Title

Some Fitting ideal computations in Iwasawa Theory over $\Q$ and in the Theory of Drinfeld Modules

Author

Ramachandran, Nandagopal

Publication Date

2024

UNIVERSITY OF CALIFORNIA SAN DIEGO

Some Fitting ideal computations in Iwasawa theory over $\mathbb{Q}$ and in the theory of Drinfeld modules

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

in

Mathematics

by

Nandagopal Ramachandran

Committee in charge:

Professor Cristian D. Popescu, Chair
Professor Russell Impagliazzo
Professor Kiran Kedlaya
Professor Dragos Oprea
Professor Claus Sorensen

2024

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

University of California San Diego

2024

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor Cristian Popescu for being an excellent mentor to me these past six years. Without his insights, guidance and constant support, I wouldn't have been able to be where I am now.

I also extend my appreciation to Kiran Kedlaya, Claus Sorensen and Dragos Oprea for serving on my thesis committee and also for the numerous courses that they taught at UCSD, through which I learned a great deal. I also thank Russell Impagliazzo for serving on my thesis committee.

I would also like to thank the UCSD Math department staff, especially Scott Rollans, Mark Whelan and Holly Proudfoot, for helping me with my teaching job assignments and other administrative paperwork.

Furthermore, I would like to thank the numerous friends I made in San Diego in the past seven years. I would like to name a few of them: Jun, Shubham, Mingjie, Woonam, Sindhana, Zeyu, Baiming, Wei, Rusiru, Poornima, Jyotsna, Balaji, Varun, Soumya, among many others. They made my life here worth living and have given me a great deal of sweet memories to look back to, including the numerous trips I have taken with them. I also thank the sport badminton for helping me relieve a lot of stress and for being a catalyst in having some good times with some dear friends.

I would also like to thank my friends from Indian Statistical Institute, where I did my undergraduate studies and my Masters, who have helped me a lot in adjusting to life outside home and in the mathematical world. I would also like to thank all my professors there, especially Prof. B. Sury, for their guidance. I would also like to thank all my school friend, teachers and close relatives who had a major role in shaping my youth.

My parents have been a huge support to me throughout my life. The person who instilled in me the love for Math problems is my father, and my mother have always encouraged me to choose my own path. They have always been there for me emotionally and as a guide in life. Without their love and care, I wouldn't be where I am now, and I can never have enough words to express my gratitude to them. I would also like to thank my grandparents, who helped my parents in my upbringing.

I would like to thank my sister and brother-in-law for their support throughout my life in the US. Their presence in the US has made me feel like I'm not far from home, and I've really enjoyed spending my short vacations with them.

Lastly, but certainly not least, I thank my beloved wife, Akanksha, for being my constant companion and for her love and support over the past eight years, as well as for the joy and happiness that is yet to come. She has been very patient with me throughout this long-distance relationship and has sacrificed her comfort for a brighter and happier future.

A major portion of Chapter 3 is being prepared for submission for publication. The dissertation author was the collaborator and the coauthor for the material below:

- C. D. Popescu, **N. Ramachandran**, *Euler factors of equivariant L-functions of Drinfeld modules and beyond*

I thank my collaborator Cristian D. Popescu, who is also my thesis advisor, for permitting me to include the materials to this dissertation.

VITA

2015	B. Math., Indian Statistical Institute Bangalore Centre
2017	M. Math., Indian Statistical Institute Bangalore Centre
2017-2022	Graduate Teaching Assistant, University of California San Diego
2022-2024	Associate Instructor, University of California San Diego
2024	Ph. D. in Mathematics, University of California San Diego

PUBLICATIONS

N. Bhardwaj, R. McCulloch, **N. Ramachandran**, K. Woo, *Integer-valued o-minimal functions*, submitted.

C. D. Popescu, **N. Ramachandran**, *Euler factors of equivariant L-functions of Drinfeld modules and beyond*, in preparation.

ABSTRACT OF THE DISSERTATION

Some Fitting ideal computations in Iwasawa theory over $\mathbb{Q}$ and in the theory of Drinfeld modules

by

Nandagopal Ramachandran
Doctor of Philosophy in Mathematics

University of California San Diego, 2024

Professor Cristian D. Popescu, Chair

This dissertation consists of two main topics. In the first one, we talk about an equivariant reformulation of the plus part of the Main Conjecture of Iwasawa theory in terms of the abstract p-adic Tate module constructed by Greither and Popescu([14]) and the cyclotomic units of $\mathbb{Q}$. Then we discuss how the Selmer module, introduced by Burns, Kurihara and Sano([1]) could be an unconditional replacement for the p-adic Tate module. In the second part, we talk about how the Euler factors in equivariant L-functions of Drinfeld modules relate to Fitting ideals of certain modules. This discussion takes us through the theory of t-motives and helps in defining the first "étale" and "crystalline" cohomology groups of a Drinfeld module defined over a finite field.

Chapter 1

Introduction

1.1 An Introduction to Iwasawa Theory

Starting from the 19th century, a central and difficult problem in algebraic number theory has been to fully understand the ideal class groups of number fields. With this in mind, Kenkichi Iwasawa, in his landmark paper [17], drawing inspiration from the analogous situation for function fields, started looking at $\mathbb{Z}_p$-extensions of a number field. More precisely, let K be a number field and let K_∞ be an infinite Galois extension of K with $\Gamma = \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$. Considering a $\mathbb{Z}_p$-extension is equivalent to considering a tower of Galois extensions

$$K = K_0 \subset K_1 \subset \ldots K_n \subset \ldots \subset K_\infty$$

with $G_n = \mathrm{Gal}(K_n/K) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Let A_n denote the p-part of the ideal class group of K_n. Then $X = \varprojlim A_n$ is a $\mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[G_n]$-module. Understanding the structure of X as a $\mathbb{Z}_p[[\Gamma]]$-module is a much easier task than understanding the structure of A_n as a $\mathbb{Z}_p[G_n]$-module. Once you understand X as a $\mathbb{Z}_p[[\Gamma]]$-module, you can take co-invariants to come down to the n-th level and deduce some properties of A_n. This setting is known as classical Iwasawa theory. Iwasawa also considered other arithmetically relevant modules other than X.

Taking its roots from here, Iwasawa theory has now developed into a vast subject where the general principle is to understand important arithmetic invariants of objects at the base level by considering infinite pro-cyclic extensions (going "up the tower") and understanding the objects at the infinite level and then descending down to the finite level. For example, for a discussion of this in the case of elliptic curves, abelian varieties, motives etc. see [24], [13], [12].

Going back to classical Iwasawa theory, the first chapter in its history was closed by Mazur and Wiles in 1984 ([25]), when they proved the Main Conjecture of Iwasawa theory over $\mathbb{Q}$. This was first formulated by Iwasawa and we'll now state the version that Mazur and Wiles provided in their paper, using notation from Washington's book ([28]).

Let $p > 2$ be prime. Consider the extension $F = \mathbb{Q}$ and $K_0 = \mathbb{Q}(\zeta_p)$. Let $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ and $K_\infty = \bigcup_n K_n$. Then K_∞/K is a $\mathbb{Z}_p$-extension, and is called the cyclotomic $\mathbb{Z}_p$-extension of K_0. Let $G = \mathrm{Gal}(K_0/F) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and $\Gamma = \mathrm{Gal}(K_\infty/K_0) \simeq \mathbb{Z}_p$. Let γ denote a topological generator of Γ, i.e. $\Gamma = \overline{\langle\gamma\rangle}$. Let $\Lambda = \mathbb{Z}_p[[\Gamma]]$ denote the Iwasawa algebra. It is easy to see that $\mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T]]$, ([28] §7.1) the one-variable power series ring with coefficients in $\mathbb{Z}_p$. Let $\omega \in \widehat{G}$ denote the Teichmüller character. Then $\widehat{G} =< \omega >$. Let $L_p(s,\omega^i)$ denote the p-adic L-function associated to ω^i. By Iwasawa's construction of p-adic L-functions ([19]), for all $i \not\equiv 1 \mod p-1$ odd, there exists a power series $f_{\omega^i} \in \mathbb{Z}_p[[T]]$ such that

$$f_{\omega^i}((1+p)^s - 1) = L_p(s,\omega^{1-i}).$$

On the other hand, let

$$\mathcal{A} = \varinjlim A_n$$

denote the injective limit of the p-part of the ideal class group of K_n's. Let X_∞ denote the Pontryagin dual of $\mathcal{A}$, i.e. $X_\infty = \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}, \mathbb{Q}_p/\mathbb{Z}_p)$. For $\chi \in \widehat{G}$, let $X_\infty(\chi)$ denote the χ-component of X_∞. With this notation, we have the Main Conjecture of Iwasawa Theory:

Theorem 1.1.1. *(**Mazur-Wiles**) For $\chi \in \widehat{G} \setminus \{\omega\}$ odd,*

$$Fitt_\Lambda(X_\infty(\chi)) = (f_\chi(T)).$$

Here Fitt_Λ denotes the 0-th Fitting ideal of a Λ-module. We define this in §1.3, and it can be thought of as a measure of the "Λ-size" of that module.

This is a statement of the form "$algebraic = analytic$", and Main Conjectures in Iwasawa Theory are usually always of this form.

This was further generalized from $\mathbb{Q}$ to any totally real field by Wiles in 1990 ([29]), and we won't discuss that here.

As seen above, the Main Conjecture talks about a connection between the class groups at the infinite level to a p-adic L-function for odd characters. Instead of looking at it character-by-character, Equivariant Iwasawa Theory looks at algebraic and analytically relevant modules/functions as a whole and try to establish a connection between them.

Our main motivation is the Equivariant Main Conjecture by Greither-Popescu ([15]), and we shall now state that here.

As before, let p denote an odd prime. Let $\mathcal{K}$ be the cyclotomic $\mathbb{Z}_p$-extension of a CM field K and let $k \subset K$ be a totally real number field such that $\mathcal{K}/k$ is abelian with Galois group $\mathcal{G}$. Let j denote the complex conjugation in $\mathcal{G}$. The "minus part" of a $\mathbb{Z}_p[[\mathcal{G}]]$-module M is the submodule of M on which j acts as -1. Let $\mathcal{S}_p$ denote the primes in $\mathcal{K}$ above p. Let $\mathcal{S}$ and $\mathcal{T}$ be two $\mathcal{G}$-equivariant finite sets of primes with $\mathcal{T} \cap (\mathcal{S} \cup \mathcal{S}_p) = \varnothing$.

The Equivariant Main Conjecture is stated under the assumption that $\mu_{\mathcal{K}} = 0$, i.e. $\mathcal{A}_{\mathcal{K}}$, the injective limit of the p-part of the class groups at the finite level, is p-divisible. Under this assumption, Greither and Popescu construct a p-adic 1-motive, denoted by $\mathcal{M}^{\mathcal{K}}_{\mathcal{S},\mathcal{T}}$, and obtain a p-adic Tate module $T_p(\mathcal{M}^{\mathcal{K}}_{\mathcal{S},\mathcal{T}})$ from this motive. We'll define this in more detail in Chapter 2. This is a $\mathbb{Z}_p[[\mathcal{G}]]$-module, and sits in an exact sequence

$$0 \to T_p(\mathcal{A}_{\mathcal{K},\mathcal{T}}) \to T_p(\mathcal{M}^{\mathcal{K}}_{\S,\mathcal{T}}) \to \mathcal{D}iv_{\mathcal{K}}(\mathcal{S} \smallsetminus \mathcal{S}_p) \otimes \mathbb{Z}_p \to 0$$

where $T_p(\mathcal{A}_{\mathcal{K},\mathcal{T}})$ denotes the p-adic Tate module of $\mathcal{A}_{\mathcal{K},\mathcal{T}}$, the injective limit of the p-part of the $\mathcal{T}$-class groups, while $\mathcal{D}iv_{\mathcal{K}}(\mathcal{S} \smallsetminus \mathcal{S}_p)$ denotes the divisors supported at primes in $\mathcal{S} \smallsetminus \mathcal{S}_p$.

On the analytic side, there is the equivariant p-adic L-function $\Theta^{(\infty)}_{S,T} \in \mathbb{Z}_p[[\mathcal{G}]]$ formed from the equivariant L-function values at the finite level. This lives on the minus part because these L-function values are 0 at even characters, and so $\Theta^{(\infty)}_{S,T} \in \mathbb{Z}_p[[\mathcal{G}]]^-$.

Now we are ready to state the Equivariant Main Conjecture as stated by Greither-Popescu ([15]):

Theorem 1.1.2. ***(Greither-Popescu)*** *Under the above hypothesis, there is an equality of $\mathbb{Z}_p[[\mathcal{G}]]^-$-ideals*

$$Fitt_{\mathbb{Z}_p[[\mathcal{G}]]^-}(T_p(\mathcal{M}^{\mathcal{K}}_{S,T})^-) = (\Theta^{(\infty)}_{S,T}).$$

This theorem is dependent on the $\mu = 0$ hypothesis, which is known only for abelian number fields ([7]). In recent work, Gambheera and Popescu ([8]), drawing inspiration from the theory of Ritter-Weiss modules and Selmer modules, proved a new Equivariant Main Conjecture without any assumptions on the μ-invariant of the number fields involved. As we mentioned earlier, the definition of the p-adic 1-motive is dependent on the $\mu = 0$ conjecture, and so the algebraic side has to be replaced. The candidate chosen for this was the minus part of the Selmer module $Sel_S^T(\mathcal{K})_p$ constructed by Burns-Kurihara-Sano ([1]), and it can be shown to be isomorphic to $T_p(\mathcal{M}_{\S,\mathcal{T}}^{\mathcal{K}})^-$ when $\mu = 0$.

Now a natural question that arises is about what happens in the plus part of these extensions. Unfortunately, the p-adic L-functions are all 0 on the plus side, and therefore, that doesn't give any useful information. Even then, there is a version of the classical Main Conjecture on the plus side. This version, which is equivalent to the Mazur-Wiles Theorem, establishes a connection between the class groups and units modulo cyclotomic units. Rubin ([22] Appendix) has given an elementary proof of this version of the Main Conjecture using the theory of Euler systems.

In Chapter 2, we'll first state this positive part of the Main Conjecture. Then we'll see how this can be collected to give an Equivariant Main Conjecture over $\mathbb{Q}$ using the p-adic Tate module of the 1-motive. Our main result (2.3.2) is just a reworking of Mazur-Wiles into an equivariant setting. Since the existence of the p-adic Tate module depends on the $\mu = 0$ conjecture, we see what could be a good replacement for this. Finally, we talk about possible future work trying to extend this to general CM fields over totally real fields.

1.2 An Introduction to Drinfeld Modules

The theory of Drinfeld modules was first introduced by Vladimir Drinfel'd in 1974 ([4]) as a generalization of the concept of elliptic curves. This was first called as elliptic modules and also serves as a generalization to the notion of a Carlitz module, first introduced by Carlitz in 1938 ([2]). Two excellent applications of the theory of Drinfeld modules (and shtukas) arise in the Langlands conjectures for GL_n and in understanding explicit class field theory for global function fields.

Let p be prime, and let q be a power of p. Let $k = \mathbb{F}_q(t)$ denote the rational function field over $\mathbb{F}_q$ and let $A = \mathbb{F}_q[t]$. Let F/k be a finite separable extension, and let $\mathcal{O}_F$ denote the integral closure of A in F. Let τ denote the q-Frobenius, and let $\mathcal{O}_F\{\tau\}$ denote the twisted ring of polynomials with coefficients in $\mathcal{O}_F$, i.e. with the property that

$$\tau \cdot x = x^q \cdot \tau$$

for all $x \in \mathcal{O}_F$. To this setup, we can define a Drinfeld module over $\mathcal{O}_F$ defined on A.

A Drinfeld module E of rank r over $\mathcal{O}_F$ is an $\mathbb{F}_q$-homomorphism

$$\phi_E : A \to \mathcal{O}_F\{\tau\}$$

$$t \mapsto t + \ldots + a_r\tau^r$$

with $a_r \neq 0$.

Let K/F be an abelian extension with Galois group G. Let $\mathcal{O}_K$ denote the integral closures of A in K.For any $\mathcal{O}_F\{\tau\}[G]$-module M, the map ϕ_E gives rise to an $A[G]$-module structure on M, and we denote this $A[G]$-module by $E(M)$.

For any maximal ideal $v_0 = (\pi_{v_0})$ of A, we can define the v_0-adic Tate module $T_{v_0}(E)$ of E by considering the torsion points of the action of $\pi_{v_0}^n$ on $E(\overline{F})$. Note that $T_{v_0}(E)$ is a A_{v_0} -module with the natural G_F-action obtained from $\overline{F}$. Inspired from the non-equivariant setting, Popescu et. al. ([6]) defines the G-equivariant first étale cohomology groups of E as

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

where $(T_{v_0}(E))^*$ denotes the A_{v_0}-dual of $T_{v_0}(E)$.

Let v be a place of $\mathcal{O}_F$ such that v is tamely ramified in K/F and E has good reduction at v, i.e. $v(a_r) = 0$. Let $\widetilde{I_v} \subset G_F$ denote the inertia group of v, and let $\widetilde{\sigma_v}$ denote a choice of Frobenius in G_F. This is well-defined up to elements in $\widetilde{I_v}$. Let v_0 be any place in A not lying below v. Then it is known ([6], [9]) that

$$P_v^{*,G}(X) = \det_{A_{v_0}[G]}(X \cdot id - \widetilde{\sigma_v} | H^1_{v_0}(E,G)^{\widetilde{I_v}})$$

is independent of v_0.

On the other hand, it is known that $\mathcal{O}_K/v$ and $E(\mathcal{O}_K/v)$ are free $\mathbb{F}_q[G]$-modules of equal rank. Then, it follows that $\mathrm{Fitt}_{A[G]}(\mathcal{O}_K/v)$ and $\mathrm{Fitt}_{A[G]}E(\mathcal{O}_K/v)$ are principal ideals and have a unique monic generator (i.e. as a polynomial in t, they have coefficient 1). We denote these generators by $|\mathcal{O}_K/v|_G$ and $|E(\mathcal{O}_K/v)|_G$, respectively.

The main result that we discuss in Chapter 3 is the following Proposition, which is Prop 1.2.5 (2) in [6]:

Proposition 1.2.1. *Let K/F and E be as above, and let v be a place of $\mathcal{O}_F$ that is tamely ramified in K/F. Then*

$$P_v^{*,G}(1) = \frac{|E(\mathcal{O}_K/v)|_G}{|\mathcal{O}_K/v|_G} \in (1 + t^{-1}\mathbb{F}_q[G][[t^{-1}]]).$$

A proof of this proposition in the case that E is the Carlitz module is given in the Appendix of [6], and our goal is a proof of this for general Drinfeld modules.

In Chapter 3, we'll first state the problem more precisely. The first step is to look at a new Drinfeld module $\overline{E}$ obtained from E by reduction $\mod v$. Most of the proof involves working with $\overline{E}$. Then we'll give an elementary proof to our statement by a direct application of a theorem of Gekeler ([9]) that helps us understand the roots of $P_v^{*,G}$ and also about how the Frobenius behaves as an endomorphism. This occupies §3.4. In §3.5, we'll state a more involved proof, thanks mostly to Popescu, involving the concept of local $\mathbb{F}_q$-shtukas. This approach helps us in defining the first étale cohomology and first crystalline cohomology groups of $\overline{E}$. More precisely, the Tate module $T_{w_0}(\overline{E})$ is of lower rank than the other Tate modules where $w_0 \in \mathrm{MSpec}(A)$ with $v|w_0$, and so we need a substitute for the w_0-adic étale cohomology group, and that is the crystalline cohomology group.

This is joint work with Cristian Popescu and will appear as a separate paper in the future ([27]).

1.3 Fitting ideals

We recall the definition of the Fitting ideal of a module over a commutative ring, and state some important results. For a nice crisp discussion on this, see the Appendix of [25].

Let R be a commutative ring with unity and let M be a finitely generated R-module. So there exists a presentation of M of the form

$$\bigoplus_I R \xrightarrow{\phi} R^n \to M \to 0$$

where I is some indexing set. Let A denote the matrix (of dimension $n \times |I|$) associated to the map ϕ. Under this setup, we have the following definition:

Definition 1.3.1. Let $i \geq 0$. The i-th Fitting ideal of M, denoted by $\mathrm{Fitt}_R^i(M)$, is defined as the R-ideal generated by all the $(n-i)\times(n-i)$ minors of A. This can be shown to be independent of the presentation we consider.

We'll be mostly concerned with 0-th Fitting ideals only, but we'll mention a couple of results involving higher Fitting ideals. We'll denote Fitt^0 by Fitt throughout this document. The 0-th Fitting ideal of a torsion R-module can be thought of as the "R-size" of M. This can be seen by observing that for a torsion $\mathbb{Z}$-module M, $\mathrm{Fitt}^0_{\mathbb{Z}}(M) = |M|\mathbb{Z}$.

Here are some simple properties of 0-th Fitting ideals:

- If M has n generators, then $\mathrm{Fitt}^i_R(M) = 0$ if $i > n$. If M has more generators than linearly independent relations (i.e. has a "free part"), then $\mathrm{Fitt}^0_R(M) = 0$.
- Let $\mathrm{Ann}_R(M)$ denote the annihilator ideal of M. If M has n generators, then

$$\mathrm{Ann}_R(M)^n \subseteq \mathrm{Fitt}_R(M) \subseteq \mathrm{Ann}_R(M).$$

- Let $\pi : R \to R'$ be a ring homomorphism. Then

$$\mathrm{Fitt}_{R'}(M \bigotimes_R R') = \pi(\mathrm{Fitt}_R(M)).R'.$$

  In particular, if $I \subset R$ is an ideal,

$$\mathrm{Fitt}_{R/I}(M/IM) = \mathrm{Fitt}_R(M)/I\mathrm{Fitt}_R(M).$$

Chapter 2

EMC over $\mathbb{Q}$: the plus part

2.1 The Main conjecture in Iwasawa theory: the plus part

Throughout this chapter, we'll assume that p is an odd prime.

Let us first restate the Main Conjecture over $\mathbb{Q}$ in terms of the even characters, instead of the odd ones. We'll follow the notation used in the Appendix by Karl Rubin in [22]. As before, we have $k = \mathbb{Q}$ and $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$. We put $G = Gal(K_0/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, and $\Gamma_n = Gal(K_n/K_0)$. At the infinite level, we have $K_\infty = \cup_n K_n$ and $\Gamma = \varprojlim \Gamma_n = Gal(K_\infty/K_0)$. Also, $Gal(K_\infty/\mathbb{Q}) \simeq G \times \Gamma$.

Let C_n denote the p-part of the ideal class group of K_n, while $E_n = \mathcal{O}_{K_n}^\times$ denotes the units of $\mathcal{O}_{K_n}$. Since the prime p is totally ramified in the extension $K_n/\mathbb{Q}$, we denote by $K_{n,p}$ the completion of K_n with respect to the unique prime above p. Let U_n denote the 1-units in $K_{n,p}$. We denote by $\mathcal{E}_n$ the group of cyclotomic units of K_n, i.e. the $\mathbb{Z}[G_n]$-module generated by $\pm\zeta_{p^{n+1}}$ and $1 - \zeta_{p^{n+1}}$. Denote by $\overline{E}_n$ the closure of $E_n \cap U_n$ in U_n and by V_n the closure of $\mathcal{E}_n \cap U_n$ in U_n. Note that all of these are

$\mathbb{Z}_p[G_n]$-modules.

Now we take inverse limits with respect to the norm maps as $n \to \infty$ and denote them by C_∞, E_∞, V_∞ and U_∞. These are all $\mathbb{Z}_p[[Gal(K_\infty/\mathbb{Q})]]$-modules. Since $\mathbb{Z}_p[[Gal(K_\infty/\mathbb{Q})]] \simeq \mathbb{Z}_p[G][[\Gamma]]$, for any $\mathbb{Z}_p[[Gal(K_\infty/\mathbb{Q})]]$-module M and any character $\chi \in \widehat{G}$, we can define the χ-part of M, which will be a Λ-module and we'll denote it by $M(\chi)$. As Λ-modules, it is known that $C_\infty(\chi)$ is finitely generated and torsion for all $\chi \in \widehat{G}$ and $U_\infty(\chi)/V_\infty(\chi)$ is finitely generated torsion for all even $\chi \in \widehat{G}$.

The following theorem, due to Serre, helps us understand the structure of finitely generated Λ-modules:

Theorem 2.1.1. ***(Serre)*** *Let M be a finitely generated Λ-module. Then there exists a quasi-isomorphism, i.e. a map with finite co-kernel and kernel, from M to*

$$\Lambda^r \oplus \prod \Lambda/p^{n_i} \oplus \prod \Lambda/f_j^{m_j}$$

where f_j's are irreducible polynomials in $\mathbb{Z}_p[T]$.

If M is torsion, then $r = 0$ and we define the characteristic ideal of M as

$$char(M) = \Big(\prod p^{n_i} \prod f_j^{m_j}\Big).$$

We are now ready to state the plus-part of the main conjecture:

Theorem 2.1.2. ***(Mazur-Wiles)*** *For all even characters $\chi \in \widehat{G}$,*

$$char(C_\infty(\chi)) = char(E_\infty(\chi)/V_\infty(\chi)).$$

2.2 The p-adic 1-motive

In this section, we define the structure $T_p(\mathcal{M})$ that forms the algebraic part of the Equivariant Main Conjecture of Greither-Popescu ([15]). Let $\mathcal{K}/k$ be an infinite abelian extension with a finite sub-extension K/k such that $\mathcal{K}$ is the cyclotomic $\mathbb{Z}_p$-extension of K. Let K_n denote the field at the n-th level of the tower $\mathcal{K}/K$.Let $\mathcal{G} = \text{Gal}(\mathcal{K}/k)$. Let $\mathcal{S}_p$ denote the set of primes in $\mathcal{K}$ lying above p and let $\mathcal{S}$ and $\mathcal{T}$ denote two disjoint finite sets of primes in $\mathcal{K}$ such that $\mathcal{T}$ doesn't contain any primes above p. Let $\mathcal{D}iv_{\mathcal{K}}(\mathcal{S} \smallsetminus \mathcal{S}_p) = \bigoplus_{v \in \mathcal{S} \smallsetminus \mathcal{S}_p} \mathbb{Z}_p.v$. We denote by $A_{K_n,\mathcal{T}}$ the p-part of the $\mathcal{T}|_{K_n}$-ray class group of K_n. Passing to the direct limits, we define

$$\mathcal{A}_{\mathcal{K},\mathcal{T}} = \varinjlim A_{K_n,\mathcal{T}}.$$

For ease of notation, we denote $\mathcal{D}iv_{\mathcal{K}}(\mathcal{S} \smallsetminus \mathcal{S}_p)$ by L and $\mathcal{A}_{\mathcal{K},\mathcal{T}}$ by J. The L stands for lattice and J for Jacobian as the theory of abstract 1-motives, as defined by Greither and Popescu, is strongly motivated by Deligne's theory of 1-motives. For more on this, check the Introduction of [15]. Note that there is a map $\delta : L \to J$ given by a divisor $D \in L$ mapping to its ideal class in J. This whole data of L, J and the map $\delta : L \to J$ will be denoted by $\mathcal{M}$ and is called a p-adic 1-motive. We can now define the p^n-torsion and the Tate module associated to $\mathcal{M}$:

Definition 2.2.1. The p^n-torsion of $\mathcal{M}$ is defined as

$$\mathcal{M}[p^n] = \{(\epsilon, D) \in J \times L \ \mid \ \epsilon^{p^n} = \delta(D)\} \otimes \mathbb{Z}_p/p^n\mathbb{Z}_p$$

and the Tate module of $\mathcal{M}$ is defined as

$$T_p(\mathcal{M}) = \varprojlim \mathcal{M}[p^n]$$

where the transition maps are given by $(\epsilon, D) \otimes \widehat{1} \mapsto (\epsilon^p, D) \otimes \widehat{1}$.

2.3 Equivariant version of MC$^+$

Now we go back to our base setting as in MC$^+$. In the notation of the previous section, we have $k = \mathbb{Q}$, $K = \mathbb{Q}(\zeta_p)$ and $\mathcal{K} = \mathbb{Q}(\zeta_{p^\infty})$. In this scenario, the prime p in

$\mathbb{Q}$ is totally ramified in $\mathcal{K}/k$ and so, by abuse of notation, we denote by p the prime above p in $\mathcal{K}$. We take $\mathcal{S} = \mathcal{S}_p = \{p\}$ and $\mathcal{T} = \varnothing$. Also, by the celebrated Ferrero-Washington theorem, we have $\mu_{\mathcal{K}} = 0$. So we have the p-adic 1-motive $\mathcal{M}$ and its Tate module $T_p(\mathcal{M})$ as defined. Our goal in this section is to relate $T_p(\mathcal{M})$ to units modulo cyclotomic units in this particular setting.

Since $\mathcal{S} \setminus \mathcal{S}_p = \varnothing$, it is easy to see that

$$T_p(\mathcal{M}) = T_p(\mathcal{A}_{\mathcal{K}}).$$

Since $\mathcal{A}_{\mathcal{K}} \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_{\mathcal{K}}}$, we have

$$\mathcal{A}_{\mathcal{K}}[p^n] = \mathrm{Hom}_{\mathbb{Z}_p}\left(\frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p, \mathcal{A}_{\mathcal{K}}\right)$$

with the usual $\mathcal{G}$-action. Taking inverse limits, we get

$$T_p(\mathcal{A}_{\mathcal{K}}) \simeq \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \mathcal{A}_{\mathcal{K}}).$$

On the other hand, we denote by $\mathcal{A}_{\mathcal{K}}^{\vee}$ the Pontryagin dual of $\mathcal{A}_{\mathcal{K}}$, i.e.

$$\mathcal{A}_{\mathcal{K}}^{\vee} = \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}_{\mathcal{K}}, \mathbb{Q}_p/\mathbb{Z}_p).$$

This also has $\mathbb{Z}_p[[\mathcal{G}]]$-module structure with the contravariant $\mathcal{G}$-action given by $(g.\tau)(x) = \tau(g^{-1}.x)$ for all $g \in \mathcal{G}$, $\tau \in \mathcal{A}_{\mathcal{K}}^{\vee}$ and $x \in \mathcal{A}_{\mathcal{K}}$.

We have a $\mathcal{G}$-equivariant non-degenerate pairing

$$T_p(\mathcal{A}_{\mathcal{K}}) \times \mathcal{A}_{\mathcal{K}}^{\vee} \to \mathbb{Z}_p$$

given by $(\sigma, \tau) \mapsto \tau \circ \sigma$. This implies that we have a $\mathbb{Z}_p[[\mathcal{G}]]$-module isomorphism

$$T_p(\mathcal{A}_{\mathcal{K}}) \simeq \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}_{\mathcal{K}}^{\vee}, \mathbb{Z}_p).$$

For each $\chi \in \widehat{G}$, taking χ-components, we have an isomorphism of Λ-modules

$$T_p(\mathcal{A}_{\mathcal{K}})(\chi) \simeq \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}_{\mathcal{K}}(\chi)^\vee, \mathbb{Z}_p).$$

Therefore,

$$char(T_p(\mathcal{A}_{\mathcal{K}})(\chi)) = char(\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}_{\mathcal{K}}(\chi)^\vee, \mathbb{Z}_p)) = char(\mathcal{A}_{\mathcal{K}}(\chi)^\vee)$$

By a theorem of Iwasawa (see Proposition 15.35 in [28]), $C_\infty(\chi)$ is quasi-isomorphic to $\mathcal{A}_{\mathcal{K}}(\chi)^\vee$, and hence share the same characteristic ideal. Combining this with the Mazur-Wiles Theorem above (see 2.1.2), we get that for all $\chi \in \widehat{G}$ even

$$char(T_p(\mathcal{A}_{\mathcal{K}})(\chi)) = char(E_\infty(\chi)/V_\infty(\chi)).$$

We now use the following fact about characteristic ideals and Fitting ideals:

Remark 2.3.1. If M is is a finitely generated torsion Λ-module with no finite submodules, then

$$\mathrm{Fitt}_\Lambda(M) = char(M).$$

Since $T_p(\mathcal{A}_{\mathcal{K}})$ is a free $\mathbb{Z}_p$-module, it doesn't have any finite $\mathbb{Z}_p$-submodules, and hence no finite Λ-submodules.

On the other hand, it is known that ([18], [28] Theorem 13.56) for $\chi \neq 1_G$,

$$U_\infty(\chi)/V_\infty(\chi) \simeq \Lambda/(g_\chi)\Lambda$$

where g_χ is the power series in Λ that gives the p-adic L-function $L_p(\chi, 1-s)$. So, this doesn't have any Λ-submodules. Since $E_\infty(\chi)/V_\infty(\chi)$ is contained in $U_\infty(\chi)/V_\infty(\chi)$, the same is true for $E_\infty(\chi)/V_\infty(\chi)$. When $\chi = 1_G$, an application of the analytic class number formula for $\mathbb{Q}_n = \mathbb{Q}(\zeta_{p^{n+1}})^G$ and the Leopoldt's conjecture for $\mathbb{Q}$ (which is a Theorem), gives us $E_\infty(1_G) = V_\infty(1_G)$. For more on this, see the proof of Appendix

Lemma 6.6 (iii) in [22]. Hence in this situation too, it doesn't have any finite submodules.

Therefore, we have

$$\mathrm{Fitt}_\Lambda(T_p(\mathcal{A}_\mathcal{K})(\chi)) = \mathrm{Fitt}_\Lambda(E_\infty(\chi)/V_\infty(\chi))$$

for all even characters $\chi \in \widehat{G}$.

Recall that we denote by $\mathbb{Z}_p[[\mathcal{G}]]^+$ the plus part of $\mathbb{Z}_p[[\mathcal{G}]]$, i.e.

$$\mathbb{Z}_p[[\mathcal{G}]]^+ = \mathbb{Z}_p[[\mathcal{G}]]/(1-j) \simeq \mathbb{Z}_p[[Gal(\mathcal{K}^+/k)]]$$

where j denotes the complex conjugation in $Gal(\mathcal{K}/k)$, and $\mathcal{K} = \mathbb{Q}(\mu_{p^\infty})^+$. For any $\mathbb{Z}_p[[\mathcal{G}]]$-module M, we denote by M^+ the $\mathbb{Z}_p[[\mathcal{G}]]^+$-submodule of M on which j acts as multiplication by $+1$. Then

$$\mathrm{Fitt}_{\mathbb{Z}_p[[\mathcal{G}]]^+}(M^+) = \bigoplus_{\chi\in\widehat{G}\text{ even}} \mathrm{Fitt}_\Lambda(M(\chi))$$

Since the component-wise Fitting ideals give us the full Fitting ideal, we have an equality of ideals:

Corollary 2.3.2. ***(equivariant EMC⁺ over** $\mathbb{Q}$**)*** *For the p-adic 1-motive associated to $\mathcal{K} = \mathbb{Q}(\mu_{p^\infty})$ and $k = \mathbb{Q}$ with $\mathcal{S} = \mathcal{S}_p$ and $\mathcal{T} = \varnothing$, we have*

$$Fitt_{\mathbb{Z}_p[[\mathcal{G}]]^+}(T_p(\mathcal{M})^+) = Fitt_{\mathbb{Z}_p[[\mathcal{G}]]^+}(E_\infty^+/V_\infty^+).$$

2.4 Unconditional EMC à la Gambheera-Popescu

The EMC as given by Greither and Popescu relies on the assumption that $\mu_\mathcal{K} = 0$. In recent work, motivated by Dasgupta and Kakde's work on the Brumer-Stark conjecture([3]), Gambheera and Popescu ([8]) formulated a new unconditional Equivariant Main Conjecture. Instead of looking at the Tate module of the p-adic 1-motive, they look at the Selmer modules that were first defined by Burns-Kurihara-Sano (reference). In this section, we'll define Selmer modules, state Gambheera-Popescu's unconditional EMC and mention how the Tate module of the p-adic 1-motive fits in this picture.

Let K/k be an abelian extension of number fields with Galois group G. Let S and T be two disjoint finite sets of primes in k with S containing all the infinite primes of k. We denote by S_K and T_K the primes in K above S and T, respectively. Let $K_T^\times = \{x \in K^\times \mid v(x-1) > 0 \ \forall \ v \in T_K\}$. Let

$$\mathcal{O}_{K,S,T}^\times = \{x \in K_T^\times \mid v(x) = 0 \ \forall \ v \notin S_K\}.$$

and

$$Y_{\overline{S \cup T}}(K) = \bigoplus_{v \notin S_K \cup T_K} \mathbb{Z}.$$

The map $x \mapsto (v(x))_{v \notin S_K \cup T_K}$ from $K_T^\times \to Y_{\overline{S \cup T}}(K)$ gives rise to the following exact sequence:

$$0 \to \mathcal{O}_{K,S,T}^\times \to K_T^\times \to Y_{\overline{S \cup T}}(K) \to Cl_S^T(K) \to 0$$

where $Cl_S^T(K)$ denotes the (S,T)-class group of K. Taking $\mathbb{Z}$-duals, we get an inclusion of $\mathbb{Z}[G]$-modules

$$(Y_{\overline{S \cup T}}(K))^* \to (K_T^\times)^*.$$

This leads us to the following definition:

Definition 2.4.1. The Selmer module associated to the data $(K/k, S, T)$ is the $\mathbb{Z}[G]$-module given by

$$Sel_S^T(K) = (K_T^\times)^* / (Y_{\overline{S \cup T}}(K))^*.$$

The p-adic Selmer module $Sel_S^T(K)_p$ associated to $(K/k, S, T)$ is the $\mathbb{Z}_p[G]$-module obtained by base-changing $Sel_S^T(K)$ from $\mathbb{Z}$ to $\mathbb{Z}_p$.

Now, as before, let K/k be an abelian extension with $\mathcal{K}$ denoting the cyclotomic $\mathbb{Z}_p$-extension of K. As before, $\mathcal{G} = \mathrm{Gal}(\mathcal{K}/k)$. Let K_n denote the n-th level of the cyclotomic tower $\mathcal{K}/K$ with $K_0 = K$. Let $G_n = \mathrm{Gal}(K_n/k)$. Then taking inverse limits up the tower, we define

$$Sel_S^T(\mathcal{K})_p = \varprojlim Sel_S^T(K_n)_p$$

where the transition map is obtained from the restriction map $(K_{n+1,T}^\times)^* \to (K_{n,T}^\times)^*$.

Theorem 2.4.2. *(**Gambheera-Popescu**) Under some mild hypotheses on S and T, there is an equality of $\mathbb{Z}_p[[\mathcal{G}]]^-$-ideals*

$$Fitt_{\mathbb{Z}_p[[\mathcal{G}]]^-}(Sel_S^T(\mathcal{K})_p^-) = (\Theta_S^T(\mathcal{K}/k)).$$

In their paper, Gambheera and Popescu have proved that, when $\mu = 0$,

$$T_p(\mathcal{M})^{-,*} \simeq Sel_S^T(\mathcal{K})_p^-$$

as $\mathbb{Z}_p[[\mathcal{G}]]^-$-modules, where $(.)^*$ denotes the $\mathbb{Z}_p$-dual. So, this unconditional version of the EMC supersedes Greither and Popescu's version of the EMC.

2.5 Future work

In future work, we would first like to write down a version of the EMC$^+$ connecting the Selmer module and the cyclotomic units. At the finite level, this is already a result, due to Burns-Kurihara-Sano ([1]). They showed the following:

Theorem 2.5.1. *(**Burns-Kurihara-Sano**) Let $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ and $k = \mathbb{Q}$ and $G_n = Gal(K_n/k)$. Let S be a finite set of places of k containing p and ∞, and let T be a finite set of places of k disjoint from S such that $\mathcal{O}_{K,S,T}^\times$ is torsion-free. Then*

$$Fitt^1_{\mathbb{Z}_p[G_n]}(Sel_S^T(K_n)_p) = Fitt_{\mathbb{Z}_p[G_n]}((\mathcal{O}_{K_n,S,T}^\times / < c_T > \otimes \mathbb{Z}_p)^\vee)$$

where $c_T = (1 - \zeta_{p^{n+1}})^{\delta_T}$ *where* $\delta_T = \prod_{\ell \in T}(1 - \ell\sigma_\ell^{-1}) \in \mathbb{Z}_p[G_{n+1}]$.

Here, c_T is actually the cyclotomic unit in this setting. So, it does turn out to be of the form units modulo cyclotomic units.

In fact, this is just a very particular case of the actual theorem that Burns, Kurihara and Sano proved. Let K/k be any abelian extension of number fields with Galois group G. Then, under the assumption that the Equivariant Tamagawa Number Conjecture holds, they give an explicit description of the higher Fitting ideals of the Selmer module in terms of Rubin-Stark units. For an excellent exposition on this, see [20].

This connection between Rubin-Stark units and the class group is expected, as Rubin-Stark units are made up of S-units and tell us information about special values of L-functions. It would be a good project to convert this general Theorem of Burns-Kurihara-Sano to an Equivariant Main Conjecture-like statement (assuming that the Rubin-Stark conjecture holds).

Chapter 3

Euler factors of Drinfeld modules

3.1 The statement of the problem

Let p be a prime number and let q be a power of p. In what follows, $k := \mathbb{F}_q(t)$ denotes the rational function field in one variable over $\mathbb{F}_q$. For any commutative $\mathbb{F}_q$-algebra R, we denote by τ the q-power Frobenius endomorphism of R. We denote by $R\{\tau\}$ the twisted polynomial ring in τ, with the property that

$$\tau \cdot x = x^q \cdot \tau \quad \forall \;\; x \in R.$$

Let F be a finite, separable extension of $\mathbb{F}_q(t)$ and let K be a finite abelian extension of F with Galois group G. We also assume that the field of constants in K is $\mathbb{F}_q$, i.e.

$$K \cap \overline{\mathbb{F}}_q = \mathbb{F}_q$$

Let us denote $\mathbb{F}_q[t]$ by A. Note that if v denotes an arbitrary normalized valuation on $\mathbb{F}_q(t)$ and ∞ denotes the normalized valuation of uniformizer $1/t$, then

$$A = \{a \in \mathbb{F}_q(t) \,\big|\, v(a) \geq 0, \text{ for all } \;\; v \neq \infty\}.$$

Let $\mathcal{O}_F$ and $\mathcal{O}_K$ denote the integral closures of A in F and K, respectively. In what follows, we abuse notation and use the same letter for normalized valuations and the associated maximal ideals of elements of strictly positive valuation.

Next, we consider a Drinfeld module E of rank $r \in \mathbb{N}$ defined on A with values in $\mathcal{O}_F\{\tau\}$. More precisely, E is given by an $\mathbb{F}_q$-algebra morphism

$$\phi_E : A \to \mathcal{O}_F\{\tau\}, \qquad t \mapsto t \cdot \tau^0 + e_1\tau + \cdots + e_r \cdot \tau^r,$$

where $a_i \in \mathcal{O}_F$, for all i and $e_r \neq 0$. This gives rise to a functor

$$E : (\mathcal{O}_F\{\tau\}[G] - \text{modules}) \to (A[G] - \text{modules}).$$

In other words, for any $\mathcal{O}_F\{\tau\}[G]$-module M, we denote by $E(M)$ the $A[G]$–module whose underlying $\mathbb{F}_q[G]$–module is M and the A-action is given by

$$t \star m = \phi_E(t) \cdot m = t \cdot m + e_1\tau \cdot m + \cdots + e_r\tau^r \cdot m.$$

Let $v_0 \in \mathrm{MSpec}(A)$ and let A_{v_0} and k_{v_0} denote the completions of A and k with respect to the valuation v_0. For all $n \in \mathbb{N}$, we denote by $E[v_0^n]$ the A_{v_0}-module of v_0^n-torsion points of E, i.e.

$$E[v_0^n] = \{x \in E(\overline{F}) | f \star x = 0, \text{ for all } f \in v_0^n\}.$$

The v_0-adic Tate module of E is defined as

$$T_{v_0}(E) = \mathrm{Hom}_{A_{v_0}}(k_{v_0}/A_{v_0}, E[v_0^\infty]).$$

Since A is a PID, we also have

$$T_{v_0}(E) = \varprojlim E[v_0^n],$$

where the transition maps in the projective limit are given by multiplication with a generator of v_0, while $E[v_0^\infty] = \bigcup_{n\geq 1} E[v_0^n]$. Recall that $E[v_0^n]$ and $T_{v_0}(E)$ are free modules of rank r over A/v_0^n and A_{v_0}, respectively, and are endowed with obvious

A_{v_0}-linear, continuous G_F-actions, where $G_F = Gal(\overline{F}/F)$.

Let $v \in \mathrm{MSpec}(\mathcal{O}_F)$, such that $v \nmid v_0$. Fix a choice of decomposition group $G(v) \subset G_F$, and a Frobenius morphism $\sigma(v) \in G(v)$. Then, it is known (see [6] and the references therein) that if E has good reduction at v (i.e. $v \nmid e_r$), the G_F-representation $T_{v_0}(E)$ is unramified at v and the polynomial

$$P_v(X) = \det_{A_{v_0}}(X \cdot I_r - \sigma(v)|T_{v_0}(E))$$

is independent of v_0 and actually lies in $A[X]$. Above, I_r denotes the $r \times r$ identity matrix.

Definition 3.1.1. Let M be an $A[G]$-module which is free of rank m as an $\mathbb{F}_q[G]$-module. Then it is known (see [6] Proposition A.4.1) that the Fitting ideal $\mathrm{Fitt}^0_{A[G]}(M)$ is principal and has a unique t–monic generator $f_M(t) \in A[G] = \mathbb{F}_q[G][t]$ of degree m. We denote this generator by $|M|_G$, i.e.

$$|M|_G = f_M(t) \in \mathbb{F}_q[G][t].$$

The following is Proposition A5.1. from the Appendix in [6]:

Proposition 3.1.2. *Assume that v is tamely ramified in K/F and let E be any Drinfeld module as above. Let w_0 denote the prime in A sitting below v and let $f(v/w_0) = [\mathcal{O}_F/v : A/w_0]$. Then the following hold:*

1. *The $\mathbb{F}_q[G]$-modules $\mathcal{O}_K/v$ and $E(\mathcal{O}_K/v)$ are free of rank $n_v = [\mathcal{O}_F/v : \mathbb{F}_q]$ and therefore $|\mathcal{O}_K/v|_G$ and $|E(\mathcal{O}_K/v)|_G$ are monic polynomials of t–degree n_v.*

2. *We have an equality*

$$|\mathcal{O}_K/v|_G = Nv$$

where Nv denotes the unique monic generator of $w_0^{f(v/w_0)}$ and $f(v/w_0) := [\mathcal{O}_F/v : A/w_0]$.

Let $I_v \subset G_v \subset G$ denote the inertia and decomposition groups of v in G, respectively. Let σ_v be the image of $\sigma(v)$ via the Galois restriction map $G(v) \twoheadrightarrow G_v$. Our goal in this chapter is the proof of the following.

Theorem 3.1.3. *Assume that $v \in \mathrm{MSpec}(\mathcal{O}_F)$ is tamely ramified in K/F and that E has good reduction at v. Then, we have an equality in $\mathbb{F}_q[G][[1/t]]$*

$$\frac{P_v(\sigma_v e_v)}{P_v(0)} = \frac{|E(\mathcal{O}_K/v)|_G}{|\mathcal{O}_K/v|_G},$$

where $e_v = \frac{1}{|I_v|}\sum_{\sigma\in I_v}\sigma$ is the idempotent of the trivial character of I_v in $A[G]$.

A proof of the above statement in the case where E is the Carlitz module C, defined by $\phi_C(t) = t + \tau$, was given in the Appendix of [6]. Below, we develop techniques which settle the above theorem for a general Drinfeld module E.

In the introduction, we had introduced the Euler Proposition 1.2(2) gives us a good understanding of $|\mathcal{O}_K/v|_G$. Therefore a major portion of our work is directed towards understanding the relation between $|E(\mathcal{O}_K/v)|_G$ and $P_v(\sigma_v e_v)$.

3.2 Reduction of $E \mod v$

In this section, we fix a prime $v \in \mathrm{MSpec}(\mathcal{O}_F)$ such that E has good reduction at v. We are not assuming that v is necessarily tamely ramified in K/F. Let us denote by w_0 the prime in A that lies below v. After reduction of $E \mod v$, we obtain the rank r Drinfeld module $\overline{E}$, given by the $\mathbb{F}_q$-algebra morphism

$$\phi_{\overline{E}} : A \to \mathcal{O}_F/v\{\tau\}$$

where $\phi_{\overline{E}}(t) = i(t)\cdot\tau^0 + ... + i(e_r)\cdot\tau^r$ with $i : A \to \mathcal{O}_F \twoheadrightarrow \mathcal{O}_F/v$ being the obvious map. Recall that, by the notation introduced above, we have a field isomorphism

$\mathcal{O}_F/v \simeq \mathbb{F}_{q^{n_v}}$.

Next, we fix $v_0 \in \mathrm{MSpec}(A)$, $v_0 \neq w_0$ and consider the characteristic polynomial of the action of the q^{n_v}-power Frobenius morphism on the free A_{v_0}–module $T_{v_0}(\overline{E})$ of rank r:

$$f_{\overline{E}}(X) = \det_{A_{v_0}}(X \cdot I_r - \mathrm{Frob}_{q^{n_v}} \mid T_{v_0}(\overline{E})).$$

Then, $f_{\overline{E}}(X)$ is independent of v_0 and lies in $A[X]$. (See §4.12 in [10].) By Theorem 4.12.15 in [10] and the discussion preceding that, we have the following.

Proposition 3.2.1. *Any root α of $f_{\overline{E}}$ satisfies the following properties:*

1. *$w(\alpha) = 0$ for all finite places w of $\mathbb{F}_q(t)(\alpha)$, except for exactly one place above w_0.*
2. *There is only one place of $\mathbb{F}_q(t)(\alpha)$ lying above ∞.*
3. *$|\alpha|_\infty = q^{\frac{n_v}{r}}$ where $|.|_\infty$ denotes the unique extension to $\mathbb{F}_q(t)(\alpha)$ of the normalized absolute value of $\mathbb{F}_q(t)$ corresponding to ∞.*
4. *$[\mathbb{F}_q(t)(\alpha) : \mathbb{F}_q(t)]$ divides r.*

Let $\mathcal{O}_v$ and F_v be the completions at v of $\mathcal{O}_F$ and F, respectively. Our choice of decomposition group $G(v)$ corresponds to choosing an embedding $\overline{F} \to \overline{F_v}$ at the level of separable closures of F and F_v, such that Galois restriction induces a group isomorphism $G(\overline{F_v}/F_v) \simeq G(v)$. Since E has good reduction at v and the Galois representations $E[v_0^n]$ are unramified at v, it is not difficult to see that we have

$$E[v_0^n] \subseteq \mathcal{O}_v^{unr}, \text{ for all } n \geq 1,$$

where $\mathcal{O}_v^{unr}$ is the integral closure of $\mathcal{O}_v$ in the maximal unramified extension F_v^{unr} of F_v in $\overline{F_v}$. Moreover, the reduction $\mod v$ map induces isomorphisms of $A_{v_0}[[\overline{G(v)}]]$–modules

$$E[v_0^n] \simeq \overline{E}[v_0^n], \qquad T_{v_0}(E) \simeq T_{v_0}(\overline{E}), \tag{3.2.2}$$

where

$$\overline{G(v)} := G(v)/I(v) \simeq G(\overline{\mathbb{F}_{q^{n_v}}}/\mathbb{F}_{q^{n_v}}).$$

The group isomorphism above sends $\overline{\sigma(v)}$ (the image of our choice of Frobenius $\sigma(v)$ in $\overline{G(v)}$) to $\mathrm{Frob}_{q^{n_v}}$. Consequently, we have an equality of characteristic polynomials in $A[X]$:

$$f_{\overline{E}}(X) = P_v(X). \tag{3.2.3}$$

Consequently, Proposition 3.2.1 gives us information on the roots of the characteristic polynomial $P_v(X)$. The following corollary regarding the coefficients of $P_v(X)$ will be particularly useful in what follows.

Corollary 3.2.4. *Let $P_v(X) = a_0 + a_1 X + \cdots + a_{r-1}X^{r-1} + X^r$, with $a_0, \ldots, a_{r-1} \in A$. Then, we have*

1. $\deg_t(a_0) = n_v$ *and* $0 < \deg_t(a_i) < n_v$, *for all* $i > 0$.
2. $P_v(X) \in \mathbb{F}_q[X][t]$ *is a polynomial of degree* n_v *in* t *with the same leading coefficient as* a_0.
3. $a_0 = \rho \cdot Nv$, *for some* $\rho \in \mathbb{F}_q^\times$, *where* Nv *is the unique monic generator of* $w_0^{f(v/w_0)}$.

Above, $\deg_t(*)$ *denotes the degree in* t *of a polynomial in* $A = \mathbb{F}_q[t]$.

Proof. Let $\alpha_1, ..., \alpha_r \in \overline{A}$ denote the roots of $P_v(X)$ in the integral closure of A. Then

$$\begin{aligned} P_v(X) = \prod_{i=1}^r (X - \alpha_i) &= (-1)^r \prod_{i=1}^r \alpha_i + (-1)^{r-1} \left(\sum_{j=1}^r \prod_{i \neq j} \alpha_i \right) X + ... + X^r \\ &= a_0 + a_1 \cdot X + \cdots + a_{r-1} \cdot X^{r-1} + X^r. \end{aligned}$$

Let $|\cdot|_\infty$ denote an extension to $\mathbb{F}_q(t)(\alpha_1, ..., \alpha_r)$ of the normalized absolute value of $\mathbb{F}_q(t)$ corresponding to ∞ (also denoted by $|\cdot|_\infty$ below.) By Proposition 1.4, we have $|\alpha_i|_\infty = q^{\frac{n_v}{r}}$, for all i. Therefore, we have

$$|a_0|_\infty = \left| \prod_{i=1}^r \alpha_i \right|_\infty = q^{n_v}, \qquad \deg_t(a_0) = \log_q(|a_0|_\infty) = n_v.$$

Furthermore, since $|\cdot|_\infty$ is non-archimedean, we have

$$|a_i|_\infty \leq q^{n_v \cdot \frac{r-i}{r}}, \qquad \deg_t(a_i) = \log_q(|a_i|_\infty) \leq n_v \cdot \frac{r-i}{r} < n_v, \qquad \text{for all } i \geq 1.$$

This concludes the proof of part (1).

Part (2) is a direct consequence of part (1). $\square$

Next, we state a general commutative algebra result regarding Fitting ideals of modules over certain rings of equivariant Iwasawa algebra type. For a proof of this result, see Proposition 4.1 in [14].

Proposition 3.2.5 (Greither–Popescu)**.** *Let R be a semi-local, compact topological ring, and let Γ be a pro-cyclic group, topologically generated by γ. Suppose that M is an $R[[\Gamma]]$–module which is free of rank n as an R–module. Let $M_\gamma \in M_n(R)$ denote the matrix of the action of γ on some R-basis of M. Then, we have an equality of $R[[\Gamma]]$–ideals*

$$\mathrm{Fitt}_{R[[\Gamma]]}(M) = \left(\det_R(X \cdot I_n - M_\gamma)\Big|_{X=\gamma}\right)$$

An immediate consequence of the above proposition is the following.

Corollary 3.2.6. *With notations as above, we have the following equalities of $A_{v_0}[[\overline{G(v)}]]$–ideals.*

$$\mathrm{Fitt}_{A_{v_0}[[\overline{G(v)}]]}(T_{v_0}(\overline{E})) = \mathrm{Fitt}_{A_{v_0}[[\overline{G(v)}]]}(T_{v_0}(E))$$
$$= \left(\det_{A_{v_0}}(X \cdot I_r - \overline{\sigma(v)} \mid T_{v_0}(E))\Big|_{X=\overline{\sigma(v)}}\right) = (P_v(\overline{\sigma(v)}))$$

for $v_0 \neq w_0$.

Proof. Apply the proposition above to $R := A_{v_0}$, $\Gamma := \overline{G(v)}$, $\gamma := \overline{\sigma(v)}$ and the module

$$M := T_{v_0}(E) \simeq T_{v_0}(\overline{E}),$$

which is A_{v_0}–free of rank r. $\square$

Next, we fix a prime $w \in \mathrm{MSpec}(\mathcal{O}_K)$ lying above v. We let $G(w) = G(v) \cap G_K$, $I(w) = I(v) \cap G_K$ and $\sigma(w) := \sigma(v)^f$, where $f := f(w/v) = [\mathcal{O}_K/w : \mathcal{O}_F/v]$. Then, $\sigma(w) \in G(w)$ is a choice of Frobenius for w and its image $\overline{\sigma(w)} \in \overline{G(w)} := G(w)/I(w)$ corresponds via the group isomorphism $\overline{G(w)} \simeq G_{\mathcal{O}_K/w}$ to $\mathrm{Frob}_{q^{fn_v}}$.

Lemma 3.2.7. *With notations as above, we have the following canonical isomorphisms of $A_{v_0}[G_v]$–modules:*

1. $T_{v_0}(\overline{E})/(1 - \overline{\sigma(w)})T_{v_0}(\overline{E}) \simeq \overline{E}(\mathcal{O}_K/w)_{v_0}$

2. $T_{v_0}(E)/(1 - \sigma(w))T_{v_0}(E) \simeq E(\mathcal{O}_K/w)_{v_0}$

where $M_{v_0} := M \otimes_A A_{v_0}$ for any A–module M.

Proof. Obviously, part (2) is a consequence of part (1) via the second isomorphism in (3.2.2) above and the observation that $E(\mathcal{O}_K/w) = \overline{E}(\mathcal{O}_K/w)$, by the definition of $\overline{E}$. In order to prove part (1), apply the functor $* \to \mathrm{Hom}_{A_{v_0}}(*, \overline{E}[v_0^\infty])$ to the exact sequence of A_{v_0}–modules

$$0 \longrightarrow A_{v_0} \longrightarrow k_{v_0} \longrightarrow k_{v_0}/A_{v_0} \longrightarrow 0.$$

Since the A_{v_0}–module $\overline{E}[v_0^\infty]$ is divisible and therefore injective (as A_{v_0} is a PID), the above functor is exact. Therefore, we obtain the following exact sequence of $A_{v_0}[\overline{G(v)}]$–modules:

$$0 \longrightarrow T_{v_0}(\overline{E}) \longrightarrow \mathrm{Hom}_{A_{v_0}}(k_{v_0}, \overline{E}[v_0^\infty]) \longrightarrow \overline{E}[v_0^\infty] \longrightarrow 0. \tag{3.2.8}$$

Now, it is easy to see that one has an isomorphism of $k_{v_0}[\overline{G(v)}]$–modules

$$k_{v_0} \otimes_{A_{v_0}} T_{v_0}(\overline{E}) \simeq \mathrm{Hom}_{A_{v_0}}(k_{v_0}, \overline{E}[v_0^\infty]), \quad \xi \otimes \phi \to (x \to \phi(\widehat{\xi \cdot x})),$$

for all $\xi, x \in k_{v_0}$ and all $\phi \in T_{v_0}(\overline{E}) = \mathrm{Hom}_{A_{v_0}}(k_{v_0}/A_{v_0}, \overline{E}[v_0^\infty])$, where $\widehat{x \cdot \xi}$ is the class of $x \cdot \xi$ in k_{v_0}/A_{v_0}.

Now, Proposition 3.2.1(3) shows that the eigenvalues of $\overline{\sigma(w)} = \overline{\sigma(v)}^f = (\mathrm{Frob}_{q^{n_v}})^f$ acting on the k_{v_0}–vector space $k_{v_0} \otimes_{A_{v_0}} T_{v_0}(\overline{E})$ are all different from 1. Consequently, $(\overline{\sigma(w)} - 1)$ is an automorphism of this k_{v_0}–vector space. Consequently, when one takes the $\overline{\sigma(w)}$–invariants and coinvariants in the exact sequence (3.2.8) above, one obtains an isomorphism of $A_{v_0}[G_v]$–modules

$$T_{v_0}(\overline{E})/(1 - \overline{\sigma(w)})T_{v_0}(\overline{E}) \simeq \overline{E}[v_0^\infty]^{\overline{\sigma(w)}=1} = \overline{E}(\mathcal{O}_K/w)_{v_0},$$

which concludes the proof of the Lemma.

$\square$

Corollary 3.2.9. *With notations as above, the following equality of $A_{(v_0)}[G]$–ideals holds:*

$$\mathrm{Fitt}_{A_{(v_0)}[\overline{G_v}]} E(\mathcal{O}_K/w)_{v_0} = \big(P_v(\overline{\sigma_v})\big),$$

for all $v_0 \in \mathrm{MSpec}(A)$, with $v_0 \neq w_0$. Here, $\overline{G}_v := G_v/I_v$, $\overline{\sigma}_v$ is the image of σ_v in $\overline{G_v}$, and $A_{(v_0)}$ is the localization of A at v_0.

Proof. First, note that since $I(v)$ acts trivially on $T_{v_0}(E)$, the isomorphism of $A_{v_0}[G_v]$–modules in Lemma 3.2.7(2) can be rewritten as an isomorphism of $A_{v_0}[\overline{G_v}]$–modules

$$T_{v_0}(E) \otimes_{A_{v_0}[[\overline{G(v)}]]} A_{v_0}[\overline{G(v)}] \simeq E(\mathcal{O}_K/w)_{v_0},$$

where the ring morphism $\pi : A_{v_0}[[\overline{G(v)}]] \twoheadrightarrow A_{v_0}[\overline{G_v}]$ is the A_{v_0}–linear map given by Galois restriction, which maps $\overline{\sigma(v)} \to \overline{\sigma_v}$. The isomorphism above permits us to apply the well known base–change property of Fitting ideals and conclude that we have equalities of $A_{v_0}[\overline{G_v}]$–ideals

$$\mathrm{Fitt}_{A_{v_0}[\overline{G_v}]} E(\mathcal{O}_K/w)_{v_0} = \pi\big(\mathrm{Fitt}_{A_{v_0}[[\overline{G(v)}]]}(T_{v_0}(E))\big) = \big(\pi(P_v(\overline{\sigma(v)})\big) = \big(P_v(\overline{\sigma_v})\big),$$

where the first equality is base–change and the second equality is Corollary 3.2.6 above. Next, observe that since $E(\mathcal{O}_K/w)$ is finite (and therefore A–torsion), we have isomorphisms

$$E(\mathcal{O}_K/w)\otimes_A A_{(v_0)} \simeq \big(E(\mathcal{O}_K/w)\otimes_A A_{(v_0)}\big)\otimes_{A_{(v_0)}} A_{v_0} \simeq E(\mathcal{O}_K/w)_{v_0}.$$

Consequently, base–change for Fitting ideals applied to the ring extension $A_{(v_0)}[G] \subseteq A_{v_0}[G]$ and the last equality of ideals displayed above gives

$$P_v(\overline{\sigma_v})A_{v_0}[G] = \mathrm{Fitt}_{A_{(v_0)}[\overline{G_v}]}\big(E(\mathcal{O}_K/w)_{v_0}\big)A_{v_0}[\overline{G_v}].$$

However, since the ring extension $A_{(v_0)}[G] \subseteq A_{v_0}[G]$ is faithfully flat (because $A_{(v_0)} \subseteq A_{v_0}$ is), we have

$$\begin{aligned}\mathrm{Fitt}_{A_{(v_0)}[\overline{G_v}]}\big(E(\mathcal{O}_K/w)_{v_0}\big) &= \mathrm{Fitt}_{A_{(v_0)}[\overline{G_v}]}\big(E(\mathcal{O}_K/w)_{v_0}\big)A_{v_0}[\overline{G_v}] \cap A_{(v_0)}[\overline{G_v}]\\ &= P_v(\overline{\sigma_v})A_{v_0}[\overline{G_v}] \cap A_{(v_0)}[\overline{G_v}] = P_v(\overline{\sigma_v})A_{(v_0)}[\overline{G_v}].\end{aligned}$$

Above, we used the fact that if $R \subseteq R'$ is a faithfully flat extension of commutative rings and I is an ideal in R, then $IR' \cap R = I$. (See [23], Chapter 2, Section 4, 4.C(ii).) □

In the next 4 sections, we provide a proof of Theorem 3.1.3. We treat first the unramified case.

3.3 The unramified case

We keep the notations and assumptions of the previous section. In addition, we assume that the prime v is unramified in K/F. Consequently, we have $\overline{G_v} = G_v$ and $\overline{\sigma_v} = \sigma_v$ throughout.

Lemma 3.3.1. *Under the current assumptions, we have an equality of $A_{(v_0)}[G]$–ideals*

$$\mathrm{Fitt}_{A_{(v_0)}[G]}(E(\mathcal{O}_K/v)_{v_0}) = (P_v(\sigma_v)),$$

for all $v_0 \in \mathrm{MSpec}(A)$, with $v_0 \neq w_0$.

Proof. In this case, we have an isomorphism of $A_{(v_0)}[G]$–modules

$$E(\mathcal{O}_K/v)_{v_0} \simeq E(\mathcal{O}_K/w)_{v_0} \otimes_{A_{(v_0)}[G_v]} A_{(v_0)}[G],$$

for all $v_0 \in \mathrm{MSpec}(A)$. (See the Appendix of [6].) Therefore, the equality in the Lemma follows from Corollary 3.2.9 and the base–change property of Fitting ideals. □

Proposition 3.3.2. *Assume that v is unramified in K/F. let $\rho \in \mathbb{F}_q^\times$ as defined in Corollary 3.2.4(3). Then,*

$$\rho^{-1}P_v(\sigma_v) = |E(\mathcal{O}_K/v)|_G.$$

The proof of this statement will occupy § 3.6?

Assuming that 3.3.2 above holds, we now have our main result:

Proposition 3.3.3. *Under the same conditions as in 3.3.2, the following hold.*

1. $\rho^{-1}P_v(0) = |\mathcal{O}_K/v|_G$.
2. $P_v(\sigma_v)/P_v(0) = |E(\mathcal{O}_K/v)|_G/|\mathcal{O}_K/v|_G$ *in* $\mathbb{F}_q[G][[t]]$, *i.e. Theorem 3.1.3 holds.*

Proof. According to Corollary 3.2.4 (see (1) and (3) in loc.cit.), $P_v(0) \in \mathbb{F}_q[t]$ and $P_v(X) \in \mathbb{F}_q[X][t] = A[X]$, viewed as polynomials in t, have degrees equal to n_v and leading coefficients equal to ρ. Therefore, $\rho^{-1}P_v(0)$ and $\rho^{-1}P_v(\sigma_v)$ are indeed monic polynomials of common t–degree n_v. Further, Corollary 3.2.4(3) shows that $\rho^{-1}P_v(0) = Nv$ which, if combined to Proposition 3.1.2(2), proves part (1) of the statement above.

Part (2) is a direct consequence of parts (1) and 3.3.2. □

Remark 3.3.4. Note that since Corollary 3.2.4 is valid in general, regardless of the ramification status of v in K/F, the polynomials $\rho^{-1}P_v(X)$ and $\rho^{-1}P_v(0)$ are monic of degree n_v in t in general. Consequently, the proof given to part (1) of the Proposition above is valid in general. Also, $\rho^{-1}P_v(e_v\sigma_v) \in A[G]$ is a monic polynomial in t of degree n_v even in the tamely ramified case.

3.4 Proof of Proposition 3.3.2

We adopt the same notation that we used in 3.3.2 and § 3.3. In order to simplify the notation, let

$$f := \rho^{-1}P_v(\sigma_v), \qquad g := \left|E(\mathcal{O}_K/v)\right|_G.$$

Then, f and g are both monic polynomials in t, of degrees equal to n_v. (See Proposition 3.1.2(2) and Corollary 3.2.4.) Further, Lemma 3.3.1 and the definition of g imply that they satisfy the following equalities

$$fA_{(v_0)}[G] = gA_{(v_0)}[G] = \mathrm{Fitt}_{A_{(v_0)}[G]}E(\mathcal{O}_K/v)_{v_0}, \quad \text{for all } v_0 \in \mathrm{MSpec}(A) \smallsetminus \{w_0\}.$$

Now, it is easy to check that the total ring of fractions of $A[G]$ is $k[G]$. Since g and f are monic, they are not zero–divisors in $A[G]$ and $k[G]$. Therefore, the equalities above imply that

$$\frac{g}{f} \in k[G] \cap \Big(\bigcap_{v_0 \neq w_0} A_{(v_0)}[G]^\times \Big).$$

This implies that there exists $\xi \in A[G]$ and $m \in \mathbb{Z}_{\geq 0}$, such that

$$\frac{g}{f} = \frac{\xi}{\pi_{w_0}^m}, \qquad \text{with } \pi_{w_0} \nmid \xi \text{ in } A[G] \text{ if } m \geq 1,$$

where π_{w_0} is the unique monic generator of the maximal ideal w_0. We claim that it suffices to show that $m = 0$. If $m = 0$, we have

$$g = \xi \cdot f, \qquad \text{with } \xi \in A[G].$$

However, since f and g are monic of the same degree in t, the element ξ is monic of degree 0 in t, and therefore $\xi = 1$. Therefore, $f = g$, which would conclude the proof of part (2) of the Proposition above.

Suppose $m > 0$. Then a reduction modulo w_0 ($A[G] \to A/w_0[G]$, sending $x \to \overline{x}$) gives the following equality

$$\overline{f} \cdot \overline{\xi} = 0 \quad \text{ in } A/w_0[G].$$

If $\overline{f}$ is a non-zero divisor, we reach a contradiction as $\pi_{w_0} \nmid \xi$ in $A[G]$ and hence $\overline{\xi} \neq 0$ in $A/w_0[G]$. This is true if $r = 1$, as then $\overline{f} = \rho^{-1}\sigma_v$, which is a unit in $A/w_0[G]$. Unfortunately, this is not always true for $r > 1$, but this argument does work in certain situations, and so we'll just state it here.

Repeating the same argument above, we can find a $\xi' \in A[G]$ and $n \in \mathbb{Z}_{\geq 0}$ such that

$$\frac{f}{g} = \frac{\xi'}{\pi_{w_0}^n}, \qquad \text{with } \pi_{w_0} \nmid \xi' \text{ in } A[G] \text{ if } n \geq 1.$$

Obviously, we also expect $n = 0$ and $\xi' = 1$. So, if $\overline{g}$ is a non-zero divisor in $A/w_0[G]$, then we are done again. In other words, we get that $\overline{g}$ is a non-zero divisor iff $\overline{f}$ is a non-zero divisor.

Let us see what it means for $\overline{g}$ and $\overline{f}$ to be non-zero divisors. Reduction modulo w_0 gives us

$$(\overline{g}) = \mathrm{Fitt}_{A/w_0[G_v]}(E(\mathcal{O}_K/w)/w_0).$$

Let $s : A/w_0[G_v] \to A/w_0$ denote the augmentation map obtained by mapping $\sigma \in G_v$ to $1 \in A/w_0$. So we get

$$(s(\overline{g})) = \mathrm{Fitt}_{A/w_0}(E(\mathcal{O}_K/w)/(w_0, \sigma_v - 1)) = \mathrm{Fitt}_{A/w_0}(E(\mathcal{O}_F/v)/w_0).$$

Note that $\overline{g}$ is a non-zero divisor iff $s(\overline{g}) \neq 0$, which happens iff $E(\mathcal{O}_F/v)/w_0 = 0$, i.e. $E(\mathcal{O}_F/v)[w_0] = 0$.

On the other hand,

$$\overline{f} = \rho^{-1}\overline{P_v(\sigma_v)}.$$

As above, $\overline{f}$ is a non-zero divisor iff $s(\overline{f}) \neq 0$, i.e. $\overline{P_v(1)} \neq 0$. Since $P_v(X) = (X - \alpha_1)\dots(X - \alpha_r)$ where α_i's are as in 3.2.4, we can conclude that $\overline{P_v(1)}$ is a non-zero divisor iff none of the α_i's are congruent to 1 modulo any prime in $\mathbb{F}_q(t)(\alpha_i)$ above w_0.

Remark 3.4.1. Of course, the proof of our main Proposition is not yet complete, but we'll take a break here to say that this much enough to prove the theorem in a very important special case: the case of primes of supersingular reduction. A prime v in $\mathrm{MSpec}(\mathcal{O}_\mathrm{F})$ for which E has good reduction $\mod v$ is said to be of supersingular reduction if the reduced Drinfeld module $\overline{E}$ satisfies the following condition:

$$\overline{E}(\overline{\mathcal{O}_F/v})[w_0] = 0$$

where $w_0 \in \mathrm{MSpec(A)}$ with $v|w_0$. An equivalent definition is the statement that there exists only one prime above w_0 in $\mathbb{F}_q(t)(\alpha)$ for any root α of $P_v(X)$. The first definition implies that $\overline{g}$ is a non-zero divisor if v is of supersingular reduction, while the second definition implies that $\overline{f}$ is a non-zero divisor in the same situation. Either way, for supersingular primes v, the Proposition has been proved. It is worth mentioning here that the topic of supersingular primes brings up a key difference between the theory of elliptic curves and the theory of Drinfeld modules. Poonen ([26]) has shown that it is possible to construct Drinfeld modules with no supersingular primes while it is known, due to Elkies([5]), that elliptic curves over $\mathbb{Q}$ have infinitely many supersingular primes.

We come back to the proof of the Proposition.

Let $T_{w_0}(\overline{E})$ denote the w_0-adic Tate module associated to $\overline{E}$. It is a free A_{w_0}-

module of rank $r' = r - h$ where h denotes the height of $\overline{E}$. Then we can look at

$$g_{\overline{E}}(X) := \det_{A_{w_0}}(X.I_{r'} - \mathrm{Frob}_{q^{d_0}}|T_{w_0}(\overline{E})) \in A_{w_0}[X].$$

Recall that there exists $\xi' \in A[G]$ and $n \in \mathbb{Z}_{\geq 0}$, such that

$$\frac{f}{g} = \frac{\xi'}{\pi_{w_0}^n}, \qquad \text{with } \pi_{w_0} \nmid \xi' \text{ in } A[G] \text{ if } n \geq 1,$$

where π_{w_0} is the unique monic generator of the maximal ideal w_0.

By 3.2.7 Part 1 and a proof very similar to that of 3.2.6, we have

$$(g) = \mathrm{Fitt}_{A_{w_0}[G]}(\overline{E}(\mathcal{O}_K/v)_{w_0}) = (g_{\overline{E}}(\sigma_v)).$$

If we prove that $g_{\overline{E}}$ divides $f_{\overline{E}}$ in $A_{w_0}[X]$, then this shows that g divides f in $A_{w_0}[G]$. Hence, this shows that $\frac{\xi'}{\pi_{w_0}^n} \in A_{w_0}[G]$, which shows that $n = 0$ and by our discussion above, this shows that we have $f = g$. So we are done with the proof once we show that $g_{\overline{E}}$ divides $f_{\overline{E}}$ in $A_{w_0}[X]$.

Since $\phi_{\overline{E}} : A \to \mathbb{F}_q\{\tau\}$ is an injection ([10] 4.5.2), we can consider A as being embedded in $\mathbb{F}_q\{\tau\}$. This can be extended to get an embedding of k in $\mathbb{F}_q(\tau)$, the division ring of fractions of $\mathbb{F}_q\{\tau\}$. Let $\mathcal{F} := \tau^{d_0} = \mathrm{Frob}_{q^{d_0}}$. Using this embedding, we can consider the field extension $k(\mathcal{F})/k$.

We first state the following Theorem due to Gekeler:([9], [10] 4.12.8):

Theorem 3.4.2. *1. There is a unique place v_ϕ of $k(\mathcal{F})$ such that $v_\phi(\mathcal{F}) > 0$. The place v_ϕ lies above w_0.*

2. There is a unique place of $k(\mathcal{F})$ over ∞. By abuse of notation, we'll use ∞ for this place too.

3. *In the category of Drinfeld modules up to isogeny,* $T_{v_\phi}(\phi) \otimes_A k = 0$ *and for* $\widetilde{v} \neq v_\phi, \infty$, $T_{\widetilde{v}}(\phi) \otimes_A k$ *is of dimension* t *over* $k(\mathcal{F})_{\widetilde{v}} := \mathcal{O}_{k(\mathcal{F}),\widetilde{v}} \otimes_A k$ *where*

$$t = \frac{r}{[k(\mathcal{F}) : k]}.$$

The third statement above is a bit vague, and we talk a bit about what it means. There exists a Drinfeld module

$$\widetilde{\phi} : \mathcal{O}_{k(\mathcal{F})} \to \mathcal{O}_F/v\{\tau\}$$

such that $\widetilde{\phi}|_A$ is isogenous to $\phi_{\overline{E}}$, and it satisfies the following properties:

- Rank of the Drinfeld module $\widetilde{\phi}$ is t.
- The characteristic of $\widetilde{\phi}$ is v_ϕ, i.e. the kernel of the map

$$\mathcal{O}_{k(F)} \xrightarrow{\phi_{\overline{E}}} \mathcal{O}_F/v\{\tau\} \xrightarrow{ev_0} \mathcal{O}_F/v,$$

  where $ev_0(\tau) = 0$, is v_ϕ.
- $T_{v_\phi}(\widetilde{\phi}) = 0$ and

$$\dim_{\mathcal{O}_{k(\mathcal{F}),\widetilde{v}}}(T_{\widetilde{v}}(\widetilde{\phi})) = t$$

  for all places $\widetilde{v} \neq v_\phi, \infty$.

We have an isomorphism of A_{w_0}-modules:

$$T_{w_0}(\widetilde{\phi}|_A) \simeq \bigoplus_{\widetilde{v}|w_0} T_{\widetilde{v}}(\widetilde{\phi}).$$

Let $m_\phi \in A[X]$ denote the minimal polynomial of $\mathcal{F}$ over A. Then, by 4.12.12.2 in [10], we have

$$P_v(X) = f_{\overline{E}}(X) = m_\phi(X)^t.$$

Now note that, in $A_{w_0}[X]$, we have the decomposition

$$m_\phi = \prod_{\widetilde{v}|w_0} m_{\widetilde{v}}$$

where $m_{\widetilde{v}}$ is of degree $d_{\widetilde{v}} := [\mathcal{O}_{k(\mathcal{F}),\widetilde{v}} : A_{w_0}]$. Here $m_{\widetilde{v}}$ is the minimal polynomial over A_{w_0} of $\mathcal{F} \in \mathcal{O}_{k(\mathcal{F}),\widetilde{v}}$.

Since $\widetilde{\phi}|_A$ is isogenous to ϕ,

$$g_{\overline{E}}(X) = \det_{A_{w_0}}(X.I_{r'} - \mathrm{Frob}_{q^{d_0}}|T_{w_0}(\phi)) = \det_{A_{w_0}}(X.I_{r'} - \mathrm{Frob}_{q^{d_0}}|T_{w_0}(\overline{\phi}|_A)).$$

Since $T_{w_0}(\overline{\phi}|_A))$ splits into the Tate modules for all primes above w_0, we have

$$g_{\overline{E}}(X) = \prod_{\widetilde{v}|w_0} \det_{A_{w_0}}(X.I_{d_{\widetilde{v}}t} - \mathrm{Frob}_{q^{d_0}}|T_{\widetilde{v}}(\widetilde{\phi})).$$

Note that $T_{v_\phi}(\widetilde{\phi}) = 0$, and hence, we have

$$g_{\overline{E}}(X) = \prod_{\widetilde{v}|w_0, \widetilde{v} \neq v_\phi} \det_{A_{w_0}}(X.I_{d_{\widetilde{v}}t} - \mathrm{Frob}_{q^{d_0}}|T_{\widetilde{v}}(\widetilde{\phi})).$$

The endomorphism $\mathrm{Frob}_{q^{d_0}}$ acts as multiplication by $\mathcal{F}$ on $T_{\widetilde{v}}(\widetilde{\phi}) \simeq \mathcal{O}^t_{k(\mathcal{F}),\widetilde{v}}$, and so we get

$$g_{\overline{E}}(X) = \prod_{\widetilde{v}|w_0, \widetilde{v} \neq v_\phi} \det_{A_{w_0}}(X.I_{d_{\widetilde{v}}t} - \mathcal{F}|\mathcal{O}_{k(\mathcal{F}),\widetilde{v}})^t.$$

Obviously $\det_{A_{w_0}}(X.I_{d_{\widetilde{v}}t} - \mathcal{F}|\mathcal{O}_{k(\mathcal{F}),\widetilde{v}}) = m_{\widetilde{v}}$ and hence we have

$$g_{\overline{E}}(X) = \prod_{\widetilde{v}|w_0, \widetilde{v} \neq v_\phi} m^t_{\widetilde{v}},$$

which clearly divides $f_{\widetilde{E}}$ in $A_{w_0}[X]$. This completes the proof.

3.5 A more involved proof: local $\mathbb{F}_q$-shtukas

We continue with the same notation as before, and we still assume that we are in the unramified case. As in the previous section, the goal in this section would be to prove that $g_{\overline{E}}$ divides $f_{\overline{E}}$ in $A_{w_0}[X]$.

Let $L_1 := \mathcal{O}_F/v$ and let $L := \overline{L_1} = \overline{\mathbb{F}_q}$ be a fixed algebraic closure. Let $\mathbb{G}_a$ denote the additive affine line, viewed as a scheme over $\mathrm{Spec}(\mathbb{F}_q)$. We think of $\overline{E}$ as a functor from the category of L_1–algebras to the category of A–modules

$$\overline{E} : [L_1\text{–alg}] \longrightarrow [A\text{–mod}], \qquad L' \to \mathbb{G}_a(L'),$$

where $\mathbb{G}_a(L')$ is endowed with a natural A–module structure via the $\mathbb{F}_q$–algebra (injective) morphism

$$A \xrightarrow{\phi_{\overline{E}}} L_1\{\tau\} \subseteq L'\{\tau\} = \mathrm{End}^{L'}_{\mathbb{F}_q}(\mathbb{G}_a).$$

Definition 3.5.1. As L is a perfect field containing L_1 (the field of definition of $\overline{E}$), we follow loc.cit. and define the t–motive over L associated to E as the left $L\{\tau\} \otimes_{\mathbb{F}_q} A = L\{\tau\}[t]$–module

$$\overline{M}(L) := \mathrm{Hom}^{L}_{\mathbb{F}_q}(\overline{E}(L), \mathbb{G}_a(L)) = L\{\tau\},$$

endowed with the left $L\{\tau\} \otimes_{\mathbb{F}_q} A$–module structure given by

$$(\lambda \otimes a) * \mu := \lambda \circ \mu \circ \phi_{\overline{E}}(a), \qquad \text{for all } \lambda \in L\{\tau\}, a \in A, \mu \in \overline{M}(L).$$

Remark 3.5.2. It is important to note that the $L\{\tau\}[t]$–module $\overline{M}(L)$ has some distinctive properties (see loc. cit. for proofs): First, it is obvious that $\overline{M}(L)$ is a free $L\{\tau\} = (L\{\tau\} \otimes 1)$–module of rank 1 (which is **the dimension** of the t–motive $\overline{M}(L)$) and (less obvious) that it is a free $L[t] = (L \otimes_{\mathbb{F}_q} A)$–module of rank r (which is **the rank** of the t–motive $\overline{M}(L)$.) Second, it is important to note that since L is perfect, $\tau\overline{M}(L)$ is an $L\{\tau\}[t]$–submodule of $\overline{M}(L)$ and, as a consequence of the definition of $\phi_{\overline{E}}$, we have

$$(1 \otimes t - \iota(t) \otimes 1)(\overline{M}(L)/\tau\overline{M}(L)) = 0,$$

where $i : A \to L_1 \subseteq L$ is the obvious $\mathbb{F}_q$–algebra map of kernel w_0.

It is not difficult to check that the evaluation pairing

$$\overline{E}(L) \times \overline{M}(L) \to \mathbb{G}_a(L), \qquad (e, \mu) \to \mu(e)$$

is perfect and leads to an isomorphism of $\mathbb{F}_q$-vector spaces

$$\overline{E}(L) \simeq \mathrm{Hom}_{L\{\tau\}}(\overline{M}(L), \mathbb{G}_a(L)).$$

This can be used to give an isomorphism of A-modules

$$\xi : \overline{E}(L) \simeq \mathrm{Hom}_{L\{\tau\}[t]}(\overline{M}(L), L((t^{-1}))/tL[t]), \qquad e \to \Big[\, \mu \to \overline{\sum_{i\geq 0} \mu(\phi_{\overline{E}}(t^i)(e)) \cdot t^{-i}}\,\Big],$$

where τ acts on $L((t^{-1}))/tL[t]$ by raising the coefficients of the Laurent series in question to the q–th power and $L[t]$ acts via multiplication. This isomorphism can be seen readily by looking at $\overline{M}(L)$ as $L\{\tau\}$ with the action given by

$$(\lambda \otimes a) \star g = \lambda \cdot g \cdot \phi_{\overline{E}}(a).$$

Then, we have an isomorphism

$$\mathrm{Hom}_{L\{\tau\}[t]}(\overline{M}(L), L((t^{-1}))/tL[t]) \to \mathrm{Hom}_{L\{\tau\}}(\overline{M}(L), \mathbb{G}_a(L))$$

given by $\mu \mapsto \overline{\mu}$ where if $\mu(g) = \overline{\sum_{i\geq 0} g_i t^{-i}}$, then $\overline{\mu}(g) = g_0$ for any $g \in L\{\tau\}$. It is worth noting that then, we have

$$\mu(g) = \sum_{i\geq 0} \overline{\mu}(g \cdot \phi_{\overline{E}}(t^i)).t^{-i}.$$

Therefore μ determines $\overline{\mu}$ and vice versa, and it is easy to check that this is an isomorphism.

For every $f \in A$, this leads to a natural isomorphism of A/f–modules

$$\xi[f] : \overline{E}[f] \simeq \mathrm{Hom}_{L\{\tau\}\otimes_{\mathbb{F}_q} A/f}\big(\overline{M}(L)/f,\, L[t]/fL[t]\big),$$

after identifying $L[t]/fL[t] \simeq (L((t^{-1}))/tL[t])[f]$ via the isomorphism $\widehat{\rho} \to \widehat{t\rho/f}$.

Now, we fix an arbitrary $v_0 \in \mathrm{MSpec}(A)$ and let $\pi_{v_0} \in A$ denote the monic generator of v_0. We let

$$A_{v_0}^{nr} := L\widehat{\otimes}_{\mathbb{F}_q} A_{v_0} := \varprojlim_n (L\otimes_{\mathbb{F}_q} A/v_0^n), \qquad \overline{M}(L)_{v_0} := \overline{M}(L)\widehat{\otimes}_A A_{v_0} := \varprojlim_n (\overline{M}(L)\otimes_A A/v_0^n).$$

Note that if $d_{v_0} := [A/v_0 : \mathbb{F}_q]$, then we have natural isomorphisms of topological rings

$$A_{v_0} \simeq \mathbb{F}_{q^{d_{v_0}}}[[\pi_{v_0}]], \qquad A_{v_0}^{nr} \simeq L[[\pi_{v_0}]]^{d_{v_0}}.$$

Further, note that since $\overline{M}(L)$ is a free $(L \otimes_{\mathbb{F}_q} A = L[t])$–module of rank r (see the Remark above), then $\overline{M}(L)_{v_0}$ is a free $A_{v_0}^{nr}$–module of rank r and, consequently, a free $L[[\pi_{v_0}]]$–module of rank rd_{v_0}. In addition, if we view Frob_q as the canonical topological generator of $Gal(L/\mathbb{F}_q) = Gal(A_{v_0}^{nr}/A_{v_0})$, then the free $A_{v_0}^{nr}$–module $\overline{M}(L)_{v_0}$ is endowed with a Frob_q–semilinear endomorphism, abusively denoted τ, and given by

$$\tau := \tau\widehat{\otimes}1 : \overline{M}(L)\widehat{\otimes}_A A_{v_0} \longrightarrow \overline{M}(L)\widehat{\otimes}_A A_{v_0}.$$

The Frob_q-semilinearity arises from the fact that $\tau(b \cdot y) = b^q \cdot \tau(y)$ for all $b \in L$ and $y \in \overline{M}(L)_{w_0}$.

The following definition is an adaptation of the definition of an effective local shtuka by Hartl-Singh ([16] Definition 2.4):

Definition 3.5.3. The data $(\overline{M}(L)_{v_0}, \tau)$ consisting of the free $A_{v_0}^{nr}$–module $\overline{M}(L)_{v_0}$ of rank r together with its Frob_q–semilinear endomorphism τ defined above is called the local $\mathbb{F}_q$–shtuka over L associated to $\overline{E}$ at v_0.

The link between the local shtuka $(\overline{M}(L)_{v_0}, \tau)$ and the Tate module $T_{v_0}(\overline{E})$ is obtained by taking the projective limit as $n \to \infty$ of the isomorphisms $\xi[\pi_{v_0}^n]$ defined above, to get an isomorphism of A_{v_0}–modules

$$\xi_{v_0}^{nr} : T_{v_0}(\overline{E}) \simeq \mathrm{Hom}_{A_{v_0}^{nr}\{\tau\}}(\overline{M}(L)_{v_0}, A_{v_0}^{nr}), \qquad \text{for all } v_0 \in \mathrm{MSpec}(A).$$

The following result is just the direct adaptation of Proposition 2.9 from [16] for our particular case. Note that $L = \overline{\mathbb{F}_q}$ is perfect.

Proposition 3.5.4. *For all $v_0 \in \mathrm{MSpec}(A)$, the local $\mathbb{F}_q$–shtuka $(\overline{M}(L)_{v_0}, \tau)$ over L splits canonically as a direct sum of local $\mathbb{F}_q$–shtukas over L*

$$(\overline{M}(L)_{v_0}, \tau) = (\overline{M}(L)_{v_0}^{\acute{e}t}, \tau) \oplus (\overline{M}(L)_{v_0}^{nil}, \tau),$$

where $\overline{M}(L)_{v_0}^{\acute{e}t}$ is the maximal $A_{v_0}^{nr}\{\tau\}$–submodule of $\overline{M}(L)_{v_0}$ on which the restriction of τ is bijective and $\overline{M}(L)_{v_0}^{nil}$ is the maximal $A_{v_0}^{nr}\{\tau\}$–submodule of $\overline{M}(L)_{v_0}$ on which the restriction of τ is topologically nilpotent (i.e. there exists an $n > 0$ such that $\tau^n(\overline{M}(L)^{nil}) \subseteq \pi_{v_0}\overline{M}(L)^{nil}$.)

Therefore, we have

$$\mathrm{Hom}_{A_{v_0}^{nr}\{\tau\}}(\overline{M}(L)_{v_0}, A_{v_0}^{nr}) = \mathrm{Hom}_{A_{v_0}^{nr}\{\tau\}}(\overline{M}(L)_{v_0}^{\text{ét}}, A_{v_0}^{nr}) \oplus \mathrm{Hom}_{A_{v_0}^{nr}\{\tau\}}(\overline{M}(L)_{v_0}^{nil}, A_{v_0}^{nr}).$$

Since τ is topologically nilpotent on $\overline{M}(L)_{v_0}^{nil}$ and as an isomorphism on $A_{v_0}^{nr}$, we have $\mathrm{Hom}_{A_{v_0}^{nr}\{\tau\}}(\overline{M}(L)_{v_0}^{nil}, A_{v_0}^{nr}) = 0$. Therefore, we have

$$\xi_{v_0}^{nr} : T_{v_0}(\overline{E}) \simeq \mathrm{Hom}_{A_{v_0}^{nr}\{\tau\}}(\overline{M}(L)_{v_0}^{\text{ét}}, A_{v_0}^{nr}).$$

The following lemma is an extension to the case of $\mathrm{GL_n}(A_{v_0}^{nr})$ of Lang's well known theorem on $\mathrm{GL}_n(L)$ (see [21]), and is due to Popescu and Hartl.

Lemma 3.5.5. *Under the above assumptions, the following hold.*

1. *The map $\mathrm{GL}_n(A_{v_0}^{nr}) \to \mathrm{GL_n}(A_{v_0}^{nr})$ taking $X \to \mathrm{Frob}_q(X)^{-1} \cdot X$ is surjective.*

2. *Any free $A_{v_0}^{nr}$–module $\mathcal{M}$ of finite rank n, endowed with a bijective, Frob_q–semilinear endomorphism t satisfies the property that the standard map*

   $$\mathcal{M}^{t=1} \otimes_{A_{v_0}} A_{v_0}^{nr} \to \mathcal{M}, \qquad a \otimes m \to am$$

   is an isomorphism of $A_{v_0}^{nr}$–modules.

Proof. Since we have a ring isomorphism $A_{v_0}^{nr} \simeq L[[\pi_{v_0}]]^{d_{v_0}}$, it suffices to prove part (1) for $\mathrm{GL}_n(L[[\pi_{v_0}]])$. So, given a matrix $A \in \mathrm{GL}_n(L[[\pi_{v_0}]])$, i.e.

$$A = A_0 + A_1 \cdot \pi_{v_0} + \dots, \qquad \text{with } A_0 \in \mathrm{GL}_n(L) \text{ and } A_i \in M_n(L), \text{ for all } i \geq 1,$$

we need to find a matrix $X \in \mathrm{GL}_n(L[[\pi_{v_0}]]$ given by

$$X = X_0 + X_1 \cdot \pi_{v_0} + \dots, \qquad \text{with } X_0 \in \mathrm{GL}_n(L) \text{ and } X_i \in M_n(L), \text{ for all } i \geq 1,$$

such that the matrices X_i satisfy the relations

$$\sum_{i=0}^{m} \mathrm{Frob}_q(X_{m-i}) \cdot A_i = X_m, \qquad \text{for all } m \geq 0.$$

Lang's theorem (see loc.cit.) implies that part (1) is true for $\mathrm{GL}_n(L)$, so we can find a matrix $X_0 \in \mathrm{GL}_n(L)$ satisfying the 0–th relation above. After multiplying the m–th relation above to the right by $A_0^{-1}\mathrm{Frob}_q(X_0)^{-1} = X_0^{-1}$ we obtain the equivalent relation

$$X_m X_0^{-1} = \mathrm{Frob}_q(X_m X_0^{-1}) + \sum_{i \geq 1}^{m} \mathrm{Frob}_q(X_{m-i}) \cdot A_i \cdot X_0^{-1},$$

which consists of one Artin–Schreier equation for each entry of $X_m X_0^{-1}$. Since L is algebraically closed, these equations have solutions. Therefore, inductively, one can find matrices X_m, for all $m \geq 0$, as desired.

Part (2) follows immediately from part (1) in a standard way: take a basis $\overline{e}$ of $\mathcal{M}$ over $A_{v_0}^{nr}$ and let A be the matrix of t in that basis. Let $X \in \mathrm{GL}_n(A_{v_0}^{nr})$ such that $A = \mathrm{Frob}_q(X)^{-1} \cdot X$. Then $\overline{e'} := X \cdot \overline{e}$ is an $A_{v_0}^{nr}$-basis of $\mathcal{M}$ which is contained in $\mathcal{M}^{t=1}$. This concludes the proof. □

By applying the Lemma above to $\mathcal{M} := \overline{M}(L)_{v_0}^{\text{ét}}$ and $t = \tau$, we conclude that we have the following natural isomorphisms of $A_{v_0}^{nr}\{\tau\}$–modules

$$\overline{M}(L)_{v_0}^{\text{ét}} \simeq (\overline{M}(L)_{v_0}^{\text{ét}})^{\tau=1} \otimes_{A_{v_0}} A_{v_0}^{nr}, \qquad \text{for all } v_0 \in \mathrm{MSpec}(A).$$

The above isomorphism leads to a further isomorphism of A_{v_0}–modules

$$\mathrm{Hom}_{A_{v_0}^{nr}\{\tau\}}(\overline{M}(L)_{v_0}^{\text{ét}}, A_{v_0}^{nr}) \simeq \mathrm{Hom}_{A_{v_0}}((\overline{M}(L)_{v_0}^{\text{ét}})^{\tau=1}, A_{v_0}), \qquad \text{for all } v_0 \in \mathrm{MSpec}(A),$$

which, if composed with the map $\xi_{v_0}^{nr}$ gives an isomorphism of A_{v_0}–modules

$$\xi_{v_0} : T_{v_0}(\overline{E}) \simeq \mathrm{Hom}_{A_{v_0}}((\overline{M}(L)_{v_0}^{\text{ét}})^{\tau=1}, A_{v_0}), \qquad \text{for all } v_0 \in \mathrm{MSpec}(A).$$

This prompts the following.

Definition 3.5.6. The first v_0–adic étale cohomolgy group of $\overline{E}$ is defined by

$$\mathrm{H}^1_{\text{ét}}(\overline{E}, A_{v_0}) := (\overline{M}(L)_{v_0}^{\text{ét}})^{\tau=1}, \qquad \text{for all } v_0 \in \mathrm{MSpec}(A).$$

Note that the maps ξ_{v_0} lead to the following A_{v_0}–module isomorphisms.

$$T_{v_0}(\overline{E})^* := \mathrm{Hom}_{A_{v_0}}(T_{v_0}(E), A_{v_0}) \simeq \mathrm{H}^1_{\text{ét}}(\overline{E}, A_{v_0}), \qquad \text{for all } v_0 \in \mathrm{MSpec}(A).$$

Further, the first v_0–adic crystalline cohomology group of $\overline{E}$ is defined by

$$\mathrm{H}^1_{cris}(\overline{E}, A_{v_0}^{nr}) := \overline{M}(L)_{v_0}.$$

Note that for all $v_0 \in \mathrm{MSpec}(A)$ we have isomorphisms and inclusions of $A_{v_0}^{nr}$–modules

$$T_{v_0}(\overline{E})^* \otimes_{A_{v_0}} A_{v_0}^{nr} = \mathrm{H}^1_{\text{ét}}(\overline{E}, A_{v_0}) \otimes_{A_{v_0}} A_{v_0}^{nr} \simeq \mathrm{H}^1_{cris}(\overline{E}, A_{v_0}^{nr})^{\text{ét}} \subseteq \mathrm{H}^1_{cris}(\overline{E}, A_{v_0}^{nr}).$$

The following holds at primes v_0 different from the characteristic of $\overline{E}$. (See [10], Chapter 5 as well.)

Lemma 3.5.7. *If v_0 is an element in $\mathrm{MSpec}(A)$ different from the characteristic w_0 of $\overline{E}$, then*

$$\overline{M}(L)_{v_0}^{\acute{e}t} = \overline{M}(L)_{v_0}, \qquad (\overline{M}(L)_{v_0})^{\tau=1} \otimes_{A_{v_0}} A_{v_0}^{nr} \simeq \overline{M}(L)_{v_0}.$$

In other words, τ is bijective on $\overline{M}(L)_{v_0}$ and we have canonical isomorphisms of $A_{v_0}^{nr}[\tau_1]$–modules

$$T_{v_0}(\overline{E})^* \otimes_{A_{v_0}} A_{v_0}^{nr} \simeq \mathrm{H}^1_{\acute{e}t}(\overline{E}, A_{v_0}) \otimes_{A_{v_0}} A_{v_0}^{nr} \simeq \mathrm{H}^1_{cris}(\overline{E}, A_{v_0}^{nr}).$$

Proof. (sketch) It is easy to show that since $\tau \nmid \phi_{\overline{E}}(\pi_{v_0}^n)$ in $L\{\tau\}$, τ is injective and therefore bijective on the finite dimensional L–vector spaces $\overline{M}(L)/\pi_{v_0}^n$, for all $n \geq 1$. The bijection of τ on $\overline{M}(L)_{v_0}$ is obtained now by taking the projective limit as $n \to \infty$. $\square$

First, take $v_0 \in \mathrm{MSpec}(A) \smallsetminus \{w_0\}$ and observe that, based on the previous Lemma and Definition, we have canonical isomorphisms of $A_{v_0}^{nr}[\tau_1]$–modules

$$T_{v_0}(\overline{E})^* \otimes_{A_{v_0}} A_{v_0}^{nr} \simeq \mathrm{H}^1_{cris}(\overline{E}, A_{v_0}^{nr}) = \overline{M}(L) \widehat{\otimes}_A A_{v_0} \simeq \overline{M}(L) \otimes_{L \otimes_{\mathbb{F}_q} A} (L \widehat{\otimes}_{\mathbb{F}_q} A_{v_0}) \simeq \overline{M}(L) \otimes_{L[t]} A_{v_0}^{nr}.$$

As a consequence, from the definition of $f_{\overline{E}}$, we have

$$f_{\overline{E}}(X) = \det_{A_{v_0}}(XI_r - \tau_1 \mid T_{v_0}(\overline{E})^*) = \det_{A_{v_0}^{nr}}(XI_r - \tau_1 \mid \mathrm{H}^1_{cris}(\overline{E}, A_{v_0}^{nr})) = \det_{L[t]}(XI_r - \tau_1 \mid \overline{M}(L)).$$

The last equality proves that $f_{\overline{E}}(X)$ is independent of v_0 and that it has coefficients in $L[t]$. Further, if one applies the analogues of Lemmas 3.5.5 and 3.5.7 to the finite, étale $\mathbb{F}_q$–shtukas $\overline{M}(L)/{v_0}^n$ over L (see [16]), one concludes that $f_{\overline{E}}(X)$ has coefficients in A_{v_0}. Since $L[t] \cap A_{v_0} = A$ (intersection viewed inside $A_{v_0}^{nr}$), $f_{\overline{E}}(X)$ has coefficients in A, as stated before.

Now, from the definitions, we also have similar natural isomorphisms of $A_{w_0}^{nr}[\tau_1]$–modules

$$\mathrm{H}^1_{cris}(\overline{E}, A_{w_0}^{nr}) = \overline{M}(L) \widehat{\otimes}_A A_{w_0} \simeq \overline{M}(L) \otimes_{L \otimes_{\mathbb{F}_q} A} (L \widehat{\otimes}_{\mathbb{F}_q} A_{w_0}) \simeq \overline{M}(L) \otimes_{L[t]} A_{w_0}^{nr}.$$

Therefore, when combining these with the second note in Definition 3.5.6, we obtain equalities

$$\begin{aligned}
f_{\overline{E}}(X) &= \det_{L[t]}(XI_r - \tau_1 \mid \overline{M}(L)) = \det_{A_{w_0}^{nr}}(XI_r - \tau_1 \mid \overline{M}(L) \otimes_{L[t]} A_{w_0}^{nr}) \\
&= \det_{A_{w_0}^{nr}}(XI_r - \tau_1 \mid \mathrm{H}^1_{cris}(\overline{E}, A_{w_0}^{nr})) \\
&= \det_{A_{w_0}^{nr}}(XI_r - \tau_1 \mid \mathrm{H}^1_{cris}(\overline{E}, A_{w_0}^{nr})^{\text{ét}}) \cdot \det_{A_{w_0}^{nr}}(XI_r - \tau_1 \mid \mathrm{H}^1_{cris}(\overline{E}, A_{w_0}^{nr})^{nil}) \\
&= \det_{A_{w_0}}(XI_{r-h} - \tau_1 \mid T_{w_0}(\overline{E})^*) \cdot \det_{A_{w_0}^{nr}}(XI_r - \tau_1 \mid \mathrm{H}^1_{cris}(\overline{E}, A_{w_0}^{nr})^{nil}) \\
&= g_{\overline{E}}(X) \cdot \det_{A_{w_0}^{nr}}(XI_r - \tau_1 \mid \mathrm{H}^1_{cris}(\overline{E}, A_{w_0}^{nr})^{nil}).
\end{aligned}$$

This shows that $g_{\overline{E}}(X)$ divides $f_{\overline{E}}(X)$ in $A_{w_0}^{nr}[X]$. However, since $g_{\overline{E}}(X), f_{\overline{E}}(X)$ are both in the polynomial ring $A_{w_0}[X] = A_{w_0}^{nr}[X]^{\tau=1}$, this divisibility holds in $A_{w_0}[X]$. This completes the proof.

3.6 The tamely ramified case

Now suppose that v is tamely ramified in K/F. Let $K' = K^{I_v}$ denote the maximal sub-extension of K/F unramified at v. Let w' denote the prime in K' lying below w. As before, we put $g = |E(\mathcal{O}_K/v)|_G$. We have

$$E(\mathcal{O}_K/v) \simeq E(\mathcal{O}_K/w') \bigotimes_{A[G_v]} A[G].$$

Hence, we have

$$g = |E(\mathcal{O}_K/w')|_{G_v}.$$

Recall that e_v denotes the idempotent of the trivial character of I_v in $A[G]$. Let $e = |I_v|$. Then, as given in the proof of Proposition A.5.1. in [6], we have

$$e_v(\mathcal{O}_K/w') = \mathcal{O}_{K'}/w' \simeq \mathcal{O}_K/w \qquad \text{and} \qquad (1-e_v)(\mathcal{O}_K/w') = w/w' = w/w^e.$$

Also, we have an equality of ideals,

$$\mathrm{Fitt}_{A[G_v]}(E(\mathcal{O}_K/w')) = \mathrm{Fitt}_{e_vA[G_v]}(e_vE(\mathcal{O}_K/w')) + \mathrm{Fitt}_{(1-e_v)A[G_v]}((1-e_v)E(\mathcal{O}_K/w')).$$

Let $s_I : A[G_v] \to A[G_v/I_v]$ denote the augmentation map with respect to I_v. It is easy to see that the kernel of this map is $(1-e_v)A[G_v]$, and hence we have an isomorphism

$$s_I : e_vA[G_v] \to A[G_v/I_v].$$

In particular, we have

$$s_I(g) = |E(\mathcal{O}_{K'}/w')|_{G_v/I_v}.$$

By the unramified case, we have

$$|E(\mathcal{O}_{K'}/w')|_{G_v/I_v} = \rho^{-1}P_v(\overline{\sigma_v})$$

where $\overline{\sigma_v}$ denotes the Frobenius of v in K'/K. Since $s_I(\sigma_v e_v) = \overline{\sigma_v}$, we can rewrite this as

$$s_I(g) = s_I(\rho^{-1}P_v(\sigma_v e_v)).$$

This implies that

$$g = \rho^{-1}P_v(\sigma_v e_v) + (1 - e_v)g'$$

for some $g' \in A[G_v]$.

By Proposition A.4.1 in [6], we have

$$\mathrm{Fitt}_{(1-e_v)A[G_v]}(E(w/w^e)) = \mathrm{Fitt}_{(1-e_v)\mathbb{F}_q[G_v][t]}(E(w/w^e)) = \det_{(1-e_v)\mathbb{F}_q[G_v][t]}(t.I - A_{E,t})$$

where $A_{E,t}$ denotes the matrix of the $(1-e_v)\mathbb{F}_q[G_v]$–endomorphism of $E(w/w^e)$ given by multiplication by t. For $x \in w/w^e$,

$$t \star x = t.x + a_1\tau.x + ... + a_r\tau^r.x$$

If A_t denotes the action of t on w/w^e and A_τ denotes the action of τ on w/w^e, then

$$A_{E,t} = A_t + a_1A_\tau + ... + a_rA_\tau^r$$

Since $\tau^N.x = 0$ for all $x \in w/w^e$ if $q^N \geq e$, the matrix A_τ is nilpotent, and hence $N = a_1A_\tau + ... + a_rA_\tau^r$ is also nilpotent. So

$$Fitt_{(1-e_v)A[G_v]}(E(w/w^e)) = \det_{(1-e_v)\mathbb{F}_q[G_v][t]}(t.I - A_t - N)$$

As in the proof of Proposition A.5.1. in [6], we can find a $\overline{\mathbb{F}}_q[G_v]$-basis $\{e_i\}_i$ of $\mathcal{O}_K/w^e \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ on which A_t is diagonal. Hence $tI - A_t$ and N commute and we have

$$\det_{(1-e_v)\overline{\mathbb{F}}_q[G_v][t]}(tI - A_t - N) = \det_{(1-e_v)\overline{\mathbb{F}}_q[G_v][t]}(tI - A_t).$$

Since

$$\det_{(1-e_v)\mathbb{F}_q[G_v][t]}(tI - A_t) = (1-e_v)Fitt_{A[G_v]}(\mathcal{O}_K/w^e) = (1-e_v)(P_v(0)),$$

we have

$$(1-e_v)g = (1-e_v)\rho^{-1}P_v(0).$$

This shows that $g' = 0$ and that completes our proof.

3.7 Future Work

In future work, we would like to extend this result to abelian t-modules. This is an informal section, and we're reusing most of the notation from §3.1.

Definition 3.7.1. A t-module E over $\mathcal{O}_F$ of dimension n is given by an $\mathbb{F}_q$-algebra morphism

$$\phi_E : A \to M_n(\mathcal{O}_F)\{\tau\}, \qquad t \mapsto M_0 \cdot \tau^0 + M_1\tau + \cdots + M_\ell \cdot \tau^\ell,$$

where $M_i \in M_n(\mathcal{O}_F)$, and $(M_0 - t \cdot I_n)^n = 0$.

Similar to the case of Drinfeld modules, for any $\mathcal{O}_F[G]\{\tau\}$-module M, we can endow M^n with two A-structures:

1. $E(M)$ denotes the A-module with action given by ϕ_E.

2. $\mathrm{Lie}_E(M)$ denotes the A-module with action given by $ev_0 \circ \phi_E$, where $ev_0 : \mathcal{O}_F\{\tau\} \to \mathcal{O}_F$ sends $\tau \mapsto 0$. For example, t acts on an element of M^n as multiplication by M_0, where M_0 is as in the definition above.

In this case too, we can define $T_{v_0}(E)$ for all $v_0 \in \mathrm{MSpec}(A)$ and get a polynomial

$$P_v(X) = \det_{A_{v_0}}(X.I - \mathrm{Frob}_{q^{d_0}}|T_{v_0}(E))$$

for each $v \in \mathrm{MSpec}(\mathcal{O}_F)$ of good reduction for E.

In [11], Green and Popescu have proved an Equivariant Tamagawa Number Formula for pure t-modules. In their work, they have defined G-equivariant L-functions whose Euler factors are

$$\left(\frac{P_v(\sigma_v e_v)}{P_v(0)}\right)^{-1}.$$

We can then define $|E(\mathcal{O}_K/v)|_G$ and $|\mathrm{Lie}_E(\mathcal{O}_K/v)|_G$ as the unique monic generators of the respective $A[G]$-Fitting ideals. Then we would like to show that

$$\frac{P_v(\sigma_v e_v)}{P_v(0)} = \frac{|E(\mathcal{O}_K/v)|_G}{|\mathrm{Lie}_E(\mathcal{O}_K/v)|_G}.$$

Much of the theory in the previous section goes through for the case of abelian modules, but an analogue of 3.2.1 doesn't hold in this case. Something similar holds for a smaller case of abelian t-modules, known as pure t-modules, but in future work, we would like to provide a proof of this in the case of general abelian t-modules.

A major portion of Chapter 3 is being prepared for submission for publication. The dissertation author was the collaborator and the coauthor for the material below:

- C. D. Popescu, **N. Ramachandran**, *Euler factors of equivariant L-functions of Drinfeld modules and beyond*

Bibliography

[1] D. Burns, M. Kurihara, and T. Sano, *On zeta elements for* $\mathbb{G}_m$, Documenta Math. **21** (2016), 555 – 626.

[2] L. Carlitz, *A class of polynomials*, Trans. Amer. Math. Soc **43** (1938), no. 2, 167 – 182.

[3] S. Dasgupta and M. Kakde, *On the Brumer–Stark conjecture*, Annals of Mathematics **197** (2023), no. 1, 289 – 388.

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

[5] N. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. **89** (1987), no. 3, 561–567.

[6] J. Ferrara, N. Green, Z. Higgins, and C.D. Popescu, *An equivariant Tamagawa number formula for Drinfeld modules and applications*, J. Algebra and Number Theory **16** (2022), no. 9, 2215–2264.

[7] B. Ferrero and L. C. Washington, *The Iwasawa invariant* μ_p *vanishes for abelian number fields*, Annals of Mathematics **109** (1979), no. 2, 377–395.

[8] R. Gambheera and C.D. Popescu, *An unconditional main conjecture in Iwasawa theory and applications*, 2023.

[9] E.-U. Gekeler, *On finite Drinfeld modules*, J. Algebra **141** (1991), no. 1, 187–203.

[10] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer Berlin, Heidelberg, 1998.

[11] N. Green and C.D. Popescu, *An equivariant Tamagawa number formula for t–modules and applications*, https://arxiv.org/abs/2206.03541 (June 2022), 27 pages.

[12] R. Greenberg, *Iwasawa theory for motives*, Adv. Stud. Pure Math. **153** (1989), 97 – 137.

[13] ______, *Iwasawa theory for p-adic representations*, Adv. Stud. Pure Math. **17** (1989), 97 – 137.

[14] C. Greither and C.D. Popescu, *The Galois Module Structure of ℓ-adic Realizations of Picard 1-motives and Applications*, Int. Math. Res. Not. **2012** (2012), no. 5, 986–1036.

[15] C. Greither and C.D. Popescu, *An Equivariant Main Conjecture in Iwasawa Theory and applications*, J. Algebraic Geom. **24** (2015), no. 4, 629 – 692.

[16] U. Hartl and R.K. Singh, *Local shtukas and divisible local Anderson modules*, Canad. J. Math. **71** (2019), no. 5, 1163–1207. MR 4010425

[17] K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. (2) **93** (1959), no. 3, 183–226. MR 3509953

[18] K. Iwasawa, *On some modules in the theory of cyclotomic fields*, Journal of the Mathematical Society of Japan **16** (1964), no. 1, 42 – 82.

[19] ______, *On p-adic l-functions*, Annals of Mathematics **89** (1969), no. 1, 198–205.

[20] M. Kurihara, *Rubin-Stark elements and ideal class groups*, RIMS Kôkyûroku Bessatsu **B53** (2015), 343–363.

[21] S. Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563. MR 86367

[22] ______, *Cyclotomic Fields I and II*, Springer New York, NY, 1989.

[23] H. Matsumura, *Commutative Algebra, Second Edition*, The Benjamin/Cummings Publishing Co. Inc., 1980.

[24] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), no. 1, 1 – 61.

[25] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. **76** (1984), no. 2, 179 – 330.

[26] B. Poonen, *Drinfeld modules with no supersingular primes*, Internat. Math. Res. Notices **1998** (1998), no. 3, 151–159.

[27] C. D. Popescu and N. Ramachandran, *Euler factors of equivariant L-functions of Drinfeld modules and beyond*, 2024+.

[28] L.C. Washington, *Introduction to Cyclotomic Fields*, Springer New York, NY, 1996.

[29] A. Wiles, *The Iwasawa Conjecture for Totally Real Fields*, Annals of Mathematics **131** (1990), no. 3, 493–540.