The result now follows from Proposition 3.3.1. □

3.4 Lattice Indices

Definition 3.4.1. Let $\Lambda \subseteq K_\infty$ be an A-lattice (see definition 3.1.2). We say that Λ is an $A[G]$*-lattice* if Λ is an $A[G]$-submodule of K_∞. We say that Λ is a *projective* $A[G]$*-lattice* or *free* $A[G]$*-lattice* if Λ is projective or free, respectively, as an $A[G]$-module.

As in Chapter 2, in order to define lattice indices, we will need to select a canonical representative of each coset of $\mathbb{F}_q((t^{-1}))[G]^\times / \mathbb{F}_q[t][G]^\times$.

Definition 3.4.2. For a finite abelian p-group P, we define the set of *monic elements* in $\mathbb{F}_q((t^{-1}))[P]^\times$ to be

$$\mathbb{F}_q((t^{-1})[P]^+ := \bigcup_{n\in\mathbb{Z}} t^{-n}\left(1 + \mathbb{F}_q[P][[t^{-1}]]\right).$$

In other words, an element of $\mathbb{F}_q((t^{-1}))[P]$ is monic if when expressed as a Laurent series with coefficients in $\mathbb{F}_q[P]$ the coefficient of the smallest power of t^{-1} with nonzero coefficient is one. In particular, the monic elements of $\mathbb{F}_q[t][P]$ are precisely the elements which are monic in the usual sense.

To define *monic* for a general finite abelian group $G = P \times \Delta$ (with P the Sylow p-subgroup of G), we will use the isomorphism

$$\psi : \mathbb{F}_q((t^{-1}))[G] \cong \prod_{[\chi] \in \widehat{G}(\mathbb{F}_q)} \mathbb{F}_q(\chi)[P]((t^{-1}))$$

of Lemma 3.2.1.

Definition 3.4.3. We define the *monic elements* in $\mathbb{F}_q((t^{-1}))[G]^\times$ to be

$$\mathbb{F}_q((t^{-1}))[G]^+ := \bigoplus_{[\chi] \in \widehat{\Delta}(\mathbb{F}_q)} \psi^{-1}(\mathbb{F}_q((t^{-1}))[P]^\times)$$

Note that this definition of monic is compatible with our definition of the monic elements in the ring $\mathbb{F}_q[t][G]$ from just after Proposition 3.3.4.

It turns out that each coset of $\mathbb{F}_q((t^{-1}))[G]^\times / \mathbb{F}_q[t][G]^\times$ contains a unique monic representative. The key theorem for showing this is the Weierstrauss Preparation Theorem. The statement and proof can be found in Theorem 5.2.2 of [14].

Theorem 3.4.4 (Weierstrauss Preparation Theorem)**.** *Let $\mathcal{O}$ be a complete local ring with maximal ideal $\mathfrak{m}$. Let*

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

be a power series in $\mathcal{O}[[x]]$ *such that not all* a_i *lie in* $\mathfrak{m}$*, say* $a_0, \ldots, a_{n-1} \in \mathfrak{m}$ *and* $a_n \in \mathcal{O}^\times$ *for some* $n \in Z$*. Then* f *can be uniquely written in the form*

$$f(x) = (x^n + b_{n-1}x^{n-1} + \cdots + b_0)u$$

with each $b_i \in \mathfrak{m}$*, and* $u \in \mathcal{O}[[x]]^\times$*.*

Proposition 3.4.5. *Let* G *be a finite abelian* p*-group. Then* $\mathbb{F}_q((t^{-1}))[G]^\times$ *has a decomposition*

$$\mathbb{F}_q((t^{-1}))[G]^\times \cong \mathbb{F}_q((t^{-1}))[G]^+ \times \mathbb{F}_q[t][G]^\times.$$

Proof. Let $f = \sum_{i \geq n} a_i t^{-i} \in \mathbb{F}_q((t^{-1}))[G]^\times$, and let $s : \mathbb{F}_q((t^{-1}))[G] \to \mathbb{F}_q((t^{-1}))$ denote the augmentation map. Note that by Proposition 3.3.3, $\mathbb{F}_q[G]$ is complete local ring since its maximal ideal I_G is nilpotent. By Proposition 3.3.3 again, since f is a unit in $\mathbb{F}_q((t^{-1}))[G]$, we have that $s(f) \neq 0$, so there is a minimal $m \in \mathbb{Z}$ such that $s(a_m) \neq 0$, i.e. $a_m \notin I_G$. Hence, by the Weierstrauss Preparation Theorem (applied to $t^n f \in \mathbb{F}_q[G][[t^{-1}]]$), we may write

$$t^n f = (t^{-m} + b_{m-1}t^{-m+1} + \cdots + b_0)u$$

with each $b_i \in I_G$ and $u \in \mathbb{F}_q[[t^{-1}]][G]^\times$. If u_0 is the constant term of u, then $u_0^{-1}t^{-n-m}u \in \mathbb{F}_q((t^{-1}))[G]^+$, and $u_0(1+b_{m-1}t+\cdots+b_0t^m) \in \mathbb{F}_q[t][G]^\times$ since $u_0 b_i \in I_G$ for $i = 0, 1, \ldots, m-1$, while the constant term is $u_0 \notin I_G$ (since $u \in \mathbb{F}_q[[t^{-1}]][G]^\times$). Hence,

$$f = (u_0^{-1}t^{-n-m}u)(u_0(1 + b_{m-1}t + \cdots + b_0t^m))$$

expresses f as a product of an element of $\mathbb{F}_q((t^{-1}))[G]^+$ and an element of $\mathbb{F}_q[t][G]^\times$. Finally, this decomposition is unique since $\mathbb{F}_q((t^{-1}))[G]^+ \cap \mathbb{F}_q[t][G]^\times = \{1\}$. □

We can use Proposition 3.4.5 to define G-equivariant lattice indices. Let $\mathcal{F}_1, \mathcal{F}_2 \subseteq K_\infty$ be two free $A[G]$-lattices. Let $\vec{e_1}, \vec{e_2}$ be $A[G]$-bases of $\mathcal{F}_1, \mathcal{F}_2$, respectively. Since $k_\infty \mathcal{F}_1 = k_\infty \mathcal{F}_2 = K_\infty$, these are $k_\infty[G]$-bases for K_∞ as well. Let $X : K_\infty \to K_\infty$ be a linear transformation which maps $\vec{e_1}$ to $\vec{e_2}$.

Definition 3.4.6. We define

$$[\mathcal{F}_1 : \mathcal{F}_2]_G = \det(X)^+,$$

where $\det(X)^+$ is the image of $\det(X)^+$ under the isomorphism

$$\mathbb{F}_q((t^{-1}))[G]^\times / \mathbb{F}_q[t][G]^\times \cong \mathbb{F}_q((t^{-1}))[G]^+$$

of Proposition 3.4.5.

Note that although $\det(X)$ depends on the choice of $A[G]$-bases for $\mathcal{F}_1, \mathcal{F}_2$, $\det(X)^+$ does not since changing the choice of bases will change $\det(X)$ by an element of $\mathbb{F}_q[t][G]^\times$.

Proposition 3.4.7. *Let $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3 \subseteq K_\infty$ be free $A[G]$-lattices.*

1. $[\mathcal{F}_1 : \mathcal{F}_2][\mathcal{F}_2 : \mathcal{F}_3] = [\mathcal{F}_1 : \mathcal{F}_3]$.

2. *If $\mathcal{F}_1 \subseteq \mathcal{F}_2$, then* $[\mathcal{F}_2 : \mathcal{F}_1] = |\mathcal{F}_2/\mathcal{F}_1|_G$.

Proof. Part (1) follows from the fact that determinant and the isomorphism of Proposition 3.4.5 are both homomorphisms.

For Part (2), note that $\mathcal{F}_2/\mathcal{F}_1$ is finite since $\mathcal{F}_1, \mathcal{F}_2$ are free A-modules of the same rank, and it is G-c.t. since both $\mathcal{F}_1$ and $\mathcal{F}_2$ are. Now,

$$0 \longrightarrow \mathcal{F}_1 \longrightarrow \mathcal{F}_2 \longrightarrow \mathcal{F}_2/\mathcal{F}_1 \longrightarrow 0$$

is a presentation of $\mathcal{F}_2/\mathcal{F}_1$ by free $A[G]$-modules. Fixing $A[G]$-bases $\vec{e_1}$ and $\vec{e_2}$ of $\mathcal{F}_1$ and $\mathcal{F}_2$, respectively, we can see that the linear transformation $X : K_\infty \to K_\infty$ which maps $\vec{e_2}$ to $\vec{e_1}$ has the same matrix in the basis $\vec{e_2}$ as the map $\mathcal{F}_1 \to \mathcal{F}_2$ above (with respect to the bases $\vec{e_1}$ and $\vec{e_2}$). Thus, $\det(X)$ generates $\mathrm{Fitt}_{A[G]}(\mathcal{F}_2/\mathcal{F}_1)$. Since $[\mathcal{F}_2 : \mathcal{F}_1]$ is defined to be the unique monic (in the sense of definition 3.4.2) element of $\det(X) \cdot A[G]^\times$, and $|\mathcal{F}_2/\mathcal{F}_1|_G$ is defined to be the unique monic generator of $\mathrm{Fitt}_{A[G]}(\mathcal{F}_2/\mathcal{F}_1)$, it follows that the two are equal. $\square$

We will also need to be able to take lattice indices for projective $A[G]$-lattices. This is done using the following proposition.

Proposition 3.4.8. *Let $\Lambda \subseteq K_\infty$ be a projective $A[G]$-lattice. Then there is a free $A[G]$ lattice $\mathcal{F} \subseteq K_\infty$ such that $\Lambda \subseteq \mathcal{F}$. Also, $\mathcal{F}/\Lambda$ is a finite $A[G]$-module which is projective as an $\mathbb{F}_q[G]$-module.*

Proof. Since $k_\infty \Lambda = K_\infty$, we may choose a $k_\infty[G]$-basis $\{e_1, \ldots, e_n\}$ for $K_\infty[G]$ such that $\{e_1, \ldots, e_n\} \subseteq \Lambda$. The free $A[G]$-lattice Λ' of basis $\{e_1, \ldots, e_n\}$ sits inside Λ with finite index. If $f \in A$ annihilates Λ/Λ', then $\mathbb{F} := \bigoplus_{i=1}^{n} A[G]\frac{e_i}{f}$ is a free $A[G]$-lattice containing Λ.

Finally, $\mathcal{F}/\Lambda$ is finite since they are both free A-modules of the same rank, and $\mathcal{F}/\Lambda$ is G-c.t. since both $\mathcal{F}$ and Λ are, and it is therefore $\mathbb{F}_q[G]$-projective by Proposition

3.3.4. $\square$

Thus, for $\Lambda \subseteq \mathcal{F}$ as above, it makes sense to consider $|\mathcal{F}/\Lambda|_G$ by Proposition 3.3.1.

Definition 3.4.9. Let $\Lambda_1, \Lambda_2 \subseteq K_\infty$ be projective $A[G]$ lattices. Choose free $A[G]$ lattices $\mathcal{F}_1, \mathcal{F}_2$ such that $\Lambda_i \subseteq \mathcal{F}_i$ for $i = 1, 2$. We define

$$[\Lambda_1 : \Lambda_2]_G = [\mathcal{F}_1 : \mathcal{F}_2]_G \frac{|\mathcal{F}_1/\Lambda_1|_G}{|\mathcal{F}_2/\Lambda_2|_G}$$

Proposition 3.4.10. *With all notation as above, $[\Lambda_1 : \Lambda_2]_G$ is independent of the choice of free $A[G]$-lattices $\mathcal{F}_1 \supseteq \Lambda_1$ and $\mathcal{F}_2 \supseteq \Lambda_2$.*

Proof. Let $\mathcal{F}_1, \mathcal{F}_1'$ be free $A[G]$-lattices containing Λ_1 and let $\mathcal{F}_1, \mathcal{F}_2'$ be free $A[G]$-lattices containing Λ_2. Since $\mathcal{F}_1$ and $\mathcal{F}_1'$ both contain Λ_1, we see that $\mathbb{F}_q(t)\mathcal{F}_1 = \mathbb{F}_q(t)\mathcal{F}_1'$, and therefore we can choose a free $A[G]$-lattice $\mathcal{F}_1''$ containing both $\mathcal{F}_1$ and $\mathcal{F}_1'$. Similarly we may choose a free $A[G]$-lattice $\mathcal{F}_2''$ containing both $\mathcal{F}_2$ and $\mathcal{F}_2'$. Then

$$\begin{aligned}
[\mathcal{F}_1 : \mathcal{F}_2]_G \frac{|\mathcal{F}_1/\Lambda_1|_G}{|\mathcal{F}_2/\Lambda_2|_G} &= [\mathcal{F}_1 : \mathcal{F}_2]_G \frac{|\mathcal{F}_1''/\Lambda_1|_G}{|\mathcal{F}_1''/\mathcal{F}_1|_G} \frac{|\mathcal{F}_2''/\mathcal{F}_2|_G}{|\mathcal{F}_2''/\Lambda_2|_G} && \text{by Proposition 3.3.6} \\
&= [\mathcal{F}_1 : \mathcal{F}_2]_G [\mathcal{F}_2 : \mathcal{F}_2'']_G [\mathcal{F}_1'' : \mathcal{F}_1]_G \frac{|\mathcal{F}_1''/\Lambda_1|_G}{|\mathcal{F}_2''/\Lambda_2|_G} && \text{by Proposition 3.4.7} \\
&= [\mathcal{F}_1'' : \mathcal{F}_2'']_G \frac{|\mathcal{F}_1''/\Lambda_1|_G}{|\mathcal{F}_2''/\Lambda_2|_G} && \text{by Proposition 3.4.7.}
\end{aligned}$$

The same argument shows that

$$[\mathcal{F}_1' : \mathcal{F}_2']_G \frac{|\mathcal{F}_1'/\Lambda_1|_G}{|\mathcal{F}_2'/\Lambda_2|_G} = [\mathcal{F}_1'' : \mathcal{F}_2'']_G \frac{|\mathcal{F}_1''/\Lambda_1|_G}{|\mathcal{F}_2''/\Lambda_2|_G}$$

as well. $\square$

Proposition 3.4.11. *Given projective $A[G]$-lattices $\Lambda_1, \Lambda_2, \Lambda_3$, we have*

1. $[\Lambda_1 : \Lambda_2]_G[\Lambda_2 : \Lambda_3]_G = [\Lambda_1 : \Lambda_3]_G$.

2. If $\Lambda_1 \subseteq \Lambda_2$, *then* $[\Lambda_2 : \Lambda_1]_G = |\Lambda_2/\Lambda_1|_G$.

Proof. Let $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ be free $A[G]$-lattices containing Λ_1, Λ_2, and Λ_3, respectively. Then

$$\begin{aligned}[\Lambda_1 : \Lambda_2]_G[\Lambda_2 : \Lambda_3]_G &= [\mathcal{F}_1 : \mathcal{F}_2]_G \frac{|\mathcal{F}_1/\Lambda_1|_G}{|\mathcal{F}_2/\Lambda_2|_G}[\mathcal{F}_2 : \mathcal{F}_3]_G \frac{|\mathcal{F}_2/\Lambda_2|_G}{|\mathcal{F}_3/\Lambda_3|_G} \\ &= [\mathcal{F}_1 : \mathcal{F}_3]_G \frac{|\mathcal{F}_1/\Lambda_1|_G}{|\mathcal{F}_3/\Lambda_3|_G} \\ &= [\Lambda_1 : \Lambda_3]_G.\end{aligned}$$

If $\Lambda_1 \subseteq \Lambda_2$, then we may choose a single free $A[G]$-lattice $\mathcal{F}$ containing both Λ_1 and Λ_2 so that

$$[\Lambda_2 : \Lambda_1]_G = [\mathcal{F} : \mathcal{F}]_G \frac{|\mathcal{F}/\Lambda_2|_G}{|\mathcal{F}/\Lambda_1|_G} = \frac{|\mathcal{F}/\Lambda_2|_G}{|\mathcal{F}/\Lambda_1|_G} = |\Lambda_2/\Lambda_1|_G,$$

where the last equality follows from Proposition 3.3.6 □

3.5 The Equivariant L-Function

We now construct the equivariant L-function associated to the data $(K/F, E)$. Fix a prime v_0 of A, and let f_0 denote the unique monic generator of v_0. For each $n \in \mathbb{Z}_+$, we let $E[v_0^n] \subset K^{\text{sep}}$ denote the v_0^n torsion points of E. In other words, $E[v_0^n]$ consists precisely of the roots of the polynomial $\varphi_E(f_0^n)$. Of course, for an $n \geq m$ we have a map $E[v_0^n] \to E[v_0^m]$ given by the action of $\varphi_E(f_0^{n-m})$, and therefore we can consider the

v_0-adic Tate module

$$T_{v_0}(E) = \varprojlim_n E[v_0^n].$$

Let r be the rank of E. Then $E[v_0^n] \cong (A/v_0^n)^r$ as A-modules (see, for example, Proposition 4.5.3 of [9]), so we see that $T_{v_0}(E) \cong A_{v_0}^r$.

Note that the absolute Galois group $G_F := \mathrm{Gal}(F^{\mathrm{sep}}/F)$ acts naturally on $T_{v_0}(E)$. Let v be a prime of O_F not dividing v_0, let $\tilde{I}_v \subseteq G_F$ denote an inertia group for v, and let $\tilde{\sigma}_v \in G_F$ be a Frobenius for v. If E has good reduction at v, then $T_{v_0}(E)$ is unramified at v by a result of Gekeler [8], so we may consider the polynomial

$$P_v(X) := \det_{A_{v_0}}(X \cdot I_r - \tilde{\sigma}_v | T_{v_0}(E)).$$

Gekeler also shows that $P_v(X)$ is independent of choice of v_0 and has coefficients in A (Corollary 3.4 of [8]).

Now, let

$$H^1_{v_0}(E) := T_{v_0}(E)^* = \mathrm{Hom}_{A_{v_0}}(T_{v_0}(E), A_{v_0}).$$

$H^1_{v_0}(E)$ has a natural G_F action: for $\varphi \in H^1_{v_0}(E)$ and $g \in G_F$,

$$(g \cdot \varphi)(x) = \varphi(g^{-1}x).$$

To get a G-equivariant version of $H^1_{v_0}(E)$, we take

$$H^1_{v_0}(E, G) = H^1_{v_0}(E) \otimes_{A_{v_0}} A_{v_0}[G],$$

endowed with the diagonal G_F action, where G_F acts on $A_{v_0}[G]$ via the projection $G_F \twoheadrightarrow G$. Of course, $H^1_{v_0}(E, G) \cong A_{v_0}[G]^r$ as an $A_{v_0}[G]$-module.

We would like to define a G-equivariant analog of $P_v(X)$ for as many primes $v \in \mathrm{Spec}(O_F)$ as possible.

Proposition 3.5.1. *Let $v \in \mathrm{Spec}(O_F)$ be a prime at which E has good reduction, and which is at most tamely ramified in K/F. Let $v_0 \in \mathrm{Spec}(A)$ such that $v \nmid v_0$. Then $H^1_{v_0}(E,G)^{\widetilde{I}_v}$ is a finitely generated projective $A_{v_0}[G]$ module, so we may consider the polynomial*

$$P_v^{*,G}(X) = det_{A_{v_0}[G]}(X - \widetilde{\sigma}_v | H^1_{v_0}(E,G)^{\widetilde{I}_v}).$$

Then

$$P_v^{*,G}(X) = \frac{X^r \cdot P_v(\sigma_v \mathbf{e}_v \cdot X^{-1})}{P_v(0)},$$

where $\mathbf{e}_v = \frac{1}{|I_v|}\sum_{\sigma \in I_v} \sigma$, $P_v^{*,G}(X)$ is independent of v_0, and $Nv \cdot P_v^{*,G}(X) \in A[G][X]$, where Nv is the monic generator of the ideal norm of v down to A.

Proof. Note that $H^1_{v_0}(E,G)^{\tilde{I}_v} = \mathbf{e}_v H^1_{v_0}(E,G)$. Hence, $H^1_{v_0}(E,G)^{\widetilde{I}_v}$ is a finitely generated projective $A_{v_0}[G]$-module since it is a direct summand of the finitely generated free $A_{v_0}[G]$-module $H^1_{v_0}(E,G) = \mathbf{e}_v H^1_{v_0}(E,G) \oplus (1-\mathbf{e}_v)H^1_{v_0}(E,G)$.

Now, let $e_1, \dots e_r$ be an A_{v_0}-basis for $T_{v_0}(E)$, and let $\hat{e}_1, \dots, \hat{e}_r$ be the dual basis of $T_{v_0}(E)^*$. Let M be the matrix for the action of $\widetilde{\sigma}_v$ in the basis $e_1, \dots, e_r$. Then the matrix for the action of $\widetilde{\sigma}_v$ on $T_{v_0}(E)^*$ in the basis $\hat{e}_1, \dots, \hat{e}_r$ is $(M^T)^{-1}$, and therefore the matrix for the action of $\widetilde{\sigma}_v$ on $H^1_{v_0}(E,G)^{\widetilde{I}_v}$ in the $A_{v_0}[G]$-basis $\hat{e}_1 \otimes \mathbf{e_v}, \dots, \hat{e}_r \otimes \mathbf{e_v}$ is $\sigma_v \mathbf{e}_v (M^T)^{-1}$.

Thus,

$$P_v^{*,G}(X) = \det(X - \sigma_v \mathbf{e}_v (M^T)^{-1}) = \det(X - \sigma_v \mathbf{e}_v M^{-1})$$
$$= X^r \det(-M^{-1}) \det(\sigma_v \mathbf{e}_v X^{-1} - M)$$
$$= \frac{X^r \cdot P_v(\sigma_v \mathbf{e}_v X^{-1})}{P_v(0)}.$$

Now, the fact that $P_v^{*,G}(X)$ is independent of v_0 follows from the formula above in terms of P_v and the fact that P_v is independent of v_0. Finally, $Nv \cdot P_v^{*,G}(X) \in A[G][X]$ by Theorem 5.1.(ii) of [8], which says that Nv and $P_v(0)$ generate the same ideal in A. □

In order to define the equivariant L-function, we need a short digression to describe *Goss's space* $\mathbb{C}_\infty^\times \times \mathbb{Z}_p$, a subset of which will be the domain of the L-function.

Definition 3.5.2. Let L be a local field of characteristic p with field of constants $\mathbb{F}_q$. A *sign function* on $L^\times$ is a homomorphism sgn: $L^\times \to \mathbb{F}_q^\times$ which is the identity on $\mathbb{F}_q^\times$. We say an element of $x \in L$ is *positive* if $\operatorname{sgn}(x) = 1$.

Note that, in particular, for any sign function sgn on a local field L of characteristic p, we must have $\operatorname{sgn}(U^{(1)}) = 1$ (where $U^{(1)}$ is the one-units of L) since $U^{(1)}$ is a $\mathbb{Z}_p$-module and p is coprime to $\left|\mathbb{F}_q^\times\right| = q - 1$.

Although there is a more general theory for arbitrary local fields of characteristic p, we will only need to work with $\mathbb{F}_q((t^{-1}))$ and the sign function $\operatorname{sgn}(\sum_{i \geq n} a_i t^{-i}) = a_n$, where $a_n \neq 0$. In particular, monic elements of $\mathbb{F}_q[t]$ are positive.

For any $\alpha \in \mathbb{F}_q((t^{-1}))$, by the isomorphism $\mathbb{F}_q((t^{-1})) = \mathbb{F}_q^\times \times (t^{-1}) \times U^{(1)}$ (where $U^{(1)}$ is the one-units of $\mathbb{F}_q((t^{-1}))$), we may write α uniquely as $\operatorname{sgn}(\alpha) t^{-i} \langle \alpha \rangle$ with $i \in \mathbb{Z}$

and $\langle\alpha\rangle \in U^{(1)}$. For positive α and $s = (x, y) \in \mathbb{C}_\infty^\times \times \mathbb{Z}_p$, we define

$$\alpha^s = x^{-v_\infty(\alpha)} \langle\alpha\rangle^y$$

where v_∞ is the t^{-1}-adic valuation, and $\langle\alpha\rangle^y$ is well-defined since $\langle\alpha\rangle \in U^{(1)}$, and $U^{(1)}$ is naturally a $\mathbb{Z}_p$-module (isomorphic to $\mathbb{Z}_p^{\aleph_0}$).

It is easy to see that the normal rule of exponentiation apply - namely, if $\alpha, \beta \in \mathbb{F}_q((t^{-1}))$ are positive and $s_1, s_2 \in \mathbb{C}_\infty^\times \times \mathbb{Z}_p$, then $(\alpha\beta)^{s_1} = \alpha^{s_1}\beta^{s_1}$ and $\alpha^{s_1+s_2} = \alpha^{s_1}\beta^{s_2}$. Also, $\mathbb{Z}$ sits inside $\mathbb{C}_\infty^\times \times \mathbb{Z}_p$ naturally via the morphism $\mathbb{Z} \to \mathbb{C}_\infty^\times \times \mathbb{Z}_p, j \mapsto s_j := (t^j, j)$, and it is easy to check that for any positive $\alpha \in \mathbb{F}_q((t^{-1}))$, α^{s_j} coincides with the usual exponentiation α^j.

The G-equivariant L-function is defined on a certain "half plane" $(\mathbb{C}_\infty^\times \times \mathbb{Z}_p)^+$ inside $\mathbb{C}_\infty^\times \times \mathbb{Z}_p$ which contains $\mathbb{Z}_{\geq 0}$ (i.e. the Euler product defining the L-function converges on this half plane).

Definition 3.5.3. We define the (incomplete) G-equivariant L-function to be the function $\widetilde{\Theta}_{K/F}^E : (\mathbb{C}_\infty^\times \times \mathbb{Z}_p)^+ \to \mathbb{C}_\infty[G]$ given by

$$\widetilde{\Theta}_{K/F}^E(s) = \widetilde{\prod_v} P_v^{*,G}(Nv^{-s})^{-1},$$

where the product is over all the primes v of O_F which are at most tamely ramified in K and at which E has good reduction.

We will be concerned with the value of this L-function at $s_0 = (1, 0)$.

The following is a theorem of Noether (see [19]) which will help us reinterpret this value in a convenient way.

Theorem 3.5.4. *Let K/F be a finite Galois extension, and let $G = \mathrm{Gal}(K/F)$. Let $R \subseteq F$ be a Dedekind domain whose field of fractions is F, and let S be the integral closure of R in K. Then S/R is tamely ramified if and only if S is a projective $R[G]$-module of constant local rank 1.*

Assume now that G is a p-group. For any prime v of F, we will let $O_{F,v}$ and $O_{K,v}$ denote the localizations of O_F and O_K, respectively, at the set $O_F \setminus v$. Similarly, for a prime w of K, let $O_{K,w}$ denote the localization of O_K at w. Note that $O_{K,v} = \bigcap_{w|v} O_{K,w}$ is the integral closure of $O_{F,v}$ in K. If $v \in \mathrm{MSpec}(O_F)$ is at most tamely ramified in O_K, then by Theorem 3.5.4 we have that $O_{K,v}$ is $O_{F,v}[G]$ projective of constant local rank 1. Since $O_{F,v}[G]$ is a local ring (by Proposition 3.3.3) it follows that, in fact, $O_{K,v} \cong O_{F,v}[G]$. Thus, we have

$$O_K/v \cong O_{K,v}/v \cong (O_{F,v}[G])/v \cong (O_{F,v})/v[G] \cong \mathbb{F}_q[G]^{n_v}$$

as $\mathbb{F}_q[G]$-modules, where $n_v = [O_F/v : \mathbb{F}_q]$. In particular, $|O_K/v|_G$ and $|E(O_K/v)|_G$ are well-defined.

Proposition 3.5.5. *Let $v \in \mathrm{MSpec}(O_F)$ be at most tamely ramified in K/F. Then O_K/v and $E(O_K/v)$ are free $\mathbb{F}_q[G]$-modules of rank $[O_F/v : \mathbb{F}_q]$. If E has good reduction at v, then*

$$P_v^{*,G}(1) = \frac{|E(O_K/v)|_G}{|O_K/v|_G}.$$

Hence, the special value we will be concerned with can be expressed as

$$\widetilde{\Theta}^E_{K/F}(0) = \widetilde{\prod_v} P_v^{*,G}(Nv^0)^{-1} = \widetilde{\prod_v} \frac{|E(O_K/v)|_G}{|O_K/v|_G}.$$

Unfortunately, the methods of [7] only work for a complete Euler product (i.e. one with an Euler factor for each prime of O_F), so we need to add factors at primes where E has bad reduction and at primes which wildly ramify in K/F. For those primes v where E has bad reduction but which are at most tame in K/F, we can, by the computation above, still make sense of $\frac{|E(O_K/v)|_G}{|O_K/v|_G}$.

Definition 3.5.6. We define

$$\Theta^E_{K/F}(0) = \prod_{v \text{ tame}} \frac{|E(O_K/v)|_G}{|O_K/v|_G}.$$

For the primes which are wildly ramified, O_K/v and $E(O_K/v)$ are no longer G-c.t. (i.e. $\mathbb{F}_q[G]$-projective), so we cannot necessarily makes sense of $|O_K/v|_G$ or $|E(O_K/v)|_G$. Instead, we replace O_K with what we call a *taming module.*

Definition 3.5.7. An $O_F\{\tau\}[G]$-submodule $\mathcal{M} \subseteq O_K$ is called a *taming module* for K/F if

1. $\mathcal{M}$ is $O_F[G]$-projective of constant local rank 1.

2. $O_K/\mathcal{M}$ is finite, supported only at wildly ramified primes.

Proposition 3.5.8. *Taming modules exist.*

Proof. Let ω' be such that $K = F[G] \cdot \omega'$. Write

$$\omega'^q = \sum_{\sigma \in G} \frac{a_\sigma}{b_\sigma} \sigma\omega'$$

with each $a_\sigma, b_\sigma \in O_F$. Set $\omega = \omega' \prod_\sigma b_\sigma$. Then it's clear that $O_F[G]\omega$ is closed under taking q-th powers.

For each wildly ramified prime v of O_F, let $T_v = O_{F,v}[G] \cdot \omega$. Note that T_v is an $O_{F,v}\{\tau\}[G]$-submodule of $O_{K,v}$. We define $\mathcal{M}$ to be the kernel of the natural map $O_K \to \bigoplus_{v \text{ wild}} O_{K,v}/T_v$, i.e. $\mathcal{M}$ sits in an exact sequence

$$0 \longrightarrow \mathcal{M} \longrightarrow O_K \longrightarrow \bigoplus_{v \text{ wild}} O_{K,v}/T_v. \tag{3.1}$$

Clearly $O_K/\mathcal{M}$ is finite since $\bigoplus_{v \text{ wild}} O_{K,v}/T_v$ is. Now, for any prime v of O_F, let $\mathcal{M}_v$ denote the localization of $\mathcal{M}$ at $O_F \setminus v$. By localizing (3.1) at the primes v of O_F, we see that $\mathcal{M}_v \cong O_{K,v}(\cong O_{F,v}[G]$ by Theorem 3.5.4) for v at most tame, and $\mathcal{M}_v \cong T_v = O_{F,v}[G]$ for v wild. This shows that $\mathcal{M}$ is projective of constant local rank 1 and that $O_K/\mathcal{M}$ is supported only at wild primes. □

Let $\mathcal{M}$ be a taming module for K/F. Since $\mathcal{M}_v \cong O_{F,v}[G]$ for any prime v of O_F, the argument used above to show $O_K/v \cong \mathbb{F}_q[G]^{n_v}$ for the tame primes of O_F shows that $\mathcal{M}_v/v \cong \mathbb{F}_q[G]^{n_v}$ as $\mathbb{F}_q[G]$-modules *for all* primes $v \in \mathrm{MSpec}(O_F)$. This motivates the following definition

Definition 3.5.9. Let $\mathcal{M}$ be a taming module for K/F. We define the completed equivariant L-value associated to $\mathcal{M}$ to be

$$\Theta_{K/F}^{E,\mathcal{M}}(0) = \prod_{v \in \mathrm{MSpec}(O_F)} \cdot \frac{|E(\mathcal{M}/v)|_G}{|\mathcal{M}/v|_G}.$$

Note that, by definition, for any tame prime v we have $\mathcal{M}_v = O_{K,v}$ so that $|E(\mathcal{M}/v)|_G = |E(O_{K,v})|_G$ and $|\mathcal{M}/v|_G = |O_{K,v}|_G$. Hence,

$$\Theta_{K/F}^{E,\mathcal{M}}(0) = \Theta_{K/F}^{E}(0) \prod_{\substack{v \in \mathrm{MSpec}(O_F) \\ v \text{ wild}}} \frac{|E(\mathcal{M}/v)|_G}{|\mathcal{M}/v|_G}$$

for any taming module $\mathcal{M}$.

3.6 The Volume Function

We will now define a volume function on a certain class of topological $A[G]$-modules. The class $\mathcal{C}$ of $A[G]$-modules we will consider are those compact $A[G]$-modules M that sit in an exact sequence of topological $A[G]$-modules of the form

$$0 \longrightarrow K_\infty/\Lambda \longrightarrow M \longrightarrow H \longrightarrow 0, \tag{3.2}$$

where

1. Λ is an $A[G]$-lattice

2. M is G-c.t

3. H is finite.

For any such M, we will call (3.2) the *structural exact sequence* for M. Note that while we refer to (3.2) as *the* structural exact sequence for M, M may actually fit into several such sequences, but it will turn out that the volume of M is independent choice of sequence to fit it into. The main relevant examples for us will be $K_\infty/\mathcal{M}$ and $E(K_\infty)/E(\mathcal{M})$, where $\mathcal{M}$ is a taming module.

First, we fix a projective $A[G]$-lattice $\Lambda_0 \subseteq K_\infty$. One can think of the volume function as a characteristic p-valued multiplicative analog of the Haar measure on a locally compact group topological G, and choosing a lattice Λ_0 is analogous to choosing a fixed subset of G to have measure 1 – we will see shortly that K_∞/Λ_0 has volume 1 with our definition of the volume function.

Ideally, we would like to define the volume of a module M of structural exact sequence (3.2) to be

$$\frac{|H|_G}{[\Lambda : \Lambda_0]_G}.$$

However, this is not well-defined because H may not be G-c.t. (and therefore we can't make sense of $|H|_G$) and Λ may not be $A[G]$-projective (and therefore we can't make sense of $[\Lambda : \Lambda_0]$). We avoid this issue by introducing the concept of an *admissible lattice*, which we now define.

Let $M \in \mathcal{C}$ with structural exact sequence (3.2). Note that since K_∞/Λ is A-divisible, it is A-injective, and therefore the exact sequence splits in the category of A-modules. Let $s : H \to M$ be an A-module morphism which splits the exact sequence.

Definition 3.6.1. Let M, s be as above. We say that an $A[G]$-lattice $\Lambda' \subseteq K_\infty$ is (M, s) - *admissible* (or simply *admissible*, if (M, s) is clear from context) if

1. $\Lambda \subseteq \Lambda'$

2. Λ' is $A[G]$-projective

3. $\Lambda'/\Lambda \times s(H)$ is an $A[G]$-submodule of M.

Proposition 3.6.2. *With (M, s) as above, admissible lattices exist.*

Proof. By Proposition 3.4.8, there exists a free $A[G]$-lattice Λ' containing Λ. Since H is finite, there is $f \in A$ which annihilates H. We claim that $\frac{1}{f}\Lambda'$ is an admissible lattice. Clearly $\frac{1}{f}\Lambda'$ satisfies (1) and (2) above. For (3), let $(a, b) \in \Lambda'/\Lambda \times s(H)$ and $\sigma \in G$. Since $\sigma \cdot (a, b) = \sigma \cdot (a, 0) + \sigma \cdot (0, b)$ and Λ'/Λ is an $A[G]$-submodule of M, it suffices to show that $\sigma \cdot (0, b) \in \Lambda'/\Lambda \times s(H)$. If we let $\sigma \cdot (a, b) = (c, d) \in K_\infty/\Lambda \times s(H) = M$, then

$$f\sigma \cdot (0, b) = \sigma f \cdot (0, b) = \sigma \cdot (0, f \cdot b) = \sigma \cdot (0, 0) = (0, 0)$$

while on the other hand

$$f\sigma \cdot (0, b) = f \cdot (c, d) = (fc, fd) = (fc, 0).$$

It follows that $fc \in \Lambda$, so that $c \in \frac{1}{f}\Lambda \subseteq \frac{1}{f}\Lambda'$. Hence, $\sigma \cdot (0, b) = (c, d) \in \Lambda'/\Lambda \times s(H)$, so $\frac{1}{f}\Lambda'$ satisfies (3) above as well. □

Note that for any (M, s) admissible lattice Λ', we get an exact sequence

$$0 \longrightarrow \Lambda'/\Lambda \times s(H) \longrightarrow M \longrightarrow K_\infty/\Lambda' \longrightarrow 0.$$

Since M and K_∞/Λ' are both G-c.t., $\Lambda'/\Lambda \times s(H)$ is as well. Since $\Lambda'/\Lambda \times s(H)$ is finite, $|\Lambda'/\Lambda \times s(H)|_G$ is well-defined.

Definition 3.6.3. We define the volume function $\mathrm{Vol} : \mathcal{C} \to \mathbb{F}_q((t^{-1}))[G]^+$ as follows. Fix a projective $A[G]$-lattice $\Lambda_0 \subseteq K_\infty$. Given $M \in \mathcal{C}$, choose a A-splitting $s : H \to M$ for the structural exact sequence of M and an (M, s) admissible lattice Λ'. Define

$$\mathrm{Vol}(M) = \frac{|\Lambda'/\Lambda \times s(H)|_G}{[\Lambda' : \Lambda_0]_G}.$$

Proposition 3.6.4. *1.* $\mathrm{Vol}(M)$ *is independent of the choice of section* s *and choice of* (M, s) *- admissible lattice.*

2. If $M_1, M_2 \in \mathcal{C}$*, then* $\frac{\mathrm{Vol}(M_1)}{\mathrm{Vol}(M_2)}$ *is independent of* Λ_0*.*

3. $\mathrm{Vol}(M)$ *is independent of choice of representative in the equivalence class* $[M] \in \mathrm{Ext}^1_{A[G]}(H, K_\infty/\Lambda)$

Proof. (1) First, suppose that Λ'_1 and Λ'_2 are two (M, s)-admissible lattices such that $\Lambda'_1 \subseteq \Lambda'_2$. We have an exact sequence

$$0 \longrightarrow \Lambda'_1/\Lambda \times s(H) \longrightarrow \Lambda'_2/\Lambda \times s(H) \longrightarrow \Lambda'_2/\Lambda'_1 \longrightarrow 0.$$

Since the modules above are all finite and G-c.t., we get that

$$|\Lambda'_2/\Lambda \times s(H)|_G = |\Lambda'_1/\Lambda \times s(H)|_G \cdot |\Lambda'_2/\Lambda'_1|_G$$

by Proposition 3.3.6. It follows that

$$\begin{aligned}
\frac{|\Lambda'_1/\Lambda \times s(H)|_G}{[\Lambda'_1 : \Lambda_0]_G} &= \frac{|\Lambda'_2/\Lambda \times s(H)|_G}{|\Lambda'_2/\Lambda'_1|_G[\Lambda'_1 : \Lambda_0]_G} && \text{by Proposition 3.3.6} \\
&= \frac{|\Lambda'_2/\Lambda \times s(H)|_G}{[\Lambda'_2 : \Lambda'_1]_G[\Lambda'_1 : \Lambda_0]_G} && \text{by Proposition 3.4.11} \\
&= \frac{|\Lambda'_2/\Lambda \times s(H)|_G}{[\Lambda'_2 : \Lambda_0]_G} && \text{by Proposition 3.4.11.}
\end{aligned}$$

This shows that the volume formula gives the same value for any two admissible lattices with one contained in the other. Given any two (M, s)-admissible lattices, we can find another (M, s)-admissible lattice which contains both of them, so it follows that $\mathrm{Vol}(M)$ is independent of choice of (M, s)-admissible lattice.

Now, let $s_1, s_2 : H \to M$ be two different A-splittings of the structural short exact sequence for M. Note that the proof of 3.6.2 constructs a lattice $\frac{1}{f}\Lambda'$ which is both (M, s_1) and (M, s_2) admissible. Also, $\frac{1}{f}\Lambda'$ has the property that $s_1(x) - s_2(x) \in \frac{1}{f}\Lambda'$ for any $x \in H$ (since $s_1(x) - s_2(x)$ is killed by f). Using this fact, one can check that the identity map on M induces an isomorphism $\left(\frac{1}{f}\Lambda'\right)/\Lambda \times s_1(H) \cong \left(\frac{1}{f}\Lambda'\right)/\Lambda \times s_2(H)$. Thus, $\left|\left(\frac{1}{f}\Lambda'\right)/\Lambda \times s_1(H)\right|_G = \left|\left(\frac{1}{f}\Lambda'\right)/\Lambda \times s_2(H)\right|_G$, which shows that the volume formula is independent of choice of A-section s.

(2) Let

$$0 \longrightarrow K_\infty/\Lambda_i \longrightarrow M_i \longrightarrow H_i \longrightarrow 0$$

be the structural exact sequence for M_i, $i = 1, 2$. If $s_1 : H_1 \to M_1$ and $s_2 : H_2 \to M_2$ are A-splittings, and Λ_1', Λ_2 are (M_1, s_1) and (M_2, s_2)-admissible lattices, respectively, then

$$\frac{\mathrm{Vol}(M_1)}{\mathrm{Vol}(M_2)} = \frac{|\Lambda_1'/\Lambda_1 \times s_1(H_1)|_G}{[\Lambda_1' : \Lambda_0]_G} \frac{[\Lambda_2' : \Lambda_0]_G}{|\Lambda_2'/\Lambda_2 \times s_2(H_2)|_G} = \frac{|\Lambda_1'/\Lambda_1 \times s_1(H_1)|_G}{|\Lambda_2'/\Lambda_2 \times s_2(H_2)|_G}[\Lambda_2' : \Lambda_1']_G$$

is independent of Λ_0.

(3) Let

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_\infty/\Lambda & \xrightarrow{\iota_1} & M_1 & \xrightarrow{\pi_1} & H & \longrightarrow & 0 \\ & & \| & & \wr\downarrow\varphi & & \| & & \\ 0 & \longrightarrow & K_\infty/\Lambda & \xrightarrow{\iota_2} & M_2 & \xrightarrow{\pi_2} & H & \longrightarrow & 0 \end{array}$$

be equivalent extensions of H by K_∞/Λ. If $s_1 : H \to M_2$ is an A-section for the top sequence and Λ_1' is an (M_1, s_1)-admissible lattice, then $s_2 = \varphi \circ s_1$ is an A-section for the bottom sequence and $\Lambda_2' = \varphi(\Lambda_1')$ is an (M_2, s_2)-admissible lattice. The fact that $\mathrm{Vol}(M_1) = \mathrm{Vol}(M_2)$ then follows from the definition of Vol and the fact that $\varphi \circ \iota_1 = \iota_2$.

□

3.7 The Equivariant Tamagawa Number Formula

Fix a taming module $\mathcal{M}$ for K/F. Note that $\mathcal{M}$ is a projective $A[G]$-lattice by definition. Also, the same proof that shows $\exp_E^{-1}(O_K)$ is an A-lattice also shows that $\exp_E^{-1}(\mathcal{M})$ is an A-lattice as well. Since $\exp_E$ commutes with the action of G, $\exp_E^{-1}(\mathcal{M})$ has a G-action as well, and is therefore an $A[G]$-lattice.

We define the class module $H(E/\mathcal{M})$ associated to $\mathcal{M}$ to be the cokernel of the map $\exp_E : \frac{K_\infty}{\exp_E^{-1}(\mathcal{M})} \to \frac{E(K_\infty)}{E(\mathcal{M})}$, i.e. $H(E/\mathcal{M})$ fits into an exact sequence

$$0 \longrightarrow \frac{K_\infty}{\exp_E^{-1}(\mathcal{M})} \xrightarrow{\exp_E} \frac{E(K_\infty)}{E(\mathcal{M})} \longrightarrow H(E/\mathcal{M}) \longrightarrow 0.$$

We will call the above exact sequence the *defining exact sequence for* $H(E/\mathcal{M})$. Since $\frac{K_\infty}{\exp_E^{-1}(\mathcal{M})}$ and $\frac{E(K_\infty)}{E(\mathcal{M})}$ are both compact and $\exp_E$ is an analytic open map, $H(E/\mathcal{M})$ is finite.

We now have everything we need to state the Equivariant Tamagawa Number Formula for Drinfeld modules:

Theorem 3.7.1 (Theorem 6.1.1 of [7])**.** *Let $\mathcal{M}$ be a taming module for K/F, and let E be a Drinfeld A-module defined over O_F. Then*

$$\Theta_{K/F}^{E,\mathcal{M}}(0) = \frac{\mathrm{Vol}(E(K_\infty/\mathcal{M}))}{\mathrm{Vol}(K_\infty/\mathcal{M})}.$$

In practice, this theorem is telling us the following. Since $E(K_\infty)/E(\mathcal{M})$ has structural exact sequence

$$0 \longrightarrow K_\infty/\exp_E^{-1}(\mathcal{M}) \longrightarrow E(K_\infty)/E(\mathcal{M}) \longrightarrow H(E/\mathcal{M}) \longrightarrow 0,$$

we have that

$$\mathrm{Vol}(E(K_\infty)/E(\mathcal{M})) = \frac{|\Lambda_1/\exp^{-1}(\mathcal{M}) \times s(H(E/\mathcal{M}))|_G}{[\Lambda_1 : \Lambda_0]_G}$$

where $s : H(E/\mathcal{M}) \to E(K_\infty)/E(\mathcal{M})$ is an A-section of the structural short exact sequence, Λ_1 is an admissible lattice for $E(K_\infty)/E(\mathcal{M})$, and Λ_0 is some fixed normalization lattice. Now, $K_\infty/\mathcal{M}$ has the simple structural exact sequence

$$0 \longrightarrow K_\infty/\mathcal{M} \longrightarrow K_\infty/\mathcal{M} \longrightarrow 0 \longrightarrow 0,$$

so we may use $\mathcal{M}$ as an admissible lattice here (since $\mathcal{M}$ is $A[G]$-projective), and therefore

$$\mathrm{Vol}(K_\infty/\mathcal{M}) = \frac{1}{[\mathcal{M} : \Lambda_0]_G}.$$

Thus, Theorem 3.7.1 says that

$$\begin{aligned}
\Theta_{K/F}^{E,\mathcal{M}}(0) &= \frac{\mathrm{Vol}(E(K_\infty)/E(\mathcal{M}))}{\mathrm{Vol}(K_\infty/\mathcal{M})} \\
&= \frac{|\Lambda_1/\exp^{-1}(\mathcal{M}) \times s(H(E/\mathcal{M}))|_G[\mathcal{M} : \Lambda_0]_G}{[\Lambda_1 : \Lambda_0]_G} \\
&= \left|\Lambda_1/\exp^{-1}(\mathcal{M}) \times s(H(E/\mathcal{M}))\right|_G[\mathcal{M} : \Lambda_1]_G.
\end{aligned}$$

From the ETNF, we obtain the following Drinfeld module analogue of the classical Brumer-Stark conjecture for number fields:

Corollary 3.7.2. *If $\mathcal{M}$ is a taming module for K/F, s is a splitting for the defining exact sequence for $H(E/\mathcal{M})$, and Λ is a $(\frac{E(K_\infty)}{E(\mathcal{M})}, s)$-admissible lattice, then*

$$[\Lambda : \mathcal{M}]_G \Theta_{K/F}^{E,\mathcal{M}}(0) \in \mathrm{Fitt}_{A[G]}(H(E/\mathcal{M}))$$

Proof. By Theorem 3.7.1, we have that

$$[\Lambda : \mathcal{M}]_G \Theta_{K/F}^{E,\mathcal{M}}(0) = \left|\Lambda/\exp_E^{-1}(\mathcal{M}) \times s(H(E/\mathcal{M}))\right|_G$$

is a generator of $\mathrm{Fitt}_{A[G]}(\Lambda/\exp_E^{-1}(\mathcal{M}) \times s(H(E/\mathcal{M})))$. Since there is an surjective map

$$\Lambda/\exp_E^{-1}(\mathcal{M}) \times s(H(E/\mathcal{M})) \twoheadrightarrow H(E/\mathcal{M})$$

of $A[G]$-module (arising from the defining exact sequence for $H(E/\mathcal{M})$, we have

$$\mathrm{Fitt}_{A[G]}(\Lambda/\exp_E^{-1}(\mathcal{M}) \times s(H(E/\mathcal{M}))) \subseteq \mathrm{Fitt}_{A[G]}(H(E/\mathcal{M}))$$

by Proposition 2.3.2. This proves the corollary. □

This chapter contains material from: J. Ferrara, N. Green, Z. Higgins, C. Popescu, *An equivariant Tamagawa number formula for Drinfeld modules and applications*, submitted (2020). The dissertation author was one of the primary investigators and authors of this paper.

Chapter 4

Iwasawa Theory of Taelman Class Modules

4.1 Setup

Fix a prime p, and let q be a power of p. Let k be the field of rational functions on a smooth projective curve X defined over $\mathbb{F}_q$, fix a closed point ∞ on X, and let A be the ring of functions which are regular away from ∞. Let $F \subseteq K$ be finite separable extensions of k with K/F abelian of Galois group G, and let O_F and O_K be the integral closures of A in F and K, respectively. Let E be a Drinfeld A-module defined over O_F.

Let $\mathcal{K}_\infty/K$ be an field extension such that $\mathcal{K}_\infty/F$ is an abelian of Galois group $\mathcal{G} := \mathrm{Gal}(\mathcal{K}_\infty/F)$ and such that

1. $\Gamma := \mathrm{Gal}(\mathcal{K}_\infty/K) \cong \mathbb{Z}_p^\alpha$ for either $\alpha \in \mathbb{Z}_+$ or $\alpha = \aleph_0$.

2. $\mathcal{K}_\infty/K$ is unramified at all finite primes (the primes of O_K).

For simplicity, we will also make the assumption that $\mathcal{G} := \mathrm{Gal}(\mathcal{K}_\infty/F) \cong G \times \Gamma$.

Fix a sequence of subextensions $K_0 = K \subseteq K_1 \subseteq K_2 \subseteq \cdots$ which are all finite Galois extensions of K such that $\mathcal{K}_\infty = \bigcup_{n \in \mathbb{Z}_+} K_n$. For each $n \in \mathbb{Z}_+$, we let O_{K_n} denote the integral closure of A in K_n. Note that since we are assume K_n/K is unramified at all finite primes, O_{K_n} is the only taming module for K_n/K.

For any $n, m \in \mathbb{Z}_{\geq 0}$ with $n \geq m$, set $\Gamma_{n,m} = \mathrm{Gal}(K_n/K_m)$. When no confusion will arise, we will let $\mathrm{Tr}_{n,m}$ denote the trace map on any $\Gamma_{n,m}$-module, i.e. the map given by the action of $\sum_{\sigma \in \Gamma_{n,m}} \sigma$. When $m = 0$, we will omit it from the notation, i.e. $\Gamma_n = \mathrm{Gal}(K_n/K)$ and $\mathrm{Tr}_n = \mathrm{Tr}_{n,0}$.

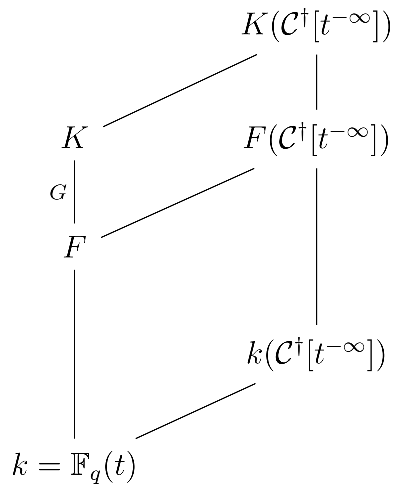
Example 4.1.1. Let K/F be finite separable extensions of $k = \mathbb{F}_q(t)$ with $G = \mathrm{Gal}(K/F)$ abelian. Let $A = \mathbb{F}_q[t]$ and let $A^\dagger = \mathbb{F}_q[t^{-1}]$. Let v_∞ denote the prime of $A^\dagger$ generated by t^{-1}, and let

$$\mathcal{C}^\dagger : A^\dagger \to A^\dagger\{\tau\}$$

$$t^{-1} \mapsto t^{-1} + \tau$$

denote the Carlitz module on $A^\dagger$.

For any $n \in \mathbb{Z}_+$, let $\mathcal{C}^\dagger[t^{-n}]$ denote the t^{-n}-torsion of the Carlitz module. Set $\mathcal{C}^\dagger[t^{-\infty}] = \bigcup_{n \in \mathbb{Z}_+} \mathcal{C}^\dagger[t^{-n}]$, and consider the following fields:



By class field theory (see [11] and [12]), for each $n \in \mathbb{Z}_+$, $\mathrm{Gal}(k(\mathcal{C}[t^{-n}])/k) \cong (A^\dagger/v_\infty^n)^\times$, so that $\mathrm{Gal}(k(\mathcal{C}^\dagger[t^{-\infty}])/k) \cong (A^\dagger_{v_\infty})^\times$. Now, we know that

$$A^\times_{v_\infty} \cong \mu_k \times U^{(1)}$$

where μ_k is the group of roots of unity in $A^\dagger_{v_\infty}$ and $U^{(1)} = 1 + t^{-1}A^\dagger_{v_\infty}$ is the group of one-units. Note that $\mu_k \cong \mathbb{F}_q^\times$, and $U^{(1)} \cong \mathbb{Z}_p^{\aleph_0}$ (see Proposition 2.8 of [13]). Hence,

$$\mathrm{Gal}(k(\mathcal{C}^\dagger[t^{-\infty}])/k) \cong \mathbb{F}_q^\times \times \mathbb{Z}_p^{\aleph_0}.$$

Furthermore, again by class field theory (see [11] and [12]), the extension $k(\mathcal{C}^\dagger[t^{-\infty}])/k$ is totally ramified at t^{-1}, tamely ramified at t, and unramified everywhere else. In fact, if L is the extension of k with $\mathrm{Gal}(L/k) \cong \mathbb{F}_q^\times$, then L/k is totally ramified at t, and $k(\mathcal{C}^\dagger[t^{-\infty}])/L$ is totally split at t. In particular, if $k_\infty \subseteq k(\mathcal{C}^\dagger[t^{-\infty}])$ is the subextension such that $\mathrm{Gal}(k(\mathcal{C}^\dagger[t^{-\infty}])/k_\infty) \cong \mathbb{F}_q^\times$, then k_∞/k is an extension such that $\mathrm{Gal}(k_\infty/k) \cong \mathbb{Z}_p^{\aleph_0}$ and k_∞/k is unramified away from t^{-1}.

Now, we have a continuous injection $\mathrm{Gal}(K(\mathcal{C}^\dagger[t^{-\infty}])/K) \to \mathrm{Gal}(k(\mathcal{C}^\dagger[t^{-\infty}])/k)$ which identifies $\mathrm{Gal}(K(\mathcal{C}^\dagger[t^{-\infty}])/K)$ with a closed subgroup of finite index in $(A^\dagger_{v_\infty})^\times$. In particular, we see that $K(\mathcal{C}^\dagger[t^{-\infty}])$ contains a unique maximal subextension $\mathcal{K}_\infty$ such that the image of $\mathrm{Gal}(\mathcal{K}_\infty/K)$ lands in $U^{(1)}$, and since $\mathrm{Gal}(\mathcal{K}_\infty/K)$ sits inside $U^{(1)} \cong \mathbb{Z}_p^{\aleph_0}$ with finite index we have $\mathrm{Gal}(\mathcal{K}_\infty/K) \cong \mathbb{Z}_p^{\aleph_0}$. This is the analogue of the cyclotomic $\mathbb{Z}_p$-extension of a number field in classical Iwasawa theory. Note that if we also assume that $K \cap k(\mathcal{C}^\dagger[t^{-\infty}]) = k$, then the assumption $\mathrm{Gal}(\mathcal{K}_\infty/F) \cong G \times \Gamma$ is also satisfied.

Let $k_\infty = \mathbb{F}_q((t^{-1}))$, the completion of k at ∞. For any $n \in \mathbb{Z}_{\geq 0}$, we let $K_{n,\infty} = K_n \otimes_k k_\infty$. Fix $m, n \in \mathbb{Z}_{\geq 0}$ with $m \leq n$. Of course, $\mathrm{Tr}_{n,m}$ maps $K_{n,\infty}$ into $K_{m,\infty}$ and O_{K_n} into O_{K_m}, and, since $\exp_E$ commutes with the action of $\Gamma_{n,m}$, $\mathrm{Tr}_{n,m}$ maps $\exp_E^{-1}(O_{K_n})$ into $\exp_E^{-1}(O_{K_m})$ as well. In other words, we have the left and middle vertical maps in the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{K_{n,\infty}}{\exp_E^{-1}(O_{K_n})} & \longrightarrow & \frac{E(K_{n,\infty})}{E(O_{K_n})} & \longrightarrow & H(E/O_{K_n}) & \longrightarrow & 0 \\ & & \downarrow \mathrm{Tr}_{n,m} & & \downarrow \mathrm{Tr}_{n,m} & & \downarrow & & \\ 0 & \longrightarrow & \frac{K_{m,\infty}}{\exp_E^{-1}(O_{K_m})} & \longrightarrow & \frac{E(K_{m,\infty})}{E(O_{K_m})} & \longrightarrow & H(E/O_{K_m}) & \longrightarrow & 0 \end{array}$$

and therefore $\mathrm{Tr}_{n,m}$ induces a map from $H(E/O_{K_n})$ to $H(E/O_{K_m})$ as well.

Now, for any prime $\mathfrak{p}$ of A, let

$$H(E/O_{K_n})_\mathfrak{p} := H(E/O_{K_n}) \otimes_A A_\mathfrak{p}$$

denote the $\mathfrak{p}$-primary part of the finite A-module $H(E/O_{K_n})$. Define

$$H_\infty^{(\mathfrak{p})} := \varprojlim H(E/O_{K_n})_\mathfrak{p}$$

where the transition maps are the trace maps. Since each $H(E/O_{K_n})_{\mathfrak{p}}$ is a module over $A_{\mathfrak{p}}[G\times\Gamma_n] \cong A_{\mathfrak{p}}[G][\Gamma_n]$, $H_\infty^{(\mathfrak{p})}$ is a module over $A_{\mathfrak{p}}[[G\times\Gamma]] := \varprojlim A_p[G\times\Gamma_n] \cong A_{\mathfrak{p}}[G][[\Gamma]]$. We would like to study the Fitting ideal of $H_\infty^{(\mathfrak{p})}$ as an $A_{\mathfrak{p}}[G][[\Gamma]]$-module. Thus, our first goal is to prove that $H_\infty^{(\mathfrak{p})}$ is finitely generated and torsion as an $A_{\mathfrak{p}}[G][[\Gamma]]$-module. In fact, we will show that $H_\infty^{(\mathfrak{p})}$ is finitely generated and torsion as an $A_{\mathfrak{p}}[[\Gamma]]$-module.

Remark. Suppose $\Gamma \cong \mathbb{Z}_p^{\aleph_0}$. Fixing such an isomorphism, for each $i \in \mathbb{Z}_+$, let $\gamma_i \in \Gamma$ be the element corresponding to the element $e_i \in \mathbb{Z}_p^{\aleph_0}$ which has 1 in the i-th component and 0 in every other component. Then the standard argument used in classical Iwasawa theory (see Theorem 7.1 of [20]) produces a topological ring isomorphism

$$A_p[[\Gamma]] \xrightarrow{\sim} A_{\mathfrak{p}}[[x_1, x_2, \dots]], \quad \gamma_i - 1 \mapsto x_i \quad \text{for all } i.$$

Under this isomorphism, the augmentation ideal I_Γ corresponds to the ideal $(x_1, x_2, \dots)$ of $A_{\mathfrak{p}}[[x_1, x_2, \dots]]$. Note that, $I_\Gamma^n \to 0$ in the profinite topology on $A_{\mathfrak{p}}[[\Gamma]]$, a fact we will need later. Also, since $A_{\mathfrak{p}}$ is the valuation ring inside a characteristic p local field, if we fix a uniformizer π for $A_{\mathfrak{p}}$, then $A_{\mathfrak{p}} \cong \mathbb{F}_q[[\pi]]$. Hence,

$$A_{\mathfrak{p}}[[\Gamma]] \cong \mathbb{F}_q[[\pi, x_1, x_2, \dots]]$$

as topological rings. Of course, an analogous result holds in the case where $\Gamma \cong \mathbb{Z}_p^d$ for some $d \in Z_+$ as well.

4.2 $H_\infty^{(\mathfrak{p})}$ is a finitely generated $A_\mathfrak{p}[[\Gamma]]$-module

To prove that $H_\infty^{(\mathfrak{p})}$ is finitely generated as an $A_\mathfrak{p}[[\Gamma]]$-module, we will use the following theorem and corollary of Balister and Howson:

Theorem 4.2.1 (Section 3 of [3]). *Let Λ be a compact topological ring with 1 and let I be a (left) ideal with $I^n \to 0$ in Λ. Let X be a compact (Hausdorff) (left) Λ-module. If X is profinite and $IX = X$, then $X = 0$.*

Corollary 4.2.2 (Section 3 of [3]). *With Λ, I, X as above, if X/IX is finitely generated as a Λ/I-module, then X is finitely generated as a Λ-module.*

In our case, our compact topological ring is $A_\mathfrak{p}[[\Gamma]]$ with the augmentation ideal I_Γ which satisfies $I_\Gamma^n \to 0$. Since $H_\infty^{(\mathfrak{p})}$ is profinite, it suffices to show that $(H_\infty^{(\mathfrak{p})})_\Gamma = H_\infty^{(\mathfrak{p})}/I_\Gamma H_\infty^{(\mathfrak{p})}$ is finitely generated as an $A_\mathfrak{p}[[\Gamma]]/I_\Gamma \cong A_\mathfrak{p}$-module. The following lemma allows us to compute the Γ coinvariants of $H_\infty^{(\mathfrak{p})}$ in terms of the Γ coinvariants of the $H(E/O_{K_n})_\mathfrak{p}$'s.

Lemma 4.2.3. *Let $\Gamma = \varprojlim \Gamma_i$ be a profinite group indexed by some directed set I. Let $H = \varprojlim H_i$ be an $A_\mathfrak{p}[[\Gamma]]$-module, with each H_i a finite $A_\mathfrak{p}[\Gamma_i]$-module such that for each $i, j \in I$ with $i \leq j$, the transition map $H_j \to H_i$ is surjective. Then*

$$\varprojlim (H_i)_\Gamma \cong \left(\varprojlim H_i\right)_\Gamma$$

Proof. For each $i \in I$, we have, by definition of $(H_i)_\Gamma$, a short exact sequence

$$0 \longrightarrow I_\Gamma H_i \longrightarrow H_i \longrightarrow (H_i)_\Gamma \longrightarrow 0 \tag{4.1}$$

As i varies over the elements of I, these exact sequences are compatible, and therefore we may take inverse limits to get an exact sequence

$$0 \longrightarrow \varprojlim I_\Gamma H_i \longrightarrow \varprojlim H_i \longrightarrow \varprojlim (H_i)_\Gamma \longrightarrow 0,$$

where the surjectivity of the map $\varprojlim H_i \to \varprojlim (H_i)_\Gamma$ follows from Lemma 15.16 of [20] since each of the terms in (4.1) is finite and therefore compact. This exact sequence fits into a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_\Gamma \varprojlim H_i & \longrightarrow & \varprojlim H_i & \longrightarrow & \left(\varprojlim H_i\right)_\Gamma & \longrightarrow & 0 \\ & & \downarrow & & \| & & \downarrow & & \\ 0 & \longrightarrow & \varprojlim I_\Gamma H_i & \longrightarrow & \varprojlim H_i & \longrightarrow & \varprojlim (H_i)_\Gamma & \longrightarrow & 0, \end{array}$$

where the top sequence is exact by definition of $\left(\varprojlim H_i\right)_\Gamma$, the leftmost and middle vertical maps are the obvious ones, and these two vertical maps induce the rightmost vertical map. By the snake lemma, the map $\left(\varprojlim H_i\right)_\Gamma \to \varprojlim (H_i)_\Gamma$ is surjective, and it is injective if and only if the inclusion $I_\Gamma \varprojlim H_i \hookrightarrow \varprojlim I_\Gamma H_i$ is an equality.

Now, suppose that Γ is finitely topologically generated, say $\Gamma = \overline{\langle \gamma_1, \gamma_2, \ldots, \gamma_r \rangle}$. Note that for every $i \in I$, we have an exact sequence

$$\bigoplus_{j=1}^{r} H_i \xrightarrow{f_i} H_i \longrightarrow (H_i)_\Gamma \longrightarrow 0 \tag{4.2}$$

where the map on the left is given by $f_i(a_1, \ldots, a_r) = \sum_j (\gamma_j - 1) a_j$. Taking inverse limits, we get an exact sequence

$$\varprojlim \bigoplus_{j=1}^{r} H_i \xrightarrow{\tilde{f}} \varprojlim H_i \longrightarrow \varprojlim (H_i)_\Gamma \longrightarrow 0 \tag{4.3}$$

where the exactness of (4.3) is again a consequence of Lemma 15.16 of [20] since all the modules in the exact sequence (4.2) are finite and therefore compact. Since the direct sums $\bigoplus_{j=1}^{r} H_i$ are finite, we have $\varprojlim \bigoplus_{j=1}^{r} H_i \cong \bigoplus_{j=1}^{r} \varprojlim H_i$. Hence, the above exact sequence becomes

$$\bigoplus_{j=1}^{r} \varprojlim H_i \xrightarrow{\tilde{f}} \varprojlim H_i \longrightarrow \varprojlim (H_i)_\Gamma \longrightarrow 0$$

with $\tilde{f}$ given by $\tilde{f}(a_1, \ldots, a_r) = \sum_j (\gamma_j - 1)a_j$. Since coker $\tilde{f} = (\varprojlim H_i)_\Gamma$, it follows that

$$(\varprojlim H_i)_\Gamma \cong \varprojlim (H_i)_\Gamma.$$

This proves the result in the case that Γ is finitely topologically generated.

Now, let Γ be any profinite group. By the work above, it suffices to show that $\varprojlim (I_\Gamma H_i) \subseteq I_\Gamma(\varprojlim H_i)$. Let $(x_i)_i \in \varprojlim (I_\Gamma H_i)$. Note that $I_\Gamma(\varprojlim H_i)$ is compact since it is the image of the compact set $I_\Gamma \times \varprojlim H_i$ under the continuous map $\Lambda \times \varprojlim H_i \to \varprojlim H_i$ given by the action of Λ. Now, for each $k \in I$, by the case for a finitely generated Γ above and our assumption that the transition maps between the H_i's are surjective, for each $k \in I$, there exists an element $y_k = (y_{k,i})_i \in I_\Gamma \varprojlim (H_i)$ such that $y_{k,i} = x_i$ for every $i \leq k$. Then it is clear that the net $(y_k)_k$ converges to x, and since $I_\Gamma(\varprojlim H_i)$ is compact and therefore closed, we get that $x = \lim y_k \in I_\Gamma(\varprojlim H_i)$. Hence, $\varprojlim (I_\Gamma H_i) \subseteq I_\Gamma(\varprojlim H_i)$, and therefore $\left(\varprojlim H_i\right)_\Gamma \cong \varprojlim \,(H_i)_\Gamma$. □

Lemma 4.2.4. *For any $n, m \in \mathbb{Z}_{\geq 0}$ with $n \geq m$, the trace map induces an isomorphism $Tr_{n,m} : (H(E/O_{K_n}))_{\Gamma_{n,m}} \xrightarrow{\sim} H(E/O_{K_m})$.*

Proof. The defining exact sequences for $H(E/O_{K_n})$ and $H(E/O_{K_m})$ are related by the commutative diagram

$$\begin{array}{ccccccccc} & & \left(\frac{K_{n,\infty}}{\exp_E^{-1}(O_{K_n})}\right)_{\Gamma_{n,m}} & \longrightarrow & E\left(\frac{K_{n,\infty}}{O_{K_n}}\right)_{\Gamma_{n,m}} & \longrightarrow & (H(E/O_{K_n}))_{\Gamma_{n,m}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Tr}_{n,m}} & & \downarrow{\scriptstyle \mathrm{Tr}_{n,m}} & & \downarrow{\scriptstyle \mathrm{Tr}_{n,m}} & & \\ 0 & \longrightarrow & \frac{K_{m,\infty}}{\exp_E^{-1}(O_{K_m})} & \longrightarrow & E\left(\frac{K_{m,\infty}}{O_{K_m}}\right) & \longrightarrow & H(E/O_{K_m}) & \longrightarrow & 0. \end{array} \tag{4.4}$$

Now, $K_{n,\infty} \cong K_{m,\infty}[\Gamma_{n,m}]$ as a $K_{m,\infty}[\Gamma_{n,m}]$ module by the normal basis theorem. It follows that $\mathrm{Tr}_{n,m} : (K_{n,\infty})_{\Gamma_{n,m}} \xrightarrow{\sim} K_{n,\infty}^{\Gamma_{n,m}} = K_{m,\infty}$ is an isomorphism. In particular, the middle and leftmost vertical maps of (4.4) are surjective, and therefore the rightmost vertical map is surjective as well by the snake lemma.

Now, by Theorem 3.5.4 and our assumption that the tower K_∞/K is unramified at all finite primes, O_{K_n} is projective as an $O_{K_m}[\Gamma_{n,m}]$-module. By Proposition 3.3.4, this implies that O_{K_n} is $\Gamma_{n,m}$-c.t., and therefore $\mathrm{Tr}_{n,m}$ induces an isomorphism

$$\mathrm{Tr}_{n,m} : (O_{K_n})_{\Gamma_{n,m}} \xrightarrow{\sim} O_{K_n}^{\Gamma_{n,m}} = O_{K_m}.$$

Since both $K_{n,\infty}$ and O_{K_n} are $\Gamma_{n,m}$-c.t., we have that

$$E\left(\frac{K_{n,\infty}}{O_{K_n}}\right)_{\Gamma_{n,m}} \cong \frac{E(K_{n,\infty})_{\Gamma_{n,m}}}{E(O_{K_n})_{\Gamma_{n,m}}}.$$

Thus, the middle vertical map of (4.4)

$$\mathrm{Tr}_{n,m} : E\left(\frac{K_{n,\infty}}{O_{K_n}}\right)_{\Gamma_{n,m}} \cong \frac{E(K_{n,\infty})_{\Gamma_{n,m}}}{E(O_{K_n})_{\Gamma_{n,m}}} \xrightarrow{\sim} E\left(\frac{K_{m,\infty}}{O_{K_m}}\right)$$

is an isomorphism. By the snake lemma, this implies that $\mathrm{Tr}_{n,m} : (H(E/O_{K_n}))_{\Gamma_{n,m}} \to H(E/O_{K_m})$ is an isomorphism. □

Theorem 4.2.5. *For any prime $\mathfrak{p}$ of A, $H_\infty^{(\mathfrak{p})}$ is a finitely generated $A_\mathfrak{p}[[\Gamma]]$-module.*

Proof. Since $H_\infty^{(\mathfrak{p})}$ is profinite and $A_\mathfrak{p}[[\Gamma]]$ is compact, it suffices, by the results of section 3 of [3], to show that $(H_\infty^{(\mathfrak{p})})_\Gamma$ is finitely generated as an $A_\mathfrak{p}[[\Gamma]]/I_\Gamma \cong A_\mathfrak{p}$-module. We have the following isomorphisms

$$\begin{aligned}
(H_\infty^{(\mathfrak{p})})_\Gamma = (\varprojlim_n H(E/O_{K_n})_\mathfrak{p})_\Gamma &\cong \varprojlim_n (H(E/O_{K_n})_\mathfrak{p})_\Gamma && \text{by Lemma 4.2.3} \\
&\cong \varprojlim_n H(E/O_K) && \text{by Lemma 4.2.4} \\
&\cong H(E/O_K),
\end{aligned}$$

so $H_\infty^{(\mathfrak{p})}$ is finite, and therefore $H_\infty^{(\mathfrak{p})}$ is a finitely generated $A_\mathfrak{p}[[\Gamma]]$-module. □

4.3 $H_\infty^{(\mathfrak{p})}$ is a torsion $A_\mathfrak{p}[[\Gamma]]$-module

Since $H_\infty^{(\mathfrak{p})}$ is finitely generated as an $A_\mathfrak{p}[[\Gamma]]$-module, its Fitting ideal $\mathrm{Fitt}_{A_\mathfrak{p}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$ is well-defined. We now want to show that $H_\infty^{(\mathfrak{p})}$ is torsion as an $A_\mathfrak{p}[[\Gamma]]$-module, since this will imply that $\mathrm{Fitt}_{A_\mathfrak{p}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$ is nontrivial. We can show this by relating $\mathrm{Fitt}_{A_\mathfrak{p}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$ to the Fitting ideals $\mathrm{Fitt}_{A_\mathfrak{p}[\Gamma_n]}(H(E/O_{K_n})_\mathfrak{p})$ at the finite levels using the following Proposition.

Proposition 4.3.1. *For any prime $\mathfrak{p}$ of A, $\mathrm{Fitt}_{A_\mathfrak{p}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$ is nonzero. There is an inclusion*

$$\mathrm{Fitt}_{A_\mathfrak{p}[[\Gamma]]}(H_\infty^{(\mathfrak{p})}) \hookrightarrow \varprojlim \mathrm{Fitt}_{A_\mathfrak{p}[\Gamma_n]}(H(E/O_{K_n})_\mathfrak{p}).$$

If $H_\infty^{(\mathfrak{p})}$ is finitely presented as an $A_\mathfrak{p}[[\Gamma]]$-module, then this injection is an equality.

Proof. Let

$$\bigoplus_{i\in I} A_{\mathfrak{p}}[[\Gamma]] \xrightarrow{\varphi} A_{\mathfrak{p}}[[\Gamma]]^t \xrightarrow{\psi} H_\infty^{(\mathfrak{p})} \longrightarrow 0$$

be a presentation of $H_\infty^{(\mathfrak{p})}$. For any $n \in \mathbb{Z}_{\geq 0}$, we claim that the maps $\varphi_n : \bigoplus_{i\in I} A_{\mathfrak{p}}[\Gamma_n] \to A_{\mathfrak{p}}[\Gamma_n]^t$ and $\psi_n : A_{\mathfrak{p}}[\Gamma_n]^t \to H(E/O_{K_n})_{\mathfrak{p}}$ which make the following diagram commute

$$\begin{array}{ccccccc} \bigoplus_{i\in I} A_{\mathfrak{p}}[[\Gamma]] & \xrightarrow{\varphi} & A_{\mathfrak{p}}[[\Gamma]]^t & \xrightarrow{\psi} & H_\infty^{(\mathfrak{p})} & \longrightarrow & 0 \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle \pi_3} & & \\ \bigoplus_{i\in I} A_{\mathfrak{p}}[\Gamma_n] & \xrightarrow{\varphi_n} & A_{\mathfrak{p}}[\Gamma_n]^t & \xrightarrow{\psi_n} & H(E/O_{K_n})_{\mathfrak{p}} & \longrightarrow & 0 \end{array} \tag{4.5}$$

(where the vertical maps are the obvious ones) make the bottom row of (4.5) exact. First, if $z_n \in H(E/O_{K_n})_{\mathfrak{p}}$ then since the trace maps between the $H(E/O_{K_m})_{\mathfrak{p}}$'s are surjective, there is a $z \in H_\infty^{(\mathfrak{p})}$ with $\pi_3(z) = z_n$. If $y \in A_{\mathfrak{p}}[[\Gamma]]^t$ is such that $\psi(y) = z$, then $\psi_n(\pi_2(y)) = z_n$. Hence, ψ_n is surjective.

Now, it is clear that $\psi_n \circ \varphi_n = 0$. Suppose that $y_n \in \ker \psi_n$. Since the restriction maps between the $A_{\mathfrak{p}}[\Gamma_m]^t$'s are surjective, there is a $y \in A_{\mathfrak{p}}[[\Gamma]]^t$ such that $\pi_2(y) = y_n$. If we take $\mathcal{G}_n := \mathrm{Gal}(K_\infty/K_n)$ coinvariants of the top row of (4.5), we obtain the commutative diagram

$$\begin{array}{ccccccc} \left(\bigoplus_{i\in I} A_{\mathfrak{p}}[[\Gamma]]\right)_{\mathcal{G}_n} & \xrightarrow{\bar{\varphi}} & (A_{\mathfrak{p}}[[\Gamma]]^t)_{\mathcal{G}_n} & \xrightarrow{\bar{\psi}} & \left(H_\infty^{(\mathfrak{p})}\right)_{\mathcal{G}_n} & \longrightarrow & 0 \\ \downarrow{\scriptstyle \bar{\pi}_1} & & \downarrow{\scriptstyle \bar{\pi}_2} & & \wr\downarrow{\scriptstyle \bar{\pi}_3} & & \\ \bigoplus_{i\in I} A_{\mathfrak{p}}[\Gamma_n] & \xrightarrow{\varphi_n} & A_{\mathfrak{p}}[\Gamma_n]^t & \xrightarrow{\psi_n} & H(E/O_{K_n})_{\mathfrak{p}} & \longrightarrow & 0 \end{array} \tag{4.6}$$

where now $\bar{\pi}_3$ is an isomorphism by Lemma 4.2.4 (see also the proof of Theorem 4.2.5). If $\bar{y}$ is the image of y in $(A_{\mathfrak{p}}[[\Gamma]]^t)_{\mathcal{G}_n}$, then $\bar{\pi}_3(\bar{\psi}(\bar{y})) = 0$, so that $\bar{\psi}(y) = 0$, and therefore there is $\bar{x} \in \left(\bigoplus_{i\in I} A_{\mathfrak{p}}[[\Gamma]]\right)_{\mathcal{G}_n}$ with $\bar{\varphi}(\bar{x}) = \bar{y}$. If $x \in \bigoplus_{i\in I} A_{\mathfrak{p}}[[\Gamma]]$ is a lift of $\bar{x}$, then

$\pi_2(\varphi(x)) = y$. Hence, $y = \varphi_n(\pi_1(x))$ is in the image of φ_n. Thus, the bottom row of (4.5) is exact.

Now, since the diagram (4.5) commutes, it follows that the natural restriction map $\mathrm{res}_n : A_{\mathfrak{p}}[[\Gamma]] \to A_{\mathfrak{p}}[\Gamma_n]$ maps $\mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$ onto $\mathrm{Fitt}_{A_{\mathfrak{p}}[\Gamma_n]}(H(E/O_{K_n})_{\mathfrak{p}})$ for any $n \in \mathbb{Z}_+$ by the definition of Fitting ideals. Since we know that $\mathrm{Fitt}_{A_{\mathfrak{p}}[\Gamma_n]}(H(E/O_{K_n})_{\mathfrak{p}})$ is nonzero, it follows that $\mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$ is nonzero as well.

For any $n \geq m$, the following diagram commutes

$$\begin{array}{ccc} \mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})}) & \longrightarrow & \mathrm{Fitt}_{A_{\mathfrak{p}}[\Gamma_n]}(H(E/O_{K_n})_{\mathfrak{p}}) \\ \downarrow & & \downarrow \mathrm{res} \\ \mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})}) & \longrightarrow & \mathrm{Fitt}_{A_{\mathfrak{p}}[\Gamma_m]}(H(E/O_{K_m})_{\mathfrak{p}}) \end{array}$$

and therefore we get a map $\mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})}) \to \varprojlim \mathrm{Fitt}_{A_{\mathfrak{p}}[\Gamma_n]}(H(E/O_{K_n})_{\mathfrak{p}})$ which is clearly injective. Finally, if $H_\infty^{(\mathfrak{p})}$ is finitely presented as an $A_{\mathfrak{p}}[[\Gamma]]$-module, then $\mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$ is finitely generated; let $(x_{1,n})_n, \ldots, (x_{\ell,n})_n \in A_{\mathfrak{p}}[[\Gamma]]$ be a set of generators. Suppose $(y_n)_n \in \varprojlim \mathrm{Fitt}_{A_{\mathfrak{p}}[\Gamma_n]}(H(E/O_{K_n})_{\mathfrak{p}})$. Then given $m \in \mathbb{Z}_+$, we know that $x_{1,m}, \ldots, x_{\ell,m}$ generate $\mathrm{Fitt}_{A_{\mathfrak{p}}[\Gamma_n]}(H(E/O_{K_n})_{\mathfrak{p}})$, so there exists a $(z_{m,n})_n \in \mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$ which is an $A_{\mathfrak{p}}[[\Gamma]]$-linear combination of $(x_{1,n})_n, \ldots, (x_{\ell,n})_n$ such that $z_{m,n} = y_n$ for $n \leq m$ (simply write y_m as an $A_{\mathfrak{p}}[\Gamma_n]$-linear combination of $x_{1,m}, \ldots, x_{\ell,m}$ and lift this linear combination to an $A_{\mathfrak{p}}[[\Gamma]]$-linear combination of $(x_{1,n})_n, \ldots, (x_{\ell,n})_n$). Clearly we have $\lim_m (z_{m,n})_n = (y_n)_n$. Also, since $\mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})}$ is a finitely generated ideal in the compact ring $A_{\mathfrak{p}}[[\Gamma]]$, $\mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$ is compact. Hence, we have $(y_n)_n = \lim_m (z_{m,n})_n \in \mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$. Thus, we get the equality

$$\mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})}) = \varprojlim \mathrm{Fitt}_{A_{\mathfrak{p}}[\Gamma_n]}(H(E/O_{K_n})_{\mathfrak{p}}).$$

□

The fact that $H_\infty^{(\mathfrak{p})}$ is torsion then immediately follows from the fact that

$$\mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})}) \subseteq \mathrm{Ann}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})}) \neq 0$$

Corollary 4.3.2. *For any prime $\mathfrak{p}$ of A, $H_\infty^{(\mathfrak{p})}$ is a torsion $A_{\mathfrak{p}}[[\Gamma]]$-module.*

As a consequence of Theorem 4.2.5 and Corollary 4.3.2, $\mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$ exists and is nontrivial.

Since $H_\infty^{(\mathfrak{p})}$ is a finitely generated torsion $A_{\mathfrak{p}}[[\Gamma]]$-module, the same is true for $H_\infty^{(\mathfrak{p})}$ as a $A_{\mathfrak{p}}[[\mathcal{G}]]$-module.

Corollary 4.3.3. *For any prime $\mathfrak{p}$ of A, $H_\infty^{(\mathfrak{p})}$ is a finitely generated and torsion $A_{\mathfrak{p}}[[\mathcal{G}]]$-module.*

4.4 An Iwasawa main conjecture

For the rest of this chapter, we will only consider the case where $k = \mathbb{F}_q(t)$ and $A = \mathbb{F}_q[t]$. In this case, we can use the ETNF for Drinfeld modules to identify some elements in the Fitting ideals of the class modules at the finite levels, which will then give us some information about $\mathrm{Fitt}_{A_{\mathfrak{p}}[[\Gamma]]}(H_\infty^{(\mathfrak{p})})$.

Proposition 4.4.1. *Let K/F be a Galois extension of function fields with Galois group G, and let $E : A \to O_F\{\tau\}$ be a Drinfeld A-module defined over O_F. Let $\mathcal{I}^E_{K/F}$ be the ideal of A generated by all the values $[\Lambda : \mathcal{M}]_G \Theta^{E,\mathcal{M}}_{K/F}(0) \in A$ as $\mathcal{M}$ ranges over all taming modules for K/F, s ranges over all A-sections for the structural exact sequence for $H(E/\mathcal{M})$, and Λ ranges over all $(\frac{E(K_\infty)}{E(O_K)}, s)$-admissible lattices. Then*

$$\mathcal{I}^E_{K/F} \subseteq \mathrm{Fitt}_A(H(E/O_K))$$

Proof. Let $\mathcal{M}$ be a taming module for K/F, s an A-section for the defining exact sequence for $H(E/\mathcal{M}_n)$, and Λ a $(\frac{E(K_\infty)}{E(O_K)}, s)$-admissible lattice. By Theorem 3.7.1, we have that

$$\Theta^{E,\mathcal{M}}_{K/F}(0) = \left|\Lambda/\exp_E^{-1}(O_K) \times s(H(E/\mathcal{M}))\right|_G [\mathcal{M} : \Lambda]_G.$$

Thus, $[\Lambda : \mathcal{M}]_G \Theta^{E,\mathcal{M}}_{K/F}(0) \in \mathrm{Fitt}_{A[G]}(\Lambda/\exp_E^{-1}(O_K) \times s(H(E/\mathcal{M})))$. By composing the surjection $\Lambda/\exp_E^{-1}(O_K) \to H(E/\mathcal{M})$ (from the defining short exact sequence for $H(E/\mathcal{M})$) with the surjection $H(E/\mathcal{M}) \to H(E/O_K)$ (since $\mathcal{M} \subseteq O_K$), we obtain a surjection $\Lambda/\exp_E^{-1}(O_K) \times s(H(E/O_K)) \to H(E/O_K)$. By properties of Fitting ideals, this implies that $\mathrm{Fitt}_{A[G]}(\Lambda/\exp_E^{-1}(O_K) \times s(H(E/O_K))) \subseteq \mathrm{Fitt}_{A[G]}(H(E/O_K))$. Hence, $[\Lambda : \mathcal{M}]_G \Theta^{E,\mathcal{M}}_{K/F}(0) \in \mathrm{Fitt}_{A[G]}(H(E/O_K))$. □

We conjecture that the inclusion in the previous proposition is actually an equality:

Conjecture 4.4.2. *Let K/F be an abelian extension of function fields with Galois group G, and let $E : A \to O_F\{\tau\}$ be a Drinfeld A-module defined over O_F. Let $\mathcal{I}^E_{K/F}$ be the ideal of A generated by all the values $[\Lambda : \mathcal{M}]_G \Theta^{E,\mathcal{M}}_{K/F}(0) \in A$ as $\mathcal{M}$ ranges over all* *taming modules for K/F, s ranges over all A-sections for the structural exact sequence for $H(E/\mathcal{M})$, and Λ ranges over all $(\frac{E(K_\infty)}{E(O_K)}, s)$-admissible lattices. Then*

$$\mathrm{Fitt}_A(H(E/O_K)) = \mathcal{I}^E_{K/F}.$$

Proposition 4.4.3. *Let $n, m \in \mathbb{Z}_{\geq 0}$ with $n \geq m$. Then the natural restriction map $res_{n,m} : A[\Gamma_n] \to A[\Gamma_m]$ maps $\mathrm{Fitt}_{A[\Gamma_n]}(H(E/O_{K_n}))$ onto $\mathrm{Fitt}_{A[\Gamma_m]}(H(E/O_{K_m}))$.*

Proof. Note that $H(E/O_{K_n}) \otimes_{A[\Gamma_n]} A[\Gamma_m] \cong (H(E/O_{K_n}))_{\Gamma_{n,m}}$ as $A[\Gamma_m]$-modules, and $(H(E/O_{K_n}))_{\Gamma_{n,m}} \cong H(E/O_{K_m})$ by Lemma 4.2.4. Then by Proposition 2.3.2, we have that

$$\mathrm{Fitt}_{A[\Gamma_m]}((H(E/O_{K_n})_{\Gamma_{n,m}}) = \mathrm{Fitt}_{A[\Gamma_m]}(H(E/O_{K_m}))$$

is the image of $\mathrm{Fitt}_{A[\Gamma_n]}(H(E/O_{K_n}))$ under the restriction map $\mathrm{res}_{n,m} : A[\Gamma_n] \to A[\Gamma_m]$.

□

Note that Proposition 4.4.3 also implies that for any prime $\mathfrak{p}$ of A, the restriction map $\mathrm{res}_{n,m} : A_\mathfrak{p}[\Gamma_n] \to A_\mathfrak{p}[\Gamma_m]$ maps $\mathrm{Fitt}_{A_p[\Gamma_n]}(H(E/O_{K_n})_\mathfrak{p})$ onto $\mathrm{Fitt}_{A_p[\Gamma_n]}(H(E/O_{K_m})_\mathfrak{p})$. If Conjecture 4.4.2 is true, then for each $n \in \mathbb{Z}_+$ we would know exactly what the elements of $\mathrm{Fitt}_{A_p[\Gamma_n]}(H(E/O_{K_n})_\mathfrak{p})$ look like, and thus, by Proposition 4.3.1, we would know exactly what the elements of $\mathrm{Fitt}_{A_\mathfrak{p}[[\Gamma]]}(H^{(\mathfrak{p})}_\infty)$ look like as well.

Bibliography

[1] Bruno Angles, Tuan Ngo Dac, and Floric Tavares-Ribeiro, *A class formula for admissible anderson modules*, (2020), hal-02490566.

[2] Bruno Anglès and Lenny Taelman, *Arithmetic of characteristic p special L-values*, Proc. Lond. Math. Soc. (3) **110** (2015), no. 4, 1000–1032, With an appendix by Vincent Bosser.

[3] P. N. Balister and S. Howson, *Note on Nakayama's lemma for compact Λ-modules*, Asian J. Math. **1** (1997), no. 2, 224–229.

[4] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London, 1986, Reprint of the 1967 original.

[5] V G Drinfel'd, *Elliptic modules*, Mathematics of the USSR-Sbornik **23** (1974), no. 4, 561–592.

[6] ______, *Elliptic modules II*, Mathematics of the USSR-Sbornik **31** (1977), no. 2, 159–170.

[7] J. Ferrara, N. Green, Z. Higgins, and C. Popescu, *An equivariant Tamagawa number formula for Drinfeld modules and applications*, https://arxiv.org/abs/2004.05144.

[8] Ernst-Ulrich Gekeler, *On finite Drinfeld modules*, J. Algebra **141** (1991), no. 1, 187–203.

[9] David Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 35, Springer-Verlag, Berlin, 1996.

[10] Cornelius Greither and Cristian D. Popescu, *The Galois module structure of ℓ-adic realizations of Picard 1-motives and applications*, Int. Math. Res. Not. IMRN (2012), no. 5, 986–1036.

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

[12] David R. Hayes, *Explicit class field theory in global function fields*, Studies in algebra and number theory, Adv. in Math. Suppl. Stud., vol. 6, Academic Press, New York-London, 1979, pp. 173–217.

[13] Kenkichi Iwasawa, *Local class field theory*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1986, Oxford Mathematical Monographs.

[14] Serge Lang, *Cyclotomic fields I and II*, second ed., Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990, With an appendix by Karl Rubin.

[15] Cristian D. Popescu, *Integral and p-adic refinements of the abelian Stark conjecture*, Arithmetic of L-functions, IAS/Park City Math. Ser., vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 45–101.

[16] The Stacks project authors, *The stacks project*, `https://stacks.math.columbia.edu`, 2021.

[17] Lenny Taelman, *A Dirichlet unit theorem for Drinfeld modules*, Math. Ann. **348** (2010), no. 4, 899–907.

[18] ______, *Special L-values of Drinfeld modules*, Ann. of Math. (2) **175** (2012), no. 1, 369–391.

[19] S. Ullom, *Integral normal bases in Galois extensions of local fields*, Nagoya Math. J. **39** (1970), 141–148.

[20] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.