Multi-Dimensional Formal Group Laws with Complex Multiplication

by

C. L. Matson

B.A., University of Virginia, 2013

M.S., University of Colorado, 2016

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics

2020

This thesis entitled:
Multi-Dimensional Formal Group Laws with Complex Multiplication
written by C. L. Matson
has been approved for the Department of Mathematics

_____

Prof. David Grant

_____

Prof. Katharine Stange

Date _____

The final copy of this thesis has been examined by the signatories, and we find that both the content and the form meet acceptable presentation standards of scholarly work in the above mentioned discipline.

Matson, C. L. (Ph.D., Mathematics)

Multi-Dimensional Formal Group Laws with Complex Multiplication

Thesis directed by Prof. David Grant

Lubin and Tate used one-dimensional formal group laws over $\mathfrak{p}$-adic fields to generate abelian extensions and, ultimately, to offer another proof of the main theorem of local class field theory. In this thesis we construct an analogue of Lubin-Tate formal group laws in higher dimensions over a $\mathfrak{p}$-adic field K with residue field $k = \mathcal{O}_K/\mathfrak{p}_K$ of order q. Although the method that Lubin and Tate used fails in higher dimensions, we make use of Hazewinkel's functional equation lemma to construct these formal group laws and show that they have $\mathfrak{p}$-integral coefficients. In particular, if $\pi \in \mathcal{O}_K$ is a uniformizer of K and $\Phi(X)$ is a d-tuple of variables $x_{i_1}, \ldots, x_{i_d} \in \{x_1, \ldots, x_d\}$ raised to q-powered exponents then we show that we can construct a d-dimensional formal group law $F_{\pi,\Phi}$ with coefficients in $\mathcal{O}_K$ such that the "multiplication-by-π" endomorphism of $F_{\pi,\Phi}$ is congruent to $\Phi(X)$ modulo $\mathfrak{p}$. We then show that this formal group law has complex multiplication by a direct product of rings of integers of unramified extensions over K, and that the complex-multiplication type of $F_{\pi,\Phi}$ is determined by the form of $\Phi(X)$. Finally, we see that if $\Phi(X)$ is a connected cycle in a certain precise sense then the π^n-torsion of the formal group law $F_{\pi,\Phi}$ generates an abelian extension over the complex multiplication field of $\Phi(X)$ over K.

Dedication

To my parents, whose curiosity and senses of fun fostered the love of learning that got me here.

Acknowledgements

I would like to thank my advisor Dr. David Grant for many helpful conversations and guidance as I wrote this thesis. I am also grateful to the handful of teachers, particularly Rocky Curtis and Francesco Matucci, who sparked my curiosity and nurtured my excitement about mathematics. I also owe thanks to my friends and loved ones for their support, their commiseration, and for many hours of pub trivia. Finally I would like to thank my cat Marshmallow, who is always ready to provide purrs and lap companionship, and whose total lack of interest in my research provided some much-needed perspective.

Contents

Chapter 1

Introduction

In 1965 [12], Jonathan Lubin and John Tate used **(one-dimensional) formal group laws** with **complex multiplication** to recast the main theorem of **local class field theory**. They showed that there exists a unique formal group law $F(x, y)$, a power series over the p-adic integers $\mathbb{Z}_p$, such that $f(x) = px + x^p$ is an endomorphism of F, meaning that $f(F(x, y)) = F(f(x), f(y))$, or simply $F \circ f = f \circ F$. More generally, suppose that K is a $\mathfrak{p}$-*adic field*, or a finite extension of the p-adic rationals $\mathbb{Q}_p$. Let $\mathcal{O}_K$ denote the ring of integers of K, $\pi \in \mathcal{O}_K$ a uniformizer, and $q = |\mathcal{O}_K/\pi\mathcal{O}_K| = |k|$ the order of the residue field k of K. For $f(x)$, $g(x) \in \mathcal{O}_K[[x]]$ we write $f(x) \equiv g(x) \pmod{\deg n}$ to mean that $f(x)$ and $g(x)$ agree on all terms of degree strictly less than n. If we then define

$$\mathcal{F}_\pi = \{f(x) \in \mathcal{O}_K[[x]] : f(x) \equiv \pi x \pmod{\deg 2} \quad \text{and} \quad f(x) \equiv x^q \pmod{\pi}\}$$

then Lubin and Tate showed that for all $f(x) \in \mathcal{F}_\pi$ there exists a unique one-dimensional formal group law F_f over $\mathcal{O}_K$ such that $F_f \circ f = f \circ F_f$. We say that F_f is a *Lubin-Tate formal group law*. For $n \geq 1$ we define $f^n(x) = \underbrace{f \circ f \circ \cdots \circ f(x)}_{n \text{ times}}$ to be the n^{th} iterate of $f(x)$ and, since $f^n(x)$ is an endomorphism of F with $f^n(x) \equiv \pi^n x \pmod{\deg 2}$, we call $f^n(x)$ the *multiplication-by-π^n* map of F and say that its roots, denoted $F[\pi^n]$, are the *π^n-torsion of F*. These generate a tower $K_\pi^n = K(F[\pi^n])$, $n = 1, 2, \ldots$ of extensions which are each totally ramified over K. Lubin and Tate showed that F has *complex multiplication* by the ring of integers of K, meaning that there is a ring monomorphism $i : \mathcal{O}_K \to \mathrm{End}(F)$. They used the endomorphism ring of F to put a module structure on the π^n-torsion, which in turn enabled them to determine the Galois group of K_π^n over K and to show that each of these groups is abelian. Finally, they used this module structure to give

an injective group homomorphism $\rho_K : K^\times \to \mathrm{Gal}(K_{ab}/K)$, where K_{ab} is the maximal abelian extension of K, and showed that this is the same homomorphism given by the Artin symbol $(-, K)$ associated to K via local class field theory.

Tate [16] showed that there is an equivalence of categories between divisible formal group laws over $\mathcal{O}_K$ and connected p-divisible groups over $\mathcal{O}_K$, which has applications to the study of abelian varieties. The significance of formal group laws in number theory goes even further. In 1999, Michael Harris and Richard Taylor [5] used formal group laws to prove the local Langlands conjecture for GL_n over a $\mathfrak{p}$-adic field. Decades after their debut in Lubin's and Tate's 1965 paper, Lubin-Tate formal group laws have also played an interesting role in algebraic topology, particularly in the area of stable homotopy theory [8].

In this thesis we will construct a generalization of these so-called Lubin-Tate formal group laws to higher dimensions and will examine the field extensions generated by their torsion points, but it is worth noting that this is not the first time that the work of Lubin and Tate has been extended.

There have been several generalizations involving one-dimensional formal group laws. Let K_{ur}^∞ denote the maximal unramified extension of K and let $\varphi : K_{ur}^\infty \to K_{ur}^\infty$ be the Frobenius automorphism over K, which is uniquely characterized by $\varphi(x) \equiv x^q \pmod{\pi}$ for all $x \in K_{ur}^\infty$. In [9], Iwasawa used a slightly more general definition of Lubin-Tate formal group law which allowed for coefficients in an unramified extension of K with the possibility of a twist; more precisely, he constructed F to satisfy $f \circ F = (\varphi_* F) \circ f$ where $\varphi_* F$ is obtained from F by applying the Frobenius φ to its coefficients. He built on the ideas of Lubin and Tate to give a lovely and thorough development of local class field theory. This inspired De Shalit [3] to develop a similar generalization called *relative* Lubin-Tate formal group laws. Fix an unramified extension K' over K and let $\zeta \in N_{K'/K}(K'^\times)$ be the norm of a uniformizer in $\mathcal{O}_{K'}$. De Shalit constructed families

$$\mathcal{F}_\zeta = \{f(x) \in \mathcal{O}_{K'}[[x]] : f(x) \equiv \pi' x \pmod{\deg 2} \text{ with } N_{K'/K}(\pi') = \zeta \text{ and } f(x) \equiv x^q \pmod{\pi'}\}$$

and studied the extensions that these generate. Laurent Berger [1] later showed that a certain tower of totally ramified extensions of K must be generated by the torsion points of a relative Lubin-Tate formal group law.

The role of higher-dimensional formal group laws in number theory has also been profound. However, the Lubin-Tate theory has not been fully generalized to higher dimensions. One attempt was made by H.

Koch in [11], but the author shows that these become isomorphic to a direct sum of one-dimensional Lubin-Tate formal groups laws over the maximal unramified extension of K. We will do more here, using a tool that was unnecessary in the one-dimensional case, the functional equation lemma of Hazewinkel. In [6], Michiel Hazewinkel gave a development of the theory of formal group laws that encompassed much of the work that had previously been done on the subject by Honda and others. In particular, he created a higher-dimensional version of Lubin-Tate formal group laws called "formal A-modules" which are formal groups with extra endomorphisms coming from some ring A. However, these are too restrictive to give all formal group laws with complex multiplication. We will use the Hazewinkel's functional equation lemma to construct a higher-dimensional analogue of formal group laws with complex multiplication, and these will prove to be useful for generating abelian extensions of $\mathfrak{p}$-adic fields.

We will now motivate the construction of this higher-dimensional analogue of formal group laws with complex multiplication. In dimension $d \geq 2$, formal group laws and their homomorphisms are d-tuples of power series in $2d$ variables and in d variables, respectively, so we let $X = (x_1, \ldots, x_d)$ and write $f(X)$ to mean

$$f(X) = (f_1(x_1, \ldots, x_d), \ldots, f_d(x_1, \ldots, x_d)).$$

When generalizing $f(x) \in \mathcal{F}_\pi$ to higher dimensions, we must decide on what linear terms and what forms modulo π to consider . The linear term of $f(X)$ is now given by its *Jacobian*, or its $d \times d$ matrix of degree one coefficients. We will typically restrict our attention to $f(X)$ whose Jacobians are diagonal matrices D whose non-zero entries are uniformizers. Such a D is called a *diagonal uniformizer matrix*.

Now we consider which variables may appear in each coordinate power series $f_i(X)$, particularly those which appear modulo π. If, for example, for $1 \leq i \leq d$, $f_i(X)$ depends only on the variable x_i then $f(X) = (f_1(x_1), \ldots, f_d(x_d))$ is the endomorphism of a direct product of one-dimensional formal group laws, so we will allow mixing of variables modulo π in order to study more interesting formal group laws. Likewise, we will also allow freedom in the exponents appearing in the form of $f(X)$ modulo π.

To make this more precise, we start by addressing another way of viewing the construction of Lubin and Tate. Let $h \geq 1$ be a positive integer and let K' be the unique unramified extension of degree h over K. If

$\pi \in \mathcal{O}_K$ is a uniformizer of K then $\pi \in \mathcal{O}_{K'}$, and since K' is unramified then π is a uniformizer of K' as well. Thus if $f(x) \in \mathcal{O}_K[[x]]$ such that $f(x) \equiv \pi x \pmod{\deg 2}$ and $f(x) \equiv x^{q^h} \pmod{\pi}$ then there exists a Lubin-Tate formal group law $F_f(x, y)$ with coefficients in $\mathcal{O}_{K'}$ (in fact, the construction shows the coefficients are in $\mathcal{O}_K$) such that f is an endomorphism of F_f, and F_f has complex multiplication by the ring of integers of K'. This suggests the idea of allowing positive powers of q to appear in the exponents of $f(X)$ modulo π. Let $h_1, \ldots, h_d$ be positive integers and let $j_1, \ldots, j_d \in \{1, \ldots, d\}$ be indices and set $\Phi(X) = \left(x_{j_i}^{q^{h_i}}\right)_{i=1}^{d}$. Such a $\Phi(X)$ is a called a *q-power tuple*.

Define the set of d-tuples of power series in X with zero constant term to be

$$\mathcal{M}_d(\mathcal{O}_K) = \{f(X) = (f_1(X), \ldots, f_d(X)) \in \mathcal{O}_K[[X]]^d : f(0) = 0\}$$

and for D a diagonal uniformizer matrix over $\mathcal{O}_K$ and $\Phi(X)$ a q-power tuple define

$$\mathcal{F}_{D,\Phi} = \{f(X) \in \mathcal{M}_d(\mathcal{O}_K) : f(X) \equiv DX \pmod{\deg 2} \quad \text{and} \quad f(X) \equiv \Phi(X) \pmod{\pi}\}.$$

In this context we can ask the following question.

Question 1.1. If $f(X) \in \mathcal{F}_{D,\Phi}$ then is there a formal group law $F_f(X, Y)$ with coefficients in $\mathcal{O}_K$ such that f is an endomorphism of F_f?

This turns out to be a surprisingly difficult question to answer directly, but it is possible to compute a counterexample $f(X) \in \mathcal{F}_{D,\Phi}$ such that $f(X)$ is an endomorphism of a unique formal group law $F_f(X, Y)$ which has coefficients in K but not in $\mathcal{O}_K$. The question we now ask is:

Question 1.2. Do there exist *any* $f(X) \in \mathcal{F}_{D,\Phi}$ for which there exists a formal group law F_f over $\mathcal{O}_K$ such that f is an endomorphism of F_f?

In Theorem 3.2.5 we see that the answer is yes, and will show that the "complex multiplication type" of F is determined by the q-power tuple $\Phi(X)$. We will also see that $\Phi(X)$ determines the possible forms of our diagonal uniformizer matrix D. Finally, we will show that, under certain conditions, the π^n-torsion of these formal group laws generate abelian extensions over L, an unramified extension of K.

Chapter 2

Preliminaries

2.1 Non-archimedean local fields of characteristic zero and their extensions

We refer the reader to Iwasawa [9] for further details. Let K be a field of characteristic zero that is complete with respect to a discrete valuation v, by which we mean a surjection $v : K \to \mathbb{Z} \cup \{\infty\}$ which for all $x, y \in K$ satisfies

$$\begin{aligned} &v(xy) = v(x) + v(y), \\ &v(x+y) \geq \min\{v(x), v(y)\}, \qquad \text{and} \\ &v(x) = \infty \iff x = 0. \end{aligned}$$

By fixing some $\rho \in \mathbb{R}$ such that $\rho > 1$ we can define a metric $|x|_v = \rho^{-v(x)}$, and we require that K is complete with respect to this metric. Let $\mathcal{O}_K = \{x \in K : v(x) \geq 0\}$ and let $\mathfrak{p}_K = \{x \in K : v(x) > 0\}$. We will see in the lemma below that $\mathcal{O}_K$ is a local ring and $\mathfrak{p}_K$ is its unique maximal ideal. If $k = \mathcal{O}_K/\mathfrak{p}_K$ is a finite field, we say that K is a *non-archimedian local field* of characteristic zero, or simply a $\mathfrak{p}$-*adic field*. It can be shown that every $\mathfrak{p}$-adic field is equivalent to a finite extension of $\mathbb{Q}_p$; for details, see [9].

Theorem 2.1.1. *$\mathcal{O}_K$ is a local ring with unique maximal ideal $\mathfrak{p}_K$. Furthermore, $\mathfrak{p}_K$ is principally generated by any $\pi \in K$ satisfying $v(\pi) = 1$.*

Proof. It is clear that $0 \in \mathcal{O}_K$ since $v(0) = \infty \geq 0$. We next observe that $1 \in \mathcal{O}_K$ because

$$v(1) = v(1 \cdot 1) = v(1) + v(1)$$

which implies that $\nu(1) = 0$. We can see that $\mathcal{O}_K$ is closed under both addition and multiplication since if $x, y \in \mathcal{O}_K$ then $\nu(x) \geq 0$ and $\nu(y) \geq 0$, so

$$\nu(x+y) \geq \min\{\nu(x), \nu(y)\} \geq 0 \quad \text{and}$$
$$\nu(xy) = \nu(x) + \nu(y) \geq 0.$$

This completes the proof that $\mathcal{O}_K$ is a subring of K.

We next see that $\mathfrak{p}_K$ is a prime ideal of $\mathcal{O}_K$. We can see by a similar argument to the one above that $\mathfrak{p}_K$ is closed under both addition and multiplication by arbitrary elements of $\mathcal{O}_K$, so it forms an ideal of $\mathcal{O}_K$. Furthermore, for $x, y \in \mathcal{O}_K$

$$xy \in \mathfrak{p}_K \implies \nu(xy) = \nu(x) + \nu(y) > 0$$

which implies that either $x \in \mathfrak{p}_K$ or $y \in \mathfrak{p}_K$. Finally, it is clear that $1 \notin \mathfrak{p}_K$ since $\nu(1) = 0$. Thus $\mathfrak{p}_K$ is a prime ideal of $\mathcal{O}_K$.

We determine that $\mathfrak{p}_K$ is the unique maximal ideal of $\mathcal{O}_K$ by showing that every element outside of $\mathfrak{p}_K$ is a unit. Let $x \in \mathcal{O}_K$ be nonzero and let $x^{-1} \in K$ be its inverse. Observe that since

$$\nu(x) + \nu\left(x^{-1}\right) = \nu\left(x \cdot x^{-1}\right) = \nu(1) = 0$$

then $x^{-1} \in \mathcal{O}_K$ if and only if $\nu(x) = -\nu(x^{-1}) = 0$. In other words,

$$\mathcal{O}_K^\times = \{x \in K : \nu(x) = 0\} = \mathcal{O}_K - \mathfrak{p}_K.$$

This proves that $\mathfrak{p}_K$ is the unique maximal ideal of $\mathcal{O}_K$.

Finally, we show that $\mathfrak{p}_K$ is principally generated. Let $\pi \in K$ be any element with $\nu(\pi) = 1$. Let $x \in \mathfrak{p}_K$, so $\nu(x) \geq 1$. Then $\nu(x/\pi) = \nu(x) - \nu(\pi) \geq 0$ so if we write $y = x/\pi$ then $y \in \mathcal{O}_K$ and $x = \pi \cdot y$. We conclude that $\mathfrak{p}_K$ is principally generated in $\mathcal{O}_K$ by any element $\pi \in K$ with valuation equal to one, and that elements of valuation one exist by our assumption that $\nu : K^\times \to \mathbb{Z}$ is surjective. □

We say that $\mathcal{O}_K$ is the *ring of integers of* K. If $\pi \in K$ satisfies $\nu(\pi) = 1$ then we say that π is a *uniformizer*. We call $k = \mathcal{O}_K/\mathfrak{p}_K$ the *residue field* of K.

Example 2.1. Fix a prime $p \in \mathbb{Z}$ and consider the p-adic rationals $\mathbb{Q}_p$, the fraction field of the p-adic integers $\mathbb{Z}_p$. Recall that the p-adic valuation is given on $\mathbb{Z}$ by $\nu_p(x) = n$ where $x \in \mathbb{Z}$ can be written as $x = p^n u$ for some $u \in \mathbb{Z}$ with $p \nmid u$, and the p-adic integers $\mathbb{Z}_p$ are the completion of $\mathbb{Z}$ with respect to the metric $|x| = p^{-\nu_p(x)}$. This valuation is extended to $\mathbb{Q}_p$ by setting $\nu(x/y) = \nu(x) - \nu(y)$. Then $K = \mathbb{Q}_p$ is a non-archimedean local field of characteristic zero and its ring of integers is $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \nu_p(x) \geq 0\}$ with unique maximal ideal $p\mathbb{Z}_p$. It is worth noting that $\mathfrak{p}_K$ is also generated by any $\pi = a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$ with $a_i \in \{0, \ldots, p-1\}$ and $a_1 \neq 0$. We conclude that $p\mathbb{Z}_p^\times$ is the set of uniformizers of $\mathbb{Q}_p$.

We now wish to investigate extensions of K. We first recall some facts about finite fields and their extensions. Let $k = \mathcal{O}_K/\mathfrak{p}_K$ be the residue field of K, with $q = |\mathcal{O}_K/\mathfrak{p}_K|$, and fix an algebraic closure Ω_k over k. The Galois group of Ω_k over k is topologically generated by the automorphism $\varphi_k : \Omega_k \to \Omega_k$ defined by $\varphi(x) = x^q$, which is called the Frobenius automorphism over k. For every $n \in \mathbb{Z}^+$ there exists a unique extension k_n of degree n over k, and if $\varphi_n = \varphi_k|_{k_n}$ is the restriction of the Frobenius to k_n then $\mathrm{Gal}(k_n/k) = \langle \varphi_n \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

Theorem 2.1.2. *Let L be a finite extension of K.*

(1) There exists a unique positive integer e and a unique valuation $\nu_L : L \to \mathbb{Z} \cup \{\infty\}$ satisfying $\nu_L(x) = e \cdot \nu_K(x)$ for all $x \in K$, and L is complete with respect to ν_L. We say that e is the ramification degree of L over K.

(2) Let $\tilde{L} = \mathcal{O}_L/\mathfrak{p}_L$ be the residue field of L. Then $\tilde{L}$ is a finite extension of k and we say that $f = [\tilde{L} : k]$ is the residue degree of L over K.

(3) If e is the ramification degree of L over K and f is the residue degree of L over K then $[L : K] = ef$.

Proof. See [9] for the proof. □

If L is an extension over K such that the ramification degree of L over K is equal to one, we say that L is *unramified* over K. Just as there is a unique extension k_n of degree n over the residue field k for every positive integer n, by Hensel's lemma there is a unique unramified extension K_n of degree n over K which satisfies $\mathcal{O}_{K_n}/\mathfrak{p}_{K_n} \cong k_n$. We obtain this extension as the splitting field of the polynomial $f_n(x) = x^{q^n} - x$ and

can see that it is unramified over K since the full degree $[K_n : K] = n$ is equal to the unramified degree of K_n over K. The union of all of the finite unramified extensions of K is called the maximal unramified extension of K and is denoted by K_{ur}^{∞}. This extension is infinitely generated, so it is not a priori complete. We denote the completion of K_{ur}^{∞} by $\bar{K}$. There exists a unique element of the Galois group of K_{ur}^{∞} over K which lifts φ_k. We call this the Frobenius of K, denoted by $\varphi = \varphi_K$, and note that if n is a positive integer then $\mathrm{Gal}(K_n/K) = \langle \varphi|_{K_n} \rangle \cong \mathbb{Z}/n\mathbb{Z} \cong \mathrm{Gal}(k_n/k)$. The Galois group of $\bar{K}$ over K is given by an inverse limit over all of the finite unramified extensions of K.

Theorem 2.1.3. *The Galois group $G = \mathrm{Gal}\,(K_{ur}^{\infty}/K) \cong \hat{\mathbb{Z}}$ via $\varphi \mapsto 1$, where $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ is the profinite completion of $\mathbb{Z}$. We say that φ is a topological generator of G since it generates a subgroup which is isomorphic to the integers and is therefore dense in the profinite topology on $\hat{\mathbb{Z}}$.*

The Galois group of K_{ur}^{∞} over K also acts naturally on $\bar{K}$.

Finally, we look at the main theorem of local class field theory, which was re-proven by Lubin and Tate using one-dimensional formal group laws.

Theorem 2.1.4. *Let K be a $\mathfrak{p}$-adic field with uniformizer π. Then there exists a homomorphism*

$$\rho_K : K^{\times} \to \mathrm{Gal}(K_{ab}/K)$$

and if L is any finite abelian extension of K then

$$\rho_K\Big(N_{L/K}\,(L^{\times})\Big)\Big|_K = 1.$$

In particular, ρ_K is uniquely characterized by the two conditions

(1) $\rho_K(\pi^n u)|_{K_{ur}^{\infty}} = \varphi^n$ for any uniformizer $\pi \in \mathfrak{p}_K$ and unit $u \in \mathcal{O}_K^{\times}$, and

(2) If L is an extension of K with $\pi \in N_{L/K}\,(L^{\times})$ then L is totally ramified over K and $\rho_K(\pi)|_L = 1$.

Proof. See [9] for the proof. □

2.2 Formal group laws over $\mathfrak{p}$-adic fields

2.2.1 Definitions and examples

To motivate the definition of a formal group law we will start with two examples. First, consider the standard way of viewing a free module as an abelian group. Let A be any ring and $N = A^d$ a free module of rank d over A. Let $a = (a_1, \dots, a_d), b = (b_1, \dots, b_d) \in N$. Since $a + b = (a_1 + b_1, \dots, a_d + b_d)$ we can say that addition is given by the polynomials $F_1(X, Y) = x_1 + y_1$, $F_2(X, Y) = x_2 + y_2$, and so on. As a more interesting example, we consider a rule for describing multiplication after a change of coordinates. Let K be a non-archimedean local field of characteristic zero and let $\mathcal{O}_K$ be its ring of integers, so that $\mathcal{O}_K$ is complete with respect to the prime ideal $\mathfrak{p}_K$. Let $U(K) = \{x \in \mathcal{O}_K : x \equiv 1 \pmod{p_K}\}$. If $u, v \in U(K)$ then we can write $u = 1 + a\pi$ and $v = 1 + b\pi$ for some $a, b \in \mathcal{O}_K$. Both the product $uv = 1 + a\pi + b\pi + (a\pi)(b\pi)$ and $u^{-1} = 1 - a\pi + (a\pi)^2 - (a\pi)^3 + \dots$ can be expressed in terms of power series in $a\pi$ and $b\pi$. This inspires us to make a change of coordinates so that $1 \mapsto 0$ and then define a formal group law $\mathbb{G}_m(x, y) = (x + 1)(y + 1) - 1 = x + y + xy$.

These are not the only ways of writing down a valid abelian group operation on $\mathfrak{p}_K^d$ by using d-tuples of power series in $2d$ variables. We will use x and y to refer to individual variables and will use $X = (x_1, \dots, x_d)$ and $Y = (y_1, \dots, y_d)$ to refer to d-tuples of variables.

Definition 2.2. Let R be a commutative ring with unit, let $X = (x_1, \dots, x_d)$ and $Y = (y_1, \dots, y_d)$ be d-tuples of variables and let $F(X, Y) \in (R[[X, Y]])^d$ be a d-tuple of power series. We will often think of these tuples as column vectors so that we can multiply on the left by $d \times d$ matrices. Write $X +_F Y := F(X, Y)$ as a reminder that we want to think of F as "adding" together the points X and Y. We say that F is a *(commutative) formal group law of dimension d over R* if it satisfies the following axioms:

(FG1) $X +_F Y \equiv X + Y \pmod{\deg 2}$, or equivalently $F_i(X, Y) = x_i + y_i +$ (higher degree terms)

(FG2) $(X +_F Y) +_F Z = X +_F (Y +_F Z)$

(FG3) $X +_F Y = Y +_F X$

If F satisfies these axioms then we may derive two additional properties:

(FG4) $X +_F \mathbf{0} = \mathbf{0} +_F X = X$, where $\mathbf{0} = (0, \ldots, 0)$ is the zero d-tuple. This requires only property (FG2).

(FG5) There exists a unique d-tuple of power series $i_F(X) \in R[[X]]^d$ such that $X +_F i_F(X) = \mathbf{0}$; this requires only property (FG1).

We denote the set of all formal group laws over R of dimension d by $\mathcal{FG}_d(R)$.

Example 2.3. (1) The additive formal group of dimension d is given by $\mathbb{G}_a(X, Y) = X + Y$. The i^{th} coordinate is given by the polynomial $x_i + y_i$.

(2) The one-dimensional multiplicative formal group law is given by

$$\mathbb{G}_m(x, y) = x + y + xy = (x + 1)(y + 1) - 1.$$

This is obtained from usual multiplication by making the change of coordinates $x \mapsto x - 1$ so that zero is the identity.

(3) For $\alpha \in \mathcal{O}_K$, the pair

$$F(X, Y) = \begin{bmatrix} x_1 + y_1 + \alpha x_2 y_2 \\ \\ x_2 + y_2 \end{bmatrix}$$

satisfies the conditions to be a 2-dimensional formal group law over $\mathcal{O}_K$. Checking these conditions is left as an exercise to the reader.

Axioms (FG2) through (FG5) mirror precisely the requirements to be an abelian group, so formal groups are often thought of as being groups "without points." By evaluating $F(X, Y)$ on a set where its coordinate power series converge, we can obtain an abelian group. More precisely, let A be a R-algebra and suppose that N is the ideal of nilpotent elements of A. Then $(N^d, +_F)$ is an abelian group. More generally, if R is complete with respect to a topology and N is the ideal of topologically nilpotent elements of a R-algebra A then $(N^d, +_F)$ is an abelian group.

Example 2.4. Let K be a $\mathfrak{p}$-adic field and $R = \mathcal{O}_K$ its ring of integers. Let $F(X, Y) \in \mathcal{FG}_d(R)$ be a d-dimensional formal group law over R.

(1) Let Ω_K be a fixed algebraic closure of K and let $A = \bar{\Omega}_K$ be its completion with respect to the unique valuation v extending the valuation v_K of K. Its ideal of topologically nilpotent elements is given by $N = \{x \in A : v(x) > 0\}$, which is the maximal ideal of the ring of integers of A. Thus $(N^d, +_F)$ is an abelian group. Later we will take this idea further by using the endomorphism ring of $F(X, Y)$ to put a module structure on N^d.

(2) Let $A = K[[X]] = K[[x_1, \ldots, x_d]]$. Its unique maximal ideal is given by $N = \{f \in A : f(0) = 0\}$, and $(N^d, +_F)$ is an abelian group.

Formal group laws have a notion of homomorphism. Define

$$\mathcal{M}_{m,n}(R) = \{f(X) \in R[[x_1, \ldots, x_n]]^m : f(X) \equiv 0 \pmod{\deg 1}\}.$$

If $m = n = d$, we write $\mathcal{M}_d(R)$. This notation is chosen to mimic the matrix notation

$$M_{m,n}(R) = \{m \times n \text{ matrices with entries in } R\}.$$

Let $F(X, Y)$ and $G(X, Y)$ be formal group laws over R of dimension d_1 and d_2, respectively, and let $f(X) \in \mathcal{M}_{d_2,d_1}(R)$. We say that $f(X)$ is an R-homomorphism from F to G if it satisfies

$$f(X +_F Y) = f(X) +_G f(Y), \quad \text{or} \quad f \circ F = G \circ f.$$

The notions of isomorphism, endomorphism, and automorphism are as usual in any category. It is easy to classify when a map is invertible by looking at the matrix of its degree one coefficients.

Let $f \in \mathcal{M}_{m,n}(R)$ and define the *Jacobian of* f to be the $m \times n$ matrix

$$J(f) := \left[\frac{\partial}{\partial x_j} f_i(\mathbf{0})\right]_{i,j}$$

for $1 \leq i \leq m$ and $1 \leq j \leq n$. Equivalently, the $(i, j)^{th}$ entry $J(f)(i, j) = a_{i,j}$ is the coefficient of x_j in the power series $f_i(X)$, the i^{th} coordinate of $f(X)$.

Lemma 2.2.1. *Let $d \geq 1$ and let $f(X), g(X) \in \mathcal{M}_d(R)$. Then $J(f(g(X))) = J(f)J(g)$ and $f(X)$ is invertible under composition if and only if $J(f)$ is invertible in $M_d(R)$. Therefore if we define*

$$\mathcal{M}_d^\times(R) = \{f(X) \in \mathcal{M}_d(R) : J(f) \in GL_d(R)\}$$

then the Jacobian is a surjective group homomorphism $J : \mathcal{M}_d^\times(R) \to GL_d(R)$.

Proof. Let $f(X), g(X) \in \mathcal{M}_d(R)$. It is a straightforward check to see that $J(f(g(X))) = J(f)J(g)$. Now suppose that $f(X)$ is invertible under composition, so there exists some $f^{-1}(X) \in \mathcal{M}_d(R)$ such that $f(f^{-1}(X)) = X$. Then $J(f)J(f^{-1}) = I_d$, so $J(f)$ and $J(f^{-1})$ are both in $GL_d(R)$.

Conversely, suppose $J(f)$ is invertible in $M_d(R)$. We can construct an inverse for $f(X)$ inductively by degree. Let $g^1(X) = J(f)^{-1}X$ and observe that $f(g^1(X)) \equiv X \pmod{\deg 2}$. Now suppose that for $n \geq 1$ we have constructed some $g^n(X)$ such that $g^n(X) \equiv g^{n-1}(X) \pmod{\deg n}$ and $f(g^n(X)) \equiv X \pmod{\deg n+1}$. We want to solve for $h^{n+1}(X) \in \mathcal{M}_d(R)$ homogeneous of degree $n+1$ such that

$$g^{n+1}(X) := g^n(X) + h^{n+1}(X) \equiv g^n(X) \pmod{\deg n+1}$$

and

$$f(g^{n+1}(X)) = f(g^n(X) + h^{n+1}(X)) \equiv f(g^n(X)) + J(f)h^{n+1}(X) \equiv X \pmod{\deg n+2}.$$

Thus we must have $J(f)h^{n+1}(X) \equiv X - f(g^n(X)) \equiv 0 \pmod{\deg n+1}$, and since $J(f)$ is invertible we can solve for $h^{n+1}(X) \in \mathcal{M}_d(R)$. This proves by induction that $f(X)$ is invertible if and only if $J(f) \in GL_d(R)$.

Finally, we note that for any $M \in GL_d(R)$ that $MX \in \mathcal{M}_d^\times(R)$, so $J : \mathcal{M}_d^\times(R) \to GL_d(R)$ is a surjective group homomorphism. □

We define $\mathcal{L}_d(\mathcal{O}_K) = \ker(J) = \{f(X) \in \mathcal{M}_d^\times(\mathcal{O}_K) : J(f) = I_d\}$. If $F, G \in \mathcal{FG}_d(\mathcal{O}_K)$ and $f : F \to G$ is a homomorphism then we say that f is *strict* if and only if $f \in \mathcal{L}_d(\mathcal{O}_K)$.

Any commutative formal group law F over R has a multiplication-by-n endomorphism for every integer n, and this map is given by repeated addition. More precisely, we define $[0]_F(X) = 0$, $[1]_F(X) = X$, and $[n]_F(X) = [n-1]_F(X) +_F X$ for all $n \geq 2$. We also define $[-n]_F(X) = i_F([n]_F(X))$, and thereby construct an endomorphism for every integer. If the residue field of k is of characteristic p then we can associate a notion called the height to any homomorphism.

Definition 2.5. Let $k = \mathcal{O}_K/\pi\mathcal{O}_K$ be the residue field of K with $\mathrm{char}(k) = p > 0$ and let $F, G \in \mathcal{FG}_d(k)$. Let $f(X) = (f_1(X), \ldots, f_d(X)) \in \mathcal{M}_d(k)$ be a homomorphism from F to G. If $k[[x_1, \ldots, x_d]]$ is finitely generated as a module over its subring $k[[f_1(X), \ldots, f_d(X)]]$ then it has rank p^h for some positive integer h and we say

that the map $f(X)$ has *height h*. If $k[[x_1, \ldots, x_d]]$ is not finitely generated over $k[[f_1(X), \ldots, f_d(X)]]$ we say that $f(X)$ has *infinite height*.

The *height* of a formal group law $F \in \mathcal{FG}_d(k)$ is defined to be the height of its multiplication-by-p endomorphism $[p]_F(X)$. The height of a formal group law $F \in \mathcal{FG}_d(\mathcal{O}_K)$ is defined to be the height of the formal group law $\tilde{F} \in \mathcal{FG}_d(k)$ obtained by reducing the coefficients of F modulo $\mathfrak{p}_K$.

Formal group laws also have a notion of direct sum.

Definition 2.6. Let $F = (F_1, \ldots, F_{d_1})$ and $G = (G_1, \ldots, G_{d_2})$ be formal group laws over K of dimension d_1 and d_2, respectively. We define the *direct sum* of F and G to be the formal group law $F \oplus G$ over K of dimension $d_1 + d_2$ which for $1 \leq i \leq d_1$ has i^{th} coordinate equal to

$$(F \oplus G)_i(X, Y) = F_i(x_1, \ldots, x_{d_1}, y_1, \ldots, y_{d_1})$$

and for $1 \leq j \leq d_2$ has $(d_1 + j)^{th}$ coordinate

$$(F \oplus G)_{d_1+j}(X, Y) = G_j(x_{d_1+1}, \ldots, x_{d_1+d_2}, y_{d_1+1}, \ldots, y_{d_1+d_2}).$$

Example 2.7. Let $\mathbb{G}_m(x, y) = x + y + xy$ and $F = (x_1 + y_1 - 5x_2y_2, x_2 + y_2)$. Then

$$\mathbb{G}_m \oplus F = \begin{bmatrix} x_1 + y_1 + x_1y_1 \\ x_2 + y_2 - 5x_3y_3 \\ x_3 + y_3 \end{bmatrix}.$$

This notion is useful in higher dimensions, as direct products of formal group laws can be described in terms of their direct summands.

2.2.2 The importance of the logarithm

Recall that K is a finite extension of $\mathbb{Q}_p$, so it is in particular a $\mathbb{Q}$-algebra. We are naturally interested in understanding the isomorphism classes of formal group laws of a fixed dimension d over K. As it turns out, the answer is simple: every formal group law $F \in \mathcal{FG}_d(K)$ is isomorphic to the additive formal group law $\mathbb{G}_a(X, Y) = (x_1 + y_1, \ldots, x_d + y_d)$, so there is only one isomorphism class over K.

Theorem 2.2.2. *Let $F(X,Y) \in \mathcal{FG}_d(K)$ and define $\lambda_n(X) = p^{-n}[p^n]_F(X)$. Then $\lim_{n\to\infty} \lambda_n(X)$ converges to $\lambda(X) \in \mathcal{M}_d(K)$ with $J(\lambda) = I_d$ and $\lambda(X +_F Y) = \lambda(X) + \lambda(Y)$, so $\lambda : F \to \mathbb{G}_a$ is an isomorphism.*

Proof. See [6] for details. □

If $\lambda : F \to \mathbb{G}_a$ is an isomorphism, we say that λ is a *logarithm* of F. We say that an isomorphism $\lambda : F \to G$ is *strict* if its Jacobian is the identity matrix, or equivalently, if $\lambda(X) \equiv X \pmod{\deg 2}$. Any commutative formal group law F over a $\mathbb{Q}$-algebra has a unique strict logarithm; we will usually refer to this as "the" logarithm of the formal group law F.

Conversely, if $\lambda(X) \in \mathcal{M}_d^\times(K)$ then we will see that there exists a unique formal group law $F(X,Y)$ over K for which $\lambda(X)$ is a logarithm. Thus elements of $\mathcal{M}_d^\times(K)$ are particularly helpful because they give us a method of constructing formal group laws explicitly.

Lemma 2.2.3. *Let $\lambda(X) \in \mathcal{M}_d^\times(K)$ and let $F(X,Y) = \lambda^{-1}(\lambda(X) + \lambda(Y))$. Then $F(X,Y)$ is a commutative formal group law and f is a K-isomorphism from F to the additive formal group law $\mathbb{G}_a$.*

Proof. Since $\lambda(X) \equiv X \pmod{\deg 2}$ it is clear that $F(X,Y) \equiv X + Y \pmod{\deg 2}$. F is associative since

$$\begin{aligned} F(X,F(Y,Z)) &= \lambda^{-1}(\lambda(X) + \lambda(F(Y,Z)) \\ &= \lambda^{-1}\Big(\lambda(X) + \lambda(\lambda^{-1}(\lambda(Y) + \lambda(Z)))\Big) \\ &= \lambda^{-1}(\lambda(X) + \lambda(Y) + \lambda(Z)) \\ &= F(F(X,Y),Z) \end{aligned}$$

and commutative since $F(X,Y) = \lambda^{-1}(\lambda(X) + \lambda(Y)) = \lambda^{-1}(\lambda(Y) + \lambda(X)) = F(Y,X)$. Therefore F is a formal group law, and λ is an isomorphism to $\mathbb{G}_a$ by definition. □

Let $F(X,Y) \in \mathcal{FG}_d(\mathcal{O}_K)$ and suppose $\lambda(X) \in \mathcal{M}_d(K)$ is a logarithm of F. If $\theta \in M_d(K)$, it is an easy exercise to see that $\theta\lambda(X)$ is also a logarithm of $F(X,Y)$. Since $\lambda(X)$ is an isomorphism then $J(\lambda)$ must be invertible, so $J(\lambda)^{-1}\lambda(X)$ is a strict logarithm of $F(X,Y)$.

Recall that $\mathcal{L}_d(K) = \{f(X) \in \mathcal{M}_d(K) : J(f) = I_d\}$.

Theorem 2.2.4. *Let K be a $\mathfrak{p}$-adic field. Then there exists a bijection*

$$\psi : \mathcal{L}_d(K) \to \mathcal{FG}_d(K)$$

defined by $\lambda \mapsto F_\lambda(X, Y) := \lambda^{-1}(\lambda(X) + \lambda(Y))$.

Proof. By lemma 2.2.3, $\psi(\lambda) = \mathcal{F}_\lambda(X, Y)$ satisfies the conditions to be a formal group law.

All that remains is to establish that ψ is invertible. Define a map $\psi' : \mathcal{FG}_d(K) \to \mathcal{L}_d(K)$ by letting $\psi'(F)$ be the unique noramlized logarithm of F obtained as in lemma 2.2.2. Then if $\lambda = \psi'(F)$, $\psi(\lambda) = \lambda^{-1}(\lambda(X)+\lambda(Y)) = F(X, Y)$ by definition. We conclude that $\psi \circ \psi'$ is the identity map on $\mathcal{FG}_d(K)$. Conversely, if $F = \psi(\lambda) = \lambda^{-1}(\lambda(X)+\lambda(Y))$ then F has a unique strict logarithm, which must by definition be λ. Therefore ψ and ψ' are inverses of each other. □

Example 2.8. Once again we will consider the multiplicative formal group law

$$\mathbb{G}_m(x, y) = (x + 1)(y + 1) - 1 = x + y + xy.$$

Its multiplication-by-p^n endomorphism is given by $[p^n](x) = (x + 1)^{p^n} - 1 = px + \cdots + x^{p^n}$. Arithmetic with binomial coefficients shows that $\lim_{n\to\infty}(1 + x)^{p^n} = 1$, which implies that $\lim_{n\to\infty}(1 + x)^{p^n-1} = (1 + x)^{-1}$. By integrating, we obtain that $p^{-n}[p^n](x)$ converges p-adically to

$$\lambda(x) = x - x^2/2 + x^3/3 - x^4/4 + \cdots = \ln(1 + x).$$

This gives us a clue as to why this map is typically called the logarithm.

Remark: Even if both $F(X, Y)$ and therefore $[p](x)$ are defined over $\mathcal{O}_K$, the logarithm does not necessarily have p-integral coefficients. However, it can be shown that the logarithm could have been obtained by integrating a differential form over $\mathcal{O}_K$. This means that we can obtain restrictions on the denominators, since the derivatives of the logarithm are integral.

Theorem 2.2.5. *Fix two formal group laws $F, G \in \mathcal{FG}_d(K)$. There exists a unique group isomorphism*

$$[-]_{F,G} : (M_d(K), +) \to (\mathrm{Hom}_K(F_1, F_2), +_{F_2})$$

satisfying $J([\theta]_{F,G}) = \theta$, and this map is given by $\theta \mapsto \lambda_G^{-1}(\theta \cdot \lambda_F(X))$. In the case that $F = G$, this is a ring isomorphism.

Proof. Let $[\theta]_{F,G}(X) = \lambda_G^{-1}(X) \circ \theta X \circ \lambda_F(X) = \lambda_G^{-1}(\theta\lambda_F(X))$. Then

$$\begin{aligned}
[\theta]_{F,G}(X) \circ F(X,Y) &= \lambda_G^{-1}(\theta\lambda_F(X)) \circ \lambda_F^{-1}(\lambda_F(X) + \lambda_F(Y)) \\
&= \lambda_G^{-1}(\theta(\lambda_F(X) + \lambda_F(Y))) \\
&= \lambda_G^{-1}\left(\theta\lambda_F(X) + \theta\lambda_F(Y)\right) \\
&= \lambda_G^{-1}(\lambda_G(X) + \lambda_G(Y)) \circ \lambda_G^{-1}(\theta\lambda_F(X)) \\
&= G(X,Y) \circ [\theta]_{F,G}(X)
\end{aligned}$$

so we have obtained a homomorphism from F to G with linear term given by θX. We can see by a similar argument that $\lambda_G(X) \circ [\theta]_{F,G}(X) \circ \lambda_F^{-1}(X)$ must be a homomorphism of $\mathbb{G}_a$, which is necessarily given by a matrix multiplication, so $[-]_{F,G}$ is a bijection.

To see that $[-]_{F,G}$ is a group homomorphism, observe that

$$\begin{aligned}
[\alpha+\beta]_{F,G}(X) \circ F(X,Y) &= (\lambda_G^{-1}(\alpha+\beta)\lambda_F) \circ (\lambda_F^{-1}(\lambda_F(X) + \lambda_F(Y)) \\
&= \lambda_G^{-1}\Big(\alpha(\lambda_F(X) + \lambda_F(Y)) + \beta(\lambda_F(X) + \lambda_F(Y))\Big) \\
&= \lambda_G^{-1}\Big(\lambda_G\left(\lambda_G^{-1}(\alpha(\lambda_F(X) + \lambda_F(Y)))\right) + \lambda_G\left(\lambda_G^{-1}(\beta(\lambda_F(X) + \lambda_F(Y)))\right)\Big) \\
&= [\alpha]_{F,G}(F(X,Y)) +_G [\beta]_{F,G}(F(X,Y))
\end{aligned}$$

Finally, let $F = G$. If $\alpha, \beta \in M_d(R)$ then

$$\begin{aligned}
[\alpha]_F(X) \circ [\beta]_F(X) &= (\lambda_F^{-1}(\alpha\lambda_F(X)) \circ (\lambda_F^{-1}(\beta\lambda_F(X)) \\
&= \lambda_F^{-1}((\alpha \cdot \beta)\lambda_F(X)) \\
&= [\alpha \cdot \beta]_F(X)
\end{aligned}$$

so we conclude that $[-]_F$ is a ring isomorphism. □

This theorem implies that a formal group law F cannot have two distinct endomorphisms with the same Jacobian matrix.

We have now obtained a method of constructing not only all commutative formal group laws, but also all homomorphisms between them. However, many of our applications of formal group laws will

require them to have integral coefficients, and this proves to be a crucial point. Even for formal group laws with integral coefficients, their logarithms will in general have denominators since they are obtained by anti-differentiating a differential form with integral coefficients. This means we will need a method of determining when a formal group law or homomorphism of formal group laws has integral coefficients. We will introduce three related constructions due to Lubin and Tate, to Honda, and to Hazewinkel.

2.2.3 Lubin and Tate, Honda, and Hazewinkel

Recall that K is a $\mathfrak{p}$-adic field with residue field $k = \mathcal{O}_K/\mathfrak{p}_K$, $q = |k|$.

Lubin and Tate worked with one-dimensional formal group laws. Their aim was to study the structure of ramified extensions over $\mathfrak{p}$-adic fields, such as the p-adic rationals $\mathbb{Q}_p$. They accomplished this by showing that the roots of certain Eisenstein polynomials could be given additional structure by recognizing them as the torsion points of formal group laws with complex multiplication.

Theorem 2.2.6. *(Lubin–Tate) Fix a uniformizer $\pi \in \mathcal{O}_K$ and a positive integer h. Let $f(x) \in \mathcal{O}_K[[x]]$ be a (single) power series satisfying*

$$f(x) \equiv \pi x \quad \text{and} \quad f(x) \equiv x^{q^h} \pmod{\pi}.$$

Then there exists a one-dimensional formal group law F such that $[\pi]_F(x) = f(x)$ and F has its coefficients in $\mathcal{O}_K$. Additionally, if $L = K^h_{ur}$ then F has complex multiplication by the ring of integers of L, meaning that there exists a ring injection $[-]_F : \mathcal{O}_L \hookrightarrow \mathrm{End}_{\mathcal{O}_L}(F)$.

Lubin and Tate proved this directly by constructing the formal group law F one degree at a time. They constructed a sequence of compatible polynomials $(F_n(x, y))$ where each F_n is of degree n, $F_n(x, y) \equiv F_{n-1}(x, y) \pmod{\deg n}$, such that $F_n(x, y) \circ f = f \circ F_n(x, y) \pmod{\deg n + 1}$. They were able to show that this could always be done by taking coefficients in $\mathcal{O}_K$, although we will see that in higher dimensions their method fails.

Throughout the rest of the section we will let L be an unramified extension of K, $\mathcal{O}_L$ its ring of integers, and $\mathfrak{p}_L$ its maximal ideal. If we take $\varphi = \varphi_K|_L$ to be the restriction of the Frobenius to L then we note that $\varphi(x) \equiv x^q \pmod{\mathfrak{p}_L}$.

Honda developed a method for constructing formal group laws of dimension $d \geq 1$ with coefficients in $\mathcal{O}_L$. Let I_d denote the $d \times d$ identity matrix.

Theorem 2.2.7. *(Honda) Let $L\{\{\tau\}\}$ be the ring of non-commutative formal power series with multiplication rule $\tau a = \varphi(a)\tau$ for $a \in L$. Let $u \in M_d(L\{\{\tau\}\})$ be a $d \times d$ matrix such that $u \equiv \pi I_d \pmod{\tau}$ and write*

$$u^{-1}\pi = I_d + \sum_{i=1}^{\infty} a_i \tau^i$$

where $a_i \in M_d(L)$ is a $d \times d$ matrix for $i \geq 1$. If $X^{q^n} = \left(x_1^{q^n}, \ldots, x_d^{q^n}\right)$ then

$$\lambda(X) = X + a_1 X^q + a_2 X^{q^2} + \ldots$$

is the logarithm of a unique formal group law $F_\lambda(X, Y) = \lambda^{-1}(\lambda(X) + \lambda(Y))$ and $F_\lambda(X, Y)$ has its coefficients in $\mathcal{O}_L$.

The results of Lubin and Tate, as well as that of Honda, were subsumed into a general result by Hazewinkel. We will eventually rephrase this in the language of Honda, which will allow us to use matrix methods, but for now we will pay homage to the author and state the following lemma as it was originally written.

Lemma 2.2.8. *(Hazewinkel's functional equation lemma) Let $A \subset L$ be a subring of a ring L, $\sigma : L \to L$ an endomorphism of L, I an ideal of A, p a prime number, and q a power of p. Let $s_1, s_2, \ldots$ be d by d matrices with coefficients in L. Further suppose $\sigma(a) \equiv a^q \pmod{I}$ for all $a \in A$ and suppose $s_k I \subseteq M_d(A)$ for all $k \geq 1$.*

Now let $g(X) \in \mathcal{M}_d(A)$. We construct a new d-tuple of power series by means of the recursion formula

$$f_g(X) = g(X) + \sum_{i=1}^{\infty} s_i \sigma_*^i f_g(X^{q^i})$$

where $\sigma_*^i f_g(X)$ is obtained from $f_g(X)$ by applying the endomorphism σ^i to the coefficients of $f_g(X)$ and where $X^{q^i} = \left(x_1^{q^i}, \ldots, x_d^{q^i}\right)$. We say that $f_g(X)$ satisfies a functional equation of type $(s_1, s_2, \ldots)$.

Let $g(X), g'(X) \in \mathcal{M}_d(A)$ and obtain $f_g(X)$ and $f_{g'}(X)$ from these power series and a functional equation as above. Suppose the Jacobian matrix $J(f_g)$ is invertible. Then $f_g(X)$ is invertible under composition, and we have

(1) the d-tuple of power series $F(X,Y) = f_g^{-1}(f_g(X) + f_g(Y))$ *has coefficients in* A*;*

(2) $f_g^{-1}(f_{g'}(X))$ *has its coefficients in* A*;*

(3) if $h(X) \in \mathcal{M}_d(A)$ *then* $f_g(h(X))$ *satisfies a functional equation of type* $(s_1, s_2, \dots)$*;*

(4) if $\alpha(X) \in A[[X]]^d$ *and* $\beta(X) \in L[[X]]^d$ *then for all* $r \geq 1$ *we have*

$$\alpha(X) \equiv \beta(X) \pmod{I^r} \iff f_g(\alpha(X)) \equiv f_g(\beta(X)) \pmod{I^r}.$$

In our case we will always take L to be a finite unramified extension of K, A to be its ring of integers $\mathcal{O}_L$, $I = \mathfrak{p}_K$, and σ to be the restriction of the Frobenius φ_K to L.

We can restate this lemma by using matrices with elements in a non-commutative power series ring, in language that is very similar to that used by Honda. Again let $\mathcal{O}_{\bar{K}}\{\{\tau\}\}$ be the ring of non-commutative power series in the variable τ with multiplication rule $\tau^i a = \varphi^i(a)\tau^i$ for $i \geq 1$ and $a \in \mathcal{O}_{\bar{K}}$. Define an action of τ on $\bar{K}[[X]]$ by $\tau^i f(X) = \varphi^i_* f(X^{q^i})$. It is a straightforward exercise to verify that this extends to an action of $M_d(\mathcal{O}_{\bar{K}}\{\{\tau\}\})$ on $\mathcal{M}_d(\bar{K})$ where, if $s_i \in M_d(\bar{K})$ for $i \geq 0$ and $f(X) \in \mathcal{M}_d(\bar{K})$, the action is given by

$$\left(\sum_{i=0}^{\infty} s_i \tau^i\right) \cdot f(X) = \sum_{i=0}^{\infty} s_i \sigma^i_* f(X^{q^i}).$$

We define the set of *functional equation matrices over* $\mathcal{O}_{\bar{K}}$ by

$$\mathcal{S}_d(\mathcal{O}_{\bar{K}}) = \{S \in M_d(\mathcal{O}_{\bar{K}}\{\{\tau\}\}) : S \equiv 0 \pmod{\tau}\}.$$

We can now restate Hazewinkel's functional equation lemma.

Lemma 2.2.9. *Let* L *be an unramified extension over* K *and let* $S \in \mathcal{S}_d(\mathcal{O}_L)$*, let* $D \in M_d(\mathcal{O}_L)$ *be a diagonal matrix whose non-zero entries are all uniformizers in* $\mathcal{O}_L$*, and let* $g(X) \in \mathcal{M}_d(\mathcal{O}_L)$*. Suppose* $\lambda(X) = \lambda_g(X) \in \mathcal{M}_d(L)$ *satisfies*

$$\lambda(X) - D^{-1}S \cdot \lambda(X) = g(X) \equiv 0 \pmod{\mathcal{O}_L}.$$

We say that $\lambda(X)$ *satisfies a functional equation of type* (D, S) *and is generated by* $g(X)$*. If* $g(X) \in \mathcal{M}_d^{\times}(\mathcal{O}_L)$ *then* $\lambda(X) \in \mathcal{M}_d^{\times}(L)$*, so* $\lambda(X)$ *is invertible under composition. Then*

(1) if $F_\lambda(X,Y) := \lambda^{-1}(\lambda(X)+\lambda(Y))$ *then* $F_\lambda(X,Y)$ *has coefficients in* $\mathcal{O}_L$*;*

(2) if $\mu(X) \in \mathcal{M}_d^\times(L)$ *also satisfies a functional equation of type* (D,S) *then* $\mu^{-1}(\lambda(X))$ *has coefficients in* $\mathcal{O}_L$ *and* $\mu^{-1}(\lambda(X))$ *is an* $\mathcal{O}_L$*-isomorphism from* F_λ *to* F_μ*;*

(3) if $h(X) \in \mathcal{M}_d(\mathcal{O}_L)$ *then there exists some* $\lambda_h(X) \in \mathcal{M}_d(L)$ *also satisfying a functional equation of type* (D,S) *such that* $\lambda(h(X)) = \lambda_h(X)$*;*

(4) if $f(X) \in \mathcal{M}_d(\mathcal{O}_L)$*,* $g(X) \in \mathcal{M}_d(L)$ *then*

$$\lambda(f) - \lambda(g) \in \mathcal{M}_d(\pi^n \mathcal{O}_L) \iff f - g \in \mathcal{M}_d(\pi^n \mathcal{O}_L).$$

If a formal group law F has a logarithm satisfying a functional equation, we will say that F is a *functional equation formal group law.*

This lemma has several important consequences. Firstly, it gives us a method for constructing formal group laws and homomorphisms with integral coefficients. Parts (2) tells us that two functional equation formal group laws $F, G \in \mathcal{FG}_d(\mathcal{O}_K)$ are isomorphic over $\mathcal{O}_K$ if they satisfy the same type of functional equation. Conversely, part (3) tells us that if λ_F is a logarithm of F satisfying a functional equation of type (D,S) and if we have an $\mathcal{O}_L$-isomorphism $h : F \to G$ then $\lambda_G(X) = h \circ \lambda_F$ is a logarithm of G and also satisfies a functional equation of type (D,S). Finally, part (4) will allow us to make conclusions about the form of $[D]_F(X)$ modulo π.

Hazewinkel's generalization of Lubin-Tate formal group laws to higher dimensions was as follows. Suppose $F \in \mathcal{FG}_d(\mathcal{O}_K)$ and $F(X,Y) = \lambda^{-1}(\lambda(X)+\lambda(Y))$, so that $\lambda(X)$ is the unique normalized logarithm of $F(X,Y)$. Then F is a *generalized Lubin-Tate formal group law* if there exist $S \in \pi^{-1}M_d(\mathcal{O}_K)$ and $g(X) \in \mathcal{M}_d(\mathcal{O}_K)$ such that $\lambda(X)$ satisfies the functional equation

$$\lambda(X) - (S\tau)\lambda(X) = g(X).$$

Our construction will include this definition but will also allow non-linear power series in τ, so it is more general.

Hazewinkel also had a notion of a d-dimensional *formal A-module*, which is a d-dimensional formal group law F over an A-algebra B that is equipped with a homomorphism $\rho : A \to \mathrm{End}_B(F)$ satisfying

$J(\rho(a)) = aI_d$ for all $a \in A$, where J is the Jacobian map and I_d is the $d \times d$ identity matrix. Our construction will allow for a more general choice of ρ.

Chapter 3

Construction of formal groups with complex multiplication

Lubin and Tate showed that if $\pi \in \mathcal{O}_K$ is a uniformizer, $q = |\mathcal{O}_K/\pi\mathcal{O}_K|$ is the order of the residue field of K, and h is a positive integer, then any power series $f(x) \in \mathcal{O}_K[[x]]$ satisfying

$$f(x) \equiv \pi x \pmod{\deg 2} \quad \text{and} \quad f(x) \equiv x^{q^h} \pmod{\pi}$$

is an endomorphism of a unique one-dimensional formal group law $F(X, Y)$ with coefficients in $\mathcal{O}_K$. They also showed that this formal group law F has complex multiplication by $\mathcal{O}_L$ where $L = K_{ur}^h$ is the unramified extension of K of degree h. If $q = p^r$ then rh is the height of $f(x)$.

In the higher-dimensional case, we will consider more options both for the linear term of $f(X)$ and for the form of $f(X)$ modulo π. Let $D \in M_d(\mathcal{O}_{\bar{K}})$ be a diagonal $d \times d$ matrix whose non-zero entries are all uniformizers in $\mathcal{O}_{\bar{K}}$. We will say that D is a *diagonal uniformizer matrix*. Suppose that $h_1, \ldots, h_d$ are positive integers and $j_1, \ldots, j_d \in \{1, \ldots, d\}$ are indices, and let $\Phi(X) = \left(x_{j_i}^{q^{h_i}}\right)_{i=1}^{d}$. We will say that $\Phi(X)$ is a *q-power tuple*.

Our generalization of Lubin and Tate's result will concern $f(X) \in \mathcal{M}_d(\mathcal{O}_{\bar{K}})$ satisfying

$$f(X) \equiv DX \pmod{\deg 2} \quad \text{and} \quad f(X) \equiv \Phi(X) \pmod{\pi}. \tag{3.1}$$

We will see in 3.1.1 that there exists a unique formal group law $F_f(X, Y) \in \mathcal{FG}_d(K)$ for which $f(X)$ is an endomorphism. While it is no longer true in multiple dimensions that *every* $f(X)$ satisfying (3.1) gives rise to $F_f \in \mathcal{FG}_d(\mathcal{O}_K)$, we will see that there do exist *some* $f(X)$ satisfying (3.1) for which F_f has coefficients in $\mathcal{O}_K$. This F_f will once again have complex multiplication by an algebra A over $\mathcal{O}_K$, but the form of A will be determined not only by the individual integers h_i but also how they interact as $\Phi(X)$ composes with itself.

3.1 Comparing the one-dimensional and higher-dimensional cases

Let $D \in M_d(K)$ be a diagonal uniformizer matrix. One similarity between the one-dimensional and higher-dimensional theories is that if $f(X) \equiv DX \pmod{\deg 2}$ then there exists a unique formal group law $F_f(X,Y) \in \mathcal{FG}_d(K)$ such that f is an endomorphism of F_f. We generalize a result of Wiles [17] to higher dimensions, which will allow us to construct a logarithm λ_f, and hence a formal group law F_f, such that f is an endomorphism of F_f.

Proposition 3.1.1. *Suppose $f \in \mathcal{M}_d(\mathcal{O}_K)$ such that $J(f) \in \pi GL_d(\mathcal{O}_K)$. Define a valuation v on $\mathcal{O}_K[[X]]$ corresponding to the ideal $m = (\pi, X) = (\pi, x_1, \ldots, x_d)$, which is maximal in $\mathcal{O}_K[[X]]$, and extend this valuation in the natural way to $K[[X]]$. Then the sequence $\lambda_n = J^{-n} f^n(X)$ converges to some $\lambda(X) \in \mathcal{L}_d(K)$ as $n \to \infty$. In addition, the formal group law $F_\lambda(X,Y) := \lambda^{-1}(\lambda(X) + \lambda(Y))$ has coefficients in K and satisfies $[J(f)]_F(X) = f(X)$.*

Proof. Notice that for any monomial $H = aX^I \in K[[X]]$, the valuation of H is given by $v(H) = v_\pi(a) + |I|$, the sum of the degree of H and the π-adic valuation of the coefficient a. To see that the limit exists, we first note that $v(f(X)) \geq 2$ and observe by induction that $v(f^n(X)) \geq n+1$ for all n. Define $\lambda_n(X) = J^{-n} f^n(X)$. Then we define $g_{m,n}(X) = \lambda_m(X) - \lambda_n(X)$ and compute that

$$\begin{aligned} g_{m,n}(X) &= \lambda_m(X) - \lambda_n(X) \\ &= J^{-m}(f^m(X) - J^{m-n} f^n(X)) \\ &= J^{-m}(f^{m-n}(X) - J^{m-n}X) \circ f^n(X) \end{aligned}$$

Since $J^{m-n}X$ is the linear term of $f^{m-n}(X)$ then $f^{m-n}(X) - J^{m-n}(X) \equiv 0 \pmod{\deg 2}$, so its lowest degree term is of degree two. Let $I = (i_1, \ldots, i_d)$ and let $a_I \in K^d$ be a d-tuple of coefficients such that $H(X) = a_I X^I$ is a homogeneous d-tuple of monomials of $f^{m-n}(X)$. Since $v(f^{m-n}) \geq m-n+1$, then $v_\pi(a_I) + |I| \geq m-n+1$ and since $v(f^n) \geq n+1$ then $v(H \circ f^n) \geq |I|(n+1) + (m-n+1-|I|)$. Thus we conclude that

$$v(g_{m,n}) \geq -m + 2(n+1) + ((m-n+1) - 2) = n+1.$$

Therefore $(\lambda_n(X))_{n=1}^\infty$ is a Cauchy sequence and so $\lambda(X) = \lim_{n\to\infty} \lambda_n(X)$ exists. Since $J(\lambda_n(X)) = I_d$ for all n, then $\lambda(X) \in \mathcal{L}_d(K)$. In particular, $\lambda(X)$ is invertible under composition.

Now notice that

$$\lambda_n(X) \circ f(X) = J^{-n} f^n(f(X)) = J^{-n} f^{n+1}(X) = J \cdot \left(J^{-(n+1)} f^{n+1}(X)\right) = J \cdot \lambda_{n+1}(X),$$

so by taking the limit as n goes to infinity we see that

$$\lambda(X) \circ f(X) = J \cdot \lambda(X).$$

This shows that if $F(X, Y) = \lambda^{-1}(\lambda(X) + \lambda(Y))$, then $[J]_F(X) = \lambda^{-1}(J \cdot \lambda(X)) = f(X)$. □

In particular, if $f(X) \in \mathcal{M}_d(K)$ such that $J(f) = DX$ then $f(X)$ is the "multiplication-by-D" endomorphism for some unique formal group law $F \in \mathcal{FG}_d(K)$. We would like to know which of these formal group laws have their coefficients in the ring of integers $\mathcal{O}_K$.

When Lubin and Tate showed that $f(x) = \pi x + x^{q^h}$ is the multiplication-by-π endomorphism for some one-dimensional formal group law $F(x, y)$ with coefficients in $\mathcal{O}_K$, they did it directly by constructing $F(x, y)$ one homogeneous piece at a time. This approach fails in higher dimensions.

Lubin and Tate constructed a sequence $(F_n(x, y))_{n=1}^{\infty}$ of polynomials $F_n(x, y)$ of degree n over $\mathcal{O}_K$ such that $F_1(x, y) = x + y$ and for all $n \geq 2$

$$F_n(x, y) \equiv F_{n-1}(x, y) \pmod{\deg n} \qquad \text{and}$$

$$F_n(f(x), f(y)) = f(F_n(x, y)) \pmod{\deg n + 1}.$$

They were able to show that if $F(x, y) = \lim_{n \to \infty} F_n(x, y)$ then $F(x, y)$ is a formal group law over $\mathcal{O}_K$ and $f(x)$ is an endomorphism of $F(x, y)$. While constructing $F_{n+1}(x, y)$ from $F_n(x, y)$, we end up needing to solve equations of the form

$$(F_n(x, y) + H_{n+1}(x, y)) \circ (f(x), f(y)) \equiv f(x) \circ (F_n(x, y) + H_{n+1}(x, y)) \pmod{\deg n + 2}$$

where $H_{n+1}(x, y)$ is homogeneous in $\mathcal{O}_K[[x, y]]$ of degree $n + 1$. This is equivalent to solving the equation

$$\left(\pi + \pi^{n+1}\right) H_{n+1}(x, y) \equiv F_n(f(x), f(y)) - f(F_n(x, y)) \pmod{\deg n + 2}. \tag{3.2}$$

Since we know by assumption that the right-hand side of this equation is congruent to zero modulo degree $n + 1$, it is clear that we can only solve for $H_{n+1}(x, y)$ with coefficients in $\mathcal{O}_K$ if the right hand side is

divisible by π. We know that $f(x) \equiv x^{q^h} \pmod{\pi}$, so in dimension one this is equivalent to requiring that $F_n\left(x^{q^h}, y^{q^h}\right) \equiv (F_n(x,y))^{q^h} \pmod{\pi}$, which is always true over $\mathcal{O}_K$ by the so-called "freshman's dream." In higher dimensions, however, this forces a non-trivial relationship between the coordinates of the d-tuple $F_n(X,Y)$. We can now only solve for $H_{n+1}(X,Y)$ with coefficients in $\mathcal{O}_K$ if, for $1 \leq i \leq d$,

$$F_{j_i}\left(X^{q^{h_i}}, Y^{q^{h_i}}\right) \equiv F_i(\Phi(X), \Phi(Y)) \pmod{\pi}.$$

Therefore, although the parallel construction in higher dimensions results in an equation similar to (3.2), it may be impossible to solve for $H_{n+1}(X,Y)$ while staying within the ring of integers $\mathcal{O}_K$. Indeed we have worked out an example in which this is the case, although the details of this computation are not included here. In order to construct formal group laws with coefficients in $\mathcal{O}_K$, we will need to take an alternate approach.

Another difference between the one-dimensional and higher-dimensional theories is in how $\Phi(X)$ affects the "complex multiplication type" of F. Let $\Phi(X) = \left(x_{j_i}^{q^{h_i}}\right)_{i=1}^{d}$ be a q-power tuple. We will soon construct a formal group law F which satisfies $[\pi]_F(X) \equiv \Phi(X) \pmod{\pi}$. Both the integers h_i and the relationships between the indices j_i will affect the endomorphism ring of F. We introduce some tools that are helpful for studying these relationships.

Definition 3.1. Let $\Phi(X) = (\Phi_i(X)) \in \mathcal{M}_d(\mathcal{O}_K)$ be a q-power tuple, so for all i we have $\Phi_i(X) = x_{j_i}^{q^{h_i}}$ for some $j_i \in \{1, \ldots, d\}$ and positive integer h_i. We define the following objects associated to $\Phi(X)$.

(1) The *index map* $\sigma_\Phi : \{1, \ldots, d\} \to \{1, \ldots, d\}$ is defined by $\sigma_\Phi(i) = j_i$ whenever $\Phi_i(X) = x_{j_i}^{q^{h_i}}$.

(2) The graph Γ_Φ associated to $\Phi(X)$ is a directed edge-labeled graph permitting loops and is constructed on the nodes $\{1, \ldots, d\}$ by letting there be an arrow from i to j_i. We label this arrow with τ^{h_i}. We will use properties of Γ_Φ to describe $\Phi(X)$; for example, if Γ_Φ is connected we will also say that $\Phi(X)$ is connected.

(3) We define S_Φ to be the adjacency matrix of the directed graph of Φ, or equivalently, the matrix whose $(i, \sigma_\Phi(i))$ entry is given by

$$S_\Phi(i, \sigma(i)) = \tau^{h_i}$$

for $1 \leq i \leq d$ and $S_\Phi(i,j) = 0$ if $j \neq \sigma_\Phi(i)$. Recall that for all $f(X) \in \mathcal{O}_{\bar{K}}[[X]]^d$ we define $\tau^n \cdot f(X) := \varphi_*^n f\left(X^{q^n}\right)$. Then the matrix S_Φ is constructed so as to satisfy

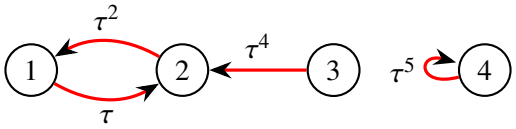
$$S_\Phi \cdot f(X) \equiv \Phi \circ f(X) \pmod{\pi}$$

for all $f(X) \in \mathcal{M}_d(\mathcal{O}_{\bar{K}})$ since the i^{th} coordinate is given by

$$(S_\Phi f)_i(X) = \tau^{h_i} f_{j_i}(X) = \varphi_*^{h_i} f\left(X^{q^{h_i}}\right) \equiv (f_{j_i}(X))^{q^{h_i}} = (\Phi \circ f)_i(X) \pmod{\pi}.$$

In particular, $S_\Phi \cdot X = \Phi(X)$.

Example 3.2. Let $\Phi(X) = \left(x_2^q, x_1^{q^2}, x_2^{q^4}, x_4^{q^5}\right)$. Then the index map $\sigma = \sigma_\Phi$ is defined by $\sigma(1) = \sigma(3) = 2$, $\sigma(2) = 1$, and $\sigma(4) = 4$. The associated graph Γ_Φ is



The corresponding adjacency matrix is

$$S_\Phi = \begin{bmatrix} 0 & \tau & 0 & 0 \\ \tau^2 & 0 & 0 & 0 \\ 0 & \tau^4 & 0 & 0 \\ 0 & 0 & 0 & \tau^5 \end{bmatrix}$$

and we observe that, as desired,

$$S_\Phi X = \begin{bmatrix} 0 & \tau & 0 & 0 \\ \tau^2 & 0 & 0 & 0 \\ 0 & \tau^4 & 0 & 0 \\ 0 & 0 & 0 & \tau^5 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} \tau x_2 \\ \tau^2 x_1 \\ \tau^4 x_2 \\ \tau^5 x_4 \end{bmatrix} = \begin{bmatrix} x_2^q \\ x_1^{q^2} \\ x_2^{q^4} \\ x_4^{q^5} \end{bmatrix} = \Phi(X).$$

Lemma 3.1.2. *Let Γ be a directed graph obtained as above. Then each connected component of Γ contains exactly one directed cycle.*

Proof. Let $\sigma = \sigma_\Phi$. Consider a node i and let $\sigma^{\mathbb{N}}(i) = \{i, \sigma(i), \sigma^2(i), \dots\} \subseteq \{1, \dots, d\}$ be its forward orbit under the index map σ. By the pigeonhole principle there must be some $n > 1$ and $0 \leq m < n$ such that $\sigma^n(i) = \sigma^m(i)$. Let n and m be minimal subject to this condition and let $b = n - m$. Then $\sigma^a(i) = \sigma^{a+b}(i)$ for all $a \geq m$, so we have detected a cycle in Γ which is unique by the minimality of m and n. Since the node i was arbitrary, the forward orbit of each node i contains a unique cycle. Let $1 \leq i, j \leq d$. If the forward orbits of nodes i and j contain the same cycle, then i and j are in the same connected component. If not, their forward orbits are disjoint. Their reverse orbits must also be disjoint, since otherwise there would be a node k such that the forward orbit of k contained two distinct cycles. This proves the claim. □

Suppose that Γ_Φ is not connected and let D be a diagonal uniformizer matrix over $\mathcal{O}_{\bar{K}}$. We will see in the next section that, for $F(X, Y) \in \mathcal{FG}_d(\mathcal{O}_K)$ arising from our upcoming construction, $F(X, Y)$ satisfies $[D]_F(X) \equiv \Phi(X) \pmod{\pi}$ if and only if F decomposes as a direct sum of formal group laws, each corresponding to a connected component of $\Phi(X)$. We can therefore restrict our attention to those q-power tuples $\Phi(X)$ which are connected.

Definition 3.3. Let Γ be the directed graph of a connected q-power tuple Φ and denote its unique cycle by γ. Define $h_\Phi = \sum_{i \in \gamma} h_i$. We say that h_Φ is the *cycle height* of Φ. Let $L = K_{ur}^{h_\Phi}$ be the unramified extension of degree h_Φ over K. We will say that L is the *complex multiplication field* (or *CM field*) of Φ over K.

Again let $\Phi(X)$ be a q-power tuple and let D be a diagonal uniformizer matrix and suppose that we have some $F(X, Y) \in \mathcal{FG}_d(\mathcal{O}_K)$ satisfying $[D]_F(X) \equiv \Phi(X) \pmod{\pi}$. We will see in the next section that if a formal group law G can be obtained from another formal group law F by relabeling the indices $\{1, \dots, d\}$ by some permutation $s \in S_d$ and rearranging the coordinate functions accordingly, then F and G are isomorphic over any ring. This means that we can relabel the indices of $\Phi(X)$ to put it into a more convenient form.

Definition 3.4. Let $\Phi(X) \in \mathcal{M}_d(\mathcal{O}_K)$ be a connected q-power tuple and let γ be its unique cycle with order $|\gamma|$. We will say that $\Phi(X)$ is in *standard form* if the index map of Φ satisfies $\sigma_\Phi(i) = i + 1$ for $1 \leq i < |\gamma|$ and $\sigma_\Phi(|\gamma|) = 1$. Notice that this form is in general not unique, although if $\Phi(X)$ consists of a single directed cycle then its standard form will depend only on a choice of base point.

For the remainder of the chapter $\Phi(X) \in \mathcal{M}_d(\mathcal{O}_K)$ will be assumed to be a connected q-power tuple that is in a choice of standard form. Although it is not required, assuming that $\Phi(X)$ is in standard form will help us state the next two definitions.

Definition 3.5. Let $\Phi(X) \in \mathcal{M}_d(\mathbb{Z})$ be a connected q-power tuple in standard form and let Γ be its directed graph with unique cycle γ. Let $|\gamma|$ be the order of γ, and let L be the CM field of Φ, so $L = K_{ur}^h$ where $h = h_\Phi$ is the cycle height of Φ. Define $\eta_1 = 0$ and $\eta_r = \sum_{j=1}^{r-1} h_j$ for $2 \leq r \leq |\gamma|$.

(1) The *embedding type* of Φ is the ring homomorphism $\iota_\Phi : L \to M_d(L)$ given by $\iota_\Phi(a) = \operatorname{diag}(a, \varphi^{e_2}(a), \ldots, \varphi^{e_d}(a))$ where $e_1 = 0$ and the other e_i are determined by the equations $e_i = e_{\sigma(i)} + h_i$ for $1 \leq i \leq d$. If $\Phi(X)$ is a single directed cycle, the embedding type is given by

$$\iota_\Phi = \operatorname{diag}\left(1, \varphi^{-\eta_2}, \ldots, \varphi^{-\eta_d}\right)$$

where '1' is the identity on L. Since this map is an embedding of $L = K_{ur}^{h_\Phi}$, then powers of the Frobenius φ are considered modulo h_Φ.

(2) We define the *type norm* $N_\Phi : \bar{K} \to \bar{K}$ by

$$N_\Phi(a) = \prod_{r=1}^{|\gamma|} \varphi^{\eta_r}(a) \qquad \text{for all } a \in \bar{K}.$$

If $h_i = 1$ for all i then this coincides with the usual definition of the norm $N_{L/K}$ from $L = K_{ur}^h$ down to K. The type norm is analogous to the "reflex norm" in the theory of complex multiplication of abelian varieties, where the complex multiplication type of the variety in question is given by $(\varphi^{e_1}, \ldots, \varphi^{e_d})$.

Since these definitions depend on a choice of standard form of Φ, it is natural to wonder how different choices of standard form affect the embedding type and type norm of Φ. It is sufficient to consider the case in which the unique cycle γ of Φ is rotated forward by one node, by which we mean $i \mapsto \sigma_\Phi(i)$ for all $i \in \gamma$. The "tails" of Φ do not affect the computation of the type norm, so we do not need to specify how they change under this isomorphism of directed graphs.

Lemma 3.1.3. *Let $\Phi(X)$ be a connected q-power tuple and let $\Phi'(X)$ be obtained from $\Phi(X)$ by the relabeling $i \mapsto \sigma_\Phi(i)$ for all indices i in the unique cycle γ of Φ. Let $n = |\gamma|$ and let $h = h_\Phi = h_{\Phi'}$ be the cycle height of*

Φ, *which is equal to the cycle height of* Φ'. *Then, for all* $a \in \bar{K}^\times$,

$$N_{\Phi'}(a) \cdot \varphi^h(a)/a = N_\Phi(\varphi^{h_n}(a)) = \varphi^{h_n}(N_\Phi(a)).$$

In particular, if $a \in L^\times = \left(K_{ur}^h\right)^\times$ *then*

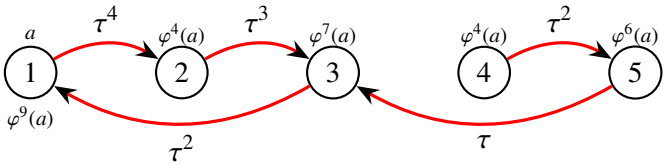
$$N_{\Phi'}(a) = N_\Phi(\varphi^{h_n}(a)) = \varphi^{h_n}(N_\Phi(a)).$$

Proof. Let $a \in \mathcal{O}_{\bar{K}}$. Then

$$\begin{aligned}
\varphi^{h_n}(N_\Phi(a)) &= \varphi^{h_n}\left(\prod_{r=0}^{n-1} \varphi^{\eta_r}(a)\right) \\
&= \varphi^{h_n}(a)\varphi^{h_n+h_1}(a)\ldots\varphi^{h_n+h_1+\cdots+h_{n-1}}(a) \\
&= a\varphi^{h_n}(a)\varphi^{h_n+h_1}(a)\ldots\varphi^{h_n+h_1+\cdots+h_{n-2}}(a)\cdot(\varphi^h(a)/a) \\
&= N_{\Phi'}(a)\cdot(\varphi^h(a)/a).
\end{aligned}$$

□

Example 3.6. Suppose $d = 5$ and $\Phi(X) = \left(x_2^{q^4}, x_3^{q^3}, x_1^{q^2}, x_5^{q^2}, x_3^q\right)$, which is a connected q-power tuple in standard form. By examination we can see that the unique cycle γ of Φ is given by $\gamma = (1, 2, 3)$. Since $h_1 + h_2 + h_3 = 4 + 3 + 2 = 9$, then the CM field of Φ is given by $L = K_{ur}^9$. Automorphisms of L over K are given by powers of the Frobenius considered modulo 9. We can use the graph Γ_Φ to help us compute the type norm of $\Phi(X)$ by looking at an orbit of an element $a \in \mathcal{O}_{\bar{K}}$.



The type norm is given by

$$N_\Phi(a) = a\varphi^4(a)\varphi^7(a)$$

for all $a \in L$. Now let us compute the embedding type ι_Φ. We can again use the graph, but this time we will consider the powers of φ to be negative. Then by definition, if $a \in L$ then

$$\iota_\Phi(a) = \mathrm{diag}\left(a, \varphi^{-4}(a), \varphi^{-7}(a), \varphi^{-4}(a), \varphi^{-6}(a)\right).$$

3.2 Using Hazewinkel's functional equation lemma

Let K' be any finite unramified extension of K and let $\Phi(X)$ be a mixed q-power tuple. The matrix S_Φ can be used to construct logarithms of formal group laws defined over $\mathcal{O}_{K'}$ by using Hazewinkel's functional equation lemma. Recall that in section 2.2.3 we defined $\mathcal{O}_{\bar{K}}\{\{\tau\}\}$ to be the ring of non-commutative power series in τ with multiplication rule $\tau^n a = \varphi^n(a)\tau^n$ for all $a \in \mathcal{O}_{\bar{K}}$, and we defined the set of $d \times d$ *functional equation matrices* over $\mathcal{O}_{\bar{K}}$ to be

$$\mathcal{S}_d(\mathcal{O}_{\bar{K}}) = \{S \in M_d(\mathcal{O}_{\bar{K}}\{\{\tau\}\}) : S \equiv 0 \pmod{\tau}\}.$$

By fixing some $S \in \mathcal{S}_d(\mathcal{O}_{K'})$, a diagonal uniformizer matrix $D \in M_d(\mathcal{O}_{K'})$, and $g(X) \in \mathcal{M}_d(\mathcal{O}_{K'})$, we can define $\lambda(X) \in \mathcal{M}_d(K')$ by the recursion formula

$$\lambda(X) - D^{-1}S \cdot \lambda(X) = (I_d - D^{-1}S) \cdot \lambda(X) = g(X).$$

We can multiply on both sides to solve for $\lambda(X)$ explicitly:

$$\lambda(X) = \left(I_d + D^{-1}S + (D^{-1}S)^2 + \dots\right) \cdot g(X) = \sum_{n=0}^{\infty} (D^{-1}S)^n \cdot g(X).$$

It is clear that $S_\Phi \in \mathcal{S}_d(\mathcal{O}_{K'})$ for any q-power tuple $\Phi(X)$, so we need only to fix a choice of diagonal uniformizer matrix $D \in M_d(\mathcal{O}_{K'})$ and $g(X) \in \mathcal{M}_d(\mathcal{O}_{K'})$ to use the recursion formula to construct $\lambda(X) \in \mathcal{M}_d(K')$.

If the Jacobian $J(g)$ is invertible in $M_d(K')$, then $\lambda(X)$ is invertible under composition. Thus $\lambda(X)$ is the logarithm of a formal group law $F_\lambda(X, Y) = \lambda^{-1}(\lambda(X), \lambda(Y))$ and by Hazewinkel's functional equation lemma 2.2.9 we can deduce that $F_\lambda(X, Y)$ has coefficients in $\mathcal{O}_{K'}$. We can also use the functional equation lemma to construct $\mathcal{O}_{\bar{K}}$-homomorphisms from F_λ to itself and to other formal group laws. The following lemma establishes a sufficient condition for two formal group laws coming from functional equations to be homomorphic over $\mathcal{O}_{\bar{K}}$.

Lemma 3.2.1. *Let $D_1, D_2 \in M_d(\mathcal{O}_{\bar{K}})$ be two diagonal uniformizer matrices and let $S_1, S_2 \in \mathcal{S}_d(\mathcal{O}_K)$ be functional equation matrices. Suppose that $\lambda, \mu \in \mathcal{M}_d^\times(K)$ satisfy functional equations of type (D_1, S_1) and (D_2, S_2), respectively. Let $F_\lambda(X, Y) = \lambda^{-1}(\lambda(X) + \lambda(Y))$ and $F_\mu(X, Y) = \mu^{-1}(\mu(X) + \mu(Y))$.*

If $\theta \in M_d(\mathcal{O}_{\bar{K}})$ *satisfies* $\theta \cdot \left(D_1^{-1} S_1\right) = \left(D_2^{-1} S_2\right) \cdot \theta$ *then* $[\theta]_{\lambda,\mu}(X) := \mu^{-1}(\theta \cdot \lambda(X))$ *has its coefficients in* $\mathcal{O}_K$ *so it is an* $\mathcal{O}_{\bar{K}}$*-homomorphism from* F_λ *to* F_μ*.*

Proof. We can see immediately that

$$\begin{aligned}
&(\theta\lambda) - (D_2^{-1} S_2) \cdot (\theta\lambda) \\
&= \theta\lambda - \theta(D_1^{-1} S_1) \cdot \lambda \\
&= \theta(\lambda - D_1^{-1} S_1 \cdot \lambda) \\
&\equiv \theta \cdot 0 \\
&\equiv 0 \pmod{\mathcal{O}_{\bar{K}}}
\end{aligned}$$

which shows that $\theta\lambda$ satisfies a functional equation of type (D_2, S_2). By part (2) of Hazewinkel's functional equation lemma 2.2.9, this implies that $\mu^{-1}(\theta\lambda(X)) = [\theta]_{\lambda,\mu}(X) \in \mathcal{M}_d(\mathcal{O}_{\bar{K}})$. □

Lemma 3.2.2. *Let* $\Phi(X) \in \mathcal{M}_d(\mathcal{O}_K)$ *be a mixed q-power tuple,* $\Gamma = \Gamma_\Phi$ *be its associated graph, and* $S = S_\Phi$ *its adjacency matrix. Let* K' *be any finite unramified extension of* K *and fix a diagonal uniformizer matrix* $D \in M_d(\mathcal{O}_{K'})$ *and a choice of* $g(X) \in \mathcal{M}_d^\times(\mathcal{O}_{K'})$*. Let* $\lambda(X) \in \mathcal{M}_d^\times(K')$ *be defined by the recursion formula* $(I_d - D^{-1}S) \cdot \lambda(X) = g(X)$ *and define*

$$F_{\Phi,D,g}(X, Y) = \lambda^{-1}(\lambda(X) + \lambda(Y)).$$

By the functional equation lemma, $F_{\Phi,D,g}$ *has coefficients in* $\mathcal{O}_{K'}$*. We also have the following.*

(1) Let $g'(X) \in \mathcal{M}_d^\times(\mathcal{O}_{K'})$*. Then* $F_{\Phi,D,g} \cong F_{\Phi,D,g'}$ *over* $\mathcal{O}_{K'}$*.*

(2) Let $\Gamma_1, \ldots, \Gamma_m$ *be the connected components of* Γ *and let* $\omega_i = |\Gamma_i|$ *for* $1 \le i \le m$*. Let* $\Phi_1, \ldots, \Phi_m$ *be corresponding q-power tuples and let* $X_1, \ldots, X_m$ *be tuples of variables of lengths* $\omega_1, \ldots, \omega_m$*, respectively. For* $1 \le i \le d$ *let* D_i *be the diagonal matrix obtained from* D *by restricting to the indices in* $\Phi_i(X)$*. Then* $F_{\Phi,D,X}$ *decomposes as a direct sum of formal group laws. More precisely,*

$$F_{\Phi,D,X} \cong \bigoplus_{i=1}^{m} F_{\Phi_i,D_i,X_i}.$$

(3) Suppose $\Psi \in \mathcal{M}_d(\mathcal{O}_K)$ is a q-power tuple such that Γ_Ψ and Γ_Φ are isomorphic as directed edge-labeled graphs. Then $F_{\Phi,D,g}$ is isomorphic to $F_{\Psi,D,g}$ over $\mathcal{O}_K$.

Proof. (1) This follows immediately from part (ii) of Hazewinkel's functional equation lemma.

(2) This follows immediately from the definition of a direct sum of formal group laws, since we can partition the index set in such a way that coordinate power series in one block of the partition depend only on the indices in that block.

(3) Suppose that $s : \Gamma_\Phi \to \Gamma_\Psi$ is an isomorphism of directed, edge-labeled graphs. This means that in Γ_Ψ there exists an arrow from $s(i)$ to $s(j)$ labeled with $\tau^{h_{s(i)}}$ if and only if in Γ_Φ there is an arrow from i to j labeled with τ^{h_i}. Then the map $h(X) = (h_i(X))$ with $h_i(X) = x_{s(i)}$ is defined over $\mathbb{Z}$ and $h : F_{\Phi,D,g} \to F_{\Psi,D,g}$ is an isomorphism of formal group laws. This isomorphism corresponds to relabeling the indices $\{1, \ldots, d\}$. Alternatively, this corresponds to conjugating the adjacency matrix of $\Phi(X)$ by a permutation matrix.

□

The lemma 3.2.1 shows that, given functional equations of type (D_1, S_1) and (D_2, S_2), we will often be interested in determining whether there is some $\theta \in M_d(\mathcal{O}_{\bar{K}})$ satisfying $\left(D_1^{-1} S_1\right)\theta = \theta\left(D_2^{-1} S_2\right)$. Let $\pi \in \mathcal{O}_K$ be any uniformizer and let $T_1, T_2 \in \pi^{-1}\mathcal{S}_d(\mathcal{O}_{\bar{K}})$. We define

$$Z(T_1, T_2) = \{\theta \in M_d(\mathcal{O}_{\bar{K}}) : T_2\theta = \theta T_1\}.$$

The following lemma will prove to be useful in showing the non-emptiness of $Z(T_1, T_2)$ in certain cases.

Lemma 3.2.3 (Iwasawa)**.** *Recall that $\bar{K}$ is the completion of the maximal unramified extension of K with respect to the extension ν of the π-adic norm ν_K. Define $\mathcal{O}_{\bar{K}} = \{x \in \bar{K} : \nu(x) \geq 0\}$ and observe that the units of this ring are given by $\mathcal{O}_{\bar{K}}^\times = \{x \in \bar{K} : \nu(x) = 0\}$. Let $m \geq 1$ be an integer and let $K' = K_{ur}^m$ be the unramified extension of K of degree m. Then we have an exact sequence*

$$1 \to \mathcal{O}_{K'}^\times \to \mathcal{O}_{\bar{K}}^\times \to \mathcal{O}_{\bar{K}}^\times \to 1$$

where the first map is the natural inclusion and the second map is given by $a \mapsto \varphi^m(a)/a$ for all $a \in \mathcal{O}_{\bar{K}}^\times$.

Proof. See Iwasawa Lemma 3.11. □

It should be noted that this lemma would not be true as written if we were working over a finite extension K' of K. In that case, if $a \in K'$ then $N_{K'/K}(a) = N_{K'/K}(\varphi(a))$ and so $\varphi(a)/a$ must be of norm one. But since $\bar{K}$ is the completion of an infinite extension, there are elements $a \in \mathcal{O}_{\bar{K}}$ which are not contained in any finite extension of K. Thus the norm map is not well-defined, so we are not restricted to elements of norm one.

Fix a q-power tuple $\Phi(X)$ and two choices of diagonal uniformizer matrices D_1 and D_2 in $M_d(\mathcal{O}_{\bar{K}})$. We are now ready to state and prove a result about $Z\left(D_1^{-1}S_\Phi, D_2^{-1}S_\Phi\right)$.

Lemma 3.2.4. *Let $\Phi(X)$ be a connected q-power tuple in standard form and let S_Φ be its adjacency matrix. Let L be the CM field of Φ and let ι be the embedding type of Φ, which embeds L into the subring of diagonal matrices in $M_d(L)$. Let $D_1, D_2 \in M_d(\mathcal{O}_{\bar{K}})$ be two choices of diagonal uniformizer matrices.*

Then there exists a diagonal matrix $\zeta = \operatorname{diag}(\zeta_1, \ldots, \zeta_d) \in M_d\left(\mathcal{O}_{\bar{K}}^\times\right)$ such that

$$\iota(L) \cdot \zeta \subseteq Z\left(D_1^{-1}S_\Phi, D_2^{-1}S_\Phi\right).$$

If $D_1 = D_2$ then we can take $\zeta = I_d$.

Proof. Let $U = D_1^{-1}D_2 = \operatorname{diag}(u_1, \ldots, u_d)$ for some units $u_1, \ldots, u_d \in \mathcal{O}_{\bar{K}}$ and let $S = S_\Phi$ and $\sigma = \sigma_\Phi$. Let $\alpha_1, \ldots, \alpha_d$ be elements of $\mathcal{O}_{\bar{K}}$ such that $\alpha = \operatorname{diag}(\alpha_1, \ldots, \alpha_d) \in Z\left(D_1^{-1}S, D_2^{-1}S\right)$. Notice that this is equivalent to saying $\alpha(US) = S\alpha$, since we can multiply through by D_2. Let us compute these two matrix products. Both products are nonzero only for entries (i, j) with $j = \sigma(i)$, $1 \le i \le d$, so we need only compare those entries. We obtain that for all i

$$(S\alpha)(i, \sigma(i)) = \tau^{h_i}\alpha_{\sigma(i)} = \alpha_{\sigma(i)}^{\varphi^{h_i}}\tau^{h_i} \qquad \text{and} \qquad (\alpha US)(i, \sigma(i)) = \alpha_i \cdot u_i\tau^{h_i}$$

and conclude that $S\alpha = \alpha(US)$ if and only if

$$\frac{\alpha_{\sigma(i)}^{\varphi^{h_i}}}{\alpha_i} = u_i \qquad \text{for all } i. \tag{3.3}$$

This shows us that knowing α_i determines α_j for all indices j since $\Phi(X)$ is connected. But is it possible to satisfy all of the conditions in (3.3) simultaneously? Since $\Phi(X)$ is in standard form then we

know that the node '1' is in the cycle of Γ, so we can combine the relations in (3.3) to get a constraint on α_1. In particular, if $h = h_\Phi$ is the cycle height of Φ and η_i is defined as in definition 3.5 for $1 \leq i \leq |\gamma|$ then we get a telescoping product

$$\frac{\alpha_1^{\varphi^h}}{\alpha_1} = \left(\frac{\alpha_2^{\varphi^{h_1}}}{\alpha_1}\right) \cdot \varphi^{h_1}\left(\frac{\alpha_3^{\varphi^{h_2}}}{\alpha_2}\right) \cdot \cdots \cdot \varphi^{h_1+\cdots+h_{|\gamma|-1}}\left(\frac{\alpha_1^{\varphi^{h_{|\gamma|}}}}{\alpha_{|\gamma|}}\right) = \prod_{i=1}^{|\gamma|} \varphi^{\eta_i}(u_i) =: N_\Phi(U), \tag{3.4}$$

where $N_\Phi(U)$ is defined by the equation above. Notice that $N_\Phi(U)$ is the type norm of $\Phi(X)$ when $u_i = u_j$ for all indices $1 \leq i, j \leq |\gamma|$; in particular, this is the case if U is a constant multiple of the identity matrix I_d. If equation (3.4) has a solution α_1 then equation (3.3) determines all entries of α.

In the case that $U = I_d$, $N_\Phi(U) = 1$ and so equation (3.4) forces $\alpha_1 \in L$. If not, we note that $N_\Phi(U)$ is a unit in $\mathcal{O}_{\bar{K}}$ and apply lemma 3.2.3 with $K' = K_{ur}^h = L$ to see that (3.4) has a solution $\alpha_1 \in \mathcal{O}_{\bar{K}}$. In fact it has many solutions; if ξ_1 satisfies (3.4) then we can see that $a\xi$ is also a solution of (3.4) for all $a \in L$. Similarly if ξ' is another solution then

$$\frac{(\xi'/\xi)^{\varphi^h}}{\xi'/\xi} = \frac{(\xi')^{\varphi^h}}{\xi'} \cdot \frac{\xi}{(\xi)^{\varphi^h}} = N_\Phi(U) \cdot N_\Phi(U)^{-1} = 1$$

so $\xi'/\xi \in L$. Therefore if ζ is any solution of equation (3.4) then the full set of solutions of (3.4) is given by $L\zeta$. The other entries are determined by the embedding type of $\Phi(X)$. This proves the claim. □

We are now ready to state and prove our main theorem on the construction of formal group laws with complex multiplication.

Theorem 3.2.5. *Let $\Phi(X) = \left(x_{j_i}^{q^{h_i}}\right) \in \mathcal{M}_d(\mathcal{O}_K)$ be a connected q-power tuple with directed graph Γ and let $\gamma \subseteq \Gamma$ be its unique cycle. Let L be the CM field of $\Phi(X)$ and let ι be its embedding type. Fix some choice of uniformizer $\pi \in \mathcal{O}_L$. Then there exists a formal group law $F(X,Y) = F_{\iota(\pi),\Phi}(X,Y) \in \mathcal{FG}_d(\mathcal{O}_K)$ for which the following hold.*

(1) $[\iota(\pi)]_F(X)$ has coefficients in $\mathcal{O}_K$ and satisfies $[\iota(\pi)]_F(X) \equiv \Phi(X) \pmod{\pi}$.

(2) If $\pi' \in \mathcal{O}_K$ is any other choice of uniformizer then $F_{\iota(\pi),\Phi}$ and $F_{\iota(\pi'),\Phi}$ are isomorphic over $\mathcal{O}_{\bar{K}}$.

(3) *If h_γ is the cycle height of Φ and $L = K_{ur}^{h_\gamma}$ is the unique unramified extension of K of degree h_γ then we have an injective ring homomorphism $\rho : \mathcal{O}_L \to \mathrm{End}_{\mathcal{O}_L}(F)$. In other words, we say that F has complex multiplication by the ring of integers of L.*

Proof. Let $S = S_\Phi \in \mathcal{S}_d(\mathcal{O}_K)$ be the matrix associated to Φ as above, so that $S(i, j) = \tau^{h_i}$ whenever $j = j_i$ and $S(i, j) = 0$ else. Recall from the definition that S_Φ is constructed to satisfy $S_\Phi \cdot X = \Phi(X)$. Let $\lambda(X) \in \mathcal{L}_d(L)$ be the d-tuple of power series satisfying the functional equation corresponding to $(\iota(\pi), S)$ and generated by $g(X) = X$. Equivalently, let $\lambda(X)$ be the unique element of $\mathcal{L}_d(L)$ satisfying $(I - \iota(\pi)^{-1}S) \cdot \lambda(X) = X$, so that

$$\begin{aligned}\lambda(X) &= X + \iota(\pi)^{-1}S \cdot X + \iota(\pi)^{-2}S^2 \cdot X + \dots \\ &= X + \iota(\pi)^{-1}\Phi(X) + \iota(\pi)^{-2}\Phi^2(X) + \dots\end{aligned}$$

By the first part of Hazewinkel's functional equation lemma, since the Jacobian of $g(X) = X$ is invertible, the resulting formal group law $F(X, Y) = \lambda^{-1}(\lambda(X) + \lambda(Y))$ has its coefficients in $\mathcal{O}_L$. We can now prove the three remaining claims.

(1) We will see that $[\iota(\pi)]_F(X)$ has its coefficients in $\mathcal{O}_L$ by showing that $\iota(\pi)\lambda(X)$ and $\lambda(X)$ satisfying the same type of functional equation and then applying part (ii) of Hazewinkel's functional equation lemma. Recall that $\lambda(X)$ satisfies a functional equation of type $(\iota(\pi), S)$, which means that

$$\lambda(X) - \iota(\pi)^{-1}S \cdot \lambda(X) \equiv 0 \pmod{\mathcal{O}_{\bar{K}}}. \tag{3.5}$$

To simplify notation, let $S_0 = \iota(\pi)^{-1}S$. By lemma 3.2.4 with $D_1 = D_2 = \iota(\pi)$, $\iota(\pi)S_0 = S_0\iota(\pi)$. This allows us to see that

$$\begin{aligned}&(\iota(\pi)\lambda(X)) - S_0 \cdot (\iota(\pi)\lambda(X)) \\ =&(\iota(\pi)\lambda(X)) - \iota(\pi)S_0 \cdot \lambda(X) \\ =&\iota(\pi)\left(\lambda(X) - S_0 \cdot \lambda(X)\right) \\ =&\iota(\pi)X \\ \equiv&0 \pmod{\mathcal{O}_{\bar{K}}}\end{aligned}$$

so we conclude that $\iota(\pi)\lambda(X)$ and $\lambda(X)$ satisfy the same type of functional equation $(\iota(\pi), S)$. By part (ii) of Hazewinkel's functional equation lemma, we conclude that

$$[\iota(\pi)]_F(X) = \lambda^{-1}(\iota(\pi)\lambda(X))$$

has its coefficients in $\mathcal{O}_L$.

To see that $[\iota(\pi)]_F(X) \equiv \Phi(X) \pmod{\pi}$, we have as in (1) that $S\iota(\pi) = \iota(\pi)S$ and conclude by induction that $S\iota(\pi)^n = \iota(\pi)^n S$ for all $n \in \mathbb{Z}$. We also know from definition 3.1 that S is constructed to satisfy $S \cdot X = \Phi(X)$, so

$$S\iota(\pi)^{-n}\Phi^n(X) = \iota(\pi)^{-n}SX \circ \Phi^n(X) = \iota(\pi)^{-n}\Phi \circ \Phi^n(X) = \iota(\pi)^{-n}\Phi^{n+1}(X)$$

for all $n \in \mathbb{Z}$. Therefore

$$\begin{aligned}
\lambda([\iota(\pi)]_F(X)) &= \iota(\pi)\lambda(X) \\
&= \iota(\pi)X + S \cdot \lambda(X) \\
&= \iota(\pi)X + \left(\Phi(X) + \iota(\pi)^{-1}\Phi^2(X) + \dots\right) \\
&= \iota(\pi)X + \lambda(\Phi(X)) \\
&\equiv \lambda(\Phi(X)) \pmod{\pi}
\end{aligned}$$

which implies that $[\iota(\pi)]_F(X) \equiv \Phi(X) \pmod{\pi}$ by part (iv) of the functional equation lemma.

(2) Let $\lambda(X), \mu(X) \in \mathcal{L}_d(K)$ be d-tuples of power series satisfying functional equations of type $(\iota(\pi), S)$ and $(\iota(\pi'), S)$, respectively, and both generated by $g(X) = X$. Let $F, G \in \mathcal{FG}_d(\mathcal{O}_K)$ be their corresponding formal group laws. By lemma 3.2.1, we know that there is an $\mathcal{O}_{\bar{K}}$-homomorphism from F to G if and only if there exists some $\theta \in M_d(\mathcal{O}_{\bar{K}})$ such that $\theta(\iota(\pi)^{-1}S) = (\iota(\pi')^{-1}S)\theta$, or equivalently, $\theta \in Z(\iota(\pi)^{-1}S, \iota(\pi')^{-1}S)$. We can apply lemma 3.2.4 to see that there exists a diagonal matrix $\zeta \in M_d(\mathcal{O}_{\bar{K}}^{\times})$ such that $Z(\iota(\pi)^{-1}S, \iota(\pi')^{-1}S) = \iota(L) \cdot \zeta$, so we can take $\theta \in \iota(\mathcal{O}_L^{\times}) \cdot \zeta$. Then $\mu^{-1}(\theta\lambda(X))$ has its coefficients in $\mathcal{O}_{\bar{K}}$ and gives us an $\mathcal{O}_{\bar{K}}$-homomorphism from F to G. Since the matrix θ is invertible then this map has an inverse and we see that F and G are isomorphic over $\mathcal{O}_{\bar{K}}$.

(3) We once again apply lemma 3.2.1 and 3.2.4 to see that $\iota(\alpha)\lambda(X)$ and $\lambda(X)$ satisfy the same type of functional equation for any $\alpha \in \mathcal{O}_L$, and therefore that $\lambda^{-1}(\iota(\alpha)\lambda(X)) = [\iota(\alpha)]_F(X)$ has coefficients in $\mathcal{O}_L$. We have already seen that the map $[-]_F(X) : M_d(L) \to \mathrm{End}_L(F)$ is a ring homomorphism in chapter 2. Since $[\iota(\alpha)]_F(X) \equiv \iota(\alpha)X \pmod{\deg 2}$, this map is also injective. Thus we have an inclusion of rings

$$\rho : \mathcal{O}_L \to \mathrm{End}_{\mathcal{O}_L}(F).$$

□

Example 3.7. Let $\Phi(X) = \left(x_2^q, x_3^{q^3}, x_1^{q^5}\right)$. Then the CM field of Φ is $L = K_{ur}^9$, the embedding type of $\Phi(X)$ is given by $\iota = (1, \varphi^{-1}, \varphi^{-4})$, and the adjacency matrix S_Φ is given by

$$S = \begin{bmatrix} 0 & \tau & 0 \\ 0 & 0 & \tau^3 \\ \tau^5 & 0 & 0 \end{bmatrix}.$$

Fix a choice of uniformizer $\pi \in \mathcal{O}_L$ and let $\lambda(X)$ be defined by the functional equation

$$(I_3 - \iota(\pi)^{-1}S) \cdot \lambda(X) = X.$$

Then

$$\begin{aligned}
\lambda(X) =& (I_3 - \iota(\pi)^{-1}S) \cdot X \\
=& X + \iota(\pi)^{-1}S \cdot X + \iota(\pi)^{-2}S^2 \cdot X + \dots \\
=& \begin{bmatrix} x_1 + \pi^{-1}x_2^q + \pi^{-2}x_3^{q^4} + \pi^{-3}x_1^{q^9} + \dots \\ x_2 + \varphi^{-1}(\pi)^{-1}x_3^{q^3} + \varphi^{-1}(\pi)^{-2}x_1^{q^8} + \varphi^{-1}(\pi)^{-3}x_2^{q^9} + \dots \\ x_3 + \varphi^{-4}(\pi)^{-1}x_1^{q^5} + \varphi^{-4}(\pi)^{-2}x_2^{q^6} + \varphi^{-4}(\pi)^{-3}x_3^{q^9} + \dots \end{bmatrix} \\
=& \sum_{n=0}^{\infty} \iota(\pi)^{-n}\Phi^n(X).
\end{aligned}$$

The formal group law $F_\lambda(X, Y)$ has complex multiplication by $\mathcal{O}_L$. We will soon see that the extensions $L_\pi^n = L(F[\pi^n])$ are abelian over L and that the Galois group $\mathrm{Gal}(L_\pi^n/L)$ is isomorphic to a subgroup of $(\mathcal{O}_L/\pi^n\mathcal{O}_L)^\times$.

If Γ is a cycle we say that the formal group law constructed in 3.2.5 has *full complex multiplication* by $\mathcal{O}_L$, the ring of integers of L. In the case that Γ is connected but is not a cycle the formal group law F will have *partial* complex multiplication by a ring of integers of an unramified extension of K.

Lemma 3.2.6. *Let $\Phi(X) \in \mathcal{M}_d(\mathcal{O}_K)$ be a connected q-power tuple, L the CM-field of $\Phi(X)$, $\iota = \iota_\Phi$ be the embedding type of $\Phi(X)$, and fix a uniformizer $\pi \in \mathcal{O}_L$. Let $F_{\iota(\pi),\Phi}(X, Y) \in \mathcal{FG}_d(\mathcal{O}_L)$ be the formal group law obtained in theorem 3.2.5.*

Then $[\iota(\pi)]_F(X)$ has finite height if and only if $\Phi(X)$ is a cycle.

Proof. Let $\tilde{L}$ be the residue field of L and let $f(X) = (f_1(X), \ldots, f_d(X)) \in \mathcal{M}_d(\tilde{L})$ be obtained from $[\iota(\pi)]_F(X)$ by reducing the coefficients modulo $\mathfrak{p}_L$, which we note is possible since $[\iota(\pi)]_F(X) \in \mathcal{M}_d(\mathcal{O}_L)$.

Recall that the height of $f(X)$ is defined to be the integer H such that the rank of $\tilde{L}[[x_1, \ldots, x_d]]$ over the free subring generated by $(f_1(X), \ldots, f_d(X)) = \left(x_{\sigma(1)}^{q^{h_1}}, \ldots, x_{\sigma(d)}^{q^{h_d}}\right)$ is equal to p^H, if this rank is finite.

If $\Phi(X)$ is a cycle then σ is surjective, so this rank is finite and is equal to $q^{h_1}q^{h_2}\ldots q^{h_d} = q^{h_1+\cdots+h_d}$. Thus the height is equal to $h_\Phi f$ where $h_\Phi = \sum h_i$ and where $q = p^f$ is the order of the residue field of K. This is also equal to the degree of the residue field extension $[\tilde{L} : \mathbb{Z}/p\mathbb{Z}] = [\tilde{L} : k][k : \mathbb{Z}/p\mathbb{Z}]$.

Conversely, suppose $\Phi(X)$ is not a cycle, which since $\Phi(X)$ is connected implies that σ is not surjective. Then there exists some $j \in \{1, \ldots, d\}$ such that every power of x_j is needed to generate $\tilde{L}[[X]]$ over the subring generated by $(f_1(X), \ldots, f_d(X))$, so the height of $\Phi(X)$ is infinite. □

Let $F(X, Y) \in \mathcal{FG}_d(\mathcal{O}_L)$ with full complex multiplication by $\mathcal{O}_L$ and let $\alpha \in \mathcal{O}_L$. We recall that $\mathbf{0} = (0, \ldots, 0)$ is the identity element in $F[\pi^n]$ and we define the *α-torsion* of $F(X, Y)$ to be the set $F[\alpha]$ of solutions of the equation $[\iota(\alpha)]_F(X) = \mathbf{0}$ with coordinates in $\mathfrak{p}_\Omega$, the prime ideal of the ring of integers of the algebraic closure Ω over K. When $\alpha = \pi^n$ for some $n \geq 1$, we can obtain extensions $L_\pi^n = L(F[\pi^n])$ of L by adjoining the coordinates of these solutions to L.

Theorem 3.2.7. *If Γ_Φ is a cycle (so that F_Φ has full complex multiplication) and $n \geq 1$ then the extension $L_\pi^n = L(F[\pi^n])$ of L obtained by adjoining the coordinates of $F[\pi^n]$ to L is abelian and*

$$\mathrm{Gal}\,(L_\pi^n/L) \subseteq (\mathcal{O}_L/\pi^n\mathcal{O}_L)^\times.$$

Proof. We first observe that since $\mathcal{O}_L \hookrightarrow \mathrm{End}_{\mathcal{O}_L}(F)$ then $F[\pi^n]$ naturally has the structure of an $\mathcal{O}_L$-module with $\alpha \cdot \zeta$ defined to be $[\alpha]_F(\zeta)$ for $\alpha \in \mathcal{O}_L$ and $\zeta \in F[\pi^n]$. By definition we have $\pi^n \cdot \zeta = \mathbf{0}$, so the action of $\mathcal{O}_L$ on $F[\pi^n]$ factors through the quotient $\mathcal{O}_L/\pi^n\mathcal{O}_L$. In fact, this is the smallest quotient through which this action can factor. Let $\zeta \in F[\pi^n]$ such that $\zeta \notin F[\pi^m]$ for $m < n$; we know that such an element exists because $|F[\pi^n]| = (q^h)^n = q^{hn}$, as is shown in Appendix B.2 in [6]. Now let $\alpha \in \mathcal{O}_L$ such that $\alpha \cdot \zeta = \mathbf{0}$. It is clear that the ideal generated by α in $\mathcal{O}_L$ must annihilate ζ and this ideal cannot be the full ring since $1 \cdot \zeta = \zeta \neq \mathbf{0}$. Therefore α is not a unit, so $\alpha = \pi^m\beta$ for some $m \geq 1$ and $\beta \in \mathcal{O}_K^\times$. It is now clear that $\beta \cdot (\pi^m \cdot \zeta) = \mathbf{0}$, but since β is a unit then in fact $\pi^m \cdot \zeta = \mathbf{0}$. By assumption $\zeta \notin F[\pi^m]$ for $m < n$ so this forces $m \geq n$, and thus $\alpha \in \pi^n\mathcal{O}_L$. This shows that $\mathcal{O}_L/\pi^n\mathcal{O}_L$ is the smallest quotient through which the action of $\mathcal{O}_L$ on $F[\pi^n]$ factors. Since $\mathcal{O}_L$ is unramified of degree $h = h_\Phi$ over K, then

$$|\mathcal{O}_L/\pi^n\mathcal{O}_L| = (q^h)^n = q^{hn} = |F[\pi^n]|.$$

We conclude that the action of $\mathcal{O}_L/\pi^n\mathcal{O}_L$ is transitive on $F[\pi^n]$. In other words, $F[\pi^n]$ is principally generated as an $\mathcal{O}_L$-module.

Now consider the action of the Galois group $G = \mathrm{Gal}(L_\pi^n/L)$ on the set $F[\pi^n]$. For any $g \in G$,

$$[\iota(\pi^n)](\zeta^g) = ([\iota(\pi^n)]^g(\zeta))^g = ([\iota(\pi^n)](\zeta))^g = \mathbf{0}^g = \mathbf{0},$$

so $F[\pi^n]^g = F[\pi^n]$. Fix an element $\zeta \in F[\pi^n]$ such that $\mathcal{O}_L \cdot \zeta = F[\pi^n]$ and fix some $g \in G$. Since $\zeta^g \in F[\pi^n]$ there exists some $\beta \in \mathcal{O}_L$ such that $\zeta^g = \beta \cdot \zeta$. We claim that in fact $\xi^g = \beta \cdot \xi$ for all $\xi \in F[\pi^n]$. To see this, let $\xi \in F[\pi^n]$ be arbitrary and let $\alpha \in \mathcal{O}_L$ such that $\xi = \alpha \cdot \zeta$. Then

$$\xi^g = (\alpha \cdot \zeta)^g = \alpha^g \cdot \zeta^g = \alpha \cdot \zeta^g = \alpha \cdot (\beta \cdot \zeta) = \beta \cdot (\alpha \cdot \zeta) = \beta \cdot \xi.$$

Define a map $f : G \to (\mathcal{O}_L/\pi^n\mathcal{O}_L)^\times$ by $\rho(g) = \beta$ where $\xi^g = \beta \cdot \xi$ for all $\xi \in F[\pi^n]$. Then ρ is a group homomorphism since if $g, h \in G$ with $g \mapsto \alpha$ and $h \mapsto \beta$ then

$$\zeta^{gh} = (\zeta^g)^h = (\alpha \cdot \zeta)^h = \alpha^h \cdot \zeta^h = \alpha \cdot (\beta \cdot \zeta) = (\alpha\beta) \cdot \zeta.$$

Let $g \in G$ and suppose $\rho(g) = 1$; then $\rho(\zeta) = 1 \cdot \zeta = \zeta$ for all $\zeta \in F[\pi^n]$ so g must be the identity in G. We conclude that we have an injective group homomorphism

$$G \hookrightarrow \mathrm{Aut}_{\mathcal{O}_L\text{-mod}}(F[\pi^n]) = \mathrm{Aut}_{\mathcal{O}_L\text{-mod}}(\mathcal{O}_L/\pi^n\mathcal{O}_L) \cong (\mathcal{O}_L/\pi^n\mathcal{O}_L)^\times,$$

and consequently that G is abelian and isomorphic to a subgroup of $(\mathcal{O}_L/\pi^n\mathcal{O}_L)^\times$. □

Therefore we have constructed a class of formal group laws with complex multiplication and have shown that, under some mild conditions, these generate abelian extensions. In the future we would like to study the ramification degree of these extensions and their norm groups to further extend the analogy with the results of local class field theory.

Bibliography

[1] Laurent Berger. Iterated extensions and relative Lubin-Tate groups. Annales mathématiques du Québec, 40(1):17–28, Jan. 2016.

[2] Robert F. Coleman. Division values in local fields. Inventiones Mathematicae, 53(2):91–116, Jun. 1979.

[3] Ehud de Shalit. Relative Lubin-Tate groups. Proceedings of the American Mathematical Society, 95(1):1–1, Jan. 1985.

[4] David Grant. Coates-Wiles towers in dimension two. Mathematische Annalen, 282(4):645–666, Dec. 1988.

[5] Michael Harris and Richard Taylor. On the geometry and cohomology of some simple Shimura varieties. Princeton University Press, Princeton, New Jersey, 2001.

[6] Michiel Hazewinkel. Formal Groups and Applications. Academic Press, Inc., New York, New York, 1978.

[7] Taira Honda. On the theory of commutative formal groups. Journal of the Mathematical Society of Japan, 22(2):213–246, Apr. 1970.

[8] M. J. Hopkins and B. H. Gross. The rigid analytic period mapping, Lubin-Tate space, and stable homotopy theory. Bulletin of the American Mathematical Society, 30(1):76–87, Jan. 1994.

[9] Kenkichi Iwasawa. Local Class Field Theory. Oxford University Press, New York, New York, 1986.

[10] Neal Koblitz. p-adic Numbers, p-adic Analysis, and Zeta Functions. Springer-Verlag, New York, New York, 1984.

[11] H. Koch. Verallgemeinerung einer konstruktion von lubin-tate in der theorie der barsotti-tate-gruppen. Symp. Math. INDAM, 15:487–498, 1973.

[12] Jonathan Lubin and John Tate. Formal complex multiplication in local fields. The Annals of Mathematics, 81(2):380, Mar. 1965.

[13] Jean-Pierre Serre. Lie Algebras and Lie Groups. Springer-Verlag, New York, New York, 1992.

[14] Joseph H. Silverman. The Arithmetic of Elliptic Curves. Springer Science & Business Media, New York, New York, 1986.

[15] Joseph H. Silverman. Advanced Topics in the Arithmetic of Elliptic Curves. Springer-Verlag, New York, New York, 1994.

[16] J. T. Tate. p-divisible groups. In Proceedings of a Conference on Local Fields, pages 158–183. Springer Berlin Heidelberg, 1967.

[17] A. Wiles. Higher explicit reciprocity laws. The Annals of Mathematics, 107(2):235, Mar. 1978.