GALOIS MODULE STRUCTURE OF LUBIN-TATE MODULES

Sebastian Tomaskovic-Moore

A DISSERTATION

in

Mathematics

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

2017

Supervisor of Dissertation

_____

Ted Chinburg, Professor of Mathematics

Graduate Group Chairperson

_____

Wolfgang Ziller, Professor of Mathematics

Dissertation Committee:
Ted Chinburg, Professor of Mathematics
Ching-Li Chai, Professor of Mathematics
Philip Gressman, Professor of Mathematics

Acknowledgments

I would like to express my deepest gratitude to all of the people who guided me along the doctoral path and who gave me the will and the ability to follow it.

First, to Ted Chinburg, who directed me along the trail and stayed with me even when I failed, and who provided me with a wealth of opportunities.

To the Penn mathematics faculty, especially Ching-Li Chai, David Harbater, Phil Gressman, Zach Scherr, and Bharath Palvannan. And to all my teachers, especially Y. S. Tai, Lynne Butler, and Josh Sabloff. I came to you a student and you turned me into a mathematician.

To Philippe Cassou-Noguès, Martin Taylor, Nigel Byott, and Antonio Lei, whose encouragement and interest in my work gave me the confidence to proceed.

To Monica Pallanti, Reshma Tanna, Paula Scarborough, and Robin Toney, who make the road passable using paperwork and cheer.

To my fellow grad students, especially Brett Frankel, for company while walking and for when we stopped to rest.

To Barbara Kail for sage advice on surviving academia.

To Dan Copel, Aaron Segal, Tolly Moore, and Ally Moore, with whom I feel at home and at ease.

To Bill and Jean Tomaskovic, who never doubted that I would make it.

To Stephanie Stern and John Moore, who raised me to follow my passions, both mathematical and artistic. I'm sure I don't realize even half of what you've done for me but I am grateful for all of it.

And most of all to Kate, who shares my ups and my downs. Whether on an adventure or safe at home, I never want to be without you. Everything I do is for you.

ABSTRACT

GALOIS MODULE STRUCTURE OF LUBIN-TATE MODULES

Sebastian Tomaskovic-Moore

Ted Chinburg

Let L/K be a finite, Galois extension of local or global fields. In the classical setting of additive Galois modules, the ring of integers $\mathcal{O}_L$ of L is studied as a module for the group ring $\mathcal{O}_K G$, where G is the Galois group of L/K. When K is a p-adic field, we also find a structure of $\mathcal{O}_K G$ module when we replace $\mathcal{O}_L$ with the group of points in $\mathcal{O}_L$ of a Lubin-Tate formal group defined over K. For this new Galois module we find an analogue of the normal basis theorem. When K is a proper unramified extension of $\mathbb{Q}_p$, we show that some eigenspaces for the Teichmüller character are not free. We also adapt certain cases of E. Noether's result on normal integral bases for tame extensions. Finally, for wild extensions we define a version of Leopoldt's associated order and demonstrate in a specific case that it is strictly larger than the integral group ring.

Contents

Chapter 1

Introduction

The classical study of additive Galois modules concerns a finite Galois extension L/K of global fields, meaning number fields or finite extensions of $\mathbb{F}_p(t)$, or non-archimedean local fields, meaning finite extensions of $\mathbb{Q}_p$ or $\mathbb{F}_p(\!(t)\!)$. Write G for the Galois group of this extension. Then the ring of integers $\mathcal{O}_L$ of L is a module for $\mathcal{O}_K$ with an action by G so we may ask questions about the structure of $\mathcal{O}_L$ as a module over the group ring $\mathcal{O}_K G$. Developments in this field include the familiar normal basis theorem; Noether's criterion, which asserts that $\mathcal{O}_L$ is locally free if and only if L/K is tame; and Leopoldt's associated order, which serves as a replacement for the coefficient ring $\mathcal{O}_K G$ in the presence of wild ramification. Details on these innovations will be given in Chapter 2. They serve as the template for the main results of this thesis.

Our object of study here will not be the ring of integers of L, but rather the

$\mathcal{O}_L$-points of a Lubin-Tate formal group. Suppose that L/K is a finite, Galois extension of non-archimedean local fields of characteristic zero, F is a Lubin-Tate formal group defined over K, and denote its points in $\mathcal{O}_L$ by $F(\mathcal{O}_L)$. Then $F(\mathcal{O}_L)$ is an abelian group by virtue of F being a formal group. It has an action of $\mathcal{O}_K$ coming from the formal $\mathcal{O}_K$-module structure on F. If $G = \mathrm{Gal}(L/K)$ then the natural G-action on elements of L commutes with both the formal group operation and the Lubin-Tate endomorphisms because both are given by power series in K. Hence, we get an $\mathcal{O}_K$-linear G-action on $F(\mathcal{O}_L)$ which makes it a module for $\mathcal{O}_K G$. This means that many theorems concerning additive Galois modules make sense when posed as questions about $F(\mathcal{O}_L)$. Chapter 3 contains the foundational definitions and facts about Lubin-Tate formal groups.

Another Galois module that has been an object of study is the multiplicative group. Greither [Gre] and later Sharifi [Sha] have given a presentation of the multiplicative group of cyclotomic extensions of $\mathbb{Q}_p$, as well as its subgroups the principal n-units, as modules for $\mathbb{Z}_p G$. This fits under the above rubric since the principal 1-units are the points of the multiplicative formal group. This precedent for the current research is covered in Chapter 4.

New research concerning the Galois module $F(\mathcal{O}_L)$ begins in Part II. The goal of Chapter 5 is a new result on pointwise convergence of the known formula $\log_F(X) = \lim_{n\to\infty} \pi^{-n}[\pi^n](X)$. Chapters 6 and 7 contain an analysis of how the $\mathcal{O}_K$-action and the Galois action, respectively, affect the valuation of elements of $F(\mathcal{O}_L)$. Also

in Chapter 6, we use the pointwise convergence of the logarithm to determine the valuation of elements comprising the image of $\log_F$. The structure of $F(\mathcal{O}_L)$ as $\mathcal{O}_K$-module is completely determined using the formal logarithm in Section 6.1.

The next three chapters adapt the statements about $\mathcal{O}_L$ described in Chapter 2 to our new Galois module $F(\mathcal{O}_L)$. The normal basis theorem inspires a theorem about freeness of $F(\mathcal{O}_L) \otimes_{\mathcal{O}_K} K$ in Chapter 8. Then certain tame extensions are investigated in Chapter 9. Finally, in Chapter 10, we define the associated order of $F(\mathcal{O}_L)$, prove that it is strictly larger than $\mathcal{O}_K$ for the π^2-torsion field of a formal group of height 2, and then use class field theory to demonstrate some elements that are not in the associated order. Also, a comparison is made to the associated order determined by Cassou-Noguès and Taylor [CNT].

Part I

Background

Chapter 2

An abridged history of additive Galois modules

In this chapter we will review selected pieces of the theory of additive Galois modules. This chapter by no means contains the entirety of what is known about the $\mathcal{O}_K G$-structure of $\mathcal{O}_L$ but only the specific theorems and concepts that will be adapted when we later replace $\mathcal{O}_L$ with the points of a Lubin-Tate formal group. A more detailed overview of results in this field, focusing especially on the local case, can be found in [Tho].

2.1 The normal basis theorem

The study of Galois modules can be said to begin with a familiar result, the normal basis theorem. It is the statement that L, when considered as a K-vector space with

K-linear G-action, i.e. as a KG-module, is a free module of rank 1. Equivalently, it says that there is a K-basis for L consisting of the G-conjugates of a single element; this is the titular *normal basis*. It is a result in algebra, but not really number theory.

To make the question more arithmetic, we can try to determine when $\mathcal{O}_L$ is free, rank 1 over $\mathcal{O}_K G$, that is, when is there a basis for $\mathcal{O}_L$ as an $\mathcal{O}_K$-module consisting of G-conjugate elements? Such a basis is an *integral normal basis*. It is enough to determine when $\mathcal{O}_L$ is free over $\mathcal{O}_K G$, since its rank will not be changed by tensoring with K, reducing it to the case of the normal basis theorem.

2.2 Tame extensions

The question of the existence of an integral normal basis was answered by E. Noether [Noe] in the case of local fields.[1] She proved that an integral normal basis exists precisely when L/K is at most tamely ramified. An extension is tamely ramified when, for each ramified prime $\mathfrak{p}$ of K with residue field of characteristic p, the ramification index of $\mathfrak{p}$ in L is prime to p. In the case of local fields, which have only one prime, a tame extension is one in which the characteristic of the residue field does not divide the subgroup of G that acts trivially on the residue field.

[1] The term *local field* should always be interpreted to mean a non-archimedean local field with finite residue field.

2.3 The associated order

If L/K is not tame then it is called *wildly ramified*. H.-W. Leopoldt [Leo] discovered a way to recover freeness for many wildly ramified extensions. Namely, one enlarges $\mathcal{O}_K G$ to the *associated order* $\mathfrak{A}_{L/K}$ of $\mathcal{O}_L$ in KG, defined as

$$\mathfrak{A}_{L/K} = \{\phi \in KG : \phi(\mathcal{O}_L) \subseteq \mathcal{O}_L\}.$$

Leopoldt proved that if K is either $\mathbb{Q}$ or $\mathbb{Q}_p$ and L is absolutely abelian, then $\mathcal{O}_L$ is free as a module for $\mathfrak{A}_{L/K}$. In one sense, the associated order is the correct ring for this question, for Martinet notes that $\mathfrak{A}_{L/K}$ is the only $\mathcal{O}_K$-order in KG over which it is possible for $\mathcal{O}_L$ to be free [Mar, §4]. Consistent with this and Noether's criterion, Bergé has proved that $\mathfrak{A}_{L/K} = \mathcal{O}_K G$ if and only if L/K is tamely ramified [Ber, Th. 1]. The associated order improves a little on Noether even when K is not $\mathbb{Q}$ or $\mathbb{Q}_p$. If L/K is an extension of p-adic fields that is at most *weakly ramified*, meaning that its second ramification group is trivial, then Byott proved that $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$ [Byo, Cor. 4.3].

Besides the above, fairly general, results, it is known whether or not $\mathcal{O}_L$ is free over its associated order in a variety of specific situations. Sometimes we also have an explicit description of the associated order. One such case is the work of Cassou-Noguès and Taylor [CNT, Ch. X], in which the authors consider the torsion field of a Lubin-Tate formal group. More will be said about their results in Section 10.4.

2.4 Ambiguous ideals

If $\mathfrak{a}$ is a so-called *ambiguous ideal*, that is, a fractional ideal of L that is stable under the action of G, then much the same questions can be asked about $\mathfrak{a}$ as about $\mathcal{O}_L$. Specifically, $\mathfrak{a}$ is a module for $\mathcal{O}_K G$ which yields L when tensored with K, so we may seek to determine when such $\mathfrak{a}$ are free over $\mathcal{O}_K G$. Ullom has proved that any ambiguous ideal is free over $\mathcal{O}_K G$ when L/K is a tame extension of local fields [Ull].

Chapter 3

Lubin-Tate formal modules

Our aim in this thesis is to replace the ring of integers in the classical theory of additive Galois modules with the group of points of a Lubin-Tate formal group. This chapter provides an introduction to Lubin-Tate formal groups.

3.1 Formal group laws

Let R be a commutative ring. A one-dimensional **formal group law** over R is a power series $F \in R[\![X, Y]\!]$ with no constant term satisfying

$$F(X, 0) = X \quad \text{and} \quad F(0, Y) = Y \tag{A1}$$

and

$$F(F(X, Y), Z) = F(X, F(Y, Z)) \tag{A2}$$

If F also satisfies

$$F(X,Y) = F(Y,X) \tag{A3}$$

then F is a **commutative formal group law**. Most formal group laws are commutative. More precisely, if R has no elements that are simultaneously torsion and nilpotent, then all one-dimensional formal group laws over R are commutative [Haz, §6.1]. In this thesis, a *formal group law* shall always mean a one-dimensional, commutative formal group law.

The first axiom, (A1), may be replaced by one of a few equivalent statements.

Lemma 3.1. *Assuming that* (A2) *holds, the following are equivalent:*

$$F(X,0) = X \quad \textit{and} \quad F(0,Y) = Y, \tag{A1}$$

$$F(X,Y) \equiv X + Y \mod (X,Y)^2, \tag{A1b}$$

$$F(X,Y) \equiv X + Y \mod XY. \tag{A1c}$$

Proof. It is clear that (A1c) implies (A1b). Also, (A1) implies (A1c) because $F(X,0)$ is the sum of all terms of $F(X,Y)$ having no Y factor and similarly for $F(0,Y)$. The implication from (A1b) to (A1) is the only one requiring (A2). Substituting $Y = Z = 0$ in that axiom, we get

$$F(X,0) = F(X,F(0,0)) = F(F(X,0),0).$$

If $F(X,0) \equiv X + aX^r \mod X^{r+1}$ for some $a \in R$ then the above equation says that

$$X + aX^r \equiv X + aX^r + a(X + aX^r)^r \equiv X + 2aX^r \mod X^{r+1},$$

which means that $a = 0$. Showing that $F(0, Y) = Y$ is the same. $\square$

There is a clear analogy between the above axioms and those defining a group. However, the reader may notice that the usual group axiom asserting the existence of inverses is missing. In fact, such an axiom is not necessary for a formal group law because it is a consequence of the first two axioms.

Lemma 3.2. *If $F \in R[\![X, Y]\!]$ is a power series satisfying* (A1) *and* (A2) *then there is a unique power series $\iota(X) \in R[\![X]\!]$ such that $\iota(X) \equiv -X \mod X^2$ and $F(X, \iota(X)) = F(\iota(X), X) = 0$.*

Proof. First we will construct ι so that $F(X, \iota(X)) = 0$ and then prove that any such ι must also satisfy $F(\iota(X), X) = 0$. The series ι may be constructed via an iterative procedure as follows.

Let $\iota_1(X) = -X$. It is clear that $F(X, \iota_1(X)) \equiv 0 \mod X^2$. Now suppose that we have $\iota_r(X)$ with $F(X, \iota_r(X)) \equiv aX^{r+1} \mod X^{r+2}$ for some $a \in R$. If we define $\iota_{r+1}(X)$ to be $\iota_r(X) - aX^{r+1}$ then $F(X, \iota_{r+1}(X)) \equiv 0 \mod X^{r+2}$ because of (A1b). Now if we define $\iota(X) = \lim_{r\to\infty} \iota_r(X)$ then it will satisfy $F(X, \iota(X)) = 0$.

Now we will show that also $F(\iota(X), X) = 0$. It is obvious that $F(\iota(X), X) \equiv 0 \mod X^2$. So suppose $r \geq 2$ is such that $F(\iota(X), X) \equiv aX^r \mod X^{r+1}$. We have

$$F(X, F(\iota(X), X)) \equiv X + aX^r \mod X^{r+1}$$

and, on the other hand,

$$F(X, F(\iota(X), X)) = F(F(X, \iota(X)), X) = F(0, X) = X.$$

So in fact $a = 0$, and thus $F(\iota(X), X) = 0$.

Uniqueness of ι can be proved in the same way as for uniqueness of inverses in a group. □

Some familiar formal group laws are the additive group

$$\hat{\mathbb{G}}_a(X, Y) = X + Y$$

and the multiplicative group

$$\hat{\mathbb{G}}_m(X, Y) = (1 + X)(1 + Y) - 1 = X + Y + XY.$$

Given a formal group law, the associated **formal group** is a group object in the category of formal schemes. If S is a complete, local R-algebra, define the **points of F in S** to be the group with underlying set $\mathfrak{m}_S$, the maximal ideal of S, and operation

$$x \underset{F}{+} y = F(x, y)$$

for any $x, y \in \mathfrak{m}_S$. We write this group as $F(S)$, or sometimes $F(\mathfrak{m}_S)$. The axioms (A1) and (A2) together with Lemma 3.2 guarantee that $F(S)$ is a group and, when F is commutative, (A3) says that it is an abelian group. This group has a filtration by the subgroups $F(\mathfrak{m}_S^i)$, the subgroups whose sets are $\mathfrak{m}_S^i$.

3.2 The logarithm

A **homomorphism of formal group laws** from G to F is a power series $f(X) \in R[\![X]\!]$ without constant term that satisfies

$$F(f(X), f(Y)) = f(G(X, Y)).$$

Clearly such a homomorphism is invertible if and only if f has a composition inverse. For example, when R is a field of characteristic zero, the usual power series $\log(1+X)$ and $\exp(X) - 1$ are mutually inverse isomorphisms between $\hat{\mathbb{G}}_m$ and $\hat{\mathbb{G}}_a$. It is evident from the definition that a homomorphism of formal group laws induces a homomorphism of functors

$$f(S) : G(S) \to F(S), x \mapsto f(x)$$

for any complete, local R-algebra S.

In fact, analogues of log and exp exist for any formal group law over a field of characteristic zero. Specifically, there is a power series

$$\log_F(X) \equiv X \mod X^2$$

with coefficients in K such that

$$\log_F(F(X, Y)) = \log_F(X) + \log_F(Y), \tag{3.1}$$

i.e. $\log_F$ is a homomorphism from F to $\hat{\mathbb{G}}_a$. One way to obtain this power series is by solving

$$\tfrac{d}{dX} \log_F(X) \tfrac{dF}{dY}(X, 0) = 1.$$

This is proved in [FV, Ch. VIII, §1]. Since the linear term of $\log_F$ is X, it has a composition inverse, which is denoted by $\exp_F$.

3.3 Lubin-Tate formal group laws

A Lubin-Tate formal group law is a formal group law over a characteristic zero local field having an endomorphism of a specific form. Let $R = \mathcal{O}_K$ be the ring of integers of a local field K of mixed characteristic $(0, p)$ and fix a prime element π of K. Let q be the order of the residue field. A power series $e(X) \in \mathcal{O}_K[\![X]\!]$ satisfying

$$e(X) \equiv \pi X \mod X^2 \quad \text{and} \quad e(X) \equiv X^q \mod \pi$$

is called a **Lubin-Tate series** [Neu, Ch. V, §2] or a **Frobenius power series** [Lan, Ch. 8, §1] for π. For a given power series $e(X)$ of this form, there is a unique formal group law $F_e \in \mathcal{O}_K[\![X, Y]\!]$ having e as an endomorphism, that is,

$$F_e(e(X), e(Y)) = e(F_e(X, Y)).$$

This formal group law is the **Lubin-Tate formal group law** associated to $e(X)$.

A Lubin-Tate formal group law comes with many more endomorphisms than just $e(X)$. For any $a \in \mathcal{O}_K$ there is a unique power series $[a](X) \in \mathcal{O}_K[\![X]\!]$ such that $[a](X) \equiv aX \mod X^2$ and $[a]$ is an endomorphism of F_e. Because of the uniqueness, we must have $[\pi](X) = e(X)$. Uniqueness also tells us that the map $[\cdot] : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F)$ is an injective homomorphism. The existence of such a homomorphism gives a formal group law the name **formal $\mathcal{O}_K$-module**. If F is a

formal module, not *a priori* a Lubin-Tate formal group law, such that $[\pi](X) \equiv X^q \mod \pi$ then in fact F is a Lubin-Tate formal group law and thus there is a one-to-one correspondence between Frobenius power series and such formal modules [Neu, Ch. V, Th. 4.6].

If $e(X)$ and $\overline{e}(X)$ are two different Lubin-Tate series, both for the uniformizer π, then in fact F_e and $F_{\overline{e}}$ are isomorphic over $\mathcal{O}_K$ [Neu, *loc. cit.*]. If a different uniformizer, $\overline{\pi}$ is chosen for K, it comes with a different set of Lubin-Tate power series and thus a different set of Lubin-Tate formal group laws. These formal group laws will not be isomorphic over $\mathcal{O}_K$ to those for π. However, there are isomorphisms defined over the completion of the maximal unramified extension of K [Lan, Ch. 8, §3].

In the sequel, F is assumed to be a Lubin-Tate formal group law for the uniformizer $\pi \in K$.

For positive integers n, let $F[\pi^n]$ denote the set of π^n-torsion points of F in $\overline{\mathbb{Q}}_p$,

$$F[\pi^n] = \{x \in \overline{\mathbb{Q}}_p : [\pi^n](x) = 0\},$$

and let $F[\pi^\infty] = \bigcup_{n \geq 1} F[\pi^n]$. For finite n, $F[\pi^n]$ is a cyclic $\mathcal{O}_K$-module generated by any primitive π^n-torsion point, i.e. any element of $F[\pi^n] - F[\pi^{n-1}]$. The π^n-torsion field of F is $L = K(F[\pi^n])$, the field obtained by adjoining all of the π^n-torsion points of F to K. It can be proved using Weierstrass preparation on the power series $[\pi^n](X)$ that L/K is totally ramified and that the ring of integers of L is generated by a primitive π^n-torsion point λ. Clearly, if a is any element

of $(\mathcal{O}_K/(\pi^n))^\times$ then $[a](\lambda)$ is also a primitive π^n-torsion point. Thus, we get an injective homomorphism $(\mathcal{O}_K/(\pi^n))^\times = \mathcal{O}_K^\times/U_K^{(n)} \to \mathrm{Gal}(L/K)$, where $U_K^{(n)}$ is the group of principal n-units of K, which sends $a \in \mathcal{O}_K^\times/U_K^{(n)}$ to the automorphism mapping $\lambda \mapsto [a](\lambda)$. By considering the degree of the polynomial obtained by Weierstrass preparation, we see that in fact this map is an isomorphism. Hence, L/K is an abelian extension of K with Galois group isomorphic to $\mathcal{O}_K^\times/U_K^{(n)}$ and degree equal to $\#\left(\mathcal{O}_K^\times/U_K^{(n)}\right) = (q-1)q^{n-1}$. Lubin-Tate formal groups are used in local class field theory because K^{ab} is the compositum of $K(F[\pi^\infty])$ and K^{nr}.

Even though $\mathcal{O}_K$ is not a field, the logarithm of a Lubin-Tate formal group is still very useful. It can be defined as in Section 3.2 to yield a power series $\log_F \in K[\![X]\!]$ and it will still satisfy (3.1). The coefficients of $\log_F$ are not too far from integral; the formal derivative $\frac{d}{dX}\log_F(X)$ has coefficients in $\mathcal{O}_K$. This is enough to guarantee that, even though $\log_F$ has nonintegral coefficients, it will converge on the valuation ideal $\mathfrak{m}$ of any algebraic extension L of K. This means that evaluation of $\log_F$ induces a homomorphism from $F(\mathfrak{m})$ to the additive group of L. Note that its image will not generally be contained in $\mathfrak{m}$ because of $\log_F$'s nonintegral coefficients. But this only happens for arguments of small valuation. If we restrict to a small enough neighborhood of zero then $\log_F$ becomes bijective. To be precise, $\log_F$ and $\exp_F$ induce mutually inverse isomorphisms between $F(\mathfrak{m}^i)$ and $\mathfrak{m}^i$ whenever $i > \frac{e_{L/K}}{q-1}$ [Lan, La. 8.6.4].

3.4 The formal group of an elliptic curve

A formal group law can be obtained from an elliptic curve. Let E be an elliptic curve defined over the field K. When completed at the identity, the group law of E becomes a morphism $\operatorname{Spec} K[\![X,Y]\!] \to \operatorname{Spec} K[\![Z]\!]$. The image of Z under the corresponding ring map is a power series $\hat{E}$ with coefficients in K. This power series will be a formal group law since it comes from a group scheme multiplication.

Given a Weierstrass model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.2}$$

for E, we can derive the power series $\hat{E}$ as follows. This approach may be found in [Sil, Ch. IV, §1] or [Hus, Ch. 12, §7]. We begin by making the change of variables

$$z = -\frac{x}{y} \quad \text{and} \quad w = -\frac{1}{y}$$

which results in z being a local parameter for E at the origin. This causes the Weierstrass equation to take the form

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3. \tag{3.3}$$

Using this expression, we may express w as a power series $w(z) \equiv z^3 \mod z^4$ in $K[\![z]\!]$. Inverting the change of variables gives Laurent series $x(z)$ and $y(z)$ in $K(\!(z)\!)$ that satisfy (3.2).

We now use $w(z)$ and z to find the power series $\hat{E}$. Regarding z_1 and z_2 as independent indeterminates, the line through $(z_1, w(z_1))$ and $(z_2, w(z_2))$ has slope

$$\lambda = \frac{w(z_2) - w(z_1)}{z_2 - z_1}.$$

The equation for the line is $w = \lambda z + \nu$, where $\nu = w(z_1) - \lambda z_1$. Write z_3 for the z-coordinate of the third intersection point of the line with E. If we substitute $w = \lambda z + \nu$ into (3.3) then we obtain a cubic polynomial in z whose roots are z_1, z_2, and z_3. Hence, the z^2 coefficient in this cubic is $-z_1 - z_2 - z_3$. This yields

$$z_3 = -z_1 - z_2 - \frac{a_1\lambda + a_3\lambda^2 + a_2\nu + 2a_4\lambda\nu + 3a_6\lambda^2\nu}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3}.$$

This means that the sum of $(z_1, w(z_1))$ and $(z_2, w(z_2))$ will have z-coordinate

$$\hat{E}(z_1, z_2) = \frac{x(z_3)}{y(z_3) + a_1 x(z_3) + a_3} \equiv z_1 + z_2 \mod (z_1, z_2)^2.$$

It is proved in [Sil] that in fact this power series has coefficients in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$.

Now suppose that E has good reduction at the prime $\mathfrak{p} \subset K$. Let $E_\mathfrak{p}$ be the base change of E to $K_\mathfrak{p}$, the completion of K at $\mathfrak{p}$, and let $\tilde{E}$ denote the reduction of E at $\mathfrak{p}$. If $\mathfrak{m}$ is the valuation ideal of $K_\mathfrak{p}$ then

$$z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right)$$

is a homomorphism of abelian groups from $\hat{E}(\mathfrak{m})$ to $E(K_\mathfrak{p})$ fitting in the exact sequence

$$0 \to \hat{E}(\mathfrak{m}) \to E(K_\mathfrak{p}) \to \tilde{E}(k) \to 0$$

where k is the residue field of K at $\mathfrak{p}$. See [Sil, Ch. VII, §2] for a proof of this.

This exact sequence tells us that $\hat{E}$ can show us some or all of the p-torsion points of E, where p is the rational prime lying below $\mathfrak{p}$. When E has ordinary reduction at $\mathfrak{p}$, the formal group will have torsion of rank one, and when E is

supersingular at $\mathfrak{p}$, the rank of $\hat{E}[p]$ is two. Furthermore, in the case where E has complex multiplication by the imaginary quadratic field K, it turns out that $\hat{E}$ is a Lubin-Tate formal group [CNT, Ch. X, §5].

Chapter 4

The case of $\hat{\mathbb{G}}_m$

The multiplicative formal group law $\hat{\mathbb{G}}_m$ is a Lubin-Tate formal group law over $\mathbb{Q}_p$ with uniformizer $\pi = p$. Therefore we may consider the question of the structure of the points of $\hat{\mathbb{G}}_m$ in extensions $L/\mathbb{Q}_p$ as a module for $\mathbb{Z}_p[\mathrm{Gal}(L/\mathbb{Q}_p)]$. The group $\hat{\mathbb{G}}_m(\mathcal{O}_L)$ is isomorphic via $x \mapsto 1 + x$ to the principal units of L. The multiplicative group of L and its subgroup the principal units have been studied as Galois modules.

In 1996, Greither gave a presentation for the multiplicative group of the cyclotomic extension $\mathbb{Q}_p(\zeta_{p^n})$ as a module for the $\mathbb{Z}_p$-group ring of $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$ [Gre]. Sharifi gave another proof of the result, using different methods, in 2014 [Sha].[2] Here we follow Sharifi's treatment.

Let p be an odd prime, n a positive integer, and $L = \mathbb{Q}_p(\zeta_{p^n})$. The principal

[2] In fact, both Greither's and Sharifi's work concerns the more general situation where L is the compositum of a cyclotomic extension and an unramified extension. The presentation here is simplified to allow an easier comparison to the results that follow.

unit group $U_L^{(1)} = \{1 + x : x \in \mathfrak{m}_L\}$ is a $\mathbb{Z}_p$-module with $\mathbb{Z}_p$-linear action by $G = \mathrm{Gal}(L/\mathbb{Q}_p)$, hence a $\mathbb{Z}_p G$-module. We have $G = \Delta \times \Gamma$ with $\Delta \cong \mu_{p-1}$ and $\Gamma = \mathrm{Gal}(L/\mathbb{Q}_p(\zeta_p)) \cong \mathbb{Z}_p$. The group of principal units decomposes into eigenspaces for powers of the Teichmüller character $\omega : \Delta \to \mathbb{Z}_p^\times$; write $D^{(r)}$ for the ω^r eigenspace for $r = 2, \ldots, p$. Each $D^{(r)}$ is a $\mathbb{Z}_p\Gamma$-module.

Theorem 4.1 ([Sha, Th. 4.1.7])**.** *The eigenspace $D^{(r)}$ is a free $\mathbb{Z}_p\Gamma$ module generated by any $u_r \in D^{(r)}$ with $v_L(u_r) = r$ for $r = 2, \ldots, p-2$. The exceptions are*

$$D^{(p)} = \zeta_{p^n}^{\mathbb{Z}_p} u_p^{\mathbb{Z}_p\Gamma} \quad \textit{and} \quad D^{(p-1)} = (1+p)^{\mathbb{Z}_p} u_{p-1}^{\mathbb{Z}_p\Gamma}$$

for suitable choices of u_p, which generates a free $\mathbb{Z}_p\Gamma$-submodule, and u_{p-1}, which is subject to the relation $N_{L/Q_p(\zeta_p)}(u_{p-1}) = 1$.

In fact, Sharifi gives a presentation for the pro-p completion of $L^\times$. It differs from $U_L^{(1)}$ only in a $\mathbb{Z}_p$ factor, which is generated by a prime element of L. In this presentation, the generator u_{p-1} is replaced by this uniformizer, which yields u_{p-1} when acted on by $\gamma - 1$, where γ is a topological generator of Γ. Note that this makes the $r = p-1$ eigenspace, like $D^{(p)}$, the product of a cyclic $\mathbb{Z}_p$-module and a free $\mathbb{Z}_p\Gamma$-module.

While Greither proves this result using Coleman theory, Sharifi's proof uses mostly elementary methods involving a precise determination of the valuation of the image of the generator u_r under elements of the group ring.

Part II

Results

Let's fix some notation for the chapters that follow. Let p be an odd rational prime and K a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$ and residue field $\mathbb{F}_q$ of order $q = p^f$. Fix a uniformizer $\pi \in K$ and write $\mathfrak{p}$ for the maximal ideal $\pi\mathcal{O}_K$. The principal unit filtration is $\mathcal{O}_K^\times \supset U_K^{(1)} \supset U_K^{(2)} \supset \cdots$ with $U_K^{(i)} = 1 + \mathfrak{p}^i$ for $i \geq 1$. The normalized valuation on K is v_K.

L will denote a finite, Galois extension of K and we write $\mathfrak{m}$ for the valuation ideal of L and v_L for the normalized valuation. As with K, the principal i-units of L are $U_L^{(i)} = 1 + \mathfrak{m}^i$ for $i \geq 1$. The Galois group of L/K is denoted by G.

We are given a Lubin-Tate formal group law $F \in \mathcal{O}_K[\![X, Y]\!]$ for the prime element π. We write the Lubin-Tate module structure as

$$[\cdot] : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F),$$

so that $[a](X) \in \mathcal{O}_K[\![X]\!]$ with $[a](X) \equiv aX \mod X^2$ for $a \in \mathcal{O}_K$. The points of F in $\mathcal{O}_L$ are $F(\mathfrak{m})$ which has underlying set $\mathfrak{m}$ and operation $x \underset{F}{+} y := F(x, y)$. Subtraction is written as $x \underset{F}{-} y$ and we also sometimes use the notation

$$\sum_i{}_F\, a_i := a_1 \underset{F}{+} a_2 \underset{F}{+} \cdots$$

for the formal group sum of a collection $\{a_i\}_i$ of elements of $F(\mathfrak{m})$. Besides being an abelian group, $F(\mathfrak{m})$ is given an $\mathcal{O}_K$-module structure by evaluating the power series $[a](X)$ for $a \in \mathcal{O}_K$. Since both F and $[a]$ have coefficients in K, the action of $G = \mathrm{Gal}(L/K)$ commutes with the $\mathcal{O}_K$-module structure and makes $F(\mathfrak{m})$ into

a module for the group ring $\mathcal{O}_K G$. We will abuse some notation and write

$$[\cdot] : \mathcal{O}_K G \to \mathrm{End}_{\mathcal{O}_K}(F(\mathfrak{m}))$$

for this action as well. The group $F(\mathfrak{m})$ has the filtration $F(\mathfrak{m}) \supset F(\mathfrak{m}^2) \supset \cdots$ and these subgroups are stable under the action of $\mathcal{O}_K G$.

If G_K is the absolute Galois group of K, the action of G_K on $F[\pi^\infty]$ is given by a character $\chi : G_K \to \mathcal{O}_K^\times$ such that $\sigma(\lambda) = [\chi(\sigma)](\lambda)$ for any $\sigma \in G_K$ and $\lambda \in F[\pi^\infty]$. Of course χ factors through $G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{nr}}K(F[\pi^\infty])/K)$, and we decompose G_K^{ab} as $\mathrm{Gal}(K^{\mathrm{nr}}/K) \times \Delta \times \Gamma_\infty$, corresponding to the decomposition $K^\times \cong \pi^{\mathbb{Z}} \times \mu_{q-1} \times U_K^{(1)}$. For finite extensions L/K such that $L \supset F[\pi^m]$, we may also write $\chi(g)$ for $g \in G = \mathrm{Gal}(L/K)$ with the understanding that its value lies in $\mathcal{O}_K^\times / U_K^{(m)}$.

Chapter 5

More on the logarithm

We saw in Section 3.2 that there is a power series $\log_F(X) \in K[\![X]\!]$ that converges on $\mathfrak{m}$ and is a homomorphism (defined over K) from F to $\hat{\mathbb{G}}_a$. In the present case where F is a Lubin-Tate formal group, another way to obtain $\log_F$ is the limit

$$\log_F(X) = \lim_{n\to\infty} \pi^{-n}[\pi^n](X),$$

in the sense that the coefficient of X^i in $\log_F(X)$ is equal to the limit as n goes to infinity of the coefficient of X^i in $\pi^{-n}[\pi^n](X)$ [Lan, La. 8.6.1]. We will show that this limit can also be used to compute $\log_F(x)$ for a particular $x \in \mathfrak{m}$. First, here is a lemma adapted from [Haz, Eq. 5.4.9].

Lemma 5.1. *For each $n \geq 1$, there are power series $\beta_{0,n}, \ldots, \beta_{n,n} \in \mathcal{O}_K[\![X]\!]$ such that $\beta_{i,n} \equiv X \mod X^2$ and*

$$[\pi^n](X) = \pi^n\beta_{0,n}(X) + \pi^{n-1}\beta_{1,n}(X^q) + \cdots + \pi\beta_{n-1,n}(X^{q^{n-1}}) + \beta_{n,n}(X^{q^n}).$$

Proof. We will show that the desired equation holds modulo X^m by induction on m. It is true for $m = 2$ since the Lubin-Tate property $[\pi](X) \equiv \pi X \mod X^2$ implies that $[\pi^n](X) \equiv \pi^n X \mod X^2$. Now suppose that it holds modulo X^m and write

$$[\pi^n](X) = \pi^n \beta_{0,n}(X) + \pi^{n-1}\beta_{1,n}(X^q) + \cdots + \beta_{n,n}(X^{q^n}) + bX^m \mod X^{m+1}.$$

Let $k \in \mathbb{Z}$ be such that $q^k \mid m$ and $q^{k+1} \nmid m$. We would like to show that $b \in \pi^{n-k}\mathcal{O}_K$. Now apply $\log_F$ to this equation. Using the fact that $\log_F(X) \equiv X \mod X^2$, as well as part (iv) of Hazewinkel's functional equation lemma [Haz, Ch. I, §2.2], we have

$$\begin{aligned} \pi^n \log_F(X) &= \log_F([\pi^n](X)) \\ &\equiv \log_F\left(\sum_{i=k+1}^{n} \pi^{n-i}\beta_{i,n}(X^{q^i})\right) + bX^m \mod (\pi^{n-k}, X^{m+1}). \end{aligned} \tag{5.1}$$

On the other hand, we can use Hazewinkel's functional equation [Haz, Ch. I, §8.3]:

$$\log_F(X) = g(X) + \pi^{-1}\log_F(X^q),$$

for some $g(X) \in \mathcal{O}_K[\![X]\!]$, to see that

$$\pi^n \log_F(X) = \pi^n g(X) + \pi^{n-1} g(X^q) + \cdots + \pi g(X^{q^{n-1}}) + \log_F(X^{q^n}).$$

This means that $\pi^n \log_F(X)$ is congruent mod π^{n-k} to a power series in $X^{q^{k+1}}$. Combining this with (5.1), we can see that, since $q^{k+1} \nmid m$, it must be the case that $\pi^{n-k} \mid b$. □

Theorem 5.2. *For any $x \in \mathfrak{m}$, we have $\log_F(x) = \lim_{n\to\infty} \pi^{-n}[\pi^n](x)$.*

Proof. Write

$$\log_F(X) = \sum_{i \geq 1} a_i X^i \quad \text{and} \quad \pi^{-n}[\pi^n](X) = \sum_{i \geq 1} b_{i,n} X^i$$

for $a_i, b_{i,n} \in K$. We know that $\lim_{n\to\infty} b_{i,n} = a_i$ for all $i \geq 1$. Define $c_{m,n}$, for $m, n \geq 1$, to be

$$c_{m,n} = \sum_{i=1}^{m} b_{i,n} x^i.$$

Then we have

$$\lim_{n\to\infty} c_{m,n} = \sum_{i=1}^{m} a_i x^i \quad \text{and} \quad \lim_{m\to\infty} c_{m,n} = \pi^{-n}[\pi^n](x).$$

Our goal is to show that $\lim_{m\to\infty} \lim_{n\to\infty} c_{m,n} = \lim_{n\to\infty} \lim_{m\to\infty} c_{m,n}$.

The previous lemma shows that $v_K(b_{i,n}) \geq -\log_q i$. Given a bound $\ell \geq 1$, first choose m sufficiently large so that $(m+i)v_L(x) - e_{L/K}\log_q(m+i) \geq \ell$ whenever $i \geq 0$. Now we would like to find a bound on $v_L(c_{m,n+r} - c_{m,n})$ for $r \geq 1$. This difference involves the coefficients of the terms of degree at most m of

$$\frac{1}{\pi^{n+r}}[\pi^{n+r}](X) - \frac{1}{\pi^n}[\pi^n](X) = \frac{1}{\pi^{n+r}}\big([\pi^r]([\pi^n](X)) - \pi^r[\pi^n](X)\big). \tag{5.2}$$

From Lemma 5.1 we see that, ignoring terms of degree greater than m, the truncated power series $[\pi^n](X)$ is divisible by $\pi^{n-\lceil \log_q m \rceil}$. Similarly, $[\pi^r](X)$ is divisible modulo X^{m+1} by $\pi^{r-\lceil \log_q m \rceil}$. Because the linear terms will cancel in (5.2), we find that

$$[\pi^r]([\pi^n](X)) - \pi^r[\pi^n](X) \equiv 0 \mod (\pi^{2(n-\lceil \log_q m \rceil)+r-\lceil \log_q m \rceil}, X^{m+1})$$

and, dividing by π^{n+r}, this yields

$$v_L(c_{m,n+r} - c_{m,n}) \geq (n - 3\log_q m)e_{L/K}.$$

Choose n sufficiently large so that the right hand side is at least ℓ. We also have, for any $s \geq 1$,

$$\begin{aligned} v_L(c_{m+s,n+r} - c_{m,n+r}) &\geq \min\{e_{L/K} v_K(b_{m+i,n+r}) + (m+i)v_L(x) \mid 1 \leq i \leq s\} \\ &\geq \min\{(m+i)v_L(x) - e_{L/K} \log_q(m+i) \mid 1 \leq i \leq s\} \geq \ell. \end{aligned}$$

Combining the two inequalities shows that $\lim_{m,n\to\infty} c_{m,n}$ exists, and hence this limit may be obtained by letting either m or n go to infinity first. □

We will use this theorem in the next chapter to get information about the image under $\log_F$ of $F(\mathfrak{m})$. This image is an object of interest e.g. in [CW].

Chapter 6

$\mathcal{O}_K$-module structure

6.1 The structure theorem

We can use the formal group logarithm, $\log_F$, to get information about the structure of the $\mathcal{O}_K$-module $F(\mathfrak{m})$.

Theorem 6.1 (Structure theorem for points of formal $\mathcal{O}_K$-modules)**.** *We have an isomorphism of $\mathcal{O}_K$-modules*

$$F(\mathfrak{m}) \cong F[\pi^m] \oplus \mathcal{O}_K^{[L:K]}$$

where $m \geq 0$ is the maximal integer such that $F[\pi^m] \subset L$, i.e. $F[\pi^m] = F[\pi^\infty] \cap L$.

Proof. For large i, the image of $\mathfrak{m}^i$ under $\exp_F$ is a free $\mathcal{O}_K$-submodule of $F(\mathfrak{m})$ of rank $[L : K]$ and finite index. Thus, the free part of $F(\mathfrak{m})$ has rank $[L : K]$. Since $\mathfrak{m}$ is a torsion-free group, $F[\pi^m]$ must be contained in the kernel of $\log_F$. Furthermore,

the quotient of $F(\mathfrak{m})$ by its torsion subgroup is free, hence of rank $[L:K]$. So the kernel of $\log_F$ is exactly $F[\pi^m]$, and $F(\mathfrak{m})$ decomposes as the direct sum of $\ker(\log_F)$ and a submodule isomorphic to $\mathrm{im}(\log_F)$. □

6.2 The action of $[\pi]$

It will be useful to know the effect of the endomorphism $[\pi]$ on the filtration $\{F(\mathfrak{m}^i)\}_{i\geq 1}$ of $F(\mathfrak{m})$. In what follows, let $e_1 = e_{L/K}/(q-1)$.

Lemma 6.2. *Suppose $z \in F(\mathfrak{m})$ and $v_L(z) = i$. Then $v_L([a](z)) = i$ for any $a \in U_K$ and*

$$\begin{aligned} v_L([\pi](z)) &= qi && \text{if } i < e_1, \\ v_L([\pi](z)) &\geq qi && \text{if } i = e_1, \\ v_L([\pi](z)) &= i + e_{L/K} && \text{if } i > e_1. \end{aligned}$$

Proof. The first statement is a result of

$$[a](X) \equiv aX \mod X^2.$$

For the second, we use the Lubin-Tate conditions

$$[\pi](X) \equiv \pi X \mod X^2 \quad \text{and} \quad [\pi](X) \equiv X^q \mod \pi$$

to write

$$[\pi](X) = \pi X + X^q + \pi X^2 g(X)$$

for some $g \in \mathcal{O}_K[\![X]\!]$. Thus, the valuation of $[\pi](z)$ will depend on how qi compares to $i + e_{L/K}$. The cases are

$$\begin{aligned}
[\pi](z) &\equiv z^q \mod \mathfrak{m}^{qi+1} && \text{if } qi < i + e_{L/K}, \\
[\pi](z) &\equiv z^q + \pi z \mod \mathfrak{m}^{qi+1} && \text{if } qi = i + e_{L/K}, \\
[\pi](z) &\equiv \pi z \mod \mathfrak{m}^{i+e_{L/K}+1} && \text{if } qi > i + e_{L/K}.
\end{aligned}$$

This proves the lemma. □

When L/K is totally ramified, i.e. there is no extension of the residue field, it is now easy to see that $F(\mathfrak{m})$ is generated as an O_K-module by any set of elements whose valuations constitute the set $S = \{i \in \mathbb{Z} : 1 \leq i \leq e_{L/K} \text{ and } q \nmid i \text{ or } i = e_{L/K}\}$.

Corollary 6.3. $F(\mathfrak{m}^{qe_1+1}) \subseteq [\pi](F(\mathfrak{m}))$.

The above lemma, combined with Theorem 5.2, allows us to determine the valuations of elements in the image of $F(\mathfrak{m})$ under $\log_F$.

Proposition 6.4. *Let $S = \{q^{-m}e_1 : m = 0, 1, 2 \ldots, v_p(e_1)\}$. Given $x \in F(\mathfrak{m})$ such that $v_L(x) \notin S$, we have*

$$v_L(\log_F(x)) = q^r v_L(x) - re_{L/K},$$

where $r = \max\{0, \lceil \log_q \frac{e_1}{v_L(x)} \rceil\}$.

Proof. To make use of Theorem 5.2, we will show that $v_L(\pi^{-n}[\pi^n](x))$ is constant and equal to the value claimed for all sufficiently large n. We can see from Lemma

6.2 that r is the smallest non-negative integer such that $v_L([\pi^r](x)) \geq e_1$. When $n \geq r$, this means that

$$v_L([\pi^n](x)) = q^r v_L(x) + (n-r)e_{L/K}.$$

Subtracting $ne_{L/K}$ from this gives the proposed formula. □

Corollary 6.5. *Let $L = K(F[\pi^n])$. The largest fractional ideal of L that is contained in $\log_F(F(\mathfrak{m}))$ is $\mathfrak{m}^{q^{n-1}+1}$.*

Proof. For this L, we have $e_1 = q^{n-1}$. Let $\lambda \in L$ be a primitive π^n-torsion point. We know that $\log_F$ induces an isomorphism between $F(\mathfrak{m}^{q^{n-1}+1})$ and $\mathfrak{m}^{q^{n-1}+1}$, which demonstrates containment in one direction. Next we show that no element of $\log_F(F(\mathfrak{m}))$ has valuation q^{n-1}. Suppose $x \in F(\mathfrak{m})$ and $v_L(\log_F(x)) = q^{n-1}$. If $v_L(x)$ lies in the set S of the above proposition, then $v_L(x) = q^i$ for some $0 \leq i \leq n-1$. But if this is the case then $x \equiv [a](\lambda) \mod \lambda^{q^i+1}$ for some $a \in K$ with $v_K(a) = i$. So if we let $x' = x \underset{F}{-} [a](\lambda)$ then we will have $v_L(x') > v_L(x)$. Repeating this procedure as necessary, we obtain $x' \in F(\mathfrak{m})$ such that $x = x' \underset{F}{+} \xi$ for some $\xi \in F[\pi^n]$, $v_L(x') \geq v_L(x)$, and $v_L(x') \notin S$. Thus $\log_F(x) = \log_F(x')$ since $\log_F(\xi) = 0$. Also, because the proposition applies to x', we will have

$$q^{n-1} = v_L(\log_F(x')) = q^r v_L(x') - r(q-1)q^{n-1}.$$

If $r < n-1$ then the equation implies that $q \mid v_L(x')$. By our construction of x', this is only possible if $v_L(x') > q^{n-1}$. But if that is the case then we will have $r = 0$, which implies that $v_L(x') = q^{n-1}$, a contradiction. On the other hand, if $n - 1 = r$

then we get $v_L(x') = (n-1)(q-1)+1$ and this implies that $\log_q(\frac{e_1}{v_L(x')}) < n-1$, and hence $r < n-1$. $\square$

Chapter 7

Galois module structure

7.1 Eigenspaces

Suppose that a finite, Galois extension L of K contains the π torsion points $F[\pi]$ of F. Then L contains the π-torsion field $K(F[\pi])$, which is a Galois extension of K with group Δ. Let $\omega : G = \mathrm{Gal}(L/K) \to \mathcal{O}_K^\times$ be the composition of the quotient map $G \to \Delta$ with the Teichmüller character $\chi|_\Delta : \Delta \xrightarrow{\sim} \mu_{q-1} \subset \mathcal{O}_K^\times$. That is, ω is the character of G giving its action on the free $\mathcal{O}_K/(\pi)$-module $F[\pi]$. For integers r, let

$$F(\mathfrak{m})^{(r)} = \{x \in F(\mathfrak{m}) : \delta(x) = [\omega(g)^r](x) \text{ for all } g \in G\}$$

be the eigenspace for ω^r acting on $F(\mathfrak{m})$. If L/K is abelian, each $F(\mathfrak{m})^{(r)}$ is a module for the $\mathcal{O}_K$-group ring of $\mathrm{Gal}(L/K(F[\pi]))$. Since ω surjects onto μ_{q-1}, we have $F(\mathfrak{m})^{(r)} = F(\mathfrak{m})^{(s)}$ if and only if $r \equiv s \mod q-1$. We shall identify the

eigenspaces by the unique r in the range $2 \leq r \leq q$. Note that $F[\pi^m] \subset F(\mathfrak{m})^{(1)}$, for m as in Theorem 6.1, because χ factors through ω.

When the exact sequence

$$1 \to \mathrm{Gal}(L/K(F[\pi])) \to G \to \Delta \to 1$$

is split, we can say more. In this case $\mathcal{O}_K G$ contains a set of mutually orthogonal idempotents $\{\varepsilon_r\}_{r=2}^{q}$, where

$$\varepsilon_r = \frac{1}{q-1} \sum_{\delta \in \Delta} \omega(\delta)^{-r} \delta$$

for $r = 2, \ldots, q$. Then we have $F(\mathfrak{m}) = \bigoplus_{r=2}^{q} F(\mathfrak{m})^{(r)}$ because $F(\mathfrak{m})^{(r)} = [\varepsilon_r](F(\mathfrak{m}))$.

Lemma 7.1. *If $L = K(F[\pi^n])$ then, for every $i \geq 1$, we have $F(\mathfrak{m}^i)^{(r)} = F(\mathfrak{m}^{i+1})^{(r)}$ unless $i \equiv r \mod q-1$ and $F(\mathfrak{m}^i)^{(r)}/F(\mathfrak{m}^{i+q-1})(r) \cong \mathbb{F}_q$.*

Proof. Note that $G = \mathrm{Gal}(L/K)$ decomposes as $G = \Delta \times \Gamma$ with $\Gamma = \mathrm{Gal}(L/K(F[\pi]))$. We know that $\mathrm{Gal}(L/K(F[\pi])) \cong U_K^{(1)}/U_K^{(n)}$. Take an arbitrary element $\alpha \in F(\mathfrak{m}^i)$ and apply the endomorphism $[\varepsilon_r]$ to it. This endomorphism acts as the projection onto the direct summand $F(\mathfrak{m}^i)^{(r)}$. We will show that, modulo $\mathfrak{m}^{i+1}$, the result is zero if $i \not\equiv r \mod q-1$, or α otherwise. The statements follow from this.

Suppose λ is a primitive π^n-torsion point of F and write $\alpha = u\lambda^i$ for $u \in \mathcal{O}_L^\times$. For $\delta \in \Delta$, we have $\delta(x) \equiv x \mod \mathfrak{m}$ since L/K is totally ramified, and

$$\delta(\lambda^i) = \delta(\lambda)^i = ([\omega(\delta)](\lambda))^i \equiv \omega(\delta)^i \lambda^i \mod \mathfrak{m}^{i+1}.$$

We conclude that $\delta(\alpha) \equiv u\omega(\delta)^i\lambda^i \mod m^{i+1}$. Then

$$\begin{aligned}[(q-1)\varepsilon_r](\alpha) &\equiv \sum_{\delta\in\Delta}{}_F[\omega(\delta)^{-r}](u\omega(\delta)^i\lambda^i) \mod \mathfrak{m}^{i+1} \\ &\equiv \sum_{\delta\in\Delta} u\omega(\delta)^{i-r}\lambda^i \mod \mathfrak{m}^{i+1}.\end{aligned}$$

This is zero modulo $\mathfrak{m}^{i+1}$ unless $i \equiv r \mod q-1$. On the other hand, if $i \equiv r \mod q-1$ then we have

$$[(q-1)\varepsilon_r](\alpha) \equiv (q-1)u\lambda^i \equiv -u\lambda^i \mod \mathfrak{m}^{i+1}.$$

So, multiplying by $q-1$, we have

$$[\varepsilon_r](\alpha) \equiv \begin{cases} 0 \mod \mathfrak{m}^{i+1} & \text{if } i \not\equiv r \mod q-1, \\ \alpha \mod \mathfrak{m}^{i+1} & \text{if } i \equiv r \mod q-1. \end{cases}$$

□

7.2 Higher ramification and filtration

The Galois group of L/K is denoted by G. Recall the function i_G defined by Serre in [Ser, Ch. IV, §1]: if $\lambda \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\lambda]$ then for $g \in G$,

$$i_G(g) = v_L(g(\lambda) - \lambda).$$

This is also equal to $\inf\{v_L(g(x)-x) : x \in \mathcal{O}_L\}$. From [Bon, La. 3.1], we know that for any $x, y \in \mathfrak{m}$, we have $v_L(x-y) = v_L(x \underset{F}{-} y)$. Thus also $i_G(g) = v_L(g(\lambda) \underset{F}{-} \lambda)$.

Lemma 7.2. *Suppose L/K is totally ramified, $g \in G$, and $x \in F(\mathfrak{m})$. Then $v_L(g(x) \underset{F}{-} x) = v_L(x) + i_G(g) - 1$ if $p \nmid v_L(x)$ and otherwise $v_L(g(x) \underset{F}{-} x) \geq v_L(x) + i_G(g)$.*

Proof. When L/K is totally ramified, we can choose λ to be a root of an Eisenstein polynomial with coefficients in K. In this case λ is a uniformizer for L. Letting $i = v_L(x)$, write $x = u\lambda^i$ with $u \in \mathcal{O}_L^\times$. Then we have

$$v_L(g(x) - x) = i + v_L\left(\frac{g(u)}{u}\left(\frac{g(\lambda)}{\lambda}\right)^i - 1\right) \tag{7.1}$$

Now, by the definition of $i_G(g)$,

$$v_L\left(\frac{g(y)}{y} - 1\right) \geq i_G(g) - v_L(y)$$

for any $y \in \mathcal{O}_L$. This tells us that $\frac{g(u)}{u} \in U_L^{(i_G(g))}$ and $\frac{g(\lambda)}{\lambda} \in U_L^{(i_G(g)-1)} - U_L^{(i_G(g))}$. When $p \nmid i$, the i-th power map induces an isomorphism of $U_L^{(i_G(g)-1)}/U_L^{(i_G(g))}$, so also $\left(\frac{g(\lambda)}{\lambda}\right)^i \in U_L^{(i_G(g)-1)} - U_L^{(i_G(g))}$ and thus the right hand side of (7.1) equals $i + i_G(g) - 1$. If instead $p \mid i$ then $\left(\frac{g(\lambda)}{\lambda}\right)^i \in U_L^{(i_G(g))}$ and this gives us the second part of the claim. □

7.3 Non-cyclic eigenspaces

In this section we assume that $K/\mathbb{Q}_p$ is unramified. This would be the case, for example, if K is an imaginary quadratic field, F was obtained from an elliptic curve E with complex multiplication by $\mathcal{O}_K$, and E has good reduction at p, which is either split or inert in K. With $K/\mathbb{Q}_p$ unramified, the principal unit group $U_K^{(1)}$ is a free $\mathbb{Z}_p$-module on generators $\{1 + bp : b \in B\}$, where B is a subset of U_K whose image in $\mathbb{F}_q$ is an $\mathbb{F}_p$-basis. When $L = K(F[\pi^n])$, this means that Γ, which is identified with $U_K^{(1)}/U_K^{(n)}$ by the character χ, will be isomorphic to $(\mathbb{Z}/p^{n-1}\mathbb{Z})^f$,

where $f = f_{K/\mathbb{Q}_p} = [\mathbb{F}_q : \mathbb{F}_p]$. Let $\gamma_1, \ldots, \gamma_f$ be the images in Γ of the generators $\{1 + bp : b \in B\} \subset U_K^{(1)}$. Making the change of variable $T_i = \gamma_i - 1$ for $i = 1, \ldots, f$, we have

$$\mathcal{O}_K\Gamma \cong \mathcal{O}_K[T_1, \ldots, T_f] / \left((1 + T_i)^{p^{n-1}} - 1\right).$$

It is clear that this is a local ring with maximal ideal $(\pi, T_1, \ldots, T_f)$.

The lower jumps of the higher ramification filtration of L/K are known to be q^i for $i = 0, 1, \ldots, n-1$ [Neu, Ch. V, Pr. 6.1]. These are the values of the function i_G and they correspond to upper jumps of $0, 1, \ldots, n-1$.

When $F = \hat{\mathbb{G}}_m$, Sharifi found that all eigenspaces $F(\mathfrak{m})^{(r)}$ except for $r = q$ and $r = q - 1$ are free over $\mathcal{O}_K\Gamma$. In the case where $K \neq \mathbb{Q}_p$, we can identify more eigenspaces that are not free.

Theorem 7.3. *Suppose that $K/\mathbb{Q}_p$ is unramified and let $L = K(F[\pi^n])$ with $n > 1$. For each $2 \leq r \leq q - 1$ such that $p \mid r$, the eigenspace $F(\mathfrak{m})^{(r)}$ is not a cyclic $\mathcal{O}_K\Gamma$-module.*

Proof. If $F(\mathfrak{m})^{(r)}$ is generated by the element u_r then obviously we must have $v_L(u_r) = r$ as this is the smallest valuation of an element in $F(\mathfrak{m})^{(r)}$. We claim that no element of $[\mathcal{O}_K\Gamma]\,(u_r)$ has valuation equal to $r+q-1$. It is clear that $v_L([\phi](u_r)) = r$ for any unit $\phi \in \mathcal{O}_K\Gamma$. The non-units comprise the ideal $(p, T_1, \ldots, T_f)$. But we have $v_L([\pi](u_r)) \geq \min(qr, r + (q-1)q^{n-1})$ by Lemma 6.2 and, applying Lemma 7.2, $v_L([T_i](u_r)) \geq r + 2(q-1)$. Since qr, $r + (q-1)q^{n-1}$, and $r + 2(q-1)$ are all strictly greater than $r + q - 1$, there is no $\phi \in \mathcal{O}_K\Gamma$ such that $v_L([\phi](u_r)) = r + q - 1$. $\square$

Chapter 8

The normal basis theorem for formal modules

In the context of the ring of integers $\mathcal{O}_L$ considered as $\mathcal{O}_K G$-module, the normal basis theorem can be stated as the fact that $\mathcal{O}_L \otimes_{\mathcal{O}_K} K$ is a free module of rank one over the group ring KG.

Theorem 8.1 (Normal basis theorem for formal modules)**.** *The tensor product $F(\mathfrak{m}) \otimes_{\mathcal{O}_K} K$ is a free module of rank one over KG.*

$$\begin{array}{ccc} F(\mathfrak{m}) & \xrightarrow{\log_F} & L \\ \uparrow & & \uparrow \\ F(\mathfrak{m}^i) & \xrightarrow{\sim} & \mathfrak{m}^i \end{array}$$

Proof. Consider the above diagram of $\mathcal{O}_K G$-modules, where i is sufficiently large to make $\log_F$ an isomorphism. We would like to tensor this diagram with K. We have $L \otimes K = L = \mathfrak{m}^i \otimes K$, and by the classical normal basis theorem L is free, rank 1

over KG. Since K is flat over $\mathcal{O}_K$, the bottom arrow in the diagram remains an isomorphism, so $F(\mathfrak{m}^i) \otimes K$ is also isomorphic to KG. Finally, $F(\mathfrak{m}^i) \otimes K$ embeds as a subspace in $F(\mathfrak{m}) \otimes K$ and these are both K-vector spaces of dimension $[L : K]$, as per our Structure Theorem 6.1, which means that the left-hand side becomes an equality as well. $\square$

When L contains $F[\pi]$ and $G \cong \Delta \times \Gamma$ with $\Delta = \mathrm{Gal}(K(F[\pi])/K)$ and $\Gamma = \mathrm{Gal}(L/K(F[\pi]))$, note that the isomorphism in the theorem preserves the eigenspace decomposition from Section 7.1. This is because is it induced by $\log_F$, which commutes with both the Lubin-Tate and the Galois actions, and therefore the idempotents $\{\varepsilon_r\}_{r=2}^{q}$ will pass through. Since each eigenspace is a module for $\mathcal{O}_K\Gamma$, we can see that the $\mathcal{O}_K$ rank of each is $[L : K(F[\pi])] = \frac{[L:K]}{q-1}$.

Chapter 9

Tame extensions

Recall from Chapter 2 that Emmy Noether proved that $\mathcal{O}_L$ is free over $\mathcal{O}_K G$ if and only if L/K is tame. In this chapter we will focus on some specific cases of tame extensions and determine whether $F(\mathfrak{m})$ is a free $\mathcal{O}_K G$-module.

9.1 Unramified extensions

One class of tame extensions is the unramified extensions. These extensions have $e_{L/K} = 1$, but we will use a weaker assumption in the theorem.

Theorem 9.1. *Suppose that $e_{L/K} < q - 1$ and L/K is tame. Then $F(\mathfrak{m})$ is free over $\mathcal{O}_K G$.*

Proof. The power series $\log_F$ and $\exp_F$ induce isomorphisms on the elements of valuation greater than $\frac{v_L(\pi)}{q-1}$. With our assumption, this means that $F(\mathfrak{m}) \cong \mathfrak{m}$ as $\mathcal{O}_K G$-modules. We know from [Ull, Th. 1] that $\mathfrak{m}$ is a free $\mathcal{O}_K G$-module. □

9.2 The tame torsion field

Among the torsion fields $K(F[\pi^n])$ of F, which are a particular focus of this thesis, the only one which is tame is the π-torsion field $K(F[\pi])$. Let's investigate freeness of this extension.

Theorem 9.2. *Let $L = K(F[\pi])$. There is an isomorphism of $\mathcal{O}_K G$-modules $F(\mathfrak{m}) \cong F[\pi] \oplus \mathcal{O}_K G$.*

Proof. For this L we have $e_{L/K} = q - 1$, so $\log_F$ induces an isomorphism between $F(\mathfrak{m}^2)$ and $\mathfrak{m}^2$. Thus we have a G-equivariant exact sequence

$$0 \to F[\pi] \to F(\mathfrak{m}) \xrightarrow{\log_F} \mathfrak{m}^2 \to 0$$

that is split by $\exp_F : \mathfrak{m}^2 \to F(\mathfrak{m}^2)$ and the quotient $F(\mathfrak{m})/F(\mathfrak{m}^2)$ is isomorphic to $F[\pi]$. Now the statement follows from [Ull, *loc. cit.*]. □

Chapter 10

The associated order

H.-W. Leopoldt created the associated order of an extension of number fields in order to recover freeness of the ring of integers in the presence of wild ramification. When $\mathcal{O}_L$ is replaced by $F(\mathfrak{m})$, we can still define an associated order and use it to investigate whether the resulting module is free.

10.1 Definition

In view of Theorem 8.1, we may define the **associated order** of a Lubin-Tate module. The group ring KG acts on $F(\mathfrak{m}) \otimes K$; this K-vector space contains $F(\mathfrak{m})$ modulo torsion as an $\mathcal{O}_K G$-submodule. Write $F(\mathfrak{m})_{\text{free}}$ for the image of $F(\mathfrak{m})$ in $F(\mathfrak{m}) \otimes K$, which may be identified with $F(\mathfrak{m})$ modulo torsion. Alternatively, $F(\mathfrak{m})_{\text{free}}$ is isomorphic to $[\pi^n](F(\mathfrak{m}))$ for any n that is large enough to kill all of the

F-torsion in L. Now the associated order of $F(\mathfrak{m})$ is defined as

$$\mathfrak{A}_{F(\mathfrak{m})} = \{\phi \in KG : \phi(x) \in F(\mathfrak{m})_{\text{free}} \text{ for all } x \in F(\mathfrak{m})_{\text{free}}\}.$$

It is an $\mathcal{O}_K$-order in KG and clearly $\mathcal{O}_K G \subseteq \mathfrak{A}_{F(\mathfrak{m})}$. For a particular $\phi \in \mathcal{O}_K G$ and $m \geq 0$, a sufficient condition for $\pi^{-m}\phi$ to be in $\mathfrak{A}_{F(\mathfrak{m})}$ is that $\phi(F(\mathfrak{m})) \subseteq [\pi^m](F(\mathfrak{m}))$. It seems likely, however, that this is also a necessary condition.

When $L \supset F[\pi]$ and $G = \Delta \times \Gamma$, the eigenspaces $F(\mathfrak{m})^{(r)}$ have an associated order in $K\Gamma$ defined as for $F(\mathfrak{m})$. These associated orders may be identified with the ideals $\varepsilon_r \mathfrak{A}_{F(\mathfrak{m})}$. When $r \neq q$, the eigenspace is free as an $\mathcal{O}_K$-module, so the two criteria—$\pi^{-m}\phi$ mapping $F(\mathfrak{m})_{\text{free}}$ into itself or ϕ having image contained in the image of $[\pi^m]$—are equivalent.

10.2 Some nonintegral elements of the associated order

As in Section 7.3, we assume that $K/\mathbb{Q}_p$ is unramified. We will make use of the description of $\mathcal{O}_K\Gamma$ as $\mathcal{O}_K[T_1, \ldots, T_f]/\left((1+T_i)^{p^{n-1}} - 1\right)$ and the upper ramification break at $0, 1, \ldots, n-1$.

Theorem 10.1. *Suppose that $K/\mathbb{Q}_p$ is unramified with $q = p^2$ and let $L = K(F[\pi^2])$. Then*

$$\frac{1}{\pi} \sum_{\sigma \in G} \chi(\sigma)^{-r} \sigma$$

is an element of the associated order $\mathfrak{A}_{F(\mathfrak{m})}$ *for* $r = 2, \ldots, q-2$.

Proof. Write $N_\Gamma = \sum_{\gamma \in \Gamma} \gamma \in \mathcal{O}_K G$. Then we have

$$\sum_{\sigma \in G} \chi(\sigma)^{-r} \sigma \equiv \varepsilon_r N_\Gamma \mod \pi$$

because $\chi(\gamma) \in U_K^{(1)}$ for $\gamma \in \Gamma$. So it is a question of showing that $[N_\Gamma](F(\mathfrak{m})^{(r)}) \subseteq [\pi](F(\mathfrak{m})^{(r)})$ for all r except q and $q-1$. With T_i as in Section 7.3, we have the congruence

$$N_\Gamma \equiv \prod_{i=1}^{2} T_i^{p-1} \mod p.$$

We will show that $T_1^{p-1} T_2^{p-1}$ must increase the valuation of an element of $F(\mathfrak{m})^{(r)}$ so that it becomes greater than q^2. By Corollary 6.3, this means that it lies in the image of $[\pi]$.

Lemma 7.2 and our knowledge of the higher ramification filtration tell us that $v_L([T_1](x)) \geq v_L(x) + q - 1$, for $x \in F(\mathfrak{m})^{(r)}$. After applying T_1 a total of $p-1$ times, we can correct by an element of $[\pi](F(\mathfrak{m}))$ to get $[1 + \gamma_1 + \cdots + \gamma_1^{p-1}](x)$, which lies in the fixed field of $\langle \gamma_1 \rangle$. Call this element y. Now $v_L([T_2](y)) \geq v_L(y) + p(q-1)$ since $[L : L^{\langle \gamma_1 \rangle}] = p$ and Lemma 7.1 says that the valuation must remain congruent to $v_L(y)$ modulo $q-1$. Therefore the minimum increase in valuation from applying $T_1^{p-1} T_2^{p-1}$ is $(q-1)^2$.

If we begin with $v_L(x) \geq 2(q-1)$ then the above increase is sufficient for $[N_\Gamma](x)$ to lie in the image of $[\pi]$. Among the positive integers less than $2(q-1)$, we have ruled out $r = q-1$ and $r = q$. We may therefore assume in what follows that $q \nmid r$ and $r \not\equiv -1 \mod q$.

It will be sufficient to show an additional increase of at least $2(q-1)$ in order to ensure that $v_L([N_\Gamma](x)) > q^2$. When $v_L(x) \not\equiv -1 \mod p$, one of the numbers $v_L(x), v_L(x)+q-1, \ldots, v_L(x)+(p-2)(q-1)$ is divisible by p. Lemmas 7.2 and 7.1 imply that T_1 will increase valuation by at least $2(q-1)$ when we encounter a valuation divisible by p. In the case when $v_L(x) \equiv -1 \mod p$, we have $v_L(y) \equiv v_L(x)-(p-1) \mod q$. Like with T_1, when applying T_2, we will be forced to take an extra step of $p(q-1)$ unless $v_L(y) \equiv -p \mod q$. This would imply that $v_L(x) \equiv -1 \mod q$, which is addressed above.

It remains to demonstrate a further increase of $q-1$ in the case where $v_L(x) \not\equiv -1 \mod p$ and where the application of T_1^{p-1} produced a total increase in valuation of just $p(q-1)$. When this happens we will have $v_L(y) \equiv v_L(x) - p \mod q$. Since we have assumed $v_L(x) \not\equiv 0 \mod q$, we have $v_L(y) \not\equiv -p \mod q$ and, as above, this results in a larger jump while applying T_2^{p-1}. □

As noted in the proof of the theorem, the specified element may be viewed as an element of the associated order of the eigenspace $F(\mathfrak{m})^{(r)}$. The presence of a nonintegral element in the associated order clearly implies that that eigenspace is not free over $\mathcal{O}_K\Gamma$. So the above result stands in contrast to Theorem 4.1 because it was precisely the eigenspaces with r not equal to p or $p-1$ that were free in the case of $\hat{\mathbb{G}}_m$.

10.3 The Kummer pairing

Another method for detecting when $\phi(F(\mathfrak{m})) \subseteq [\pi^m](F(\mathfrak{m}))$ is to use the **Kummer pairing**.[3] It is a map

$$\langle \cdot, \cdot \rangle_m : L^\times \times F(\mathfrak{m}) \to F[\pi^m],$$

where $m \geq 1$ is an integer such that L contains the group $F[\pi^m]$ of π^m-torsion points of F. If $\alpha \in L^\times$ and $\beta \in F(\mathfrak{m})$ then $\langle \alpha, \beta \rangle_m$ is defined to be $\sigma_\alpha(\gamma) \underset{F}{-} \gamma$, where σ_α is the element of G_L^{ab} associated to α by reciprocity and $\gamma \in \overline{\mathbb{Q}}_p$ is such that $[\pi^m](\gamma) = \beta$. The Kummer pairing has the property that $\langle \alpha, \beta \rangle_m = 0$ for all $\alpha \in L^\times$ if and only if $\beta \in [\pi^m](F(\mathfrak{m}))$.

Theorem 10.2. *Suppose that $K/\mathbb{Q}_p$ is unramified and let $L = K(F[\pi^n])$ with $n \geq 2$. Then*

$$\frac{1}{\pi} \sum_{\sigma \in G} \chi(\sigma)^{-1} \sigma$$

is not an element of the associated order $\mathfrak{A}_{F(\mathfrak{m})}$.

Proof. Let α be an element of $L^\times$ and $\beta \in F(\mathfrak{m})$. We have

$$\begin{aligned}
\left\langle \alpha, \left[\sum_{\sigma \in G} \chi(\sigma)^{-1} \sigma \right] (\beta) \right\rangle_1 &= \sum_{\sigma \in G} \underset{F}{\sigma} \left(\left\langle \sigma^{-1}(\alpha), [\chi(\sigma)^{-1}](\beta) \right\rangle_1 \right) \\
&= \sum_{\sigma \in G} \underset{F}{\left\langle \sigma^{-1}(\alpha), [\chi(\sigma)\chi(\sigma)^{-1}](\beta) \right\rangle_1} \\
&= \left\langle N_{L/K}(\alpha), \beta \right\rangle_1 .
\end{aligned}$$

[3] This pairing is called the *local Kummer symbol* in [Lan, Ch. 8, §5] and the *generalized Hilbert pairing* in [FV, Ch. VIII, §2].

Now, L is the class field of $\pi^{\mathbb{Z}} U_K^{(n)}$ and, since $(L^\times)^p$ is a subgroup of the left kernel of the pairing, we will start with the observation that $U_K^{(n)} \subseteq (L^\times)^p$. This comes from the assumption that $K/\mathbb{Q}_p$ is unramified, for then $U_K^{(n)} \subseteq (K^\times)^{p^{n-1}} \subseteq (L^\times)^p$.

It remains to show that $\langle \pi, \beta \rangle_1 \neq 0$ for some β. For this β, take a so-called *π-primary element*. Such elements can be obtained as $\beta = E_F(a[\pi](X))\big|_{X=\lambda}$ where a is any element of $\mathcal{O}_K$, λ is a primitive π^n-torsion point, and E_F is the Artin-Hasse exponential associated to F [FV, Ch. VIII, §2.3]. For this β we have $\langle \pi, \beta \rangle_1 = [a](\lambda)$ and clearly this may be nonzero. □

10.4 Comparison to the additive, Kummer case

Cassou-Noguès and Taylor have determined the associated order of the ring of integers of the division fields of F in the "Kummer" case, that is, considering $K(F[\pi^{m+r}])$ as an extension of $K(F[\pi^r])$ for integers $r \geq m \geq 1$. Use the notation $M = K(F[\pi^r])$ and $N = K(F[\pi^{m+r}])$, so that N/M is a Galois extension with group isomorphic to $F[\pi^m]$. Specifically, we fix a primitive π^{m+r}-torsion point α and define $\psi : \Gamma = \mathrm{Gal}(N/M) \to F[\pi^m]$ by $\psi(\gamma) = \gamma(\alpha) \underset{F}{-} \alpha$. This map is an isomorphism known as the *Kummer isomorphism*. In [CNT, Ch. X], the authors consider the ring of integers $\mathcal{O}_N$ as an additive Γ-module. They determine that the associated order of this module inside $M\Gamma$ is

$$\mathfrak{A}_{N/M} = \mathcal{O}_M + \sum_{i=0}^{q^m-2} \mathcal{O}_M \sigma_i,$$

where $\sigma_i = \frac{1}{\pi^m} \sum_{\gamma \in \Gamma} \psi(\gamma)^i(\gamma - 1)$.

We would like to make a comparison between their associated order and the elements of $\mathfrak{A}_{F(N)}$ described in Theorems 10.1 and 10.2. An obstacle to this comparison is that while the Galois module $\mathcal{O}_M$ can use $\mathcal{O}_N$ as its ring of scalars, a Lubin-Tate formal group only admits scalar multiplication by $\mathcal{O}_K$. Therefore we will compute the intersection of $\mathfrak{A}_{N/M}$ with $K\Gamma$.

Proposition 10.3. *The intersection of $\mathfrak{A}_{N/M}$ with $K\Gamma$ is generated as an $\mathcal{O}_K\Gamma$-module by $\tau_i = \frac{1}{\pi^{m-i}} \sum_{\gamma \in H_i} \gamma$ for $i = 0, \ldots, m-1$, where $H_i = \mathrm{Gal}(N/K([\pi^{i+r}]))$.*

Proof. It is clear that $\tau_i \in K\Gamma$ for all i. Next we show that $\tau_i \in \mathfrak{A}_{N/M}$. Let $M_i = N^{H_i}$, so that $M = M_0 \subset M_1 \subset \cdots \subset M_m = N$. Then we have $\mathfrak{A}_{N/M} \cap K\Gamma = \mathfrak{A}_{N/M_0} \cap K\Gamma \supseteq \mathfrak{A}_{N/M_1} \cap K\Gamma \supseteq \cdots \supseteq \mathfrak{A}_{N/M_m} \cap K\Gamma = \mathcal{O}_K$. By Cassou-Noguès and Taylor's result, τ_i is an element of $\mathfrak{A}_{N/M_{m-i}}$ (it is the σ_0 generator).

To finish the proof, we show that if ϕ is any element of $\mathfrak{A}_{N/M} \cap K\Gamma$ then the coefficients of the elements of $H_i - H_{i+1} \subset \Gamma$ agree up to an element of $\mathcal{O}_K$.

If $\theta \in \mathrm{Gal}(M/K)$ then it restricts to an automorphism of $F[\pi^m]$. Let θ_* be the automorphism of Γ such that $\theta \circ \psi = \psi \circ \theta_*$. Using the correspondence between θ and θ_*, the Galois group of M/K can act on $\phi \in M\Gamma$ in two ways—write $\theta \cdot \phi$ for θ acting on the coefficients of ϕ and ϕ^θ for the action on elements of Γ via θ_*^{-1}. One checks that these two actions agree on σ_i for all i. Now if we act on $\phi \in \mathfrak{A}_{N/M} \cap K\Gamma$ we are guaranteed to have invariance under the left action because θ fixes K. If we let $\phi = a + \sum_{i=0}^{q^m-2} b_i\sigma_i$ with $a \in \mathcal{O}_M$ then, since $\theta \cdot \sigma_i = \sigma_i^\theta$ for all

i, we have $\phi^\theta - \phi = \phi^\theta - \theta \cdot \phi = a - \theta(a) \in \mathcal{O}_M$, that is, $\phi^\theta - \phi \in \mathcal{O}_M \cap K\Gamma = \mathcal{O}_K$. This proves the above claim, for we note that, since $\mathrm{Gal}(M/K)$ acts transitively on the set of primitive π^i-torsion points, the θ_* act transitively on $H_i - H_{i+1}$ for $i = 0, \ldots, m-1$. □

The π^2-torsion field, the subject of Theorem 10.1, is an instance of a Kummer tower with $r = m = 1$. With $N = K(F[\pi^2])$ and $M = K(F[\pi])$, the proposition says that $\mathfrak{A}_{N/M} \cap K\Gamma$ is generated over $\mathcal{O}_K\Gamma$ by $\tau_0 = \pi^{-1} \sum_{\gamma \in \Gamma} \gamma$. This means that, if the same eigenspace decomposition from Section 7.1 is applied to the additive Galois module $\mathcal{O}_N$, this τ_0 will lie in the associated order of every eigenspace. However, for the points of F in $\mathcal{O}_N$, we have seen in the previous two sections that while τ_0 does indeed lie in the associated order of $F(\mathfrak{m})^{(r)}$ for $r = 2, \ldots, q-2$, the same is not true for $r = q$. We have found by computation of examples that τ_0 may fail to be in the associated order of $F(\mathfrak{m})^{(q-1)}$, but as yet we do not have a proof of a general statement like Theorem 10.2.

Bibliography

[Ber] Anne-Marie Bergé, *À propos de l'ordre associé à l'anneau des entiers d'une extension, d'après H. Jacobinski*, Séminaire de Théorie des Nombres de Bordeaux (1971–1972), Exp. no. 8.

[Bon] Mikhail V. Bondarko, *Cohomology of formal group moduli and deeply ramified extensions*, Mathematical Proceedings of the Cambridge Philosophical Society **135** (2003), no. 1, 19–24.

[Byo] Nigel P. Byott, *Integral Galois module structure of some Lubin-Tate extensions*, Journal of Number Theory **77** (1999), no. 2, 252–273.

[CNT] Philippe Cassou-Noguès and Martin J. Taylor, *Elliptic functions and rings of integers*, Progress in Mathematics, vol. 66, Birkhäuser, 1987.

[CW] John Coates and Andrew Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Inventiones Mathematicae **39** (1977), no. 3, 223–251.

[FV] Ivan B. Fesenko and Sergei V. Vostokov, *Local fields and their extensions*,

2nd ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, 2002.

[Gre] Cornelius Greither, *On Chinburg's second conjecture for abelian fields*, Journal für die reine und angewandte Mathematik **479** (1996), 1–37.

[Haz] Michiel Hazewinkel, *Formal groups and applications*, Pure and Applied Mathematics, vol. 78, Academic Press, 1978.

[Hus] Dale Husemöller, *Elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 111, Springer-Verlag, 2004.

[Lan] Serge Lang, *Cyclotomic fields I and II*, combined 2nd ed., Graduate Texts in Mathematics, vol. 121, Springer-Verlag, 1990.

[Leo] Heinrich-Wolfgang Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, Journal für die reine und angewandte Mathematik **201** (1959), 119–149.

[Mar] Jacques Martinet, *Anneau des entiers d'une extension galoisienne considéré comme module sur l'algèbre du groupe de Galois*, Colloque de Théorie des Nombres de Bordeaux (1969), Bulletin de la Société Mathématique de France, Mémoire **25** (1971), 123–126.

[Neu] Jürgen Neukirch, *Algebraic number theory*, Vol. 322, Springer-Verlag, 1999.

[Noe] E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, Journal für die reine und angewandte Mathematik **167** (1932), 147–152.

[Ser] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, 1979.

[Sha] Romyar T. Sharifi, *Galois module structure of local unit groups*, Algebra & Number Theory **7** (2013), no. 1, 157–191.

[Sil] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, 2009.

[Tho] Lara Thomas, *On the Galois module structure of extensions of local fields*, Actes de la Conférence "Fonctions L et Arithmétique", Publications Mathématiques de Besançon. Algèbre et Théorie des Nombres (2010), 157–194.

[Ull] Stephen V. Ullom, *Integral normal bases in Galois extensions of local fields*, Nagoya Mathematical Journal **39** (1970), 141–146.