p-ADIC L-FUNCTIONS OF A SPECIFIED MODULUS

KEVIN POWELL

1. Introduction

The intent of the present summary is to present de Shalit's construction of a p-adic L-function of a given modulus $\mathfrak{f}$ over an imaginary quadratic field.

Let $\mathfrak{f}$ and $\mathfrak{p}$ be non-trivial integral ideals of an imaginary quadratic extension K of $\mathbb{Q}$. Suppose that $\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p} = p$ is a prime. Hence p splits in K. The p-adic L-function of modulus $\mathfrak{f}$ is a function on the continuous p-adic characters of $\mathcal{G}(\mathfrak{f}) = \mathrm{Gal}(K(\mathfrak{f}\mathfrak{p}^\infty)/K)$ given by

$$L_{p,\mathfrak{f}}(\epsilon) = \int_{\mathcal{G}(\mathfrak{f})} \epsilon^{-1}(\sigma) d\mu(\mathfrak{f}, \sigma)$$

for a certain integral measure $\mu(\mathfrak{f})$. The purpose of this summary is to describe the construction of this measure. Some of the objects involved will be formal groups, elliptic curves and elliptic units.

2. Elliptic curves: a brief synopsis

Definition 2.1. An **elliptic curve** is a pair (E,O) over the field L where E is nonsingular curve defined over L of genus 1 and O is a point on that curve.

We will assume that $L \subset \mathbb{C}$. Every elliptic curve over a field L of characteristic 0 has a Weierstrass model of the form

$$y^2 = 4x^3 - g_2 x - g_3 \tag{1}$$

with $g_2, g_3 \in L$ and $\Delta_E = g_2^3 - 27g_3^2 \neq 0$, which ensures that the polynomial $4x^3 - g_2 x - g_3$ has 3 distinct roots e_1, e_2, e_3. The point O (the point at ∞) is given by $[(0,1,0)]$ in terms of homogenous coordinates x, y, z in $zy^2 = 4x^3 - g_2 xz^2 - g_3 z^3$.

Definition 2.2. The j-invariant of E is given by $j(E) = \frac{1728 g_2^3}{\Delta_E}$ (which is independent of the model chosen for E).

Remark 2.3. Although this model is not suitable for reductions modulo 2 and 3, this form simplifies the calculations in the present paper. That being the case, the primes considered here in $\mathcal{O}_L$ will be those not lying above 2 or 3. The results contained here or to which I make reference can be generalized to consider these excluded primes. See ([5], 1.11). This particular Weierstrass form is unique up to a change $(g_2, g_3) \mapsto (u^4 g_2, u^6 g_3)$ where $u \in L^\times$.

The map $\psi : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ given by $(x,y) \mapsto x$ is a double cover ramified exactly at e_1, e_2, e_3, O. Endowing a complex analytic structure on $E(\mathbb{C})$, it is, as a manifold, topologically homeomorphic to two copies of $\mathbb{P}^1(\mathbb{C})$ where the branch cut between $\psi(e_1)$ and $\psi(e_2)$ on one copy is glued to the same branch cut on the other copy. Similarly, the branch cuts from $\psi(e_3)$ and $\psi(O)$ are glued together. Thus, E

is homeomorphic to a torus so that $H_1(E,\mathbb{Z}) = [\gamma_1]\mathbb{Z}+[\gamma_2]\mathbb{Z}$ for two noncontractible loops γ_1 and γ_2.

Let α be a path from O to any point $P \in E(\mathbb{C})$. The differential $\omega_E = \frac{dx}{y}$ is holomorphic on E. The integral $\int_\alpha \frac{dx}{y}$ depends only on the homology class of the path α. By taking the $\mathbb{Z}$-lattice Λ_E generated by periods $\int_{\gamma_1}\omega_E$ and $\int_{\gamma_2}\omega_E$, the map

$$P \mapsto \int_O^P \omega_E \mod \Lambda_E \tag{2}$$

is a well-defined holomorphic isomorphism $E(\mathbb{C}) \to \mathbb{C}/\Lambda$. Conversely, given a $\mathbb{Z}$-lattice $\Lambda \in \mathbb{C}$, $\mathbb{C}/\Lambda \simeq E_\Lambda(\mathbb{C})$ for some elliptic curve E_Λ [8, VI.5.2].

Definition 2.4. Denote the the map given in (2) by Ψ_E. This map and the lattice Λ_E depends on the choice of model for E.

Definition 2.5. The Weierstrass $\wp$-function with respect to Λ is given by:

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right). \tag{3}$$

Proposition 2.6. *For $z \neq 0$, $\Psi_E^{-1}(z) = (\wp(z), \wp'(z), 1)$ and $\Psi_E(0) = O$.*

Proof. [8, VI.5.2] □

The map Ψ_E^{-1} transfers the group structure of $\mathbb{C}/\Lambda$ to the points of $E(\mathbb{C})$. This is the same as the group structure of E naturally induced by $\mathrm{Pic}^0(E)$ (See [8, VI.5.2]). Among the points of $E(\mathbb{C})$, this group law has a nice geometric description as follows (See [8, III.2]). Let $A = [(x_1, y_1, z_1)]$ and $B = [(x_2, y_2, z_2)]$ be two points in $E(\mathbb{C})$ such that both of them are not simultaneously O. Let l_1 be the line between them in $\mathbb{P}^2(\mathbb{C})$ or the tangent line if $A = B$. This line will intersect $E(\mathbb{C})$ at a point R distinct from A and B. Let l_2 denote the line between R and O or the tangent line if $R = O$. Then, l_2 will intersect $E(\mathbb{C})$ at a point C distinct from R and O if l_2 is not the tangent to $E(\mathbb{C})$ at O. If l_2 is tangent to $E(\mathbb{C})$ at O, let $C = 0$. If $+_E$ denotes the addition described, $A +_E B = C$. It will be noted that this description depends on the embedding of E into $\mathbb{P}^2(\mathbb{C})$ which is intrinsically given by the model of E.

We have the following proposition which will be useful to us:

Proposition 2.7. *If $A \in E(\mathbb{C})$ such that $A = [(x_0, 0, 1)]$, then*

$$A +_E A = 0$$

Proof. Let $S(x,y) = -y^2 + 4x^3 - g_2x - g_3$. In affine coordinates, the tangent line to $E(\mathbb{C})$ at A is given by the points (x,y) satisfying

$$\begin{pmatrix}\partial S/\partial x|_{(x_0,0)} & \partial S/\partial y|_{(x_0,0)}\end{pmatrix} \cdot \begin{pmatrix} x - x_0 & y\end{pmatrix}^{\mathrm{T}} = 0.$$

Since $\partial S/\partial y|_{x_0,0} = 0$, the line l_1 in the description above is given by $x = x_0$. In homogeneous coordinates, l_1 is given by $x = x_0 z$ so that $O = [(0,1,0)]$ lies on l_1. Continuing through the description, $R = O$ and l_2 is tangent to O. Hence, $A +_E A = 0$.

□

3. The Associated Formal Group

Let R be a commutative ring such that 2 and 3 are not zero divisors (the necessity of the second condition will be apparent below).

Definition 3.1. A formal group law over R is a binary operation $[+]$ on $xR[[x]]$ defined by $f[+]g = F(f,g)$ where $F(x,y) \in R[[x,y]]$ satisfies the following properties:

(1) $F(x,y) = F(y,x)$ (so $[+]$ is commutative)
(2) $F(F(x,y),z) = F(x,F(y,z))$ (so $[+]$ is associative)
(3) $F(x,y) \equiv x + y \mod \deg 2$

Proposition 3.2. *The set and binary operation $(xR[[x]],[+])$ form an abelian group with $0 \in xR[[x]]$ as the identity element.*

Now suppose we parameterize E by $t = \frac{-2x}{y}$, $w = \frac{-2}{y}$ so that O corresponds to $t = 0$. Let E be given by a Weierstrass model as in (1) such that $g_2, g_3 \in R$. To discuss the formal group law $\hat{E}$ over R, we first find formal solutions $(x(t), y(t))$ to the Weierstrass equation (1) for $x(t), y(t) \in R[[t]]$. Using $x = \frac{t}{w}$ and $y = \frac{-2}{w}$, from (1) we obtain $w = t^3 - \frac{g_2}{4}tw^2 - \frac{g_3}{4}w^3$. Set

$$g(w) = t^3 - \frac{g_2}{4}tw^2 - \frac{g_3}{4}w^3 \in R[[t]][w].$$

Let $g^{(n)}$ denote $g \circ g \circ g \circ ... \circ g$ where g appears n times. Then we wish to show that $\lim_{n\to\infty} g^{(n)}(w)$ converges to an element of $R[[t]]$. Since $R[[t]]$ is complete with respect to (t), we may apply Hensel's lemma [8, IV.1.2] as follows. Let $h(w) = g(w) - w$, $w_0 = 0$ so that $h(w_0) \in t^3R[[t]]$ and $h'(w_0) = -1$. Then, the sequence $w_{m+1} = w_m + h(w_m)$ converges to an element $\tilde{w}$ in $R[[t]]$ which uniquely satisfies $h(\tilde{w}) = 0$ and $\tilde{w} \in tR[[t]]$.

In the coordinates (t,w), let $A = (t_1, w_1)$, $B = (t_2, w_2)$, and $C = A +_E B = (t_3, w_3)$. It can be shown that the geometric description of $+_E$ applied in these coordinates yields that $t_3 \in R[[t_1, t_2]]$ such that $t_3 \equiv t_1 + t_2 \mod (t_1^2, t_2^2, t_1t_2)$ [8, IV.1]. The group structure of E implies that by setting $F(t_1, t_2) = t_3$, F is a formal group law.

Definition 3.3. Let $\hat{E}$ denote the formal group law F obtained in the previous paragraph.

4. Morphisms between Formal Group Laws

Definition 4.1. Let F and G be formal group laws over the commutative ring R so they respectively induce the abelian groups $A = (xR[[x]],[+]_F)$ and $B = (xR[[x]],[+]_G)$. We define $\mathrm{Hom}_R(F,G) \subset \mathrm{Hom}_{\mathrm{Ab}}(A,B)$ to be the morphisms given by power series $f \in xR[[x]]$ such that $h(x) \mapsto f(h(x))$. That is, $f \circ F = G \circ f$.

One can either check using properties of a formal group law G that $\mathrm{Hom}_R(F,G)$ is an abelian group or consider it as a power series subgroup of $\mathrm{Hom}_{\mathrm{Ab}}(A,B)$.

Proposition 4.2. *The map $\Upsilon : (\mathrm{Hom}_R(F,G),[+]_G) \to (R,+)$ given by $f \mapsto f'(0)$ is an injective group homomorphism.*

Proof. That the map is a homomorphism follows from $f(x)[+]_G g(x) \equiv (f'(0) + g'(0))x \mod \deg 2$. So, we focus on injectivity.

Let $F(x,y) = \sum_{i,j=0}^{\infty} \alpha_{ij} x^i y^j$ and $G(x,y) = \sum_{i,j=0}^{\infty} \beta_{ij} x^i y^j$. By virtue of being formal group laws:

$$\alpha_{00} = \beta_{00} = 0 \tag{4}$$

$$\alpha_{01} = \alpha_{10} = \beta_{01} = \beta_{10} = 1 \tag{5}$$

$$\alpha_{i0} = \alpha_{0i} = \beta_{0i} = \beta_{i0} = 0 \quad \text{if } i > 1 \tag{6}$$

since where (6) follows since 0 is the additive identity of the two formal group laws. Also, let $f(x) = \sum_{i=1}^{\infty} a_m x^m$. Suppose that

$$f \circ F(x,y) = G(f(x), f(y)) \tag{7}$$

and let c_{uv} be the coefficient of $x^u y^v$ on either side. Then, we obtain two expressions for c_{uv}. On the left of (7), we obtain:

$$c_{uv} = \sum_{m, i_1 + \cdots + i_m = u, j_1 + \cdots + j_m = v} a_m (\alpha_{i_1 j_1} \cdots \alpha_{i_m j_m}).$$

On the right of (7), we obtain:

$$c_{uv} = \sum_{m,n, i_1 + \cdots + i_m = u, j_1 + \cdots + j_n = v} \beta_{mn} (a_{i_1} \cdots a_{i_m})(a_{j_1} \cdots a_{j_n}).$$

Let $N \in \mathbb{Z}^+$. Suppose $u + v = N$. We claim that on the left of (7), the coefficient of a_N is $\binom{N}{u}$. We prove the claim as follows. Let $k \in \{1, ..., N\}$. Suppose $\alpha_{i_1 j_1} \cdots \alpha_{i_N j_N} \neq 0$. To avoid the presence of $\alpha_{l,0}$ for $l > 1$, by (6) we must have $i_k = 0$ and $j_k = 1$ or $i_k = 1$ and $j_k = 1$ for each $k = 1, ..., N$. There are precisely $\binom{N}{u}$ ways to do this. Then, using (5) completes the claim.

On the right, only the a_k for $k < N$ appear since $i_1 + \cdots + i_m + j_1 + \cdots + j_n = N$ and we may assume that $i_k, j_k > 0$ for $k = 1, ..., n$ since $a_0 = 0$. Thus, a_N is uniquely determined by a_k for $k < N$ since R is a domain of characteristic 0. Therefore, f is uniquely determined by a choice of a_1. □

We now can make the following definition:

Definition 4.3. If $a \in \Upsilon(\mathrm{Hom}_R(F,G))$, define $[a]_{F,G} = \Upsilon^{-1}(a)$. If $F = G$, we use the notation $[a]_F$.

Let Q denote the fraction field of the commutative ring R. We will see that $[a]_{F,G}$ is defined over Q for any $a \in Q$. To do so, we use the formal logarithm described below.

Definition 4.4. We define the additive formal group law over a R to be $\hat{G}_a(x,y) = x + y$.

Definition 4.5. Let F be a formal group law. If $[1]_{F,\hat{G}_a}$ exists, it is called the formal normalized logarithm of F and denoted as λ_F.

Proposition 4.6. *If F is defined over R, λ_F exists over Q.*

Proof. See (See [3, 4.1]). One consequence of the proof is that we must have $\lambda_F'(x) \in R$ so that $\lambda_F(x) = x + \sum_{n \geq 1} \frac{a_n}{n} x^n$ where $a_n \in R$. □

We observe that for $a \in Q$, $[a]_{\hat{G}_a}(x)$ exists and is given by ax. Then

$$\lambda_G^{-1} \circ [a]_{\hat{G}_a} \circ \lambda_F \in \mathrm{Hom}_Q(F, G)$$

and is given by $[a]_{F,G}$. Thus, it makes sense to discuss $[a^{-1}]_{F,G}$ over Q. In particular, $[a^{-1}]_F$ is the composition inverse of $[a]_F$. But this is only a special case of the following well-known fact about power series: if $f \in xR[[x]]$ and $f'(0)$ is invertible in R, then f has a composition inverse g in $xR[[x]]$ such that $g'(0) = f'(0)^{-1}$.

5. Relative Lubin-Tate Formal Group Laws

We discuss formal group laws that are induced from certain power series in one variable. These will be termed relative Lubin-Tate formal group laws.

Let p be any prime. Fix a complete algebraic closure $\mathbb{C}_p$ of $\mathbb{Q}_p$ containing all extensions of $\mathbb{Q}_p$ in what follows. Fix k as a finite unramified extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}$, maximal ideal $\mathfrak{p}$, and $q = |\mathcal{O}_k/\mathfrak{p}|$. Let ν be the normalized valuation that uniquely extends ν_p to k (i.e. $\nu(k^\times) = \mathbb{Z}$). Fix $d \in \mathbb{N}$. Then let ν', $\mathcal{O}'$, $\mathfrak{p}'$, q' be the corresponding objects for the unique unramified extension k' of k with $[k' : k] = d$. Let ϕ be the Frobenius automorphism in $\mathrm{Gal}(k^{ur}/k)$ where k^{ur} is the maximal unramified extension of k in $\mathbb{C}_p$. Then, ϕ^d is the Frobenius automorphism in $\mathrm{Gal}(k^{ur}/k')$. Let R represent the valuation ring of any complete unramified extension of k containing k'. In particular, $\mathcal{O}' \subset R \subset \mathcal{O}_{\hat{k}^{ur}}$.

Definition 5.1. Let $\xi \in k^\times$ where $\nu(\xi) = d$. Define

$$\mathfrak{F}_\xi = \{f \in x\mathcal{O}'[[x]] \mid \mathrm{N}_{k'/k}(f'(0)) = \xi, f \equiv x^q \mod \mathfrak{p}'\}.$$

Lemma 5.2. *Let $f, g \in \bigcup_{\nu(\xi)=d} \mathfrak{F}_\xi$, and let $F_1(x_1, ..., x_n)$ be a linear form in $R[x_1, ..., x_n]$. Suppose that $f \circ F_1 \equiv F_1^\phi \circ (g, ..., g) \mod \deg 2$. Then there exists a unique $F \in R[[x_1, ..., x_n]]$ satisfying:*

(i) $F \equiv F_1 \mod \deg 2$

(ii) $f \circ F = F^\phi \circ (g, ..., g)$.

Proof. See the proof of [5, I.1.4] noting that the argument does not depend on f and g being in the same set $\mathfrak{F}_\xi$. The proof also remains valid with R in place of $\mathcal{O}'$. □

Corollary 5.3. *Let $f \in \mathfrak{F}_\xi$. Also let $a, b \in x\mathcal{O}'[[x]]$. Then, there exists a unique formal group law F over $\mathcal{O}'$ such that: $f(a)[+]_{F^\phi} f(b) = f(a[+]_F b)$ where F^ϕ is the series $F(x, y)$ with ϕ applied to the coefficients. In other words, $f \in \mathrm{Hom}_{\mathcal{O}'}(F, F^\phi)$.*

Proof. In the lemma, let $f = g$ and $F_1(x, y) = x + y$. Then let F_f be the power series $F \in \mathcal{O}'[[x, y]]$ obtained. Clearly, $F_f(y, x)$ meets condition (i). Condition (ii) also holds since reversing the order of inputs on the right does the same on the left. Thus, by uniqueness, $F_f(x, y) = F_f(y, x)$. For associativity, applying condition (ii) twice to F_f in $f \circ F_f(F_f(x, y), z)$ yields $F_f(F_f(f(x), f(y)), f(z))$ thus giving that $F_f(F_f(x, y), z)$ satisfies condition (ii). Similarly, $F_f(x, F_f(y, z))$ does too. They both are congruent to $x + y + z \mod \deg 2$. Hence by uniqueness, they are equal. Consequently, F_f is the desired formal group law. □

Definition 5.4. A formal group law of the form F_f is called a relative Lubin-Tate formal group law.

The subsets of R which correspond via Υ to the morphisms of these group laws over the ring R have a nice description dependent on $\mathrm{N}_{k'/k}(f'(0))$ and $\mathrm{N}_{k'/k}(g'(0))$. We make this description precise.

Definition 5.5. If F_f and F_g are defined over $\mathcal{O}'$ and $a \in \Upsilon(\mathrm{Hom}_R(F_f, F_g))$, define $[a]_{f,g} = \Upsilon^{-1}(a)$. The notation $[a]_f$ will denote $[a]_{f,f}$.

Definition 5.6. Let $\pi_1, \pi_2 \in \mathcal{O}'$ such that $\nu(\pi_1) = \nu(\pi_2) = 1$. Set $A_{\pi_1,\pi_2} = \{a \in \mathcal{O}_{\hat{k}^{ur}} \mid a^{\phi-1} = \pi_1^{-1}\pi_2\}$

Proposition 5.7. *$\Upsilon(\mathrm{Hom}_R(F_f, F_g)) = A_{\pi_1,\pi_2} \cap R$ where $\pi_1 = f'(0)$ and $\pi_2 = g'(0)$.*

Proof. If $a \in A_{\pi_1,\pi_2} \cap R$, then by Proposition 5.2, a unique series $h \in R[[x]]$ exists such that $h \equiv ax \mod \deg 2$ and $g \circ h = h^{\phi} \circ f$. This is because on the linear terms the equality $\pi_2 ax = a^{\phi}\pi_1 x$ is satisfied. Now, $[a]_{F_f,F_g}$ is defined over Q and meets the same conditions uniquely. Therefore, $h = [a]_{F_f,F_g}$ so that $h \in \mathrm{Hom}_R(A, B)$.

Now given $h \in \mathrm{Hom}_R(F_f, F_g)$, we show $\Upsilon(h) \in A_{\pi_1,\pi_2}$. Note that over Q, $(h^{\phi})^{-1} \circ g \circ h$ satisfies properties (i) and (ii) of Proposition 5.2 with $L(x) = \pi_1 x$ and $[\pi_1]_f = f$ used for both of the other series in (ii). Therefore, by uniqueness, $(h^{\phi})^{-1} \circ g \circ h = f$. Equating the coefficients of x in this equality gives that $h'(0) \in A_{\pi_1,\pi_2}$.

□

Note that if $\mathrm{N}_{k'/k}\frac{\pi_2}{\pi_1} = 1$, Hilbert's Theorem 90 gives that $A_{\pi_1,\pi_2} \cap R$ is nonempty. More strongly from [3, 3.11], $\phi - 1$ is a surjection $\mathcal{O}^{\times}_{\hat{k}^{ur}} \to \mathcal{O}^{\times}_{\hat{k}^{ur}}$ so that A_{π_1,π_2} is never empty. Since $p^{\phi-1} = 1$, then $ap^m \in A_{\pi_1,\pi_2}$ for any $a \in A_{\pi_1,\pi_2}$ and $m \in \mathbb{Z}$. So in particular, if $A_{\pi_1,\pi_2} \cap R$ is nonempty, then $A_{\pi_1,\pi_2} \cap R^{\times}$ is nonempty.

Proposition 5.8. *Let $\xi, \xi' \in k^{\times}$ such that $\nu(\xi) = \nu(\xi') = d$. Two consequences of the above discussion are:*
(i) *If $f, g \in \mathfrak{F}_{\xi}$, then $F_f \simeq F_g$ over $\mathcal{O}'$.*
(ii) *$F_f \simeq F_g$ over $\mathcal{O}_{\hat{k}^{ur}}$ for $f \in \mathfrak{F}_{\xi}$, $g \in \mathfrak{F}_{\xi'}$.*

6. Torsion in Relative Lubin Tate Formal groups

Definition 6.1. A formal group is a group whose addition is given by a formal group law.

Example 6.2. Let E be an elliptic curve defined over L with Weierstrass model as given by (1). Let $\mathfrak{P}$ be a prime of L and $\nu_{\mathfrak{P}}$ denote $\mathfrak{P}$-adic valuation associated to the prime $\mathfrak{P}$. Denote by $L_{\mathfrak{P}}$ the completion of L with respect to $\mathfrak{P}$. If $\nu_{\mathfrak{P}}(g_1) > 0$ and $\nu_{\mathfrak{P}}(g_2) > 0$, then let R denote the valuation ring of $L_{\mathfrak{P}}$, we may define the formal group law as in Definition 3.3.

It is evident that $\hat{E}(a, b)$ converges if a and b lie in the maximal ideal $\mathcal{O}_M$ of any field M containing $L_{\mathfrak{P}}$. Also it is clear that $\hat{E}(a, b) \in \mathcal{O}_M$. Hence $\mathcal{O}_M$ is an abelian group with respect to $[+]_{\hat{E}}$.

Definition 6.3. Let A be a topological group. The A-valued points of the formal group law F, denoted $F(A)$, is the formal group $(A, [+]_F)$. The group $F(A)$ exists if $F(a, b)$ converges for all $a, b \in A$.

Example 6.4. The group described in Example 6.2 is denoted $\hat{E}(\mathcal{O}_M)$.

Let $\mathfrak{p}_{\mathbb{C}_p}$ denote the maximal ideal of $\mathcal{O}_{\mathbb{C}_p}$ and let $\xi, \xi' \in k'$ such that $\nu(\xi) = \nu(\xi') = d$. Suppose that $f \in \mathfrak{F}_\xi$ and $g \in \mathfrak{F}_{\xi'}$. Then for any $a \in A_{\pi_1,\pi_2}$, $[a]_{f,g}$ induces a homomorphism $[a]_{f,g} : F_f(\mathfrak{p}_{\mathbb{C}_p}) \to F_g(\mathfrak{p}_{\mathbb{C}_p})$. If $a \in \mathcal{O}^\times_{\hat{k}^{ur}}$, then $a^{-1} \in A_{\pi_1,\pi_2}$ so that $[a^{-1}]_{f,g}$ induces the inverse of the homomorphism induced by $[a]_{f,g}$.

We will use the notation $[a]_{f,g}$ to denote the induced map on $\mathfrak{p}_{\mathbb{C}_p}$-valued points. Then $\ker([a]_{f,g})$ will denote the kernel of the induced map.

If π is a uniformizer in $\mathfrak{p}$, $[a]_f = [u]_f \circ [\pi^n]_f$ for some $u \in \mathcal{O}^\times$ so that $[u]_f$ is an isomorphism. Further, since $[u]_f \circ [\pi^n]_f = [\pi^n]_f \circ [u]_f$ by uniqueness properties, $[u]_f$ induces a F_f-automorphism of $\ker[a]_f$. Consequently, $\ker[a]_f = \ker[b]_f$ for any $a, b \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$. Now we can make the following definition.

Definition 6.5. Define W_f^n to be $\ker[a]_f$ for any $a \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$.

Definition 6.6. Set $f^{(i)}$ to be $\phi^{i-1}(f) \circ ... \circ \phi(f) \circ f$.

Remark 6.7. Applying $f \circ F_f = F_f^\phi \circ f$ repeatedly, replacing f with $\phi^j(f)$ and F_f with $F_f^{\phi^j}$, we see that $f^{(i)} \in \mathrm{Hom}_{\mathcal{O}'}(F_f, F_{\phi^i(f)})$.

Lemma 6.8. *Set W_f^n to be* $\ker(f^{(n)})$. *Then: $W_f^n \subset W_f^{n+1}$*

Proof. Note that $f^{(n)} = [a]_{f,\phi^n(f)}$ for some $a \in \mathcal{O}'$. Choosing $b \in \mathcal{O}$ such that $\nu(a) = \nu(b)$, $[a]_{f,\phi(f)} = [ab^{-1}]_{f,\phi^n(f)} \circ [b]_f$ gives the equivalence since $[ab^{-1}]_{f,\phi^n(f)}$ is an isomorphism.

The second statement follows since $f^{(n+1)} = \phi^n(f) \circ f^{(n)}$.

□

We also note the following with regards to $f^{(n)}$: since F_f is defined over $\mathcal{O}'$, $F_f^{\phi^d} = F_f$. Also, the x coefficient of $f^{(d)}$ is $N_{k'/k}(\pi_1) = \xi$. Hence,

$$f^{(d)} = [\xi]_{f,f} = [\xi]_f \in \mathrm{End}(F_f).$$

Definition 6.9. $\widetilde{W_f^n} = W_f^n \setminus W_f^{n-1}$, $W_f = \cup_n W_f^n$.

If $f, g \in \mathfrak{F}_\xi$, $F_f \simeq F_g$ over $\mathcal{O}'$ gives that $k'(W_f^n)$ is independent of f. We can therefore make the following definitions.

Definition 6.10. $k_\xi^n = k'(W_f^n)$ and $k_\xi = k'(W_f)$.

The rest of this section summarizes basic properties of these extensions as given in [3, IV, V] and [5, I.1].

Any unit $u \in \mathcal{O}^\times$ induces an automorphism of W_f via the morphism $[u]_f$ that is valuation preserving. This automorphism is also induced by a Galois element $\sigma_u \in \mathrm{Gal}(k_\xi/k)$. The map $u \mapsto \sigma_u$ is bijective and independent of f.

In particular, we have the isomorphism $\kappa : \mathrm{Gal}(k_\xi/k) \to \mathcal{O}'^\times$ defined in the proposition below.

Proposition 6.11. *Let $\xi \in \mathcal{O}$ such that $\nu(\xi) = d$. Choose any $f \in \mathfrak{F}_\xi$. Then there exists a unique isomorphism $\kappa : \mathrm{Gal}(k_\xi/k) \to \mathcal{O}'^\times$ which is independent of f such that $\kappa(\sigma)$ is the unique element of $\mathcal{O}'^\times$ such that $[\kappa(\sigma)]_{f,\sigma(f)}(w) = \sigma(w)$ for all $w \in W_f^1$. If $\sigma \in \mathrm{Gal}(k_\xi/k')$, then $\kappa(\sigma) \in \mathcal{O}$ and $[\kappa(\sigma)]_f$ is defined over $\mathcal{O}$.*

Proof. See [3, IV, V] and [5, I.1] □

We also have the following:

Proposition 6.12. (1) $|W_f^n| = q^n$.
(2) k_ξ^n *is a totally ramified extension of* k' *of degree* $(q-1)q^{n-1}$.
(3) *Each element of* $\tilde{W}_f^n$ *is a uniformizer in* k_ξ^n.
(4) W_f *is an* $\mathcal{O}$*-module.*
(5) $\kappa(\mathrm{Gal}(k_\xi/k_\xi^n)) = 1 + \mathfrak{p}^n$.

Proof. See [3, IV, V] and [5, I.1] □

Example 6.13. Let $\hat{G}_m$ denote the multiplicative formal group law, which is given by $\hat{G}_m(x,y) = (1+x)(1+y)-1$. Then, $\hat{G}_m = F_f$ where $f(x) = (1+x)^p - 1$, $k = \mathbb{Q}_p$ and $k' = \mathbb{Q}_p$. Because $k' = k$, we call $\hat{G}_m$ an absolute Lubin Tate formal group law in contrast to calling it "relative." In this case, $W_f^n = \{\zeta - 1 \mid \zeta \in \mu_{p^n}\}$.

7. Coleman Power Series

Let k, k', and f be as before. Let $\mathcal{O} = \mathcal{O}_k$, $\mathcal{O}' = \mathcal{O}_{k'}$, and $\mathcal{O}'_n = \mathcal{O}_{k_\xi^n}$.

Proposition 7.1. *There exists a unique multiplicative operator*

$$\mathfrak{N}_f : \mathcal{O}'[[t]] \to \mathcal{O}'[[t]]$$

such that for all $h \in \mathcal{O}'[[t]]$,

$$\mathfrak{N}_f h \circ f = \prod_{\omega \in W_f^1} h(t[+]\omega).$$

Proof. Let $h \in \mathcal{O}'[[t]]$. Note that f has a formal composition inverse over k' so that $\mathfrak{N}_f$ is well-defined if $\mathfrak{N}_f h \in \mathcal{O}'[[t]]$. Let $g_0 = \prod_{\omega \in W_f^1} h(t[+]\omega)$. Then $g_0(x[+]w) = g_0(x)$ for $w \in W_f^1$. In particular, $g_0(0[+]w) = g_0(0) = g_0(w)$ so that all roots of f are roots of $g_0(x) - g_0(0)$. By the Weierstrass Preparation Theorem, there exists $g_1(t) \in \mathcal{O}'[[t]]$ such that $g_0(t) - g_0(0) = g_1(t) \cdot f(t)$. This implies $g_1(t[+]w) = g_1(t)$ for $w \in W_f^1$. We may then define $g_2(t) \in \mathcal{O}'[[t]]$ such that $g_1(t) - g_1(0) = g_2(t) \cdot f(t)$ and continue in this manner to produce:

$$g_0(t) = g_0(0) + g_1(0) \cdot f(t) + g_2(0) \cdot f^2(t) + \cdots .$$

Consequently, $\mathfrak{N}_f h = g_0 \circ f^{-1} \in \mathcal{O}'[[t]]$ as desired.
Multiplicativity follows easily from the formula given above for $\mathfrak{N}_f h \circ f$.
□

Definition 7.2. Because of multiplicativity, the operator $\mathfrak{N}_f$ extends to $\mathcal{O}'((t)) \to \mathcal{O}'((t))$. It is called the Coleman norm operator.

Proposition 7.3. *The operator* $\mathfrak{N}_f$ *satisfies the following:*
(i) $\mathfrak{N}_f h \equiv h^\phi \mod \mathfrak{p}'$
(ii) $\mathfrak{N}_{f^\phi} h = \mathfrak{N}_f^\phi h^{\phi^{-1}}$
(iii) Let $\mathfrak{N}_f^{(i)} = \mathfrak{N}_{\phi^{i-1}(f)} \circ \cdots \circ \mathfrak{N}_{\phi(f)} \circ \mathfrak{N}_f$, *Then*

$$(\mathfrak{N}_f^{(i)}) \circ f^{(i)}(t) = \prod_{w \in W_f^i} h(t[+]w).$$

(iv) If $h \in \mathcal{O}'[[t]]$ *and* $h \equiv 1 \mod (\mathfrak{p}')^i$ *($i \geq 1$), then* $\mathfrak{N}_f h \equiv 1 \mod (\mathfrak{p}')^{i+1}$

Proof. See ([5], I.2.1) □

Definition 7.4. Let $\mathcal{O}'_n = \mathcal{O}_{k_\xi^n}$.

The following result arises from the properties of Coleman's norm operator.

Proposition 7.5. *Given*

$$\beta = \{\beta_n\}_n \in \varprojlim_n (\mathcal{O}'_n)^\times$$

where the inverse limit is with respect to the maps $\mathrm{N}_{k_\xi^{n+1}/k_\xi^n}$ *and given*

$$\eta = \{\eta_n\}_n \in \varprojlim_n \tilde{W}^n_{\phi^n(f)},$$

there exists a unique power series $g_\beta \in \mathcal{O}'[[x]]$ *such that*

$$(g_\beta)^{\phi^{-n}}(\eta_n) = \beta_n \tag{8}$$

for all $n \geq 1$.

Proof. See ([5], I.2.2)

□

Definition 7.6. The power series g_β is called the Coleman power series associated to the pair (η, β).

Proposition 7.7. *Let* β *and* β' *be in*

$$\{\beta_n\}_n \in \varprojlim_n (\mathcal{O}'_n)^\times.$$

The following properties hold:

(i) $g_{\beta_1\beta_2} = g_{\beta_1} \cdot g_{\beta_2}$.
(ii) $\mathfrak{N} g_\beta = g_\beta^\phi$
(iii) If $v(\beta_0) = 0$, *then* $g_\beta(0)^{1-\phi^{-1}} = \beta_0$.
(iv) If $\sigma \in \mathrm{Gal}(k_\xi/k)$, *then* $g_{\sigma(\beta)} = g_\beta^\sigma \circ [\kappa(\sigma)]_{f,\sigma(f)}$.

Proof. See ([5], I.2.3) □

8. Measures Derived from Coleman Power Series

Let k, k', ξ, f, $\mathcal{O}_k$, $\mathcal{O}'$, and $\mathcal{O}'_n$ be as before. let $G = \mathrm{Gal}(k_\xi/k') \simeq \mathbb{Z}_p^\times$ and let $\mathcal{G} = \mathrm{Gal}(k_\xi/k)$. For this section, fix an isomorphism $\theta : \hat{G}_m \to F_f$. Let

$$\beta \in \varprojlim_n (\mathcal{O}'_n)^\times \text{ and } \omega \in \varprojlim_n \tilde{W}^n_{\phi^n(f)}.$$

We summarize some properties of distributions [5, I.3.1].

Definition 8.1. Let P be a profinite group and M and abelian group. We define the set of M-valued distributions on P, $\mathfrak{D}(P, M)$, to be the collection of finitely additive functions from the Boolean algebra of compact-open subsets of P to M.

If M is a bounded subset of $\mathbb{C}_p$, then elements of $\mathfrak{D}(P, M)$ are called p-adic measures. If M is in the closed unit disk of $\mathbb{C}_p$, then elements of $\mathfrak{D}(P, M)$ are called integral measures.

If M is a commutative ring, $\mathfrak{D}(P, M)$ is also a ring with $(\lambda \cdot \mu)(U) = \lambda(U) \cdot \mu(U)$ for $\mu, \lambda \in \mathfrak{D}(P, M)$ and $U \subset P$ ([5, I.3.1]).

In particular, if $\chi \in \mathrm{Hom}(P, \mathbb{C}_p^\times)$, then:

$$\int_P \chi d(\lambda\mu) = \int_P \chi d(\lambda) \cdot \int_P \chi d(\mu) \tag{9}$$

Definition 8.2. Let $S \subset \mathfrak{D}(P, M)$ be the multiplicative set of nonzero divisors. Define a psuedo-measure as an element $\mu/\lambda \in S^{-1}\mathfrak{D}(P, M)$. Then define:

$$\int_P \chi d(\mu/\lambda) = (\int_P \chi d\mu)/(\int_P \chi d\lambda)$$

for any $\chi \in \mathrm{Hom}(p, \mathbb{C}_p^\times)$.

If P is finite we have that $\mathfrak{D}(P, M) \simeq M[P]$ via the map $\lambda \mapsto \sum_{\sigma \in P} \lambda(\{\sigma\})\sigma$. If P is not finite,

$$\mathfrak{D}(P, M) = \varprojlim \mathfrak{D}(P/H, M)$$

where $[P : H] < \infty$.

We will turn our attention to the case when $P = G \simeq \mathbb{Z}_p^\times$.

Proposition 8.3. *Let R be the valuation ring of a complete extension of $\mathbb{Q}_p$. Given a power series $h(s) \in R[[s]]$, there exists an R-valued measure μ on $\mathbb{Z}_p$ such that*

$$h(s) = \int_{\mathbb{Z}_p} (1+s)^\alpha d\mu(\alpha).$$

Proof. Let $n \geq 1$. Write

$$h(s) \mod ((s+1)^{p^n} - 1) = \sum_{i=0}^{p^n - 1} a_{n,i}(1+s)^i.$$

Define $\mu_n : \mathbb{Z}/p^n\mathbb{Z} \to R$ by $\mu_n(i) = a_{n,i}$. If $i \equiv j \mod p^n$, then $(s+1)^i \equiv (s+1)^j \mod (s+1)^{p^n} - 1$. Consequently,

$$\sum_{\substack{0 \leq i \leq p^{n+1}-1 \\ i \equiv j \mod P^n}} a_{n+1,i} = a_{n,j}$$

which is the distribution relation:

$$\sum_{\substack{0 \leq i \leq p^{n+1}-1 \\ i \equiv j \mod P^n}} \mu_{n+1}(i) = \mu_n(j).$$

Since R is a bounded set, this distribution determines a bounded measure.

□

Definition 8.4. Define

$$a_\beta(s) = (\log g_\beta) \circ \theta(s)$$

and

$$\widetilde{a_\beta}(s) = a_\beta(s) - \frac{1}{p} \sum_{w \in W_f^1} (\log g_\beta) \circ (\theta(s)[+]w).$$

Proposition 8.5. *The series $\widetilde{a_\beta}$ lies in $\mathcal{O}_{\hat{k}^{ur}}[[s]]$.*

Proof. Let $\mathfrak{p}'$ denote the valuation ideal of k'. We make the following calculation:

$$g_\beta^p \equiv g_\beta \circ f \mod \mathfrak{p}'$$

$$g_\beta^p \equiv \mathfrak{N} g_\beta \circ f \mod \mathfrak{p}' \text{ (by proposition 7.7 (ii))}$$

$$g_\beta^p \equiv \prod_{w \in W_f^1} g_\beta(\theta[+]w) \mod \mathfrak{p}' \text{ (by the definition of } \mathfrak{N})$$

$$p \log g_\beta \equiv \sum_{w \in W_f^1} \log g_\beta(\theta[+]w) \mod \mathfrak{p}' \text{ (composing power series)}$$

Hence the expression

$$\log g_\beta - \frac{1}{p} \sum_{w \in W_f^1} \log g_\beta(\theta[+]w)$$

has coefficients which are p-integral. □

Definition 8.6. Define μ_β to be the $\mathcal{O}_{\hat{k}^{ur}}$-valued measure on $\mathbb{Z}_p$ given by the power series $\widetilde{a_\beta}$.

Proposition 8.7. *The measure μ_β is supported on $\mathbb{Z}_p^\times$.*

Proof. Write $a'_\beta = a_\beta \mod ((s+1)^{p^n} - 1) = \sum_{i=0}^{p^n-1} a_i (s+1)^i$. Then:

$$\frac{1}{p} \sum_{\zeta \in \mu_p} a'_\beta(s[+]\zeta - 1) = \frac{1}{p} \sum_{i=1}^{p^n-1} \sum_{j=0}^{p-1} a_i((s+1)\zeta^j - 1 + 1)^i = \sum_{p|i} a_i (s+1)^i.$$

So,

$$\widetilde{a_\beta} \mod ((s+1)^{p^n} - 1) = \sum_{i=1}^{p^n-1} a_i (s+1)^i - \frac{1}{p} \sum_{\zeta \in \mu_p} a'_\beta(s[+]\zeta - 1) = \sum_{p \nmid i} a_i (s+1)^i.$$

□

We consider μ_β as a measure on G via the isomorphism $\kappa : G \to k^\times \simeq \mathbb{Z}_p^\times$.

Proposition 8.8. *Let $\sigma \in G$ and let be a subset of G. Then $\mu_{\sigma(\beta)}(\sigma U) = \mu_\beta(U)$.*

Proof. This result is a consequence of $g_{\sigma(\beta)} = g_\beta^\sigma \circ [\kappa(\sigma)]$.

□

Corollary 8.9. *The measure μ_β extends to $\mathcal{G}$ as follows: Let $\sigma \in \mathcal{G}$. If U is contained in the coset σG, then define $\mu_\beta(U) = \mu_\beta(\sigma^{-1}U)$.*

Recall the definition of the additive formal group $\hat{G}_a(x,y) = x + y$ and the multiplicative formal group $\hat{G}_m(x,y) = (x+1)(y+1) - 1$. Fix an isomorphism $\theta : \hat{G}_m \to F_f$. Then, by uniqueness of $\lambda_{\hat{G}_a}$,

$$\theta'(0)^{-1} \lambda_{F_f} \circ \theta = \lambda_{\hat{G}_a} = \log(1+s)$$

where $\log(1+s)$ is considered as its Taylor expansion about $s = 0$. So

$$\frac{d}{ds}\theta(s) = \theta'(0)/((1+s)\frac{d}{dt}\lambda_{F_f}(t)).$$

This motivates the following:

Definition 8.10. Define

$$\tilde{\mathcal{D}} = \frac{\theta'(0)}{\lambda'_{F_f}(t)} \frac{d}{dt}.$$

Considering θ as a function of s, this is equivalently from the discussion above:

$$\mathcal{D} = (1+s)\frac{d}{ds}.$$

Proposition 8.11. *The "Coates-Wiles homomorphism" integral is given as* $\int_G \kappa(\sigma)^k d\mu_\beta(\sigma)$ *and is equal to* $\mathcal{D}^k(\widetilde{a_\beta})(0)$.

Proof. When $k = 1$,

$$\mathcal{D}(\widetilde{a_\beta})(0) = \mathcal{D}\int_G (1+s)^{\kappa(\sigma)} d\mu(\sigma)\Big|_{s=0} = \int_G \mathcal{D}(1+s)^{\kappa(\sigma)} d\mu(\sigma)\Big|_{s=0} =$$

$$= \int_G (1+s)\frac{d}{ds}(1+s)^{\kappa(\sigma)} d\mu\Big|_{s=0} = \int_G \kappa(\sigma)(1+s)^{\kappa(\sigma)} d\mu\Big|_{s=0}.$$

An identical argument gives the inductive step. □

Proposition 8.12. *The proof of the last proposition gave the following identity:* $\mathcal{D}^k\widetilde{a_\beta}(s) = \int_{\mathbb{Z}_p} \alpha^k (1+s)^\alpha d\mu_\beta(\alpha)$

Proposition 8.13. *Let* $G_n = \mathrm{Gal}(k_\xi/k_\xi^n) = \kappa^{-1}(1+p^n\mathbb{Z}_p)$ *for* $n \geq 1$. *Then:*

$$\mu_\beta(G_n) = \frac{1}{p^n}\sum_{j=0}^{p^n-1} a_\beta(\zeta_{p^n}^j - 1)\cdot\zeta_{p^n}^{-j}.$$

Proof. Write $a'_\beta = a_\beta \mod ((s+1)^{p^n} - 1) = \sum_{i=0}^{p^n-1} a_i(s+1)^i$. Then,

$$a'_\beta = \sum_{p\nmid i} a_i(s+1)^i + \sum_{p|i} a_i(s+1)^i.$$

where $\widetilde{a_\beta} \mod ((s+1)^{p^n}-1) = \sum_{p\nmid i} a_i(s+1)^i$. We prove the proposition replacing a_β with $\widetilde{a_\beta}$ after realizing the following calculation:

$$\frac{1}{p^n}\sum_{j=0}^{p^n-1}\sum_{p|i} a_i(\zeta_{p^n}^j - 1 + 1)^i\cdot\zeta_{p^n}^{-j} =$$

$$\sum_{p|i}\sum_{j=0}^{p^n-1} a_i(\zeta_{p^n}^j)^i\cdot\zeta_{p^n}^{-j} = \sum_{p|i}\sum_{j=0}^{p^n-1} a_i\cdot\zeta_{p^n}^i = 0.$$

By the definition of μ_β, $\widetilde{a_\beta}(\zeta_{p^n}^j - 1) = \int_{\mathbb{Z}_p}\zeta_{p^n}^{j\alpha} d\mu_\beta(\alpha)$ so that

$$\sum_{j=0}^{p^n-1}\widetilde{a_\beta}(\zeta_{p^n}^j-1)\cdot\zeta_{p^n}^{-j} = \int_{\mathbb{Z}_p}\sum_{j=0}^{p^n-1}\zeta_{p^n}^{j(\alpha-1)} d\mu_\beta(\alpha)$$

$$= p^n\int_{\alpha\equiv 1 \mod p^n} d\mu_\beta(\alpha) = p^n\mu_\beta(G_n).$$

□

Proposition 8.14. *With G_n as before:*

$$\mathcal{D}\widetilde{a_\beta}(0) = \frac{1}{p^n}\sum_{j=0}^{p^n-1} \mathcal{D}^k(a_\beta)(\zeta_{p^n}^j - 1)\cdot\zeta_{p^n}^{-j}.$$

Proof. Proceed as in the proof of proposition 8.13 replacing a_i by $i^k a_i$ with the variation

$$\begin{aligned}\sum_{j=0}^{p^n-1} \mathcal{D}^k\widetilde{a_\beta}(\zeta_{p^n}^j - 1)\cdot\zeta_{p^n}^{-j} &= \int_{\mathbb{Z}_p} \alpha^k \sum_{j=0}^{p^n-1} \zeta_{p^n}^{j(\alpha-1)} d\mu_\beta(\alpha)\\ &= p^n \int_{\alpha\equiv 1 \mod p^n} \alpha^k d\mu_\beta(\alpha) = p^n\mathcal{D}^k\widetilde{a_\beta}(0).\end{aligned}$$

□

9. Morphisms of Elliptic Curves and Complex Multiplication

Let E_1 and E_2 be an elliptic curves with Weierstrass models as given in (1). We define $\mathrm{Hom}(E_1, E_2)$, the set of isogenies from A to B, to be the set of rational maps that respect $+_{E_1}$ and $+_{E_2}$. The holomorphic group isomorphisms Ψ_{E_1} and Ψ_{E_2} allow us to identify $\mathrm{Hom}(E_1, E_2)$ with $\mathrm{Hom}_{Ab}(\mathbb{C}/\Lambda_{E_1}, \mathbb{C}/\Lambda_{E_2})$ [8, VI.4]. Let

$$A_{E_1,E_2} = \{a \in \mathbb{C} \mid a\Lambda_{E_1} \subset \Lambda_{E_2}\}. \tag{10}$$

As abelian groups, [8, VI.4.1] gives the following:

$$\mathrm{Hom}(E_1, E_2) \simeq \mathrm{Hom}_{Ab}(\mathbb{C}/\Lambda_{E_1}, \mathbb{C}/\Lambda_{E_2}) \simeq A_{E_1,E_2}. \tag{11}$$

Given $a \in A_{E_1,E_2}$, define $[a]_{E_1,E_2} \in \mathrm{Hom}(E_1, E_2)$ by the identification made in (11). The association $a \mapsto [a]_{E_1,E_2}$ is illustrated by the following commutative diagram:

$$\begin{array}{ccc} \mathbb{C}/\Lambda_{E_1} & \xrightarrow{a\cdot} & \mathbb{C}/\Lambda_{E_2} \\ \downarrow{\scriptstyle \Psi_{E_1}^{-1}} & & \downarrow{\scriptstyle \Psi_{E_2}^{-1}} \\ E_1 & \xrightarrow{[a]_{E_1,E_2}} & E_2 \end{array}$$

If $E_1 = E_2$, we use the notation $[a]_{E_1}$.

Definition 9.1. We define the degree of $[a]_{E_1,E_2}$ to be $|\ker[a]_{E_1,E_2}| = |a^{-1}\Lambda_{E_2}/\Lambda_{E_1}|$. This agrees with the more general definition of the degree of an isogeny [8, III.4.10].

Let E be an elliptic curve with Weierstrass model as given in (1). Let K be an imaginary quadratic extension of $\mathbb{Q}$. For an integral ideal $\mathfrak{f}$ of K, let $K(\mathfrak{f})$ denote the ray class field of K of modulus $\mathfrak{f}$.

Definition 9.2. E is said to admit complex multiplication by $\mathcal{O}_K$ if $A_{E,E} = \mathcal{O}_K$.

If E admits complex multiplication by $\mathcal{O}_K$, it can be shown that the minimal field of definition for E is the Hilbert class field of K denoted $K(1)$ as the ray class field of K of modulus 1 [9, II.4.3].

If E admits complex multiplication by $\mathcal{O}_K$ then Λ_E is of the form $\mathfrak{a}\Omega$ for an integral ideal $\mathfrak{a}$ of K and a complex number $\Omega \in \mathbb{C}$. This is seen as follows. If $\Lambda_E = w_1\mathbb{Z} + w_2\mathbb{Z}$ and $\alpha \in \mathcal{O}_K$, then $\alpha w_1 = aw_1 + bw_2$ where $a, b \in \mathbb{Z}$. Then,

$(\alpha - a)w_1/b = \omega_2$. Consequently, $b/w_1\Lambda \subset \mathcal{O}_K$. An $\mathcal{O}_K$-submodule of $\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$.

Let $\mathfrak{a}$ be an integral ideal of K. We define:

Definition 9.3.

$$E[\mathfrak{a}] = \{T \in E \mid [a]_E(T) = O \text{ for all } a \in \mathfrak{a}\}.$$

By (11), $|E[\mathfrak{a}]| = |\mathfrak{a}^{-1}\Lambda_E/\Lambda_E|$.

Definition 9.4. Also define $E_{\text{tors}} = \cup_{\mathfrak{a}} E[\mathfrak{a}]$ where the union is over all integral ideals of K.

We now fix an elliptic curve E, an imaginary quadratic extension K of $\mathbb{Q}$, and an integral ideal $\mathfrak{f}$ of K. We assume that E admits complex multiplication by $\mathcal{O}_K$, E is defined over $L = K(\mathfrak{f})$, and that $L(E_{\text{tors}})/K$ is abelian.

Let $\mathrm{I}_K^{\mathfrak{f}}$ denote the set of fractional ideals of K relatively prime to $\mathfrak{f}$. For a fractional ideal $\mathfrak{b}$, let $\sigma_{\mathfrak{b}}$ denote the Artin symbol $(\mathfrak{b}, K^{ab}/K)$. Let $\mathbb{I}_K$ denote the idele group of K. For $s \in \mathbb{I}_K$, let $[s, K]$ denote the reciprocity symbol for s. Let (s) denote the ideal $\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(s_{\mathfrak{p}})}$ where the product is over all primes in K and $\nu_{\mathfrak{p}}$ is the valuation at $\mathfrak{p}$. (The expression $\nu_{\mathfrak{p}}(s_{\mathfrak{p}})$ is nonzero at only finitely many primes $\mathfrak{p}$.)

We have the identification $K/\mathfrak{a} \simeq \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}$ where $\mathfrak{p}$ ranges through all the prime ideals of K [9, II.8.1]. With this identification, we define multiplication of $K/\mathfrak{a}$ by $s \in \mathbb{I}_K$ as $(t_{\mathfrak{p}})_{\mathfrak{p}} \mapsto (s_{\mathfrak{p}} t_{\mathfrak{p}})_{\mathfrak{p}}$ for $(t_{\mathfrak{p}})_{\mathfrak{p}} \in \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}$.

We may now state the following major results for elliptic curves admitting complex multiplication.

Proposition 9.5. *The Main Theorem of Complex Multiplication*

Let E be as above. Fix an integral ideal $\mathfrak{a}$ of K and complex number Ω such that $\Lambda_E = \mathfrak{a}\Omega$. Let σ be an automorphism of $\mathbb{C}$ fixing K. Choose $s \in \mathbb{I}_K$ such that $[s, K] = \sigma|_{K^{ab}}$. Then there exists a unique holomorphic isomorphism $\Xi : \mathbb{C}/s^{-1}\Lambda_E \to E^{\sigma}(\mathbb{C})$ such that the following diagram commutes:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{s^{-1}} & K/s^{-1}\mathfrak{a} \\ \downarrow{\scriptstyle \Omega\Psi_E^{-1}} & & \downarrow{\scriptstyle \Omega\Xi} \\ E(\mathbb{C}) & \xrightarrow{\sigma} & E^{\sigma}(\mathbb{C}) \end{array}$$

Proof. See [9, II.8.2] □

Remark 9.6. We note that

$$\Psi_E(E_{\text{tors}}) = \bigcup_{\mathfrak{b}} \mathfrak{b}^{-1}\mathfrak{a}\Omega/\mathfrak{a}\Omega = K\Omega/\mathfrak{a}\Omega$$

where the union is over all fractional ideals of K.

In the book of de Shalit [5, II.1.5], the theorem of complex multiplication takes on the following form:

Proposition 9.7. *The Main Theorem of Complex Multiplication*

Let E be as above. We recall that $L = K(\mathfrak{f})$. Then given a fractional ideal $\mathfrak{c}$ of K such that $(\mathfrak{f}, \mathfrak{c}) = 1$, there exists a unique $\alpha \in L^{\times}$ such that the following diagram commutes for any integral ideal $\mathfrak{b}$ such that $(\mathfrak{b}, \mathfrak{c}) = 1$:

$$\begin{array}{ccc} \mathfrak{b}^{-1}\Lambda_E/\Lambda_E & \xrightarrow{\alpha\cdot} & \mathfrak{b}^{-1}(\alpha\mathfrak{c}^{-1}\Lambda_E)/(\alpha\mathfrak{c}^{-1}\Lambda_E) \\ \downarrow \Psi_E^{-1} & & \downarrow \Psi_{E^{\sigma_\mathfrak{c}}}^{-1} \\ E[\mathfrak{b}] & \xrightarrow{\sigma_\mathfrak{c}} & E^{\sigma_\mathfrak{c}}[\mathfrak{b}] \end{array}$$

where $E^{\sigma_\mathfrak{c}} \simeq \mathbb{C}/\alpha\mathfrak{c}^{-1}\Lambda_E$, $\deg([\alpha]_E) = \mathrm{N}_{K/\mathbb{Q}}\mathfrak{c}$, *and* $[\alpha]_E$ *is defined as a rational map in coordinates* x *and* y *over* L.

Definition 9.8. Define $\kappa_0 : \mathrm{I}_K^\mathfrak{f} \to \mathbb{C}^\times$ to be given by the correspondence $\mathfrak{c} \mapsto \alpha$ of Proposition 9.7.

Remark 9.9. In [5], κ_0 is notated as Λ.

Proposition 9.10. κ_0 *satisfies the cocycle condition:* $\kappa_0(\mathfrak{ab}) = \kappa_0(\mathfrak{a})^{\sigma_\mathfrak{b}}\kappa_0(\mathfrak{b}) = \kappa_0(\mathfrak{b})^{\sigma_\mathfrak{a}}\kappa_0(\mathfrak{a})$

Proof. We give another description of the map κ_0. Let ω_E be the invariant differential associated with E as in the description of (2). Let $\mathfrak{a}$ be a fractional ideal of K and let $P \in E(\mathbb{C})$. Let O_E and $O_{E^{\sigma_\mathfrak{a}}}$ denote the points at infinity respectively of E and $E^{\sigma_\mathfrak{a}}$. Denote $[\kappa_0(\mathfrak{a})]_{E,E^{\sigma_\mathfrak{a}}}$ by $\gamma_\mathfrak{a}$. The rational map $\gamma_\mathfrak{a}$ induces the pull-back map $\gamma_\mathfrak{a}^* : \Omega_{E^{\sigma_\mathfrak{a}}} \to \Omega_E$ where $\Omega_{E^{\sigma_\mathfrak{a}}}$ and Ω_E denote the spaces of meromorphic differential 1-forms on $E^{\sigma_\mathfrak{a}}$ and E respectively. Let δ represent any path from O_E to P. Then $\gamma \circ \delta$ is a path from $O_{E^{\sigma_\mathfrak{a}}}$ to $P^{\sigma_\mathfrak{a}}$

Recall the description of the map Ψ_E. The the map $\mathbb{C}/\Lambda_E \to \mathbb{C}/\Lambda_{E^{\sigma_\mathfrak{p}}}$ given by multiplication by $\kappa_0(\mathfrak{p})$ may be described as:

$$\int_\delta \omega_E \mod \Lambda_E \mapsto \int_{\gamma_\mathfrak{a}(\delta)} \omega_{E^{\sigma_\mathfrak{a}}} \mod \Lambda_{E^{\sigma_\mathfrak{a}}} = \int_\delta \gamma_\mathfrak{a}^*(\omega_{E^{\sigma_\mathfrak{a}}}) \mod \Lambda_E. \tag{12}$$

Since $\omega_{E^{\sigma_\mathfrak{a}}}$ is an invariant differential, by the proof of [8, III.5.6], $a\omega_E = \gamma_\mathfrak{a}^*(\omega_{E^{\sigma_\mathfrak{a}}})$ for some $a \in L$. By (12), $a = \kappa_0(\mathfrak{a})$.

So

$$\kappa_0(\mathfrak{a})\omega_E = \gamma_\mathfrak{a}^*(\omega_{E^{\sigma_\mathfrak{a}}}). \tag{13}$$

For an integral ideal $\mathfrak{c}$ of K, let $x_\mathfrak{c}$ and $y_\mathfrak{c}$ denote the x and y coordinates of $E^{\sigma_\mathfrak{c}}$. Notice that $x^{\sigma_\mathfrak{c}} = x_\mathfrak{c}$ and $y^{\sigma_\mathfrak{c}} = y_\mathfrak{c}$. Recall the standard differential $\omega_E = -2dx/y$. Since $\omega_{E^{\sigma_\mathfrak{c}}} = -2dx^{\sigma_\mathfrak{c}}/y^{\sigma_\mathfrak{c}}$, we write $\omega_{E^{\sigma_\mathfrak{c}}} = \omega_E^{\sigma_\mathfrak{c}}$.

Then since $\gamma^*(\omega_{E^{\sigma_\mathfrak{a}}})) = -2dx^{\sigma_\mathfrak{a}} \circ \gamma_\mathfrak{a}/y^{\sigma_\mathfrak{a}} \circ \gamma_\mathfrak{a}$, we may write

$$\gamma^*(\omega_{E^{\sigma_\mathfrak{a}}})) = \omega_E^{\sigma_\mathfrak{a}} \circ \gamma_\mathfrak{a} = \kappa_0(\mathfrak{a})\omega_E \tag{14}$$

Let $\gamma_{\mathfrak{a},\mathfrak{b}}$ denote the map $[\kappa_0(\mathfrak{b})]_{E^{\sigma_\mathfrak{a}},E^{\sigma_\mathfrak{a}\mathfrak{b}}}$.

The maps $\gamma_{\mathfrak{a},\mathfrak{b}}$ and $\gamma_\mathfrak{b}^{\sigma_\mathfrak{a}}$ both satisfy the uniqueness property of the Main Theorem of Complex Multiplication and so represent the same isogeny. Likewise, $\gamma_{\mathfrak{ab}} = \gamma_{\mathfrak{a},\mathfrak{b}} \circ \gamma_\mathfrak{a}$.

Then,

$$\kappa_0(\mathfrak{ab})\omega_E = \omega_E^{\sigma_{\mathfrak{a}\mathfrak{b}}} \circ \gamma_{\mathfrak{a},\mathfrak{b}} \circ \gamma_\mathfrak{a} = (\omega_E^{\sigma_\mathfrak{b}})^{\sigma_\mathfrak{a}} \circ \gamma_\mathfrak{b}^{\sigma_\mathfrak{a}} \circ \gamma_\mathfrak{a} = (\omega_E^{\sigma_\mathfrak{b}} \circ \gamma_\mathfrak{b})^{\sigma_\mathfrak{a}} \circ \gamma_\mathfrak{a} = \kappa_0(\mathfrak{b})^{\sigma_\mathfrak{a}}\omega_E^{\sigma_\mathfrak{a}} \circ \gamma_\mathfrak{a} = \kappa_0(\mathfrak{b})^{\sigma_\mathfrak{a}}\kappa_0(\mathfrak{a})\omega_E.$$

□

Definition 9.11. For a number field M, let $P_M^\mathfrak{m}$ denote all principal fractional ideals $\mathfrak{R} = (a)$ of M such that $a \equiv 1 \mod \mathfrak{m}$.

It can be checked that κ_0 has the property that if $\mathfrak{c} \in P_K^{\mathfrak{f}}$ then $\kappa_0(\mathfrak{c}) \in K^\times$, $\mathfrak{c} = (\kappa_0(\mathfrak{c}))$ and $\kappa_0(\mathfrak{c}) \equiv 1 \mod \mathfrak{f}$.

This motivates the following definition:

Definition 9.12. Let $\mathfrak{m}$ be an integral ideal of K. A grossencharacter ψ of type A_0 of conductor $\mathfrak{m}$ over the field M is a homomorphism $\mathrm{I}_M^{\mathfrak{m}} \to \bar{\mathbb{Q}}^\times$ such that there exists a unique $\gamma \in \mathbb{Z}[\mathrm{Gal}(M/\mathbb{Q})]$, called the infinity type of ψ, such that if $\mathfrak{R} \in P_K^{\mathfrak{m}}$, then $\psi(\mathfrak{R}) = \alpha^\gamma$ for some $\alpha \in M^\times$ such that $\mathfrak{R} = (\alpha)$ and $\alpha \equiv 1 \mod \mathfrak{m}$. The ideal $\mathfrak{m}$ is maximal with respect to this property. If M is an imaginary quadratic extension, the infinity type of ψ may be denoted (k, j) where $\gamma = k + j\tau$, τ denoting complex conjugation.

Remark 9.13. We will use the word grossencharacter to mean a grossencharacter of type A_0.

With this definition, we may state a weakened form of the Main Theorem of Complex Multiplication [5, II.1.3]. It is weaker because it considers the action of $\sigma \in \mathrm{Gal}(L^{ab}/L)$ in contrast to $\mathrm{Gal}(K^{ab}/K)$.

Proposition 9.14. *Weak Form of Complex Multiplication*

Let E be as above. There exists a unique grossencharacter $\psi_{E/L}$ of L of conductor $\mathfrak{f}\mathcal{O}_L$ such that the following diagram commutes for any fractional ideal $\mathfrak{R}$ of L such that $(\mathfrak{R}, \mathfrak{f}\mathcal{O}_L) = 1$ and $\mathfrak{r} = \mathrm{N}_{L/K}\mathfrak{R}$ and any fractional ideal $\mathfrak{b}$ of K such that $(\mathfrak{b}, \mathfrak{f}) = 1$ and $(\mathfrak{b}\mathcal{O}_L, \mathfrak{R}) = 1$.

$$\begin{array}{ccc} \mathfrak{b}^{-1}\Lambda_E/\Lambda_E & \xrightarrow{\psi_{E/L}(\mathfrak{R})\cdot} & \mathfrak{b}^{-1}(\psi_{E/L}(\mathfrak{R})\mathfrak{r}^{-1}\Lambda_E)/(\psi_{E/L}(\mathfrak{R})\mathfrak{r}^{-1}\Lambda_E) \\ \downarrow \Psi_E^{-1} & & \downarrow \Psi_{E^{\sigma_\mathfrak{R}}}^{-1} \\ E[\mathfrak{b}] & \xrightarrow{\sigma_\mathfrak{R}} & E^{\sigma_\mathfrak{R}}[\mathfrak{b}] \end{array}$$

Notation: $\sigma_\mathfrak{R} = (\mathfrak{R}, L^{ab}/L)$.

Because $L(E_{\mathrm{tors}})/K$ is assumed to be abelian, we have the following:

Proposition 9.15. *Let E be as above. There exists a grossencharacter ϕ of K of type $(1, 0)$ such that $\psi_{E/L} = \phi \circ \mathrm{N}_{L/K}$.*

Proof. [7, 7.44] □

Remark 9.16. Let $\mathfrak{R}$ be an ideal of L. Since $(\mathfrak{R}, L^{ab}/L)|_{K^{ab}} = (\mathrm{N}_{L/K}\mathfrak{R}, K^{ab}/K)$, if $\mathfrak{a} \in P_K^{\mathfrak{f}}$, $\kappa_0(\mathfrak{a}) = \phi(\mathfrak{a})$ for any choice of ϕ in proposition 9.15 for $\mathfrak{a} \in P_K^{\mathfrak{f}}$.

Fix a grossencharacter ϕ of K as given in proposition 9.15.

Lemma 9.17. *$E[\mathfrak{a}] \simeq \mathfrak{a}^{-1}\Lambda/\Lambda \simeq \mathcal{O}_K/\mathfrak{a}$ as $\mathcal{O}_K/\mathfrak{a}$-modules.*

Proof. See ([9], II.1.4). □

Lemma 9.18. *Let $(\mathfrak{a}, \mathfrak{f}) = 1$. Then $\mathrm{Gal}(L(E[\mathfrak{a}])/L)$ is isomorphic to a subquotient of $(\mathcal{O}_K/\mathfrak{a})^\times$.*

Proof. Let $\mathfrak{b}$ be an integral ideal of K such that $\sigma_\mathfrak{b}|_{L(E[\mathfrak{a}])} = 1$. From Lemma 9.17, $\kappa_0(\mathfrak{b}) \cdot \mathfrak{a}^{-1}\Lambda/\Lambda \simeq \kappa_0(\mathfrak{b}) \cdot \mathcal{O}_K/\mathfrak{a}$. Since $\kappa_0(\mathfrak{b})$ acts trivially on $E[\mathfrak{a}]$, $\kappa_0(\mathfrak{b}) \cdot \mathcal{O}_K/\mathfrak{a} \simeq \mathcal{O}_K/\mathfrak{a}$ as $\mathcal{O}_K$-modules. Hence, $\kappa_0(\mathfrak{b}) \equiv 1 \mod \mathfrak{a}$. Hence, we may define a map $\varrho : \mathrm{Gal}(L(E[\mathfrak{a}])/L) \to (\mathcal{O}_K/\mathfrak{a})^\times$ by $\sigma \mapsto \kappa_0(\mathfrak{b})$ for any $\mathfrak{b}$ such that $\sigma = \sigma_\mathfrak{b}|_{L(E[\mathfrak{a}])}$. By Proposition 9.15, ϱ is a multiplicative homomorphism. □

Let $\mathfrak{g}_f, \mathfrak{g}_\infty$ denote the nonarchimedean and archimedean parts of a modulus $\mathfrak{g}$ respectively. By class field theory, we have

$$K_\mathfrak{g}/K_{\mathfrak{g},1} \simeq (\mathcal{O}_K/\mathfrak{g}_f)^\times \times \prod_{i=1}^{r} \langle -1 \rangle$$

where r is the number of real places dividing $\mathfrak{g}_\infty$ and we also have the following exact sequence:

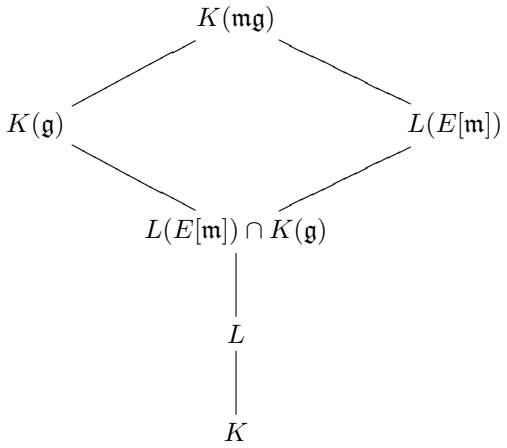
$$1 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap K_{\mathfrak{g},1}) \to K_\mathfrak{g}/K_{\mathfrak{g},1} \to \mathrm{CL}_K^\mathfrak{g} \to \mathrm{CL}_K \to 0.$$

Define $w_\mathfrak{g} = |\mu(K) \cap K_{\mathfrak{g},1}|$. Suppose that $w_\mathfrak{g} = 1$. Since $K/\mathbb{Q}$ is an imaginary quadratic extension, Dirichlet's unit theorem gives us that $\mathcal{O}_K^\times = \mu(K)$. Hence the sequence becomes:

$$1 \to \mu(K) \to (\mathcal{O}_K/\mathfrak{g})^\times \to \mathrm{CL}_K^\mathfrak{g} \to \mathrm{CL}_K \to 0. \tag{15}$$

Proposition 9.19. *Suppose that $\mathfrak{f} \mid \mathfrak{g}$, $w_\mathfrak{g} = 1$, and $(\mathfrak{m}, \mathfrak{g}) = 1$. Then, $L(E[\mathfrak{m}])$ and $L(E[\mathfrak{g}])$ are linearly disjoint over L and $\mathrm{Gal}(L(E[\mathfrak{m}])/L) \simeq (\mathcal{O}_K/\mathfrak{m})^\times$.*

Proof. We are considering the following diagram:



Note that $w_{\mathfrak{mg}} = 1$. Then using equation (15) for $\mathfrak{mg}$ and $\mathfrak{g}$ and comparing group indices we obtain:

$$[K(\mathfrak{mg}) : K(\mathfrak{g})] = |\mathrm{CL}_K^{\mathfrak{mg}}/CL_K^\mathfrak{g}| = |(\mathcal{O}_K/\mathfrak{mg})^\times/(\mathcal{O}_K/\mathfrak{g})^\times|.$$

Since $(\mathfrak{m}, \mathfrak{g}) = 1$, this equals $|(\mathcal{O}_K/\mathfrak{m})^\times|$.

By Lemma 9.18, $|\mathrm{Gal}(L(E[\mathfrak{m}])/L)| \leq |(\mathcal{O}_K/\mathfrak{m})^\times|$ and so by the Galois correspondence $|(\mathcal{O}_K/\mathfrak{m})^\times| = |\mathrm{Gal}(L(E[\mathfrak{m}])/K(\mathfrak{g}) \cap L(E[\mathfrak{m}]))|$. Thus,

$$|(\mathcal{O}_K/\mathfrak{m})^\times| = |\mathrm{Gal}(L(E[\mathfrak{m}])/K(\mathfrak{g}) \cap L(E[\mathfrak{m}]))| \leq$$

$$|\mathrm{Gal}(L(E[\mathfrak{m}])/L)| \leq |(\mathcal{O}_K/\mathfrak{m})^\times|.$$

Hence, $L = K(\mathfrak{g}) \cap L(E[\mathfrak{m}])$ thus completing the argument. □

Corollary 9.20. *Let $\mathfrak{g}$ be an integral ideal of K such that $\mathfrak{f} \mid \mathfrak{g}$. Then $L(E[\mathfrak{g}]) = K(\mathfrak{g})$.*

Remark 9.21. An elliptic curve E defined over $L = K(\mathfrak{f})$ where $w_{\mathfrak{f}} = 1$ that has complex multiplication by $\mathcal{O}_K$, such that $L(E_{\text{tors}})/K$ is abelian exists by [5, II.1.4].

10. Good Reduction

Fix E as in the previous section with $w_g = 1$. We will assume E is of this form for the remainder of the summary.

Definition 10.1. Suppose that E is defined over a local field M with valuation ν and valuation ring R. A minimal Weierstrass model $y^2 = 4x^3 - g_2x - g_3$ for E over M is one such that $\nu(\Delta_E)$ is minimized subject to the conditions $g_2, g_3 \in R$.

Recall that the model may be altered by a change $(g_2, g_3) \mapsto (u^4g_2, u^6g_3)$ with $u \in M^\times$. This gives that the condition in the above definition will be met.

Definition 10.2. Let $\mathfrak{P}$ be a prime of L and $\nu_{\mathfrak{P}}$ its valuation. Let $y^2 = 4x^3 - g_2'x - g_3'$ be a minimal Weierstrass model of E over $L_{\mathfrak{P}}$. Then, E has good reduction at $\mathfrak{P}$ if and only if $\nu_{\mathfrak{P}}(\Delta_E) \neq 0$.

Proposition 10.3. *Let $\mathfrak{m}$ be an integral ideal of K relatively prime to a prime $\mathfrak{P}$ of L. Then, E has good reduction at a prime $\mathfrak{P}$ if and only if $L(E[\mathfrak{m}^\infty])/L$ is unramified at $\mathfrak{P}$.*

Proof. See [9, IV.10.3] for a weaker version. See [6] for this result. □

Proposition 10.4. *Let $\mathfrak{p}$ be a prime of K. Let $L_n = L(E[\mathfrak{p}^n])$, $0 \leq n \leq \infty$. All primes here are assumed to be relatively prime to $\mathfrak{f}$. Then:*

(i) All the primes above $\mathfrak{p}$ are totally ramified in L_∞/L.

(ii) Primes not above $\mathfrak{p}$ are finitely ramified and unramified if they are primes of good reduction.

(iii) If $\mathfrak{p}$ is split in $K/\mathbb{Q}$, every prime not above $\mathfrak{p}$ of good reduction is finitely decomposed in L_∞/L.

Proof. (i) This will follow from Proposition 11.4.

(ii) Let $\mathfrak{g}$ be an integral ideal of K such that $\mathfrak{f} \mid \mathfrak{g}$ (then $L(E[\mathfrak{g}]) = K(\mathfrak{g})$ by 9.20). Let $M = K(\mathfrak{g})$ and let $\mathfrak{P}$ be a prime of M relatively prime to $\mathfrak{g}$. Suppose that σ is in the inertia subgroup of $\text{Gal}(L^{ab}/M)$ over $\mathfrak{P}$. Then choose $\mathfrak{R}$ such that $\sigma_{\mathfrak{R}} = \sigma|_{K^{ab}}$. Since $[\psi_{E/M}(\mathfrak{R})](T) = T^\sigma$ for $T \in E[\mathfrak{g}]$ and since $E[\mathfrak{g}] \subset M$, then $T^\sigma = T$ so that $L(E[\mathfrak{p}^\infty])/L$ is unramified at $\mathfrak{P}$. This shows that $\mathfrak{P}$ is finitely ramified. That unramified primes not above $\mathfrak{p}$ give good reduction is part of Proposition 10.3.

(iii) Let $\mathfrak{R}$ be a prime in L over which E has good reduction which is not above $\mathfrak{p}$. Then since $\mathfrak{R}$ is unramified in L_∞/L, by proposition 9.5, the order of the decomposition group of $\mathfrak{R}$ in L_n/L, which is cyclic, is the least integer m for which $\psi_{E/L}(\mathfrak{R})^m \equiv 1 \mod \mathfrak{p}^n(\mathcal{O}_K)_{\mathfrak{p}}$. If $\mathfrak{p}$ is split, $(\mathcal{O}_K)_{\mathfrak{p}} \simeq \mathbb{Z}_p$ where $p = \mathfrak{p}\bar{\mathfrak{p}}$. Under this identification, $\psi_{E/L}(\mathfrak{R}) \mapsto c \in \mathbb{Z} \subset \mathbb{Z}_p$ such that $c \in \mathbb{Z}_p^\times$. Choose n so that $c < p^n$. Then the order of c in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ multiplies by p for every increase of n by 1. The degree of L_{n+1}/L_n will be seen to be p later from Proposition 11.4. Thus, $\mathfrak{R}$ is finitely decomposed.

□

11. The Lubin-Tate Structure of $\hat{E}$

Let E be as before and $w_g = 1$. Fix a split integral prime $\mathfrak{p}$ in K relatively prime to 6 such that $(\mathfrak{p}, \mathfrak{f}) = 1$. Let $\mathfrak{P}$ be a prime lying above $\mathfrak{p}$ and let $\mathcal{O}'$ be the

valuation ring of $L_{\mathfrak{P}}$. Let $\nu_{\mathfrak{P}}$ be the valuation of $L_{\mathfrak{P}}$ at $\mathfrak{P}$. Suppose that the model of E is chosen so that $\nu_{\mathfrak{P}}(g_2)$ and $\nu_{\mathfrak{P}}(g_3)$ are non-negative so that we may define $\hat{E}$ over the ring $\mathcal{O}'$.

We want the map $[\kappa_0(\mathfrak{p})]_{E,E^{\sigma_\mathfrak{p}}}$ to formally induce a morphism in $\mathrm{Hom}(\hat{E}, \hat{E}^{\sigma_\mathfrak{p}})$. First we need the following:

Proposition 11.1. *The power series expansion in the t-coordinate $t = \dfrac{-2x}{y}$ about $t = 0$ of Ψ_E is the formal logarithm $\lambda_{\hat{E}} : \hat{E} \to \hat{G}_a$ and is defined over L.*

Proof. Recall from (3) that $\wp(z) = \dfrac{1}{z^2} + g(z)$ for a function $g(z)$ that is holomorphic in a neighborhood of $z = 0$. Hence

$$t = \frac{-2x}{y} = \frac{-2z^{-2} - 2g(z)}{-2z^{-3} + g'(z)} = \frac{z + z^3 g(z)}{1 - (z^3/2)g'(z)}$$

which has a formal z expansion with z-coefficient 1. Because Ψ_E is a group homomorphism where the addition law on $\mathbb{C}/\Lambda_E$ is given by $\hat{G}_a$, the z expansion described is the formal group law homomorphism $[1]_{\hat{G}_a,\hat{E}}$. From Proposition 4.6, $\lambda_{\hat{E}} = [1]_{\hat{E},\hat{G}_a}$ and is defined over L.

□

Definition 11.2. Given elliptic curves E_1 and E_2 and an isogeny $[\alpha]_{E_1,E_2}$, we define $[\alpha]_{\hat{E}_1,\hat{E}_2}$ as the power series map that makes the following diagram commute:

$$\begin{array}{ccc} \hat{G}_a & \xrightarrow{[\alpha]_{\hat{G}_a}} & \hat{G}_a \\ {\scriptstyle \lambda_{\hat{E}_1}}\uparrow & & \downarrow{\scriptstyle \lambda^{-1}_{\hat{E}_2}} \\ \hat{E}_1 & \xrightarrow{[\alpha]_{\hat{E}_1,\hat{E}_2}} & E_2 \end{array}$$

Let $f = [\kappa_0(\mathfrak{p})]_{\hat{E},\hat{E}^{\sigma_\mathfrak{p}}}$. Then, $f \in L[[t]]$. The map f is also given coordinate-wise in the following manner. Let $t = -2x/y$ be a point away from O on E with $y \neq 0$. Let $(x_1, y_1) = [\kappa_0(\mathfrak{p})]_{E,E^{\sigma_\mathfrak{p}}}(x, y)$. Then, $f(t) = -2x_1/y_1$.

From Proposition 10.3, since $\mathfrak{p}$ is unramified in $K(E[\mathfrak{f}\bar{\mathfrak{p}}])$, E has good reduction at every prime over $\mathfrak{p}$ in L. From the statements and proofs of [9, II.4.2,4.4,5.3], the Main Theorem of Complex Multiplication gives that $[\kappa_0(\mathfrak{p})]_{E,E^{\sigma_\mathfrak{p}}}$ is a lift of the Frobenius map $(x, y) \to (x^p, y^p) \mod \mathfrak{P}$. Hence, $[\kappa_0(\mathfrak{p})]_{E,E^{\sigma_\mathfrak{p}}}(x, y) \equiv (x_1^p, y_1^p) \mod \mathfrak{P}$. That is, $f(t) \equiv t^p \mod \mathfrak{P}$. Under the natural inclusion $L \mapsto L_{\mathfrak{P}}$, $f(t) \in \mathcal{O}'[[t]]$.

One way to see that $\nu_{\mathfrak{P}}(f'(0)) = 1$ is the following argument which is similar to ([2], 18.3.1). Since $f \in \mathrm{Hom}(\hat{E}, \hat{E}^{\sigma_\mathfrak{p}})$, differentiating with respect to t_2 yields:

$$f'(\hat{E}(t_1, t_2)) \cdot \partial\hat{E}/\partial t_2(t_1, t_2) = \partial\hat{E}^{\phi}/\partial t_2(f(t_1), f(t_2))f'(t_2).$$

Then set $t_2 = 0$ to see:

$$f'(t_1)\partial\hat{E}/\partial t_2(t_1, 0) = \partial\hat{E}^{\phi}/\partial t_2(f(t_1), 0)f'(0).$$

Since $\partial\hat{E}/\partial t_2(t_1, 0) = 1 + t_1 + ... \in \mathcal{O}'[[t]]$ has a multiplicative inverse in $\mathcal{O}'[[t_1]]$, then $f'(0) \equiv 0 \mod \mathfrak{P}$ so that $f(t) \equiv g(t^p) \mod \mathfrak{P}$ for some power series $g \in \mathcal{O}'[[t]]$.

Suppose that $f'(0) = u\pi^n$ for some uniformizer π and unit u. Then from the above argument, $[\pi]_{E,E^{\sigma_\mathfrak{p}}} \in \mathrm{Hom}_{L_\mathfrak{P}}(\hat{E}, \hat{E}^{\sigma_\mathfrak{p}})$ is a power series in $\mathcal{O}'[[t^{pk}]]$ for some $k \geq 1$. Then, f must be a power series in t^{pkn}. Since $f \equiv t^p \mod \mathfrak{P}$, $kn = 1$ so that $n = 1$. Hence, $f'(0)$ is a uniformizer.

Let $k' = L_\mathfrak{P}$, $k = K_\mathfrak{p}$, and $\xi = \mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}(f'(0))$. Then above arguments give the following:

Proposition 11.3. *With $k' = L_\mathfrak{P}$, $k = K_\mathfrak{p}$, and $\xi = \mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}(f'(0))$, we have $\hat{E} = F_f$.*

Since the points $E[\mathfrak{p}^n]$ lie away from $y = 0$ by Proposition 2.7, we may apply f to these points. So for $T \in E[\mathfrak{p}^n]$ written in the form $-2x/y$, $f(T) = 0$ which implies that $T^p \equiv 0 \mod \mathfrak{P}$ so that $\nu_\mathfrak{P}(T) > 0$. Thus, we have the inclusion $E[\mathfrak{p}^n] \subset W_f^n$ which is equality since $|E[\mathfrak{p}^n]| = |W_f^n|$. Recall from Proposition 9.19 that $\mathrm{Gal}(L(E[\mathfrak{p}^n])/L) \simeq (\mathcal{O}_K/\mathfrak{p}^n)^\times \simeq ((\mathcal{O}_K)_\mathfrak{p}/\mathfrak{p}^n)^\times \simeq \mathrm{Gal}(k_\xi^n/k)$. Since $\mathrm{Gal}(k_\xi^n/k)$ is isomorphic to the decomposition subgroup of $\mathrm{Gal}(L(E[\mathfrak{p}^n])/L)$ at $\mathfrak{P}$, we obtain the following:

Corollary 11.4. *The extensions $L_n = L(E[\mathfrak{p}^n])$ are totally ramified over L of degree $p^{n-1}(p-1)$ and $E[\mathfrak{p}^n] = W_f^n$.*

12. Semilocal construction

Let E be as in the previous section. Let $\mathfrak{p}$ be as in the previous section and fix an embedding $\iota_p : \bar{\mathbb{Q}} \to \mathbb{C}_p$ such that $\mathfrak{p}$ is the place induced by the inclusion $K \subset \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$.

Definition 12.1. Let $\Phi = L \otimes_K K_\mathfrak{p}$, $R = \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_\mathfrak{p}$, $L' = L(E[\bar{\mathfrak{p}}^\infty])$, $\Phi' = L' \otimes_K K_\mathfrak{p}$, $R' = \mathcal{O}_{L'} \otimes_{\mathcal{O}_K} \mathcal{O}_\mathfrak{p}$. Let $\widehat{\Phi}$, $\widehat{R}$, $\widehat{\Phi'}$ and $\widehat{R'}$ denote the completions of these objects.

Definition 12.2. The complex number Ω_0 is called the complex period of E.

Definition 12.3. Let $W_f^{n,s}$ be the image of $E[\mathfrak{p}^n]$ in $L_\infty \otimes_K K_\mathfrak{p}$ via the map $m \mapsto m \otimes 1$. The s stands for "semilocal".

Note that $\Omega_0 \in \mathfrak{f}^{-1}\Lambda/\Lambda = \Psi_E^{-1}(E[\mathfrak{f}])$. By the Main Theorem of Complex Multiplication, $[\kappa_0(\mathfrak{p})]^{\sigma_\mathfrak{p}^{-n}}(T) = T^{\sigma_\mathfrak{p}}$ for $T \in E^{\sigma_\mathfrak{p}^{-n}}[\mathfrak{f}]$ so that $[\kappa_0(\mathfrak{p})]^{\sigma_\mathfrak{p}^{-n}}$ induces a bijective map $E^{\sigma_\mathfrak{p}^{-n}}[\mathfrak{f}] \to E^{\sigma_\mathfrak{p}^{-n+1}}[\mathfrak{f}]$. Hence, Ω_0 uniquely defines

$$\{\Omega_n\}_n \in \varprojlim_n \Psi_{E^{\sigma_\mathfrak{p}^{-n}}}(E^{\sigma_\mathfrak{p}^{-n}}[\mathfrak{f}])$$

with respect the maps $\Psi_{E^{\sigma_\mathfrak{p}^{-n+1}}} \circ [\kappa_0(\mathfrak{p})]^{\sigma_\mathfrak{p}^{-n}} \circ \Psi^{-1}_{E^{\sigma_\mathfrak{p}^{-n}}}$.

This gives

$$\{\Omega_0 - \Omega_n\}_n \in \varprojlim_n \mathfrak{p}^{-n}\Lambda_{\mathfrak{p}^{-n}}/\Lambda_{\mathfrak{p}^{-n}}.$$

Definition 12.4. We will fix $\hat{\omega} = (\Psi^{-1}_{E^{\sigma_\mathfrak{p}^{-n}}}(\Omega_0 - \Omega_n))_n$.

It follows that $\hat{\omega}_n$ is in

$$\tilde{W}^{n,s}_{f^{\sigma_\mathfrak{p}^{-n}}} = W^{n,s}_{f^{\sigma_\mathfrak{p}^{-n}}} - W^{n-1,s}_{f^{\sigma_\mathfrak{p}^{-n}}}.$$

Recall the definition of $\hat{G}_m$ as given in Example 6.13.

Proposition 12.5. *Consider $\hat{G}_m$ and $\hat{E}$ as formal group laws over $\widehat{R'}$. Then there exists an isomorphism $\theta : \hat{G}_m \to \hat{E}$ such that the following is satisfied for $(\mathfrak{c}, \mathfrak{f}\bar{\mathfrak{p}}) = 1$:*

$$[\kappa_0(\mathfrak{c})]_{\hat{E},\hat{E}^{\sigma_\mathfrak{c}}} \circ \theta = \theta^{\sigma_\mathfrak{c}} \circ [\mathrm{N}_{K/\mathbb{Q}}\mathfrak{c}]_{\hat{G}_m} \tag{16}$$

Let $\Omega_p = \theta'(0)$. We have that $\Omega_p \in \widehat{R'}^\times$ is uniquely determined by (16) modulo $\mathcal{O}_\mathfrak{p}^\times$.

Proof. We only show the existence of $b \in \widehat{R'}^\times$ which satisfies the condition $b^{\sigma_\mathfrak{c}-1} = \kappa_0(\mathfrak{c})\mathrm{N}\mathfrak{c}^{-1}$ which is a condition satisfied by Ω_p. For the other details see [5, II.4.3]. Suppose that $\sigma_\mathfrak{c}$ fixes L and $E[\bar{\mathfrak{p}}^m]$ pointwise. Since $\sigma_\mathfrak{c}$ fixes L, $\kappa_0(\mathfrak{c}) = \phi(\mathfrak{c})$. Also, it follows that $\mathfrak{c} \in P_K^\mathfrak{f}$, so that $\mathfrak{c} = (\phi(\mathfrak{c}))$ since ϕ is a grossencharacter. Thus, $\phi(\mathfrak{c})\bar{\phi}(\mathfrak{c}) = \mathrm{N}\mathfrak{c}$. Since $\sigma_\mathfrak{c}$ fixes $E[\mathfrak{p}^{\bar{m}}]$ pointwise, then multiplication by $\phi(\mathfrak{c})$ is trivial on $(\mathcal{O}_K/\mathfrak{p}^{\bar{m}})^\times$ by Lemma 9.17. Hence, $\phi(\mathfrak{c}) \equiv 1 \mod \mathfrak{p}^{\bar{m}}$. Equivalently, $\bar{\phi}(\mathfrak{c}) \equiv 1 \mod \mathfrak{p}^m$.

The above paragraph yields $\kappa_0(\mathfrak{c})\mathrm{N}\mathfrak{c}^{-1} \equiv 1 \mod \bar{\mathfrak{p}}^m$. Since κ_0 is a cocycle by Proposition 9.10, we may extend the map $\mathfrak{c} \mapsto \kappa_0(\mathfrak{c})\mathrm{N}\mathfrak{c}^{-1}$ for $\mathfrak{c}$ with the above conditions to a continuous 1-cocycle $\vartheta : \mathrm{Gal}(L'/K) \to \widehat{R'}^\times$. Since $\mathrm{Gal}(L'/K)$ is unramified, Hilbert's Theorem 90 gives us that $H^1(\mathrm{Gal}(L'/K), \widehat{R'}) = 1$. Therefore, ϑ is a 1-coboundary. That is, it is equal to $b^{\sigma_\mathfrak{c}-1}$ for some b in $\widehat{R'}$.

□

Fix a choice of θ from Proposition 12.5.

Let $\mathcal{M}_0$ be the set of all elements of L_∞ having positive valuation via the embedding ι_p. Let $\mathcal{M}$ denote the closure of the image of $\mathcal{M}_0$ in $L_\infty \otimes_K K_\mathfrak{p}$ via the inclusion $m \mapsto m \otimes 1$.

Definition 12.6. Fix

$$\hat{\zeta} = \{1 - \zeta_{p^n}\}_n \otimes 1 \in \varprojlim_n \hat{G}_m(\mathcal{M})$$

where ζ_{p^n} is a primitive p^nth root of unity for all $n \geq 0$ and the inverse limit is given with respect to the maps $[p]_{\hat{G}_m}$ such that

$$\theta^{\sigma_\mathfrak{p}^{-n}}((\zeta_{p^n} - 1) \otimes 1) = \omega_n \otimes 1.$$

Let $c \in \mathcal{O}_K$ such that $c \in \mathcal{O}_{K_\mathfrak{p}}^\times$ under the canonical embedding $K \to K_\mathfrak{p}$. Since $\hat{E} = F_f$, then $[c]_f$ gives an endomorphism of $\hat{E}(\mathcal{M})$. Hence, $[c]_f \circ \theta$ gives an isomorphism $\hat{G}_m(\mathcal{M}) \to \hat{E}(\mathcal{M})$ satisfying the condition of Proposition 12.5. Multiplying Ω_p by c is equivalent to replacing θ by $[c]_f \circ \theta$. Since $\Psi_{E^{\sigma_\mathfrak{p}^{-n+1}}} \circ [c]_f \circ \Psi^{-1}_{E^{\sigma_\mathfrak{p}^{-n}}}$ is multiplication by c, this process also replaces $\Omega_0 - \Omega_n$ by $c(\Omega_0 - \Omega_n)$ or Ω_0 by $c\Omega_0$. This may be applied reversely. If the pair $(\Omega_0, \Omega_\mathfrak{p})$ corresponds to E, then so does $(c\Omega_0, c\Omega_\mathfrak{p})$ reflecting our choice of Ω_0 and θ.

13. A Coleman Power Series Derived from E

Let $\mathfrak{p}$, R, Φ, R', Φ', $\mathcal{M}$, and θ be as in section 12. Recall that $\Lambda_E = \mathfrak{f}\Omega_0$ and that $\hat{\omega} = (\Psi^{-1}_{E^{\sigma_\mathfrak{p}-n}}(\Omega_n - \Omega_0))_n$.

The previous local results on Coleman power series may be interpreted semilocally. The proofs and theorems may be generalized. Let $\mathcal{O}'_n$ denote the valuation

ring of $L(E[\mathfrak{p}^n])_{\mathfrak{P}}$ where $\mathfrak{P}$ lies over $\mathfrak{p}$. Then $\mathcal{O}_{L(E[\mathfrak{p}^n])} \otimes_K K_{\mathfrak{p}} \simeq \oplus_{i-1}^{r} \mathcal{O}_n$ where r is the number of distinct primes $\mathfrak{P}$ lying abover $\mathfrak{p}$ in $L(E[\mathfrak{p}^n])_{\mathfrak{P}}$. We describe this isomorphism canonically such that $m \otimes 1$ is sent to the image of m in the inclusion $L(E[\mathfrak{p}^n]) \to L(E[\mathfrak{p}^n])_{\mathfrak{P}}$.

This isomorphism allows us to project the formal group $\hat{E}$ defined over Φ component-wise. If there exists a norm coherent sequence $\hat{u} = (u_n)_n$ of units in the tower given by the fields $L(E[\mathfrak{p}^n])_{\mathfrak{P}}$, we may naturally consider $(u_n \otimes 1)_n$ component-wise as norm coherent sequences of units. A similar statement holds for sequences of torsion points. Coleman power series can thus naturally be extended to this semilocal setting. We do this so that we get the full strength of the map κ_0. If g_β is a coleman power series, then for $(\mathfrak{c}, \mathfrak{pf}) = 1$, $g_\beta \circ [\kappa_0(\mathfrak{c})]_{\hat{E}, \hat{E}^{\sigma_\mathfrak{c}}}$ satisfies the defining property (8) of the series $g_{\sigma_\mathfrak{c}(\beta)}$. This will follow from the following fact:

If $T \in W_{f^{\sigma_\mathfrak{p}^{-n}}}^{n,s}$, $g_\beta(T)^{\sigma_\mathfrak{c}} = g_\beta^{\sigma_\mathfrak{c}}(T^{\sigma_\mathfrak{c}}) = g_\beta^{\sigma_\mathfrak{c}}(\kappa_0(\mathfrak{c}))$.

This key idea allows us to extend measures defined by Coleman power series on $\mathcal{G} = \mathrm{Gal}(L_\infty/L)$ to $G = \mathrm{Gal}(L_\infty/K)$. We have the following two propositions:

Proposition 13.1. *Let β and β' be norm coherent sequences as in the paragraph above. Let*

$$\hat{\omega} = \{\omega_n \otimes 1\}_n \in \varprojlim_n \hat{E}^{\sigma_\mathfrak{p}^{-n}}(\mathcal{M}).$$

Then there exists a unique Coleman power series $g_\beta \in R[[t]]^\times$ satisfying $g_\beta^{\sigma_\mathfrak{p}^{-n}}(\omega_n) = \beta_n$ with properties analogous to the local ones:

(i) $g_{\beta\beta'} = g_\beta \cdot g_{\beta'}$.

(ii) $g_\beta^\phi \circ [\kappa_0(\mathfrak{p})]_{f, \sigma_\mathfrak{p}(f)}(t) = \prod_{\omega \in W_f^{n,s}} g_\beta(t[+]_{\hat{E}}\omega)$

(iii) $g_\beta(0)^{1-\sigma_\mathfrak{p}^{-1}} = \beta_0$.

(iv) If $\sigma_\mathfrak{c} \in \mathrm{Gal}(L_\infty/K)$, then $g_{\sigma_\mathfrak{c}(\beta)} = g_\beta^{\sigma_\mathfrak{c}} \circ [\kappa_0(\mathfrak{c})]_{\hat{E}, \hat{E}^\sigma}$.

Proposition 13.2. *Let β and $\hat{\omega}$ be as in Proposition 13.1. There exists a unique $\widehat{R'}$-valued measure μ_β on $\mathcal{G}$ such that*

$$a_\beta(s) = (\log g_\beta) \circ \theta(s) = \int_G (1+s)^\alpha d\mu(\alpha).$$

(From proposition 9.19, $G \simeq \mathbb{Z}_p^\times$).

We use results on certain special functions to obtain what we call elliptic units which will give β for the measure we wish to construct.

Definition 13.3. Define

$$\Theta_{\Lambda,\mathfrak{a}}(z) = \frac{\Delta_\Lambda}{\Delta_{\mathfrak{a}^{-1}\Lambda}} \cdot \prod_{u \in \mathfrak{a}^{-1}\Lambda/\Lambda}{}' \frac{\Delta_\Lambda}{(\wp(z,\Lambda) - \wp(u,\lambda))^6}$$

where the $'$ indicates that the product is over all $u \in \mathfrak{a}^{-1}\Lambda/\Lambda$ such that $\wp(z,\Lambda) - \wp(u,\lambda) \neq 0$.

Proposition 13.4. *(The Distribution Relation)*

Let $(\mathfrak{a}, \mathfrak{b}) = 1$. Then:

$$\prod_{v \in \mathfrak{b}^{-1}\Lambda/\Lambda} \Theta_{\Lambda,\mathfrak{a}}(z+v) = \Theta_{\mathfrak{b}^{-1}\Lambda,\mathfrak{a}}(z)$$

Proof. See ([5],II.2.3)

□

Definition 13.5. Let $\Theta_{\mathfrak{a},n} = \Theta_{\mathfrak{p}^n\Lambda,\mathfrak{a}}(\Omega_0)$. We call $\Theta_{\mathfrak{a},n}$ an elliptic unit.

From ([5],II.2), $\Theta_{\mathfrak{a},n}$ has the following properties:

Proposition 13.6. *Let $n \geq 1$, $(\mathfrak{c},\mathfrak{p}) = 1$, and $(\mathfrak{c},\mathfrak{f}) = 1$. Then:*
(i) $\sigma_{\mathfrak{c}}(\Theta_{\mathfrak{a},n}) = \Theta_{\mathfrak{a}\mathfrak{c},n}\Theta_{\mathfrak{c},n}^{\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})}$.
(ii) $\mathrm{N}_{L_m/L_n}(\Theta_{\mathfrak{a},m}) = \Theta_{\mathfrak{a},n}$.
(iii) $\Theta_{\mathfrak{a},n}$ *is a unit outside* $\mathfrak{p}$ *in* L_n.

Proof. See [5, II.2.4].

□

From here on, we will fix an integral ideal $\mathfrak{a}$ of K and also set β so that

$$\beta = (\Theta_{\mathfrak{a},n} \otimes 1)_n \tag{17}$$

By the choice of $\Theta_{\mathfrak{a},n}$, the function $\Theta_{\Lambda,\mathfrak{a}}(\Omega_0 - \lambda_{\hat{E}}(t)) \otimes 1$ expressed as a power series expansion is the semilocal Coleman power series associated to the pair $(\hat{\omega},\beta)$ *if* its coefficients lie in R. See [5, II.4.9] for a proof of this fact.

Proposition 13.7. *Let $r(z)$ be the power series expansion of $\Theta_{\Lambda,\mathfrak{a}}(\Omega_0 - z)$ at $z = 0$. Then the Coleman power series relative to the pair $(\hat{\omega},\beta)$ is given by $g_\beta = r \circ \lambda_{\hat{E}}$ where $\lambda_{\hat{E}}$ is defined over Φ.*

14. Eisenstein numbers

Let N denote $\mathrm{N}_{K/\mathbb{Q}}$ and let the notation in the last section be the same here.

In this section we acquire the tools we need to relate $g_\beta = \Theta_{\Lambda,\mathfrak{a}}(\Omega_0 - \lambda_{\hat{E}})$ to values of certain L-functions. The necessary connection is made using identities of Eisenstein functions which we give in this section.

Let $\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$ be a $\mathbb{Z}$-lattice in $\mathbb{C}$, ordered so that $\tau = w_1/w_2$ belongs to the upper half plane.

Define the quantities

$$\eta_1 = w_1 \sum_{n\in\mathbb{Z}} \sum_{\substack{m\,\in\,\mathbb{Z} \\ mw_1 \neq -nw_2}} \frac{1}{(mw_1 + nw_2)^2},$$

$$\eta_2 = w_2 \sum_{m\in\mathbb{Z}} \sum_{\substack{n\,\in\,\mathbb{Z} \\ mw_1 \neq -nw_2}} \frac{1}{(mw_1 + nw_2)^2},$$

and

$$A(\Lambda) = \frac{1}{2\pi i}(w_1\bar{w}_2 - \bar{w}_1 w_2).$$

Then we define

$$\eta(z,\Lambda) = \frac{w_1\eta_2 - w_2\eta_1}{2\pi i A(\Lambda)}\bar{z} + \frac{\bar{w}_2\eta_1 - \bar{w}_1\eta_2}{2\pi i A(\Lambda)}z.$$

Further let

$$\zeta(z,\Lambda) = \frac{1}{z} + \sum_{\substack{m,\,n\,\in\,\mathbb{Z} \\ mw_1 \neq -nw_2}} \left(\frac{1}{z - mw_1 - nw_2} + \frac{1}{mw_1 + nw_2} + \frac{z}{(mw_1 + nw_2)^2}\right)$$

We may now make the following definitions of Eisenstein functions.

Definition 14.1.

$$E_1(z,\Lambda) = \zeta(z,\Lambda) - \eta(z,\Lambda)$$

$$E_k(z,\Lambda) = \frac{-d^k}{dz^k} E_1(z,\Lambda).$$

$$E_k(z,\Lambda,\mathfrak{a}) = \mathrm{N}\mathfrak{a} \cdot E_k(z,\Lambda) - E_k(z,\mathfrak{a}^{-1}\Lambda)$$

From [5, II.3.1], we have the following results the first of which relates $\Theta_{\Lambda,\mathfrak{a}}$ to $E_k(z,\Lambda,\mathfrak{a})$:

Proposition 14.2.

$$E_k(z,\Lambda,\mathfrak{a}) = \frac{1}{12}(-1)^{k+1}\frac{d^k}{dz^k}\log\Theta_{\Lambda,\mathfrak{a}}(z).$$

Proposition 14.3. *For $k > 3$,*

$$E_k(z,\Lambda) = (k-1)! \cdot \sum_{w\in\Lambda}(z+w)^{-k}.$$

Now we give the following notation for L-functions:

Definition 14.4. Suppose that $\chi : \mathrm{Gal}(L_\infty/K) \to \mathbb{C}^\times$. Let

$$L_{\mathfrak{m}}(\chi,z) = \sum_{(\mathfrak{a},\mathfrak{m})=1} \chi(\mathfrak{a})(\mathrm{N}\mathfrak{a})^{-z}.$$

Further let

$$L_{\mathfrak{m}}^{\mathfrak{c},M}(\chi,z) = \sum_{\substack{(\mathfrak{a},\,\mathfrak{m})\,=\,1\\(\mathfrak{a},\,M/K)\,=\,(\mathfrak{c},\,M/K)}} \chi(\mathfrak{a})(\mathrm{N}\mathfrak{a})^{-z}.$$

Proposition 14.5. *Let $\mathfrak{m}$ be an integral ideal and v a primitive $\mathfrak{m}$-division point (that is, $v \in \mathfrak{m}^{-1}\Lambda$ but $v \notin \mathfrak{b}^{-1}\Lambda$ if $\mathfrak{b} \mid \mathfrak{m}$ and $\mathfrak{b} \neq \mathfrak{m}$). Then for $(\mathfrak{c},\mathfrak{m}\mathfrak{f}) = 1$,*

$$E_k(v,\Lambda) = E_k(\kappa_0(\sigma_{\mathfrak{c}})v, \kappa_0(\sigma_{\mathfrak{c}})\mathfrak{c}^{-1}\Lambda) = \kappa(\sigma_{\mathfrak{c}})^{-k}E_k(v,\mathfrak{c}^{-1}\Lambda)$$

Proof. See [5, II.3.3]. The proof uses Proposition 13.6. □

Lemma 14.6. *Let $\mathfrak{g}$ be an integral ideal and the conductor of a grossencharacter ϕ of K. If $w_{\mathfrak{g}} = 1$, then $\phi((a)) = a$ for any $a \equiv 1 \mod \mathfrak{g}$.*

Proof. Suppose that $(a) = (b)$ such that $a \equiv b \equiv 1 \mod \mathfrak{g}$. Then, a/b is a unit which is $\equiv 1 \mod \mathfrak{g}$. Since $w_{\mathfrak{g}}$ is the number of units $\equiv 1 \mod \mathfrak{g}$ in K, $a/b = 1$. □

Proposition 14.7. *Suppose that the conductor of ϕ, divides $\mathfrak{m}$. Then for $(\mathfrak{c},\mathfrak{m}) = 1$,*

$$E_k(\Omega_0, \mathfrak{c}^{-1}\mathfrak{m}\Omega_0) = (k-1)!\Omega_0^{-k} \cdot \phi(\mathfrak{c})^k \cdot L_{\mathfrak{m}}^{\mathfrak{c},K(\mathfrak{m})}(\bar{\phi}^k, k)$$

Proof. We only mention the key ideas for the proof.

For $k > 3$, use proposition 14.3 and compute:

$$\begin{aligned}
&\Omega_0^{-k} \sum_{w \in \mathfrak{c}^{-1}\mathfrak{m}\Omega_0} \Omega_0^k (\Omega_0 + w)^{-k} \\
&= \Omega_0^{-k} \sum_{w \in \mathfrak{c}^{-1}\mathfrak{m}\Omega_0} \big(1 + \frac{w}{\Omega_0}\big)^{-k} \\
&= \Omega_0^{-k} \sum_{w \in \mathfrak{c}^{-1}\mathfrak{m}} (1+w)^{-k}.
\end{aligned}$$

Lemma 14.6 may be applied to yield $\phi((1+w)) = 1 + w$.

The identity $(\mathrm{N}\mathfrak{b})^{-k} = \bar{\phi}^{-k}(\mathfrak{b})\phi^{-k}(\mathfrak{b})$ is also used.

See [5, II.3.5] for more details.

□

15. The Key Ingredients

Let θ be fixed as above (from Proposition 16 relative to $\hat{\zeta} = (1 - \zeta_{p^n})_n$ and $\hat{\omega}$). Also let β be as in (17); and let a_β, $\widetilde{a_\beta}$ and $\mathcal{D}$ be as before. Recall that we have fixed $\iota_p : \bar{\mathbb{Q}} \to \mathbb{C}_p$.

We make the definition:

Definition 15.1. Let $\delta_k(\beta) = \mathcal{D}^k(a_\beta)(0)$, $\widetilde{\delta_k(\beta)} = \mathcal{D}^k(\widetilde{a_\beta})(0)$.

The map ι_p induces a map $\widehat{\Phi'} \to \mathbb{C}_p$ via the completed tensor product functor. We will use μ_β^0 and $\delta_k(\beta)^0$ to represent $\iota_p \circ \mu_\beta$ and $\iota_p \circ \delta_k(\beta)$ respectively.

In the results that follow, we use the following conventions: if $\chi : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$, then χ extends to a character $\chi : I_K^{\mathfrak{f}} \to \mathbb{C}^\times$. We also may think of ϕ as a function on $\mathcal{G}$ [5, II.1.1].

Proposition 15.2. *Let $\chi : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$ and S be a collection of integral ideals of K such that $\{\sigma_\mathfrak{c} \mid \mathfrak{c} \in S\}$ is a set of coset representatives for G in $\mathcal{G}$. Then:*

$$\left(1 - \frac{(\chi\phi^k)(\mathfrak{p})}{p}\right) \cdot \sum_{\mathfrak{c} \in S} (\chi\phi^k)(\mathfrak{c}^{-1}) \cdot \delta_k(\sigma_\mathfrak{c}(\beta))^0 = \int_{\mathcal{G}} (\chi\phi^k)(\sigma_\mathfrak{c}) d\mu_\beta^0(\sigma_\mathfrak{c}). \tag{18}$$

Proof. We give some ideas of the proof.

Consider

$$\begin{aligned}
\mathcal{D}^k\left(\frac{1}{p} \sum_{w \in W_f^1} \log g_\beta(\theta(s)[+]w\right) &= \frac{1}{p}\mathcal{D}^k\Big(\log(\mathfrak{N} g_\beta \circ f \circ \theta(s))\Big) \\
&= \frac{1}{p}\mathcal{D}^k(\log(g_\beta^{\sigma_\mathfrak{p}} \circ \theta([p](s)))).
\end{aligned}$$

Thus,

$$\delta_k(\beta) = \widetilde{\delta_k}(\beta) + p^{k-1}\mathcal{D}^k(\log g_\beta^{\sigma_\mathfrak{p}} \circ \theta)([p](s))|_{s=0} = \widetilde{\delta_k}(\beta) + p^{k-1}\phi(\delta_k).$$

Next, we use $g_{\sigma_\mathfrak{c}(\beta)} = \sigma_\mathfrak{c}(g_\beta) \circ [\kappa_0(\mathfrak{c})]$ and $[\kappa_0(\mathfrak{c})] \circ \theta = \theta^{\sigma_\mathfrak{c}} \circ [\mathrm{N}_{K/\mathbb{Q}}\mathfrak{c}]$ to obtain

$$\begin{aligned}
\delta_k(\sigma_\mathfrak{c}(\beta)) &= \mathcal{D}^k(\log \sigma_\mathfrak{c}(g_\beta) \circ \theta^{\sigma_\mathfrak{c}} \circ [\mathrm{N}_{K/\mathbb{Q}}\mathfrak{c}])|_{s=0} = \\
&= \mathrm{N}_{K/\mathbb{Q}}\mathfrak{c}^k \mathcal{D}^k((\log \sigma_\mathfrak{c}(g_\beta) \circ \theta^{\sigma_\mathfrak{c}}) \circ [\mathrm{N}_{K/\mathbb{Q}}\mathfrak{c}])|_{s=0} = \mathrm{N}_{K/\mathbb{Q}}\mathfrak{c}^k \sigma_\mathfrak{c}(\delta_k(\beta))
\end{aligned}$$

Note that this also gives:

$$\widetilde{\delta_k}(\sigma_{\mathfrak{c}}(\beta))^0 = \mathrm{N}_{K/\mathbb{Q}}\mathfrak{c}^k \sigma_{\mathfrak{c}}(\widetilde{\delta_k}(\beta)^0)$$

Inserting for $\delta_k(\sigma_{\mathfrak{c}}(\beta))^0$ on the left side of (18), we obtain:

$$\left(1 - \frac{(\chi\phi^k)(\sigma_{\mathfrak{p}})}{\mathfrak{p}}\right) \cdot \sum_{\mathfrak{c}\in S} (\chi\phi^k)(\mathfrak{c}^{-1}) \cdot \mathrm{N}_{K/\mathbb{Q}}\mathfrak{c}^k \sigma_{\mathfrak{c}}(\delta_k(\beta)^0).$$

Refer to [5, II.4.7] to see how this simplifies.

□

Definition 15.3. Let $\delta_{k,n}(\beta) = \mathcal{D}^k(a_\beta)(\zeta_{p^n} - 1)$, $\widetilde{\delta_{k,n}(\beta)} = \mathcal{D}^k(\widetilde{a_\beta})(\zeta_{p^n} - 1)$.

We let $\delta_{k,n}(\beta)^0$ and $\widetilde{\delta_{k,n}(\beta)}^0$ respectively denote the images of $\delta_{k,n}(\beta)$ and $\widetilde{\delta_{k,n}(\beta)}$ via ι_p.

Definition 15.4. Let $\chi : \mathrm{Gal}(L_n/K) \to \mathbb{C}^\times$. Let n be the exact power of $\mathfrak{p}$ in the conductor of χ and let S_n denote a collection of integral ideals of K such that $\{\sigma_{\mathfrak{c}} \mid \mathfrak{c} \in S_n\}$ is a set of coset representatives for $\mathrm{Gal}(L_\infty/L_n)$ in $\mathcal{G}$. Define

$$\tau(\chi) = \frac{1}{p^n} \sum_{\mathfrak{b}\in S_n} \chi(\mathfrak{b})\zeta_{p^n}^{-\kappa_0(\mathfrak{b})}.$$

Proposition 15.5.

$$\tau(\chi) \cdot \sum_{\mathfrak{c}\in S_n} (\chi\phi^k)(\mathfrak{c}^{-1})\delta_{k,n}(\sigma(\beta))^0 = \int_{\mathcal{G}} (\chi\phi^k)(\sigma) d\mu_\beta^0(\sigma).$$

Proof. We just give a portion of the proof.

Define $G_n = \mathrm{Gal}(L_\infty/L_n)$.

Since χ is trivial on G_n, a change of variables with $\mu_{\sigma_{\mathfrak{c}}(\beta)}(U) = \mu_\beta(\sigma_{\mathfrak{c}}^{-1}U)$ yields:

$$\int_{\mathcal{G}} (\chi\phi^k)(\sigma) d\mu_\beta^0(\sigma) = \sum_{\mathfrak{c}\in S_n} \chi\phi^k(\mathfrak{c}^{-1}) \cdot \int_{G_n} \phi^k(\sigma) d\mu_\beta^0(\sigma)$$

From proposition 8.14, this is:

$$\sum_{\mathfrak{c}\in S_n} \chi\phi^k(\mathfrak{c}^{-1}) \cdot \frac{1}{p^n} \sum_{j=0}^{p^n-1} \mathcal{D}^k(a_\beta)(\zeta_{p^n}^j - 1) \cdot \zeta_{p^n}^{-j}$$

See [5, 4.8] for more details.

□

Proposition 15.6. *$\delta_{k,n}(\beta) = -12 \cdot \Omega_p^k \cdot E_k(\Omega_n; \Lambda, \mathfrak{a})$. ([5], II.4.10)*

Proof. Recall that $g_\beta(t) = \Theta_{\Lambda,\mathfrak{a}}(\Omega_0 - \lambda_{\hat{E}}(t))$ by Proposition 13.7. Also recall from Proposition 11.1 that the z coordinate in $\mathbb{C}/\Lambda_E$ is given by $\lambda_{\hat{E}}(t)$ (locally about $t = 0$). Also, as the formal normalized logarithm of $\hat{E}$, $\lambda'_{\hat{E}}(0) = 1$. Using $\tilde{D}$ from Definition 8.10, we calculate:

$$\mathcal{D}^k(a_\beta)(\zeta_{p^n} - 1) = \tilde{\mathcal{D}}^k \log g_\beta(t)|_{t=\theta(\zeta_{p^n}-1)}$$

$$= \Omega_p^k \cdot \frac{d^k}{dz^k} \log \Theta_{\mathfrak{a},\Lambda}(\Omega_0 - z)|_{z=\Psi^{-1}_{E^{\sigma_{\mathfrak{p}}^{-n}}}\left((\hat{\omega}_0)_n\right)=\Omega_0-\Omega_n}$$

$$= (-1)^k \Omega_p^k \cdot \left(\frac{d^k}{dz^k} \log \Theta_{\mathfrak{a},\Lambda} \right)(\Omega_n).$$

Now use the identity $E_k(\Omega_n, \Lambda, \mathfrak{a}) = \dfrac{1}{12}(-1)^{k+1} \dfrac{d^k}{dz^k} \log \Theta_{\Lambda,\mathfrak{a}}(\Omega_n)$ from Proposition 14.2.

□

A consequence of Proposition 14.7 is the following:

Proposition 15.7. *Let $k \geq 1$, $n \geq 0$, and choose a prime q, $(q, \mathfrak{f}) = 1$, such that $\mathrm{N}_{K/\mathbb{Q}}\mathfrak{q} \equiv 1 \mod \mathfrak{p}^n$, $(\mathfrak{q}, L/K) = (\mathfrak{p}^n, L/K)$. Then*

$$\Omega_p^{-k} \cdot \delta_{k,n}(\beta) =$$

$$\Omega_0^{-k} \cdot (-12)(k-1)! \cdot \phi^k(\mathfrak{p}^n) \cdot \left(\mathrm{N}(\mathfrak{a}) \cdot L^{\mathfrak{q},L_n}_{\mathfrak{f}\mathfrak{p}^n}(\bar{\phi}^k, k) - \phi^k(\mathfrak{a}) \cdot L^{\mathfrak{q}\mathfrak{a},L_n}_{\mathfrak{f}\mathfrak{p}^n}(\bar{\phi}^k, k) \right)$$

Proof. See [5, II.4.10]. □

The propositions of this section may be combined to show that the measure μ^0_β which we constructed satisfies the following (see [5, 4.11]):

Proposition 15.8. *Let ϵ be a grossencharacter of type $(k, 0)$ and conductor dividing $\mathfrak{f}\mathfrak{p}^\infty$ where n is the exact power of $\mathfrak{p}$ in this conductor. Also let $\chi = \epsilon\phi^{-k}$ (grossencharacter of type $(1, 0)$).*

Let $\mathcal{G}' = \mathrm{Gal}(K(\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^n)/K)$. Define

$$G(\epsilon) = \frac{\phi^k(\mathfrak{p}^n)}{p^n} \cdot \sum_{\substack{\sigma \in \mathrm{Gal}(K(\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^\infty)/K) \\ \sigma|_{K(\mathfrak{f}\bar{\mathfrak{p}}^\infty)} = (\mathfrak{p}^n, K(\mathfrak{f}\bar{\mathfrak{p}}^\infty)/K)}} \chi(\sigma)(\sigma(\zeta_{p^n}))^{-1}$$

Then:

$$\Omega_p^{-k} \cdot \int_{\mathcal{G}} \epsilon(\sigma) d\mu^0_\beta(\sigma) = \tag{19}$$

$$\Omega_0^{-k} \cdot 12(k-1)! \cdot G(\epsilon) \left(1 - \frac{\epsilon(\mathfrak{p})}{p}\right) \cdot (\epsilon(\mathfrak{a}) - \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})) \cdot L_{\mathfrak{f}}(\epsilon^{-1}, 0).$$

Proof. See ([5],II.4.11). The main idea is to combine the results of Propositions 15.2, 15.5, and 15.7. To adjust the partial L-functions in 15.7, one utilizes $\phi(\mathfrak{b})\bar{\phi}(\mathfrak{b}) = \mathrm{N}\mathfrak{b}$ and the summations that come from Propositions 15.2 and 15.5.

□

16. The p-adic L-function $L_{p,\mathfrak{f}}$

Definition 16.1. Let χ be a grossencharacter of type A_0 of K with infinity type (k, j). Then,

$$L_{\infty,\mathfrak{m}}(\chi, z) = \frac{\Gamma(z - \min(k,j))}{(2\pi)^{z-\min(k,j)}} L_{\mathfrak{m}}(\chi, z)$$

If χ is a grossencharacter of type $(-k,0)$, then $L_{\infty,\mathfrak{m}}(\chi,0) = \Gamma(k)L_{\mathfrak{m}}(\chi,0) = (k-1)!L_{\mathfrak{m}}(\chi,0)$.

Note that the right side of (19) may be written as a constant multiplied by an $\int_{\mathcal{G}} \epsilon d(\sigma_{\mathfrak{a}} - \mathrm{N}\mathfrak{a})$ where $\sigma_{\mathfrak{a}} - \mathrm{N}\mathfrak{a} \in \mathcal{O}_{\hat{k}^{ur}}[[\mathcal{G}]] \simeq \mathfrak{D}(\mathcal{G}, \mathcal{O}_{\hat{k}^{ur}})$.

From Definition 8.2, $\mu_\beta^0/(\sigma_{\mathfrak{a}} - \mathrm{N}\mathfrak{a})$ is a psuedo-measure and integrating ϵ with repsect to $\mu_\beta^0/(\sigma_{\mathfrak{a}} - \mathrm{N}\mathfrak{a})$ is defined as $(\int_{\mathcal{G}} \epsilon d\mu_\beta^0)/(\int_{\mathcal{G}} \epsilon d(\sigma_{\mathfrak{a}} - \mathrm{N}\mathfrak{a}))$. From (19), integration of ϵ with repsect to this pseudo-measure is independent of the choice of $\mathfrak{a}$ and is dependent only on $\mathfrak{f}$. The next proposition actually gives that this psuedo-measure (divided by 12) is actually an integral measure dependent only on $\mathfrak{f}$. We call it $\mu(\mathfrak{f})$.

Proposition 16.2. *Let $\mathfrak{a}$ be an integral ideal of K such that $(\mathfrak{a}, \mathfrak{fp}) = 1$. Let $\mu_{\mathfrak{a}}$ be the measure μ_β^0 described above and used in Proposition 15.8. The psuedo-measure $\mu_\beta^0/12(\sigma_{\mathfrak{a}} - \mathrm{N}\mathfrak{a})$ is independent of any choice of $\mathfrak{a}$ and is an integral measure. Denote this measure by $\mu(\mathfrak{f})$. It uniquely satisfies the following for any grossencharacter ϵ of type $(k,0)$ and conductor dividing $\mathfrak{fp}^\infty$:*

$$\Omega_p^{-k} \cdot \int_{\mathcal{G}(\mathfrak{f})} \epsilon(\sigma) d\mu(\mathfrak{f})(\sigma) = \Omega_0^{-k} \cdot G(\epsilon)\left(1 - \frac{\epsilon(\mathfrak{p})}{p}\right) \cdot L_{\infty,\mathfrak{f}}(\epsilon^{-1}, 0). \tag{20}$$

In particular, the objects Ω_0, Ω_p, and $\mu(\mathfrak{f}))$ uniquely satisfy (20).

Proof. (See [5],II.4.12)

□

Definition 16.3. We may thus define the p-adic L-function of modulus $\mathfrak{f}$ as

$$L_{p,\mathfrak{f}}(\epsilon) = \int_{\mathcal{G}(\mathfrak{f})} \epsilon(\sigma) d\mu(\mathfrak{f})(\sigma)$$

(for continuous ϵ in $\mathrm{Hom}(\mathcal{G}, \mathbb{C}_p)$) such that there exists $(\Omega_0, \Omega_p) \in \mathbb{C}^\times \times \mathbb{C}_p^\times$ such that $\mu(\mathfrak{f})$ satisfies:

$$\Omega_p^{-k} \cdot L_{p,\mathfrak{f}}(\epsilon) = \Omega_0^{-k} \cdot G(\epsilon)\left(1 - \frac{\epsilon(\mathfrak{p})}{p}\right) \cdot L_{\infty,\mathfrak{f}}(\epsilon^{-1}, 0)$$

for any grossencharacter ϵ of type $(k,0)$ and conductor dividing $\mathfrak{fp}^\infty$.

This condition determines the measure $\mu(\mathfrak{f})$.

References

[1] B. Gross, *Arithmetic of elliptic curves with complex multiplication*, Springer-Verlag, 1980.
[2] Michiel Hazewinkel, *Formal Groups and Applications*, New York: Academic Press, Inc., 1978.
[3] Kenkichi Iwasawa, *Local Class Field theory*, New York: Oxford University Press, 1986.
[4] Serge Lang, *Cyclotomic Fields I and II*, New York: Springer-Verlag, 1990.
[5] Ehud de Shalit, *Iwasawa Theory of Elliptic Curves with Complex Multiplication*, Orlando: Academic Press Inc., 1987.
[6] J.P. Serre and J. Tate, "Good Reduction of Abelian Varieties," Ann. Math. **88** (1968), 492-517.
[7] Goro Shimura, *Introduction to the Theory of Automorphic Functions*,Iwanami Shoten Publishers and Princeton University Press, 1971.
[8] Joseph H. Silverman, *The Arithmetic of Elliptic Curves 2nd Edition*, New York: Springer, 1986.
[9] Joseph H Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, New York: Springer-Verlag, 1994.